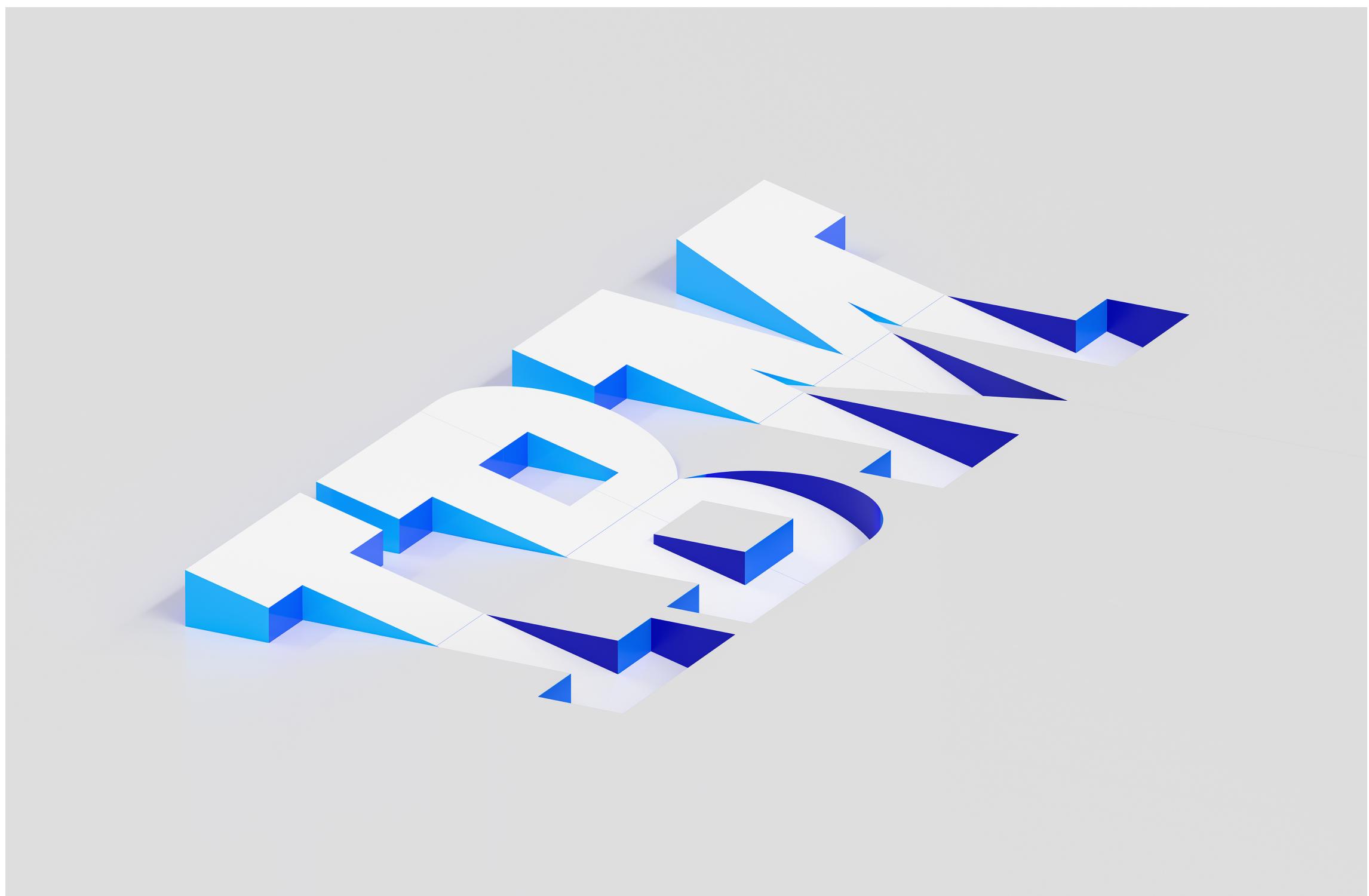


IBM Cloud for SAP | IBM Power Virtual Servers for SAP

Solution guide



Edition notices

This PDF was created on 2025-06-03 as a supplement to *IBM Cloud for SAP / IBM Power Virtual Servers for SAP* in the IBM Cloud docs. It might not be a complete set of information or the latest version. For the latest information, see the IBM Cloud documentation at <https://cloud.ibm.com/docs/sap>.

Get started

IBM Cloud® for SAP is the continuation of a 50+ year IBM-SAP alliance across hardware, software, and services.

With over 60 IBM data centers worldwide, the IBM Cloud® SAP-Certified Infrastructure gives you the flexibility to run your SAP workloads in the IBM Cloud when and where you need them. You can quickly address issues such as:

- Rapidly expanding or contracting capacity
- Moving SAP workloads to the cloud
- Supplementing an existing private cloud architecture.

The following documentation provides design considerations and guidance for provisioning the infrastructure to support SAP workloads, including:

- SAP Business Applications such as SAP S/4HANA or SAP BW/4HANA
- SAP Technical Applications such SAP HANA database server and SAP NetWeaver application server

You can use this information to help planning your SAP installation and running your SAP workloads on IBM Cloud.

The following documentation does not replace any SAP implementation-related documentation.

Before you begin

Before you install the SAP software components on IBM Cloud, you need an:

- SAP S-User ID to review the relevant SAP documentation and download SAP installation media
- IBM ID to create an IBM Cloud account

Summary of an SAP landscape installation onto Cloud IaaS

This table summarizes the SAP landscape installation steps for you and your team:

Task	Details
Read the Overview of IBM Cloud® for SAP	Identify the various offerings that are available for your SAP landscape. Provides a high-level comparison of your options.
Read the relevant documents in the following topic groups:	<ul style="list-style-type: none">• Infrastructure environments section for your specific environment, such as IBM Power Systems Infrastructure environment introduction• Infrastructure certified for SAP• Sizing process for SAP Systems <p>Read these documents to identify the detailed infrastructure options and design considerations that apply to your SAP landscape.</p>
Read the relevant SAP software documentation.	Short lists of planning considerations are available to assist under topic groups: <ul style="list-style-type: none">• SAP Business Applications• SAP Technical Applications• SAP AnyDB databases <p>Lists of usage, network, storage, database, and OS considerations are available for SAP Business Applications, SAP Technical Applications, SAP AnyDB databases, SAP Development Applications. References to SAP installation documents are also included.</p>
<i>Optional:</i> Read the relevant SAP Business Partner certified solutions documents	Various SAP Open Ecosystem Partners are available from IBM Cloud, with documents on how to best use these solutions for your SAP deployment.
<i>Optional:</i> Read the relevant IBM-SAP innovation solutions documents	IBM Cloud® for SAP

Read and follow the documents in the Pre-requisites for SAP Workloads topic group	Prepare the credentials, account structure, connectivity, software downloads, support procedures, and licensing that is needed before you begin your deployment.
Read and follow the Provisioning topic groups in the How to section	For your specific infrastructure, follow the provisioning guidelines to set up the first servers at the sizes that are required to run your SAP systems. Planning your SAP landscape with the business is crucial to success. It is likely these documents might be read many months after the topics listed in the other steps.
Revisit Task 3 , and follow the relevant SAP software documentation to install SAP on the infrastructure	It is important to follow SAP guidance clearly, including any additional reference guidance available on SAP Notes for your chosen applications. This stage is the same as installations into servers hosted at on-premises data centers.

Overview of your SAP landscape installation steps

Next steps

Review the following documentation at for your relevant configuration:

- [Fast Path of IBM Cloud Intel Bare Metal on Classic Infrastructure](#)
- [Fast Path of IBM Cloud Intel Bare Metal Servers on VPC Infrastructure](#)
- [Fast Path of IBM Cloud Intel Virtual Servers on VPC Infrastructure](#)
- [Fast Path of IBM Power Virtual Servers](#)
- [Fast Path of IBM Cloud for VMware on Classic Infrastructure](#)

Overview of IBM Cloud® for SAP

Introduction

IBM Cloud® for SAP is for enterprises who believe that empowering their SAP workloads also empowers their business. IBM Cloud® for SAP provides your enterprise with full cloud capabilities. So, you can run your mission-critical SAP workloads with secure, reliable, and compliant infrastructure, and take advantage of options to append more cloud services to transform the business.

Our IBM Cloud® for SAP offerings are designed based on over 50+ years of IBM-SAP expertise (since 1972). The on-demand flexible compute options for various SAP Business Application scenarios range from cloud-native SAP and burst compute all the way to high performance with enterprise-grade availability.

IBM and SAP multi-decade alliance is why IBM was selected as one of SAP's strategic infrastructure providers for hybrid cloud. Support for SAP's suite of products is available through the highly scalable, open, and security-rich IBM Cloud. With this partnership, SAP applications can expand to major markets; this expansion is made possible by more than 60 IBM Cloud data centers worldwide.

IBM Cloud® for SAP was launched in late 2014, with our SAP HANA certified Bare Metals as a strategic partner with SAP HANA Enterprise Cloud (HEC). Our SAP HANA certified Bare Metals were first released as Infrastructure-as-a-Service in early 2017, the first Cloud Service Provider to provide high-performance Bare Metal IaaS for SAP HANA and SAP NetWeaver.

Using various configurations of the SAP Technical Applications, you can confidently run SAP Business Applications such as:

- SAP S/4HANA
- SAP BW/4HANA
- SAP BO-BI
- SAP CAR
- ...more

Our rigorous certification process with SAP make sure that your workloads are supported.

We deliver these cloud capabilities for SAP to improve your business, and provide more solutions from SAP Partners to accelerate your SAP implementations.

IBM provides you with the most powerful available cloud building blocks so that you can design and implement SAP landscapes that meet your current business needs and your requirements for the future.

Our infrastructure options are designed to support all your SAP workloads in different scenarios, including business applications based on:

- SAP HANA
- SAP AnyDB
- SAP NetWeaver
- Other SAP products that use other technologies (for example, older applications such as SAP Content Server, or newer applications such as SAP Data Intelligence)

Our key offerings are SAP-certified Infrastructure-as-a-Service, which we append with more capabilities specific to SAP workloads.

Supported SAP Business Applications

- SAP S/4HANA AnyPremise edition
- SAP S/4HANA Cloud SaaS Extended edition (by request to SAP)
- SAP BW/4HANA
- SAP CAR
- SAP Commerce (formerly SAP Hybris Commerce)
- SAP ECC
- SAP BW
- SAP Business One
- SAP Business Objects Business Intelligence Suite (BOBJ/BO-BI)
- SAP Data Intelligence 3.x / SAP Data Hub 2.x
- ...more

Supported SAP Technical Applications

- SAP HANA
- SAP NetWeaver
- SAPRouter
- SAP Web Dispatcher
- SAP Fiori Front-end Server
- SAP Gateway
- SAP Solution Manager
- SAP Content Server
- Adobe Document Services (ADS) for SAP
- SAP Process Orchestration (PO) - Process Integration (PI)
- SAP Landscape Management (LaMa)
- SAP Secure Logon Server (SLS)
- AnyDB - IBM Db2
- AnyDB - Microsoft SQL Server
- AnyDB - SAP MaxDB
- AnyDB - SAP ASE
- ...more

Supported SAP Development Applications

SAP Business Technology Platform (BTP) (including SAP Cloud Connector)

SAP-certified Infrastructure-as-a-Service (IaaS) offerings

The IBM Cloud SAP-Certified IaaS gives you the flexibility to run your SAP workloads in the IBM Cloud when you need them, where you need them with over 60 IBM data centers worldwide. You can quickly address issues such as:

- Rapidly expanding and contracting capacity (as needed)
- Migrating SAP workloads to the cloud
- Supplementing existing on-premises virtualized infrastructure architectures.

The IBM Cloud® for SAP portfolio primarily consists of five offerings:

1. IBM Cloud Bare Metal
2. IBM Cloud Bare Metal with Intel Optane DC Persistent Memory
3. IBM Cloud Virtual Servers
4. IBM Power Virtual Servers (complementary offering from IBM Power Systems, with connection through IBM Cloud)
5. IBM Cloud for VMware

More information on the Infrastructure offerings within the IBM Cloud® for SAP portfolio, see [Infrastructure certified for SAP](#).

These offerings are spread across two primary infrastructure environments, and one separated environment that uses IBM Power technologies:

- [IBM Cloud Classic Infrastructure environment](#). The original environment and network, formerly known as the Softlayer network.
- [IBM Cloud VPC Infrastructure environment](#). The latest environment and network, with the newest technologies and networking capabilities.
- [IBM Power Systems Infrastructure environment](#). The environment maintained by IBM Power Systems built of IBM Power enterprise components, which has links to either Classic Infrastructure and VPC Infrastructure.



Tip: Our documents provide detailed considerations and information for building your SAP environments at each layer for all offerings. However, if you are interested in quickly finding the information related specifically to one of the IaaS offerings, then you may consider using the Fast Path Site Maps for [Intel Bare Metal](#), [Intel Virtual Servers](#), and [IBM Power Virtual Servers](#) and [VMware SDDC](#).

Certifications summary

- SAP S/4HANA (AnyPremise edition), which uses SAP HANA scale-up.
- SAP BW/4HANA, which uses SAP HANA scale-up.
- SAP BW/4HANA, which uses SAP HANA scale-out.



Note: For more details on SAP S/4HANA scale-out with IBM Cloud, read [SAP S/4HANA additional design considerations](#), which describes while this is possible, IBM-SAP prefer to discuss first to understand the business requirements. This is to avoid transactional performance issues, which may occur with SAP S/4HANA scale-out.

Benchmarks summary

- SAP S/4HANA (AnyPremise edition), which uses SAP HANA scale-up (world record, as of writing - 2020-07-01).
- SAP BW/4HANA, which uses SAP HANA scale-up (world record, as of writing - 2020-07-01)
- SAP BW/4HANA, which uses SAP HANA scale-out

SAP's Platform-as-a-Service (PaaS) offerings

IBM Cloud also enables the use of cloud-native SAP technologies. IBM-SAP work on multiple open source projects together and both companies use similar technology underpinnings. You can reduce your SAP implementation project timelines and long-term maintenance by adopting the "Side-by-Side Extensibility" model that SAP recommends for custom development with their SAP Business Applications.

The portfolio includes a variation of SAP's Platform-as-a-Service, which is designed for increased security of cloud-native SAP extensions. This SAP PaaS variation can be combined with IBM Cloud's various PaaS options, functions, and services.

Affiliate offerings for SAP's PaaS by request only:

- SAP Business Technology Platform (BTP) Private Edition, using Red Hat OpenShift Virtualization

However, the core cloud-native SAP technologies are able to be used directly with Red Hat OpenShift on IBM Cloud or other IBM Cloud capabilities (such as Cloud Foundry) in the same way as deploying to SAP Business Technology Platform (BTP). This is because many of the cloud-native SAP technologies are built upon widely supported cloud-native technologies. However, to deploy outside of the SAP Business Technology Platform (BTP) ecosystem requires general knowledge of cloud-native technologies, and will require more manual effort (not described in this documentation series) because the SAP multitarget application (MTA) archive format is not supported outside SAP Business Technology Platform (BTP).

Cloud-native SAP technologies which are portable, directly to Red Hat OpenShift on IBM Cloud or Cloud Foundry from IBM Cloud, examples include:

- [SAP Fundamental Library Styles component library](#) for UI Frameworks (Angular, React, Vue, and other frameworks)
- [SAPUI5 Framework](#) (and upstream project [OpenUI5](#))

SAP's Software-as-a-Service (SaaS) offerings

IBM Cloud is also available as an option underneath SAP's Software-as-a-Service (SaaS) products.

IBM Cloud offerings for SAP's SaaS by request only:

SAP S/4HANA Cloud SaaS, Extended Edition; using IBM Cloud SAP-certified IaaS _(IBM Cloud is a strategic premier partner, requires PMC contract with a services partner)

SAP Partner ecosystem solutions offerings

IBM Cloud provides numerous solutions from SAP's Partner ecosystem. These solutions can reduce SAP implementation project timelines or increase the efficiency of SAP Systems that are running maintenance on IBM Cloud. IBM Cloud works closely with these SAP Partners (who are also IBM Business Partners) to offer their capabilities from the IBM Cloud catalog.

These solutions from SAP Partners may not apply to all SAP software or all Infrastructure within the IBM Cloud® for SAP portfolio; please see the individual sections under the *SAP Partner certified solutions* topic group.

This table summarises the available SAP Partner solutions:

SAP Partner	Solution name	Solution description
Veeam	Veeam Backup & Replication for SAP HANA	Backint backups from SAP HANA

Comparing the different SAP-certified IaaS offerings

When you compare the different SAP-certified IaaS offerings available on IBM Cloud, keep in mind that each offering was designed to provide flexibility for various scenarios. Each offering provides different levels of performance criteria, security, and risk-acceptance.

Each of these SAP-certified offerings is available to support numerous different SAP Business or SAP Technical Applications. However they differ in the performance they can achieve:

- Bare Metal very offers high performance. This option has no software-related overheads as it is purely an OS and the SAP software that uses local SSD storage. However, the SAP workload cannot move around as easily.
- Intel Virtual Servers for VPC uses an IBM Cloud managed hypervisor. This option provides lower total cost of ownership when coupling Suspend Discounts and Sustained Usage Discounts, with more flexibility and an abundance of extra features for security and networking. However, the performance and sizing are lower than other options.
- IBM Power Virtual Servers use the enterprise-grade IBM PowerVM Type 1. This option is a complementary offering from IBM Power Systems, with connection through IBM Cloud, that provides significant scalability on robust hardware with significant flexibility and many more features available. But, this option does not allow root-access control of IBM PowerVM underneath where some SAP tools would ordinarily provide integration.
Commonly this is paired with existing IBM Power or IBM Z infrastructure in on-premises data centers, to create a Hybrid Cloud model which drives modernization using paired capabilities from either on-premises or Cloud that address the business needs (e.g. security, flexibility, speed etc.) and business strategy
- VMware is a Type 2 hypervisor. This option has a minor reduction in the available performance. But this option also has vastly more flexibility and optimization in running SAP workloads, including:
 - Full root-access control to all VMware features
 - Capability to install more software that uses VMware capabilities (for example, SAP Landscape Management)
 - Ability to bridge the network with any existing VMware installations

This content is a high-level summary, for more details please see [Infrastructure certified for SAP](#); in addition there are multiple pages describing each profile available across the infrastructure options.

Our recommendation is to investigate what your current business requirements are and what are your future requirements for growth. This information helps you understand the short-term and long-term needs for running your SAP Systems. After you know your short-term and long-term needs, complete an SAP Sizing exercise.

This exercise provides you with enough information to establish what IaaS and surrounding needs you might have, which can help to evaluate decision points such as:

- Whether to move the existing SAP workload to cloud quickly or steadily (for example, avoid data center expiry fees versus potential business disruption)
- Whether to migrate the existing SAP ECC system to SAP S/4HANA, or build from the ground up on the cloud.
- What your current sizings of your SAP Systems are, and their projected increases.
- How to align your move to cloud and SAP rollouts to meet business needs. For example, connectivity to existing applications in on-premises data centers, intermittent or offline locations such as factories or front-line business operators, mobile device connectivity while retaining security and more.

The following documentation sections provide details to help understand how IBM Cloud® for SAP can empower your business and help you to make informed decisions for your IaaS, PaaS, SaaS, and SAP Partner solution choices.

Release notes

Use these release notes to learn about the latest updates to SAP on IBM Cloud.

May 2025

- You can deploy [SAP Application Server/SAP NetWeaver sr2 profiles](#) on IBM Power Virtual Servers.
- New documentation: [Custom OS image build process](#) on RHEL for SAP solutions on IBM Power Virtual Server.
- New documentation: [SAP NetWeaver with Db2](#) on RHEL x86_64 Virtual Server Instance in IBM Cloud VPC.

April 2025

- Enhanced the [fast path for Power Virtual Server](#) with improved headings, intuitive navigation, and enriched informational content.
- Introduced 3 new [x86_64 Bare Metal certified profiles](#) for SAP HANA on IBM Cloud Classic.
- Introduced 12 new [x86_64 VSI certified profiles \(vx3*\)](#) for SAP HANA on IBM Cloud VPC.

March 2025

- **New SAP HANA database profiles:** Introduced [ch2 and bh2 certified profiles](#) for SAP HANA database on IBM Power10 machines.
- **Migration options:** New documentation on [migration paths](#) for transitioning from on-premises environments to Power Virtual Server.
- **High availability best practices:** New documentation on [implementing high availability](#) scenarios for Power Virtual Server.
- **Backup strategies:** New documentation on [comprehensive backup strategies](#) for SAP HANA database on Power Virtual Server.
- **SAP workload monitoring:** Learn how to [monitor SAP workloads](#) using IBM Cloud Monitoring instance and Prometheus server.
- **VPC File Storage tutorial:** New [tutorial](#) for accessing VPC file storage shares from Power Virtual Server instances.

Fast path site maps

Fast Path of IBM Cloud Intel Virtual Servers on VPC Infrastructure

This page is a collection of shortcuts to the documentation sections for each offering, excluding general information that applies to all offerings, such as SAP Sizing.

Use the links in this section to quickly access relevant documents that you are already familiar with.

Learn

An Infrastructure-as-a-Service (IaaS) environment consists primarily of compute, storage, and network components from a specified region (such as the US) and a designated site location (also referred to as zone, which is a data center site). For more information:

- [IBM Cloud VPC Infrastructure environment introduction](#)

Certified Infrastructure-as-a-Service for SAP HANA database server is available in many variations, each with different capabilities and sizes to fit many different SAP workload scenarios. For more information:

- [Infrastructure certified for SAP - IBM Intel Virtual Server](#)

The following is an overview of the SAP-certified profiles with IBM Power Virtual Servers for SAP HANA and SAP NetWeaver. For more information:

- [IBM Cloud Intel Virtual Server certified profiles for SAP HANA](#)
- [IBM Cloud Intel Virtual Server certified profiles for SAP NetWeaver](#)
- [Compute Profiles of SAP-certified IBM Cloud Intel Virtual Server](#)

Your business and functional requirements determine the SAP solutions powered by the SAP HANA Database Server or SAP NetWeaver Application Server, and therefore determine how your applications are run in the available infrastructure. For more information:

- [Connectivity options within the IBM Cloud VPC Infrastructure network](#)
- [Bring-your-own network \(Subnet/CIDR/IP address range\) - VPC Infrastructure](#)
- [Networking Traffic Segregation security considerations - VPC Infrastructure separation of subnets](#)

Your enterprise IT organization can select from a variety of operating systems from the IBM Cloud for SAP portfolio. For more information:

- [OS Bring your Own Image/License for VPC Infrastructure](#)

Tutorials

- [SAP NetWeaver deployment to Intel Virtual Server on VPC Infrastructure that uses RHEL](#)

How To

Provisioning IBM Cloud Virtual Servers for SAP HANA and SAP NetWeaver:

- [Planning your deployment](#)
- [Deploying your infrastructure](#)
- [Using IBM Metrics Collector for SAP \(IMCS\) on Linux](#)

Help

- [Requesting support for SAP-certified IBM Cloud Intel Virtual Servers](#)
- [SAP ONE Support process](#)
- [FAQ - IBM Cloud for SAP](#)

Fast Path of IBM Cloud Intel Bare Metal Servers on VPC Infrastructure

This topic is a collection of shortcuts to the documentation sections for each offering, excluding general information that applies to all offerings, such as SAP Sizing.

Use the links in this section to quickly access relevant documents that you are already familiar with.

Learn

An Infrastructure-as-a-Service (IaaS) environment consists primarily of compute, storage, and network components from a specified region (such as the US) and a designated site location (also referred to as zone, which is a data center site). For more information:

- [IBM Cloud VPC Infrastructure environment introduction](#)

Certified Infrastructure-as-a-Service for SAP is available in many variations, each with different capabilities and sizes to fit many different SAP workload scenarios. For more information:

- [Infrastructure certified for SAP - Intel Bare Metal servers on VPC Infrastructure](#)

The following is an overview of the SAP-certified profiles with IBM Cloud Bare Metal servers for SAP HANA and SAP NetWeaver. For more information:

- [IBM Cloud Intel Bare Metal Server certified profiles for SAP HANA](#)
- [IBM Cloud Intel Bare Metal Server certified profiles for SAP NetWeaver](#)
- [Compute Profiles of SAP-certified IBM Cloud Bare Metal Server](#)

Therefore, your business and functional requirements determine the SAP solutions powered by the SAP HANA Database Server or SAP NetWeaver Application Server, and how your applications are run in the available infrastructure. For more information:

- [Connectivity options within the IBM Cloud VPC Infrastructure network](#)
- [Bring-your-own network \(Subnet/CIDR/IP address range\) - VPC Infrastructure](#)
- [Networking Traffic Segregation security considerations - VPC Infrastructure separation of subnets](#)

Your enterprise IT organization can select from various operating systems from the IBM Cloud for SAP portfolio. For more information:

- [OS Bring your Own Image/License for VPC Infrastructure](#)

How To

Provisioning IBM Cloud Virtual Servers for SAP HANA and SAP NetWeaver:

- [Planning your deployment](#)
- [Deploying your infrastructure](#)

Help

- [Requesting support for SAP-certified IBM Cloud Bare Metal Servers](#)
- [SAP ONE Support process](#)
- [FAQ - IBM Cloud for SAP](#)

Fast Path of IBM Cloud Intel Bare Metal on Classic Infrastructure

This page is a collection of shortcuts to the documentation sections for each offering, excluding general information that applies to all offerings, such as SAP Sizing.

Use the links in this section to quickly access relevant documents that you are already familiar with.

Learn

An Infrastructure-as-a-Service (IaaS) environment consists primarily of compute, storage, and network components from a specified region (such as the US) and a designated site location (also referred to as zone, which is a data center site). For more information:

- [IBM Cloud Classic Infrastructure environment introduction](#)

Certified Infrastructure-as-a-Service for SAP HANA database server is available in many variations, each with different capabilities and sizes to fit many different SAP workload scenarios. For more information:

- [Infrastructure certified for SAP - Bare Metal server](#)

The following is an overview of the SAP-certified profiles with IBM Cloud Bare Metal servers for SAP HANA and SAP NetWeaver. For more information:

- [Intel Bare Metal server certified profiles for SAP HANA](#)
- [Intel Bare Metal server certified profiles for SAP NetWeaver](#)
- [Compute Profiles of SAP-certified Bare Metal on Classic Infrastructure](#)

Your business and functional requirements determine the SAP solutions powered by the SAP HANA Database Server or SAP NetWeaver Application Server, and therefore determine how your applications are run in the available infrastructure. For more information:

- [Connectivity options within the IBM Cloud Classic Infrastructure network](#)
- [Sample storage configurations on Classic Infrastructure](#)

Your enterprise IT organization can select from a variety of operating systems from the IBM Cloud for SAP portfolio. For more information:

- [OS Bring your Own Image/License for IBM Cloud Intel Bare Metal](#)

Depending on your scenarios, the following information may be also relevant:

- [SAP NetWeaver - Configure high availability in Classic Infrastructure](#)
- [SAP on IBM Db2 using Intel Bare Metal](#)
- [SAP MaxDB using Intel Bare Metal](#)

Tutorials

- [SAP NetWeaver deployment to Bare Metal on Classic Infrastructure, using RHEL](#)
- [SAP NetWeaver deployment to Bare Metal on Classic Infrastructure, when you are using Windows Server](#)

How To

Provisioning IBM Cloud Bare Metal server for SAP HANA and SAP NetWeaver:

- [Planning your deployment](#)
- [Deploying your infrastructure](#)

Help

- [Requesting support for SAP-certified IBM Cloud Bare Metal servers](#)
- [SAP ONE Support process](#)
- [FAQ - IBM Cloud for SAP](#)

Fast Path of IBM Cloud for VMware on Classic Infrastructure

This page is a collection of shortcuts to the documentation sections for each offering, excluding general information that applies to all offerings, such as SAP Sizing.

Use the links in this section to quickly access relevant documents that you are already familiar with.

Learn

An Infrastructure-as-a-Service (IaaS) environment consists primarily of compute, storage, and network components from a specified region (such as the US) and a designated site location (also referred to as zone, which is a data center site). For more information:

- [IBM Cloud Classic Infrastructure environment introduction](#)

Certified Infrastructure-as-a-Service for SAP HANA database server is available in many variations, each with different capabilities and sizes to fit many different SAP workload scenarios. For more information:

- [Infrastructure certified for SAP - VMware Software-Defined Data Center](#)

The following is an overview of the SAP-certified profiles with IBM Cloud Bare Metal servers for SAP HANA and SAP NetWeaver. For more information:

- [VMware SSDC certified profiles for SAP HANA](#)
- [VMware SSDC certified profiles for SAP NetWeaver](#)
- [Compute Profiles of SAP-certified VMware on Classic Infrastructure](#)

Your business and functional requirements determine the SAP solutions powered by the SAP HANA Database Server or SAP NetWeaver Application Server, and therefore determine how your applications are run in the available infrastructure. For more information:

- [Connectivity options within the IBM Cloud Classic Infrastructure network](#)
- [Bring-your-own network \(Subnet/CIDR/IP address range\) - Classic Infrastructure with VMware](#)
- [Networking Traffic Segregation security considerations - VMware on classic infrastructure separation of subnets](#)

Your enterprise IT organization can select from a variety of operating systems from the IBM Cloud for SAP portfolio. For more information:

- [OS Bring your Own Image/License for VMware SDDC](#)

How To

Provisioning VMware SDDC for SAP HANA and SAP NetWeaver:

- [Planning your deployment](#)
- [Deploying your infrastructure](#)

Help

- [Requesting support for SAP-certified VMware SDDC](#)
- [SAP ONE Support process](#)
- [FAQ - IBM Cloud for SAP](#)

Fast path of IBM Power Virtual Server

Use this collection of shortcuts for rapid access to key documentation about SAP solutions on IBM Power Virtual Server.

Overview

An Infrastructure-as-a-Service (IaaS) environment consists primarily of compute, storage, network, and virtualization components from a specified region (such as the US) and a designated zone or data center. For more information, see [Architecture for IBM Power Virtual Server in IBM data center](#). For information about the zones, see [IBM Cloud regions](#).

Planning

SAP solution architecture

Your business and functional requirements determine the scope for your SAP solutions. Consider your nonfunctional requirements in addition, and map the application components to the infrastructure components.

Refer to [Connectivity options within the IBM Power Virtual Server network, connection through IBM Cloud](#)

Deployment

- Compute
 - [Sizing process for SAP Systems](#)
 - [Mapping CPUs derived from SAPS to an IBM Power Virtual Server](#)
 - [SAP HANA certified instances on IBM Power Virtual Server](#)
 - [SAP NetWeaver certified instances on IBM Power Virtual Server](#)
 - [OS for IBM Power Virtual Servers](#)
 - [Bring-your-own-OS \(custom OS image and BYOL License\)](#)
- Storage
 - [General storage configurations on IBM Power Virtual Server Infrastructure](#)

High availability

- [Implementing high availability for SAP applications on IBM Power Virtual Server](#)

Disaster recovery

- [Planning Disaster Recovery for SAP solutions on IBM Cloud](#)

Tutorials

Deployment

- [Accessing File Storage for VPC from IBM Power Virtual Server instances](#)

How to

Deployment

- Preparing the deployment
 - [Planning your deployment](#)
 - [Deploying IBM Cloud VPC infrastructure for Power Virtual Server workloads](#)
 - [Deploying SAP Power Virtual Server workloads](#)
- Running the deployment
 - [Deploying SAP applications on Power Virtual Server](#)
 - [SAP license key with IBM Power Systems Virtual Servers](#)

High availability

- General preparation steps
 - [Creating instances for a high availability cluster](#)
- Cluster deployment in a single Power Virtual Server workspace
 - [Implementing a Red Hat Enterprise Linux High Availability Add-On cluster](#)
 - [Configuring SAP HANA scale-up system replication in a Red Hat Enterprise Linux High Availability Add-On cluster](#)
 - [Configuring SAP HANA cost-optimized scale-up system replication in a Red Hat Enterprise Linux High Availability Add-On cluster](#)
 - [Configuring SAP HANA active/active \(read enabled\) system replication in a Red Hat Enterprise Linux High Availability Add-On cluster](#)
 - [Configuring SAP HANA multitier system replication in a Red Hat Enterprise Linux High Availability Add-On cluster](#)
 - [Configuring SAP HANA multitarget system replication in a Red Hat Enterprise Linux High Availability Add-On cluster](#)
 - [Configuring high availability for SAP S/4HANA \(ASCS and ERS\) in a Red Hat Enterprise Linux High Availability Add-On cluster](#)
 - [Configuring an active-passive NFS server in a Red Hat Enterprise Linux High Availability Add-On cluster](#)
- Cluster deployment in a multizone region environment
 - [Implementing a Red Hat Enterprise Linux High Availability Add-On cluster in a multizone region environment](#)
 - [Configuring high availability for SAP S/4HANA \(ASCS and ERS\) in a Red Hat Enterprise Linux High Availability Add-On cluster in a multizone region environment](#)

Backup and restore

- [Backup strategies for SAP HANA on IBM Power Virtual Server](#)

Monitoring

- Overview
 - [Getting started with IBM Cloud Monitoring for SAP systems](#)
 - [Monitoring for IBM Power Systems Virtual Servers](#)
- Setting-up
 - [Prerequisites](#)
 - [Creating a monitoring instance in IBM Cloud®](#)
 - [Setup and configuration of a monitoring host](#)
 - [Configuration of Prometheus server metric forwarding](#)
 - [Launching the monitoring UI and working with dashboards](#)

Migration

- [Overview - Migrating SAP servers between on-premises and IBM Cloud® on IBM Power Virtual Server](#)
- [Hybrid Cloud Network Consideration for SAP applications on IBM Power Virtual Server](#)
- [Migrating SAP S/4HANA to IBM Power Virtual Server](#)
- [Migrating SAP ERP 6.0 with Oracle to IBM Power Virtual Server](#)
- [Migrating SAP ERP 6.0 with IBM Db2 to IBM Power Virtual Server](#)
- [Migrating from SAP ERP 6.0 to S/4HANA to IBM Power Virtual Server](#)

Help

- [Getting help and support from IBM Cloud or SAP](#)
- [SAP-certified IBM Power Virtual Servers](#)

Infrastructure environments

IBM Cloud® Virtual Private Cloud (VPC) Infrastructure environment introduction

An Infrastructure-as-a-Service (IaaS) environment consists of many components - primarily compute, storage, and network from a specified region (such as the US) and a designated site location (also referred to as a zone), which is a data center site.

Deployment and management

IBM Cloud VPC Infrastructure offerings, such as virtual or bare metal servers, are deployed through the [IBM Cloud VPC Infrastructure console](#).

Alternatively, deployments can be made and managed by using:

- IBM Cloud CLI
- IBM Cloud VPC Infrastructure API calls that use an IBM Cloud API key
- [Terraform Provider for IBM Cloud](#) by using an IBM Cloud API key

For more information, see [Managing VPC Infrastructure \(IAM\)](#).

Locations - availability zones

With availability zones across North and South America, Europe, Asia, and Australia, you can provision cloud resources where (and when) you need them. Many regions are available globally, with multiple availability zones in each region. Each availability zone is connected to the IBM Cloud global private network, making data transfers faster and more efficient anywhere in the world.

For more information about IBM Cloud availability zones, data centers, and Points of Presence (PoPs), see the [global regions, availability zones, and data centers map](#).

Compute Resources

Two types of compute resource can be deployed in IBM Cloud VPC Infrastructure environment:

- Intel Virtual Server Instances (VSIs)
- Intel Bare Metal Servers

These compute resources are offered in different profiles that define CPU and RAM combinations.

For more information, see [Infrastructure certified for SAP](#).

Networking

The IBM Cloud VPC infrastructure network, is robust, secure, and flexible; powered by the latest in networking hardware, with the best networking capabilities. It allows definable isolation and creation of a network within the cloud.

IBM Cloud VPC Infrastructure network

Global

Region

VPC

Availability zone (with address prefix)

Subnet

Networking component layers overview

Every IBM Cloud® Virtual Private Cloud is created for a region, and spans multiple availability zones.

When you deploy a VPC in an availability zone, an [address prefix](#) is used for that specified zone.

Each VPC Zone (and the address prefix) contains one or more subnets. You can define each subnet manually by choosing the IP range and the subnet mask, or you can choose the number of IP addresses needed. A newly created compute resource is deployed into this subnet and can also be attached to further subnets.

Networking connectivity

[IBM Cloud® Virtual Private Cloud network overview](#) demonstrates the connectivity for the environment. Issues with network connectivity can cause delays for your project if you do not plan properly, regardless of how you plan to use your system.

In general, IBM Cloud VPC has a highly available, high-bandwidth network that is connected to every compute resource, be it bare metal servers or physical servers, which, in the VSI case, serve a hypervisor. Each physical server (host), which serves a hypervisor, divides the network into virtual network interfaces (vNICs) that are attached to the virtual server.

Depending on the profile of your virtual server, the total available network bandwidth to the virtual server is in the range of 4 Gbps to 64 Gbps. It's important to consider that each vNIC has a maximum throughput of 16 Gbps, so to achieve maximum throughput, up to 4 additional vNICs must be attached to the virtual server (that is, a virtual server might have a maximum of 5 vNICs attached).

If you need to connect to your virtual or bare metal server through the public internet (also known as inbound to a server), you can order a *Floating IP* and attach to the server's vNIC, in other words: you can attach one *Floating IP* per server.

If you want to connect to the public internet from your server (also known as outbound from a server), you need to attach a *Public Gateway* to the VPC. This gateway provides access to the internet for an entire subnet.

The following inter-connectivity options are available:

- VPC zone to zone,
- VPC to VPC,
- VPC to Classic Infrastructure,
- VPC to IBM Power Systems Infrastructure,
- VPC to on-premises data centers by using a VPC VPN Gateway

When a connection to the public internet is not acceptable because of security measures, you can deploy an IPsec Gateway into your VPC to connect to your server. For more information, see [Connectivity to your SAP system landscape - VPC VPN Gateway](#). Or, you can have an even closer integration into your backbone infrastructure by an IBM Cloud Direct Link. For more information, see [Connectivity to your SAP system landscape - IBM Cloud Direct Link](#).

Server resources that are in IBM Cloud Classic Infrastructure can be connected through *Transit Gateways*. These virtual devices are used to connect your private VLAN subnets in the *Classic Infrastructure* to your VPC subnets.

For more information, see [About Networking for VPC](#) and [Setting up access to classic infrastructure](#).



Important: Extra requirements exist in Classic Infrastructure networking to enable the *Transit Gateway*, be sure to review documentation before you change your Classic Infrastructure or VPC Infrastructure networking topology and configuration.



Note: It is advised that your networking department contact [IBM Cloud Support](#) after determining the layout of your landscape and the connectivity that is required on the SAP application layer.

Networking protection

IBM Cloud® offers further protection mechanisms that can provide your Virtual Servers for VPC with a layer of security that you can configure and adapt anytime. Two key principles are:

- **Network Access Control Lists (ACL)**: Available for use by all subnets in all zones. ACLs attach to a subnet and provide subnet-level protection by limiting a subnet's inbound and outbound traffic.
- **Security Groups**: Available for use by all subnets on all zones that are attached to a vNIC of any server that provides instance-level protection by acting as a firewall to restrict a vNIC inbound and outbound traffic.

For more information, see [Security in your VPC](#).

Subnets to separate traffic

If you want to separate different network traffic types in your landscape, either because of security restrictions or because of throughput considerations, you can configure and attach multiple subnets to your VPC and make them available to your compute resources, too.

Network Access Control List

Network Access Control Lists (ACLs) are used to manage `allow` and `deny` rules on a subnet level. ACLs are used to manage network traffic between subnets, too. The default ACL for a subnet opens the subnet for all traffic. If you wanted more strict security measures, you would need to add rules to the ACL. When you add rules, keep in mind that required services like DNS or OS patch and packages downloads might be affected by those rules. For more information, see [Security in your VPC](#).

Security Groups

A Security Group is a set of *allow-only* firewall rules. You can apply these rules to one or more bare metal servers or VSIs. You can also create a default Security Group with Secure Shell (SSH) and ICMP (ping) during VPC creation, which allows ICMP and SSH from any IP address. These rules need to restrict the IPs or IP ranges from which you are planning to access the VPC.

Storage

Block storage is provided with your virtual servers and uses input/output operations per second (IOPS) to determine storage needs. It is ideal for storage-intensive applications with high I/O needs, such as an OS, and database and application software. This option is the perfect companion for SAP HANA workloads.

All Block storage is selected based on capacity (GB) and performance (IOPS) measurements and is required to meet a specific SAP Workload.

IOPS values are measured based on 16 KB block size with a 50-50 read/write mix. To achieve a maximum I/O throughput, it's advisable to look at the tier and custom profiles available for storage and find the optimal combination of size and IOPS.

Storage volumes differ in performance, depending on their IOPS tier. You can select among 3, 5, and 10 IOPS/GB (see [Tiered IOPS profiles](#)). You can also select a [custom size](#) (in GB and IOPS) that is based on the size of the storage.

If you need more than the initially provisioned storage in your server, you can attach extra volumes to it later. Contact [IBM Cloud Support](#) for extension options if the attached storage is insufficient for your workload.

Shared Storage

Block storage can be detached and attached to other servers at any time, but, only to one server at the same time.

No shared storage for servers is available in VPC at time of writing.

Classic Infrastructure environment introduction

An Infrastructure-as-a-Service (IaaS) environment consists of many components. These components are primarily compute, storage, a network from a specified region (such as the US), and a designated site location (also referred to as zone, which is a data center site).

Deployment and management

IBM Cloud Classic Infrastructure offerings (such as Bare Metal Servers) are deployed through the [IBM Cloud Classic Infrastructure console](#).

Alternatively, deployments can be made and managed by using:

- IBM Cloud CLI
- IBM Cloud Classic Infrastructure API (Softlayer API) calls that use an IBM Cloud Classic Infrastructure API key
- [Terraform Provider for IBM Cloud](#) that uses an IBM Cloud Classic Infrastructure API key

For more information, see [Managing IBM Power Virtual Servers \(IAM\)](#).

Locations - Data centers

With data centers across North and South America, Europe, Asia, and Australia, you can provision cloud resources where (and when) you need them. You can choose from many regions globally, and each region has multiple data centers. Each data center is connected to the IBM Cloud global private network, making data transfers faster and more efficient anywhere in the world.

For more information about IBM Cloud availability zones, data centers, and points of presence (PoPs), see the [global regions and availability zones and data centers map](#).

Networking

The classic infrastructure network, is robust, secure, and flexible; built upon matured networking principles combined with the latest in networking hardware.

IBM Cloud Classic Infrastructure network

Global

Region

Data center

Data center Pod

VLAN (Public and Private)

Subnet (Public and Private)

Networking component layers overview

 **Note:** Classic Infrastructure was formerly known as Softlayer.

The IBM Cloud Classic Infrastructure network provides connectivity across a global footprint of over 60 IBM Cloud data centers and 28 points of presence (PoPs). Connections are available to leading global network providers and communications service providers.

The IBM Cloud Classic Infrastructure network consists of three distinct and redundant network architectures that are seamlessly integrated in the secured network-within-a-network topology (multiple isolated logical networks, for example VLANs). This configuration means if an outage occurs in a data center on the public network, the traffic is routed and traverses through other established networks. Routing the traffic across other networks and through another data center provides continued server availability.

The three distinct and redundant network architectures within the secured network-within-a-network topology are:

- **Public network:** provides carrier grade internet connectivity to multi-home backbone carriers. On public IP, the connection is made to the IBM Cloud network PoP closest to the origin request. Traffic travels directly across the IBM Cloud data center to the data center network backbone into the correct data center, minimizing the network hops and handoffs between providers that add network latency.
- **Private network:** provides complete control of the secured networking traffic without performance degradation if significant public network traffic occurs at the same time; the private network has three functional areas:
 - **Host to and from Host:** network traffic in the private VLANs assigned to you. **Bandwidth is free and unmetered.**
 - **Host to and from Backend Services:** network traffic to and from the private VLAN to OS update servers, NTP, DNS resolvers, network storage and more. **Bandwidth is free and unmetered.**
 - **VPN and direct connections to and from VLAN:** network traffic to and from an existing internal network over direct connection or VPN that uses a distinct stand-alone network to the secure private VLAN. **Bandwidth is free and unmetered.**
 - **Data center to Data center interconnectivity:** provides secure connectivity between hosts across IBM Cloud data center locations. **Bandwidth is free and unmetered.**
- **Management network:** provides Out-Of-Band Management (OOBM) accessible through VPN (for example the built-in SSL VPN for administration) or direct connection (for example IBM Cloud Direct Link). Network management allows Remote Console access through the IPMI network interface for Bare Metals hosts on the private network. **Bandwidth is free and unmetered.**

This network-within-a-network topology design provides maximum accessibility, security, and control for your IT infrastructure. The topology provides the ease of a public network with the security of a private network by keeping systems accessible to administrators and safely off-limits to external users.

Networking VLANs

The Virtual LAN (VLAN) assigned to you on the Classic Infrastructure network, provides an enterprise-grade private network with full isolation and security. Each VLAN is either public or private, and each VLAN is assigned to a specific data center for a specific IBM Cloud Account.

The following information is a summary of [Getting started with VLANs on Classic Infrastructure](#) and [About VLANs on Classic Infrastructure](#).

A VLAN can have multiple Subnets for you to use to segregate traffic, for example:

- Public VLAN
 - Public Primary Subnet (default)
 - Public Secondary Portable Subnet
 - Public Secondary Static Subnet
- Private VLAN
 - Private Primary Subnet (default)
 - Private Secondary Portable Subnet

If you want to separate different types of network traffic in your landscape, use subnets in your network design to separate network traffic and use more Virtual LANs (VLANs) only when required.

Keep in mind that the additional VLANs and Subnets lead to traffic segregation, not increased performance; the increased performance is gained when additional VLANs and Subnets are associated to a host. When multiple network interfaces are used, two performance increases are possible depending on the use case:

- Bonding of the network interfaces, creating a network path with the network throughput of both interfaces
- Traffic segregation using two networks, then isolating high volumes of traffic to a specific network which avoids a single network becoming a bottleneck. For example, a network for storage I/O only

By default, your server has a Primary Public IP address and Primary Private IP address. If you want your server to be private, you can turn off the public interface by either:

- Ordering your server as private-only
- Using the console or the OS after the server is provisioned

Alternatively, the server can be attached to a public VLAN and private VLAN that is associated with a Gateway Appliance. In this arrangement, the server has a DMZ with a public network facing VLAN and private network facing VLAN.

Networking subnets

In Classic Infrastructure, the VLAN has different types of Subnets. The following information is a summary of [Getting started with subnet and IPs on Classic Infrastructure](#) and [About subnets and IP on Classic Infrastructure](#).

Different types of subnets in Classic Infrastructure:

1. **Public and Private Primary Subnet**
 - Auto-assigned when provisioning resources (for example, Bare Metal) into a Public and Private VLAN
 - [Primary subnets have limitations](#)
2. **Public and Private Secondary Portable Subnet**
 - Appends new subnet to Public and Private VLAN
 - Provides IP addresses for assignment to any resource within a VLAN, can assign Portable IP to multiple resources as a Floating IP
 - Enables connection to multiple resources from a single Portable IP
3. **Public Secondary Static Subnet**
 - Appends new subnet to Public VLAN
 - Provides IP addresses for assignment to one resource within a VLAN (that uses the existing Primary IP or Portable IP of the resource as the "routing endpoint")
 - Enables connection to one resource by using any of the Static IPs plus the original Primary IP or Portable IP.
4. **Public Secondary Global Subnet also known as Global IP addresses**
 - Appends single Internet-accessible IP from IBM Cloud private backbone to any VLAN worldwide
 - Provides single IP address for assignment to one resource within any VLAN worldwide (using the existing Primary IP or Portable IP of the resource as the "routing endpoint")
 - Enables connection to one resource from any data center or VLAN on IBM Cloud backbone or from Public Internet

Networking connectivity

Issues with network connectivity can cause significant delays for your project. Plan your network carefully, regardless of how you plan to use your system.

Each provisioned server has network interfaces, available at a speed of 100 Mb/s, 1 Gb/s, and 10 Gb/s.

In general, you have two interface choices:

- An external interface with a *Public IP*
- An internal interface that is provided with a *Private IP*; in compliance with IETF RFC 1918. You can also choose a single internal interface with a "private IP."

Both options can be made redundant through:

- On Linux®, a "bonding interface"
- On Windows Server, a Windows Network Interface Card (NIC) Teaming

Depending on your use case, a Public IP might be acceptable for proof-of-concept (PoC) landscapes because the external IP might be easier to use. However, this arrangement has some implications:

- A potential security risk exists even though a basic firewall is installed and preconfigured.
- If you want to use a public interface, be sure to choose a sufficiently high value for **Public Bandwidth** when you order your server. This value

determines the total amount of data that can be transferred through the interface during a one-month period. You either need to know the amount of data that is transferred at least by the order of magnitude or switch to the second option.

Access to the resources on the IBM Cloud Classic Infrastructure is available with greater security:

- Using the SSL Virtual Private Network (VPN), default available through the IBM Cloud Classic Infrastructure console
- Using the IPSec Virtual Private Network (VPN)
- Using a Gateway Appliance with Firewall, Network Address Translation (NAT)
- Direct Link

These connectivity options can provide you with a higher bandwidth, which help you in transferring larger amounts of data into an IBM Cloud data center.



Note: It is advised that your networking department contact [IBM Cloud Support](#) after you determine the layout of your landscape and the connectivity that is required on the SAP application layer.

Storage

Within Classic Infrastructure, three types of storage are available:

- Local Disk Storage (SSD)
- Network Block Storage (LUNs only) that uses IBM Cloud Block Storage (Classic)
- Network File Storage (file system installed) that uses IBM Cloud File Storage (Classic)

Local disk storage is provided with your Bare Metal Servers and available in your choice of RAID configuration (by using a dedicated RAID Controller). It is ideal for storage-intensive applications with high I/O needs, such as an OS, database, and application software. This storage is the perfect companion for SAP HANA workloads.



Note: Bare Metals with local disk storage use disks physically inserted into the drive bays; it is not using a SmartNIC to present network block storage as if it were local disk storage.

In addition to the local storage, you might require network storage (to expand beyond the Local SSD Disk total capacity, or for redundancy and backups). These require more network consumption to access Network Block Storage and Network File Storage that are using the same physical network interfaces and the impact should be validated.

Both IBM Cloud Block Storage for Classic or IBM Cloud File Storage for Classic can serve as either backup space or as storage for extra software components that are installed on your server.

All IBM Cloud Block Storage for Classic or IBM Cloud File Storage for Classic is selected based on capacity (GB) and performance (IOPS) measurements.

IOPS are measured based on 16 KB block size with a 50/50 read/write mix. To achieve a maximum I/O throughput, it's advisable to look at the tier and custom profiles available for storage and find the optimal combination of size and IOPS.

If you need more than the initially provisioned storage in your virtual server, you can attach extra volumes to a virtual server later. Contact [IBM Cloud Support](#) for extension options if the attached storage is insufficient for your workload.

For more information, see [Getting started with Block Storage for Classic](#) and [Getting started with IBM Cloud File Storage for Classic](#).

Compute

Three primary types of IaaS are available within the IBM Cloud Classic Infrastructure:

1. Bare Metal server
2. Classic Virtual Servers (not SAP certified)
3. VMware, available in two options:
 - **Intel Bare Metal and VMware vSphere (ESXi OS)**, requires manual VMware setup and configuration
 - **IBM Cloud for VMware Solutions Dedicated**

Bare Metal and both VMware options are SAP-certified.

Classic Virtual Servers are not SAP-certified. For this type of IaaS, the IBM Cloud VPC Infrastructure environment provides Intel Virtual Servers which are SAP-certified.

For more information, see [Infrastructure certified for SAP](#).

IBM Power Systems Infrastructure environment introduction



Note: This is a complementary offering from IBM Power Systems, with low latency access to IBM Cloud services

An Infrastructure-as-a-Service (IaaS) environment consists of many components - primarily compute, storage, and network from a specified region (such as the US) and a designated site location (also referred to as zone, which is a data center site).

Deployment and management

IBM Power Virtual Server is an IBM Power Systems enterprise Infrastructure-as-a-service (IaaS) offering.

These IBM Power Virtual Servers are physically located with low-latency connectivity to the IBM Cloud Classic Infrastructure or VPC Infrastructure. In the data centers, the Power Virtual Servers are separated from the rest of the IBM Cloud servers with separate networks and direct-attached storage. This infrastructure design enables Power Virtual Servers to maintain key enterprise software certification and support as its architecture is identical to certified on-premises infrastructure. The internal networks are fenced but have connectivity options to the rest of environments and services on IBM Cloud.

IBM Power Systems Infrastructure offerings (such as IBM Power Virtual Server) are deployed using the [IBM Power Infrastructure console available through IBM Cloud](#).

Alternatively, you can create and manage deployments with any of the following methods:

- IBM Power Infrastructure plug-in for IBM Cloud CLI
- IBM Power Infrastructure API calls with an IBM Cloud API key
- [Terraform Provider for IBM Cloud](#) with an IBM Cloud API key

For more information, see [Managing IBM Power Virtual Servers \(IAM\)](#).

Locations - Data centers

With data centers across North and South America, Europe, Asia, and Australia, you can provision IBM Power Infrastructure resources where (and when) you need them.

You can choose from multiple data centers globally.

Each data center with IBM Power Infrastructure uses a separate enterprise-grade network which is connected using IBM Cloud Direct Link to the IBM Cloud global private network, making data transfers faster and more efficient anywhere in the world.

For more information about IBM Cloud availability zones / data centers and points of presence (PoPs) where IBM Power Infrastructure can be connected to, see the [global regions and availability zones / data centers map](#).

Networking

The IBM Power Systems Infrastructure network, is built upon IBM Power's enterprise-grade secure networking hardware and connectivity; it can be bridged to the separate IBM Cloud networks (either Classic Infrastructure network or VPC Infrastructure network).

IBM Power Virtual Server Group network on IBM Cloud

Global

Resource Group

Region

Datacenter

Datacenter colocation Room

VLAN (Public and Private) used internally, effectively transparent to the administrator

Subnet (Public and Private)

Networking component layers overview

Connectivity is available to the IBM Power Systems Infrastructure network leveraging connectivity options available from leading global network providers and TelCo providers in addition to the connectivity options available using the IBM Cloud global footprint of more than 60 IBM Cloud data centers and 28 points of presence (PoPs).

Networking VLANs and Subnets

The following information is a summary of [Getting started with the Power Edge Router](#) and [Configuring and adding a private network subnet](#).

The Virtual LAN (VLAN) on the IBM Power Systems Infrastructure network, provides an enterprise-grade private network with full isolation and security. Each VLAN is Public or Private, and is assigned to a specific data center for a specific IBM Cloud Account.

Each VLAN is associated with a single Subnet, for example:

- Public VLAN **(only one per region)**
 - Public Subnet
- Private VLAN
 - Private Subnet

A **Public Subnet** is the quickest and simplest way to connect to an IBM Power Virtual Server instance. The public network is protected by a firewall and only the following network protocols are allowed:

- SSH (port 22)
- HTTPS (port 443)
- Ping (ICMP)
- IBM i 5250 console emulation with SSL (port 992)



Note: For the public network, other ports are blocked and can be routed through SSH.

A **Private Subnet** is required for the connection of your virtual instances with systems outside of the IBM data centers and for communication between multiple instances in an SAP three-tier system. This subnet is an internal network that can be used to connect individual IBM Power Virtual Servers with each other.

If you want to separate different types of network traffic in your landscape, you can order more subnets (and their respective VLANs).

Keep in mind that the additional VLANs and subnets lead to traffic segregation, not increased performance; the increased performance is gained when additional VLANs and Subnets are associated to a host. When multiple network interfaces are used, two performance increases are possible depending on the use case:

- Bonding of the network interfaces, creating a network path with the network throughput of both interfaces
- Traffic segregation using two networks, then isolating high volumes of traffic to a specific network which avoids a single network becoming a bottleneck. For example, a network for storage I/O only

With IBM Power Virtual Server as an example, a single threaded Linux network interface may reach 100% CPU Thread utilization even though the performance limits of the network path itself are still not reached. Additional network interfaces attached to another VLAN and Subnet will therefore increase performance

By default, your server has a Private IP address. If you use public subnets, a public IP address is assigned in addition.

Networking connectivity

Issues with network connectivity can cause delays for your project if you do not plan properly, regardless of how you plan to use your system.

If you need to connect to your virtual server through the public internet, in other words, inbound to a virtual server, you can order *Public IPs* and attach them to the virtual server per vNIC.

Various interconnectivity options available, for example:

- IBM Power Systems Infrastructure bridged to IBM Cloud Classic Infrastructure
- IBM Power Systems Infrastructure bridged to IBM Cloud VPC Infrastructure
- IBM Power Systems Infrastructure bridged to on-premises data centers by using IBM Direct Link

Direct Link on Classic is also used for closer integration into your backbone infrastructure, for more information, see [Connectivity to your SAP system landscape](#).

For more explanation information about IBM Power Systems Infrastructure, see [IBM Power Virtual Servers](#).



Note: Have your networking department contact the IBM Power Virtual Servers Support Team, handled by using [IBM Cloud Support](#) after you determine the layout of your landscape and the connectivity that is required on the SAP application layer.

Storage

Within IBM Power Systems Infrastructure, there are two types of storage available:

- Block Storage Tier 1 (storage for mission critical application with best characteristics, e.g. NVMe flash storage)
- Block Storage Tier 3 (default storage type with optimized price/performance, e.g. SSD flash storage)



Note: Do not mix storage types on an IBM Power Virtual Server.

Block Storage is provided with your IBM Power Virtual Servers and storage requirements are defined using input/output operations per second (IOPS) and the capacity (GB). High performance block storage is ideal for storage-intensive applications with high I/O needs, such as an OS, and database and application software. For SAP HANA workloads, Tier 1 of block storage is supported only.

All Block Storage is selected based on capacity (GB), currently the performance (IOPS) measurement cannot be fine-tuned.

Block Storage for IBM Power Virtual Servers is powered underneath by [IBM FlashSystem family](#) connected through the Fibre Channel protocol.

For further information, see [hardware specifications for IBM Power Virtual Servers](#).

Contact [IBM Cloud Support](#) for extension options if the attached storage is insufficient for your workload.

Compute

There is only one type of IaaS available within the IBM Power Systems Infrastructure environment:

1. IBM Power Virtual Servers

The IBM Power Virtual Servers are SAP-certified.

Currently following IBM Power Systems hardware are utilized by IBM Power Virtual Servers:

- S922 – optimized for SAP NetWeaver application server
- E980 – optimized for SAP HANA database server

For more information, see [Infrastructure certified for SAP](#).

Infrastructure certified for SAP

Certified Infrastructure-as-a-Service for SAP HANA database servers and for SAP NetWeaver based applications is available in many variations, each with different capabilities and sizing available to fit many different SAP workload scenarios.

For the official and full platform list of Infrastructure-as-a-Service from IBM that is SAP certified and supported for SAP HANA, see the [SAP Certified and Supported SAP HANA Hardware Directory - Certified IaaS Platforms - IBM Cloud](#). For an official list of SAP NetWeaver and SAP HANA supported bare metal and virtual servers, see [SAP Note 2927211](#).



Tip: The documents provide detailed considerations and information for building your SAP environments at each layer for all offerings. However, if you are interested in quickly finding the information that is related specifically to one of the IaaS offerings, then you might consider using the Fast Path Site Maps for [Intel Bare Metal \(Classic\)](#), [Intel Bare Metal \(VPC\)](#), [Intel Virtual Servers \(VPC\)](#), [IBM Power Virtual Servers](#), and [VMware SDDC](#).

Intel Bare Metal servers on Classic Infrastructure

IBM Cloud® Bare Metal Servers are physical servers with numerous customization capabilities.

The servers are dedicated for your use, or your customer's, and not shared in any part, including server resources, with other IBM Cloud customers.

These servers are managed by the account holder, either you, your customer, or your services partner, depending on your business operations.

These servers are provisioned with your choice of operating system (OS) image that is directly installed to bare metal.

Because customization is controlled on bare metal servers, fast provisioning times of in the range 1 - 4 hours are obtainable with worldwide availability.

For larger systems (greater 4 TB DRAM), there is a longer validation period for checking the hardware components (particularly RAM), but the machines are usually available within 24 hours.

For more information about Bare Metal servers on Classic Infrastructure, see [IBM Cloud Bare Metal Servers](#) on ibm.com and [IBM Cloud Bare Metal Servers for Classic - server options](#) on IBM Cloud Docs.

Intel Virtual Servers on VPC Infrastructure

IBM® Virtual Servers are virtual machine servers with extensive customization capabilities.

The servers run on a hypervisor that is managed by IBM Cloud, providing you flexible compute by using a scalable infrastructure (available in multi-tenant or dedicated single-tenant).

These servers are managed by the account holder, either you, your customer, or your services partner, depending on your business operations.

These servers are provisioned with your choice of operating system (OS) image that is installed to Virtual Servers.

IBM Cloud VPC Infrastructure is available for:

- Intel Virtual Servers, based on the latest hardware designs with large improvements across networking performance (up to 80 Gbps), provision times (5x faster), and a flexible selection of extra features

For more information about Virtual Servers on VPC Infrastructure, see [What is IBM Cloud VPC?](#) and [IBM Cloud Virtual Server for VPC](#) on ibm.com and [IBM Cloud Intel Virtual Servers on VPC Infrastructure](#) on IBM Cloud Docs.

Intel Bare Metal servers on VPC Infrastructure

IBM Cloud® Bare Metal Servers are physical servers with numerous customization capabilities.

The servers are dedicated for your use, or your customer's, and not shared in any part, including server resources, with other IBM Cloud customers.

These servers are managed by the account holder, either you, your customer, or your services partner, depending on your business operations.

These servers are provisioned with your choice of operating system (OS) image that is directly installed to bare metal.

Because customization is controlled on bare metal servers, fast provisioning times of in the range 1 - 4 hours are obtainable with worldwide availability.

For larger systems (greater 3 TB DRAM), there is a longer validation period for checking the hardware components (particularly RAM), but the machines are usually available within 24 hours.

For more information about Bare Metal servers on VPC Infrastructure, see [Deploy IBM Cloud Bare Metal Servers on VPC Infrastructure](#) on ibm.com and [About Bare Metal Servers for VPC](#) on IBM Cloud Docs.

IBM Power Virtual Server



Note: This is a complementary offering from IBM Power Systems, with low latency access to IBM Cloud services

IBM Power Virtual Servers are virtual machine servers with enterprise-grade performance and extensive customization capabilities. These IBM Power Virtual Servers are also known as an IBM Power Logical Partitions (LPARs).

The servers run on IBM PowerVM (Type 1 hypervisor) managed by IBM Power Systems and facilitated by IBM Cloud are a form of Infrastructure-as-a-Service (IaaS) provisioned with your choice of operating system (IBM AIX or Linux®) image that is installed and infrastructure customization (such as dedicated CPU performance or shared CPU for optimized costs). By using the IBM PowerVM underneath, the customization of the Virtual Servers is flexible, with fast self-service provisioning available in worldwide locations - all with pay-as-you-use billing that makes it easier for you to scale up and out.

IBM Power Virtual Servers are colocated in the same IBM Cloud data centers that are used by both IBM Cloud Classic Infrastructure and VPC Infrastructure, but are separated from the rest of the IBM Cloud servers with separate networks and storage. They can be connected to/from an on-premises network, the IBM Cloud Classic Infrastructure or IBM Cloud VPC Infrastructure networks by using IBM Cloud® Direct Link on Classic.

The IBM Power Virtual Servers can be used for several workload scenarios such as disaster recovery, development environments, partial IT infrastructure moves and enabling you to stay competitive with flexible scaling of infrastructure capacity in a hybrid cloud deployment. This Infrastructure-as-a-Service (IaaS) offering is designed for large mission-critical workloads where scale-up over 12 TB of memory and density of 6,000 SAPS per CPU Core are required to meet performance.

As the IBM Power Virtual Servers are IaaS once provisioned are managed by the account holder; either you, your customer, or your services partner depending on your business operations model.

IBM Power Systems clients who rely on on-premises data center deployments for their infrastructure, can now quickly and economically extend their IBM Power resources into the cloud in a matter of minutes. The IBM Power Virtual Servers provide:

- **Straightforward billing:** Hourly rates on Monthly Billing, with IBM PowerLinux customers can use Bring-your-own-License (BYOL), to use their own licenses for the OS Images provided by IBM Power Virtual Servers and reduce costs of their Cloud environment.
- **Enterprise Hybrid Cloud deployment:** run workloads on IBM Power in both Cloud IaaS and on-premises, accessing Cloud's self-service, fast delivery, elasticity, and connectivity to other IBM Cloud® services. Although your Linux® workloads are running in IBM Power Virtual Servers, you keep the same scalable, resilient, production-ready features that Power Systems hardware is known to provide.
- **Infrastructure customization:** Flexibility of IBM Power Virtual Servers hardware capabilities:
 - Cores (CPU)
 - Memory (RAM)
 - Data volume size
 - Data volume type / performance tier
 - Network interfaces
 - PowerVM Host Pinning Policy (soft or hard)
 - PowerVM Host CPU Binding (dedicated or shared)

For more explanation information about IBM Power Virtual Servers, see [IBM Power Virtual Servers](#) on ibm.com and [IBM Power Systems Virtual Servers](#) on IBM Cloud Docs.

Constructs for provisioning IBM Power Virtual Servers

As the IBM Power Virtual Server is a complementary offering from IBM Power Systems, it is accessed as an additional offering from the IBM Cloud catalog. To begin using IBM Power Virtual Servers, an instantiation of an IBM Power Virtual Server resource group must first be made.

The below sections explain this in more detail.

Resource versus Resource Group

A **resource** in the context of IBM Power Virtual Servers is not a user, it's anything that you can create from the catalog, for example, an IBM Power Virtual Server. A **resource group** contains multiple resources, for example, a set of servers used strictly for development activities. For more information, see [Creating resources](#).

Service versus instance

There is difference between an IBM Power Virtual Server **service** and an IBM Power Virtual Server **instance**. Think of the IBM Power Virtual Server **service** as a container for all IBM Power Virtual Server **instances** at a specific geographic location. The IBM Power Virtual Server **service** is available from the **Resource list** in the IBM Cloud® UI. The service can contain multiple IBM Power Virtual Server **instances**.

For example, you can have two IBM Power Virtual Server **services**, one in Dallas and another in Washington DC. Each service can contain multiple IBM Power Virtual Server **instances**. For more information, see [Getting started with IBM Cloud IBM Power Virtual Server](#).

 **Note:** All instances of an SAP system must run in the same service. Multiple systems can be distributed through different services, in which case IT operations teams must ensure that latency is acceptable for their scenarios.

IBM Power CPU type - dedicated or shared

For **shared** processors, you choose the number of CPUs that the new server is entitled to use. This number should correspond to the number of CPUs that were the result of your sizing. The entitled CPUs should be sufficient for normal production operation and to cover workload during peak time. Don't count on additional CPUs that you might get out of the shared processor pool for uncapped processors.

For **dedicated** processors, the number of dedicated CPUs should correspond to the number of CPUs that were the result of your sizing.

For more information about shared and dedicated processors, see [Assigning the appropriate processor entitled capacity](#) and [Power Virtual Servers processor types](#).

 **Note:** Depending on the SAP workload, supported processor options are restricted. For more information, see [SAP Note 2855850](#).

SAP HANA and IBM Power Virtual Server

See [SAP Note 2947579 - SAP HANA on IBM Power Virtual Servers](#) for SAP HANA support on IBM Power Virtual Servers.

SAP HANA workloads that use IBM Power Virtual Servers run on IBM Power System E980, with Block Storage powered by [IBM FlashSystem family](#) connected through the Fibre Channel protocol. For more information about these systems and how they're used inside the IBM Power Virtual Server service, see the data sheet below:

Data sheet:

- [IBM Power System E980 \(9080-M9S\)](#)

For further information, see [hardware specifications for IBM Power Virtual Servers](#).

SAP NetWeaver and IBM Power Virtual Server

See [SAP Note 2855850 - SAP Applications on IBM Power Virtual Servers](#) for SAP NetWeaver support on IBM Power Virtual Servers.

SAP NetWeaver and SAP AnyDB workloads that use IBM Power Virtual Servers are run on IBM Power System S922 and IBM Power System E980, with Block Storage powered by [IBM FlashSystem family](#) connected through the Fibre Channel protocol. For more information about these systems and how they're used inside the IBM Power Virtual Server service, see the following data sheets:

Data sheets:

- [IBM Power System S922 \(9009-22A\)](#)
- [IBM Power System E980 \(9080-M9S\)](#)

For further information, see [hardware specifications for IBM Power Virtual Servers](#).

VMware Software-Defined Data Center

IBM Cloud and VMware partner to bring the capabilities of VMware for SAP into Cloud by using VMware vSphere installed to IBM Cloud® Bare Metal Servers.

This enables secure single-tenant compute with full root control to the hypervisor, providing optimized performance with high agility, resiliency, and elastic compute costs. Since Dec-2007, when VMware first announced support for SAP, there has been continuous improvement to VMware-SAP capabilities, which provide flexible delivery of SAP project implementations and easier maintenance of SAP Systems; all these capabilities are available with VMware and IBM Cloud.

In short, IBM Cloud provides two levels of VMware, which are both SAP-certified:

- **Intel Bare Metal and VMware vSphere (ESXi OS)**, requires manual VMware setup and configuration
- **IBM Cloud for VMware Solutions Dedicated**, fully automated VMware SDDC setup and configuration
 - *includes optional BYOL and access to advanced VMware capabilities, such as VMware HCX for seamless bidirectional network extension and connection to existing VMware clusters on-premises*

For more information about IBM Cloud for VMware on Classic Infrastructure, see [IBM Cloud for VMware](#). Additional information is available on:

- [IBM Cloud Intel Bare Metal and VMware vSphere \(ESXi OS\)](#) for the manual VMware setup and configuration
- [IBM Cloud for VMware Solutions Dedicated](#) for fully automated VMware SDDC setup and configuration

Compliance

IBM treats your data with the same safeguards as our own, the security is built to IBM's rigorous standards and certified for compliance.

IBM Cloud is designed for organizations who are building a cloud environment, which is security-rich, open, hybrid Cloud (i.e., on-premises data center workloads) and multi-cloud. Deployments to IBM Cloud include many secure and regulated workloads, by using our extensive IBM Cloud compliance programs with clear delineation of roles and responsibilities.

[IBM Cloud compliance programs](#) provide compliance and trust certifications, which reaffirm IBM's commitment to protection of customer data and applications. These compliance programs are for regulations, standards, and frameworks across Global, Government, Industry, and Regional.

More supplementary information to the IBM Cloud compliance programs is available on IBM Cloud service offering descriptions and terms which contain links to individual "**Data Processing and Protection data sheets**" for IBM Cloud offerings.

Each IBM Cloud® for SAP offering uses different infrastructure configurations and approaches to providing the service and will therefore be certified independent of each other. These certifications can be checked on the previous links or clarified by contacting IBM Cloud or your IBM representative. Following is a small extract from the full list of recognized compliance, certifications, attestations, or reports available across the various IBM Cloud® for SAP offerings:

- ISO 27001
- ISO 27017
- ISO 27018
- EU-US Privacy Shield Policy
- GDPR Ready
- Germany Federal Office for Information Security (BSI) C5
- HIPAA for Healthcare USA
- ITAR Compliant
- PCI-DSS for Payment Card Industry USA
- Singapore Multi-Tier Cloud Security Standard (MTCS)
- SOC1 Type 2
- SOC2 Type 2
- SOC3
- ...more

Infrastructure profiles for SAP HANA database servers

Intel Virtual Server certified profiles on VPC infrastructure for SAP HANA

Profiles list



Note: The published names are subject to change.

The following list gives you an overview of the SAP-certified profiles with Virtual Servers for VPC:

Profile	vCPU	Memory (RAM GiB)	SAPS	SAP HANA Processing Type
Memory Optimized				
mx2-8x64 mx2d-8x64	8	64	10,280	SAP Business One (**)
mx2-16x128 mx2d-16x128	16	128	20,565	OLTP (*) SAP Business One (**)
mx2-32x256 mx2d-32x256	32	256	41,130	OLTP (*) SAP Business One (**)
mx2-48x384 mx2d-48x384	48	384	56,970	OLTP (*) SAP Business One (**)
Very High Memory Optimized				
vx2d-16x224	16	224	17,046	OLTP (*)
vx2d-44x616	44	616	46,875	OLAP/OLTP (*)
vx2d-88x1232	88	1,232	93,750	OLAP/OLTP (*)
vx2d-144x2016	144	2,016	153,410	OLAP/OLTP (*)
vx2d-176x2464	176	2,464	187,500	OLAP/OLTP (*)
Ultra High Memory Optimized				
ux2d-8x224	8	224	8,623	OLTP (*)
ux2d-16x448	16	448	17,246	OLTP (*)
ux2d-36x1008	36	1,008	38,803	OLTP (*)
ux2d-48x1344	48	1,344	51,737	OLTP (*)
ux2d-72x2016	72	2,016	77,606	OLTP (*)
ux2d-100x2800	100	2,800	107,785	OLTP (*)
ux2d-200x5600	200	5,600	215,570	OLTP (*)

IBM Cloud Virtual Servers for VPC certified for SAP HANA

(*): RHEL 7.6 for SAP Solutions, RHEL 7.9 for SAP Solutions, RHEL 8.1 for SAP Solutions, RHEL 8.2 for SAP Solutions, RHEL 8.4 for SAP Solutions, RHEL 8.6

for SAP Solutions, RHEL 8.8 for SAP Solutions, RHEL 8.10 for SAP Solutions, RHEL 9.0 for SAP Solutions, RHEL 9.2 for SAP Solutions, RHEL 9.4 for SAP Solutions\n SLES 12 SP4, SLES 12 SP5, SLES 15, SLES 15 SP1, SLES 15 SP2, SLES 15 SP3, SLES 15 SP4, SLES 15 SP5, SLES 15 SP6\n \n (**): SLES 12 SP4, SLES 15, SLES 15 SP1, SLES 15 SP2, SLES 15 SP3, SLES 15 SP4, SLES 15 SP5



Note: Please, regard the supported operated systems that are mentioned in the footnotes.

For more information, see [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#).

Understanding Virtual Server profile names

With IBM Cloud® Virtual Servers for Virtual Private Cloud, the profile families that are certified for SAP are: *Memory Optimized*, *Very High* and *Ultra High Memory Optimized*.

- All the Memory family profiles cater to memory intensive workloads, such as demanding database applications and in-memory analytics workloads, and are especially designed for SAP HANA workloads.

For more information, see chapter [x86-64 instance profiles](#).

The first letter of the profile name indicates the profile family that is mentioned in the profile list:

First letter	Characteristics of the related profile family
m	<i>Memory Optimized</i> family, higher vCPU to memory ratio 1:8
v	<i>Very High Memory Optimized</i> family, very high vCPU to memory ratio 1:14
u	<i>Ultra High Memory Optimized</i> family, ultra high vCPU to memory ratio 1:28

IBM Cloud® Virtual Servers for Virtual Private Cloud Profile Families

\n The Virtual Server profile names are contextual and sequential. See the following example:

Profile name	Naming convention	What it means
mx2-16x128	m	<i>Memory Optimized</i> family
	x	Intel x86_64 CPU Architecture
	2	The generation for the underlying hardware
	d	the optional 'd' in the name indicates that the server is equipped with one or more internal SSD storage devices (*)
	-	spacer
	16	16 vCPU
	x	spacer
	128	128 GiB RAM

Profile naming for SAP HANA



Note: (*) Note for Virtual Server Instances using instance storage on SSD: you must not place any SAP workload related data on such instance storage, because data loss may occur in certain situations - see more information here: [About instance storage](#).

Profiles available on Hourly Consumption Billing

All IBM Cloud Virtual Servers for VPC are available with Hourly Consumption Billing, which includes Suspend Discounts and Sustained Usage Discounts.

With Suspend Discounts, storage charges occur only if the server is in Shutdown state. With Sustained Usage Discount, the more a server is used, the less the cost per hour.

Storage specifications

When the virtual server profiles for SAP HANA are initially provisioned, the servers all have one pre-configured volume (vda) attached with the following basic layout:

File system	Partition	Storage type	Size (GB)	Nr. of IOPS
/	vda1	Pre-configured boot volume	100	3,000
/boot	vda2	Pre-configured boot volume	0.25	3,000

Storage configuration of the default virtual server deployment (boot volume)

IBM® Cloud Block Storage for Virtual Private Cloud

[IBM® Cloud Block Storage for Virtual Private Cloud](#) volumes for Virtual Servers can be created based on different **volume profiles** that provide different levels of IOPS per gigabyte (IOPS/GB). For more information, see [IOPS tiers](#).

You must consider the total IOPS required for your installation and the performance characteristics of your database. One option is to collocate multiple directories into a single large volume with high IOPS, versus isolating directories into individual small volumes with an insufficient number of IOPS for the workload characteristics.

For an overview of all available storage profiles, see [VPC Block Storage Profiles](#).

Storage for SAP HANA - single-node

To fulfill the KPIs defined by SAP HANA, each profile needs different storage volumes that are listed in details in the following sections. **These configurations are mandatory storage configurations, not sample storage configurations**, because they are the tested and certified storage layouts that comply with **SAP HANA Tailored Data Center Integration**. It is highly recommended to stick to these specific guidelines.

⚠ Important: Customers who want to choose different layouts are advised to follow the [SAP HANA TDI Overview](#) and [SAP HANA TDI FAQ](#) when they order different storage sizes and types. Then, they must run SAP's performance measurement tool HCMT - see [SAP Note 2493172 - SAP HANA Hardware and Cloud Measurement Tools](#) and follow the instructions of the [HCMT guide](#).

💡 Note: For all of the following layouts consider that the volume names might differ - we assume that the naming follows the sequence of ordering the storage, that is, 1st order -> **vdd**, 2nd order -> **vde**, and so on. **All block storage volumes** must be ordered with the predefined profile of **10 IOPS/GB** (high performance). One exception might be /hana/shared partition where 5 IOPS/GB (medium performance) are sufficient - but ONLY IF you assigned a dedicated volume for this partition. For all profiles optional: one appropriately sized block storage volume or several equally sized volumes that are gathered to a volume group, with the predefined profile of 5 IOPS/GB (medium performance) attached to the Virtual Server for backups.

[SAP's recommended file system layout](#) must be available for SAP HANA deployment.

mx2-* profiles - Storage Layouts

The following table shows the required physical volumes, related volume groups, logical volumes, and their characteristics:

Profile	File system	Logical Volume	LV Size (GB)	Volume Group	Physical Volume	PV Size (GB)
mx2-8x64 and mx2-16x128 and mx2-32x256	/hana/shared	hana_shared_lv	256	hana_vg	vdd	500
	/hana/data	hana_data_lv	256		vde	500

	/hana/log	hana_log_lv	988		vdf	500
mx2-48x384	/hana/shared	hana_shared_lv	384	hana_vg	vdd	500
	/hana/data	hana_data_lv	616		vde	500
					vdf	500
	/hana/log	hana_log_lv	400	hana_log_vg	vdg	100
					vdh	100
					vdi	100
					vdj	100

Storage layout for mx2-* profiles based virtual servers

mx2-* profiles - Setup Instructions

See the step by step instructions for setting up the assets here. Mind the different volume names.

- [for the mx2-8x64, mx2-16x128 and mx2-32x256 profiles](#)
- [for the mx2-48x384 profile](#)

vx2d-* profiles - Storage Layouts

The following table shows the required volumes and related volume groups, if necessary, and their characteristics:

Profile	File	Logical	LV Size	Volume Group	Physical	PV Size
	system	Volume	(GB)		Volume	(GB)
vx2d-16x224	/hana/shared	hana_shared_lv	224	hana_vg	vde	1,120
	/hana/data	hana_data_lv	672			
	/hana/log	hana_log_lv	224			
vx2d-44x616	/hana/shared		n/a	vdd	616	
	/hana/data		n/a	vde	1,848	
	/hana/log	hana_log_lv	576	hana_log_vg	vdg	192
					vdh	192
vx2d-88x1232	/hana/shared		n/a	vdd	1,232	
	/hana/data		n/a	vde	3,696	
	/hana/log	hana_log_lv	576	hana_log_vg	vdf	192

					vgd	192
					vdh	192
vx2d-144x2016	/hana/shared		n/a	vdd	2,016	
	/hana/data	hana_data_lv	4,096	hana_data_vg	vde	1,024
					vdf	1,024
					vgd	1,024
					vdh	1,024
vx2d-176x2464	/hana/shared		n/a	vdd	2,464	
	/hana/data	hana_data_lv	5,120	hana_data_vg	vde	1,280
					vdf	1,280
					vgd	1,280
					vdh	1,280
	/hana/log	hana_log_lv	576	hana_log_vg	vdi	192
					vdj	192
					vdk	192

Storage for vx2* profile based virtual servers

vx2d-* profiles - Setup Instructions

See the step by step instructions for setting up the file systems here. The according volume sizes are captured in the table 6. Read the section [Adding Block Storage for VPC](#) to see how to attach the volumes to the HANA server. Some disks are governed by the Linux Logical Volume Manager LVM or lvm2.



Note: For each profile, consider the specified volume sizes in table 6 and always make sure that the correct disks are given for the respective commands. The Linux command `fdisk -l` shows which disk is to the volume, for example `/dev/vde`.

vx2d-16x224

1. Create the volume group for LVM.

```
$ [root@vx2d-16x224 ~]# pvcreate /dev/vde
[root@vx2d-16x224 ~]# vgcreate hana_vg /dev/vde
```

2. After the volume group is created, three logical volumes are defined on top. These logical volumes reflect the file system size requirements for SAP HANA.

```
$ [root@vx2d-16x224 ~]# lvcreate -L 224G -n hana_shared_lv hana_vg
[root@vx2d-16x224 ~]# lvcreate -L 224G -n hana_log_lv hana_vg
[root@vx2d-16x224 ~]# lvcreate -l 100%VG -n hana_data_lv hana_vg
```

3. Next, add these entries to /etc/fstab

```
$ LABEL=HANA_SHARED /hana/shared xfs defaults,inode64 0 0
LABEL=HANA_LOG /hana/log xfs defaults,swalloc,inode64 0 0
LABEL=HANA_DATA /hana/data xfs defaults,largeio,swalloc,inode64 0 0
```

4. Finally, a file system needs to be created on top of each volume group and then mounted:

```
$ [root@vx2d-16x224 ~]# mkfs.xfs -L HANA_SHARED /dev/mapper/hana_vg-hana_shared_lv
[root@vx2d-16x224 ~]# mkfs.xfs -L HANA_LOG /dev/mapper/hana_vg-hana_log_lv
[root@vx2d-16x224 ~]# mkfs.xfs -L HANA_DATA /dev/mapper/hana_vg-hana_data_lv

[root@vx2d-16x224 ~]# mkdir -p /hana/shared
[root@vx2d-16x224 ~]# mkdir -p /hana/log
[root@vx2d-16x224 ~]# mkdir -p /hana/data

[root@vx2d-16x224 ~]# mount -a
```

vx2d-44x616 and vx2d-88x1232

1. Create the volume group for LVM. Only /hana/log is assigned to the LVM.

```
$ [root@vx2d-44x616 ~]# pvcreate /dev/vdf /dev/vdg /dev/vdh
[root@vx2d-44x616 ~]# vgcreate hana_log_vg /dev/vdf /dev/vdg /dev/vdh
```

2. After the volume group is created, the logical volume for /hana/log needs to be defined on top. This logical volume reflects the file system size requirement for SAP HANA.

```
$ [root@vx2d-44x616 ~]# lvcreate -i 3 -I 64 -l 100%VG -n hana_log_lv hana_log_vg
```

3. Now proceed with the same instructions that are listed in steps 3 and 4 [profile vx2d-16x224](#).

vx2d-144x2016 and vx2d-176x2464

1. Create the volume group for LVM. /hana/log and /hana/data are assigned to the LVM.

```
$ [root@vx2d-144x2016 ~]# pvcreate /dev/vde /dev/vdf /dev/vdg /dev/vdh
[root@vx2d-144x2016 ~]# pvcreate /dev/vdi /dev/vdj /dev/vdk
[root@vx2d-144x2016 ~]# vgcreate hana_data_vg /dev/vde /dev/vdf /dev/vdg /dev/vdh
[root@vx2d-144x2016 ~]# vgcreate hana_log_vg /dev/vdi /dev/vdj /dev/vdk
```

2. After the volume group is created, two logical volumes need to be defined on top. These logical volumes reflect the file system size requirements for SAP HANA.

```
$ [root@vx2d-144x2016 ~]# lvcreate -i 4 -I 64 -l 100%VG -n hana_data_lv hana_data_vg
[root@vx2d-144x2016 ~]# lvcreate -i 3 -I 64 -l 100%VG -n hana_log_lv hana_log_vg
```

3. Now proceed with the same instructions that are listed in steps 3 and 4 [profile vx2d-16x224](#).

ux2d-* profiles - Storage Layouts

The following table shows the required volumes and related volume groups, if necessary, and their characteristics:

Profile	File	Logical	LV Size	Volume Group	Physical	PV Size
	system	Volume	(GB)		Volume	(GB)
ux2d-8x224	/hana/shared	hana_shared_lv	224	hana_vg	vde	1,120
	/hana/data	hana_data_lv	672			

	/hana/log	hana_log_lv	224			
ux2d-16x448	/hana/shared	hana_shared_lv	448	hana_vg	vde	2,240
	/hana/data	hana_data_lv	1,344			
	/hana/log	hana_log_lv	448			
ux2d-36x1008	/hana/shared	n/a	vdd	1,008		
	/hana/data	hana_data_lv	2,016	hana_data_vg	vde	1,008
					vdf	1,008
	/hana/log	hana_log_lv	576	hana_log_vg	vdg	192
					vdh	192
					vdi	192
ux2d-48x1344	/hana/shared	n/a	vdd	1,344		
	/hana/data	hana_data_lv	2,700	hana_data_vg	vde	1,350
					vdf	1,350
	/hana/log	hana_log_lv	576	hana_log_vg	vdg	192
					vdh	192
					vdi	192
ux2d-72x2016	/hana/shared	n/a	vdd	2,016		
	/hana/data	hana_data_lv	4,096	hana_data_vg	vde	1,024
					vdf	1,024
					vdg	1,024
	/hana/log	hana_log_lv	576	hana_log_vg	vdh	1,024
					vdi	192
					vdj	192
					vdk	192

ux2d-100x2800	/hana/shared	n/a	vdd	2,800		
	/hana/data	hana_data_lv	8,400	hana_data_vg	vde	2,100
					vdf	2,100
					vdg	2,100
					vdh	2,100
	/hana/log	hana_log_lv	576	hana_log_vg	vdi	192
					vdj	192
					vdk	192
<hr/>						
ux2d-200x5600	/hana/shared	n/a	vdd	5,600		
	/hana/data	hana_data_lv	16,800	hana_data_vg	vde	4,200
					vdf	4,200
					vdg	4,200
					vdh	4,200
	/hana/log	hana_log_lv	576	hana_log_vg	vdi	192
					vdj	192
					vdk	192

Storage for ux2* profile based virtual servers

ux2d-* profiles - Setup Instructions

See the step by step instructions for setting up the file systems here. The according volume sizes are captured in the table 7. Read the section [Adding Block Storage for VPC](#) to see how to attach the volumes to the HANA server. Some disks are governed by the Linux Logical Volume Manager LVM or lvm2.



Note: For each profile, consider the specific volume sizes in table 7 and always make sure that the correct disks are given for the respective commands. The Linux command `fdisk -l` shows which disk has been mapped to the volume, for example `/dev/vde`.

ux2d-8x224 and ux2d-16x448

1. Create the volume group for LVM.

```
$ [root@ux2d-8x224 ~]# pvcreate /dev/vde
[root@ux2d-8x224 ~]# vgcreate hana_vg /dev/vde
```

2. After the volume group is created, three logical volumes are defined on top. These logical volumes reflect the file system size requirements for SAP HANA.

```
$ [root@ux2d-8x224 ~]# lvcreate -L 224G -n hana_shared_lv hana_vg
## or lvcreate -L 448G -n hana_shared_lv hana_vg

[root@ux2d-8x224 ~]# lvcreate -L 224G -n hana_log_lv hana_vg
## or lvcreate -L 448G -n hana_log_lv hana_vg
```

```
[root@ux2d-8x224 ~]# lvcreate -l 100%VG -n hana_data_lv hana_vg
```

3. Now proceed with the same instructions that are listed in steps 3 and 4 [profile vx2d-16x224](#).

ux2d-36x1008 and ux2d-48x1344

1. Create the volume groups for LVM. /hana/log and /hana/data are assigned to the LVM.

```
$ [root@ux2d-36x1008 ~]# pvcreate /dev/vde /dev/vdf  
[root@ux2d-36x1008 ~]# pvcreate /dev/vdg /dev/vdh /dev/vdi  
[root@ux2d-36x1008 ~]# vgcreate hana_data_vg /dev/vdg /dev/vdh /dev/vdi  
[root@ux2d-36x1008 ~]# vgcreate hana_log_vg /dev/vdg /dev/vdh /dev/vdi
```

2. After the volume groups are created, two logical volumes need to be defined on top. These logical volumes reflect the file system size requirements for SAP HANA.

```
$ [root@ux2d-36x1008 ~]# lvcreate -i 2 -I 64 -l 100%VG -n hana_data_lv hana_data_vg  
[root@ux2d-36x1008 ~]# lvcreate -i 3 -I 64 -l 100%VG -n hana_log_lv hana_log_vg
```

3. Now proceed with the same instructions that are listed in steps 3 and 4 [profile vx2d-16x224](#).

ux2d-72x2016, ux2d-100x2800, and ux2d-200x5600

1. Create the volume groups for LVM. /hana/log and /hana/data are assigned to the LVM.

```
$ [root@ux2d-72x2016 ~]# pvcreate /dev/vde /dev/vdf /dev/vdg /dev/vdh  
[root@ux2d-72x2016 ~]# pvcreate /dev/vdi /dev/vdj /dev/vdk  
[root@ux2d-72x2016 ~]# vgcreate hana_data_vg /dev/vde /dev/vdf /dev/vdg /dev/vdh  
[root@ux2d-72x2016 ~]# vgcreate hana_log_vg /dev/vdi /dev/vdj /dev/vdk
```

2. After the volume groups are created, two logical volumes need to be defined on top. These logical volumes reflect the file system size requirements for SAP HANA.

```
$ [root@ux2d-72x2016 ~]# lvcreate -i 4 -I 64 -l 100%VG -n hana_data_lv hana_data_vg  
[root@ux2d-72x2016 ~]# lvcreate -i 3 -I 64 -l 100%VG -n hana_log_lv hana_log_vg
```

3. Now proceed with the same instructions that are listed in steps 3 and 4 [profile vx2d-16x224](#).

Storage for SAP HANA - multi-node

In an SAP HANA scale-out (multi-node) configuration, storage needs to be accessible from different nodes at the same time, and needs to be able to failover from one node to the other.

Thus, for SAP HANA scale-out configurations, file shares need to be deployed, and local block storage is out of scope for the SAP HANA installation. Those file shares require so-called **mount targets** to be created to allow access to the file shares from dedicated subnets. IBM Cloud recommends using the primary subnet for storage access because routes will not require any changes to access the storage servers for the file shares, if the mount target is defined on this subnet. Two additional subnets are required for SAP HANA inter-node (internal) communication, and for client access.

SAP HANA in scale-out configuration requires a shared volume for its **/hana/shared** file system, and a **/hana/log** and **/hana/data** volume for each node. Follow the [mount option recommendation by NetApp](#) for setting up your target OS' fstab. See the following sample for an SAP HANA system of system ID 'BHB':

1. **/hana/shared**

```
$ fsf-tok0551b-fz.adn.networklayer.com:/903586db_f968_4bf7_bbd5_0926fb7a26ce /hana/shared/BHB nfs  
sec=sys,rw,vers=4,minorversion=1,hard,timeo=600,rsize=65536,wsize=65536,intr,noatime,lock 0 0
```

2. **/hana/data**

```
$ fsf-tok0551a-fz.adn.networklayer.com:/2b33d3df_9081_47c2_910a_a29356716d51/BHB/mnt00001 /hana/data/BHB/mnt00001 nfs  
sec=sys,rw,vers=4,minorversion=1,hard,timeo=600,rsize=65536,wsize=65536,intr,noatime,lock 0 0  
fsf-tok0551b-fz.adn.networklayer.com:/ec39996c_346a_4815_a74f_4048382e6ecc/BHB/mnt00002 /hana/data/BHB/mnt00002 nfs  
sec=sys,rw,vers=4,minorversion=1,hard,timeo=600,rsize=65536,wsize=65536,intr,noatime,lock 0 0
```

3. **/hana/log**

```
$ fsf-tok0551b-fz.adn.networklayer.com:/7bdee46e_b95f_4ff7_89b8_5273e8f9199d/BHB/mnt00001 /hana/log/BHB/mnt00001 nfs
sec=sys,rw,vers=4,minorversion=1,hard,timeo=600,rsize=65536,wsize=65536,intr,noatime,lock 0 0
fsf-tok0551b-fz.adn.networklayer.com:/2bca0419_3aef_40ca_b38f_8b9717c93905/BHB/mnt00002 /hana/log/BHB/mnt00002 nfs
sec=sys,rw,vers=4,minorversion=1,hard,timeo=600,rsize=65536,wsize=65536,intr,noatime,lock 0 0
```

You cannot follow NetApp's recommendation regarding `rsize` and `wsize` option, these parameters are limited to 65536 by the file share implementation.

To fulfill SAP's requirements about storage layout and through-put and latency KPIs, see details here: [Persistent Data Storage in the SAP HANA Database](#)). In any case, they must comply with the TDI performance KPIs (see [SAP Note 2613646](#)) verified by [SAP HANA Hardware and Cloud Measurement Tools](#) and also ensure SAP's support for it. IBM Cloud recommends 10 IOPS per GB or Custom profile file shares for meeting SAP's KPIs.

Bare Metal Server certified profiles on VPC infrastructure for SAP HANA

Profiles list

The following table gives you an overview of the SAP-certified profiles with bare metal servers for VPC. The vCPUs in this list are CPU cores and their secondary threads. The term vCPU is kept for comparison with their virtual counterparts.

Profile	vCPU	Memory (RAM GiB)	SAPS	SAP HANA
				Processing Type
Compute Optimized				
cx2d-metal-96x192	96	192	107,400	SAP Business One (**)
Balanced				
bx2d-metal-96x384	96	384	124,130	OLTP/OLAP (*) SAP Business One (**)
Memory Optimized				
mx2d-metal-96x768	96	768	127,620	OLTP/OLAP (*) SAP Business One (**)
Ultra High Memory Optimized				
ux2d-metal-112x3072	112	3,072	140,730	OLTP/OLAP (*)
ux2d-metal-224x6144	224	6,144	294,730	OLTP/OLAP (*)

IBM Cloud Bare Metal Servers for VPC certified for SAP HANA - Intel Cascade Lake CPU

Profiles hosted on Intel Sapphire Rapids CPU

Profile	vCPU	Memory (RAM GiB)	SAPS	aSAPS (1)	SAP HANA
					Processing Type
Balanced					
bx3d-metal-48x256	48	256	93,670	18,400	OLTP/OLAP (*)
bx3d-metal-64x256	64	256	124,520	24,600	OLTP/OLAP (*)
bx3d-metal-192x1024	192	1.024	297,770	57,400	OLTP/OLAP (*)
Memory Optimized					
mx3d-metal-48x512	48	512	97,830	18,700	OLTP/OLAP (*)

mx3d-metal-64x512	64	512	128,750	24,200	OLTP/OLAP (*)
mx3d-metal-96x1024	96	1.024	182,670	33,700	OLTP/OLAP (*)
mx3d-metal-128x1024	128	1.024	239,300	46,000	OLTP/OLAP (*)

IBM Cloud Bare Metal Servers for VPC certified for SAP HANA - Intel Sapphire Rapids CPU

(1): aSAPS is the metric that is derived from the [SAP quote-to-cash \(Q2C\) Benchmark](#).

(*): RHEL 8.4 for SAP Solutions, RHEL 8.6 for SAP Solutions, RHEL 8.8 for SAP Solutions, RHEL 8.10 for SAP Solutions, RHEL 9.0 for SAP Solutions, RHEL 9.2 for SAP Solutions, RHEL 9.4 for SAP Solutions\n SLES 12 SP5, SLES 15 SP2, SLES 15 SP3, SLES 15 SP4, SLES 15 SP5, SLES 15 SP6

(**): SLES 15 SP2, SLES 15 SP3, SLES 15 SP4, SLES 15 SP5

For more information, see [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#).



Important: For SAP HANA deployments that use IBM Cloud Bare Metal Servers for VPC, only single-node deployments are supported. Multi-node / scale-out is not currently supported.

Understanding Bare Metal Server profile names

With IBM Cloud Bare Metal Servers for VPC, the profile families that are certified for SAP are: *Compute Optimized*, *Balanced*, *Memory Optimized*, and *Ultra High Memory Optimized*.

- *Compute Optimized* family profiles provide more compute power, and they have more cores with less memory.
- *Balanced* family profiles provide a good mix of performance and scalability for more common workloads.
- *Memory Optimized* and *Ultra High Memory Optimized* family profiles cater to memory intensive workloads, such as demanding database applications and in-memory analytics workloads, and are especially designed for SAP HANA workloads.

For more information, see [x86-64 bare metal server profiles](#).

The first letter of the profile name determines the profile family. The ratio of cores (*number of vCPUs*) to RAM (*amount of GiB*) is one of the key attributes of a profile family.

First letter	Characteristics of the related profile family	Ratio Cascade Lake	Ratio Sapphire Rapids
c	<i>Compute Optimized</i> family	1:2	n/a
b	<i>Balanced</i> family	1:4	1:4 or 1:5.33
m	<i>Memory Optimized</i> family	1:8	1:8 or 1:10.67
u	<i>Ultra High Memory Optimized</i> family	1:27.43	n/a

IBM Cloud Bare Metal Servers for VPC Profile Families

The bare metal server profile names are contextual and sequential. See the following example:

Profile name	Naming convention component	What it means
mx2d-metal-96x768	m	<i>Memory Optimized</i> family
	x	Intel x86_64 CPU architecture
	?	The Intel generation for the underlying hardware
	2	Cascade Lake
	3	Sapphire Rapids

d	the optional 'd' in the name indicates that the server is equipped with one or more SSD storage devices
—	<i>spacer</i>
metal	<i>metal</i> in the name indicates that this is a bare metal server
—	<i>spacer</i>
96	96 vCPU
x	<i>spacer</i>
768	768 GiB RAM

Profile naming for SAP HANA

Profiles available on Hourly Consumption Billing

All IBM Cloud Bare Metal Servers for VPC are available with Hourly Consumption Billing, which includes Suspend Discounts and Sustained Usage Discounts. With Suspend Discounts, storage charges occur only if the server is in shutdown state. With Sustained Usage Discount, the more a server is used, the less the cost per hour.

Storage specifications

When the bare metal server profiles for SAP HANA are initially provisioned, the servers all have one pre-configured disk (sda) and provide the root partition `/` with about 890 GB and the partition `/boot/efi` with 100 MB or less. Depending on storage volume type, the specific OS release and version the storage layout and partition sizes are differing a little.

In addition to these partitions, Bare Metal Servers for VPC have up to 8 NVMEs – depending on their RAM size – which need to be configured after the server deployment.

To fulfill the KPIs defined for SAP HANA, each profile needs different storage volumes that are listed in detail in the following sections. These storage configurations are recommended. They are certified storage layouts that comply with **SAP HANA Tailored Data Center Integration** (TDI) Phase 5.



Important: If a specific memory sizing needs to be performed, customers are advised to follow [the instructions here](#) and if it turns out that different logic volume sizes are required then in addition the [SAP HANA TDI Overview](#) and [SAP HANA TDI FAQ](#) must be considered. In that case, users must run SAP's performance measurement tool HCMT - see [SAP Note 2493172 - SAP HANA Hardware and Cloud Measurement Tools](#) and follow the instructions of the [HCMT guide](#) to check compliance with SAP's KPIs.



Note: This holds true especially, if file shares are used for SAP HANA installations. They can be deployed and mounted in arbitrary ways to provide additional storage, for example for backups, as needed. For SAP HANA data and log files, however, they have to be evaluated.

In any case, [SAP's recommended file system layout](#) must be available for SAP HANA deployment.

Bare Metal Servers for VPC - Storage Layouts

The following table shows the required physical volumes, related volume groups, logical volumes, and their characteristics:

Profile	File	Logical	LV Size	Volume Group	Physical
	system	Volume	(GiB)		Volume
cx2d-metal-96x192	/hana/shared	hana_shared_lv	192	vg0	nvme0n1- nvme3n1-
	/hana/log	hana_log_lv	192	vg0	
	/hana/data	hana_data_lv	min. 576	vg1	nvme4n1- nvme7n1-

bx2d-metal-96x384	/hana/shared	hana_shared_lv	384	vg0	nvme0n1- nvme3n1-
	/hana/log	hana_log_lv	384	vg0	
	/hana/data	hana_data_lv	min. 1,152	vg1	nvme4n1- nvme7n1-
mx2d-metal-96x768	/hana/shared	hana_shared_lv	768	vg0	nvme0n1- nvme3n1-
	/hana/log	hana_log_lv	512	vg0	
	/hana/data	hana_data_lv	min. 2,304	vg1	nvme4n1- nvme7n1-
ux2d-metal-112x3072	/hana/shared	hana_shared_lv	3,072	vg0	nvme0n1- nvme3n1-
	/hana/log	hana_log_lv	512	vg0	
	/hana/data	hana_data_lv	min. 9,216	vg1	nvme4n1- nvme7n1-
ux2d-metal-224x6144	/hana/shared	hana_shared_lv	6,144	vg0	nvme0n1- nvme1n1-
	/hana/log	hana_log_lv	512	vg0	
	/hana/data	hana_data_lv	<i>the remaining space ~17,190</i>	vg0	

Storage layout for Bare Metal Servers for VPC



Note: Profile `ux2d-metal-224x6144` is equipped with different set of disks, so jump directly to ["Steps for setting up storage for the ux2d-metal-224x6144 profile"](#).

Steps for setting up storage for the profiles up to 3,072 GiB

Note, that both volume groups vg0 and vg1 are not fully used. Remaining space can be used to extend the listed sizes, which are only minimum sizes, or can be used for other purposes. However, do not point I/O load at the remaining space since that impacts SAP HANA's performance.

To ensure a higher level of availability and failure resilience, RAID10 logical volumes are built on-top the under-laying NVMEs, based on Linux's logical volume manager.

These steps show a step-by-step guide for setting up the volume groups, logical volumes, and file systems. Size information differs and can be retrieved from the storage layout table.

1. Log in to the OS and install the lvm2 package, if not installed already.

```
$ [root@mx2d-metal-96x768 ~]# yum install lvm2
```

This command applies to RHEL, on SLES use 'zypper install' instead.

2. Create the volume groups.

```
$ [root@mx2d-metal-96x768 ~]# vgcreate vg0 /dev/nvme0n1 /dev/nvme1n1 /dev/nvme2n1 /dev/nvme3n1  
[root@mx2d-metal-96x768 ~]# vgcreate vg1 /dev/nvme4n1 /dev/nvme5n1 /dev/nvme6n1 /dev/nvme7n1
```

3. Create logical volumes on top of the volume groups.

```
$ [root@mx2d-metal-96x768 ~]# lvcreate --type raid10 -i 2 -m 1 -L 768G -I 64 -n hana_shared_lv vg0
```



Note: 768G needs to be adapted to the hana_shared volume size specific to your memory size in the sizing table. Sizes for hana_log can be found there, too, and can be used in the lvcreate command as well.

```
$ [root@mx2d-metal-96x768 ~]# lvcreate --type raid10 -i 2 -m 1 -L 512G -I 64 -n hana_log_lv vg0
```

4. Create hana_data. Either modify the size with the -L option according to the sizing table, or the use the entire volume group with -l 100%FREE :

```
$ [root@mx2d-metal-96x768 ~]# lvcreate --type raid10 -i 2 -m 1 -l 100%FREE -I 64 -n hana_data_lv vg1
```

5. Create file systems on the logical volumes. In this example, XFS is used and is mounted by label. Mount by label is not a requirement and can be adapted according to your needs:

```
$ [root@mx2d-metal-96x768 ~]# mkfs.xfs -L HANA_SHARED -K /dev/mapper/vg0-hana_shared_lv  
[root@mx2d-metal-96x768 ~]# mkfs.xfs -L HANA_LOG -K /dev/mapper/vg0-hana_log_lv  
[root@mx2d-metal-96x768 ~]# mkfs.xfs -L HANA_DATA -K /dev/mapper/vg1-hana_data_lv
```

6. Add the following lines to /etc/fstab and create the required directory paths with mkdir.

```
$ LABEL=HANA_SHARED /hana/shared xfs defaults 0 0  
LABEL=HANA_LOG /hana/log xfs defaults,swalloc,inode64 0 0  
LABEL=HANA_DATA /hana/data xfs defaults,largeio,swalloc,inode64 0 0
```

7. You can now mount the file systems.

Steps for setting up storage for the ux2d-metal-224x6144 profile

To ensure a higher level of availability and failure resilience, RAID1 logical volumes are built on-top the under-laying NVMEs, based on Linux's logical volume manager.

These steps show a step-by-step guide for setting up the volume groups, logical volumes, and file systems.

1. Log in to the OS and install the lvm2 package, if not installed already.

```
$ [root@ux2d-metal-224x6144 ~]# yum install lvm2
```

This command applies to RHEL, on SLES use 'zypper install' instead.

2. Create the volume group.

```
$ [root@ux2d-metal-224x6144 ~]# vgcreate vg0 /dev/nvme0n1 /dev/nvme1n1
```

3. Create logical volumes hana_shared_lv and hana_log_lv on top of the volume group.

```
$ [root@ux2d-metal-224x6144 ~]# lvcreate --type raid1 -L 6144G -n hana_shared_lv vg0  
[root@ux2d-metal-224x6144 ~]# lvcreate --type raid1 -L 512G -n hana_log_lv vg0
```

4. Create logical volume hana_data_lv.

```
$ [root@ux2d-metal-224x6144 ~]# lvcreate --type raid1 -l 100%FREE -n hana_data_lv vg0
```

5. Create file systems on the logical volumes. In this example, XFS is used and is mounted by label. Mount by label is not a requirement and can be adapted according to your needs:

```
$ [root@ux2d-metal-224x6144 ~]# mkfs.xfs -L HANA_SHARED -K /dev/mapper/vg0-hana_shared_lv  
[root@ux2d-metal-224x6144 ~]# mkfs.xfs -L HANA_LOG -K /dev/mapper/vg0-hana_log_lv  
[root@ux2d-metal-224x6144 ~]# mkfs.xfs -L HANA_DATA -K /dev/mapper/vg0-hana_data_lv
```

6. Add the following lines to `/etc/fstab` and create the required directory paths with `mkdir`.

```
$ LABEL=HANA_SHARED /hana/shared xfs defaults 0 0
LABEL=HANA_LOG /hana/log xfs defaults,swalloc,inode64 0 0
LABEL=HANA_DATA /hana/data xfs defaults,largeio,swalloc,inode64 0 0
```

7. You can now mount the file systems.

Check [SAP Note 2777782](#) for RHEL and [SAP Note 2684254](#) for SLES to adapt your OS configuration settings according to the requirements for SAP HANA.

Intel Bare Metal server certified profiles on Classic infrastructure for SAP HANA

Profiles list



Note: The published names are subject to change.

This table provides an overview of the SAP-certified profiles with Intel Bare Metal:

Profile	CPU Cores	CPU Threads (aka. vCPU)	Memory (RAM GB)	SAPS	SAP HANA Processing Type
BI.S3.H2.192 Appliance	36	72	192 GB	78,850	OLAP/OLTP ⁽¹⁾ SAP Business One ⁽³⁾
BI.S3.H2.384 Appliance	36	72	384 GB	79,430	OLAP/OLTP ⁽¹⁾ SAP Business One ⁽³⁾
BI.S3.H2.768 Appliance	36	72	768 GB	79,630	OLAP/OLTP ⁽¹⁾ SAP Business One ⁽³⁾
BI.S4.H2.192 Appliance	32	64	192 GB	82,470	OLAP/OLTP ⁽²⁾ SAP Business One ⁽³⁾
BI.S4.H2.384 Appliance	32	64	384 GB	85,130	OLAP/OLTP ⁽²⁾ SAP Business One ⁽³⁾
BI.S4.H2.384_v3 Appliance	16	32	384 GB	60,420	OLAP/OLTP ⁽²⁾
BI.S4.H2.768 Appliance	40	80	768 GB	112,830	OLAP/OLTP ⁽²⁾ SAP Business One ⁽³⁾
BI.S4.H2.768_v2 Appliance	48	96	768 GB	124,620	OLAP/OLTP ⁽²⁾
BI.S4.H2.768_v3 Appliance	16	32	768 GB	60,420	OLAP/OLTP ⁽²⁾
BI.S4.H2.1500 Appliance	56	112	1536 GB	147,220	OLAP/OLTP ⁽²⁾
BI.S4.H2.3000 Appliance	56	112	3072 GB	135,127	OLAP/OLTP ⁽²⁾
BI.S4.H4.3000 Appliance	112	224	3072 GB	285,970	OLAP/OLTP ⁽²⁾
BI.S4.H4.6000 Appliance	112	224	6144 GB	285,970	OLAP/OLTP ⁽²⁾
BI.S4.H8.6000 Appliance	224	448	6144 GB	550,670	OLAP/OLTP ⁽²⁾
BI.S4.H8.12000 Appliance	224	448	12288 GB	550,670	OLAP/OLTP ⁽²⁾
BI.S5.H2.1000 Appliance	96	192	1 TB	297,370	OLAP/OLTP ⁽⁴⁾

BI.S5.H2.2001 Appliance	96	192	2 TB	297,370	OLAP/OLTP ⁽⁴⁾
BI.S5.H2.2000 Appliance	120	240	2 TB	322,550	OLAP/OLTP ⁽⁴⁾
BI.S5.H2.3000 Appliance	120	240	3 TB	327,295	OLAP/OLTP ⁽⁴⁾
BI.S5.H2.4000 Appliance	120	240	4 TB	329,350	OLAP/OLTP ⁽⁴⁾

Certified IBM Cloud Bare Metal Servers for SAP HANA

⁽¹⁾: RHEL 7.4 for SAP Solutions, RHEL 7.6 for SAP Solutions, RHEL 7.9 for SAP Solutions, RHEL 8.2 for SAP Solutions\n SLES 12 SP2, SLES 12 SP4, SLES 12 SP5, SLES 15, SLES 15 SP1, SLES 15 SP2, SLES 15 SP3

⁽²⁾: RHEL 7.6 for SAP Solutions, RHEL 7.9 for SAP Solutions, RHEL 8.2 for SAP Solutions, RHEL 8.6 for SAP Solutions, RHEL 8.10 for SAP Solutions, RHEL 9.2 for SAP Solutions \n SLES 12 SP4, SLES 12 SP5, SLES 15, SLES 15 SP1, SLES 15 SP2, SLES 15 SP3, SLES 15 SP4

⁽³⁾: SLES 12 SP4, SLES 15, SLES 15 SP1, SLES 15 SP2, SLES 15 SP3, SLES 15 SP4

⁽⁴⁾: RHEL 8.10 for SAP Solutions, RHEL 8.6 for SAP Solutions, RHEL 9.2 for SAP Solutions, RHEL 9.4 for SAP Solutions \n SLES 15, SLES 15 SP1 , SLES 15 SP2, SLES 15 SP3, SLES 15 SP4



Note: Please regard the supported operated systems mentioned in the footnotes.

For more information see [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#).

A number of these Profiles are also available as "Boot-only" which have the same configuration but only the boot drives are inserted. This configuration lets you customize the Local SSD Storage and the attachment of either Network Block or File storage options.

Understanding Bare Metal profile names

The Bare Metal profile names are contextual and sequential. This example uses an SAP HANA certified server to list and describe the naming conventions:

Profile name	Naming convention component	What it means
BI.S4.H2.1500	BI	IBM Cloud Infrastructure
	S4	Series 4 (CPU generation) <ul style="list-style-type: none"> • S3: Intel Skylake/Kaby Lake • S4 is Intel Cascade Lake • S5: Intel Sapphire Rapids
	H	HANA-certified server
	2	2-socket server
	1500	1500 GB RAM

Profile naming scheme for SAP HANA certified servers

Profiles available on Hourly Consumption Billing

The following Bare Metal servers are available on **Hourly** Consumption Billing:

- BI.S4.H2.192 Appliance
- BI.S4.H2.384 Appliance
- BI.S4.H2.768 Appliance
- BI.S4.H2.1500 Appliance
- BI.S4.H2.3000 Appliance
- BI.S4.H2.192 (boot only)
- BI.S4.H2.384 (boot only)

- BI.S4.H2.768 (boot only)
- BI.S4.H2.1500 (boot only)
- BI.S4.H2.3000 (boot only)

Storage specifications

The following dual-socket servers are available in the Appliance delivery model for SAP HANA, with preconfigured disk storage.



Note: These Profiles do not use any Network Block or File storage options that are mounted to the Bare Metal server. These Profiles use only Local SSD Storage devices that are physically attached through a RAID Controller inside the server.

BI.S3.H2.192 Appliance

Link to Profile: [BI.S3.H2.192 Appliance](#)

Physical Disk and RAID Configuration

RAID	Components	Drives	Array	Total Capacity
RAID 1	2x 960 GB 5100	hdd0, hdd1	RAID1-A	960 GB
RAID 1	2x 960 GB 5100	hdd2, hdd3	RAID1-B	960 GB
Global hot spare	1x 960 GB 5100	hdd4		

Configuration for BI.S3.H2.192

Disk mount points and Partitions

Array	Partition	Name	Size (GB)
RAID1-A	/dev/sda		
	/dev/sda1	/boot	50
	/dev/sda2	/	150
	/dev/sda3	/usr/sap	150
	/dev/sda4	/hana/log	
RAID1-B	/dev/sdb		
	/dev/sdb1	/hana/shared	250
	/dev/sdb2	/hana/data	<i>remaining capacity</i>

Partitions for BI.S3.H2.192

BI.S3.H2.384 Appliance

Link to Profile: [BI.S3.H2.384 Appliance](#)

Physical Disk and RAID Configuration

RAID	Components	Drives	Array	Total Capacity
RAID 1	2x 960 GB 5100	hdd0, hdd1	RAID1-A	960 GB
RAID 10	4x 960 GB 5100	hdd2, hdd3, hdd4, hdd5	RAID1-B	1920 GB

Global hot spare	1x 960 GB 5100	hdd6
Configuration for BI.S3.H2.384		

Disk mount points and Partitions

Array	Partition	Name	Size (GB)
RAID1-A	/dev/sda		
	/dev/sda1	/boot	50
	/dev/sda2	/	150
	/dev/sda3	/usr/sap	150
RAID1-B	/dev/sda4	/hana/log	<i>remaining capacity</i>
	/dev/sdb		
	/dev/sdb1	/hana/shared	500
	/dev/sdb2	/hana/data	<i>remaining capacity</i>

Partitions for BI.S3.H2.384

BI.S3.H2.768 Appliance

Link to Profile: [BI.S3.H2.768 Appliance](#)

Physical Disk and RAID Configuration

RAID	Components	Drives	Array	Total Capacity
RAID 1	2x 960 GB 5100	hdd0, hdd1	RAID1-A	960 GB
RAID 10	4x 960 GB 5100	hdd2, hdd3, hdd4, hdd5	RAID1-B	1920 GB
Global hot spare	1x 960 GB 5100	hdd6		

Configuration for BI.S3.H2.768

Disk mount points and Partitions

Array	Partition	Name	Size (GB)
RAID1-A	/dev/sda		
	/dev/sda1	/boot	50
	/dev/sda2	/	150
	/dev/sda3	/usr/sap	150
RAID1-B	/dev/sda4	/hana/log	<i>remaining capacity</i>
	/dev/sdb		
	/dev/sdb1	/hana/shared	800

	/dev/sdb2	/hana/data	<i>remaining capacity</i>
Partitions for BI.S3.H2.768			
BI.S4.H2.192 Appliance			

Link to Profile: [BI.S4.H2.192 Appliance](#)

Physical Disk and RAID Configuration

RAID	Components	Drives	Array	Total Capacity
RAID 1	2x 960 GB 5100	hdd0, hdd1	RAID1-A	960 GB
RAID 1	2x 960 GB 5100	hdd2, hdd3	RAID1-B	960 GB
Global hot spare	1x 960 GB 5100	hdd4		

Configuration for BI.S4.H2.192

Disk mount points and Partitions

Array	Partition	Name	Size (GB)
RAID1-A	/dev/sda		
	/dev/sda1	/boot	50
	/dev/sda2	/	150
	/dev/sda3	/usr/sap	150
	/dev/sda4	/hana/log	<i>remaining capacity</i>
RAID1-B	/dev/sdb		
	/dev/sdb1	/hana/shared	250
	/dev/sdb2	/hana/data	<i>remaining capacity</i>

Partitions for BI.S4.H2.192

BI.S4.H2.384 and BI.S4.H2.384_v2 Appliance

Link to Profile: [BI.S4.H2.384 Appliance](#)

Physical Disk and RAID Configuration

RAID	Components	Drives	Array	Total Capacity
RAID 1	2x 960 GB 5100	hdd0, hdd1	RAID1-A	960 GB
RAID 10	4x 960 GB 5100	hdd2, hdd3, hdd4, hdd5	RAID1-B	1920 GB
Global hot spare	1x 960 GB 5100	hdd6		

Configuration for BI.S4.H2.384

Disk mount points and Partitions

Array	Partition	Name	Size (GB)
-------	-----------	------	-----------

RAID1-A	<code>/dev/sda</code>		
	<code>/dev/sda1</code>	<code>/boot</code>	50
	<code>/dev/sda2</code>	<code>/</code>	150
	<code>/dev/sda3</code>	<code>/usr/sap</code>	150
	<code>/dev/sda4</code>	<code>/hana/log</code>	<i>remaining capacity</i>
RAID1-B	<code>/dev/sdb</code>		
	<code>/dev/sdb1</code>	<code>/hana/shared</code>	500
	<code>/dev/sdb2</code>	<code>/hana/data</code>	<i>remaining capacity</i>
	Partitions for BI.S4.H2.384		

BI.S4.H2.768, BI.S4.H2.768_v2, and BI.S4.H2.768_v3 Appliance

Link to Profile: [BI.S4.H2.768 Appliance](#)

Physical Disk and RAID Configuration

RAID	Components	Drives	Array	Total Capacity
RAID 1	2x 960 GB 5100	<code>hdd0</code> , <code>hdd1</code>	RAID1-A	960 GB
RAID 10	4x 960 GB 5100	<code>hdd2</code> , <code>hdd3</code> , <code>hdd4</code> , <code>hdd5</code>	RAID1-B	1920 GB
Global hot spare	1x 960 GB 5100	<code>hdd6</code>		
Configuration for BI.S4.H2.768				

Disk mount points and Partitions

Array	Partition	Name	Size (GB)
RAID1-A	<code>/dev/sda</code>		
	<code>/dev/sda1</code>	<code>/boot</code>	50
	<code>/dev/sda2</code>	<code>/</code>	150
	<code>/dev/sda3</code>	<code>/usr/sap</code>	150
	<code>/dev/sda4</code>	<code>/hana/log</code>	<i>remaining capacity</i>
RAID1-B	<code>/dev/sdb</code>		
	<code>/dev/sdb1</code>	<code>/hana/shared</code>	800
	<code>/dev/sdb2</code>	<code>/hana/data</code>	<i>remaining capacity</i>
	Partitions for BI.S4.H2.768		

BI.S4.H2.1500 Appliance

Link to Profile: [BI.S4.H2.1500 Appliance](#)

Physical Disk and RAID Configuration

RAID	Components	Drives	Array	Total Capacity
RAID 1	2x 960 GB SSD SED	hdd0, hdd1	RAID1-A	960 GB
RAID 1	2x 3.8 TB SSD SED	hdd2, hdd3	RAID1-B	3.8 TB
Global hot spare	1x 3.8 TB SSD SED	hdd4		

Configuration for BI.S4.H2.1500

Disk mount points and Partitions

Array	Partition	Name	Size (GB)
RAID1-A	/dev/sda		
	/dev/sda1	/boot	50
	/dev/sda2	/	150
	/dev/sda3	/usr/sap	150
RAID1-B	/dev/sda4	/hana/log	<i>remaining capacity</i>
	/dev/sdb		
	/dev/sdb1	/hana/shared	1024
	/dev/sdb2	/hana/data	<i>remaining capacity</i>

Partitions for BI.S4.H2.1500

BI.S4.H2.3000 Appliance

Link to Profile: [BI.S4.H2.3000 Appliance](#)

Physical Disk and RAID Configuration

RAID	Components	Drives	Array	Total Capacity
RAID 1	2x 960 GB SSD SED	hdd0, hdd1	RAID1-A	960 GB
RAID 10	4x 3.8 TB SSD SED	hdd2, hdd3, hdd4, hdd5	RAID1-B	7.6 TB
Global hot spare	1x 3.8 TB SSD SED	hdd6		

Configuration for BI.S4.H2.3000

Disk mount points and Partitions

Array	Partition	Name	Size (GB)
RAID1-A	/dev/sda		
	/dev/sda1	/boot	50
	/dev/sda2	/	150
	/dev/sda3	/usr/sap	150

	/dev/sda4	/hana/log	<i>remaining capacity</i>
RAID1-B	/dev/sdb		
	/dev/sdb1	/hana/shared	1024
	/dev/sdb2	/hana/data	<i>remaining capacity</i>
Partitions for BI.S4.H2.3000			

BI.S4.H4.3000 Appliance

Link to Profile: [BI.S4.H4.3000 Appliance](#)

Physical Disk and RAID Configuration

RAID	Components	Drives	Array	Total Capacity
RAID 1	2x 960 GB SSD SED	hdd0, hdd1	RAID1-A	960 GB
RAID 10	4x 3.8 TB SSD SED	hdd2, hdd3, hdd4, hdd5	RAID1-B	7.6 TB
Global hot spare	1x 3.8 TB SSD SED	hdd6		
Configuration for BI.S4.H4.3000				

Disk mount points and Partitions

Array	Partition	Name	Size (GB)
RAID1-A	/dev/sda		
	/dev/sda1	/boot	50
	/dev/sda2	/	150
	/dev/sda3	/usr/sap	150
	/dev/sda4	/hana/log	<i>remaining capacity</i>
RAID1-B	/dev/sdb		
	/dev/sdb1	/hana/shared	1024
	/dev/sdb2	/hana/data	<i>remaining capacity</i>
Partitions for BI.S4.H4.3000			

BI.S4.H4.6000 Appliance

Link to Profile: [BI.S4.H4.6000 Appliance](#)

Physical Disk and RAID Configuration

RAID	Components	Drives	Array	Total Capacity
RAID 1	2x 960 GB SSD SED	hdd0, hdd1	RAID1-A	960 GB
RAID 10	4x 3.8 TB SSD SED	hdd2, hdd3, hdd4, hdd5	RAID1-B	7.6 TB
Global hot spare	1x 3.8 TB SSD SED	hdd6		
Configuration for BI.S4.H4.6000				

Disk mount points and Partitions

Array	Partition	Name	Size (GB)
RAID1-A	/dev/sda		
	/dev/sda1	/boot	50
	/dev/sda2	/	150
	/dev/sda3	/usr/sap	150
RAID1-B	/dev/sdb		
	/dev/sdb1	/hana/shared	1024
	/dev/sdb2	/hana/data	<i>remaining capacity</i>

Partitions for BI.S4.H4.6000

BI.S4.H8.6000 Appliance

Link to Profile: [BI.S4.H8.6000 Appliance](#)

Physical Disk and RAID Configuration

RAID	Components	Drives	Array	Total Capacity
RAID 1	2x 960 GB SSD SED	hdd0, hdd1	RAID1-A	960 GB
RAID 10	4x 3.8 TB SSD SED	hdd2, hdd3, hdd4, hdd5	RAID1-B	7.6 TB
Global hot spare	1x 3.8 TB SSD SED	hdd6		

Configuration for BI.S4.H8.6000

Disk mount points and Partitions

Array	Partition	Name	Size (GB)
RAID1-A	/dev/sda		
	/dev/sda1	/boot	50
	/dev/sda2	/	150
	/dev/sda3	/usr/sap	150
RAID1-B	/dev/sdb		
	/dev/sdb1	/hana/shared	1024
	/dev/sdb2	/hana/data	<i>remaining capacity</i>

Partitions for BI.S4.H8.6000

BI.S4.H8.12000 Appliance

Link to Profile: [BI.S4.H8.12000 Appliance](#)

Physical Disk and RAID Configuration

RAID	Components	Drives	Array	Total Capacity
RAID 1	2x 960 GB SSD SED	hdd0, hdd1	RAID1-A	960 GB
RAID 10	8x 3.8 TB SSD SED	hdd2, hdd3, hdd4, hdd5, hdd6, hdd7, hdd8, hdd9	RAID1-B	15.2 TB
Global hot spare	1x 3.8 TB SSD SED	hdd10		

Configuration for BI.S4.H8.12000

Disk mount points and Partitions

Array	Partition	Name	Size (GB)
RAID1-A	/dev/sda		
	/dev/sda1	/boot	50
	/dev/sda2	/	150
	/dev/sda3	/usr/sap	150
RAID1-B	/dev/sda4	/hana/log	<i>remaining capacity</i>
	/dev/sdb		
	/dev/sdb1	/hana/shared	1024
	/dev/sdb2	/hana/data	<i>remaining capacity</i>

Partitions for BI.S4.H8.12000

BI.S5.H2.1000 Appliance

Link to Profile: [BI.S5.H2.1000 Appliance](#)

Physical Disk and RAID Configuration

By default, a boot volume is attached to the instance, mapped to `/dev/nvme0n1`. The default boot volume size is 480 GB which is composed of two 480 GB SSDs in RAID1 for redundancy. In addition this server has 5 x 3.2 TB sized NVMe local storage mapped to `/dev/nvme#n1`, # being the disk number 1 to 5.

Disk mount points and Partitions

Partition	Name	Size (GB)
/dev/nvme0n1p2	/boot	10
/dev/nvme0n1p3	/	150
/dev/nvme0n1p5	/usr/sap	137
/dev/nvme3n1	/hana/log	1,000
/dev/nvme2n1	/hana/shared	3,000

/dev/nvme4n1	/hana/data	3,000
Configuration for BI.S5.H2.1000		

BI.S5.H2.2001 Appliance

Link to Profile: [BI.S5.H2.2001 Appliance](#)

Physical Disk and RAID Configuration

By default, a boot volume is attached to the instance, mapped to `/dev/nvme0n1`. The default boot volume size is 480 GB which is composed of two 480 GB SSDs in RAID1 for redundancy. In addition this server has 7 x 3.2 TB sized NVMe local storage mapped to `/dev/nvme#n1`, # being the disk number 1 to 7.

Disk mount points and Partitions

Partition	Name	Size (GB)
<code>/dev/nvme0n1p2</code>	<code>/boot</code>	10
<code>/dev/nvme0n1p3</code>	/	150
<code>/dev/nvme1n1</code>	<code>/usr/sap</code>	3,000
<code>/dev/nvme5n1</code>	<code>/hana/log</code>	3,000
<code>/dev/nvme4n1</code>	<code>/hana/shared</code>	3,000
<code>/dev/mapper/hana_data_vg-hana_data_lv</code>	<code>/hana/data</code>	5,900

Configuration for BI.S5.H2.2001

Boot-only servers

By default, IBM Cloud Bare Metal Servers come with high-performance and highly reliable internal storage based on solid-state disks and high-performance RAID adapters.

For projects with different requirements, such as storage snapshots, that don't have a very high through-put requirement, IBM Cloud offers "boot-only servers."

Boot-only servers have the same configuration as standard Bare Metal Servers, however, only the boot disks for the operating system are configured. The storage required for the SAP file systems - `/usr/sap`, `/hana/shared`, `/hana/data`, and `/hana/log` - is not provided, significantly reducing the server cost.

To run SAP HANA on a boot-only server, you must add IBM Cloud storage to the server.

SAP HANA Tailored Data Center Integration (TDI) requirements must be met to run SAP HANA as Production for the SAP System/s, or in a production-like environment. To fulfill SAP HANA TDI key performance indicators (TDIs), storage performance must meet minimum values.

IBM Cloud File Storage for Classic with Boot-only services

To run SAP HANA in production and production-like setups that use IBM Cloud File Storage for Classic, based on the Network File System (NFS) protocol, requires:

- Minimum of 8 K IOPS for `/hana/log`
- Minimum of 7 K IOPS for `/hana/data`

You can share storage areas for `/hana/shared` with `/hana/log` or `/hana/data` if these areas are too large for your particular use case.

For non-production use, you can use one storage area for `/hana/shared`, `/hana/log`, and `/hana/data`.

These minimums are for either *Endurance* or *Performance* options available with IBM Cloud File Storage for Classic:

- Endurance storage is a predefined IOPS per GB of storage, for example, 0.25 up to 10 IOPS per GB.
- Performance storage has different ranges of IOPS per GB, depending on the total size of the storage device. This option is more customizable.

This table compares the file storage (using NFS protocol) and the performance IOPS range for the capacity:

File Storage capacity (GB)	Performance custom IOPS
20-39	100-1,000
40-79	100-2,000
80-99	100-4,000
100-499	100-6,000
500-999	100-10,000
1,000-1,999	100-20,000
2,000-2,999	200-40,000
3,000-3,999	200-48,000
4,000-7,999	300-48,000
8,000-9,999	500-48,000
10,000-12,000	1,000-48,000
Up to 24,000	Up to 96,000 by special request
Up to 18,000	Up to 180,000 by special request

IBM Cloud File Storage for Classic Performance storage GB and IOPS

BI.S4.H2.192 (boot only)

Link to Profile: [BI.S4.H2.192 \(boot only\)](#)

Required configuration of disk mount points and Partitions

Array	Partition	Name	Size (GB)
RAID1-A	/dev/sda		
	/dev/sda1	/boot	50
	/dev/sda2	/	150
	/dev/sda3	/usr/sap	150
RAID1-B	/dev/sda4	/hana/log	<i>remaining capacity</i>
	/dev/sdb		
	/dev/sdb1	/hana/shared	250
	/dev/sdb2	/hana/data	<i>remaining capacity</i>

Configuration for BI.S4.H2.192 (boot only)

BI.S4.H2.384 (boot only)

Link to Profile: [BI.S4.H2.384 \(boot only\)](#)

Required configuration of disk mount points and Partitions

Array	Partition	Name	Size (GB)
RAID1-A	/dev/sda		
	/dev/sda1	/boot	50
	/dev/sda2	/	150
	/dev/sda3	/usr/sap	150
RAID1-B	/dev/sdb		
	/dev/sdb1	/hana/shared	500
	/dev/sdb2	/hana/data	<i>remaining capacity</i>
			Configuration for BI.S4.H2.384 (boot only)

BI.S4.H2.768 (boot only)

Link to Profile: [BI.S4.H2.768 \(boot only\)](#)

Required configuration of disk mount points and Partitions

Array	Partition	Name	Size (GB)
RAID1-A	/dev/sda		
	/dev/sda1	/boot	50
	/dev/sda2	/	150
	/dev/sda3	/usr/sap	150
RAID1-B	/dev/sdb		
	/dev/sdb1	/hana/shared	800
	/dev/sdb2	/hana/data	<i>remaining capacity</i>
			Configuration for BI.S4.H2.768 (boot only)

BI.S4.H2.1500 (boot only)

Link to Profile: [BI.S4.H2.1500 \(boot only\)](#)

Required configuration of disk mount points and Partitions

Array	Partition	Name	Size (GB)
RAID1-A	/dev/sda		
	/dev/sda1	/boot	50

	/dev/sda2	/	150
	/dev/sda3	/usr/sap	150
	/dev/sda4	/hana/log	<i>remaining capacity</i>
RAID1-B	/dev/sdb		
	/dev/sdb1	/hana/shared	1024
	/dev/sdb2	/hana/data	<i>remaining capacity</i>

Configuration for BI.S4.H2.1500 (boot only)

BI.S4.H2.3000 (boot only)

Link to Profile: [BI.S4.H2.3000 \(boot only\)](#)

Required configuration of disk mount points and Partitions

Array	Partition	Name	Size (GB)
RAID1-A	/dev/sda		
	/dev/sda1	/boot	50
	/dev/sda2	/	150
	/dev/sda3	/usr/sap	150
	/dev/sda4	/hana/log	<i>remaining capacity</i>
RAID1-B	/dev/sdb		
	/dev/sdb1	/hana/shared	1024
	/dev/sdb2	/hana/data	<i>remaining capacity</i>

Configuration for BI.S4.H2.3000 (boot only)

VMware SDDC certified profiles for SAP HANA

Profiles list



Note: The published names are subject to change.

The following table is an overview of the SAP-certified profiles with either:

- Intel Bare Metal and VMware vSphere (ESXi), manual VMware setup and configuration
- IBM Cloud for VMware Solutions Dedicated, automated VMware SDDC setup and configuration

Profile	CPU	CPU Threads (also known as. vCPU)	Memory (RAM	SAPS (after VMware hypervisor 10%)	SAP HANA Processing
	Cores		GiB)		Type
BI.S3.H2.192 (VMware)	36	72	192 GB	70,965	OLAP/OLTP
BI.S3.H2.384 (VMware)	36	72	384 GB	71,487	OLAP/OLTP

BI.S3.H2.768 (VMware)	36	72	768 GB	71,667	OLAP/OLTP
BI.S4.H2.192 (VMware)	32	64	192 GB	74,223	OLAP/OLTP
BI.S4.H2.384 (VMware)	32	64	384 GB	76,617	OLAP/OLTP
BI.S4.H2.768 (VMware)	40	80	768 GB	101,547	OLAP/OLTP
BI.S4.H2.1500 (VMware)	56	112	1536 GB	132,498	OLAP/OLTP
BI.S4.H2.3000 (VMware)	56	112	3072 GB	121,614	OLAP/OLTP
BI.S4.H4.3000 (VMware)	112	224	3072 GB	257,373	OLAP/OLTP
BI.S4.H4.6000 (VMware)	112	224	6144 GB	257,373	OLAP/OLTP
BI.S4.H8.6000 (VMware)	224	448	6144 GB	495,603	OLAP/OLTP

SAP HANA servers

Understanding Bare Metal profile names

The Bare Metal profile names are contextual and sequential, below uses an SAP HANA certified server as an example:

Profile name	Naming convention component	What it means
BI.S4.H4.3000	BI	IBM Cloud Infrastructure
	S3	Series 3 (processor generation) <ul style="list-style-type: none"> • S3 is Intel Skylake/Kaby Lake • S4 is Intel Cascade Lake
	H	HANA-certified server
		#-socket server (2, 4 or 8)

GiB RAM (rounded, exact RAM amount is in the table)

Profile naming for SAP HANA

SAP HANA certified instances on IBM Power Virtual Server

A SAP HANA certified instance or profile on IBM Power Virtual Server defines attributes, such as physical CPU cores and RAM, which determine the size and performance capabilities of the virtual server instance.

SAP HANA Profile Naming Convention

Provision SAP HANA on IBM Power Virtual Servers by selecting one of the certified profiles.

SAP HANA profile names follow a contextual and sequential naming convention. The following table illustrates an example of an SAP HANA certified instance profile:

Profile name	Naming convention component	Description
sh2-33x1900	sh2	Profile prefix
	-	separator
	33	33 physical CPU Cores
	x	separator
	1900	1900 GiB RAM

Profile naming scheme for SAP HANA



Note: Refer to [SAP Note 2947579 - SAP HANA on IBM Power Virtual Servers](#) for up-to-date information on certified SAP HANA profiles.

Simultaneous Multithreading (SMT) on IBM Power for SAP HANA

SAP HANA profiles for Power servers operate in **SMT4 or SMT8 mode**. Simultaneous Multithreading (SMT) on IBM Power enables multiple independent threads to execute within a single physical processor core.

1. In **SMT4 mode**, four parallel threads can run on a single physical processor core. The operating system sees four logical processors per physical processor core.
2. In **SMT8 mode**, eight parallel threads can run on a single physical processor core. The operating system sees eight logical processors per physical processor core.

IBM Power10 Certified Instances for SAP HANA

The following table lists available profile families for IBM Power10 processor-based servers:

Families	Description
Profiles with sr2 prefix	Profiles with the prefix <code>sr2</code> are custom profiles that support selection of any combination of physical CPU cores and memory. Combinations that are certified by SAP for productive usage are documented in SAP Note 2947579 - SAP HANA on IBM Power Virtual Servers and in SAP HANA hardware directory . Custom profiles may be deployed through CLI or API only.
Profiles with sh2 prefix	Profiles with the prefix <code>sh2</code> support HANA database sizes up to 1900 GiB.
Profiles with bh2 prefix	Profiles with the prefix <code>bh2</code> are balanced profiles and are best suited for midsize databases and common cloud applications with moderate traffic.
Profiles with ch2 prefix	Profiles with the prefix <code>ch2</code> are compute intensive profiles and are best suited for moderate to high web traffic workloads. Compute profiles are best suited for cpu-intensive workloads, such as heavy web traffic, production batch processing, and front-end web servers.

Profile families for Power10 server generation

sr2 - Certified Profiles

The following SAP HANA profiles with prefix **sr2** on IBM Power Virtual Server are supported:

Profile name	CPU cores	Virtual CPUs	Memory (GiB)	SAPS	SMT Mode	Workload Type
sr2-7x256	7	28	256	42,000	SMT4	OLTP

sr2-7x384	7	28	384	42,000	SMT4	OLTP
sr2-14x512	14	56	512	84,000	SMT4	OLTP
sr2-14x740	14	56	740	84,000	SMT4	OLTP/OLAP
sr2-12x950	12	48	950	72,000	SMT4	OLTP/OLAP
sr2-24x1024	24	96	1,024	144,000	SMT4	OLTP/OLAP
sr2-12x1450	12	48	1,450	72,000	SMT4	OLTP/OLAP
sr2-24x1536	24	96	1,536	144,000	SMT4	OLTP/OLAP
sr2-25x1900	25	200	1,900	190,000	SMT8	OLTP/OLAP
sr2-22x2950	22	88	2,950	132,000	SMT4	OLTP/OLAP
sr2-35x3000	35	280	3,000	266,000	SMT8	OLTP/OLAP
sr2-40x3072	40	160	3,072	240,000	SMT4	OLTP/OLAP
sr2-35x3900	35	280	3,900	266,000	SMT8	OLTP/OLAP
sr2-35x4450	35	140	4,450	210,000	SMT4	OLTP/OLAP
sr2-87x6000	87	696	6,000	661,200	SMT8	OLTP/OLAP
sr2-80x6144	80	640	6,144	608,000	SMT8	OLTP/OLAP
sr2-64x6144	64	256	6,144	384,000	SMT4	OLTP/OLAP
sr2-87x7000	87	696	7,000	661,200	SMT8	OLTP/OLAP
sr2-87x7600	87	696	7,600	661,200	SMT8	OLTP/OLAP
sr2-80x9216	80	320	9,216	480,000	SMT4	OLTP/OLAP
sr2-80x12288	80	320	12,288	480,000	SMT4	OLTP/OLAP
sr2-80x14400	80	320	14,400	480,000	SMT4	OLTP/OLAP
sr2-165x30500	165	1,320	30,500	1,254,000	SMT8	OLTP/OLAP/OLTP scale-out (up to 4 nodes)

P10 Certified Instance profiles with sr2 prefix

sr2 Certified profile	IOPs required	Sample storage config	Sample storage tier	IOPs obtained	Alternative configuration (cost effective)
sr2-7x256	12,000	4 x 128 GB	Tier 0	12,800	4 x 32 GB using 'Fixed IOPs'
sr2-7x384	12,000	4 x 128 GB	Tier 0	12,800	4 x 32 GB using 'Fixed IOPs'
sr2-14x512	12,000	4 x 128 GB	Tier 0	12,800	4 x 64 GB using 'Fixed IOPs'

sr2-14x740	12,000	4 x 128 GB	Tier 0	12,800	4 x 92 GB using 'Fixed IOPs'
sr2-12x950	12,000	4 x 128 GB	Tier 0	12,800	
sr2-24x1024	12,000	4 x 128 GB	Tier 0	12,800	
sr2-12x1450	12,000	4 x 128 GB	Tier 0	12,800	
sr2-24x1536	12,000	4 x 128 GB	Tier 0	12,800	
sr2-25x1900	12,000	4 x 128 GB	Tier 0	12,800	
sr2-22x2950	12,000	4 x 128 GB	Tier 0	12,800	
sr2-35x3000	12,000	4 x 128 GB	Tier 0	12,800	
sr2-40x3072	12,000	4 x 128 GB	Tier 0	12,800	
sr2-35x3900	12,000	4 x 128 GB	Tier 0	12,800	
sr2-35x4450	12,000	4 x 128 GB	Tier 0	12,800	
sr2-87x6000	12,000	4 x 128 GB	Tier 0	12,800	
sr2-64x6144	12,000	4 x 128 GB	Tier 0	12,800	
sr2-80x6144	12,000	4 x 128 GB	Tier 0	12,800	
sr2-87x7000	12,000	4 x 128 GB	Tier 0	12,800	
sr2-87x7600	12,000	4 x 128 GB	Tier 0	12,800	
sr2-80x9216	12,000	4 x 128 GB	Tier 0	12,800	
sr2-80x12288	12,000	4 x 128 GB	Tier 0	12,800	
sr2-80x14400	12,000	4 x 128 GB	Tier 0	12,800	
sr2-165x30500	12,000	4 x 128 GB	Tier 0	12,800	
Sample log file system configurations for SAP HANA profiles with sr2 prefix					
sr2 Certified profile	IOPs required	Sample storage config	Sample storage tier	IOPs obtained	Alternative configuration (cost effective)
sr2-7x256	8,000	4 x 670 GB	Tier 3	8,400	4 x 103 GB using 'Tier 0'
sr2-7x384	8,000	4 x 670 GB	Tier 3	8,400	4 x 154 GB using 'Tier 0'
sr2-14x512	8,000	4 x 670 GB	Tier 3	8,400	4 x 206 GB using 'Tier 0'
sr2-14x740	8,000	4 x 670 GB	Tier 3	8,400	4 x 298 GB using 'Tier 0'

sr2-12x950	8,000	4 x 670 GB	Tier 3	8,400
sr2-24x1024	8,000	4 x 670 GB	Tier 3	8,400
sr2-12x1450	8,000	4 x 670 GB	Tier 3	8,400
sr2-24x1536	8,000	4 x 670 GB	Tier 3	8,400
sr2-25x1900	8,000	4 x 765 GB	Tier 3	9,180
sr2-22x2950	8,000	4 x 1188 GB	Tier 3	14,256
sr2-35x3000	8,000	4 x 1208 GB	Tier 3	14,499
sr2-40x3072	8,000	4 x 1237 GB	Tier 3	14,844
sr2-35x3900	8,000	4 x 1570 GB	Tier 3	18,846
sr2-35x4450	8,000	4 x 1792 GB	Tier 3	21,504
sr2-87x6000	8,000	4 x 2416 GB	Tier 3	28,998
sr2-64x6144	8,000	4 x 2474 GB	Tier 3	29,691
sr2-80x6144	8,000	4 x 2474 GB	Tier 3	29,691
sr2-87x7000	8,000	4 x 2819 GB	Tier 3	33,831
sr2-87x7600	8,000	4 x 3060 GB	Tier 3	36,729
sr2-80x9216	8,000	4 x 3711 GB	Tier 3	44,538
sr2-80x12288	8,000	4 x 4948 GB	Tier 3	59,385
sr2-80x14400	8,000	4 x 5799 GB	Tier 3	69,594
sr2-165x30500	8,000	4 x 12283 GB	Tier 3	147,405

Sample data file system configurations for SAP HANA profiles with sr2 prefix

sr2 Certified profile	IOPs required	Sample storage config	Sample storage tier	IOPs obtained	Alternative configuration
sr2-7x256	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
sr2-7x384	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
sr2-14x512	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
sr2-14x740	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
sr2-12x950	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'

sr2-24x1024	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
sr2-12x1450	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
sr2-24x1536	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
sr2-25x1900	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
sr2-22x2950	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
sr2-35x3000	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
sr2-40x3072	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
sr2-35x3900	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
sr2-35x4450	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
sr2-87x6000	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
sr2-64x6144	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
sr2-80x6144	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
sr2-87x7000	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
sr2-87x7600	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
sr2-80x9216	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
sr2-80x12288	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
sr2-80x14400	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
sr2-165x30500	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'

Sample shared file system configurations for SAP HANA profiles with sr2 prefix

sh2 - Certified Profiles

The following SAP HANA profiles with prefix **sh2** on IBM Power Virtual Server are supported:

Profile name	CPU cores	Virtual CPUs	Memory (GiB)	SAPS	SMT Mode	Workload Type
--------------	-----------	--------------	--------------	------	--------------------------	---------------

sh2-4x256	4	16	256	24,000	SMT4	OLTP
sh2-12x256	12	48	256	42,000	SMT4	OLTP
sh2-7x256	7	28	256	42,000	SMT4	OLTP
sh2-4x384	4	16	384	24,000	SMT4	OLTP
sh2-7x384	7	28	384	42,000	SMT4	OLTP
sh2-12x384	12	48	384	42,000	SMT4	OLTP
sh2-4x512	4	16	512	24,000	SMT4	OLTP
sh2-7x512	7	28	512	42,000	SMT4	OLTP
sh2-12x512	12	48	512	42,000	SMT4	OLTP
sh2-4x768	4	16	768	24,000	SMT4	OLTP
sh2-7x768	7	28	768	42,000	SMT4	OLTP
sh2-12x768	12	48	768	42,000	SMT4	OLTP/OLAP
sh2-4x1000	4	16	1,000	24,000	SMT4	OLTP
sh2-12x1000	12	48	1,000	42,000	SMT4	OLTP/OLAP
sh2-7x1000	7	28	1,000	42,000	SMT4	OLTP
sh2-16x1000	16	64	1,000	96,000	SMT4	OLTP/OLAP
sh2-25x1000	25	100	1,000	150,000	SMT4	OLTP/OLAP
sh2-4x1500	4	16	1,500	24,000	SMT4	OLTP
sh2-7x1500	7	28	1,500	42,000	SMT4	OLTP
sh2-12x1500	12	48	1,500	42,000	SMT4	OLTP/OLAP
sh2-16x1500	16	64	1,500	96,000	SMT4	OLTP/OLAP
sh2-25x1500	25	100	1,500	150,000	SMT4	OLTP/OLAP
sh2-8x1900	8	64	1,900	60,800	SMT8	OLTP
sh2-16x1900	16	128	1,900	121,600	SMT8	OLTP/OLAP
sh2-25x1900	25	200	1,900	190,000	SMT8	OLTP/OLAP
sh2-33x1900	33	264	1,900	250,800	SMT8	OLTP/OLAP

P10 Certified Instance profiles with sh2 prefix

sh2 Certified profile	IOPs required	Sample storage config	Sample storage tier	IOPs obtained	Alternative configuration (cost effective)
--------------------------	------------------	--------------------------	------------------------	------------------	---

sh2-4x256	12,000	4 x 128 GB	Tier 0	12,800	4 x 32 GB using 'Fixed IOPs'
sh2-7x256	12,000	4 x 128 GB	Tier 0	12,800	4 x 32 GB using 'Fixed IOPs'
sh2-12x256	12,000	4 x 128 GB	Tier 0	12,800	4 x 32 GB using 'Fixed IOPs'
sh2-4x384	12,000	4 x 128 GB	Tier 0	12,800	4 x 48 GB using 'Fixed IOPs'
sh2-7x384	12,000	4 x 128 GB	Tier 0	12,800	4 x 48 GB using 'Fixed IOPs'
sh2-12x384	12,000	4 x 128 GB	Tier 0	12,800	4 x 48 GB using 'Fixed IOPs'
sh2-4x512	12,000	4 x 128 GB	Tier 0	12,800	4 x 64 GB using 'Fixed IOPs'
sh2-7x512	12,000	4 x 128 GB	Tier 0	12,800	4 x 64 GB using 'Fixed IOPs'
sh2-12x512	12,000	4 x 128 GB	Tier 0	12,800	4 x 64 GB using 'Fixed IOPs'
sh2-4x768	12,000	4 x 128 GB	Tier 0	12,800	4 x 96 GB using 'Fixed IOPs'
sh2-7x768	12,000	4 x 128 GB	Tier 0	12,800	4 x 96 GB using 'Fixed IOPs'
sh2-12x768	12,000	4 x 128 GB	Tier 0	12,800	4 x 96 GB using 'Fixed IOPs'
sh2-4x1000	12,000	4 x 128 GB	Tier 0	12,800	
sh2-7x1000	12,000	4 x 128 GB	Tier 0	12,800	
sh2-12x1000	12,000	4 x 128 GB	Tier 0	12,800	
sh2-16x1000	12,000	4 x 128 GB	Tier 0	12,800	
sh2-25x1000	12,000	4 x 128 GB	Tier 0	12,800	
sh2-4x1500	12,000	4 x 128 GB	Tier 0	12,800	
sh2-7x1500	12,000	4 x 128 GB	Tier 0	12,800	
sh2-12x1500	12,000	4 x 128 GB	Tier 0	12,800	
sh2-16x1500	12,000	4 x 128 GB	Tier 0	12,800	
sh2-8x1900	12,000	4 x 128 GB	Tier 0	12,800	
sh2-16x1900	12,000	4 x 128 GB	Tier 0	12,800	

sr2-25x1900	12,000	4 x 128 GB	Tier 0	12,800	
sr2-33x1900	12,000	4 x 128 GB	Tier 0	12,800	
Sample log file system configurations for SAP HANA profiles with sh2 prefix					
sh2 Certified profile	IOPs required	Sample storage config	Sample storage tier	IOPs obtained	Alternative configuration (cost effective)
sh2-4x256	8,000	4 x 670 GB	Tier 3	8,400	4 x 103 GB using 'Tier 0'
sh2-7x256	8,000	4 x 670 GB	Tier 3	8,400	4 x 103 GB using 'Tier 0'
sh2-12x256	8,000	4 x 670 GB	Tier 3	8,400	4 x 103 GB using 'Tier 0'
sh2-4x384	8,000	4 x 670 GB	Tier 3	8,400	4 x 154 GB using 'Tier 0'
sh2-7x384	8,000	4 x 670 GB	Tier 3	8,400	4 x 154 GB using 'Tier 0'
sh2-12x384	8,000	4 x 670 GB	Tier 3	8,400	4 x 154 GB using 'Tier 0'
sh2-4x512	8,000	4 x 670 GB	Tier 3	8,400	4 x 206 GB using 'Tier 0'
sh2-7x512	8,000	4 x 670 GB	Tier 3	8,400	4 x 206 GB using 'Tier 0'
sh2-12x512	8,000	4 x 670 GB	Tier 3	8,400	4 x 206 GB using 'Tier 0'
sh2-4x768	8,000	4 x 670 GB	Tier 3	8,400	4 x 309 GB using 'Tier 0'
sh2-7x768	8,000	4 x 670 GB	Tier 3	8,400	4 x 309 GB using 'Tier 0'
sh2-12x768	8,000	4 x 670 GB	Tier 3	8,400	4 x 309 GB using 'Tier 0'
sh2-4x1000	8,000	4 x 670 GB	Tier 3	8,400	
sh2-7x1000	8,000	4 x 670 GB	Tier 3	8,400	
sh2-12x1000	8,000	4 x 670 GB	Tier 3	8,400	
sh2-16x1000	8,000	4 x 670 GB	Tier 3	8,400	
sh2-25x1000	8,000	4 x 670 GB	Tier 3	8,400	
sh2-4x1500	8,000	4 x 670 GB	Tier 3	8,400	
sh2-7x1500	8,000	4 x 670 GB	Tier 3	8,400	

sh2-12x1500	8,000	4 x 670 GB	Tier 3	8,400
sh2-16x1500	8,000	4 x 670 GB	Tier 3	8,400
sh2-8x1900	8,000	4 x 765 GB	Tier 3	8,400
sh2-16x1900	8,000	4 x 765 GB	Tier 3	8,400
sr2-25x1900	8,000	4 x 765 GB	Tier 3	8,400
sr2-33x1900	8,000	4 x 765 GB	Tier 3	8,400

Sample data file system configurations for SAP HANA profiles with sh2 prefix

sh2 Certified profile	IOPs required	Sample storage config	Sample storage tier	IOPs obtained	Alternative configuration
sh2-4x256	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
sh2-7x256	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
sh2-12x256	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
sh2-4x384	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
sh2-7x384	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
sh2-12x384	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
sh2-4x512	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
sh2-7x512	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
sh2-12x512	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
sh2-4x768	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
sh2-7x768	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
sh2-12x768	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
sh2-4x1000	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
sh2-7x1000	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'

sh2-12x1000	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
sh2-16x1000	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
sh2-25x1000	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
sh2-4x1500	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
sh2-7x1500	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
sh2-12x1500	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
sh2-16x1500	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
sh2-8x1900	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
sh2-16x1900	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
sr2-25x1900	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
sr2-33x1900	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'

Sample shared file system configurations for SAP HANA profiles with sh2 prefix

bh2 - Certified Profiles

The following SAP HANA profiles with prefix **bh2** on IBM Power Virtual Server are supported:

Profile name	CPU cores	Virtual CPUs	Memory (GiB)	SAPS	SMT Mode	Workload Type
bh2-35x3000	35	280	3000	266,000	SMT8	OLTP/OLAP
bh2-35x3900	35	280	3900	266,000	SMT8	OLTP/OLAP

P10 Certified Instance profiles with bh2 prefix

bh2 Certified profile	IOPs required	Sample storage config	Sample storage tier	IOPs obtained	Alternative configuration (cost effective)
bh2-35x3000	12,000	4 x 128 GB	Tier 0	12,800	
bh2-35x3900	12,000	4 x 128 GB	Tier 0	12,800	

Sample log file system configurations for SAP HANA profiles with bh2 prefix

bh2 Certified profile	IOPs required	Sample storage config	Sample storage tier	IOPs obtained	Alternative configuration (cost effective)
bh2-35x3000	8,000	4 x 1208 GB	Tier 3	14,499	

bh2-35x3900	8,000	4 x 1570 GB	Tier 3	18,846	
Sample data file system configurations for SAP HANA profiles with bh2 prefix					
bh2 Certified profile	IOPs required	Sample storage config	Sample storage tier	IOPs obtained	Alternative configuration
bh2-35x3000	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'

bh2-35x3900	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
Sample shared file system configurations for SAP HANA profiles with bh2 prefix					

ch2 - Certified Profiles

The following SAP HANA profiles with prefix **ch2** on IBM Power Virtual Server are supported:

Profile name	CPU cores	Virtual CPUs	Memory (GiB)	SAPS	SMT Mode	Workload Type
ch2-87x6000	87	696	6,000	661,200	SMT8	OLTP/OLAP
ch2-80x6144	80	640	6,144	608,000	SMT8	OLTP/OLAP
ch2-87x7000	87	696	7,000	661,200	SMT8	OLTP/OLAP
ch2-87x7600	87	696	7,600	661,200	SMT8	OLTP/OLAP

P10 Certified Instance profiles with ch2 prefix

ch2 Certified profile	IOPs required	Sample storage config	Sample storage tier	IOPs obtained	Alternative configuration (cost effective)
ch2-87x6000	12,000	4 x 128 GB	Tier 0	12,800	
ch2-80x6144	12,000	4 x 128 GB	Tier 0	12,800	
ch2-87x7000	12,000	4 x 128 GB	Tier 0	12,800	
ch2-87x7600	12,000	4 x 128 GB	Tier 0	12,800	

Sample log file system configurations for SAP HANA profiles with ch2 prefix

ch2 Certified profile	IOPs required	Sample storage config	Sample storage tier	IOPs obtained	Alternative configuration (cost effective)
ch2-87x6000	8,000	4 x 2416 GB	Tier 3	28,998	
ch2-80x6144	8,000	4 x 2474 GB	Tier 3	29,691	
ch2-87x7000	8,000	4 x 2819 GB	Tier 3	33,831	
ch2-87x7600	8,000	4 x 3060 GB	Tier 3	36,729	

Sample data file system configurations for SAP HANA profiles with ch2 prefix

ch2 Certified profile	IOPs required	Sample storage config	Sample storage tier	IOPs obtained	Alternative configuration
ch2-87x6000	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'

ch2-80x6144	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
ch2-87x7000	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
ch2-87x7600	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'

Sample shared file system configurations for SAP HANA profiles with ch2 prefix

IBM Power9 Certified Instances for SAP HANA

The following profile families are available for IBM Power9 processor-based servers.

Families	Description
Profiles with cnp prefix	Profiles with the prefix <i>cnp</i> are custom profiles for test or development use only. These profiles are not intended for production use and are not supported or certified for SAP production. Each profile must have minimum of two physical CPU cores.
Profiles with ush1 prefix	Profiles with the prefix <i>ush</i> are small profiles and are best suited for balanced workloads that require less CPU and storage consumption.
Profiles with bh1 prefix	Profiles with the prefix <i>bh1</i> are balanced profiles and are best suited for midsize databases and common cloud applications with moderate traffic.
Profiles with ch1 prefix	Profiles with the prefix <i>ch1</i> are compute intensive profiles and are best suited for moderate to high web traffic workloads. Compute profiles are best suited for cpu-intensive workloads, such as heavy web traffic, production batch processing, and front-end web servers.
Profiles with mh1 prefix	Profiles with the prefix <i>mh1</i> are very high memory profiles and are best suited for server OLAP databases, such as SAP NetWeaver.
Profiles with umh prefix	Profiles with the prefix <i>umh</i> are ultra memory profiles that provide the highest vCPU-to-memory ratios for serving in-memory OLTP databases, such as SAP HANA.

Profile families for Power9 server generation

ush1 - Certified Profiles

The following SAP HANA profiles with prefix **ush1** on IBM Power Virtual Server are supported:

Profile name	CPU cores	Virtual CPUs	Memory (GiB)	SAPS	SMT Mode	Workload Type
ush1-4x128	4	32	128	24,000	SMT8	OLAP/OLTP
ush1-4x256	4	32	256	24,000	SMT8	OLAP/OLTP
ush1-4x384	4	32	384	24,000	SMT8	OLAP/OLTP
ush1-4x512	4	32	512	24,000	SMT8	OLAP/OLTP
ush1-4x768	4	32	768	24,000	SMT8	OLAP/OLTP

P9 Certified Instance profiles with ush1 prefix

ush1	IOPs	Sample	Sample	IOPs	Alternative configuration
Certified profile	required	storage config	storage tier	obtained	(cost effective)
ush1-4x128	12,000	4 x 128 GB	Tier 0	12,800	4 x 16 GB using 'Fixed IOPs'
ush1-4x256	12,000	4 x 128 GB	Tier 0	12,800	4 x 32 GB using 'Fixed IOPs'
ush1-4x384	12,000	4 x 128 GB	Tier 0	12,800	4 x 48 GB using 'Fixed IOPs'
ush1-4x512	12,000	4 x 128 GB	Tier 0	12,800	4 x 64 GB using 'Fixed IOPs'
ush1-4x768	12,000	4 x 128 GB	Tier 0	12,800	4 x 96 GB using 'Fixed IOPs'
Sample log file system configurations for SAP HANA profiles with ush1 prefix					
ush1	IOPs	Sample	Sample	IOPs	Alternative configuration
Certified profile	required	storage config	storage tier	obtained	(cost effective)
ush1-4x128	8,000	4 x 670 GB	Tier 3	8,040	4 x 81 GB using 'Tier 0'
ush1-4x256	8,000	4 x 670 GB	Tier 3	8,040	4 x 103 GB using 'Tier 0'
ush1-4x384	8,000	4 x 670 GB	Tier 3	8,040	4 x 154 GB using 'Tier 0'
ush1-4x512	8,000	4 x 670 GB	Tier 3	8,040	4 x 206 GB using 'Tier 0'
ush1-4x768	8,000	4 x 670 GB	Tier 3	8,040	4 x 309 GB using 'Tier 0'
Sample data file system configurations for SAP HANA profiles with ush1 prefix					
ush1	IOPs	Sample	Sample	IOPs	Alternative configuration
Certified profile	required	storage config	storage tier	obtained	
ush1-4x128	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
ush1-4x256	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
ush1-4x384	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
ush1-4x512	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
ush1-4x768	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
Sample shared file system configurations for SAP HANA profiles with ush1 prefix					

bh1 - Certified Profiles

The following SAP HANA profiles with prefix **bh1** on IBM Power Virtual Server are supported:

Profile name	CPU cores	Virtual CPUs	Memory (GiB)	SAPS	SMT Mode	Workload Type
bh1-16x1600	16	128	1,600	96,000	SMT8	OLAP/OLTP
bh1-20x2000	20	160	2,000	120,000	SMT8	OLAP
bh1-22x2200	22	178	2,200	132,000	SMT8	OLAP
bh1-25x2500	25	200	2,500	150,000	SMT8	OLAP
bh1-30x3000	30	240	3,000	180,000	SMT8	OLAP
bh1-35x3500	35	280	3,500	210,000	SMT8	OLAP
bh1-40x4000	40	320	4,000	240,000	SMT8	OLAP
bh1-50x5000	50	400	5,000	300,000	SMT8	OLAP
bh1-60x6000	60	480	6,000	360,000	SMT8	OLAP/OLTP
bh1-70x7000	70	560	7,000	420,000	SMT8	OLAP
bh1-80x8000	80	640	8,000	480,000	SMT8	OLAP
bh1-100x10000	100	800	10,000	600,000	SMT8	OLAP
bh1-120x12000	120	900	12,000	720,000	SMT8	OLAP
bh1-140x14000	140	1,120	14,000	840,000	SMT8	OLAP

P9 Certified Instance profiles with bh1 prefix

bh1 Certified profile	IOPs required	Sample storage config	Sample storage tier	IOPs obtained
bh1-16x1600	12,000	4 x 128 GB	Tier 0	12,800
bh1-20x2000	12,000	4 x 128 GB	Tier 0	12,800
bh1-22x2200	12,000	4 x 128 GB	Tier 0	12,800
bh1-25x2500	12,000	4 x 128 GB	Tier 0	12,800
bh1-30x3000	12,000	4 x 128 GB	Tier 0	12,800
bh1-35x3500	12,000	4 x 128 GB	Tier 0	12,800
bh1-40x4000	12,000	4 x 128 GB	Tier 0	12,800
bh1-50x5000	12,000	4 x 128 GB	Tier 0	12,800
bh1-60x6000	12,000	4 x 128 GB	Tier 0	12,800
bh1-70x7000	12,000	4 x 128 GB	Tier 0	12,800
bh1-80x8000	12,000	4 x 128 GB	Tier 0	12,800

bh1-100x10000	12,000	4 x 128 GB	Tier 0	12,800	
bh1-120x12000	12,000	4 x 128 GB	Tier 0	12,800	
bh1-140x14000	12,000	4 x 128 GB	Tier 0	12,800	
Sample log file system configurations for SAP HANA profiles with bh1 prefix					
bh1 Certified profile	IOPs required	Sample storage config	Sample storage tier	IOPs obtained	
bh1-16x1600	8,000	4 x 670 GB	Tier 3	8,040	
bh1-20x2000	8,000	4 x 805 GB	Tier 3	9,666	
bh1-22x2200	8,000	4 x 886 GB	Tier 3	10,632	
bh1-25x2500	8,000	4 x 1006 GB	Tier 3	12,081	
bh1-30x3000	8,000	4 x 1208 GB	Tier 3	14,499	
bh1-35x3500	8,000	4 x 1409 GB	Tier 3	16,914	
bh1-40x4000	8,000	4 x 1611 GB	Tier 3	19,332	
bh1-50x5000	8,000	4 x 2013 GB	Tier 3	24,165	
bh1-60x6000	8,000	4 x 2416 GB	Tier 3	28,998	
bh1-70x7000	8,000	4 x 2819 GB	Tier 3	33,831	
bh1-80x8000	8,000	4 x 3222 GB	Tier 3	38,664	
bh1-100x10000	8,000	4 x 4027 GB	Tier 3	48,330	
bh1-120x12000	8,000	4 x 4833 GB	Tier 3	19,332	
bh1-140x14000	8,000	4 x 5638 GB	Tier 3	67,662	
Sample data file system configurations for SAP HANA profiles with bh1 prefix					
bh1 Certified profile	IOPs required	Sample storage config	Sample storage tier	IOPs obtained	Alternative configuration
bh1-16x1600	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
bh1-20x2000	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
bh1-22x2200	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
bh1-25x2500	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
bh1-30x3000	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'

bh1-35x3500	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
bh1-40x4000	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
bh1-50x5000	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
bh1-60x6000	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
bh1-70x7000	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
bh1-80x8000	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
bh1-100x10000	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
bh1-120x12000	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
bh1-140x14000	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'

Sample shared file system configurations for SAP HANA profiles with bh1 prefix

ch1 - Certified Profiles

The following SAP HANA profiles with prefix **ch1** on IBM Power Virtual Server are supported:

Profile name	CPU cores	Virtual CPUs	Memory (GiB)	SAPS	SMT Mode	Workload Type
ch1-60x3000	60	480	3,000	360,000	SMT8	OLAP
ch1-70x3500	70	560	3,500	420,000	SMT8	OLAP
ch1-80x4000	80	640	4,000	480,000	SMT8	OLAP
ch1-100x5000	100	800	5,000	600,000	SMT8	OLAP
ch1-120x6000	120	900	6,000	720,000	SMT8	OLAP
ch1-140x7000	140	1,120	7,000	840,000	SMT8	OLAP

P9 Certified Instance profiles with ch1 prefix

ch1 Certified profile	IOPs required	Sample storage config	Sample storage tier	IOPs obtained
ch1-60x3000	12,000	4 x 128 GB	Tier 0	12,800
ch1-70x3500	12,000	4 x 128 GB	Tier 0	12,800
ch1-80x4000	12,000	4 x 128 GB	Tier 0	12,800
ch1-100x5000	12,000	4 x 128 GB	Tier 0	12,800

ch1-120x6000	12,000	4 x 128 GB	Tier 0	12,800
ch1-140x7000	12,000	4 x 128 GB	Tier 0	12,800

Sample log file system configurations for SAP HANA profiles with ch1 prefix

ch1 Certified profile	IOPs required	Sample storage config	Sample storage tier	IOPs obtained
ch1-60x3000	8,000	4 x 1208 GB	Tier 3	14,499
ch1-70x3500	8,000	4 x 1409 GB	Tier 3	16,914
ch1-80x4000	8,000	4 x 1611 GB	Tier 3	19,332
ch1-100x5000	8,000	4 x 2013 GB	Tier 3	24,165
ch1-120x6000	8,000	4 x 2416 GB	Tier 3	28,998
ch1-140x7000	8,000	4 x 2819 GB	Tier 3	33,831

Sample data file system configurations for SAP HANA profiles with ch1 prefix

ch1 Certified profile	IOPs required	Sample storage config	Sample storage tier	IOPs obtained	Alternative configuration
ch1-60x3000	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
ch1-70x3500	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
ch1-80x4000	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
ch1-100x5000	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
ch1-120x6000	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
ch1-140x7000	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'

Sample shared file system configurations for SAP HANA profiles with ch1 prefix

mh1 - Certified Profiles

The following SAP HANA profiles with prefix **mh1** on IBM Power Virtual Server are supported:

Profile name	CPU cores	Virtual CPUs	Memory (GiB)	SAPS	SMT Mode	Workload Type
mh1-8x1440	8	64	1,440	48,000	SMT8	OLAP
mh1-10x1800	10	80	1,800	60,000	SMT8	OLAP
mh1-12x2160	12	96	2,160	72,000	SMT8	OLAP
mh1-16x2880	16	128	2,880	96,000	SMT8	OLAP

mh1-20x3600	20	160	3,600	120,000	SMT8	OLAP
mh1-22x3960	22	176	3,960	132,000	SMT8	OLAP
mh1-25x4500	25	200	4,500	150,000	SMT8	OLAP
mh1-30x5400	30	240	5,400	180,000	SMT8	OLAP
mh1-35x6300	35	280	6,300	210,000	SMT8	OLAP
mh1-40x7200	40	320	7,200	240,000	SMT8	OLAP
mh1-50x9000	50	400	9,000	300,000	SMT8	OLAP
mh1-60x10800	60	460	10,800	360,000	SMT8	OLAP
mh1-70x12600	70	560	12,600	420,000	SMT8	OLAP
mh1-80x14400	80	640	14,400	480,000	SMT8	OLAP
mh1-90x16200	90	720	16,200	540,000	SMT8	OLAP
mh1-100x18000	100	800	18,000	600,000	SMT8	OLAP
mh1-125x22500	125	1,000	22,500	750,000	SMT8	OLAP

P9 Certified Instance profiles with mh1 prefix

mh1 Certified profile	IOPs required	Sample storage config	Sample storage tier	IOPs obtained
mh1-8x1440	12,000	4 x 128 GB	Tier 0	12,800
mh1-10x1800	12,000	4 x 128 GB	Tier 0	12,800
mh1-12x2160	12,000	4 x 128 GB	Tier 0	12,800
mh1-16x2880	12,000	4 x 128 GB	Tier 0	12,800
mh1-20x3600	12,000	4 x 128 GB	Tier 0	12,800
mh1-22x3960	12,000	4 x 128 GB	Tier 0	12,800
mh1-25x4500	12,000	4 x 128 GB	Tier 0	12,800
mh1-30x5400	12,000	4 x 128 GB	Tier 0	12,800
mh1-35x6300	12,000	4 x 128 GB	Tier 0	12,800
mh1-40x7200	12,000	4 x 128 GB	Tier 0	12,800
mh1-50x9000	12,000	4 x 128 GB	Tier 0	12,800
mh1-60x10800	12,000	4 x 128 GB	Tier 0	12,800
mh1-70x12600	12,000	4 x 128 GB	Tier 0	12,800

mh1-80x14400	12,000	4 x 128 GB	Tier 0	12,800	
mh1-90x16200	12,000	4 x 128 GB	Tier 0	12,800	
mh1-100x18000	12,000	4 x 128 GB	Tier 0	12,800	
mh1-125x22500	12,000	4 x 128 GB	Tier 0	12,800	
Sample log file system configurations for SAP HANA profiles with mh1 prefix					
mh1 Certified profile	IOPs required	Sample storage config	Sample storage tier	IOPs obtained	
mh1-8x1440	8,000	4 x 670 GB	Tier 3	8,040	
mh1-10x1800	8,000	4 x 670 GB	Tier 3	8,040	
mh1-12x2160	8,000	4 x 869 GB	Tier 3	10,437	
mh1-16x2880	8,000	4 x 1159 GB	Tier 3	13,917	
mh1-20x3600	8,000	4 x 1449 GB	Tier 3	17,397	
mh1-22x3960	8,000	4 x 1594 GB	Tier 3	19,137	
mh1-25x4500	8,000	4 x 1812 GB	Tier 3	21,747	
mh1-30x5400	8,000	4 x 2174 GB	Tier 3	26,097	
mh1-35x6300	8,000	4 x 2537 GB	Tier 3	30,447	
mh1-40x7200	8,000	4 x 2899 GB	Tier 3	34,797	
mh1-50x9000	8,000	4 x 3624 GB	Tier 3	43,497	
mh1-60x10800	8,000	4 x 4349 GB	Tier 3	51,194	
mh1-70x12600	8,000	4 x 5074 GB	Tier 3	60,894	
mh1-80x14400	8,000	4 x 5799 GB	Tier 3	69,594	
mh1-90x16200	8,000	4 x 6524 GB	Tier 3	78,294	
mh1-100x18000	8,000	4 x 7249 GB	Tier 3	86,994	
mh1-125x22500	8,000	4 x 9061 GB	Tier 3	108,741	
Sample data file system configurations for SAP HANA profiles with mh1 prefix					
mh1 Certified profile	IOPs required	Sample storage config	Sample storage tier	IOPs obtained	Alternative configuration
mh1-8x1440	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
mh1-10x1800	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'

mh1-12x2160	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
mh1-16x2880	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
mh1-20x3600	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
mh1-22x3960	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
mh1-25x4500	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
mh1-30x5400	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
mh1-35x6300	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
mh1-40x7200	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
mh1-50x9000	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
mh1-60x10800	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
mh1-70x12600	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
mh1-80x14400	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
mh1-90x16200	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
mh1-100x18000	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
mh1-125x22500	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'

Sample shared file system configurations for SAP HANA profiles with mh1 prefix

umh - Certified Profiles

The following SAP HANA profiles with prefix **umh** on IBM Power Virtual Server are supported:

Profile name	CPU cores	Virtual CPUs	Memory (GiB)	SAPS	SMT Mode	Workload Type
umh-4x960	4	32	960	24,000	SMT8	OLTP
umh-6x1440	6	48	1,440	36,000	SMT8	OLTP
umh-8x1920	8	64	1,920	48,000	SMT8	OLTP
umh-10x2400	10	80	2,400	60,000	SMT8	OLTP

umh-12x2880	12	96	2,880	72,000	SMT8	OLTP
umh-16x3840	16	128	3,840	96,000	SMT8	OLTP
umh-20x4800	20	160	4,800	120,000	SMT8	OLTP
umh-22x5280	22	176	5,280	132,000	SMT8	OLTP
umh-25x6000	25	200	6,000	150,000	SMT8	OLTP
umh-30x7200	30	240	7,200	180,000	SMT8	OLTP
umh-35x8400	35	280	8,400	210,000	SMT8	OLTP
umh-40x9600	40	320	9,600	240,000	SMT8	OLTP
umh-50x12000	50	400	12,000	300,000	SMT8	OLTP
umh-60x14400	60	480	14,400	360,000	SMT8	OLTP

P9 Certified Instance profiles with umh prefix

umh Certified profile	IOPs required	Sample storage config	Sample storage tier	IOPs obtained
umh-4x960	12,000	4 x 128 GB	Tier 0	12,800
umh-6x1440	12,000	4 x 128 GB	Tier 0	12,800
umh-8x1920	12,000	4 x 128 GB	Tier 0	12,800
umh-10x2400	12,000	4 x 128 GB	Tier 0	12,800
umh-12x2880	12,000	4 x 128 GB	Tier 0	12,800
umh-16x3840	12,000	4 x 128 GB	Tier 0	12,800
umh-20x4800	12,000	4 x 128 GB	Tier 0	12,800
umh-22x5280	12,000	4 x 128 GB	Tier 0	12,800
umh-25x6000	12,000	4 x 128 GB	Tier 0	12,800
umh-30x7200	12,000	4 x 128 GB	Tier 0	12,800
umh-35x8400	12,000	4 x 128 GB	Tier 0	12,800
umh-40x9600	12,000	4 x 128 GB	Tier 0	12,800
umh-50x12000	12,000	4 x 128 GB	Tier 0	12,800
umh-60x14400	12,000	4 x 128 GB	Tier 0	12,800

Sample log file system configurations for SAP HANA profiles with umh prefix

umh Certified profile	IOPs required	Sample storage config	Sample storage tier	IOPs obtained
--------------------------	------------------	--------------------------	------------------------	------------------

umh-4x960	8,000	4 x 670 GB	Tier 3	8,040
umh-6x1440	8,000	4 x 670 GB	Tier 3	8,040
umh-8x1920	8,000	4 x 773 GB	Tier 3	9,279
umh-10x2400	8,000	4 x 966 GB	Tier 3	11,598
umh-12x2880	8,000	4 x 1159 GB	Tier 3	13,917
umh-16x3840	8,000	4 x 1546 GB	Tier 3	18,558
umh-20x4800	8,000	4 x 1933 GB	Tier 3	23,196
umh-22x5280	8,000	4 x 2126 GB	Tier 3	25,518
umh-25x6000	8,000	4 x 2416 GB	Tier 3	28,998
umh-30x7200	8,000	4 x 2899 GB	Tier 3	34,797
umh-35x8400	8,000	4 x 3383 GB	Tier 3	40,596
umh-40x9600	8,000	4 x 3866 GB	Tier 3	46,395
umh-50x12000	8,000	4 x 4833 GB	Tier 3	57,996
umh-60x14400	8,000	4 x 5799 GB	Tier 3	69,594

Sample data file system configurations for SAP HANA profiles with umh prefix

umh Certified profile	IOPs required	Sample storage config	Sample storage tier	IOPs obtained	Alternative configuration
umh-4x960	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
umh-6x1440	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
umh-8x1920	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
umh-10x2400	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
umh-12x2880	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
umh-16x3840	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
umh-20x4800	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
umh-22x5280	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
umh-25x6000	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'

umh-30x7200	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
umh-35x8400	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
umh-40x9600	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
umh-50x12000	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'
umh-60x14400	3,000	1 x 200 GB	Tier 0	5,000	1 x 1000 GB using 'Tier 3'

Sample shared file system configurations for SAP HANA profiles with umh prefix

cnp - Custom Profiles

IBM Power Virtual Servers provide fully customizable CPU cores and memory (RAM in GiB). Configure a virtual server instance by specifying a custom size for the IBM Power Virtual Server profile, following SAP HANA for IBM Power Systems best practices and SAP's guidance for non-production SAP HANA instances.

Custom profiles are designed exclusively for non-production development or testing purposes. These profiles are not intended, supported, or certified for SAP production environments and cannot be used to move from a non-production environment to a production environment.

Each profile requires a minimum of two dedicated cores. For storage performance requirements, refer to the [Storage Guidelines for SAP HANA](#). For additional details on storage, refer to the [storage tiers section](#) section in the [What is a Power Systems Virtual Server?](#) documentation.



For more details, refer to [SAP Note 2947579 - SAP HANA on IBM Power Virtual Servers](#).

Infrastructure profiles for SAP NetWeaver-based application servers

Intel Virtual Server certified profiles on VPC infrastructure for SAP application server

Profiles list



Note: The published names are subject to change.

The following tables provide an overview of the SAP-certified profiles for Virtual Servers for VPC:

SAP-certified profiles hosted on Intel Cascade Lake CPUs

Profile	vCPU	Memory (RAM GiB)	SAPS
Compute Optimized			
cx2-2x4 cx2d-2x4	2	4	2,238
cx2-4x8 cx2d-4x8	4	8	4,475
Balanced			
cx2-8x16 cx2d-8x16	8	16	8,950
cx2-16x32 cx2d-16x32	16	32	17,900
cx2-32x64 cx2d-32x64	32	64	35,800
cx2-48x96 cx2d-48x96	48	96	53,700
cx2-64x128 cx2d-64x128	64	128	71,600
cx2-96x192 cx2d-96x192	96	192	107,400
cx2-128x256 cx2d-128x256	128	256	143,200
Balanced			
bx2-2x8 bx2d-2x8	2	8	2,306
bx2-4x16 bx2d-4x16	4	16	4,613
bx2-8x32 bx2d-8x32	8	32	9,225
bx2-16x64 bx2d-16x64	16	64	18,450
bx2-32x128 bx2d-32x128	32	128	36,900

bx2-48x192	48	192	55,350
bx2d-48x192			
bx2-64x256	64	256	81,685
bx2d-64x256			
bx2-96x384	96	384	122,528
bx2d-96x384			
bx2-128x512	128	512	163,370
bx2d-128x512			
Memory Optimized			
mx2-2x16	2	16	2,571
mx2d-2x16			
mx2-4x32	4	32	5,141
mx2d-4x32			
mx2-8x64	8	64	10,283
mx2d-8x64			
mx2-16x128	16	128	20,565
mx2d-16x128			
mx2-32x256	32	256	41,130
mx2d-32x256			
mx2-48x384	48	384	56,970
mx2d-48x384			
mx2-64x512	64	512	81,015
mx2d-64x512			
mx2-96x768	96	768	121,523
mx2d-96x768			
mx2-128x1024	128	1,024	162,030
mx2d-128x1024			
Very High Memory Optimized			
vx2d-2x28	2	28	2,131
vx2d-4x56	4	56	4,262
vx2d-8x112	8	112	8,523
vx2d-16x224	16	224	17,046
vx2d-44x616	44	616	46,875
vx2d-88x1232	88	1,232	93,750
vx2d-144x2016	144	2,016	153,410
vx2d-176x2464	176	2,464	187,500

Ultra High Memory Optimized				
Profile	vCPU	Memory (RAM GiB)	SAPS	aSAPS ⁽¹⁾
ux2d-2x56	2	56	2,156	
ux2d-4x112	4	112	4,312	
ux2d-8x224	8	224	8,623	
ux2d-16x448	16	448	17,246	
ux2d-36x1008	36	1,008	38,803	
ux2d-48x1344	48	1,344	51,737	
ux2d-72x2016	72	2,016	77,606	
ux2d-100x2800	100	2,800	107,785	
ux2d-200x5600	200	5,600	215,570	

IBM Cloud Virtual Servers for VPC hosted on Intel Cascade Lake CPUs

SAP-certified profiles hosted on Intel Sapphire Rapids CPUs

Profile	vCPU	Memory (RAM GiB)	SAPS	aSAPS ⁽¹⁾
Compute Optimized				
cx3d-2x5	2	5	2,661	
cx3d-4x10	4	10	5,321	
cx3d-8x20	8	20	10,642	
cx3d-16x40	16	40	21,284	
cx3d-24x60	24	60	31,926	
cx3d-32x80	32	80	42,568	
cx3d-48x120	48	120	63,852	
cx3d-64x160	64	160	85,136	
cx3d-96x240	96	240	127,703	
cx3d-128x320	128	320	170,270	
cx3d-176x440	176	440	234,120	
Balanced				
bx3d-2x10	2	10	2,616	
bx3d-4x20	4	20	5,232	
bx3d-8x40	8	40	10,463	

bx3d-16x80	16	80	20,926
bx3d-24x120	24	120	31,388
bx3d-32x160	32	160	41,850
bx3d-48x240	48	240	62,775
bx3d-64x320	64	320	83,699
bx3d-96x480	96	480	125,548
bx3d-128x640	128	640	167,397
bx3d-176x880	176	880	230,170

Memory Optimized

mx3d-2x20	2	20	2,590
mx3d-4x40	4	40	5,180
mx3d-8x80	8	80	10,359
mx3d-16x160	16	160	20,718
mx3d-24x240	24	240	31,076
mx3d-32x320	32	320	41,434
mx3d-48x480	48	480	62,150
mx3d-64x640	64	640	82,866
mx3d-96x960	96	960	124,299
mx3d-128x1280	128	1,280	165,731
mx3d-176x1760	176	1,760	227,880

Very High Memory Optimized

vx3d-2x32	2	32	2,513	485
vx3d-4x64	4	64	5,026	969
vx3d-8x128	8	128	10,051	1,937
vx3d-16x256	16	256	20,102	3,873
vx3d-24x384	24	384	30,153	5,810
vx3d-32x512	32	512	40,204	7,746
vx3d-48x768	48	768	60,306	11,619

vx3d-64x1024	64	1,024	80,408	15,491
vx3d-88x1408	88	1,408	110,560	21,300
vx3d-96x1536	96	1,536	120,611	23,237
vx3d-128x2048	128	2,048	160,815	30,982
vx3d-176x2816	176	2,816	221,120	42,600

IBM Cloud Virtual Servers for VPC hosted on Intel Sapphire Rapids CPUs

⁽¹⁾: aSAPS is the metric that is derived from the [SAP quote-to-cash \(Q2C\) Benchmark](#).

For more information, see [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#).

Understanding Virtual Server profile names

With IBM Cloud® Virtual Servers for Virtual Private Cloud, the profile families that are certified for SAP are: *Compute Optimized*, *Balanced*, *Memory Optimized*, *Very High Memory Optimized*, and *Ultra High Memory Optimized*.

- *Compute Optimized* family profiles provide more compute power, and they have more cores with less memory.
- *Balanced* family profiles provide a good mix of performance and scalability for more common workloads.
- All the memory family profiles cater to memory intensive workloads, such as demanding database applications and in-memory analytics workloads, and are especially designed for SAP HANA workloads.

For more information, see chapter [x86-64 instance profiles](#).

The first letter of the profile name indicates the profile family mentioned above. One of the key instance attributes is the ratio of core (*number of vCPUs*) to RAM (*amount of GiB*):

First letter	Characteristics of the related profile family	Ratio Cascade Lake	Ratio Sapphire Rapids
c	<i>Compute Optimized</i> family	1:2	1:2.5
b	<i>Balanced</i> family	1:4	1:5
m	<i>Memory Optimized</i> family	1:8	1:10
v	<i>Very High Memory Optimized</i> family	1:14	1:16
u	<i>Ultra High Memory Optimized</i> family	1:28	n/a

IBM Cloud® Virtual Servers for Virtual Private Cloud Profile Families

For SAP HANA, only the memory profile families are used, for NetWeaver also the *Compute Optimized* and the *Balanced* families may be considered. The Virtual Server profile names are contextual and sequential. See here one example:

Profile name	Naming convention	What it means
mx?-16x128	m	<i>Memory Optimized</i> family
	x	Intel x86_64 CPU Architecture
?		The Intel generation for the underlying hardware
2		Cascade Lake
3		Sapphire Rapids

d	the optional 'd' in the name indicates that the server is equipped with one or more internal SSD or NVMe storage devices (*)
—	<i>spacer</i>
16	16 vCPU
x	<i>spacer</i>
128	128 GiB RAM

Profile naming for SAP HANA



Note: (*) Note for Virtual Server Instances using temporary local SSD or NVMe storage: you must not place any SAP workload related data on such instance storage, because data loss may occur in certain situations - see more information here: [About instance storage](#).

Profiles available on Hourly Consumption Billing

All IBM Cloud Virtual Servers for VPC are available with Hourly Consumption Billing, which includes Suspend Discounts and Sustained Usage Discounts. With Suspend Discounts, storage charges occur only if the server is in Shutdown state. With Sustained Usage Discount, the more a server is used, the less the cost per hour.

Storage specifications

When the virtual server profiles for SAP HANA are initially provisioned, the servers all have one pre-configured volume (vda) attached with the following basic layout:

File system	Partition	Storage type	size (GB)	Nr. of IOPS
/	vda1	Pre-configured boot volume	100	3,000
/boot	vda2	Pre-configured boot volume	0.25	3,000

Storage configuration of the default virtual server deployment (boot volume)

To fulfill the size and I/O requirements for SAP application server or SAP AnyDB, more [IBM® Cloud Block Storage for Virtual Private Cloud](#) volumes need to be added as data volumes to the virtual server configuration.

Block Storage Volumes for Virtual Servers can be created based on different **volume profiles** that provide different levels of IOPS per gigabyte (IOPS/GB). For more information, see [IOPS tiers](#) for details.

You must consider the total IOPS required for your installation and the performance characteristics of your database. One option is to colocate multiple directories into a single large volume with high IOPS, versus isolating directories into individual small volumes with an insufficient number of IOPS for the workload characteristics.

For an overview of all available storage profiles, see [VPC Block Storage Profiles](#).

For SAP application server and SAP AnyDB, a minimum of 5 IOPS/GB is recommended.

Samples of storage configurations that use Intel Virtual Server (Gen2) profiles are available under [Storage design considerations](#).

Bare Metal Server certified profiles on VPC Infrastructure for SAP application server

Profiles list



Note: The published names are subject to change.

These tables give you an overview of the SAP-certified bare metal profiles for VPC that represent dedicated servers that provide physical cores. vCPU measurements are used in profile naming only. vCPU to physical cores are a 2:1 ratio (e.g 96 vCPU = 48 physical cores). The term vCPU is kept for comparison with their virtual counterparts.

Profiles hosted on Intel Cascade Lake CPU

Profile	vCPU	Memory (RAM GiB)	SAPS
Compute Optimized			
cx2d-metal-96x192	96	192	101,070
Balanced			
bx2d-metal-96x384	96	384	124,130
Memory Optimized			
mx2d-metal-96x768	96	768	127,620
Ultra High Memory Optimized			
ux2d-metal-112x3072	112	3,072	140,730
ux2d-metal-224x6144	224	6,144	294,730

IBM Cloud Bare Metal Servers for VPC certified for SAP application server - Intel Cascade Lake CPU

Profiles hosted on Intel Sapphire Rapids CPU

Profile	vCPU	Memory (RAM GiB)	SAPS	aSAPS ⁽¹⁾
Compute Optimized				
cx3d-metal-48x128	48	128	62,029	n/a
cx3d-metal-64x128	64	128	63,950	n/a
Balanced				
bx3d-metal-48x256	48	256	93,670	18,400
bx3d-metal-64x256	64	256	124,520	24,600
bx3d-metal-192x1024	192	1.024	297,770	57,400
Memory Optimized				
mx3d-metal-16x128	16	128	30,030	n/a
mx3d-metal-48x512	48	512	97,830	18,700
mx3d-metal-64x512	64	512	128,750	24,200
mx3d-metal-96x1024	96	1.024	182,670	33,700
mx3d-metal-128x1024	128	1.024	239,300	46,000
Very High Memory Optimized				
vx3d-metal-16x256	16	256	35,520	n/a
Ultra High Memory Optimized				

ux3d-metal-16x512	16	512	34,320	n/a
IBM Cloud Bare Metal Servers for VPC certified for SAP application server - Intel Sapphire Rapids CPU				

⁽¹⁾: aSAPS is the metric that is derived from the [SAP quote-to-cash \(Q2C\) Benchmark](#).

For more information, see [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud (VPC) Infrastructure environment] (<https://me.sap.com/notes/2927211>): external].

Understanding Bare Metal Server profile names

With IBM Cloud Bare Metal Servers for VPC, the profile families that are certified for SAP are: *Compute Optimized*, *Balanced*, *Memory Optimized*, and *Ultra High Memory Optimized*.

- *Compute Optimized* family profiles provide more compute power, and they have more cores with less memory.
- *Balanced* family profiles provide a good mix of performance and scalability for more common workloads.
- *Memory Optimized*, *Very High Memory Optimized*, and *Ultra High Memory Optimized* family profiles cater to memory intensive workloads, such as demanding database applications and in-memory analytics workloads, and are especially designed for SAP HANA workloads.

For more information, see [x86-64 bare metal server profiles](#).

The first letter of the profile name indicates the profile family mentioned above. One of the key instance attributes is the ratio of core (*number of vCPUs*) to RAM (*amount of GiB*):

First letter	Characteristics of the related profile family	Ratio Cascade Lake	Ratio Sapphire Rapids
c	<i>Compute Optimized</i> family	1:2	1:2 or 1:2.67
b	<i>Balanced</i> family	1:4	1:4 or 1:5.33
m	<i>Memory Optimized</i> family	1:8	1:8 or 1:10.67
v	<i>Very High Memory Optimized</i> family	1:27.43	1:16
u	<i>Ultra High Memory Optimized</i> family	1:27.43	1:32

IBM Cloud Bare Metal Servers for VPC Profile Families

The Bare Metal Server profile names are contextual and sequential. See the following example:

Profile name	Naming convention	What it means
	component	
mx2d-metal-96x768	m	<i>Memory Optimized</i> family
	x	Intel x86_64 CPU architecture
	?	The Intel generation for the underlying hardware
	2	Cascade Lake
	3	Sapphire Rapids
	d	the optional 'd' in the name indicates that the server is equipped with one or more additional NVMe SSD storage devices
	—	spacer
	metal	<i>metal</i> in the name indicates that this is a bare metal server
	—	spacer

96	96 vCPU
x	spacer
768	768 GiB RAM
Profile naming for SAP application server	

Profiles available on Hourly Consumption Billing

All IBM Cloud Bare Metal Servers for VPC are available with Hourly Consumption Billing, which includes Suspend Discounts and Sustained Usage Discounts. With Suspend Discounts, storage charges occur only if the server is in Shutdown state. With Sustained Usage Discount, the more a server is used, the less the cost per hour.

Storage specifications

When the bare metal server profiles for SAP application server are initially provisioned, the servers have one or more pre-configured disks attached.

1. Servers that are hosted on Cascade Lake CPU have one disk (sda) with the following basic layout:

File system	Partition	Storage type	Size
	sda1	Pre-configured BIOS volume	1 MB
/boot/efi	sda2	Pre-configured boot volume	100 MB
/	sda3	Pre-configured root volume	9.9 GB
Storage configuration of the default bare metal server deployment (boot volume)			

2. Servers that are hosted on Sapphire Rapids CPU

See the appropriate profile in [x86-64 bare metal server profiles](#).

Internal Storage

Your bare metal server on VPC comes with a number of internal NVMEs, depending on its size. For SAP application server based deployment, you can use the NVMEs that are listed as block devices to the operating system. The NVMEs are under “/dev/nvmeXn1” (X from 0 to the number of NVMEs in total, minus 1). Use the NVMEs according to your requirements and needs. However, to increase failure resilience, you might have to install Linux Logical Volume Manager (LVM) to add RAID configuration, like RAID1 or RAID5. Since NVMEs are provisioned, performance considerations are mostly not an issue.

External Storage

If more storage needs are to be added to your bare metal server on VPC, for example, for backup purposes, NFS-based [file shares](#) can be created and mounted. Learn more details in the corresponding chapter [Creating file shares and mount targets](#).

Intel Bare Metal server certified profiles on Classic infrastructure for SAP application server

Profiles list for Intel servers

The following is an overview of the SAP-certified profiles with Bare Metal Intel servers:

Profile	CPU Cores	CPU Threads (aka. vCPU)	Memory (RAM GB)	SAPS
BI.S3.NW32	4	8	32 GB	11,970
BI.S3.NW64	4	8	64 GB	12,750
BI.S3.NW192	36	72	192 GB	78,850

BI.S3.NW384	36	72	384 GB	79,430
BI.S3.NW768	36	72	768 GB	79,630
BI.S4.NW192	32	64	192 GB	82,470
BI.S4.NW384	32	64	384 GB	85,130
BI.S4.NW384_v3	16	32	384 GB	60,420
BI.S4.NW768	40	80	768 GB	112,830
BI.S4.NW768_v2	48	96	768 GB	124,620
BI.S4.NW768_v3	16	32	768 GB	60,420
BI.S4.NW1500	56	112	1.5 TB	147,220
BI.S4.NW3000	56	112	3 TB	135,127

Intel servers certified for SAP application server

See also [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#).

Understanding Bare Metal profile names

The Bare Metal profile names are contextual and sequential, below uses a server that is certified for SAP application server as an example:

Profile name	Naming convention component	What it means
BI.S3.NW384	BI	IBM Cloud Infrastructure
	S3	Series 3 (CPU generation) <ul style="list-style-type: none"> • S3: Intel Skylake/Kaby Lake • S4: Intel Cascade Lake • S5: Intel Sapphire Rapids
	NW	SAP application server (NetWeaver) certified server
	H2	HANA-(*) and SAP application server certified server, 2 sockets
	384	384 GB RAM

Profile naming for Intel servers certified for SAP application server



Note: (*) Only the servers that are listed in the [SAP Hardware Directory](#) are supported for HANA workloads.

Profiles available on Hourly Consumption Billing

The following Bare Metal servers are available on **Hourly** Consumption Billing:

- BI.S3.NW32 (OS Options)
- BI.S4.NW192 (OS Options)
- BI.S4.NW384 (OS Options)
- BI.S4.NW768 (OS Options)

AMD Bare Metal server certified profiles on Classic infrastructure for SAP application

server

Profiles list



Note: The published names are subject to change.

The following is an overview of the SAP-certified profiles with AMD Bare Metal:

Profile	CPU Cores	CPU Threads (aka. vCPU)	Memory (RAM GB)	SAPS
BI.S4A.NW2000	96	192	2 TB	265,650
BI.S4A.NW4000	96	192	4 TB	267,450

AMD servers certified for SAP application server

See also [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#).

Understanding Bare Metal profile names

The Bare Metal profile names are contextual and sequential, below uses a server that is certified for SAP application server as an example:

Profile name	Naming convention component	What it means
BI.S4A.NW2000	BI	IBM Cloud Infrastructure
	S4A	Series 3 (processor generation) <ul style="list-style-type: none">• S3: Intel Skylake/Kaby Lake• S4: Intel Cascade Lake• S4A: AMD 2nd Gen EPYC• S5: Intel Sapphire Rapids
	NW	SAP application server (NetWeaver) certified server
	2000	2000 GB RAM

Profile naming for AMD servers certified for SAP application server

VMware SDDC certified profiles for SAP NetWeaver

Profiles list



Note: The published names are subject to change.

The following table is an overview of the SAP-certified profiles with either:

- Intel Bare Metal and VMware vSphere (ESXi), manual VMware setup and configuration
- IBM Cloud for VMware Solutions Dedicated, automated VMware SDDC setup and configuration

Profile	CPU Cores	CPU Threads (also known as. vCPU)	Memory (RAM GiB)	SAPS (after VMware hypervisor 10%)
BI.S3.NW192 (VMware)	36	72	192 GB	70,965
BI.S3.NW384 (VMware)	36	72	384 GB	71,487
BI.S3.NW768 (VMware)	36	72	768 GB	71,667

BI.S4.NW192 (VMware)	32	64	192 GB	74,223
BI.S4.NW384 (VMware)	32	64	384 GB	76,617
BI.S4.NW768 (VMware)	40	80	768 GB	101,547
BI.S4.NW1500 (VMware)	56	112	1536 GB	132,498
BI.S4.NW3000 (VMware)	56	112	3072 GB	121,614

Intel servers certified for SAP application server

Understanding Bare Metal profile names

The Bare Metal profile names are contextual and sequential, below uses an SAP HANA certified server as an example:

Profile name	Naming convention component	What it means
BI.S3.NW768	BI	IBM Cloud Infrastructure
	S3	Series 3 (processor generation) <ul style="list-style-type: none"> • S3 is Intel Skylake/Kaby Lake • S4 is Intel Cascade Lake
	NW	SAP application server (NetWeaver) certified server

GiB RAM (rounded, exact RAM amount is in the table)

Profile naming for Intel servers certified for SAP application server

SAP Application Server certified instances on IBM Power Virtual Server

SAP Application Server certified instances on IBM Power Virtual Servers are available with fully adjustable CPU Cores and Memory (RAM GiB). It is permitted to define a custom size of the IBM Power Virtual Server instance to use for SAP Application Servers or SAP NetWeaver, in accordance with existing SAP Application Server, SAP NetWeaver or SAP AnyDB for IBM best practices and guidance from SAP.

For SAP applications the following virtual server configurations are supported. Flexible SAP Application Server certified instances on IBM operate in **SMT8 mode**. Simultaneous Multithreading (SMT) on IBM Power enables multiple independent threads to execute within a single physical processor core. In SMT8 mode, eight parallel threads can run on a single physical processor core. The operating system sees eight logical processors per physical processor core. Given SAP Application Server instance sizing is flexible, it must follow the standard SAP sizing guidelines by using the following SAPS benchmark calculation:

Power System type	SAPS per CPU Core (using SMT-8)
S1022	7,600
E1080	7,600
S922	5,570
E980	6,000

IBM SAP NetWeaver certified instances on IBM Power Virtual Server



Note: SAP NetWeaver certified instances on E1050 are currently not supported.

For more information, see [SAP Note 2855850 - SAP Applications on IBM Power Virtual Servers](#).

Predefined SAP Application Server instances on IBM Power Virtual Servers

SAP Application Server certified instances on IBM Power Virtual Servers are also available as predefined configurations. A predefined SAP Application Server certified instance or profile on IBM Power Virtual Server defines attributes, such as physical CPU cores and RAM, which determine the size and performance capabilities of the virtual server instance.

SAP Application Server Profile Naming Convention

SAP Application Server profile names follow a contextual and sequential naming convention. The following table illustrates an example of an SAP Application certified instance profile:

Profile name	Naming convention component	Description
sr2-2x32	sr2	Profile prefix
	-	<i>separator</i>
	2	2 physical CPU Cores
	x	<i>separator</i>
	32	32 GiB RAM

Profile naming scheme for SAP Application Servers

sr2 – Predefined SAP Application Server Profiles

The following predefined SAP Application Server profiles with prefix **sr2** on IBM Power Virtual Server are available. Profiles with **sr2** prefix are custom profiles that may be deployed through **CLI or API only**.

Profile name	CPU cores	Virtual CPUs	Memory (GiB)	SAPS	SMT Mode	Workload Type
sr2-2x32	2	16	32	15,200	SMT8	SAP Application Server/SAP NetWeaver
sr2-3x64	3	24	64	22,800	SMT8	SAP Application Server/SAP NetWeaver
sr2-4x64	4	32	64	30,400	SMT8	SAP Application Server/SAP NetWeaver
sr2-6x128	6	48	128	45,600	SMT8	SAP Application Server/SAP NetWeaver
sr2-8x128	8	64	128	60,800	SMT8	SAP Application Server/SAP NetWeaver
sr2-12x256	12	96	256	91,200	SMT8	SAP Application Server/SAP NetWeaver
sr2-16x256	16	128	256	121,600	SMT8	SAP Application Server/SAP NetWeaver

P10 predefined Instance profiles with sr2 prefix for SAP Application Servers

Profile name	Sample storage config	Sample storage tier	IOPs obtained
sr2-2x32	1 x 50GB	Tier 0	1,250
sr2-3x64	1 x 50GB	Tier 0	1,250
sr2-4x64	1 x 50GB	Tier 0	1,250
sr2-6x128	1 x 50GB	Tier 0	1,250
sr2-8x128	1 x 50GB	Tier 0	1,250

sr2-12x256	1 x 50GB	Tier 0	1,250
sr2-16x256	1 x 50GB	Tier 0	1,250

Sample file system configurations for SAP Application Server profiles with sr2 prefix

Plan your SAP workloads

Sizing process for SAP Systems

After you decide which SAP solutions you want to use, you need to determine the number of hosts that are required to support your SAP landscape and make sure that the host servers are correctly sized.

SAP sizing is a detailed activity (and often a project in itself) to map business requirements into Infrastructure/Hardware requirements.

Understanding SAP sizing

The SAP sizing methodology for SAP HANA or SAP NetWeaver technical applications is based on SAP benchmarks, such as information from SAP and actual customer experiences.

The base SAP workload unit is an SAP Application Performance Standard (SAPS).

The SAPS is a definition of throughput that is coined by SAP capacity planning and performance testing personnel. For example, 100 SAPs is defined as 2,000 fully business processed order-line items per hour in the standard SAP Sales and Distribution (SAP SD) application benchmark. This example is equivalent to 2,400 SAP SD transactions per hour with the SAP Enterprise Resource Planning (SAP ERP) solution.

The benchmarking test determines and rates the infrastructure processing power based on its capability to run and process transactions at close to 100% CPU load with a response time of less than 1 second.

The capability of processors is measured during the standard (SAP SD) benchmark test that is certified by SAP. For more information about the benchmark test that is certified by SAP, see [SAP Standard Application Benchmarks](#) and [Practical Guidelines and Techniques for Sizing your SAP Landscape for Optimal Performance and Scalability](#).

SAP sizing is primarily based on:

- Business throughput (Throughput based sizing); includes database table size increase from new objects, CPU time to complete processing transactions or batch job runs within a time limit (decided by the business)
- Business concurrent users (User based sizing); includes usage patterns and categorization of user's based upon their daily transactions
- Business need for High Availability and Disaster Recovery
- Business need for multiple SAP applications and add-ons, which are integrated into one landscape

SAP sizing is used to determine:

- Support for design of the Application Server structure and configurations:
 - SAP Systems
 - SAP Tiering/Tracks
 - SAP Instances
 - SAP Clients
- Support for design of the Database Server structure and configurations:
 - System Type e.g. Distributed
 - Deployment Type e.g. MDC
 - Processing Type e.g. OLAP
 - Sizing Type and Deployment Method e.g. Expert Sizing with TDIV5/6
 - High Availability and Disaster Recovery
- Processor and Memory requirements
- Storage requirements
- Network requirements and topology
- Backup strategy

SAP sizing inaccuracies can cause risks to SAP implementation projects:

Project risk from inaccurate SAP Sizing	Mitigations of SAP Sizing inaccuracy
--	--------------------------------------

- | | |
|------------------------------------|---|
| Incomplete/Insufficient input data | <ul style="list-style-type: none"> • Information discovery requires support from business departments and the IT organization /n - Communication issues are a common cause of invalid data therefore assignment of a project manager to run workshops is recommended /n - Any unknown data will become an assumption |
|------------------------------------|---|

Assumptions are not verified	/n - Assumptions must be documented and need a verification process included in the project plan
------------------------------	--

Custom code and special data structures	/n - Hard to predict scenarios, that are solved by custom code and special data structures, require a verification process to determine whether there is an impact to infrastructure (commonly processing and storage)
---	--

SAP Sizing inaccuracies can cause risks to SAP implementation projects

SAP logical structure and SAP Sizing impacts for infrastructure

There are multiple ways in which the SAP logical structure and SAP sizing activities can impact infrastructure-related requirements, three key ways are highlighted below:

1. Business Requirements

Business requirements, such as 99.99% uptime or 3 downtime windows per year, effect logical design and structure of the SAP Landscape. The logical structure is made up of:

- SAP Systems
- SAP Tiering
- SAP Tracks
- SAP Instances
- SAP Clients

1. SAP sizing results

Each decision in the logical structure is reflected by the SAP Sizing project/exercise outcome:

- SAPS benchmark threshold required
- Size of database (memory and disk storage)
- etc.

1. Infrastructure requirements

SAP sizing results will heavily impact Infrastructure needs:

- Number of hosts required
- Performance/Size of hosts required
- Storage capacity for hosts
- Networking performance and isolation between hosts
- etc.

Migrating an existing SAP System

If you plan to migrate an existing SAP system (from any source) to your IBM Cloud environment, you can determine the SAPS numbers from the SAPS numbers of your current environment.

Use the information about your current workload (the CPUs and RAM used) and get the SAPS equivalents for your CPU from the [SAP SD Benchmarks results](#) of your existing hardware.

Using the SAP QuickSizer

The [SAP QuickSizer](#) is a web-based tool that is provided by SAP; it is available to all customers and business partners of SAP. Sizing information is input directly into the tool. The tool sizes SAP HANA or SAP NetWeaver servers.



Note: You need an SAP S-user ID to use the QuickSizer.

The QuickSizer calculates the workload (in a measurement unit called SAPS) and adjusts the workload to allow for suitable processor use. So, if a workload

of 4,800 SAP SD benchmark transactions per hour is required, the tool calculates this workload as 200 SAPS. For example, an IT department determined that to avoid system overloads during high-usage periods, a target processor load of 33% is allowed. A processor that can provide 200 SAPS at 33% load means that the processor is capable of 600 SAPS at 100% load. Therefore, a system capable of 600 SAPS becomes the benchmark to which any new infrastructure must adhere.

While the sizing method might be considered conservative, consider that all SAPS calculations for your servers are based on highly tuned SAP systems that run only specific SAP SD workloads. Depending on the type of SAP application, any custom configuration or custom coding in your system, your results can vary. Also, requirements for your project, such as proof-of-concept (PoC) or regarding performance and response time, might be different.

After you determine your SAP applications and the SAPS numbers are calculated through the SAP QuickSizer, or based on your current landscape, you can choose from the IBM Cloud® for SAP portfolio and the various infrastructure sizes available (as profiles or customizable/flexible in some cases).

Assessment of SAP HANA with the SAP Quick Sizer

SAP HANA is supported in production on single-node and multi-node SAP HANA-certified servers. The SAP HANA database uses column storage for some tables and fields, reducing the storage below row storage in traditional Relation Database Management System (RDMS); data can be highly compressed and compression ratios can range from 3:1 to over 10:1 based on the source data and database.

Sizing SAP HANA correctly is key to the success of your project. It is a best practice to complete the sizing before you order any SAP HANA certified server from IBM Cloud® for SAP. Improperly sized memory or storage requirements can lead to an upgrade and migration to a larger server.

Main memory is one of the most important resources to consider when you size an SAP HANA-certified appliance.

The [SAP HANA Master Guide](#) provides a starting point for sizing-related topics.

The [Sizing SAP HANA - SAP HANA Master Guide](#) information within the guide provides guidance on how to size your SAP HANA system. It points to the different installation and migration scenarios for both greenfield installations and existing systems.

This information includes a link to the SAP HANA version of the SAP Quick Sizer tool (an SAP S-user ID is required to access the tool). The page also lists the SAP Notes that are related to sizing your SAP HANA server.

For more information on SAP Sizing

For more information about sizing, see the following resources:

- [Sizing SAP HANA - SAP HANA Master Guide](#)
- [Quick Sizer](#)
- [SAP Note 1736976 - Sizing Report for BW-on-HANA](#)
- [SAP Note 1872170 - Suite on HANA memory sizes](#)
- [SAP Note 1793345 - Sizing for SAP Suite on HANA](#)
- [SAP Note 1514966 - SAP HANA: Sizing SAP HANA](#)
- [SAP Certified and Supported SAP HANA Hardware](#)
- [SAP Note 2055470 - SAP HANA on Power Planning and Installation Specifics - Central Note](#)
- [SAP HANA Storage Requirements](#)
- [SAP Certified Enterprise Storage Hardware for SAP HANA](#)

SAP applications effect on sizing

Primarily, when sizing SAP applications there are design considerations related to the Infrastructure, OS, Database Server and Application Server. These are covered in this topic group "Sizing and Planning SAP Workloads":

- Networking design considerations
- Storage design considerations
- Compute and OS design considerations
- SAP HANA Database design considerations
- SAP NetWeaver design considerations

However, for each SAP Business Application and SAP Technical Application there are different implementation design considerations - which will change for each business and the scenario.

Beyond the topic group "Sizing and Planning SAP Workloads", there are individual topic groups with additional information and considerations for your SAP implementation:

- **SAP Business Applications**

- [SAP S/4HANA](#)
- [SAP BW/4HANA](#)
- [SAP Commerce](#)

- **SAP AnyDB databases**

- [AnyDB - IBM Db2](#)
- [AnyDB - SAP MaxDB](#)
- [AnyDB - SAP ASE](#)
- [AnyDB - SAP IQ](#)

Define your SAP system landscape

Your business and functional requirements determine the SAP solutions that are powered by the SAP HANA Database Server or SAP NetWeaver Application Server, and therefore determine how your applications are run the infrastructure available.

Your requirements have an influence on how you size your server. You have a wide selection of SAP NetWeaver-based applications (which may use SAP HANA) to choose from, including SAP S/4HANA, SAP ERP Central Component (ECC), SAP BW/4HANA, SAP BW and many more solutions for different business operations.

For a complete list of solutions, see [ABAP Platform and SAP NetWeaver](#). For information about supported operating systems and database platforms, see [SAP Product Availability Matrix \(PAM\)](#). Search for Product Availability Matrix. An SAP S-User ID is required.

Determining your SAP applications

An SAP landscape is a group of two or more SAP systems that usually include development, quality and test, and production.

One SAP system consists of one or more *SAP instances*, which are a group of processes that are started and stopped at the same time. These *SAP instances* are grouped to form a specified SAP system for a defined use for a region or business unit. Then, the instances are grouped in a landscape as development, test, or production SAP systems with one or multiple tracks (such as "project" and "business"). This landscape design is up to each business, dependent on business requirements.

Landscapes have several possible configurations, such as server (CPU, RAM) size and storage size, for all SAP solutions in the market. These solutions include SAP NetWeaver-based products. SAP NetWeaver-based products range from older solutions, such as SAP ECC and SAP BW (that use "AnyDB" vendors that are approved by SAP), to the new range of SAP solutions, such as SAP S/4HANA and SAP BW/4HANA (that use SAP HANA database). Beyond the enterprise resource planning (ERP) and enterprise data warehouse (EDW) examples, there are many available SAP products or add-ons for different industries and business types or operating geographies.

SAP NetWeaver-based products are designed to run on SAP NetWeaver-certified hosts, and SAP HANA-based products are designed to run on SAP HANA-certified hosts. The certified operating systems and supported database systems for IBM Cloud are listed in [SAP Note 2927211](#).

More solutions are available from SAP that are not SAP NetWeaver-based and many third-party software options that might integrate with SAP can affect the planning of your system landscape. For example, SAP HANA can run as a database for an SAP NetWeaver stack-based solution or as a stand-alone entity depending on your usage scenario.



Note: Contact [SAP Support](#) if you plan to deploy and integrate non-SAP NetWeaver-based or third-party software into your SAP landscape on IBM Cloud.

You want to be as detailed as possible when you determine the size of your server based on the applications that you plan to run, potential growth, and performance. Additionally, keep in mind your storage and memory requirements for your applications. SAP systems in a landscape have specific requirements for connectivity, either among each other or to external systems.

Questions during your determination of the SAP landscape:

- How do you intend to use the applications? Is the intended use for development and testing, or production?
- How do you intend to connect your SAP workloads in Cloud to your existing network and systems?
- How will the database be used? Transactional (OLTP) or Analytical (OLAP)? Serving only the SAP Business Applications, or as part of your wider IT strategy extracting value from the advanced SAP HANA Components, which are available (such as predictive analytics or Cloud Foundry via XSA)
- How do you intend to deploy the applications and databases? And to what level of resiliency (that is, HA/DR strategy)?

If you plan to migrate an on-premises SAP installation into the IBM Power Virtual Servers environment, make sure that you don't carry over existing performance issues. Run an up-to-date sizing report, and review a recent SAP Early Watch report of your SAP system. For more information, see [SAP EarlyWatch Alert](#) and [SAP Note 207223 - SAP EarlyWatch Alert Processed at SAP](#).

Each deployment of SAP HANA Database Server or SAP NetWeaver Application Server will have items to consider. These are included under each relevant section of this documentation.

For further information regarding SAP Landscapes, guidance has been released by IBM Power Systems, which provide excellent detailed agnostic information and guidance regarding SAP Landscapes components and setup (which applies to running SAP on any infrastructure, on-premises data centers or Cloud IaaS):

- [SAP on IBM Power Systems Best Practices Guide](#) (click the link in the middle of the page)
- [IBM Power Systems Virtualization Operation Management for SAP Applications](#)
- [SAP HANA on IBM Power Systems and IBM System Storage - Guides](#)

Reviewing any relevant SAP and IBM Cloud documentation

Review the following documentation to help you determine any prerequisites for the SAP products that you plan to install.

If your organization is new to IBM Cloud, read the following SAP documentation to help with your planning phase and implementation:

- [SAP workloads on IBM Cloud®](#)
- [Get started with IBM Cloud®](#)
- [Creating an IBM Cloud® account](#)
- [How to create an SAP S-user ID](#). Note that only super administrators or S-users with the required authorization are allowed to create S-user IDs for your company's SAP Customer Number (SCN)
- The [Guide Finder for SAP NetWeaver and ABAP Platform](#) to search for SAP NetWeaver-related documentation, including installation guides.
- Applicable [installation guides](#); requires an SAP S-user ID.
- SAP release notes, which can be found in the application help of the relevant SAP product documentation on the [SAP Help Portal](#); requires an SAP S-user ID.
- [SAP HANA Help](#)
- [SAP NetWeaver Help](#)
- [SAP HANA Master Guide](#)
- [SAP Product Availability Matrix \(PAM\)](#); requires an SAP S-user ID.
- [SAP Notes](#); requires an SAP S-user ID.
- Third-party documentation

Selecting your SAP-certified infrastructure

This expands on the introduction [Comparing the different SAP-certified IaaS offerings](#), which summarizes the benefits of each different Infrastructure option.

You are ready to define the number of host servers and size of those hosts after:

- the business has defined their requirements
- decided which SAP applications to use
- read the SAP installation documentation
- understood the various design considerations

Often your first filter of the infrastructure options is minimum SAPS, which has been calculated using the SAP QuickSizer, and this will primarily define the CPU performance requirements. For the official certification documents, see the [SAP Standard Application Benchmarks](#) which helps to confirm the IaaS you are choosing from IBM Cloud is the correct IaaS for your needs.

Full details of the Profiles available for each Infrastructure option available through IBM Cloud, were provided in the previous topic group, which lists all the IaaS Offerings available for either SAP HANA or SAP NetWeaver (and SAP AnyDB):

- SAP HANA profiles
 - [Intel Bare Metal server certified profiles for SAP HANA](#)
 - [Intel Virtual Server certified profiles for SAP HANA](#)
 - [IBM Power Virtual Server certified profiles for SAP HANA](#)
 - [VMware SDDC certified profiles for SAP HANA](#)
- SAP NetWeaver profiles
 - [Intel Bare Metal server certified profiles for SAP NetWeaver](#)
 - [Intel Virtual Server certified profiles for SAP NetWeaver](#)

- [IBM Power Virtual Server certified profiles for SAP NetWeaver](#)
- [VMware SDDC certified profiles for SAP NetWeaver](#)

Distributing your SAP Landscape on IBM Cloud Bare Metal and Virtual Servers

Generally, the entire infrastructure for the operation of all closely coupled runtime components of an SAP software solution must be installed on either Intel Virtual Servers (Gen2) or on Bare Metal Servers from IBM Cloud.

To assist customers looking to combine performance for the database and flexibility for the application solution/s, testing has been performed when combining environments and networks.

Intel Bare Metal Servers from IBM Cloud in the IBM Cloud Classic Infrastructure environment may offer greater performance capabilities. Notably, this includes larger memory, local SSD storage in RAID arrays, access to IPMI, and more. Intel Virtual Servers (Gen2), on the other hand provide more flexibility.

RDBMs on Intel Bare Metal Servers in the older IBM Cloud Classic Infrastructure environment that comply to [SAP Note 2414097](#), are supported when connected to the SAP AS on Intel Virtual Server (Gen2) in the IBM Cloud VPC Infrastructure environment - when placed in the same location (that is, Datacenter / Availability Zone) and using an IBM Cloud Transit Gateway local routing.

Mapping CPUs derived from SAPS to an IBM Power Virtual Server



Note: This is a complementary offering from IBM Power Systems, with low latency access to IBM Cloud services

When you create an IBM Power Virtual Server by using the IBM Cloud console:

- For SAP NetWeaver, you select the number of CPUs of your server
- For SAP HANA, you select an instance profile with a predefined number of CPUs and memory size that suits your workload

While your data must fit into the instance memory with space for data growth defined by the business and SAP Sizing process, choosing an instance profile with more CPUs improves performance.

To find SAP certified profiles for Cloud IaaS, see [SAP Certified and Supported SAP HANA Hardware Directory - Certified IaaS Platforms - IBM Cloud](#); this includes IBM Power Virtual Servers, which can be found by using filter "CPU Architecture" and selecting IBM Power9.

To find SAP certified IBM Power Systems Hardware, see [SAP Certified and Supported SAP HANA Hardware Directory - IBM Power Systems](#).

For more information, see [Creating an IBM Power Virtual Server](#). For information about the pricing difference between CPU types, see [Pricing for IBM Power Systems Virtual Servers on IBM Cloud®](#). For a description of the technical differences between dedicated, shared capped, and shared uncapped CPUs, see [this FAQ](#).

Monitoring your system with SAP tools

SAP system monitoring is available through the [SAP Host Agent](#), which provides monitoring functions that are similar to on-premises installations.

Monitoring for IBM Cloud Intel Virtual Servers (Gen2), on VPC Infrastructure

The operating system metrics that the SAP Host Agent provides require the use of [IBM Cloud Metrics Collector for SAP](#) and the correct SAP Host Agent patch level.

Monitoring for IBM Power Virtual Servers

For Infrastructure as a Service (IaaS) environments such as IBM Power Virtual Servers, the operating system metrics that the SAP Host Agent provides were enhanced. Make sure that you have the prerequisite SAP Host Agent patch level installed. For a description of the new metrics and required SAP Host Agent patch level, see [SAP Note 2932766 - SAP on IBM Power Virtual Servers: Key Monitoring Metrics](#).

Monitoring your system with IBM Cloud Monitoring for SAP systems

The IBM Cloud Monitoring provides a great solution for monitoring SAP systems on top of your deployed infrastructure. For information on how to set up a monitoring instance and collect metrics from SAP systems, see [SAP Monitoring with IBM Cloud Monitoring](#).

Support from IBM Cloud or SAP

For full information regarding support from IBM Cloud or SAP, please read [Getting help and support from IBM Cloud or SAP](#).

Connectivity to your SAP system landscape

IBM Cloud has many connectivity options, including low latency worldwide connections between your private internal network and IBM Cloud's private network backbone.

You can securely connect to your infrastructure in multiple ways by using various protocols and ports, based on the infrastructure chosen and the different network types:

- [Classic Infrastructure](#) network (formerly Softlayer network)

- Intel Bare Metal
- Classic Intel Virtual Servers
- VMware solutions

- [VPC Infrastructure](#) network

- Intel Virtual Servers (Generation 2)

Interconnectivity between IBM Cloud network

- **Transit Gateway**, handling interconnectivity across the IBM Cloud private backbone between the networks with defined and controlled communication between resources worldwide across the IBM Cloud network or across multiple IBM Cloud accounts (useful for Managed Service Providers of SAP). Transit Gateways are used to support hybrid workloads, frequent data transfers, and private workloads by providing dynamic scalability, high availability, and private, in-transit data between hosts on IBM Cloud.

- Local routing, connect VPCs in same region
- Global routing, connect VPCs across regions
- Classic Infrastructure routing, connect to VLANs on Classic Infrastructure network
- Cross-account connection (also known as account-to-account routing), connect VPCs across multiple IBM Cloud accounts. See [Adding a cross-account connection \(VPC only\)](#)

Connectivity options within the IBM Cloud Classic Infrastructure network

- **Classic SSL VPN**, basic SSL Tunnel with user/password to various PoP or Data centers, which is built in to IBM Cloud® Classic Infrastructure, enabled per user account and is a good option for administrators during initial stages of deployments to IBM Cloud. It is not for bulk users due to bandwidth caps.

- **Classic IPsecVPN**, service from the IBM Cloud catalog, which can be provisioned and has advanced configuration options available for the IPsec Tunnel

- **IBM Cloud® Direct Link for Classic Infrastructure**, the most robust connection available in varying types from your internal network to IBM Cloud's Availability Zones (also known as data centers) that use Network Service Providers, Point of Presence (PoP), or directly between the data center colocation Room (also called a Meet Me Room). This option is available up to 10 Gbps network throughput as a Routed OSI Layer-2/3 connection, and is designed for enterprise workload connections. **Note: If you are using VPC Infrastructure, this option is not necessary as IBM Cloud® Direct Link 2.0 can also connect to Classic Infrastructure**

- More information on [Direct Link 1.0](#). To find from a specified site location to IBM Cloud and which network service providers are available, use [Cloud Pathfinder for IBM Cloud](#) (powered by [Cloudscene](#))

IBM Cloud® Classic Infrastructure offers firewalls that can provide your Bare Metal Servers with a layer of security that is provisioned on demand and designed to eliminate service interruptions.

Within the Classic Infrastructure network, there are many Gateway Appliance and Firewalls to help prevent unwanted traffic from hitting your server, help reduce your attack vulnerability, and let your server resource be dedicated for its use. Based on your specific performance and feature requirements, you can choose one of the following options:

- Shared firewall (multiple options, see [Getting Started Hardware Shared Firewall](#)),
- [Fortinet FortiGate security appliance](#).

Connectivity options within the IBM Cloud VPC Infrastructure network

- **Floating IP**, a public internet IPv4 address, which can be configured with Security Groups to allow only certain network connection access on defined protocols and ports from specified source/target addresses. For initial tests option is often used, with more detail in the short guide on [Connecting to your Linux Virtual Server instance](#).

- **VPC IPsecVPN**, service from the IBM Cloud catalog and deploys a VPN Gateway to a VPC and creating a VPN Connection with advanced configuration options available for the IPsec Tunnel; including integration with authentication strategies such as Microsoft Active Directory.

- **IBM Cloud® Direct Link 2.0**, the latest enhancement and the most robust connection available, now with access to both Classic Infrastructure network and VPC Infrastructure network simultaneously from your internal network to IBM Cloud's Availability Zones (Data centers) that use Network Service Providers, Point of Presence (PoP), or directly between the data center colocation Room (also called a Meet Me Room). This is

available up to 10 Gbps network throughput as a Routed OSI Layer-2/3 connection, and is designed for enterprise workload connections.

- More information on ["Use a VPC/VPN gateway for secure and private on-premises access to cloud resources"](#).

IBM Cloud Direct Link 2.0

Network back-bone infrastructure of a customer site can be directly connected to IBM Cloud, by using IBM Cloud Direct Link. On-premises resources can be connected to multiple VPCs, and VPC can provide Bring-your-own-IP or other custom IP ranges.



Note: Technical requirements and restrictions exist in the availability of IBM Cloud Direct Link in different regions. A detailed description of IBM Cloud Direct Link can be found in [Getting started with IBM Cloud® Direct Link](#).

Accessing the classic infrastructure



Note: Optional setup.

IBM Cloud VPC infrastructure can access other resources on IBM Cloud Classic Infrastructure, such as high-performance IBM Cloud® Bare Metal Servers designed for SAP HANA.

You have multiple options to achieve this access, notably a one-to-one association, or IBM Cloud® Transit Gateway with increased flexibility. This is described in the above section [Interconnectivity between IBM Cloud network](#).



Important: All options require upgrading the IBM Cloud account to be VRF-enabled.

For more information on VPC access to Classic Infrastructure, see [Setting up access to classic infrastructure](#). For more information on Transit Gateway, see [Getting started with IBM Cloud Transit Gateway](#).

Network connectivity and network security for SAP systems running in IBM Power Virtual Server

Network connectivity

To arrange connection through to IBM Cloud or an on-premises network, a private subnet must exist for the IBM Power Virtual Server.

- Power Virtual Server workspace will be connected over [Transit gateway](#) to:
 1. The Virtual Private Cloud(VPC) with VPC instances (Windows, HANA Studio)
 2. Other Power Virtual Server workspaces
 3. On-premises networks through [Direct Link](#).
- By using **local** transit gateway, the networks in the **same region** are connected. In order to connect networks from **another** regions, **global** transit gateway must be used.
- Other IBM Cloud services may be reached directly through public IBM Cloud service IPs or hostnames or over [Virtual Private Endpoints](#) configured in connected VPC (like IBM Cloud Object Storage etc.)

Network connectivity over VPN

IBM Power Virtual Server do not support a native VPN Service. However, IBM Cloud provides two [VPN services](#):

1. VPN for VPC offers site-to-site gateways, which connect your on-premises network to the IBM Cloud VPC network.
 2. Client VPN for VPC offers client-to-site servers, which allow clients on the internet to connect to VPN servers, while still maintaining secure connectivity.
- Once connectivity to VPC Network is established, it is then easier to reach the IBM Power Virtual Server instances provided that the VPC and Power Virtual Server workspace are attached to same Transit Gateway.
 - Outgoing public internet and external network traffic from Power Virtual Server instances goes over the internet proxy service running on Virtual Server Instance (VSI) in VPC.
 - Incoming public internet and external network traffic to Power Virtual Server instances are achieved using [Cloud Internet Service](#) and [Load Balancer Service](#).

Network Security

By considering all network connectivity options, we differentiate between connections coming to Power Virtual Server workspace over VPC and

directly through transit gateway.

On the target side (IBM Cloud networks or the on-premises network), it is required to perform the necessary configuration of the network security and permit connections to be established to/from IBM Power Virtual Servers.

Download and install SAP software and applications

SAP software installation media must be obtained from SAP directly, and requires valid license agreements with SAP in order to access these files.

All downloads of SAP software installation media are handled through the [SAP Support Portal](#) and the [SAP for Me](#). This was formerly called the SAP Marketplace (SMP) and may still be referred as this in some SAP documentation.

Downloads can be performed directly to a target server (when outbound internet connectivity is permitted), or could be downloaded to an administrator laptop and uploaded to an IBM Cloud storage option (such as IBM Cloud® Object Storage).

To perform a specific SAP installation, there are many different SAP software components and different installation media compressed archive files. The software might potentially use:

- SAP's own compression format called "SAP Archive (SAR)" which can only be decompressed with the SAPCAR program
- SAP's own compression format for Java called "Software Component Archive (SCA)"
- Provided in ZIP or RAR (self-extracting EXE) compression formats

The many various SAP software components to download can be downloaded individually by using a web browser, or these download items can be added to the [SAP Download Basket](#) to make it easier for downloading all files by using the [SAP Download Manager](#) (a Java GUI application).

After the SAP software installation media downloads, follow the standard SAP installation procedure that is documented in the applicable [SAP installation guide](#) for your SAP version and components and the corresponding [SAP Notes](#). The installation guide and SAP Notes require an SAP S-user ID to view.

It is important to remember that any SAP software installation will require some OS configuration; some of this information is available under the [Compute and OS Design Considerations](#) section. This OS configuration can be done before or after the SAP software installation media downloads have completed.



Tip: For IBM Power, you may want to install AIX Toolbox for Linux Applications for easier handling of SAP software.

For more help with SAP Download Manager, see:

- [SAP Note 2272824 - How to Download SAP Solution Manager - SAP ONE Support Launchpad](#)
- [SAP Note 1371839 - How to install SAP Download Manager - SAP ONE Support Launchpad](#)
- [SAP Note 2624390 - What is the current version of SAP Download Manager?](#)

Bring your own SAP product license

The IBM Cloud® SAP-Certified infrastructure is "bring your own license" (BYOL) capable for your SAP products. You need to apply the corresponding license for your SAP products after installation. If you are new to SAP, start exploring under [SAP All Products](#). You can also contact SAP Sales or SAP Support for details on how to obtain the required licenses.

Database licenses for SAP general information

It is recommended to check the license type of your Database Server for your SAP installation scenario onto IBM Cloud to avoid unsupported scenarios. Typically the license types are:

- Full-use database license. Supports both SAP and non-SAP software, unrestricted usage of all functions
- Runtime database license. Solely to support software licensed from SAP, restricted usage of functions required by the SAP Business Application. This usage can include databases from other vendors if those databases were purchases as OEM products through SAP.

SAP AnyDB - Bring your own IBM Db2 license

If you purchased your SAP and IBM Db2 (for Linux, UNIX, Windows also known as LUW) licenses as part of an original equipment manufacturer (OEM) application-specific licensing (ASL) agreement, you can download and apply license files from the [SAP Support Portal](#); click **Download Software**. For more information, see [SAP Note 816773 - DB6: Installing the Application-Specific Db2 License from SAP](#).

However, if you purchased IBM Db2 from IBM or an IBM Business Partner, you must use the license files that are provided by your vendor instead.

SAP HANA licenses

SAP HANA licenses are handled by the SAP HANA Cockpit.

SAP NetWeaver and SAP Business Application licenses

Both the SAP NetWeaver application server license and the SAP Business Application license are handled by SAPGUI (or variation thereof).

Creating an SAP license key

The SAP license key, `saplikey` or `SLICENSE`, displays a "hardware key" based on the hardware ID.

Use the following steps to create your SAP license key.

1. Run the `saplikey -get` command on the server that you're using as the SAP message server. As an alternative to the `saplikey` command and if your SAP system is already installed, you can use the `SLICENSE` transaction to retrieve the `HARDWARE KEY`.
2. Use the `HARDWARE KEY` output value to generate a valid SAP software license from [SAP Support](#). Select **Request Keys** and enter your SAP S-user ID.
3. Use the SAP system data to create a valid license key.
4. Use the SAP transaction `SLICENSE` or the `saplikey` command to install the license on your SAP system.

SAP license key with IBM Power Virtual Servers



Note: This is a complementary offering from IBM Power Systems, with low latency access to IBM Cloud services

SAP changed the mechanism for licensing when an IBM Power Virtual Server is running on the IBM Cloud®. In the IBM Cloud, the product license is not dependent on the underlying hardware that's running the server. The license is associated with the virtual server.

The hardware key is no longer based on the hardware ID, but on the partition UUID of the logical partition (LPAR). The partition UUID is persisted by the platform across restarts, reconfigurations, OS reinstalls, and partition migrations, making it independent of the hardware that is running the virtual servers.

When you request an SAP software license, be sure to use the `HARDWARE KEY` that was generated with an SAP kernel that has the minimum level that is required for running on IBM Cloud. The minimum SAP Kernel patch level of the kernel is found in [SAP Note 2879336](#). Otherwise, your SAP software license becomes invalid as soon as your virtual server is moved to different hardware in the IBM Cloud®.

Infrastructure for SAP design considerations

Networking design considerations

The SAP systems in a landscape have specific requirements for servers, operating systems, network setup, and supported storage.

In some regards, SAP workloads that use a Cloud Service Provider (such as IBM Cloud® for SAP) Infrastructure-as-a-Service is similar to existing practices (over many decades) for running SAP workloads that use an external data center or a data center provider. An SAP landscape has specific requirements for connectivity, between hosts within Cloud IaaS and to external systems, IBM Cloud® for SAP provides a rich set of functions beyond hosting of SAP systems to improve your SAP landscape.

To assist your project's planning phase, the below sections provide IBM Cloud® for SAP portfolio design considerations for **Networking**.

Preface: units of measure for data/information

Often the throughput Network Storage is shown in Mbps or Gbps.

It is important to note, that Mb (Megabits) is a decimal prefix and MiB (Mebibyte) is a binary prefix so they are on different scales. More confusion arises because MiB (Mebibyte) was commonly known in Microsoft Windows as **Megabyte**.

For future reference throughout the networking documentation, Mb (Megabits) and MiB (Mebibyte) is used based on the system of units (SI) defined by IEC and adopted by IEEE, ISO, and NIST.

For example,:

- 100 Mbps (Megabits per second), would be 12 MiB/s (Mebibyte per second)
- 1000 Mbps (Megabits per second) also known as 1 Gbps (Gigabits per second), would be 120 MiB/s (Mebibyte per second)
- 10 Gbps (Gigabits per second), would be 1200 MiB/s (Mebibyte per second)

Networking connectivity considerations

For an overview of the connectivity options available, see [Determining access to your SAP system landscape](#).

SAP Systems are often the focal point of business operations, with a great number of integrated applications (including legacy applications).

In most circumstances for SAP workloads, a connection to the existing internal network is required, and it is recommended to use **IBM Cloud® Direct Link 2.0** to operate the secure, low-latency, high-throughput (available up to 10 Gbps) as a Routed OSI Layer-2/3 connection.

These connectivity options are dependent on business requirements, for example, whether the business wants to use Cloud and also decrease security risk by isolating network flows through their existing networking structure and security. In these "disconnected" or "private-only" connectivity designs, it is best to request IBM Cloud® for additional information and discuss your use cases.

In addition, it is strongly not recommended by SAP to split the SAP System tiering across On-Premises location/s and Cloud locations and it is up to the business to evaluate this; for example, it is not recommended by SAP to retain SAP AnyDB run from infrastructure in an On-Premises location and connect to SAP NetWeaver run from infrastructure in a Cloud location. For IBM Power Virtual Servers this split of SAP System tiering is not supported.

Bring-your-own network (Subnet/CIDR/IP address range)

It is often a business preference to Bring-your-own Subnet/CIDR/IP address range (BYOIP) to your IBM Cloud account; this is available depending on the Infrastructure selection and environment.

VPC Infrastructure

When using VPC Infrastructure, it is possible to define and use your own subnet. See [VPC - Bring your own subnet](#).

This changes depending on whether [RFC 1918](#) IANA reserved IPv4 private network address spaces are in use, because any IP Address within these ranges is considered non-routable. These addresses are not unique on the Internet as they could be used by any private network without any coordination with IANA or an Internet registry, so these addresses are only unique within a private network. These IPv4 private network address spaces are:

- Class A - 10.0.0.0/8
- Class B - 172.16.0.0/12
- Class C - 192.168.0.0/16

If you use a bring-your-own subnet range **which is** defined under [RFC 1918](#) IANA reserved IPv4 private network address spaces, then connectivity to an existing internal network is possible when using any VPC functions (for example, Public Gateway or Floating IPs).

It is not supported to use a bring-your-own subnet range **not** defined under [RFC 1918](#) IANA reserved IPv4 private network address spaces because this would not permit connectivity to an existing internal network when used with a Public Gateway (PGW) and Floating IPs.

Classic Infrastructure with VMware

If the existing business operates SAP on VMware, it is possible to use IBM Cloud for VMware along with VMware HCX and IBM Cloud® Direct Link to create a bridged bidirectional network between existing Datacenter with VMware and IBM Cloud for VMware. This uses the existing VMware service mesh routing into VMware HCX and into overlay from VMWare NSX on IBM Cloud for VMware, which creates:

- An encrypted Migration Tunnel that uses HCX Cloud Gateway (CGW) + HCX WAN Optimizer (WAN-OPT)
- An encrypted Application Tunnel that uses HCX High Throughput Layer 2 Concentrator (HT L2C)

More information and is described on [IBM Cloud for VMware Solutions - VMware HCX overview](#).

Network Topology considerations

Dependent on the count and configuration of SAP Systems that are combined with the arrangement of the network flows between these systems for security or performance reasons, the Network Topology will be significantly different. The design of this topology reflects the requirements from the business for security, performance, cost, flexibility, and connectivity.

Using the Enterprise Resource Planning (ERP) business application, for example, an SAP System hosting the Production instance that uses the SAP System Tiering approach using High Availability of SAP NetWeaver and SAP HANA:

- SAP NetWeaver, there are at least four hosts instead of 1:
 - Central Services (ASCS)
 - Primary Application Server (PAS), also known as Central Instance (CI)
 - Enqueue Replication Server Instance (ERS)
 - Additional Application Server (AAS)
- SAP HANA, there are at least 2 hosts (possibly 3) instead of 1:
 - SAP HANA primary node (*using SAP HANA System Replication*)
 - SAP HANA secondary failover node (*using SAP HANA System Replication*)
 - SAP HANA tertiary disaster recovery failover node (*using SAP HANA System Replication*)
- This describes 1 SAP System within the SAP Landscape. An SAP Landscape might use:
 - One Track, 5 SAP Systems (Sandbox > Development > Testing > Staging > Production)
 - Dual Track, 5 SAP Systems (Sandbox > New Feature Development + Maintenance Development > New feature testing + Maintenance testing > Staging > Production)

Therefore for an SAP Landscape potentially 30 to 50 instances of SAP, spread across 10-50 host servers (physical or virtualized) might be required. This is before more business applications are added for specific business operations, industry, or geographic functions.

The size of the SAP Landscapes have a direct impact on the Network Topology.

Typically, although this varies from case to case, the following networks are required to meet the scenarios and performance that is required by the business that uses SAP Business Applications:

- Internal network for communication between multiple instances in an SAP Landscape with different SAP System Tiering approaches
- Network for the management and storage transfers of database systems
- Network that is used in production

However, in the simplest scenario there might be one private network for all purposes. It depends on business requirements.

Additional management systems to enable SAP systems

Depending on your operating system, SAP workload, and network connectivity, you might need to configure access to many more SAP and non-SAP systems. The following is a list of various management systems that your SAP workloads might require to operate:

- OS packages update server, with the different subscription channels of the OS packages for SAP HANA and SAP NetWeaver.
 - For IBM Power Virtual Servers, you can use publicly available AIX SUMA or SUSE update repositories, or use your own AIX NIM or

SUSE RMT servers.

- Software and patches download server. When the software is downloaded onto the server, you can use various protocols to transfer the files such as SCP or SFTP to transfer the software to the target server for installation.
- Time server (NTP), using NTP on IBM Cloud private backbone, public internet NTP or private NTP host.
- Gateway (and Proxy) and Firewall hosts
- Bastion/Jump host. Enables secured pass-through to your Cloud resources from public internet or other network access; often this uses tightly secured SSH on a non-default port.
- Jump host that is enabled with VNC or RDP. Enables GUI access to a target machine (if GUI and VNC or RDP is installed on the target).
- VPN hosts. Enables secured connection to your existing internal network.
- Network Routing hosts, via TelCo or Network Service Provider. Enables secured private high-throughput connection to your existing internal network.
- Backup management service hosts
- Network file storage, via Network File System (for example, NFSv3 or NFSv4.1). Runs file system commands encapsulated by TCP/IP packets.
- Network block storage, using iSCSI protocol controlled by MPIO. Runs SCSI commands encapsulated by TCP/IP packets.
- Network block storage, using Fibre Channel (FC) protocol. Runs SCSI commands encapsulated by FC frames.



Note: Fibre Channel is only required for IBM Power Virtual Servers, and is handled for you during provisioning.

Hybrid Cloud setup for SAP

The following are specific configuration items that you need consideration when planning your SAP landscape, by using your existing on-premises SAP support systems in combination with IBM Cloud® for SAP portfolio to create a Hybrid Cloud setup:

- [SAP Transport Management System \(STMS also known as. TMS\)](#). Configure STMS based on Transport Groups to prevent file sharing across data centers.
- [SAProuter](#). Provides access to SAP Online Service System (OSS). Use your on-premises SAProuter to access the OSS. This SAProuter can be used through further SAProuter hops if IP-based routing is not allowed between your IBM Cloud-based systems and your on-premises SAProuter. Alternatively, you might consider setting up another SAProuter that is based on one IBM Cloud-based server with a public IP and connect it to the SAP OSS system through the internet.
- [SAP Solution Manager](#). Access to the SAP Solution Manager has different connectivity requirements between an SAP Solution Manager and its managed systems. The differences depend on your usage scenario. These scenarios require an understanding of the required network connectivity.
- If you are deploying public gateways or floating IPs, you need to look into the details of Network Address Translation (NAT) and the behavior of SAP applications. Refer to the [SAP document on NAT](#) to consider potential issues on the application layer, especially in the SAP Remote Function Calls (RFCs).

Networking consumption considerations

Traditional SAP workload network communication is relatively small with under 100 MiB network traffic per day possible, such as:

- User transactions from SAPGUI; for Windows, for Java (used with macOS or Linux)
- User transactions from SAP WebGUI
- User transactions with SAP web Dynpro apps from SAP NetWeaver Business Client (NWBC)
- SAP Remote Function Call (SAP RFC) between SAP and non-SAP systems
- SAP iDOC Inbound/Outbound between SAP and non-SAP systems with third-parties (for example, banks, suppliers)

However, there are much larger SAP workload network communications too consuming significantly more network traffic, such as:

- SAPUI5 preinstall libraries and themes for SAP Fiori Launchpad and Apps
 - 10 MiB - 25 MiB (estimate) per new session that is loaded from SAP web Assistant (also known as. XRay), these preinstall libraries are then cached by the browser. *Once cached the libraries are available for use in any new browser tab, even after browser restart or SAP Fiori logout; until browser cache cleared*
 - 20 KiB - 500 KiB (estimate) per each new Fiori app that is loaded within the session
- SAP HANA System Replication (HSR) Sync or Async, streaming Gigabyte's of data per month from primary to secondary (or tertiary) nodes

With increased traffic of new design SAP software, it is possible to heavily exceed the amount of network traffic seen in past SAP usage.

Designing your SAP applications to use the IBM Cloud private backbone for these data transfers is important, as there are no ingress/egress charges; whereas usage over public internet incurs egress charges.

You should estimate the amount of data that is transferred. During initial project implementation stages, this can be difficult. However at least by an order of magnitude estimate should be performed.

Networking Throughput performance considerations

SAP generally recommends 10 Gbps (redundant) network throughput for traffic between its application servers and SAP HANA databases, and for other SAP HANA clients, such as SAP Business Intelligence.

For deployments of SAP NetWeaver using SAP AnyDB with local storage, even for three-tier setups, 1 Gbps networks are usually sufficient.

Networking Latency performance considerations

For your business operations and non-SAP dependent systems, you may require certain latency key performance indicators (KPIs) to be met. This should consider the site location of your hosts, and testing the latency by using the IBM Cloud private backbone network.

The testing of latency by using the Round Trip Time (RTT) metric is necessary when designing High Availability (HA) and Disaster Recovery (DR) for SAP HANA.

If a HA failover is being designed within one site location, in almost all cases this will be achievable for SAP HANA System Replication requirements.

However, if designing High Availability for SAP HANA across multiple sites within a Region, or if designing Disaster Recovery across multiple Regions then the latency that uses the Round Trip Time (RTT) metric must be carefully tested and considered.

This is because IBM Cloud seeks to ensure high availability of the platform, by using geographically dispersed site locations with fault tolerance (for example, different risk assessments). More information available on [How IBM Cloud ensures high availability and redundancy](#).

In particular, for VPC Infrastructure the Availability Zones are geographically dispersed locations within the Region. For most workloads, this design provides more redundancy across the Region. However, SAP HANA System Replication requires low network latency, which can become difficult to meet the necessary Round Trip Time (RTT) metric due to current technology physical data transfer limitations of cabling from a physics perspective (that is, speed of light over fiber Optic cable).

Networking Ports security considerations

The following information is a brief summary of [SAP Help Portal - TCP/IP Ports of All SAP Products](#), which provides an example of the considerations that are required for the security of your SAP Systems and entire IT infrastructure landscape on IBM Cloud.

Depending on the SAP Technical Applications used and the business scenarios being addressed, different hosts will need ports to be opened. Typically, to meet this requirement, the Firewall Port Groups are combined with Firewall Rules. You can also use individual Firewall Rules per host, although this often becomes unmanageable.

The below table includes some of the key Ports to use with SAP Systems that use SAP NetWeaver and SAP HANA, which need correction, depending on the SAP Technical Application's instance number; the instance numbers 00, 01, 02 are the defaults across the various SAP Technical Applications and will be in different patterns (these patterns are shown with `code blocks` highlighting):

SAP	Component	Port
Technical		
Application		
SAP Router		
	SAP Router	3200
	SAP Router	3299
SAP		
NetWeaver		
	SAP NetWeaver AS Primary App Server (PAS Dialog) Instance 01	3201

SAP NetWeaver AS PAS Gateway Instance 01	3301
SAP NetWeaver AS Central Services Messenger Server (ASCS MS) Instance 01	3602
SAP NetWeaver AS PAS Gateway (with SNC Enabled) Instance 01	4801
SAP NetWeaver AS ICM HTTP (Port 80 prefix)	8001
SAP NetWeaver AS ICM HTTPS (Secure, Port 443 prefix)	44301
SAP NetWeaver sapctrl HTTP (<i>Dual Host install</i>)	50113
SAP NetWeaver sapctrl HTTPS (<i>Dual Host install</i>)	50114
SAP HANA	
SAP HANA sapctrl HTTP (<i>One Host install</i>)	50013
SAP HANA sapctrl HTTPS (<i>One Host install</i>)	50014
SAP HANA Internal Web Dispatcher	30006
SAP HANA MDC System Tenant SYSD Index Server	30013
SAP HANA MDC Tenant 1 Index Server	30015
SAP HANA ICM HTTP Internal Web Dispatcher	8000
SAP HANA ICM HTTPS (Secure) Internal Web Dispatcher	4300
SAP Web Dispatcher	
SAP Web Dispatcher ICM HTTP (Port 80 prefix) Instance Number 90	8090
SAP Web Dispatcher ICM HTTPS (Secure, Port 443 prefix) Instance Number 90	44390
SAP HANA XSA	
SAP HANA XSA Instance 00 Client HTTPS for the connection to the xscontroller-managed Web Dispatcher (platform router) for purposes of user authentication.	30032
SAP HANA XSA Instance 00 Internal HTTPS for the connection from the xscontroller-managed Web Dispatcher (platform router) to xsuaaserver for purposes of user authentication.	30031
SAP HANA XSA Instance 00 Client HTTPS for the connection to the xscontroller-managed Web Dispatcher for purposes of data access.	30030
SAP HANA XSA Instance 00 Dynamic Range Internal HTTPS for the connection from the client to the xscontroller-managed Web Dispatcher (Platform Router) for access to the application instance.	51000-51500
SAP HANA XSA Instance 00 Internal HTTPS xseexecagent to xscontroller	30029
SAP HANA XSA Instance 00 Web Dispatcher HTTP(S) routing	30033

SAP
NetWeaver
Java

SAP NetWeaver AS Java P4 Port	50304
SAP NetWeaver AS Java P4 Port	50404

Common Ports used with SAP Technical Applications

Networking Traffic Segregation security considerations

You can separate different network traffic types in your landscape, either because of security restrictions or because of throughput considerations.

Segregation of networks is useful for the following SAP workload use cases:

- Multiple servers that exchange data
 - SAP Systems in a three-tier logical architecture, where the SAP database and SAP application instances are on different hosts.
- Multiple SAP Systems that exchange large amounts of data
 - Database servers, which need to have low network latency and high network throughput to network block/file storage therefore need to avoid firewalls. However the database still needs protection for other systems and networks access.

To use segregation of networks effectively, interconnectivity must be allowed under specific conditions.

VPC Infrastructure separation of subnets

To separate traffic, use multiple subnets.

Each VPC for a region can contain multiple subnets. These subnets within the VPC are enabled to communicate with each other, unless blocked by a Network ACL or Security Group. Therefore, two virtual servers in VPC infrastructure can have a virtual network interfaces (vNIC) on different subnets from each other.

The Network ACL or Security Group would allow specific network interconnectivity flows across these separate subnets.



Note: However, a virtual server in VPC infrastructure cannot have multiple virtual network interfaces (vNICs) assigned to multiple subnets.

Classic infrastructure separation of subnets

To separate traffic, use multiple VLAN and subnets therein.

Each VLAN is either public or private and is specific to the data center and the data center Pod. The VLAN can contain multiple subnets. These subnets within the VLAN are enabled to communicate with each other, unless blocked by a Gateway Appliance.

Therefore, two bare metal hosts in classic infrastructure might have physical network interface cards that are assigned to different VLAN and subnets from each other.

The Gateway Appliance would allow specific network interconnectivity flows across these separate subnets.

A bare metal server by default (can change depending on the hardware specifications) use physical network interface cards (NICs) and consume four ethernet ports:

- `eth0` NIC / `eth2` redundant NIC
 - Public VLAN, as DMZ trunked to Gateway Appliance
 - Public primary subnet
 - Public IP behind DMZ
- `eth1` NIC / `eth3` redundant NIC
 - Private VLAN, as DMZ trunked to Gateway Appliance
 - Private primary subnet
 - Private IP behind DMZ
- `mgmt0` --- IPMI (Admin Network Zone)

Bare metals can be reconfigured from default specific if the hardware specifications allow for it, with more subnets. This allows for maximum separation of traffic and can increase performance by using different network interface cards (NICs) to handle more network throughput in parallel. An example of this reconfiguration might be:

- `eth0` NIC / `eth2` redundant NIC
 - Public VLAN, as DMZ trunked to Gateway Appliance
 - Public primary subnet
 - Public IP behind DMZ
- `eth1` NIC / `altered to eth4` redundant NIC
 - Private VLAN, as DMZ trunked to Gateway Appliance
 - Private primary subnet
 - Private IP behind DMZ
- `eth3` additional NIC / `eth5` additional redundant NIC
 - Private VLAN
 - Private secondary portable subnet A
 - Private IP behind DMZ
 - Private secondary portable subnet B
 - Private IP behind DMZ
- `mgmt0` --- IPMI (Admin Network Zone)



Note: Such reconfiguration, as the example, will not be available in all scenarios.

For SAP HANA and the high network performance and security that is required, additional VLANs can assist. Read the recommendations by SAP for on-premises environments on [SAP HANA Network Requirements](#) and identify the suitable network configuration for meeting your business needs.

VMware on classic infrastructure separation of subnets

To separate traffic with IBM Cloud for VMware Solutions Dedicated, use multiple subnets within the VMware Overlay VXLAN (powered by VMware NSX).

In IBM Cloud for VMware Solutions Dedicated, the VMware Overlay VXLAN (powered by VMware NSX) is connected back to public VLAN and private VLAN on the classic infrastructure network as the underlay; the VMware NSX management utilizes the private secondary portable subnets to achieve the VXLAN. This provides full control of the network design when running on VMware, and allows assigning VMware VM's an IP from any defined range.

If instead using a manual deployment of VMware to a bare metal, the VMware vSwitch would directly use the private VLAN's secondary portable subnet to assign VMware VM's an IP address from the classic infrastructure network.

Traffic segregation needs to be considered carefully within VMware deployments, because elaborate VMware-based deployments, where different kinds of network traffic might need to be more strictly separated for security reasons.

Storage design considerations

The SAP systems in a landscape have specific requirements for servers, operating systems, network setup, and supported storage.

For SAP workloads that use a Cloud Service Provider, Infrastructure-as-a-Service is similar to existing practices used to run SAP workloads in external data centers or by a data center provider. An SAP landscape has specific requirements for connectivity, between hosts within Cloud IaaS and to external systems. IBM Cloud® for SAP provides a rich set of functions to improve your SAP landscape, beyond hosting SAP systems.

To assist your project's planning phase, the below sections provide IBM Cloud® for SAP portfolio design considerations for **Storage**.

Preface: units of measure for data/information

Storage performance refers to the read/write performance from storage file system. Often the throughput Network Storage is shown in Mbps or Gbps, whereas for Local Disk storage is shown in MiB/s.

It is important to note, that Mb (Megabits) is a decimal prefix and MiB (Mebibyte) is a binary prefix so they are on different scales. More confusion arises because MiB (Mebibyte) was commonly known in Microsoft Windows as `Megabyte`.

For future reference throughout the storage documentation, Mb (Megabits) and MiB (Mebibyte) is used based on the system of units (SI)

defined by IEC and adopted by IEEE, ISO, and NIST.

For example:

- 100 Mbps (Megabits per second), would be 12 MiB/s (Mebibyte per second)
- 1000 Mbps (Megabits per second) also known as 1 Gbps (Gigabits per second), would be 120 MiB/s (Mebibyte per second)
- 10 Gbps (Gigabits per second), would be 1200 MiB/s (Mebibyte per second)

Storage configuration for SAP HANA

With any SAP HANA certified profile that is listed as Appliance, storage is already provided or must be attached precisely as described.

When you provision more storage for an SAP HANA instance, you must adhere to mandatory TDI storage requirements. See the [SAP HANA TDI Overview](#), [SAP HANA TDI FAQ](#), [SAP Note 2493172 - SAP HANA Hardware and Cloud Measurement Tools](#), and follow the instructions of the [HCMT guide](#). Additional guidance you may find [here](#).

For more information for IBM Power Virtual Server, see [IBM System Storage Architecture and Configuration Guide for SAP HANA TDI v2.31.pdf](#).

The requirements include multiple volumes that are assigned to the DATA and LOG LVMS, with the striping and multipath enhancements increase I/O performance. For more information, see the following documents:

- [SAP HANA Tailored Data Center Integration \(TDI\) Overview](#)
- [SAP HANA Tailored Data Center Integration FAQ \(Updated May 2020\)](#)
- For file system sizes, see [SAP HANA Storage Requirements](#)

Storage performance considerations

It is important to calculate your project requirements before you decide on a storage solution. This calculation is critical for selecting network storage because of storage variations and performance considerations.

Storage impacts on Recovery Time Objective (RTO) of SAP HANA backups

If you need to restore an SAP HANA system, then the IOPS of your storage has a significant influence on your restore window. Backup windows are not as critical with SAP HANA since all backups are online backups no matter how you configure SAP HANA.

For example, by using IBM Cloud Block Storage for Classic, you can calculate for an approximate 12 TB restore of SAP HANA at a maximum speed. You must create three physical storage devices (block storage iSCSI LUNs) because the maximum size per device is 4 TB. You can create a stripe over these three devices with the Linux® Logical Volume Manager and create one logical device of 12 TB.

The 12 TB provides 3x10 IOPS/GB, which is a total of 122,880 IOPS/GB at 16 KB. This amount gives you a restore time of 1.875 GB per second, or a total restore time of under 2 hours. Since the measurement for the IOPS is taken at a 50/50 distribution of read and write, you can consider the numbers as a lower boundary of restore performance. It is advisable to do backup and restore tests if you rely on a certain restore window.

Network Block Storage considerations

The following sections describe the storage considerations that use network block storage for SAP workload scenarios that use various IBM Cloud infrastructure options.

Network Block or File storage for VMware on Classic Infrastructure

Using VMware for SAP workloads on IBM Cloud is certified. However it requires choice of the storage and would use the "TDI" delivery model for which you would need to run validation checks to gain SAP Support. Therefore, it is important to consider the correct storage for your VMware hosts when they are running SAP workloads.

For VMware clusters, where SAP workloads are run across multiple VMware vSphere hypervisor nodes, storage must be shared across these hypervisor nodes.

VMware is available to work with Block storage or File storage from IBM Cloud. To help you select Block storage or File storage for running SAP on VMware, see [VMware Technical Paper on Storage Protocol Comparison](#).

When you are using Network Block or File storage, do not expect that certification performance benchmarks to remain the same. Particularly after factoring in the hypervisor overheads as described in [Compute Profiles of SAP-certified VMware on Classic Infrastructure](#).

For VMware datastores (where the virtual machine .VMDK virtual disks are located), the recommendations are:

- For SAP HANA, use Local SSD disks for the datastore in a RAID10 configuration
- For SAP HANA, with network storage, use 10 IOPS/GB with each vSphere node that hosts SAP that uses a network interface card with 10 Gbps connection
- For SAP NetWeaver or SAP AnyDB, with network storage, use at least 4 IOPS/GB with each vSphere node that hosts SAP that uses a network interface card with 10 Gbps connection

To achieve maximum IOPS on a volume, adequate network resources need to be in place. Other considerations include private network usage outside of storage and host side, and application-specific tunings (for example, IP stacks and queue depths). For more information, see [Getting started with Block Storage](#) and [Getting started with File Storage](#) for more information on storage tiers and performance.

The storage to use with either the VMware manual setup (Bare Metal with VMware OS Image) or VMware automated setup (IBM Cloud for VMware Solutions Dedicated), is described in:

- [Storage to use with VMware vSphere on IBM Cloud Bare Metals](#) provides further direction on how to integrate storage in an ESX environment.
- [Storage to use with IBM Cloud for VMware Solutions Dedicated](#)

Block Storage for Virtual Servers on VPC Infrastructure

For network storage, IOPS per GB is limited and performance depends on the workload. For relational database management systems (RDBMS), it might be advisable to use the same volume for both the database's log and data storage. This setup depends on the behavior of your application.

In general, for typical RDBMS-based applications, a 5 IOPS/GB profile is reasonable.

If your application uses dedicated key performance indicators (KPIs) on storage performance, test the storage throughput before you begin software deployment. By using volume manager-based software RAID (like LVM), you meet almost every KPI.

Sample storage configurations on Classic Infrastructure

The following sections demonstrate storage configurations in various different SAP workload scenarios, which are using **Classic Infrastructure**.

Sample storage configuration for IBM Db2 that use Intel Bare Metal

Table 1 is a sample storage configuration for a 256 GB server with 50,000 [SAPS](#), 1.5 TB at 6,000 IOPS for a central system with SAP. The system uses an IBM Db2 database with external [IBM Cloud Block Storage for Classic](#) or [IBM Cloud File Storage for Classic](#) (4 IOPS/GB). The calculation for the IOPS is:

- $6,000 \text{ IOPS} / 1,500 \text{ GB} = 4 \text{ IOPS/GB}$ needed for external storage. It is assumed that 3,000 GB is for backup at 2 IOPS/GB (medium performance).

File system	number of volumes	Storage type	IOPS/GB	GB	IOPS
/	1	Internal	N/A	150 GB	N/A
/boot	1	Internal	N/A	0.25 GB	N/A
swap	1	Internal	N/A	256 GB	N/A
/db2 (including logs)	1	Internal	N/A	250 GB	N/A
sapdata	1	External	4 IOPS/GB	1,500 GB	6,000
backup/log and backup	1	External	2 IOPS/GB	3,000 GB	6,000

Sample storage layout based on IOPS calculation

Sample storage configurations on VPC Infrastructure

The following sections demonstrate storage configurations in various different SAP workload scenarios, when you are using **VPC Infrastructure**.

Sample storage configuration for SAP AnyDB with IBM Db2 that uses Intel Virtual Server

For SAP AnyDB that uses IBM Db2 on **mx2-32x256** profile the volumes that are needed are:

- 1x 500 GB volumes; one block storage volume of 500 GB size, with a custom volume profile that supports up to 10,000 **Max IOPS** attached to the Virtual Server
- 1x 2,000 GB volume; one block storage volume of 2,000 GB size, with a lower 4,000 IOPS (medium performance) attached to the Virtual Server for backups

Disk mount points and volumes for IBM Db2

After you attach the two data volumes, two new virtual disks will appear in the Virtual Server, see the following table. In this example, those disks are **vdd**, **vde**, and **vdf**.

File system	Volume	Storage type	IOPS/GB	GB	IOPS
/	vdal	Pre-configured boot volume	N/A	100 GB	3,000
/boot	vda2	Pre-configured boot volume	N/A	0.25 GB	3,000
/db2	vdd (can vary)	Data volume	20 IOPS/GB	500 GB	10,000
backup/log and backup	vde (can vary)	Data volume	5 IOPS/GB	2,000 GB	4,000

Sample storage configuration

Table 1 shows a basic layout of the file system to support an IBM Db2 installation. Generally, an IBM Db2 installation uses subdirectories that can be segmented into independent volumes.

For example, `"/db2/<DBSID>"`, `"/db2/<DBSID>/log_dir"`, and several `"sapdata<n>"`, where the folder `"log_dir"` contains the online logs files of the database and the `"sapdata<n>"` contains the data itself. For example, see the Db2 documentation here: [Required File Systems for IBM Db2 for Linux, UNIX, and Windows](#).

Sample storage configurations for SAP HANA

Further information about [storage specifications for Virtual Server](#) are available, the below shows only the configuration steps required.

mx2-8x64, mx2-16x128 and mx2-32x256 profiles



Note: The mx2-8x64 profile is certified for SAP Business One on HANA only.

For Virtual Server created based on the **mx2-8x64**, **mx2-16x128** and **mx2-32x256** profiles, there are:

- 3x 500 GB volumes; three block storage volumes of 500 GB size, with a custom volume profile that supports up to 10,000 **Max IOPS** attached to the Virtual Server
- 1x 2,000 GB volume; one block storage volume of 2,000 GB size, with a lower 4,000 IOPS (medium performance) attached to the Virtual Server for backups

After attaching the three data volumes, three new virtual disks will appear in the virtual server, see the table that follows. In this example, those disks are **vdd**, **vde** and **vdf**.

The disks are visible in the operating system of the virtual server as follows:

```
$ [root@hana256-vsi ~]# fdisk -l

Disk /dev/vdd: 536.9 GB, 536870912000 bytes, 1048576000 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/vde: 536.9 GB, 536870912000 bytes, 1048576000 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

```
Disk /dev/vdf: 536.9 GB, 536870912000 bytes, 1048576000 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

These three disks must be managed under the Linux® Logical Volume Manager (LVM), and deployed as logical volumes. In order to achieve that, first put the three devices under LVM control. For example, make them physical volumes:

```
$ [root@hana256-vsi ~]# pvcreate /dev/vdd /dev/vde /dev/vdf
```

Then, create a volume group from the physical volumes. The name of the volume group can be chosen according to your preferences, in our sample it is `hana_vg`:

```
$ [root@hana256-vsi ~]# vgcreate hana_vg /dev/vdd /dev/vde /dev/vdf
```

After creating the volume group, three logical volumes need to be defined on top. These logical volumes reflect the file system size requirements for SAP HANA. The following commands are for a 256 GB virtual server:

```
$ [root@hana256-vsi ~]# lvcreate -i 3 -I 64K -L 256GB -n hana_log_lv hana_vg
[root@hana256-vsi ~]# lvcreate -i 3 -I 64K -L 256GB -n hana_shared_lv hana_vg
[root@hana256-vsi ~]# lvcreate -i 3 -I 64K -l 100%FREE -n hana_data_lv hana_vg
```

For a 128 GB virtual server, in the example above `-L 256GB` must be replaced by `-L 128GB` and for 64 GB by `-L 64GB` accordingly. These commands will not result in the smallest possible file system size, but they create the smallest configuration, which will fulfill the SAP HANA KPIs. Finally, a file system needs to be created on top of each volume group:

```
$ [root@hana256-vsi ~]# mkfs.xfs /dev/mapper/hana_vg-hana_log_lv
[root@hana256-vsi ~]# mkfs.xfs /dev/mapper/hana_vg-hana_data_lv
[root@hana256-vsi ~]# mkfs.xfs /dev/mapper/hana_vg-hana_shared_lv
```

The following entries to `/etc/fstab` will mount the file systems after their mount points (`/hana/data`, `/hana/log` and `/hana/shared`) have been created:

```
$ /dev/mapper/hana_vg-hana_log_lv    /hana/log xfs defaults,swalloc,nobarrier,inode64
/dev/mapper/hana_vg-hana_shared_lv /hana/shared xfs defaults,inode64 0 0
/dev/mapper/hana_vg-hana_data_lv   /hana/data xfs defaults,largeio,swalloc,inode64 0 0
```

mx2-48x384 profile

For Virtual Server created based on the **mx2-48x384** profile there are:

- 3x 500 GB volumes; three block storage volumes of 500 GB size, with a custom volume profile that supports up to 10,000 **Max IOPS** attached to the Virtual Server is required
- 4x 100 GB volumes; four block storage volumes of 100 GB size, with a custom volume profile that supports up to 6,000 **Max IOPS** attached to the Virtual Server is required
- *Optional:* 1x 2,000 GB volume; one block storage volume of 2,000 GB size, with a lower 4,000 IOPS (medium performance) attached to the Virtual Server for backups

After attaching the seven data volumes, seven new virtual disks will appear in the Virtual Server, see the table that follows. In this example, those disks are `vdd`, `vde`, `vdf`, `vdg`, `vdh`, `vdi`, `vdj`.

These three disks must be managed under the Linux® Logical Volume Manager (LVM), and deployed as logical volumes. In order to achieve that, first put the three devices under LVM control. For example, make them physical volumes:

```
$ [root@hana384-vsi ~]# pvcreate /dev/vd[d,e,f,g,h,i,j]
```

Then, two different volume groups need to be created:

```
$ [root@hana384-vsi ~]# vgcreate hana_vg /dev/vdh /dev/vdi /dev/vdj
[root@hana384-vsi ~]# vgcreate hana_log_vg /dev/vdd /dev/vde /dev/vdf /dev/vdg
```

Next, three logical volumes need to be defined on top. These logical volumes reflect the file system size requirements for SAP HANA. The

following commands are for a 384 GB virtual server:

```
$ [root@hana384-vsi ~]# lvcreate -l 100%VG -i 4 -I 64K -n hana_log_lv hana_log_vg  
[root@hana384-vsi ~]# lvcreate -i 3 -L 384G -I 64K -n hana_shared_lv hana_vg  
[root@hana384-vsi ~]# lvcreate -i 3 -l 100%FREE -I 64K -n hana_data_lv hana_vg
```

Finally, a file system needs to be created on top of each volume group:

```
$ [root@hana384-vsi ~]# mkfs.xfs /dev/mapper/hana_log_vg-hana_log_lv  
[root@hana384-vsi ~]# mkfs.xfs /dev/mapper/hana_vg-hana_data_lv  
[root@hana384-vsi ~]# mkfs.xfs /dev/mapper/hana_vg-hana_shared_lv
```

The following entries to `/etc/fstab` mount the file systems after their mount points (`/hana/data`, `/hana/log` and `/hana/shared`) have been created:

```
$ /dev/mapper/hana_log_vg-hana_log_lv    /hana/log xfs defaults,swalloc,nobarrier,inode64  
/dev/mapper/hana_vg-hana_shared_lv /hana/shared xfs defaults,inode64 0 0  
/dev/mapper/hana_vg-hana_data_lv    /hana/data xfs defaults,largeio,swalloc,inode64 0 0
```

General storage configurations on IBM Power Virtual Server Infrastructure

The following sections provides general recommendations for storage configurations of different SAP workloads on IBM Power Virtual Servers.

General storage guidelines for SAP application on IBM Power Virtual Server

- For boot volume it is recommended to use `Fixed IOPs` or `Tier 0`.
- An additional Capacity for `/usr/sap` using `Fixed IOPs` or `Tier 0` on a separate storage volume is recommended.

General storage guidelines for SAP HANA on IBM Power Virtual Server

- Use block storage volumes with minimum `12,000 IOPS` for SAP HANA `log` file system. SAP HANA log file system size is usually up to `512 GB`. We recommend to stripe file system over `4` storage volumes.
- Use block storage volumes with minimum `8,000 IOPS` for SAP HANA data file system. SAP HANA `data` file system size depends on memory size. SAP recommends to ensure `120-150%` of memory configured for the virtual machine. We recommend to stripe file system over `4` storage volumes.
- SAP does not provide any performance requirements for SAP HANA `shared` file system. We recommend to configure minimum `3000 IOPS` for the file system. Block storage volume striping is not required. As alternative, SAP HANA shared file system may reside on NFS volume.
- For OS boot volume we recommend to use `Fixed IOPs` or `Tier 0`.
- An additional capacity for `/usr/sap` on `Fixed IOPs` or `Tier 0` on a separate storage volume is recommended.
- See following documentation for [sample storage configurations for SAP HANA certified profiles on IBM Power Virtual Server](#).

Sample storage configuration for Oracle DB on IBM AIX that use the IBM Power Virtual Server

Table 2 is a sample configuration for an AIX IBM Power Virtual Server for an SAP NetWeaver application server that uses Oracle as the example.

The storage cannot be combined within the same IBM Power Virtual Server, and can be either Tier 1 or Tier 3. The recommendation is to provision three more disks to enable separation between the OS, database, and application layer. Disk size depends on if the installation is Greenfield or if the server is a copy of an "on-premises" AIX server you decided to use as a sizing reference.

The naming convention for the LVM entries is optional, but the advice is to include the SID of your SAP NetWeaver system, especially if you plan to install one or more instances.

Storage	Volume group	Logical volume	Mount point
OS disk	Default configuration	Default configuration	Default configuration
Application disk	app<sid>vg	lvusrsap	/usr/sap
		lvusrsap{SID}	/usr/sap/{SID}

	lvusrsapmnt	/sapmnt/{SID}
	lvusrsaptrans	/usr/sap/trans
	lvsapDAH	/usr/sap/DAH
Database storage	db<sid>vg	lv{SID}arch
		/oracle/{SID}/oraarch
		lv{SID}reorg
		/oracle/{SID}/sapreorg
		lv{SID}origlogA
		/oracle/{SID}/origlogA
		lv{SID}origlogB
		/oracle/{SID}/origlogB
		lv{SID}ora
		/oracle/{SID}
		lv{SID}sapdata1
		/oracle/{SID}/sapdata1
		lv{SID}sapdata2
		/oracle/{SID}/sapdata2
		lvorastage
		/oracle/stage
		lv{SID}sapdata3
		/oracle/{SID}/sapdata3
		lv{SID}sapdata4
		/oracle/{SID}/sapdata4
		lv{SID}oraclient
		/oracle/client

Sample storage layout for Oracle

For more information, see [SAP Note 2172935](#).

Sample storage configuration for IBM Db2 SaaS on IBM AIX that use the IBM Power Virtual Server

Table 3 is a sample storage configuration for an AIX IBM Power Virtual Server for an IBM Db2 SaaS server.

The storage cannot be combined within the same IBM Power Virtual Server, and can be either Tier 1 or Tier 3. The recommendations are to provision three more disks to enable separation between the OS, database, and application layer. Disk size depends on whether the installation is Greenfield or the server is a copy of an "on-premises" AIX server that you decided to use as a sizing reference.

The naming convention for the LVM entries is optional, but the advice is to include the SID of your SAP NetWeaver system especially if you plan to install one or more instances.

Storage	Volume group	Logical volume	Mount point
OS disk	Default configuration	Default configuration	Default configuration
Application disk	app<sid>vg	lvusrsap	/usr/sap
		lvusrsap{SID}	/usr/sap/{SID}
		lvusrsapmnt	/sapmnt/{SID}
		lvusrsaptrans	/usr/sap/trans
		lvsapDAH	/usr/sap/DAH
Db2 database storage I	<sid>db2vg	loglv{SID}	NA

	lv{SID}db2	/db2/{SID}	
	lvhome{SID}	/db2/db2{SID}	
	lv{SID}db2dump	/db2/{SID}/db2dump	
	lv{SID}logdir	/db2/{SID}/log_dir	
	lv{SID}log_archive	/db2/{SID}/log_archive	
	lv{SID}saptmp	/db2/{SID}/saptemp1	
	lv{SID}db2sw	/db2/db2/<DBSID>/db2_sw	
Db2 database storage II	<sid>db2datvg	lv{SID}sapdata1	/db2/{SID}/sapdata1
		lv{SID}sapdata2	/db2/{SID}/sapdata2
		lv{SID}sapdata3	/db2/{SID}/sapdata3
		lv{SID}sapdata4	/db2/{SID}/sapdata4

Sample storage layout for Db2 on Cloud

For more information, see [Required File Systems for IBM Db2 for Linux, UNIX, and Windows](#) and [SAP Note 1707361](#).

Compute and OS design considerations

The SAP systems in a landscape have specific requirements for servers, operating systems, network setup, and supported storage.

In some regards, SAP workloads that use a cloud service provider (such as IBM Cloud® for SAP) Infrastructure-as-a-Service (IaaS) is similar to existing practices over many decades for running SAP workloads by using an external data center or data center provider. An SAP landscape has specific requirements for connectivity, between hosts within a cloud environment and to external systems. IBM Cloud® for SAP provides a rich set of functions beyond hosting of SAP systems to improve your SAP landscape.

The [SAP-certified IaaS offerings](#) provide different compute options and variations of capabilities and sizing for SAP workloads. They are available on IBM Cloud in many IBM data centers around the world. See the current data centers in [IBM Cloud regions](#).

To assist your project's planning phase, the following sections provide IBM Cloud® for SAP portfolio design considerations for **Compute and OS**.

Compute Performance considerations

The IBM Cloud® for SAP portfolio is ideal for practically all SAP use case scenarios. You can use your servers for mission-critical workloads, as your test environment, or your business continuity disaster recovery (BCDR) site.

SAP application server work processes scheduling and scaling

CPU thread consumption affects the following processes.

- Dialog Work Process
- Update Work Process
- Background Work Process
- Enqueue Work Process
- Spool Work Process

Compute Profiles of SAP-certified Bare Metal on Classic Infrastructure

You are offered SAP-certified servers, which have various pre-configured combinations of the amount of RAM and number of CPUs.

For SAP HANA workloads, these combinations represent the [appliance delivery model](#) of SAP HANA hardware certification. Except, that IBM

Cloud does not pre-install SAP HANA platform. Therefore, the characteristics of the server (amount of RAM and disks) cannot be changed during the ordering process or through a support ticket after servers are deployed.

Servers that are intended for SAP application server based workloads, the configuration is more flexible, i.e. you may add or remove disks as you like.

SAP HANA database servers and SAP application servers run on IBM Cloud Classic using [Intel Bare Metal server certified profiles on Classic infrastructure for SAP HANA](#). In addition, SAP application servers run on IBM Cloud Classic using [Intel Bare Metal server certified profiles on Classic infrastructure for SAP application server](#). For more information, see [Intel Bare Metal servers on Classic Infrastructure](#).

Compute Profiles of SAP-certified Bare Metal on VPC Infrastructure

SAP HANA database servers and SAP application servers run on IBM Cloud VPC using [Intel Virtual Server certified profiles on Classic infrastructure for SAP HANA](#). In addition, SAP application servers run on IBM Cloud Classic using [Intel Bare Metal server certified profiles on Classic infrastructure for SAP application server](#). For more information, see [Intel Bare Metal servers on Classic Infrastructure](#).

Compute Profiles of SAP-certified Virtual Servers on VPC Infrastructure

IBM Cloud® for SAP provides SAP-certified infrastructure by using IBM's latest virtual servers which are available with instantaneous provisioning, and are offered in different profiles that define vCPU and RAM combinations.

SAP HANA database servers and SAP application servers run on IBM Cloud VPC using [Intel Virtual Server certified profiles on VPC infrastructure for SAP HANA](#). In addition, SAP application servers run on IBM Cloud VPC using [Intel Virtual Server certified profiles on VPC infrastructure for SAP application server](#). For more information, see [Intel Virtual Servers on VPC Infrastructure](#).

SAP HANA certified instances on IBM Power Virtual Server

SAP HANA database servers and SAP application servers run on IBM Power Systems using [IBM Power Virtual Server certified profiles for SAP HANA](#). For more information, see [SAP HANA and IBM Power Virtual Server](#), [SAP NetWeaver and IBM Power Virtual Server](#), and [SAP NetWeaver certified instances on IBM Power Virtual Server](#).

All SAP application server ABAP-based products and SAP application server Java-based products are supported on IBM Power Virtual Servers. For SAP application server-based SAP products, see [SAP Note 2855850 - SAP Applications on IBM Power Virtual Servers](#).

All SAP HANA-based products are supported on IBM Power Virtual Servers. For support requirements, see [SAP Note 2923984 - SAP on IBM Power Virtual Servers: Support prerequisites](#).

For all other software components or third-party products, contact [SAP Support](#).

Compute Profiles of SAP-certified VMware on Classic Infrastructure



Note: VMware runs on the same SAP-certified Bare Metals. Therefore, the VMware vSphere (ESXi) installation on the certified hardware enables the VMware-SAP certification and agreements to be valid. Therefore, all VMware-SAP certification guidance must be followed (as described in SAP Notes for VMware-SAP).

VMware SDDC is available as a customer-controlled root-access hypervisor, which is certified to run SAP workloads. Providing VMware SDDC does not automatically provide a pre-sized virtual machine for SAP HANA or SAP application server upon provisioning either the OS image with VMware vSphere (ESXi) for the Bare Metal or the fully automated setup from IBM Cloud for VMware Solutions Dedicated. You choose how to size and configure your SAP Workloads (for SAP HANA, size and configuration is under the SAP HANA TDI delivery model).

When you run SAP workloads on VMware, you have significant flexibility and the full capabilities which VMware built to run SAP workloads over decades is available to use.

Using VMware for SAP workloads on IBM Cloud is certified, by using the "TDI" delivery model for which you would need to run validation checks to gain SAP Support.

However, VMware SDDC is a Type 2 hypervisor and therefore does have a small overhead of CPU/RAM that is used for running ESXi on the Bare Metal server. This CPU/RAM overhead is then available for virtual machines to use. On average this overhead is 10%, and is expected by VMware-SAP in virtualized environments. Therefore, customers are encouraged to size correctly and test performance before you go live.

Both, VMware and SAP agree to the physical to virtual overhead of <10% on average, and provide:

- The estimation of <10% average overhead with equation **"physical SAPS - 10%"** for virtualized SAPS to use when you size virtual machines
- The estimation of **"between 0.5% and 3%"** subtracted from total available physical RAM. Although, *"the actual RAM overhead can be*

defined only after the VMs are configured"

- Only for half-socket VMs and sharing of NUMA Node between two VMs. Keep in mind that "additional performance impact" and a "sizing buffer of at least 15%" of the CPU (SAPS) is recommended.

Sources:

- [Page 29ff, Configuration and sizing guidelines](#)
- [SAP Help Portal - SAP HANA on VMware vSphere](#)

Several other SAP-defined rules must be followed to deploy SAP HANA in a VMware SDDC environment. For more information, see the following documentation:

- [SAP Note 2161991 - VMware vSphere configuration guidelines](#)
- [SAP Note 2937606 - SAP HANA on VMware vSphere 7.0 in production](#)
- [SAP Note 3372365 - SAP HANA on VMware vSphere 8](#)
- [SAP Note 2779240 - Workload-based sizing for virtualized environments](#)
- [SAP HANA Tailored Data Center Integration Frequently Asked Questions](#)

Operating Systems considerations

The IBM Cloud® for SAP portfolio provides various Operating Systems for the Enterprise IT organization to select from.

Operating Systems supported

You need to consult [SAP Note 2414097](#) for a list of guest operating systems (OS) to deploy SAP HANA and SAP application server-based systems. An SAP S-user ID is required to access the SAP Note.

For the Operating System, the SAP HANA certified servers are available with the following operating systems:

- Red Hat Enterprise Linux for SAP HANA
- SUSE Linux Enterprise Server for SAP HANA
- VMware vSphere hypervisor (ESXi) + created Guest OS with RHEL/SLES

For the Operating System, the SAP application server certified servers are available with the following operating systems:

- IBM AIX (only on IBM Power Virtual Server)
- Red Hat Enterprise Linux for SAP Applications
- SUSE Linux Enterprise Server for SAP Applications
- VMware vSphere hypervisor (ESXi) + created Guest OS with RHEL/SLES/WinS
- Windows Server

For SAP HANA release versions (including SPS and Revision and Patch numbers), support is only available for pre-defined and specific major.minor releases of an Operating System (for example, RHEL 9.2). This information is shown in [SAP 2235581 - SAP HANA: Supported Operating Systems](#). An example is available in the SAP Note attachment [SAP_HANA_OS_Release_Support_Matrix.pdf](#).

For SAP application server release versions, support is available for each major release of an Operating System (for example, SLES 15) meaning each subsequent release is available for use (example: SLES 15 SPS3, SLES 15 SP4, and so on). This information is shown in the [SAP Product Availability Matrix \(PAM\)](#).

OS configuration for SAP

Each infrastructure has various operating systems with various images for those operating systems available on-demand.

Each of these on-demand OS images (for example, RHEL 9.2 for SAP HANA) is provided as shipped (also known as the "general availability" / "stock image" release) by each of the vendors (for example, Red Hat). These OS images are provided with access from the OS Package Manager to the OS package update channels specific to the OS Packages for SAP. The OS package update channels permit updates to the OS according to the latest SAP Notes for the relevant Operating System with the specified OS kernel versions, OS package versions, and OS package for SAP versions that are required.

Therefore, for OS images, you need to perform the following actions.

- OS configuration according to SAP guidance.
- OS package updates according to SAP guidance, which may include updates to specified OS kernel versions (for example, for RHEL 9.2 see SAP Note [3108302 - SAP HANA DB: Recommended OS Settings for RHEL 9](#)).

OS for Virtual Servers on VPC Infrastructure

For a list of operating systems and databases available for SAP application server-based system deployments, see [SAP Note 2927211](#).



Note: An SAP S-user ID is required to access the SAP Note.

OS for IBM Power Virtual Servers

For the Linux® versions to deploy for SAP HANA, see [SAP Note 2947579 - SAP HANA on IBM Power Virtual Servers](#). An SAP S-user ID is required to access the SAP Note.

For the version of IBM AIX or Linux on Power to deploy for SAP application server-based systems, see [SAP Note 2855850 - SAP Applications on IBM Power Virtual Servers](#). An SAP S-user ID is required to access the SAP Note. License fees for AIX are covered by your monthly billing rate.

Operating system for SAP HANA	Image name (Client supplied subscription)	Image name (IBM provided subscription)
Red Hat Enterprise Linux (RHEL) 8.4	RHEL8-SP4-SAP-BYOL	RHEL8-SP4-SAP
Red Hat Enterprise Linux (RHEL) 8.6	RHEL8-SP6-SAP-BYOL	RHEL8-SP6-SAP
Red Hat Enterprise Linux (RHEL) 8.8	RHEL8-SP8-SAP-BYOL	RHEL8-SP8-SAP
Red Hat Enterprise Linux (RHEL) 8.10	RHEL8-SP10-SAP-BYOL	RHEL8-SP10-SAP
Red Hat Enterprise Linux (RHEL) 9.2	RHEL9-SP2-SAP-BYOL	RHEL9-SP2-SAP
Red Hat Enterprise Linux (RHEL) 9.4	RHEL9-SP4-SAP-BYOL	RHEL9-SP4-SAP
SUSE Linux Enterprise Server (SLES) for SAP 15 SP2	SLES15-SP2-SAP-BYOL	SLES15-SP2-SAP
SUSE Linux Enterprise Server (SLES) for SAP 15 SP3	SLES15-SP3-SAP-BYOL	SLES15-SP3-SAP
SUSE Linux Enterprise Server (SLES) for SAP 15 SP4	SLES15-SP4-SAP-BYOL	SLES15-SP4-SAP
SUSE Linux Enterprise Server (SLES) for SAP 15 SP5	SLES15-SP5-SAP-BYOL	SLES15-SP5-SAP
SUSE Linux Enterprise Server (SLES) for SAP 15 SP6	SLES15-SP6-SAP-BYOL	SLES15-SP6-SAP
Operating systems for IBM Power Virtual Servers on SAP HANA		
Operating system for SAP application server	Image name (Client supplied subscription)	Image name (IBM provided subscription)
Red Hat Enterprise Linux (RHEL) 8.4	RHEL8-SP4-SAP-NETWEAVER-BYOL	RHEL8-SP4-SAP-NETWEAVER
Red Hat Enterprise Linux (RHEL) 8.6	RHEL8-SP6-SAP-NETWEAVER-BYOL	RHEL8-SP6-SAP-NETWEAVER
Red Hat Enterprise Linux (RHEL) 8.8	RHEL8-SP8-SAP-NETWEAVER-BYOL	RHEL8-SP8-SAP-NETWEAVER
Red Hat Enterprise Linux (RHEL) 8.10	RHEL8-SP10-SAP-NETWEAVER-BYOL	RHEL8-SP10-SAP-NETWEAVER
Red Hat Enterprise Linux (RHEL) 9.2	RHEL9-SP2-SAP-NETWEAVER-BYOL	RHEL9-SP2-SAP-NETWEAVER

Red Hat Enterprise Linux (RHEL) 9.4	RHEL9-SP4-SAP-NETWEAVER-BYOL	RHEL9-SP4-SAP-NETWEAVER
SUSE Linux Enterprise Server (SLES) for SAP 15 SP2	SLES15-SP2-SAP-NETWEAVER-BYOL	SLES15-SP2-SAP-NETWEAVER
SUSE Linux Enterprise Server (SLES) for SAP 15 SP3	SLES15-SP3-SAP-NETWEAVER-BYOL	SLES15-SP3-SAP-NETWEAVER
SUSE Linux Enterprise Server (SLES) for SAP 15 SP4	SLES15-SP4-SAP-NETWEAVER-BYOL	SLES15-SP4-SAP-NETWEAVER
SUSE Linux Enterprise Server (SLES) for SAP 15 SP5	SLES15-SP5-SAP-NETWEAVER-BYOL	SLES15-SP5-SAP-NETWEAVER
SUSE Linux Enterprise Server (SLES) for SAP 15 SP6	SLES15-SP6-SAP-NETWEAVER-BYOL	SLES15-SP6-SAP-NETWEAVER
AIX 7.2		7200-05-08 or later
AIX 7.3		7300-02-01 or later

Operating systems for IBM Power Virtual Servers on SAP application server

OS when you use VMware SDDC

VMware SDDC is available as a customer-controlled root-access hypervisor, which is available as an OS image for the Bare Metal or available with fully automated setup from IBM Cloud for VMware Solutions Dedicated. The VMware licensing can be included or BYOL.

However, when you run a VMware SDDC, the Virtual Machine's Guest OS licensing and subscriptions (to the relevant package update channels, including OS Packages for SAP) is covered by you.

Only the following operating systems are supported as guest Operating Systems for VMware SDDC and SAP workloads.

- Red Hat Enterprise Linux (RHEL) for SAP
- SUSE Linux Enterprise Server for SAP
- Microsoft Windows Server

See [SAP Note 2414097](#) for version details.

Refer to [Installing VMware vSphere ESXi by using Remote Console and Virtual Media](#) and other VMware.com documentation to install a Guest OS.

Bring-your-own-OS (custom OS image and BYOL License)

When you have your own operating system image and license, it can be used with IBM Cloud and the OS install based on the vendor's instructions.

Infrastructure	Bring your own OS documentation	SAP supported workloads
Intel Bare Metal Servers on Classic Infrastructure	OS BYOL and custom image (BYOS) by using the "no OS" option during provisioning	SAP HANA by using TDI deployment SAP NetWeaver AS
Intel Virtual Servers (Gen2) on VPC Infrastructure	OS BYOL and Custom image (BYOS) by using Importing and managing custom images	SAP HANA by using TDI deployment SAP NetWeaver AS
IBM Power Virtual Server in the IBM Power Infrastructure environment	Linux OS BYOL and Custom Image (BYOS) by using Capturing and importing an RHEL image and Capturing and importing a SLES image	SAP HANA, SAP application server

IBM Power Virtual Server in the IBM Power Infrastructure environment	Unix OS BYOL and Custom Image (BYOS) by using Importing a boot image for IBM AIX or IBM i	SAP NetWeaver AS
VMware SDDC on IBM Cloud	OS BYOL and custom image (BYOS) by using standard Virtual Machine Guest OS guidance from VMware documentation	Supported according to SAP-VMware guidance

Bring your own customized OS image and BYOL License

Planning Disaster Recovery for SAP solutions on IBM Cloud

Disaster Recovery (DR) is a strategic plan that helps organizations respond to unplanned events such as natural disasters, power outages, cyberattacks, and other disruptive events. The primary goal of a DR plan is to minimize the impact of such disruptions and enable the organization to continue or quickly resume critical operations. A well-structured DR plan provides quick recovery, independent of the cause of the disruption to reduce potential revenue loss, brand damage, and customer dissatisfaction.

Design and implement a disaster recovery strategy for organizations that run SAP systems in the IBM Cloud by completing the following steps:

1. Assess your business needs by including processes to identify critical data, determine Recovery Time Objectives (RTO), and set Recovery Point Objectives (RPOs).
2. Design the disaster recovery strategy by including the data replication methods, backup locations, and failover and fallback procedures.
3. Implement the disaster recovery strategy by using IBM Cloud services such as IBM Virtual Private Cloud (VPC), IBM Power Virtual Servers, and IBM Cloud Object Storage. These services facilitate automation, scalability, and enhanced redundancy.
4. Configure the network and security settings focusing on VPCs, VPNs, direct links, access controls, and encryption.
5. Ensure that you regularly test, monitor, and maintain your disaster recovery plan to ensure its effectiveness and relevance.

Assessing your business needs

Understand your business needs before you design the DR strategy. Analyze the required data, applications, and information. Identify the critical systems of your business. Each application has specific RTO and RPO requirements, which are described as service classes or tiers.

Defining resiliency tiers

Categorize your applications to resiliency tiers based on their RTO and RPO requirements.

The following list is an example of how you can classify a resiliency tier:

- Tier 1: Continuous availability (RTO <= 1 hour and RPO <= 1 hour)
- Tier 2: Advanced recovery (> 1 hour to <= 24 hours and RPO < 2 hours to <= 24 hours)
- Tier 3: Standard recovery (> 24 hours to <= 72 hours and RPO: Last Backup)
- Tier 4: No recovery (Not applicable)

Designing your disaster recovery strategy for IBM Cloud

After you thoroughly assess your business needs, design a DR strategy that meets your needs. Consider the following operations:

Data replication

Select one of the following data replication methods according to your RTOs and RPOs:

- SAP HANA System Replication, IBM Db2 HADR, or Oracle Data Guard, which uses the database layer of the SAP system for data replication.
- [Global Replication Services \(GRS\)](#) in IBM Power Virtual Server that provides an asynchronous replication and advanced network configuration for quick data transfer to distant locations.
- [File share replication](#) in IBM Virtual Private Cloud (VPC) that creates replicas of your file shares in another zone in the same geography. With the File Share Replication feature, you can keep a read-only copy of your file share in a different zone. If you have another VPC in the target region, you can also create a replica in another region in the same location.

Backup and restore

Perform regular backups of critical data and systems and make sure that they are stored in a secure and accessible location. Backups must be

aligned with disaster recovery obligations and tested regularly to ensure completeness and successful execution.

Failover and failback

Plan for an automated failover to a secondary site during a disaster. Set up procedures for restoring data to the primary site after the disaster is resolved.

An automated failover and failback procedure in DR plans offers the following benefits:

- Minimizes downtime
- Ensures efficiency
- Maintains consistency
- Scales to complex environments
- Optimizes resource allocation
- Facilitates testing
- Reduces costs
- Improves the overall resiliency

Implementing your Disaster Recovery strategy in IBM Cloud

Build your DR plan based on the infrastructure and services in the IBM Cloud. Consider the following key services.

IBM Virtual Private Cloud

Create a snapshot for a file share in VPC. A snapshot is an instant copy of your file share that is mapped to the lifecycle of the file share. For more information, see [Planning File Storage for VPC snapshots](#).

IBM Power Virtual Server

Deploy virtual servers in multiple regions to increase redundancy and availability. Use [Global Replication Services \(GRS\)](#) for asynchronous block storage replication.

IBM Cloud Object Storage

Use IBM Cloud Object Storage, a scalable and cost-effective solution, to store backups and replicated data. The IBM Cloud Object Storage provides features such as resiliency, durability, geographic redundancy, support for incremental backups, data separation, and staging.

Cobalt Iron - Secure Automated Backup

Create backups across multiple environments by using Cobalt Iron, which provides a secure, automated, and cost-effective solution. It includes centralized management of the backup policies, advanced compliance features, and disaster recovery support.

For more details about backup strategies in IBM Power Virtual Server, see [Secure automated backup with Compass for AIX and Linux](#).

Configuring networking and security

Create network and security measures to protect data from unauthorized access, theft, or corruption during transmission and storage. These measures are important in a disaster recovery scenario in which data might be transferred between the primary and secondary sites or stored in the cloud. Use encryption, access controls, and secure protocols to maintain data confidentiality, integrity, and availability. Verify that your DR plan includes an efficient network and security configuration. Consider the following key services:

Virtual Private Cloud (VPC)

Create isolated networks for a disaster recovery environment with IBM Cloud VPC. It provides logical isolation, custom networking policies, multi-region coverage, high-speed networking, and support for core services.

VPN and Direct Link

Use VPN or Direct Link to establish secure connections between your on-premises infrastructure and IBM Cloud.

Access Controls and Encryption

Implement strict access controls and encrypt data in transit and at rest.

Documenting and testing your Disaster Recovery plan

Document your disaster recovery plans and make them available to business units and operations. Test recovery plans regularly to verify whether they restore the necessary services and networks with minimal impact. Consider the following actions:

Defining roles and responsibilities

Define roles and responsibilities in a DR plan. A defined DR plan reduces confusion and improves response times as tasks are identified. In addition, a clearly defined DR plan provides the following benefits:

- Avoids duplication of effort and considers the complete recovery process
- Facilitates effective communication and coordination among team members
- Promotes accountability by ensuring that each role has an assigned owner responsible for execution

Staff training

Ensure that your IT staff is trained on the latest disaster recovery procedures and tools. Training ensures that all team members understand their roles during a disaster. This clarity is mandatory for a coordinated response and minimizes confusion when an incident occurs. Regular training helps staff familiarize with the DR procedures and reduce the chance of errors during execution. This familiarity significantly speeds up the recovery process, minimizes downtime, and prevents the adverse impact on business operations.

Arranging for disaster recovery drills

Conduct regular disaster recovery trainings to simulate disaster scenarios and validate your failover and fallback procedures. Include the following disaster recovery exercises in the DR plan to minimize downtime and contribute to an effective DR strategy:

- Test the plan.
- Train personnel
- Identify and resolve issues
- Verify compliance
- Document lessons learned

Performance testing

Demonstrate the effectiveness of the DR plan to assure the stakeholders that your organization can recover from disruptions and maintain business continuity. Test the DR environment performance regularly for the following reasons:

- Verify that the DR infrastructure manages the required workload and recovers in the defined Recovery Time Objective (RTO). It determines that critical applications and services are restored quickly and minimizes the downtime and its associated costs.
- Identify possible limitations in the DR environment, allowing for necessary adjustments and optimizations before a real disaster occurs. A proactive approach can prevent unexpected issues during an actual recovery.
- Provide observability about the actual recovery time and data loss. In-depth observability improves the RPO and aligns the DR environment with your organization's risk tolerance.

Compliance audits

Review your DR plan regularly to be compliant with industry regulations and standards. Many industries have regulatory requirements for disaster recovery planning and staff training.

Continuous monitoring and improvement of the DR plan

Update the disaster recovery plan regularly based on lessons that are learned from incidents, tests, identified risks, and changes in recovery objectives and priorities. The updates must reflect changes in business operations, infrastructure, and technology.

Monitoring tools

Use IBM Cloud monitoring tools to track the health and performance of your DR environment. Monitoring tools provide observability to the DR infrastructure to quickly identify and respond to issues. The tools also help to identify possible obstructions or limitations in the DR environment to make adjustments and optimizations before an actual disaster.

SAP HANA database design considerations

It is important to consider the design of your SAP HANA configuration and deployment to ensure the SAP Business Applications use the full capabilities available with SAP HANA database server.

There are many decisions for SAP HANA design, which are taken to support the business requirements for the SAP Business Application. These design decisions for SAP HANA influence your infrastructure decisions. In the table, some of the sample decisions for these SAP HANA design considerations in the high-level overview are explained in detail.

High-level overview breakdown of SAP HANA design considerations and example decisions:

Design item	Example decision
Sizing Type	Standard sizing
Deployment Method	Appliance deployment
Deployment Type	MDC
System Type	Distributed, scale-out
Processing Type	OLAP, scale-out
Storage Type	Network File Storage (NFS)
Storage Flesytem	NFS mount points
High Availability fencing mechanism	STONITH
High Availability replication mode	SAP HANA System Replication, Full Synchronous replication within same Availability Zone or Data center
Disaster Recovery fencing mechanism	STONITH
Disaster Recovery replication mode	SAP HANA System Replication, Asynchronous replication to different Region
Backups	Backint native, daily complete backup + incremental backup every 30 minutes
SAP HANA Components	Live Cache Apps (LCAPPS), Extended Application Services Advanced (XSA - Cloud Foundry)

High-level overview breakdown of SAP HANA design considerations and example decisions

SAP HANA performance indicators and sizing

You have various performance indicators which guide the design decisions for sizing and planning an SAP HANA deployment onto Cloud IaaS. Each of these performance indicators defined with consideration to meeting the business requirements, determine whether the infrastructure is suitable. These considerations include compute capacity, storage capacity and latency, network throughput and latency in addition to the design decisions for SAP HANA database server.

Examples of these performance indicators for SAP HANA include:

Indicator	Description
Memory	<ul style="list-style-type: none">Leading factors for SAP Sizing (and cost of landscape + licenses)Determined by data footprint (business and metadata in the column and row store) after compression and by extra SAP HANA components used (such as cache store)

CPU	<ul style="list-style-type: none"> Compared to SAP AnyDB options, more CPU power is required to fully benefit from the parallel processing capabilities of SAP HANA for optimal response times. The large parallelization in analytical scenarios influence on Response Times. Therefore, CPU requirement is more important for analytical scenarios. Mixed transactional and analytic workloads are supported by SAP HANA but compete for shared resources.
------------	---

Disk capacity size	<ul style="list-style-type: none"> Disk capacity that is required for data persistence for logging and cache data
Disk throughput (I/O)	<ul style="list-style-type: none"> Disk capacity size depends on the type of database store usage (such as row and column) Sufficient I/O performance is required to enable processes to run with acceptable data throughput and storage system latency (that is, read/write from or to the disk)

Network Load	<ul style="list-style-type: none"> Network throughput bandwidth in gigabits per second (Gbps): <i>Amount of data transferred between SAP Application Servers and Database Servers</i> <i>Amount of data transferred between SAP Application and End User</i> Network latency roundtrip in milliseconds (ms): <i>Time between SAP Application Servers and Database Servers</i> <i>Time between hosts and any network-attached storage</i> <i>Time between SAP Application and End User</i>
---------------------	--

Example performance indicators for SAP HANA

SAP HANA Sizing Type and Deployment Method

Sizing type refers to the exercise of sizing SAP HANA, using either pre-defined or custom configurations.

Whereas the deployment method (sometimes referred as delivery model) refers to running IaaS certified for SAP HANA, which is either pre-defined or custom configurations.

Here is the summary of the Appliance and TDI deployment methods:

Appliance	TDI
Application	Application
Database	Custom Database sizing (including CPU:DRAM ratios)
Linux Operating System	Select from defined range of supported Linux® Operating System versions
<i>Virtualization (optional)</i>	<i>Virtualization (optional)</i>
Server	Server
Storage	Custom Storage

Appliance vs. TDI deployment methods

The following sub-sections describe the appliance deployment method for Standard Sizing type, and the TDI deployment method for Expert Sizing. Detailed documentation regarding the methods and types are shown in SAP documentation:

- [SAP HANA Administration Guide for SAP HANA Platform](#)
- [SAP HANA Server Installation and Update Guide](#)
- [SAP About Benchmarks - Sizing Types - Expert Sizing](#)
- [Expert Sizing & Methods of Sizing Validation](#)
- [Sizing Methods and Tools](#)

Appliance deployment method for Standard sizing type

Standard sizing type

This term refers to a sizing exercise where pre-defined configuration sizes are defined based on hardware testing and t-shirt sizing for meeting specific benchmarks to arrive at a sizing result for the hardware requirements of an SAP application (such as network, CPU, Memory, Storage).

Appliance deployment method

Supported hardware for SAP HANA depends on the deployment method. The appliance deployment method uses pre-defined validated SAP-optimized hardware by SAP-certified hardware partners that are running a specific operating system. These hardware options are offered in various configuration sizes.

Partners (such as Cloud Service Providers) offer appliances with multiple layers of redundant hardware, software and network components, which do not interrupt SAP HANA operations and defend against system outage. These components include:

- Redundant power supplies and fans and uninterrupted power supply (UPS)
- Enterprise grade error-correcting memories
- Fully redundant network switches and routers
- Disk storage systems that use batteries to guarantee writing even in the presence of power failure.
- Disk storage systems that use striping and mirroring for redundancy and recovery from disk failures.

In collaboration with SAP, a Cloud Service Provider defines the correct sizing when designing SAP-certified IaaS for SAP HANA with the appliance deployment method:

- Ensures maximum performance with the hardware capable of meeting specified workloads; providing dedicated memory for SAP HANA after the resident memory of OS and other programs is accounted for and with swapping to disk disabled.
- To maximize performance and throughput, SAP recommends that you scale up as far as possible (acquire the configuration with the highest processor and memory specification for the application workload) before scaling out (for deployments with greater data volume requirements).
- You can copy a database to machines from different SAP HANA appliance vendors with different hardware configurations, if both the source and target machines are compliant with the SAP HANA appliance specifications.

TDI deployment method for Expert sizing

Expert sizing type

Expert sizing type refers to a sizing exercise where customer-specific data is analyzed and used to put more detail on the sizing result for the hardware requirements of an SAP application (such as network, CPU, Memory, Storage).

According to SAP, expert sizing typically includes "exploring some business processes in more detail, both on functional and technical level" (quotation source: [Sizing Types - Expert Sizing](#)).

Therefore, with expert sizing, there are no standardized tools used to conduct the sizing and it will often require significant effort and SAP expertise. Projects that use expert sizing often use an external consulting and system implementation business partner to assist the internal SAP team.

For expert sizing, the following steps are likely to be performed (source: [Sizing Types - Expert Sizing](#)):

- Identify the most important queries/apps/scenarios
- Identify, how they are used, for example, filter criteria, authorizations.
- Run these queries/apps/scenarios on representative test data (quality of test data and quantity of test data). Ideally, on a recent copy of the production data
- Measure resource consumption (CPU/memory) and response times
- Perform a forecast calculation based on the expected usage of the queries/apps/scenarios

TDI deployment method

Supported hardware for SAP HANA depends on the deployment method. The TDI deployment method uses **custom-defined hardware** by SAP-certified hardware partners that use flexible OS or SAP HANA versions; these can be configured to any size (under the maximum configuration tested by SAP).

Partners (such as Cloud Service Providers) offer TDI with various configuration options and redundancy options. These options depend on whether you select scale-up or scale-out sizing, and must be installed by an appointed SAP HANA certified administrator. These *may* include:

- Redundant power supplies and fans and uninterrupted power supply (UPS)
- Enterprise grade error-correcting memories
- Fully redundant network switches and routers
- Disk storage systems use batteries to guarantee writing even in the presence of power failure
- Disk storage systems that use striping and mirroring for redundancy and recovery from disk failures

SAP and a cloud service provider agree to support the customer for a selected scale-up or scale-out sizing by using SAP-certified IaaS for SAP HANA with the TDI deployment method:

- This provides different system design options regarding scale-up and scale-out variations; the SAP HANA database must then be validated before use in Production systems that use the SAP HANA Hardware and Cloud Measurement Tool (HCMT) for TDI testing when requested by the SAP Support organization.
- To maximize performance and throughput, SAP recommends that you scale up as far as possible (acquire the configuration with the highest processor and memory specification for the application workload) before scaling out (for deployments with greater data volume requirements).

SAP HANA Deployment Types

SAP HANA can be deployed in various layouts, with various configurations of abstraction and logical separation of database schemas. Different deployment types are designed for different use cases, and SAP defines those which are approved (with/without restrictions) for production SAP Systems and those which are not approved. See detailed information here on [SAP HANA Deployment Types - SAP HANA Server Installation and Update Guide](#) and a summary of this information:

- Approved for production
 - Dedicated also known as, single application on one SAP HANA System (SCOS)
 - Multitenant Database Containers (MDC)
- Approved for production (with restrictions)
 - Virtualized Single Tenant - restrictions to the hypervisor; see [SAP Note 1788665 - SAP HANA Support for virtualized / partitioned \(multi-tenant\) environments](#)
 - Multiple applications on one SAP HANA System (MCOD) - supported only for approved applications; see [SAP Note 1661202 - Support multiple applications one SAP HANA database / tenant DB](#)
 - Multiple SAP HANA Systems on one host (MCOS)



Note: Multi-SID hosted with the same physical host, requires significant attention to detailed tasks related to system administration and performance management. For more information, see [SAP Note 1681092 - Multiple SAP HANA systems \(SIDs\) on the same underlying servers](#)

SAP HANA System Type

System Types are listed by SAP on [SAP HANA System Types](#) as:

- Single-host system - one SAP HANA instance on one host server
- Multi-node / distributed / scale-out cluster

A single-host system is the simplest system installation type. It is possible to run an SAP HANA system entirely on one host server and then scale the system up as needed.

A multi-node / distributed / scale-out cluster is a system installation across multiple host servers with a limit on the CPU/RAM for each host node and a limit on the number of host nodes that can be used. *Information on the maximum scale-out configurations, is listed in the [SAP Note 3557729 - Understanding the Maximum Number of Nodes in SAP HANA TDI Scale-Out System](#).*

SAP HANA scale-out cluster

Use of scale-out is primarily designed for SAP BW/4HANA or SAP BW on HANA. The [Scale-up and Scale-out for SAP BW/4HANA](#) considerations at the application-layer is covered separately. These consideration are in addition to database-layer considerations described in the following sections.



Note: It is important to note that if your SAP HANA database server nodes or SAP NetWeaver application server components are distributed across multiple availability zones and data centers, SAP will not support your SAP HANA scale-out cluster (also known as,

SAP HANA multi-node system).

Networking

SAP HANA multi-node requires certain networks be in place to function. Before you order other components of your system, these networks must be set up correctly and together with the database nodes. Separation of the network flows/traffic can improve performance (that is, keeping high storage traffic separate from the user traffic) when more network interfaces are attached to the server.

As a summary of the network separation, you need in SAP HANA scale-out cluster to have:

- A client-side network, which connects the SAP Advanced Business Application Programming (SAP ABAP) application servers, SAP HANA Studio clients, and any other network client to the multi-node system. The network throughput and availability options depend on the environment and usage scenario of your SAP HANA multi-node system. Consider the amount of data transferred from and to the SAP HANA database, and the availability key performance indicators (KPIs), required for your application.
- A storage network, which connects to the Network Storage (File/NFS or Block/iSCSI dependant on infrastructure selection). The network throughput and availability options depend on the environment and usage scenario of your SAP HANA multi-node system. Consider the throughput and latency required to provide 10,000 IOPS is available to each SAP HANA node.
- An internode network for SAP HANA internal communication that is set up equivalent to the storage network. The internode network is only used for communication between nodes and the data transfer that might be required between the nodes during operations.

Within each environment is a separate networking design. The classic infrastructure environment network is the forerunner and is the most robust option of many traditional and physical networking concepts. The VPC Infrastructure environment network is a software-defined network. The IBM Power environment network (as a complementary offering from IBM Power Systems) is designed with networking principles for enterprise-grade performance.

Given these environment networks are different, configuring extra NIC throughput changes for the different infrastructure options:

- **Bare Metal, on Classic Infrastructure network:** To maximize performance and redundancy, the physical network interfaces (NIC) are provided with 10 Gbps and then provisioned with bonding using Link Aggregation Control Protocol (LACP). The switches are configured automatically when ordering redundancy on the physical NIC. *Additional NIC cards might be added, depending on the physical machine specification and physical switch availability of ports.*
- **Intel Virtual Server, on VPC Infrastructure network:** To maximize performance and redundancy, up to 5 network interfaces (vNIC) on multiple Subnets can be added.
- **IBM Power Virtual Server, on IBM Power Infrastructure network:** To maximize performance redundancy, multiple network interfaces (vNIC) attached to different VLANs (and their respective Subnets) can be added.
- **VMware for SAP, on Classic Infrastructure network....**
 - **IBM Cloud for VMware Solutions, on Classic Infrastructure network:** redundant adapters for VMware are set up by the VMware vSphere Distributed Switch (VDS) using [VDS on NSX-T](#), in accordance with current VMware best practices for SDDC. While subject to change, redundancy is configured by setting every distributed switch with the [Route Based on Originating Virtual Port](#) load balancing algorithm. All port groups used by the algorithm should be configured to use teamings across 2 uplinks (Active: 0,1).
 - **IBM Cloud Bare Metal with VMware vSphere (manual configuration)**, on Classic Infrastructure network: adapters are suggested to utilise the best practices, however the vSwitch could use LACP bonding of the physical NIC adapters

Scale-out storage

Data is distributed across the multiple SAP HANA nodes, which are hosting the single database.

Follow the guidelines in [Sizing SAP HANA - SAP HANA Master Guide](#) to determine the required total storage capacity size for your target SAP HANA system.

The SAP HANA shared volume, and each of the data and log volumes, must be accessible to all nodes (which may be easier to allow network storage access to all nodes within the Subnet used for storage connectivity). There are specific performance criteria that must be met by the attached Network File System (NFS) volumes:

- `/hana/data/` and `/hana/log` volumes, individual volumes are required for each node with a minimum of 10 IOPS/GB
- `/hana/shared` volume, required to be shared across all nodes with a minimum of 10 IOPS/GB and recommended to increment further to 12 IOPS/GB

For Classic Infrastructure:

- Read [SAP HANA on NetApp FAS Systems with NFS](#) to assist configuration of your SAP HANA multi-node system.
- Use the following Network File System (NFS) mount options in `/etc/fstab` for each volume to mount -
`rw,bg,hard,timeo=600,intr,noatime,vers=4,minorversion=1,lock,rsize=1048576,wsize=1048576`.

After you mount all of your volumes to all the nodes, your multi-node servers are configured and ready to install the SAP HANA multi-node database. Follow the steps in the [SAP HANA Server Installation and Update Guide](#)) to install an SAP HANA database of your required version.

SAP HANA performance

After an SAP HANA database server is operational, it is important to inspect the performance to ensure it will meet your business application requirements. This is particularly important for any deployments using the TDI deployment method.

SAP HANA performance validation

The [SAP HANA Hardware and Cloud Measurement Tools \(HCMT\)](#) replaces the previous *SAP HANA HW Configuration Check Tool (HW CCT)*. The HCMT binary executable is run before an SAP HANA installation (commonly), and performs a series of automated tests which analyses the system performance.

The output of the HCMT execution, is a result archive file - `hcmtresult-[timestamp].zip`.

This HCMT result archive file is then uploaded to the [SAP HANA Hardware and Cloud Measurement Analysis \(HCMA\)](#) for detailed analysis.

For information about downloading, installing, and configuring the HCMT tool, see [SAP Note 2493172 - SAP HANA Hardware and Cloud Measurement Tools](#).

SAP HANA overheads impact on available memory

Every SAP HANA database server reserves a small allocation of memory for the operating system and other services required to operate.

SAP provide a rule of thumb for these overheads:

- Reserved for OS = 10% of the first 64 GB + 3% of all remaining memory
- Reserved for SAP HANA services and caches = 50 GB

The example demonstrates the net capacity for SAP HANA when using 4TB Memory (DRAM) after the memory reservation overheads have been taken into consideration:

Physical Memory	4096 GB DRAM
Reserved for OS	127 GB
Available for SAP HANA	3969 GB
Reserved for SAP HANA services and caches	50 GB
Net capacity available for SAP HANA data + temporary disk space	3919 GB

Example of SAP HANA net capacity

This is shown in more detail on [SAP Note 2296290 - New Sizing Report for SAP BW/4HANA](#) under attachment SAPBW4HANA_Sizing_V2.6.4.pdf

SAP HANA High Availability and Disaster Recovery (HA/DR)

The first requirement for SAP HANA High Availability (HA) and Disaster Recovery (DR), is to use the correct Operating System (OS) add-ons for SAP High Availability. Be sure to discuss OS for SAP HA details with IBM Cloud Support before your deployment.

The OS supported and deployed by IBM Cloud for running SAP HANA with HA/DR are:

- Red Hat Enterprise Linux (RHEL)
- SUSE Enterprise Linux Server (SLES)

The IBM Cloud environment does not support any preconfigured high availability (HA) scenarios. However, it does let you implement HA solutions for SAP HANA through Red Hat Enterprise Linux HA extensions, in a similar manner to existing deployments using Traditional On-Premises data centers.

SAP HANA System Replication (HSR) is configured with an automated fail-over from one server to a replica, using various **replication modes** designed by SAP to fit:

- Different SAP Business Applications
- Different business risk acceptance of unplanned downtime
- Different infrastructure resiliency cost profiles

Refer to SAP documentation on SAP HANA System Replication (HSR) and OS vendor documentation on SAP HANA HA/DR; or consult SAP for recommendations on your landscape design for further clarity.

For more information on system replication, and network throughput and latency, see

- [How To Perform System Replication for SAP HANA - Version 5.4 January 2018](#)
- [Network Configuration for SAP HANA System Replication](#)
- [SAP Help - SAP HANA System Replication Guide](#)
- [Troubleshoot System Replication - SAP HANA Troubleshooting and Performance Analysis Guide](#)
- [SAP Note 1999880 - FAQ: SAP HANA System Replication](#)
- [SAP Note 2057595 - FAQ: SAP HANA High Availability](#)

For more information on setting up the HA cluster extensions of the OS, view the Linux vendor documentation.

SUSE Linux Enterprise Server for SAP:

- [SAP HANA System Replication Scale-Up - Performance Optimized Scenario](#)
- [SUSE Linux Enterprise High Availability Extension](#)

Red Hat Enterprise Linux for SAP:

- [Supported HA Scenarios for SAP HANA, SAP S/4HANA, and SAP NetWeaver](#)
- [Automated SAP HANA System Replication in Scale-Up in pacemaker cluster](#)

SAP NetWeaver design considerations

It is important to carefully consider the configuration, deployment, and design of your SAP solution stack.

SAP NetWeaver-based systems can be deployed in two ways:

- A central system, which is a single-host installation (two-tier)
- A distributed system, which is a multi-host installation (three-tier); this option might be chosen for system scalability

You can choose to distribute the workload across multiple servers or keep the workload on one server for simplicity, depending on your business requirements.

SAP system architecture models

The architecture of SAP NetWeaver-based systems is based on a multitier client/server design that consists of three main layers: the presentation layer (user front-end), the application layer, and the database layer.

Two commonly architecture models are used for deploying SAP NetWeaver-based solutions.

- A two-tier architecture model refers to a separate presentation layer and an application and database layer. Both the application and the database are installed together on a single host.
- In the three-tier architecture model, the presentation, application, and database layers are installed on separate hosts. The three-tier architecture configuration is highly scalable. Multiple servers can be installed for the application layer, and in an SAP HANA scale-out implementation even for the database layer.

SAP NetWeaver Application Server ABAP systems consist of the following components, which can run on a single host or distributed across multiple hosts.

- ABAP Central Services (ASCS), which includes an ABAP message server and a Standalone Enqueue Server
- Primary Application Server (PAS), which includes an ABAP dispatcher process and ABAP work processes
- Additional Application Servers (AAS)



Note: Since SAP NetWeaver release 7.5, the term PAS refers to the SAP application server that is installed first for the system. The architecture of the PAS and the other application servers is the same (see [SAP Note 2360614 - Primary Application Server \(PAS\) Instance Directory renamed as of SAP Netweaver 7.50](#)). In previous releases, the ASCS services were integrated into the PAS instance and such instances were commonly referred to as the Central Instance.

To create a high availability environment for SAP NetWeaver-based systems, distribute each of these components on separate hosts.

- Database server
- ABAP Central Services (ASCS)
- Enqueue Replication Server (ERS), which provides extra protection for the ASCS lock table
- PAS
- AAS

Configuring high availability for SAP NetWeaver

IBM Cloud provides automation for implementing selected high availability scenarios for SAP NetWeaver-based or S/4HANA deployments in IBM Cloud VPC.

For details on available scenarios with automated deployment in IBM Cloud VPC, see the following information.

- [SAP S/4HANA HA deployment on IBM Cloud VPC](#).

Other high availability scenarios that aren't covered by the existing automation can be implemented based on the high availability solution available for your chosen operating system.

For a high availability configuration, you need to add extra hardware and software components to your landscape.

If you require extra software licenses, access to different software repositories, or both, contact [IBM Cloud support](#) for assistance.

This configuration information applies to both the high availability software for SAP NetWeaver and the high availability software for your chosen relational database management system (RDBMS). The setup procedures are no different from the setup procedures in an on-premises environment and require similar hardware and software configuration steps.

Overview of SAP NetWeaver high availability configurations

A number of documents provide in-depth help on planning and installing an HA environment for SAP services. The documents include information on failover, replication, scale-out, and disaster recovery (DR). References to specific documents are provided where appropriate.

All operating systems and distributions that are supported by IBM Cloud for an SAP solution deployment (Windows Server, Red Hat Enterprise Linux, and SUSE Linux Enterprise Server) come with high availability software and specific extensions. The supported operating systems and distributions are described in these documents:

- [New Failover Clustering Improvements in Windows Server 2012 and Its Benefits for SAP NetWeaver High Availability](#) provides a description based on Microsoft Windows Server Failover Clustering (WFSC) for SAP NetWeaver implementations.
- The following documents provide guidance on deploying SAP NetWeaver in a high availability Linux environment.
 - [Supported High Availability Solutions by SLES for SAP Applications](#)
 - [Red Hat HA Solutions for SAP HANA, S/4HANA and NetWeaver based SAP Applications](#)
 - [Building High Availability for SAP NetWeaver and SAP HANA on Linux](#) is an SAP best practice document and provides a detailed technical description with a strong focus on SAP HANA.

For more high availability products certified by SAP partners under the SAP Application Server High Availability Interface Certification Program, see [SAP High Availability - Certified HA-Interface Partners](#).

For databases other than SAP HANA, refer to the documentation for your database for more information on high availability and disaster recovery configurations.

Shared access to one of these storage elements is required to support the failover of high availability systems:

- Network File System (NFS); *on-premises deployments can also use Common Internet File System (CIFS) storage*
- iSCSI-based storage

Local storage that is combined with a replication method is required to support DR system failover.

As with on-premises installations, consider the performance and latency requirements of the database product as part of your deployment planning.

Configuring high availability in Classic Infrastructure

The IBM Cloud environment does not offer pre-configured high availability deployments for SAP solutions. However, you can configure high availability scenarios based on the high availability solution that is available for your chosen operating system.

See [High availability and fencing considerations](#) and [High availability and network considerations](#) for lists of things that you need to consider for your deployment. Apart from these considerations, configuring high availability for SAP NetWeaver and its database doesn't differ from other on-premises installations.

High availability and fencing considerations

To protect the integrity of shared resources in a high availability cluster, a fencing mechanism is required to isolate failing cluster nodes. Intel processor-based clusters often use an Intelligent Platform Management Interface (IPMI) feature for fencing. Due to the enterprise security implementation in the IBM Cloud Classic Infrastructure environment, network-based access to remote management devices by using IPMI isn't available.

In the absence of an IPMI-enabled device, fencing mechanisms based on shared storage devices are used. In an IBM Cloud environment, shared storage devices are typically implemented by providing an iSCSI LUN to your servers.

For example, a File Share Witness (FSW) can be used on a Microsoft Windows cluster. See [Managing quorum and witnesses](#) for information on configuring and managing quorum in Windows Server based deployments.

Linux-based clusters can use an SBD (Storage-Based Death or STONIT Block Device) based implementation for fencing. For more information on cluster fencing and SBD, see [Pacemaker Explained - Fencing](#) and [Using SBD With Pacemaker](#).

IBM Cloud block storage has built-in high availability features. A single shared iSCSI LUN does not introduce a single point of failure (SPOF) as the network layout is redundant. However, a specific cluster solution might require more than one shared device.

High availability and network considerations

An IBM Cloud Classic Infrastructure environment-based installation comes with one of the following network configurations:

- Private network

- Public network
- Public and private networks
- Two private networks (on special request, depending on server type and physical hardware components configuration)

As with on-premises installations, extra network adapters can be ordered depending on the physical restrictions of the hardware. The restriction is the same as for on-premises installations, which is the number of NIC cards that can fit into the server.

When deploying server hardware, avoid single points of failure in your network topology by ordering redundant network adapters.

Redundant adapters for bare metal servers are set up in a failover configuration by using Link Aggregation Control Protocol (LACP). Bonding interfaces are used for Linux and teaming adapters are used for Microsoft Windows. These setups provide a logical interface for redundancy and increased bandwidth.

When you deploy IBM Cloud for VMware Solutions, redundant adapters for VMware are set up using an NSX-T distributed switch. This is in line with current VMware best practices for the *Software-Defined Data Center* (see [VMware NSX-T design](#)). Although subject to change, redundancy is configured by setting each *Distributed Switch* to use the [Route Based on Originating Virtual Port](#) load balancing algorithm. All included port groups use teaming over 2 uplinks (active: 0,1).

If you are deploying VMware vSphere on IBM Bare Metal in a manual installation that uses vSwitch, you can use LACP bonding of the physical NIC adapters. This configuration choice depends on the need for increased throughput (for example bonding) versus redundant stability (for example load balancing with teaming).

The NIC adapters are connected to redundant switches, so no additional single point of failures is introduced. The redundant infrastructure can be used by the ordered VLANs.

For some network requirements, such as disaster recovery replication scenarios, you need to consider the location of the connected devices and any new network requirements specific to the scenario. Sometimes, the IBM Cloud Classic Infrastructure's file or block storage with snapshot backups might fulfill your requirements. Check with IBM Cloud Support to determine which solution is best for your business needs.

Configuring high availability in IBM Cloud VPC

Review the documentation on automated high availability deployment at [SAP S/4HANA HA deployment on IBM Cloud VPC](#).

For scenarios that are not covered by automation, or where the available automation doesn't fit, you can always implement a high availability solution manually. In this case, the same information applies as in [Configuring high availability in Classic Infrastructure](#).

Configuring high availability for IBM Power Virtual Server

To implement high availability scenarios for SAP applications on IBM Power Virtual Server, see [Implementing high availability for SAP applications on IBM Power Virtual Server](#).

SAP Business Applications extra design considerations

SAP S/4HANA

SAP S/4HANA is the leading Enterprise Resource Planning (ERP) software that is designed for the largest enterprises, in any country worldwide within any industry, with extensive business processes and customization.

ERP software integrates all business management and operations into one cohesive application to coordinate business execution, such as accounting and financing, purchasing and inventory, sales and customer relationships. An ERP can be considered a hub of all business operations. Various applications and all parts of the business can be connected into ERP, from the factory to the headquarters. The ERP software as a whole can have many add-on components (functional and industry) that provide different business functions for different lines of businesses and industries.

SAP S/4HANA is a major release of ERP software from SAP designed to run with the SAP HANA database exclusively. Previous major releases of ERP from SAP, known as SAP ECC and SAP R/3, could use various relational database vendors.

SAP S/4HANA acts as the "Digital Core" for large enterprises with upgraded UX, business workflows, and technology upgrades, to enable as many extensions as possible using Cloud Native technologies.

For more information, see [SAP S/4HANA](#)

IBM Cloud® for SAP infrastructure options are certified to SAP NetWeaver application server and SAP HANA database server, which run the SAP S/4HANA business application.

Preface: variants of SAP S/4HANA

The SAP S/4HANA business application has multiple variants, each with different functional and customization levels, which are available as different operational models. The model that you select affects the SAP S/4HANA deployment.

Primarily the software operational models are grouped into two categories:

- **SAP S/4HANA "AnyPremise"** (*formerly "On-Premise" Edition*), which is the same software installation and hosting by the business or a business's subcontractors. This option provides the business **full** control over the functions and deployment of the software, but with **more** deployment effort and management overheads to keep the SAP Systems running.
- **SAP S/4HANA Cloud SaaS**, which is the same software but installed and hosted by SAP along with SAP Partner subcontractors. This model provides the business with **less** control over the software functions and deployment, but with **less** deployment effort and management overheads to keep the SAP Systems running.

Within each of the software operational models, multiple software deployment options are available:

- SAP S/4HANA "AnyPremise" Edition (*formerly "On-Premise" Edition*
 - Deployment to existing Traditional On-Premises data center
 - Deployment to Cloud IaaS
- SAP S/4HANA Cloud SaaS
 - SAP S/4HANA Public Cloud **Extended (EX)** Edition, *SaaS provided by SAP along with SAP Partner subcontractors*
 - SAP S/4HANA Public Cloud **Essentials (ES)** Edition, *SaaS provided by SAP along with SAP Partner subcontractors*
 - SAP S/4HANA Private Cloud, *SaaS extension of SAP HANA Enterprise Cloud (HEC) provided by SAP along with SAP Partner subcontractors*

More information on the variants of SAP S/4HANA software is available from SAP. A concise explanation on the variants of SAP S/4HANA is available from SAP America, see [SAP Community Blogs - Product Information - SAP S/4HANA Cloud Deployment Options \(June 17, 2019\)](#).



Note: Regarding SAP S/4HANA, the IBM Cloud® for SAP portfolio documentation refers to SAP HANA and SAP NetWeaver installations as using SAP-certified Cloud Infrastructure-as-a-Service options for running SAP S/4HANA "AnyPremise" deployment to Cloud IaaS. All further descriptions in the following sections refer to SAP S/4HANA "AnyPremise".

Additional decisions for implementation and maintenance

In addition to selecting a variant of SAP S/4HANA (the operational model and the deployment model), many SAP-run customers need to make several other decisions, for example:

SAP S/4HANA adoption strategy

- New SAP customer first-time implementation
- ERP Migration (Brownfield)
 - System Conversion (also known as Brownfield)
 - Selective Data Transition (that uses Shell Conversion or Mix&Match)
- ERP Re-Implementation (Greenfield)

SAP S/4HANA delivery model for the project implementation, from the list of SAP Partners

- A Global Systems Integrator (GSI) for SAP
- A Managed Services Provider (MSP) for SAP

SAP S/4HANA maintenance model for ongoing support, from the list of SAP Partners

- An Application Management Services provider (AMS) for SAP
- A Managed Services Provider (MSP) for SAP

A list of all SAP Partners is maintained on the [SAP Partner Finder tool](#). The list has more information about SAP Partners, including:

- Partnership category (for example, Consulting & Implementation Services)
- Partnership level (for example, Platinum, Gold, Silver)

Awards for these SAP Partners are shown on the [SAP Partners information page](#).

These choices particularly affect how your SAP S/4HANA "AnyPremise" Edition on Cloud IaaS is deployed, operated, and maintained. For example, a GSI has exceeding depth of experience in implementation, functional configuration and development - with the flexibility to create a bespoke solution for the business requirements. However, the GSI has less experience in maintenance. Conversely, an MSP has more restrictions on the implementation to ensure more successful maintenance.

Given the division of skills in traditional on-premises data center implementations of SAP workloads during previous decades, there were multiple tasks handled by the Data Center Provider. It is suggested to consider the skills of your SAP Partners in the following areas because the Cloud Service Provider is not responsible for those activities previously fulfilled by the Data Center Provider:

- Cloud Account and IAM setup
- Networking setup (including security)
- Storage setup
- Infrastructure Sizing for SAP
- OS Configuration (including security)

Further information on [Moving SAP Workloads](#) is described in the FAQ.

Compute considerations

Depending on the business requirements and risk acceptance, the primary decision for any Cloud IaaS running SAP workloads which Cloud Tenancy model to use:

- Single-Tenant infrastructure, **dedicated** compute resources that are accessed with a private logical network within the Cloud provider network backbone that uses:
 - Bare Metal
 - Virtual Servers on Dedicated Hosts
 - VMware SDDC
- Multi-Tenant infrastructure, **shared** compute resources that are accessed with a private logical network within the Cloud provider network backbone that uses Virtual Servers

After you decide on the Cloud Tenancy model that meets your business and IT risk needs, the focus is then on sizing and throughput requirements:

- Output of your [SAP Sizing activities](#)
- Benchmark metric "SAPS", which demonstrates the total transactional throughput of the Infrastructure

More information that compares different Infrastructure types is in [Comparing the different SAP-certified IaaS offerings](#), with more detail under [Infrastructure certified for SAP](#). All SAPS benchmarks are listed for each Profile under each Infrastructure type that is offered in the IBM Cloud® for SAP portfolio.

SAP HANA considerations

The SAP S/4HANA business application is affected by multiple [SAP HANA Database Server design considerations](#).

SAP S/4HANA is considered a "Mixed Workload", as the business application primarily does Transactional processing (OLTP), but SAP S/4HANA also does Analytical processing (OLAP) through SAP S/4HANA **Embedded Analytics**.

During SAP Sizing, decision making, and Infrastructure selection, SAP S/4HANA is often considered as OLTP only. This representation is not a fully accurate view of the business application, but serves as the closest representation for use with SAP Benchmarks information. However, for the SAP HANA infrastructure, the sizing is most often determined by the Memory (DRAM) capacity size.

Scale-up and Scale-out

It is important to note that if you are using SAP HANA in scale-out deployment the transaction throughput of the system might be affected.

[SAP Note 2428711 - S/4HANA Scale-Out Sizing](#) limits an SAP HANA scale-out to up to four nodes in total. This limit applies to S/4HANA deployments on IBM Cloud to prevent our customers from experiencing transactional throughput issues. IBM Cloud® for SAP does not actively publish those specifications.

Instead, we advise customers who have exceptionally large SAP HANA requirements for running an SAP S/4HANA production instance (particularly those requirements over 14-18TB of DRAM) to discuss their requirements with IBM-SAP. Discussions with IBM and SAP worldwide technical experts can provide more accurate advice on the business problem and identify alternative paths forward.

Alternates can include, the creation of a Hybrid Cloud model with the use of the available high-performance scale-up options in traditional datacenter deployments.

An example of Hybrid Cloud used with SAP S/4HANA when exceeding 14-18TB of DRAM, would be the use of IBM Power9 hardware provided by IBM Power Systems, deployed into Traditional On-Premises datacenters. The maximum **IBM Power9 hardware can support 28TB of DRAM for SAP HANA 2.0 scale-up**. These complementary offerings are already successfully running many customers SAP workloads at these largest memory footprints, through a close partnership and engineering discussions with SAP, therefore may suit the business needs for such exceptional scale-up requirements. For more information regarding SAP HANA on IBM Power Systems, see [SAP Note 2188482 - SAP HANA on IBM Power Systems: Allowed Hardware](#).

SAP NetWeaver considerations

The SAP S/4HANA business application is impacted by multiple [SAP NetWeaver Application Server design considerations](#).

Versioning and upgrades

SAP S/4HANA no longer has a stand-alone shipment of SAP NetWeaver Application Server (ABAP) which can be used.

The **SAP S/4HANA Server** component is required to install SAP S/4HANA. This component is briefly titled as SAP ABAP Platform and historically called SAP NetWeaver AS ABAP.

For SAP S/4HANA "AnyPremise" 20xx (for example, 2020), the **SAP S/4HANA Server contains**:

- SAP ABAP Platform 20xx and SAP Kernel 7.7x (*the version number of these components are only shown after the installation is completed*)
- ADT for Eclipse
- Other additional technology components to run SAP S/4HANA



Important: For this reason, when you are running older SAP S/4HANA versions (such as 1511, 1610, 1709) it is not possible to upgrade SAP NetWeaver AS ABAP 7.5+ in isolation. All upgrades must be handled by using SAP Maintenance Planner for the entire stack on a specified OS (for example, Red Hat Linux®, SUSE Linux, IBM AIX, Windows Server).

SAP BW/4HANA

SAP BW/4HANA is the leading enterprise data warehouse (EDW) software, which is designed for analyzing mass amounts of structured and unstructured data from multiple sources. EDW software deciphers business data into tangible and actionable insights that are used for reporting business performance against metrics and identifying opportunities or gaps in existing business practices.

SAP BW/4HANA is a major release of EDW software from SAP designed to use the analytical capabilities of the SAP HANA database exclusively. Previous major releases of EDW from SAP were known as SAP BW, which might use various relational database vendors. SAP BW/4HANA acts as the insights engine for large enterprises with upgraded UX, data integration, and technologies upgrades to enable real-time decision making and digital business processes.

For more information, see [SAP BW/4HANA](#).

IBM Cloud® for SAP infrastructure options are certified to SAP NetWeaver application server and SAP HANA database server, which run the SAP BW/4HANA business application.

Preface: variants of SAP BW/4HANA and other analytics solutions from SAP

For analytics, there are multiple interlocking solutions from SAP and variants for each solution. The primary SAP analytics solutions are:

- SAP BW/4HANA, the EDW software using SAP HANA Platform with runtime database license
- SAP Data Warehouse Cloud (SaaS), the EDW software available as-a-Service using SAP HANA Cloud Services
- SAP HANA Platform Enterprise Edition, the database server and analytical components when leveraging the full-use license and can be used to construct custom/native EDW.
- *The analytical SAP HANA components include Self Service Analytics Library (SAL), Smart Data Access (SDA), Smart Data Integration (SDI), Smart Data Streaming (SDS), Remote Data Sync (RDS), and in addition, for Hadoop integration, the use of SAP HANA Spark Controller optionally with SAP Vora.*

There are additional SAP analytics solutions, each with different software deployment options, some of which are summarized below:

- SAP BW/4HANA
 - Deployment to existing traditional on-premises data center
 - Deployment to Cloud IaaS
- SAP HANA Platform Enterprise Edition
 - Deployment to existing traditional on-premises data center
 - Deployment to Cloud IaaS
 - SAP HANA Enterprise Cloud (HEC), *Managed DBaaS*
- SAP HANA Cloud Services
 - SAP HANA Cloud, *DBaaS (released in 2020 to replace SAP HANA Service, which in 2018 replaced SAP HANA One)*
 - SAP Analytics Cloud, SaaS
 - SAP Data Warehouse Cloud, SaaS
- SAP Business Objects Business Intelligence Suite (BOBJ/BO-BI)
- SAP Data Intelligence 3.x, using Kubernetes (*released in 2019 to replace SAP Data Hub 2.x*)

More information on the variants of SAP analytics solutions is available from SAP:

- [SAP.com - Business Analytics Tools and Solutions](#)
- [SAP Community Blogs - Technical Articles - SAP \(HANA\) Cheat Sheet](#)



Note: Regarding SAP BW/4HANA, the IBM Cloud® for SAP portfolio documentation refers to SAP HANA and SAP NetWeaver installations as using SAP-certified Cloud Infrastructure-as-a-Service options for running SAP BW/4HANA deployment to Cloud IaaS.

Additional decisions for implementation and maintenance

The project implementation and maintenance/support of SAP BW/4HANA selects from the list of SAP Partners:

- Project implementations
 - A Global Systems Integrator (GSI) for SAP
 - A Managed Services Provider (MSP) for SAP
- Maintenance/support
 - An Application Management Services provider (AMS) for SAP
 - A Managed Services Provider (MSP) for SAP

A list of all SAP Partners is maintained on the [SAP Partner Finder tool](#). The list has more information about SAP Partners, including:

- Partnership category (for example, Consulting & Implementation Services)
- Partnership level (for example, Platinum, Gold, Silver)

These choices particularly affect how your SAP BW/4HANA on Cloud IaaS is deployed, operated, and maintained. For example, a GSI has

exceeding depth of experience in implementation, functional configuration, and development - with the flexibility to create a bespoke solution for the business requirements. However, the GSI has less experience in maintenance. Conversely, an MSP has more restrictions on the implementation to ensure more successful maintenance.

Given the division of skills in traditional on-premises data center implementations of SAP workloads during previous decades, there were multiple tasks handled by the Data Center Provider. It is suggested to consider the skills of your SAP Partners in the following areas because the Cloud Service Provider is not responsible for those activities previously fulfilled by the Data Center Provider:

- Cloud account and IAM setup
- Networking setup (including security)
- Storage setup
- Infrastructure sizing for SAP
- OS configuration (including security)

Further information on [Moving SAP Workloads](#) is described in the FAQ.

Compute considerations

Depending on the business requirements and risk acceptance, the primary decision for any Cloud IaaS running SAP workloads is which Cloud Tenancy model to use:

- Single-tenant infrastructure, **dedicated** compute resources that are accessed with a private logical network within the cloud provider network backbone that uses:
 - Bare metal
 - Virtual servers on dedicated hosts
 - VMware SDDC
- Multi-tenant infrastructure, **shared** compute resources that are accessed with a private logical network within the cloud provider network backbone that uses virtual servers.

After you decide on the Cloud Tenancy model that meets your business and IT risk needs, the focus is then on sizing and throughput requirements:

- Output of your [SAP sizing activities](#)
- Benchmark metric "SAPS", which demonstrates the total transactional throughput of the infrastructure

More information that compares different infrastructure types is in [Comparing the different SAP-certified IaaS offerings](#) with more detail under [Infrastructure certified for SAP](#). All SAPS benchmarks are listed for each profile under each infrastructure type that is offered in the IBM Cloud® for SAP portfolio.

SAP HANA considerations

The SAP BW/4HANA business application is an analytical processing (OLAP) workload and is affected by multiple [SAP HANA Database Server design considerations](#).

During SAP sizing, decision making, and infrastructure selection for the SAP HANA infrastructure to support OLAP workloads, the sizing is most often determined by the memory (DRAM) capacity size.

Scale-up and Scale-out

SAP BW/4HANA is built to take advantage of the analytical capabilities of SAP HANA and is regularly used in scale-out scenarios to analyze huge volumes of data (including data beyond ERP transactional data, such as Hadoop data lakes).

It is important to understand SAP BW/4HANA certifications to ensure your infrastructure selection meets business requirements, particularly for business decisions on lead times of analytics and reporting or quantity of data to be analyzed.

All SAP-certified infrastructure on Cloud for OLAP (i.e. SAP BW/4HANA) is listed in [SAP HANA Directory - Certified IaaS Platforms - OLAP application type](#). For performance benchmarks of the SAP-certified infrastructure for SAP BW/4HANA, these are listed in the [SAP BW edition for SAP HANA benchmark directory \(BWH\)](#).

There are a few considerations to be mindful of when looking at the directories from SAP and comparing infrastructure performance for SAP BW/4HANA:

- The CSV Export file of the SAP BWH benchmark directory will not contain important configuration notes, such as "Segmentation" notes where the quoted memory is reduced (for example, 4,048 GB DRAM is only permitted with 3,904 GB DRAM). This often occurs when the

certified infrastructure is a virtual machine. This is also not shown on the main site; it is only viewable on the certification PDF of each certified infrastructure.

- The benchmark certification is for a specific number of scale-out nodes; however, this is multiplied by SAP for the IaaS certification so that the same tested infrastructure configuration might be approved for additional scale-out (reaching larger total memory footprint).
 - Benchmark certification example: **8 scale-out nodes which includes the 1 Parent + 7 Child nodes; using infrastructure with 6,144 GB DRAM for total memory of 49,152 GB**
 - IaaS certification based on the same benchmark certification example: **16 scale-out nodes which includes 15 Active nodes (1 Parent + 14 Child nodes) + 1 Standby node; using infrastructure with 6,144 GB DRAM for total memory of 92,160 GB**

The following table provides examples of how these benchmarks could be inferred to help the business perform sizing decisions for SAP BW/4HANA:

<i>Benchmark data point: (by sequence shown in benchmark reports)</i>	<i>Phase 1: Data load (seconds)</i>	<i>Phase 2: Query executions per hour</i>	<i>Phase 2: Records selected</i>	<i>Phase 3: Runtime of complex query phase (seconds)</i>
Measurement interpretation:	Lower is better	Higher is better	Higher is better	Lower is better
Benchmark impacting factors:	Impacted by quantity of initial records to load	Impacted by number of records selected in Phase 2		Impacted by number of records selected in Phase 2
Example comparison calculation for infrastructure selections (attempts to account for the impacting factors):	<i>Seconds to load 1 billion records might help comparisons of read from storage (for example, divide Phase 1 data load in seconds by initial records)</i>	<i>Total records parsed per hour during Query Execution might help comparisons of calculations performed by CPU (for example, multiply query executions per hour by records selected)</i>		<i>Total records parsed per minute during complex query might help comparisons of calculations performed by CPU (for example, divide records selected by runtime of complex query seconds, then multiply by 60)</i>

Examples of inferring benchmark results into sizing decisions

Additional SAP Notes regarding SAP BW/4HANA and sizing for scale-out:

- [SAP Note 2296290 - New Sizing Report for SAP BW/4HANA](#)
- [SAP Note 2347382 - SAP BW/4HANA – General Information \(Installation, SAP HANA, security corrections...\)](#)
- [SAP Note 2561976 - SAPBWNews SAP BW/4HANA 1.0 SP 08](#)
- [SAP Note 2908965 - SAPBWNews SAP BW/4HANA 2.0 SP 06](#)
- [SAP Note 2671297 - SAP BW on SAP HANA and SAP BW/4HANA in a SAP HANA, active/active read-enabled option environment](#)

SAP Commerce

SAP Commerce (formerly SAP Hybris Commerce) is part of the Customer Experience (CX) portfolio under the SAP C/4HANA suite.

Due to the design and business purpose and the nature of SAP Commerce, the installation, deployment, and additional development code is much more suited to a DevOps way of working. Project teams often use agile SDLC/PM methodologies (such as Scrum or SAFe). As an example of the flexibility, SAP Commerce runs across multiple different Operating Systems that are supported by SapMachine, a downstream OpenJDK release that is maintained and supported by SAP.

Therefore, deployments of SAP Commerce are available in different variants; we detail the following to assist understanding what IBM Cloud® for SAP can provide:

- **SAP Commerce "on-premises edition" variants:**
 - SAP Commerce "on-premises edition" with on-premises data center

- SAP Commerce "on-premises edition" on Cloud IaaS
- **SAP Commerce Cloud (PaaS solution) variants:**
 - SAP Commerce Cloud hosted on SAP Infrastructure (also known as CCv1 using VMs)
 - SAP Commerce Cloud in the Public Cloud (also known as CCv2 using Kubernetes)

Within the IBM Cloud® for SAP portfolio, infrastructure is supported for *SAP Commerce "on-premises edition" on Cloud IaaS*.

This solution involves an installation of the SAP Commerce software onto Cloud IaaS, according to SAP installation and best practice guidance:

- [Installation and Upgrading SAP Commerce](#)
- [SAP Commerce Architecture](#)

For a typical development environment of SAP Commerce, it is straightforward (compared to other SAP software) to shut down the instantiation/s and reduce costs outside of business hours through less Cloud resource consumption; however, depending on the implementation the time to start again can be significant. This decision is required by the project team, and might not be suitable if a worldwide development team is in-place.

More information is available on [SAP Commerce](#) help portal.



Note: IBM Power Virtual Servers are not available for SAP Commerce.

SAP Business One (B1)

SAP Business One is an enterprise resource planning (ERP) software that is especially designed for small-to-medium enterprises. It integrates business management - accounting and financing, purchasing and inventory, sales and customer relationships, and project management and operations - into one application.

The single application eliminates the need for multiple installations and interfaces across separate modules. As your business grows, you can expand SAP Business One to fit your needs by adding one of over 500 add-on solutions from SAP Partners. It runs on both the SAP HANA and Microsoft SQL Server platforms and helps with the day-to-day operations of your enterprise. For more information, see [SAP Business One](#).

Several IBM Cloud® for SAP infrastructure options are certified to run SAP Business One.

Before you implement SAP Business One, considerations need to be made how are you going to use the application. For example, how many concurrent users will use the application at one time? Do you need only the Financial Management and Sales and Customer Management modules to start? Maybe you need all the modules (for more information about modules, see [SAP Business One Features](#)).

SAP Business One installation guides

You have the choice of working with an SAP partner or installing the software yourself onto Cloud IaaS.

The main documentation to read for SAP Business One are:

- [SAP Help Portal - SAP Business One on SAP HANA](#)
- [SAP Help Portal - SAP Business One on Microsoft SQL Server](#)

After which, the administrator guides to read for SAP Business One are:

- [SAP Business One on SAP HANA Administrator Guide](#)
- [SAP Business One on Microsoft SQL Administrator Guide](#)

Lastly, review the hardware requirements guidance for SAP Business One:

- [Latest SAP Business One Hardware Requirements Guide](#)
- [SAP Business One Platform Support Matrix](#)

For a list of Microsoft Windows Server versions supported for the following SAP Business One server platforms, see the [SAP Business One Platform Support Matrix](#).

More information on SAP HANA versions can be found in

- [SAP Note 2058870 - SAP Business One, version for SAP HANA on public Infrastructure-as-a-Service \(IaaS\) platforms](#)
- [SAP Note 2801340 - Overview Note for SAP Business One 9.3 PL11, version for SAP HANA](#)
- [SAP Note 3328136 - Overview Note for SAP Business One 10.0 FP 2208 Hotfix 02, version for SAP HANA](#)
- [SAP Note 3284687 - Overview Note for SAP Business One 10.0 FP 2305, version for SAP HANA](#)

The [SAP Business One community page](#) has links to blogs where community members share their experiences with implementing and running SAP Business One.

SAP Business One upgrade guides

SAP Business One offers you several upgrade options when a new release is available.

These options are available if you're using SAP HANA or Microsoft SQL. See the [SAP Business One upgrade patches and programs information](#) for more detail on upgrades, patches, and hot fixes.

SAP Business One training information

Training is available on the integration framework for SAP Business One. The self-paced, online course takes you through scenario design basics, the integration of SAP Business One, and integrating the SAP Business One database. For more information, see the [OpenSAP courses on SAP Business One](#).

Training is also available on the different SAP Business One modules. For more information about courses, see [SAP Training for Business One](#) or the online training available with SAP Learning Hub.

Infrastructure options for SAP Business One

Please check [SAP Business One, version for SAP HANA Platform Support Matrix](#) for supported OS versions of your SAP Business One release. [All the listed IBM Cloud servers for SAP Business One on SAP HANA](#) show the certified SLES operating systems versions.

SAP Business One is supported on the following Bare Metal servers:

- on Classic
 - [BI.S3.H2.192](#)
 - [BI.S3.H2.384](#)
 - [BI.S3.H2.768](#)
 - [BI.S4.H2.192](#)
 - [BI.S4.H2.384](#)
 - [BI.S4.H2.768](#)
- on VPC
 - [cx2d-metal-96x192](#)
 - [bx2d-metal-96x384](#)
 - [mx2d-metal-96x768](#)

SAP Business One is also supported for the following Intel virtual server profiles:

- on VPC
 - [mx2-8x64](#)
 - [mx2-16x128](#)
 - [mx2-32x256](#)
 - [mx2-48x384](#)



Note: IBM Power Virtual Servers are not available for SAP Business One

SAP AnyDB and SAP HANA extra design considerations

AnyDB - IBM Db2

The SAP systems in a landscape have specific requirements for servers, operating systems, network setup, and supported storage.

Deploying SAP AnyDB on IBM Cloud is similar to deployments with infrastructure with on-premises data centers. You can use the information that is provided from SAP and the RDBMS providers.

To assist your project's planning phase, more design considerations are provided for **SAP AnyDB - IBM Db2** with IBM Cloud® for SAP.

Overview of IBM Db2 for SAP with IBM Cloud®

Several unique capabilities and features are available with IBM Db2. All supported database features that are mentioned in [SAP Note 1555903 - DB6: Supported IBM Db2 Database Features](#) are available with IBM Cloud, except for:

- The IBM Db2 pureScale feature.
- Support for integrated cluster managers for HADR or shared disk high-availability clusters.

Before you start deploying the IBM Db2 software, ensure that:

- Check all relevant IBM Db2 information and prerequisites.
- Check all relevant SAP and IBM Db2 information and prerequisites (for example, SAP Notes). Also, check the versions and fix pack levels of IBM Db2 that are supported.
- All required packages are installed for the relevant OS that you are using for IBM Db2.

Documentation of IBM Db2 for SAP

A good place to start is the [SAP community page for IBM Db2](#).

IBM Db2 support on SAP-certified Cloud IaaS:

- [IBM Knowledge Center for Db2 - Support for Db2 on public clouds \(BYOSL, SAP Notes, Reference blueprints\)](#)

IBM Db2 versions and fix pack levels that are supported by SAP:

- [SAP Note 101809 - DB6: Supported Db2 Versions and Fix Pack Levels](#)

IBM Db2 11.5 on **UNIX/Linux** prerequisites documentation:

- [General IBM Db2 prerequisites on UNIX and Linux®](#)

IBM Db2 and SAP NetWeaver on UNIX/Linux:

- [Installation of SAP Systems based on the Application Server ABAP of SAP NetWeaver 7.1 to 7.52 on UNIX: IBM Db2 LUW](#)
- [Installation of SAP Systems based on the Application Server Java of SAP NetWeaver 7.1 to 7.5 on UNIX: IBM Db2 LUW](#)
- [SAP Note 1707361 - Inst. Systems based on NW 7.1 and Higher: UNIX Db2 for LUW](#)

IBM Db2 and SAP NetWeaver on Windows:

- [Installation of SAP Systems based on the Application Server ABAP of SAP NetWeaver 7.1 to 7.52 on Windows: IBM Db2 LUW](#)
- [Installation of SAP Systems based on the Application Server Java of SAP NetWeaver 7.1 to 7.5 on Windows: IBM Db2 LUW](#)
- [SAP Note 1707362 - Inst. Systems based on NW 7.1 and Higher: Windows Db2 LUW](#)



Note: In the IBM Knowledge Center for Db2, the documentation links provided refer to specific pages on an IBM Db2 version. You can switch to the correct version by clicking the "Change version or product" in the upper left area of the IBM Knowledge Center.

SAP on IBM Db2 using Intel Bare Metal

See [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#) for supported IBM Db2 database versions.

A sample configuration is shown in:

- [Quick Study Tutorial - SAP NetWeaver deployment to Bare Metal on Classic Infrastructure, using RHEL](#)
- [Quick Study Tutorial - SAP NetWeaver deployment to Bare Metal on Classic Infrastructure, using Windows Server](#)

SAP on IBM Db2 using Intel Virtual Servers

See [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#) for supported IBM Db2 database versions.

A sample configuration is shown in:

- [Quick Study Tutorial - SAP NetWeaver deployment to Intel Virtual Server on VPC Infrastructure, using RHEL](#)

SAP on IBM Db2 using IBM Power Virtual Servers



Note: This is a complementary offering from IBM Power Systems, with low latency access to IBM Cloud services

See [SAP Note 2855850 - SAP Applications on IBM Power Virtual Servers](#) for supported IBM Db2 database versions on AIX running on IBM Power Virtual Servers.

Infrastructure size considerations

When you use IBM Db2 with SAP applications, follow the general SAP sizing rules as described in the SAP Quick Sizer documentation. However, certain IBM Db2 functions require special considerations.

When you use IBM Db2 columnar organized tables, also known as IBM Db2 BLU Acceleration, the minimal recommended server configuration is 64 GB memory and 4 CPU cores exclusively available for the database workload. For more information about sizing and usage of Db2 BLU Acceleration, see [SAP Note 1819734 - DB2: Use of BLU Acceleration](#).

File Systems for IBM Db2

The following information describes the File Systems that are required for IBM Db2 with SAP NetWeaver:

- [Recommended file system types for Db2](#)
- [Required file systems for IBM Db2 with SAP NetWeaver ABAP \(example is for Unix/Linux\)](#)

SWPM and IBM Db2 port conflict

The default port is **5912** for the TCP/IP communication between the Db2 server and the Db2 client when you are using SWPM to install SAP software.

However, this port is already defined and reserved by the [IANA Service Name and Transport Protocol Port Number Registry](#).

Choose a different port during the installation with SWPM.

Alternatively, it is possible to remove the entry for this port number from the **/etc/services** file:

```
$ ...
cpdlc      5911/sctp          # Controller Pilot Data Link Communication
fis        5912/tcp           # Flight Information Services
fis        5912/udp           # Flight Information Services
fis        5912/sctp          # Flight Information Services
ads-c     5913/tcp           # Automatic Dependent Surveillance
...
```

SAP application-specific considerations

SAP Business Warehouse with IBM Db2

When Using SAP Business Warehouse with the DB2 Database Partitioning Feature, a stable and fast network connections need to be established between all hosts in the Db2 DPF cluster. For details, check the following Information: [SAP Business Warehouse on IBM Db2 for Linux, UNIX, and Windows 10.5 and Higher: Administration Tasks](#).

AnyDB - Microsoft SQL Server

The SAP systems in a landscape have specific requirements for servers, operating systems, network setup, and supported storage.

Deployment of SAP AnyDB on IBM Cloud is similar to deployments with infrastructure with on-premises data centers. Therefore, use the

information that is provided from SAP and the RDBMS providers.

To assist your project's planning phase, there are additional design considerations for **SAP AnyDB - Microsoft SQL Server** with IBM Cloud® for SAP.

Overview of MS SQL Server for SAP with IBM Cloud

Before you start deploying the MS SQL Server software, ensure that:

- Check all relevant SAP and MS SQL Server information and prerequisites (for example, SAP Notes); including versions and fix pack levels of MS SQL Server that are supported
- All required packages are installed for the relevant OS that you are using for MS SQL

Documentation of MS SQL Server for SAP

A good entry point into the documentation is the [SAP community page for MS SQL Server](#). For a current overview of the combinations of MS SQL Server, SAP NetWeaver (or other SAP components), and operating systems - see the [Product Availability Matrix \(PAM\)](#).

MS SQL Server database and SAP NetWeaver on Windows

- [Installation of SAP Systems Based on the Application Server ABAP of SAP NetWeaver 7.3 EHP1 to 7.52 : MS SQL Server](#)
- [Installation of SAP Systems Based on the Application Server Java of SAP NetWeaver 7.5 and SAP Solution Manager 7.2 SR2 Java : MS SQL Server](#)

MS SQL Server licensing supported by SAP

- [SAP Note 1491158 - Information About the Microsoft SQL Server License Scope](#)
- [SAP Note 398136 - Support Policy for Microsoft SQL Server](#)

MS SQL Server release/support information

- [SAP Note 2807743 - Release planning for Microsoft SQL Server 2019](#)
- [SAP Note 2779625 - Setting up Microsoft SQL Server 2019](#)
- [SAP Note 2492596 - Release planning for Microsoft SQL Server 2017](#)
- [SAP Note 2484674 - Setting up Microsoft SQL Server 2017](#)
- [SAP Note 2201059 - Release planning for Microsoft SQL Server 2016](#)
- [SAP Note 1177356 - MS SQL Server: End of Support for SAP Releases](#)
- [SAP Note 62988 - Service packs for MS SQL Server](#)

SAP on MS SQL Server using Intel Bare Metal

See [SAP Note 2414097 - SAP Applications on IBM Cloud: Supported DB/OS and IBM Cloud Bare Metal Server Types](#) for supported MSSQL database versions.

A sample configuration is shown in:

- [Quick Study Tutorial - SAP NetWeaver deployment to Bare Metal on Classic Infrastructure, using Windows Server](#)

SAP on MS SQL Server using Intel Virtual Servers (Gen2)

See [SAP Note 2927211 - SAP Applications on IBM Virtual Private Cloud: Supported DB/OS and IBM Gen 2 Virtual Server Instances](#) for supported MSSQL database versions.

A sample configuration is shown in:

- [SAP NetWeaver deployment to Intel Virtual Server \(Gen2\) on VPC Infrastructure that uses Windows Server](#)

AnyDB - SAP MaxDB

The SAP systems in a landscape have specific requirements for servers, operating systems, network setup, and supported storage.

Deploying SAP AnyDB on IBM Cloud is similar to deploying the infrastructure with on-premises data centers. Therefore, use the information that is provided from SAP and the RDBMS providers.

To assist your project's planning phase, extra design considerations are listed for **SAP AnyDB - SAP Max DB** with IBM Cloud® for SAP.

Overview of SAP MaxDB with IBM Cloud®

Before you start deploying SAP MaxDB software, be sure to:

- Check all relevant SAP MaxDB information and prerequisites (for example, SAP Notes)
- Verify that all required packages are installed for the relevant OS that is used for SAP MaxDB

Documentation of SAP MaxDB

A good entry point into the documentation is the [SAP community page for SAP MaxDB](#).

SAP MaxDB documentation:

- [SAP Help Portal - SAP MaxDB](#)
- [SAP Note 767598 - Available SAP MaxDB documentation](#)
- [SAP Note 1020175 - FAQ: SAP MaxDB installation, upgrade, or applying a patch](#)

For a current overview of the combinations of SAP MaxDB, SAP NetWeaver (or other SAP components), and operating systems, see the [Product Availability Matrix \(PAM\)](#).

SAP MaxDB using Intel Bare Metal

See [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#) for supported SAP MaxDB versions.

SAP MaxDB using Intel Virtual Servers

See [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#) for supported SAP MaxDB versions.

SAP MaxDB using IBM Power Virtual Servers

See [SAP Note 2855850 - SAP Applications on IBM Power Virtual Servers](#) for supported SAP MaxDB versions.

AnyDB - SAP ASE

The SAP systems in a landscape have specific requirements for servers, operating systems, network setup, and supported storage.

Deployment of SAP AnyDB on IBM Cloud is similar to deployments with infrastructure with on-premises data centers. Therefore, use the information that is provided from SAP and the RDBMS providers.

To assist your project's planning phase, more design considerations are provided for **SAP AnyDB - SAP ASE** with IBM Cloud® for SAP.

Overview of SAP ASE with IBM Cloud®

Before you start the software deployment of SAP ASE, ensure that:

- Check all relevant SAP ASE information and prerequisites (for example, SAP Notes)
- All required packages are installed for the relevant OS that is used for SAP ASE

Documentation of SAP ASE

A good entry point into the documentation is the [SAP Community page for SAP Adaptive Server Enterprise \(ASE\)](#).

SAP ASE documentation:

- [SAP Help Portal - SAP Adaptive Server Enterprise \(ASE\)](#)
 - [SAP Help Portal - SAP Adaptive Server Enterprise \(ASE\) Installation and Upgrade Guide for Linux®](#)
 - [SAP Help Portal - SAP Adaptive Server Enterprise \(ASE\) Installation and Upgrade Guide for IBM AIX](#)
 - [SAP Help Portal - SAP Adaptive Server Enterprise \(ASE\) Installation and Upgrade Guide for Windows](#)
- [SAP Note 1748888 - Installing Systems Based on NW 7.3 and Higher: SAP ASE](#)
- [SAP Note 2489781 - SAP ASE 16.0 SP03 Supported Operating Systems and Versions](#)

For a current overview of the combinations of SAP ASE, SAP NetWeaver (or other SAP components), and operating systems - see the [Product](#)

[Availability Matrix \(PAM\)](#)

SAP ASE and SAP NetWeaver **on UNIX/Linux**:

- [Installation of SAP Systems Based on the Application Server ABAP of SAP NetWeaver 7.3 to 7.52 on UNIX/Linux: SAP Adaptive Server Enterprise](#)
- [Installation of SAP Systems Based on the Application Server Java of SAP NetWeaver 7.3 to 7.5 on UNIX/Linux: SAP Adaptive Server Enterprise](#)

SAP ASE and SAP NetWeaver **on Windows**:

- [Installation of SAP Systems Based on the Application Server ABAP of SAP NetWeaver 7.3 to 7.52 on Windows: SAP Adaptive Server Enterprise](#)
- [Installation of SAP Systems Based on the Application Server Java of SAP NetWeaver 7.3 to 7.5 on Windows: SAP Adaptive Server Enterprise](#)

SAP ASE using Intel Virtual Servers

See [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#) for supported SAP ASE database versions.

SAP ASE using IBM Power Virtual Servers



Note: This is a complementary offering from IBM Power Systems, with low latency access to IBM Cloud services.

See [SAP Note 2855850 - SAP Applications on IBM Power Virtual Servers](#) for supported SAP ASE database versions on AIX running on IBM Power Virtual Servers.

AnyDB - SAP IQ

The SAP systems in a landscape have specific requirements for servers, operating systems, network setup, and supported storage.

Deployment of SAP AnyDB on IBM Cloud is similar to deployments with infrastructure with on-premises data centers. Therefore, use the information that is provided from SAP and the RDBMS providers.

To assist your project's planning phase, more design considerations for **SAP AnyDB - SAP IQ** with IBM Cloud® for SAP are provided.

Overview of SAP IQ with IBM Cloud

Before you start deploying the SAP IQ software:

- Check all relevant SAP IQ information and prerequisites (for example, SAP Notes)
- Verify that all required packages are installed for the relevant OS that is used for SAP IQ

Documentation of SAP IQ

A good entry point into the documentation is the [Support Content SAP IQ](#).

SAP IQ documentation:

- [SAP Help Portal - SAP IQ](#)

For a current overview of the combinations of SAP IQ, SAP NetWeaver (or other SAP components), and operating systems, see the [Product Availability Matrix \(PAM\)](#).

SAP HANA Database

The SAP systems in a landscape have specific requirements for servers, operating systems, network setup, and supported storage.

To assist your project's planning phase, more design considerations are provided for **SAP HANA Database** with IBM Cloud® for SAP.

SAP HANA Database Overview

SAP HANA offers a robust set of capabilities, including database management, database administration, data security, multi-model processing,

application development, and data virtualization.

The SAP HANA database is a hybrid in-memory database that combines row-based, column-based, and object-based database technology. It allows online transaction processing (OLTP) and online analytical processing (OLAP) on one system, without the need for redundant data storage or aggregates.

It is optimized to exploit the processing capabilities of multi-core/CPU architectures. With this architecture, SAP applications can benefit from current bar down technologies.

The [SAP HANA database](#) is the heart of SAP's in-memory technology offering, helping customers to improve their operational efficiency, agility, and flexibility.

Overview of SAP HANA database for SAP NW with IBM Cloud

Before you start deploying the SAP HANA database, ensure that:

- Only software installed by certified hardware partners, or any person holding certification, is recommended for use on the SAP HANA system. Do not install any other software on the SAP HANA system. The components of SAP HANA can only be installed by certified hardware partners, or any person holding certification. Furthermore, it must be installed on validated hardware running an approved operating system.
- An SAP HANA system comprises multiple isolated databases and may consist of one host or a cluster of several hosts.
- An SAP HANA system is identified by a single system ID (SID) and contains one or more tenant databases and one system database. Databases are identified by a SID and a database name. From the administration perspective, there is a distinction between tasks performed at system level and those performed at database level. Database clients, such as the SAP HANA cockpit, connect to specific databases.
- The SAP HANA XS advanced application server is a layer on top of SAP HANA that provides the platform for running SAP HANA-based Web applications. It is an integral part of the SAP HANA system.
- A system may consist of one host or a cluster of several hosts. This is referred to as a multiple-host, distributed system, or scale-out system and supports scalability and availability.
- The following sections provide overview information about these aspects of system architecture.



Note: You can find a complete list of all SAP HANA components and the corresponding SAP HANA hardware and software requirements in the Product Availability Matrix (PAM), in the SAP HANA Hardware Directory, and in the SAP Community Network.

Documentation of SAP HANA database

SAP HANA hardware and software requirements are described in the SAP HANA Master Guide at:

- [SAP HANA Hardware and Software Requirements](#)

SAP HANA support on SAP-certified Cloud IaaS:

- [Certified and Supported SAP HANA Hardware – Certified IaaS Platforms](#)

SAP HANA and SAP NetWeaver on UNIX/Linux:

- [Installation of SAP Systems Based on the Application Server ABAP of SAP NetWeaver 7.3 EHP1 to 7.52 on UNIX: SAP HANA Database](#)
- [Installation of SAP Systems Based on the Application Server Java of SAP NetWeaver 7.5 and SAP Solution Manager 7.2 SR2 Java on UNIX: SAP HANA Database](#)
- [Installation of SAP ABAP Systems on UNIX : SAP HANA 2.0 Database - Using Software Provisioning Manager 2.0Software Logistics Toolset 1.0, Current Version SWPM 2.0](#)

HANA and SAP NetWeaver on Windows:

- [Installation of SAP Systems Based on the Application Server ABAP of SAP NetWeaver 7.3 EHP1 to 7.52 on Windows: SAP HANA Database](#)
- [Installation of SAP Systems Based on the Application Server Java of SAP NetWeaver 7.5 and SAP Solution Manager 7.2 SR2 Java on Windows: SAP HANA Database](#)
- [Installation of SAP ABAP Systems on Windows : SAP HANA 2.0 Database - Using Software Provisioning Manager 2.0](#)

SAP on SAP HANA using Intel Bare Metal

See [SAP Note 2414097 - SAP Applications on IBM Cloud: Supported DB/OS and IBM Cloud Bare Metal Server Types](#) for supported SAP HANA database versions.

A sample configuration is shown in:

- [Quick Study Tutorial - SAP NetWeaver deployment to Bare Metal on Classic Infrastructure, using RHEL](#)
- [Quick Study Tutorial - SAP NetWeaver deployment to Bare Metal on Classic Infrastructure, using Windows Server](#)

SAP on SAP HANA using Intel Virtual Servers (Gen2)

See [SAP Note 2927211 - SAP Applications on IBM Virtual Private Cloud: Supported DB/OS and IBM Gen 2 Virtual Server Instances](#) for supported MSSQL database versions.

A sample configuration is shown in:

- [Quick Study Tutorial - SAP NetWeaver deployment to Intel Virtual Server \(Gen2\) on VPC Infrastructure, using RHEL](#)
- [Quick Study Tutorial - SAP NetWeaver deployment to Intel Virtual Server \(Gen2\) on VPC Infrastructure that uses Windows Server](#)

SAP partner certified solutions

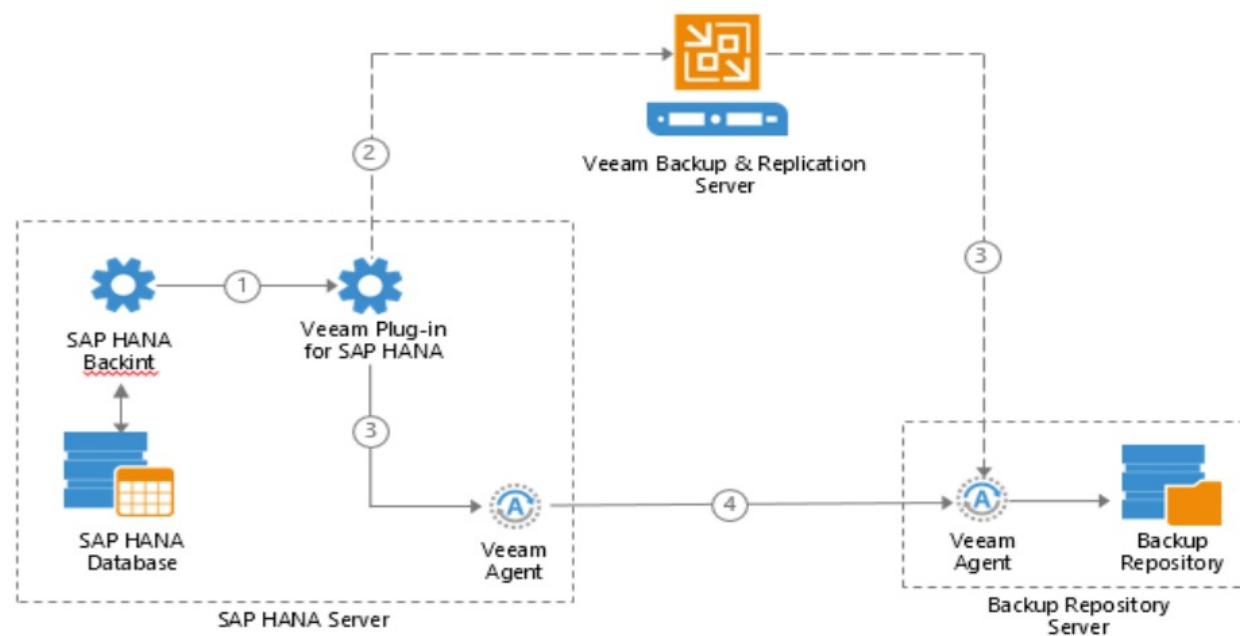
Veeam for SAP HANA backups

⊖ **Deprecated:** This document is out of date, it is being updated for Veeam 10.x and replaced in November-2020 with new content.

Veeam Backup & Replication can be provisioned and deployed from the IBM Cloud catalog to provide protection for SAP HANA workloads on certified IBM Cloud® for SAP infrastructure. Veeam performs SAP HANA **Backint**-based backup and restore of databases and logs, and is listed on the [SAP Certified Solutions Directory](#).

Veeam overview and considerations

Below is high-level overview of how an SAP **Backint** database backup is performed:



SAP HANA Backint database backup overview

Veeam Plug-in, which acts as a go-between for SAP HANA and Veeam Backup repository, is installed on the SAP HANA server. Veeam Backup & Replication is provisioned on either IBM Cloud Bare Metal Servers or IBM Cloud Classic Virtual Servers.



Note: IBM Cloud Classic Virtual Servers are used for the sample deployment.

Veeam Plug-in connects to the Veeam Backup & Replication server and creates a backup job. Once a backup job is requested, Veeam Plug-in starts a Veeam Transport Agent on the SAP HANA server and on the backup repository, which transports data to the backup repository. For more information, see [How Veeam Plug-in for SAP HANA Works](#).

At this time, Veeam is able to provision with IBM Cloud® for VMware Solutions Dedicated only.

System considerations

Veeam Backup & Replication has a very high-performance data mover engine embedded within its components that is used for

- Reading VM data from production storage
- Applying compression/de-duplication
- Writing the resulting data stream to backup storage

The efficiency that it performs these operations is impacted by available resources, including network bandwidth, storage performance, and server processing capacity.

Systems requirements

- **vSphere.** Veeam supports vSphere (ESXi) and vCenter environments v4.1 and greater. While Veeam is suited for backup of individual

vSphere (ESXi) hosts, vCenter, if deployed, is the preferred interface into a vSphere environment. vCenter provides added configuration and ease of management.

Veeam supports all OS types compatible with VMware.

VMs with disks in the SCSI bus-sharing mode are not supported as VMware does not support snapshotting VMs with those types of disks.

The following disk types are skipped from processing automatically and are not supported:

- RDM virtual disks in physical mode,
- independent disks,
- disks connected via in-guest iSCSI initiator,
- and VMs with pass-through virtual disks.

■ **IBM Cloud Classic Virtual Servers**. Veeam Backup & Replication components are provisioned on IBM Cloud Classic Virtual Servers.

Minimum requirements are

- 4-core
- 8 GB RAM
- 1 Gb network uplink speed

Veeam supports Windows Server 2012 and later, however, Windows Server 2016 is recommended for the advanced storage optimization and efficiency presented by the Resilient File System (ReFS).

- **Storage**. IBM Block Storage for Classic Endurance block storage with LUN's from 1 TB to 2 TB, 0.25 IOPS/GB performance level is recommended for hosting the Veeam backup repository. You are encouraged to thoroughly test other performance levels before selecting the performance storage level for your production Veeam repository.
- **Throughput**. For the initial full backup, Veeam ignores empty or deleted VM storage blocks. For example, if a VM has been allocated 1 TB of storage, thin or thick provisioned, and only consumes 450 G, Veeam only processes 450 G for that VM. For ongoing incremental backups, Veeam only processes VM data blocks changed since the last backup.

Based on preliminary results, the standard Veeam virtual server processes approximately 220 GB of VM data per hour, which means if total active VM data to be backed up is 1 TB, the initial backup takes approximately 4.5 hours. Based on a 10% per day VM change rate, the daily incremental backup takes approximately 45 minutes.

Veeam Reference material

- [Veeam Backup & Replication Quick Start Guide for VMware vSphere](#)
- [Veeam Support Knowledge Base](#)
- [Veeam Backup & Replication Best Practices](#)

{:android: data-hd-operatingsystem="android"}{:api: .ph data-hd-interface="api"}{:audio: .audio} {:attention: .attention} {:authenticated-content: .authenticated-content} {:beta: .beta} {:c#: .ph data-hd-programlang="c#"} {:cli: .ph data-hd-interface="cli"} {:codeblock: .codeblock} {:curl: .ph data-hd-programlang="curl"} {:deprecated: .deprecated} {:dotnet-standard: .ph data-hd-programlang="dotnet-standard"} {:experimental: .experimental} {:exception: .exception} {:external: target="_blank" .external} {:fast-path: .fast-path} {:faq: data-hd-content-type="faq"} {:generic: data-hd-programlang="generic"} {:go: .ph data-hd-programlang="go"} {:help: data-hd-content-type="help"} {:here: .ph data-hd-vposition="here"} {:hide-dashboard: .hide-dashboard} {:hide-in-docs: .hide-in-docs} {:important: .important} {:ios: data-hd-operatingsystem="ios"} {:java: .ph data-hd-programlang="java"} {:javascript: .ph data-hd-programlang="javascript"} {:middle: .ph data-hd-position="middle"} {:node: .ph data-hd-programlang="node"} {:note: .note} {:objectc: .ph data-hd-programlang="Objective C"} {:php: .ph data-hd-programlang="PHP"} {:pre: .pre} {:preview: .preview} {:python: .ph data-hd-programlang="python"} {:release-note: data-hd-content-type="release-note"} {:remember: .remember} {:requirement: .requirement} {:restriction: .restriction} {:right: .ph data-hd-position="right"} {:row-headers: .row-headers} {:ruby: .ph data-hd-programlang="ruby"} {:screen: .screen} {:shortdesc: .shortdesc} {:step: data-tutorial-type="step"} {:support: data-reuse="support"} {:swift: .ph data-hd-programlang="swift"} {:tag-security: .tag data-tag-color="red"} {:tag-devops: .tag data-tag-color="magenta"} {:tag-app: .tag data-tag-color="purple"} {:tag-datastore: .tag data-tag-color="blue"} {:tag-network: .tag data-tag-color="cyan"} {:tag-observability: .tag data-tag-color="teal"} {:tag-management: .tag data-tag-color="teal"} {:tag-vpc: .tag data-tag-color="dark-teal"} {:tag-compute: .tag data-tag-color="green"} {:tag-ibm-cloud: .tag data-tag-color="blue"} {:tag-cp4d: .tag data-tag-color="magenta"} {:tag-iks: .tag data-tag-color="blue"} {:tag-roks: .tag data-tag-color="red"} {:tag-schematics: .tag data-tag-color="purple"} {:tag-classic-inf: .tag data-tag-color="warm-gray"} {:tag-satellite: .tag data-tag-color="magenta"} {:tag-linux: .tag data-tag-color="red"} {:tag-macos: .tag data-tag-color="cool-gray"} {:tag-windows: .tag data-tag-color="cyan"} {:tag-new: .tag data-tag-color="green"} {:tag-updated: .tag data-tag-color="blue"} {:tag-deprecated: .tag data-tag-color="red"} {:tag-red: .tag data-tag-color="red"} {:tag-magenta: .tag data-tag-color="magenta"} {:tag-purple: .tag data-tag-color="purple"} {:tag-blue: .tag data-tag-color="blue"} {:tag-cyan: .tag data-tag-color="cyan"} {:tag-teal: .tag data-tag-color="teal"} {:tag-dark-teal: .tag data-tag-color="dark-teal"} {:tag-green: .tag data-tag-color="green"} {:tag-cool-gray: .tag data-tag-color="cool-gray"} {:tag-warm-gray: .tag data-tag-color="warm-gray"} {:term: .term} {:terraform: .ph data-hd-

interface="terraform"}{:tip: .tip} {:troubleshoot: data-hd-content-type="troubleshoot"}{:tsCauses: .tsCauses} {:tsResolve: .tsResolve} {:tsSymptoms: .tsSymptoms} {:tutorial: data-hd-content-type="tutorial"}{:ui: .ph data-hd-interface="ui"}

IBM Security Services for SAP

IBM Cloud® Security Services for SAP offer a cybersecurity solution that automates the monitoring and protection of SAP applications on IBM Cloud, and keeps workloads compliant and secure from inside and outside threats.

IBM Services for SAP, developed in partnership with IBM Security Software and other business partners, implement and configure the SAP landscape to meet IT environment requirements for continuous workload visibility and protection.

Through continuous monitoring, IBM Security Services are able to deliver near real-time preventive, detective, and corrective solutions for securing SAP systems and applications with unmatched coverage and protection. This protection includes context-aware insight across SAP NetWeaver ABAP or Java and SAP HANA platforms, with network security, security management, and associated workflows.

IBM Security Services for SAP offer the following features:

- Comprehensive understanding of vulnerabilities and potential attack vectors
- Methods to implement and avoid defects in ABAP code or SAP Transports
- Identifying configuration vulnerabilities for ABAP, Java, and HANA environments
- Identifying missing or outdated SAP notes and patches
- Identifying, monitoring and review of highly privileged SAP accounts
- Enabling continuous monitoring of vulnerabilities with integration to existing SIEM solution

Key benefits of requesting IBM Security Services for SAP to assist with your IBM Cloud® for SAP deployments:

- Consultative engagement methods centered on your business objectives
- Experienced end-to-end architectural experts that work jointly with the IBM Cloud team
- Accelerated cloud adoption for successful implementation of SAP workloads on the cloud
- Prescriptive best practices for solution implementation by using IBM Cloud Services products and features
- Rapid learning and risk mitigation through access to IBM Cloud experts

For more information, see [IBM.com - IBM Security - SAP Security and GRC Strategy Services](#).

Procedure to request IBM Security Services for SAP

To begin with IBM Security Services for SAP, use either:

- Live Chat with IBM Security Sales, by using [IBM.com - IBM Security](#) and click **Let's talk** in the botttom-left
- [Email with IBM Security Sales](#)

Procedure to request IBM Security Services for SAP, directly from IBM Cloud for VMware Solutions

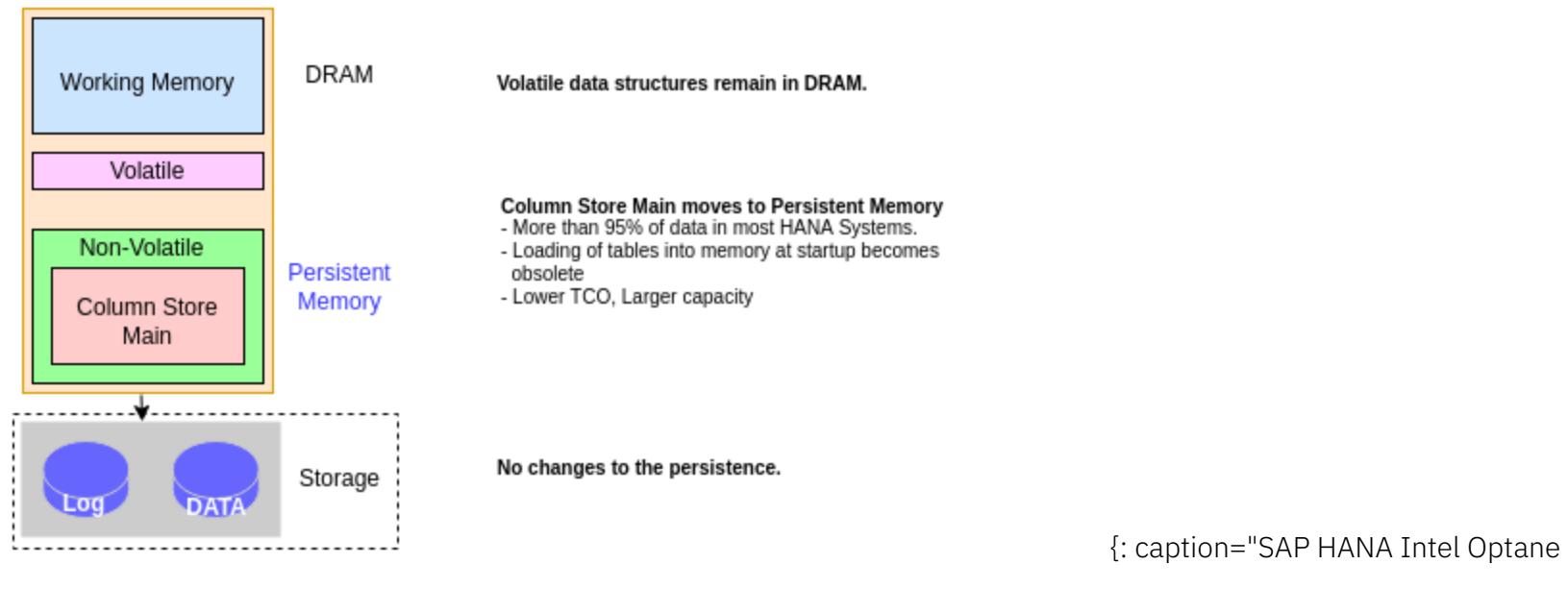
Because of the close collaboration between IBM Cloud for VMware with SAP and IBM Security Services for SAP, the quickest way to use IBM Security Services in combination with SAP workloads on VMware is to:

1. Open the IBM Cloud for VMware Solutions console. Scroll down to the **Services** section and on the **Featured Workload Solutions** card click **IBM Security Services for SAP**.
2. On the **IBM Security Services for SAP** page, in the **Engage IBM Security Services** box, provide the requested details, and click **Request a consultation**.

An IBM Cloud for VMware Solutions representative will contact you by using your IBM Cloud contact information to help you with the solution that you need.

SAP HANA with Intel Optane Persistent Memory (PMEM)

SAP HANA now has a non-volatile in-memory option on Bare Metal servers. Intel Optane™ persistent memory (PMEM) retains its contents like traditional storage options but with speeds similar to main memory.



{: caption="SAP HANA Intel Optane PMem [1] overview" caption-side="bottom"}

Many systems with large data storage and retrieval needs use DRAM for fast data retrieval. DRAM is costly and data does not persist when the server is rebooted or shutdown. On startup, data must be reloaded from storage.

With Intel Optane PMEM, data is retained in memory during system restarts and power outages, providing faster start times. PMEM provides near-DRAM performance and is also byte-addressable.

Intel Optane PMEM modules are installed with DRAM in the same dual in-line memory module (DIMM) slot. PMEM modules do not function without any DRAM DIMMs installed. The current configurations supports DRAM to PMEM ratios of 1:1, 1:2, and 1:4.

SAP HANA uses App Direct mode, in which the application stores data on the persistent memory. HANA2 SP04 release or higher was co-engineered by SAP and Intel to use the unique dual memory and storage capability of the PMem modules.

In App Direct mode, the applications directly access the memory and control the direct load and store of the PMem and DRAM DIMMs memory resources. In this mode, the PMem acts as byte-addressed persistent memory that is mapped to the system physical address space. App Dir mode uses regions, which are groups of one or more PMem modules that appear to be a single logical virtual address space. Regions are partitioned into one or more namespaces, similar to hard disk partitions.

Persistent memory is a Bare Metal profile option

You order persistent memory as part of ordering your Bare Metal server.

Bare Metal server profiles for the DRAM:PMEM ratios include:

DRAM:PMEM ratio	Bare Metal Profile
1:1	BI.S4.H2.1.5TB RAM + 1.5TB Persistent Memory
1:1	BI.S4.H4.3TB RAM + 3TB Persistent Memory
1:1	BI.S4.H8.6TB RAM + 6TB Persistent Memory
1:2	BI.S4.H2.768GB RAM + 1.5TB Persistent Memory
1:2	BI.S4.H2.1.5TB RAM + 3TB Persistent Memory
1:2	BI.S4.H2.768GB RAM + 3TB Persistent Memory
1:2	BI.S4.H4.1.5TB RAM + 3TB Persistent Memory
1:2	BI.S4.H4.3TB RAM + 6TB Persistent Memory
1:2	BI.S4.H8.3TB RAM + 6TB Persistent Memory
1:2	BI.S4.H8.6TB RAM + 12TB Persistent Memory
1:4	BI.S4.H2.384GB RAM + 1.5TB Persistent Memory

1:4	BI.S4.H4.768GB RAM + 3TB Persistent Memory
1:4	BI.S4.H4.1.5TB RAM + 6TB Persistent Memory
1:4	BI.S4.H8.1.5TB RAM + 6TB Persistent Memory
1:4	BI.S4.H8.3TB RAM + 12TB Persistent Memory

DRAM:PMEM ratios

Sizing

Standard HANA sizing rules apply to a 1:1 ratio configured server. The PMem size is the maximum HANA database size capacity. For example, the BI.S4.H4 profile can host a database of up to approximately 3 TB (compressed). If the server is hosting multiple systems or tenants, you have a total maximum data capacity of 3 TB (for example 3 x 1 TB databases or 2 x 1.5 TB systems). HANA uses both the DRAM and PMem and manages memory use for both data and application logic.

Post-provisioning

When you order your Bare Metal server with persistent memory, regions are created by the provisioning engine. As part of post-provisioning, you create the namespaces that you need. For more information, see [Deploying your infrastructure](#).

Backup, recovery, and system replication

Backup, recovery, and system replication are part of standard Bare Metal configuration. You perform the same steps for post provisioning on the Bare Metal servers as you do for SAP HANA.

-
1. This diagram originally appeared in the [SAP Community blog by Andreas Schuster](#) ↵

Quick study deployment of SAP

SAP NetWeaver deployment to Intel Virtual Server on VPC Infrastructure that uses RHEL



Note: A Quick Study, someone who is able to learn new things quickly.

These Quick Study Tutorials provide a single sample configuration, with less detailed instructions, as an introduction for customers who prefer hands-on tasks to increase their pace of learning.

The following information provides an introduction for customers who are new to IBM Cloud® Virtual Private Cloud (VPC) Gen 2 environment. Two sample configurations are provided to help you through the ordering process to the start of the SAP installation.

The first configuration sample is simple, a single node 128 GB, 32 vCPU server. The second is an advanced configuration of two nodes by adding a second virtual server to the landscape. The sample layouts might not be your preferred layout. The purpose of this guidance is to show you two possibilities if you are not experienced with the Linux® operating system or with VPC Gen 2.

Virtual private cloud

Provision your compute services on virtual private cloud

Create a fully customizable, software-defined virtual network with superior isolation in IBM Public Cloud.

VPC environments

Gen 1 Compute [View docs](#)
Generation 1 compute offers a broad selection of general purpose profiles and is available in all VPC regions.

Gen 2 Compute [View docs](#)
Generation 2 compute offers improved networking performance (up to 80 Gbps) and five times faster provisioning than generation 1 compute.

Recent VPCs

Name	Region
No VPCs created for Gen 1 compute	

Create VPC for Gen 1

View all

Name	Region
sap-2-tier-vpc	London
sap-3-tier-vpc	London
sap-t2-vpc	Frankfurt
sap-test-inst	London
sap-test-vpc	Frankfurt

Create VPC for Gen 2

IBM Cloud VPC

Step 1: Securing Access

Security is one of the biggest concerns when you run your business-critical applications in a cloud environment. To secure your connection to your IBM® Virtual Servers, a public SSH key can be uploaded to your account, per region. These public keys are deployed to your virtual servers instances to allow access to the servers.



Tip: Before you continue, create an SSH public key that you can upload later to the region of your choice when you are creating the virtual server instance. Follow the steps that are [documented here](#).

You use security groups to restrict access to and from IP ranges, protocols, and ports. Security groups aren't within the scope of this guidance, and the default security group that is deployed with your sample VPC can suffice. However, you might have to add extra ports for exceptions to the access restrictions, such as, the SAP Software Provisioning Manager and for the ports that are being used by your SAP NetWeaver based application.

Step 2: Creating an IBM Cloud VPC and subnet

IBM Cloud® compute resources are kept in a global region within a VPC. Use the following steps to create a VPC and its subnet.

1. Log in to the [IBM Cloud console](#) with your unique credentials.

2. Click **Menu icon** > **VPC Infrastructure** > **Network** > **VPCs** and click **New virtual private cloud** > **Create VPC for Gen 2**.

Virtual Private Clouds						
Regions						
Status	Virtual Private Cloud	Resource group	Subnets	Default ACL	Default Security Group	
● Available	sap-2tier-vpc	Default	1	rope-whiny-backwater-portal-snort-spiritual	geometry-errand-hatless-delivery-trench-cavalier	:
● Available	sap-3tier-vpc	Default	2	sprung-magnifier-scrambler-riveting-proactive-cupping	giggle-custody-snowshoe-overvalue-send-reforest	:
● Available	sap-test-inst	Default	1	emptier-extending-shortly-steerable-retouch-countdown	satisfied-curator-gigolo-enchanted-whiny-daydream	:
● Available	sap-test-vpc-lon	Default	1	rippling-overdraft-relax-retaining-eternal-grasp	nearness-trillion-henna-scruffy-threelfold-wolverine	:

Data will update in 41 seconds

Creating a VPC

1. Enter a unique **Name** for the VPC, for example, *sap-test-inst*.
2. Keep the default **Resource group**. Use resource groups to organize your account resources for access control and billing purposes. For more information, see [Best practices for organizing resources in a resource group](#). For this example, you can use the default value.
3. *Optional: Tags*. Enter tags to help you organize and find your resources. You can add more tags later. For more information, see [Working with tags](#).
4. Keep the **Default security group** settings, which allow inbound SSH and ping traffic to virtual server instances in this VPC.
5. *Optional: Classic access*. Select whether you want to enable your VPC to access classic infrastructure resources. For more information, see [Setting up access to classic infrastructure](#).

Important: You can enable a VPC for classic access only while you are creating it. In addition, you can have only one classic access VPC in your account at any time.

6. *Optional: Default address prefixes*. Disable this option if you don't want to assign default subnet address prefixes to each zone in your VPC. After you create your VPC, you can go to its details page and set your own subnet address prefixes. If you do disable this option, the **New subnet for VPC** section will be hidden, and will require manual definition after the VPC is created. Leave the default value.

Note: If you want to create the subnet and your own subnet address prefixes later, become familiar with important details of VPC networking. For more information, see [About networking for VPC](#) and [Designing an addressing plan for a VPC](#).

New subnet for VPC

1. Enter a unique **Name** for the VPC subnet, for example, *sap-subnet1*.
2. Select a **Resource group** for the subnet. For this example, keep the value default.
3. Select a **Location** for the subnet, for example, *LON, London 3*. The location consists of a region and a zone.

Tip: The region that you select is used as the region of the VPC. All additional resources that you create in this VPC are created in the selected region.

4. Enter an **Address prefix**, **Number of addresses**, and an **IP range** for the subnet. The IP range is entered in CIDR notation, for example: *10.240.0.0/24*. In most cases, you can use the default IP range. If you want to specify a custom IP range, you can use the IP range calculator to select a different address prefix or change the number of addresses.

Important: A subnet cannot be resized after it is created.

5. Keep the default value for **Subnet access control list**. A new default ACL is created that you can configure later following these steps in: [Configuring the ACL](#).
6. Attach a public gateway to the subnet if you want to allow all attached resources to communicate with resources on the public internet. However, keep in mind, that public gateways are for 'outbound traffic', 'inbound traffic' would require a **Floating IP**. See [Preparing the virtual server instance for your workload](#).



Tip: You can also attach the public gateway after you create the subnet.

7. Click **Create virtual private cloud**. The VPC appears in the Virtual Private Clouds page immediately.

Step 3: Creating a Virtual Server Instance

Use the following steps to create a virtual server instance.

1. Click **Virtual server instances > New instance**.

2. Enter a unique **Name** for the virtual server, for example, `sap-app-vsi`. The name that you enter becomes the hostname.



Important: SAP hostnames must consist of a maximum of 13 alpha-numeric characters. See [SAP Note 611361](#) for further details.

3. Select the **Virtual private cloud** in which to attach the virtual server instance, for example, `sap-test-inst`.

4. Keep the **Resource group** default.

5. *Optional: Tags.* Enter tags to help you organize and find your resources. You can add more tags later. For more information, see [Working with tags](#).

6. The **Location** in which you created your subnets is already selected. The location consists of a region and a zone.

7. Select **Catalog image > ibm-redhat-7-6-amd64-sap-applications-1** as the OS image.

Name	Operating system	Created
ibm-redhat-7-6-amd64-sap-hana-1	Red Hat Enterprise Linux	February 6, 2020 7:00
ibm-redhat-7-6-amd64-sap-applications-1	Red Hat Enterprise Linux	February 6, 2020 7:00

Catalog image for SAP NetWeaver

\$ For every SUSE Linux®; Enterprise and Red Hat®; Enterprise Linux®; version there are two different Catalog Images available each: one for SAP HANA and one for SAP NetWeaver (Applications). In these images, the specific repositories are enabled, so you can install the OS packages that are required to install SAP HANA or SAP NetWeaver.
{: note}

1. Click **All profiles > Balanced** and select `bx2-32x128`. For more information about SAP-certified profiles, see [Intel Virtual Server certified profiles for SAP NetWeaver](#).

Balanced compute and memory resources. Best for common cloud workloads that require a balance of performance and scalability, such as mid size databases and common cloud applications with moderate traffic.

bx2-2x8	2 vCPUs	8 GB RAM	4 Gbps
bx2-4x16	4 vCPUs	16 GB RAM	8 Gbps
bx2-8x32	8 vCPUs	32 GB RAM	16 Gbps
bx2-16x64	16 vCPUs	64 GB RAM	32 Gbps
bx2-32x128	32 vCPUs	128 GB RAM	64 Gbps
bx2-48x192	48 vCPUs	192 GB RAM	80 Gbps

i Large Profile

To take full advantage of the full 64 Gbps bandwidth, you will need to add an additional network interface

SSH keys

sap-test-key ▾ New key

Balanced profiles for SAP NetWeaver

Setting an SSH key

If you uploaded your public key for the VPC's region, select it and skip to the next section (Attaching storage). Otherwise, follow these steps.

1. Click **New key**.
2. Enter a unique **Name**, for example, *sap-ssh-key*.
3. Keep the default **Resource group**.
4. The **Region** in which you created your subnets is already selected.
5. *Optional: Tags*. Enter tags to help you organize and find your resources. You can add more tags later. For more information, see [Working with tags](#).
6. Paste the **Public key**, that you created according to [the guidelines mentioned in Securing Access](#).
7. Click **Add SSH key**.
8. *Optional: User data*, leave blank.

Attaching a block storage volume

To have file system space available beyond what is required by the operating system, you need to attach a block storage volume to your virtual server instance. This storage volume is used by the application that you're installing. In this example, the application is the Relational Database Management System (RDBMS) required for an SAP NetWeaver stack.

1. Click **New volume**.
2. Enter *sap-app-vol1* for **Name**.
3. Select *Custom* for **Profile**.
4. Enter *500* for **Size**.
5. Enter *10000* for **IOPS**. **Throughput** defaults to *156.25 MiBps*.
6. Keep the **Encryption** and **Auto Delete** defaults.

Location - London 3

New block storage volume

Create a new block storage volume to attach to this instance.

Name
sap-app-vol1

Profile
Custom

Size
Between 10 and 2000 GB.
500

IOPS
Between 100 and 10000.
10000

Learn more about size and IOPS.

Throughput
156.25 MiBps

Encryption
Provider managed

Auto Delete ⓘ

Cancel **Attach**

Attaching a block storage volume

1. Click **Attach**.
2. Keep the **Network interfaces** default.
3. Click **Create virtual server instance**. After the Virtual Servers for VPC is provisioned and ready for SSH logon, you can begin installing the SAP NetWeaver applications.

Step 4: Preparing the virtual server instance for your workload

IBM® Virtual Servers are accessed through IPsec connections into your VPC. Configuring IPsec-based access to virtual server instances is beyond the scope of this guidance. For simplicity, and to quickly access the deployed instance, you can assign a *Floating IP* to your virtual server instance. This IP is assigned to a gateway that forwards ports and protocols according to the defined security groups.

Network interfaces ⓘ			
Interface	Subnet Name	Private IP	Floating IP
eth0	sap-subnet1	10.242.128.8	158.176.180.39
Floating IP			

By assigning the IP, you can directly `ssh` into your virtual server instance - in our example, the command is

```
$ ssh -i ~/.ssh/sap-ssh-key root@158.176.180.39
```

To update the operating system for your virtual server instance to the latest level, run `yum update` and restart the virtual server instance.

The SAP NetWeaver Software Provisioning Manager (SWPM) doesn't allow products to install to hostnames that don't resolve to an external IP on the server instance. Because of this restriction, the default settings in the virtual server instance need to be adapted. Edit `/etc/hosts` and comment out the lines that resolve the hostname to the IPv4 AND IPv6 localhost addresses. Instead, the hostname must resolve to the external IP address of your virtual server (see the example). In our example, the hostname resolves to `10.242.128.8`, the private IP

displayed in Figure 6. In this example, we append a sample default domain. Adapt this example to your specific environment.

These lines are an example of an `/etc/hosts` file. Take care that both references of localhost to the hostname, IPv4 and IPv6 are in comments (or deleted).

```
$ # The following lines are desirable for IPv4 capable hosts

#127.0.0.1 sap-app-vsi sap-app-vsi
127.0.0.1 localhost.localdomain localhost
127.0.0.1 localhost4.localdomain4 localhost4

# The following lines are desirable for IPv6 capable hosts

#:1 sap-app-vsi sap-app-vsi
::1 localhost.localdomain localhost
::1 localhost6.localdomain6 localhost6
10.242.128.8 sap-app-vsi.saptest.com sap-app-vsi
```

To prevent the IBM Cloud `cloudinit` process from reverting the content of `/etc/hosts` to the previous values on the next restart, change the configuration in `/etc/cloud/cloud.cfg`. Change `manage_etc_host` from `True` to `False`.

Finally, you need to adapt your storage by creating a file system on the attached storage volume. You can identify the newly attached volume by its size by entering `/sbin/fdisk -l` and checking the sizes. To safely identify it, find the device ID by clicking **Device** on the Virtual server instances for VPC page.

Data volumes

Name	Device	Size	Max IOPS	MiBps	Encryption
sap-app-vol1	07a7-184b4a2f-d7...	500	10000	156.25	Provider managed

Data volumes

1. On the Overview page, check the first 20 digits in **Device**, and find the same ID under `/dev/disk/by-id`. Our example device is `07a7-184b...`.

```
$ [root@sap-app-vsi ~]# ls -als /dev/disk/by-id/ | grep 07a7-184b4a2f-d768-4
0 lrwxrwxrwx 1 root root 11 May 3 08:30 virtio-07a7-184b4a2f-d786-4 -> ../../vdb
```

In our example, it's `virtio-07a7-184b4a2f-d786-4`, which is linked to `/dev/vdb`.

1. Create a file system on this path:

```
$ [root@sap-app-vsi ~]# mkfs.xfs /dev/vdb
```

2. Find the related UUID in `/dev/disk/by-uuid`:

```
$ [root@sap-app-vsi ~]# ls -als /dev/disk/by-uuid/ | grep vdb
0 lrwxrwxrwx 1 root root 11 May 10 08:31 1350230e-8058-4fe5-bbc0-cc27253ff778 -> ../../vdb
```

3. Add the UUID to `/etc/fstab`, in our example:

```
$ UUID=1350230e-8058-4fe5-bbc0-cc27253ff778 /db2 xfs defaults 0 0
```

4. Create a file system to use for the greater part of your installation, since we are using IBM Db2, we choose:

```
$ [root@sap-app-vsi ~]# mkdir /db2
[root@sap-app-vsi ~]# mount /db2
```

5. Add swap space for SWPM. We are adding a minimum swap space to the system.

```
$ [root@sap-app-vsi ~]# dd if=/dev/zero of=/swapfile bs=1M count=8192
8192+0 records in
8192+0 records out
8589934592 bytes (8.6 GB) copied, 24.701 s, 348 MB/s

[root@sap-app-vsi ~]# chmod 0600 /swapfile
```

```
[root@sap-app-vsi ~]# mkswap /swapfile
Setting up swap space version 1, size = 8388604 KiB
no label, UUID=e7a63777-521a-44a7-abcc-0d17e1876a78
```

- Add the following line to your `/etc/fstab`.

```
$ /swapfile    none    swap    sw    0 0
```

- Activate the swap space:

```
$ [root@sap-app-vsi ~]# swapon -a
```

You're now ready to install the SAP product of your choice. Your next step is to [download and install your SAP software and applications](#) if a single virtual server sample is sufficient for your needs.

Step 5: Installing two virtual server instances in a 3-tier setup

A more complex scenario involves installing two virtual servers. One server is the SAP NetWeaver Application Server (`sap-app-vsi`) and the other server is the database server for SAP NetWeaver. Given that we have two virtual servers of the same layout, per the example, Figures 8 and 9 are an overview of the virtual servers.

Virtual server instances

Status	Name	Virtual Private Cloud	Profile	Private IP
Powered On	sap-app-vsi	sap-test-vpc	bx 2-3 2x128	10.243.128.7
Powered On	sap-app2-vsi	sap-test-vpc	bx 2-3 2x128	10.243.128.9

Volume details

Name	sap-app2-vol2
Resource group	Default
Attachment type	—
ID	r010-9cddc9a2-0073-49d4-9131-a36a63c72621
Created	May 12, 2020 8:39:39 PM
Location	Fran kfurt3
Size	200 GB
Profile	10 IOPS/GB
MaxIOPS	3000
Throughput	4688 MiBps
Encryption	Provider managed

Attached instances

Name	Auto Delete
There are no instances attached to this volume.	

Attach virtual server instance

sap-app2-vsi

Cancel Attach volume

Block storage volumes for VPC

Both virtual servers have one extra attached volume and a *Floating IP*. A smaller volume is attached to `sap-app-vsi`, which is the application server. `sap-app2-vsi` has a slightly larger volume to host the RDBMS and the SAP Central Services (ASCS) instance. A second volume is needed on `sap-app2-vsi` to host the SAP NetWeaver stack. Create another volume from the Block storage volumes for VPC page and name it `sap-app2-vol2`. Attach `sap-app2-vol2` to our virtual server by selecting its details screen.

Status	Name	Resource group	Location	Size	Max IOPS	Attachment type	Encryption
Available	sap-rvol1	Default	Frankfurt3	20GB	3000	Data	Provider managed
Available	sap-app-vsi-boot	Default	Frankfurt3	100GB	3000	Boot	Provider managed
Available	sap-app2-vol1	Default	Frankfurt3	200GB	3000	Data	Provider managed
Available	sap-app2-vsi-boot	Default	Frankfurt3	100GB	3000	Boot	Provider managed

Block storage volumes for VPC

Step 6: Preparing your network

To segregate network traffic, as SAP recommends, deploy a second subnet. One network is used for client access, the other for communication between the SAP ABAP stack and the RDBMS.

Use Figure 11 as your guide to create a new subnet named `sap-test-net2`.

Click **Menu icon** > **VPC Infrastructure** > **Network** > **Subnets** and click **New subnet**.

All subnets for VPC

Gen 2 compute
This subnet will be created for use with generation 2 compute resources. It cannot be used with generation 1 instances.
[Switch to Gen 1 compute](#)

New subnet for VPC

Name: sap-test-net2 **Virtual private cloud**: sap-test-vpc

Resource group
The resource group can't be changed after the network is created.
[Learn about resource groups](#)

Location: Frankfurt, Frankfurt3

IP range selection
We have calculated the most efficient location for your IP range (CIDR block) to maximize your available IP addresses. You can customize the IP range by selecting a different address prefix, changing the number of addresses or by entering your IP range manually.

Address prefix	Number of addresses	IP range
10.243.128.0/18	256	10.243.129.0/24

Address space 10.243.128.0 to 10.243.191.255

IP range: 10.243.129.0/24

Subnet access control list: VPC Default (dropdown-flashbulb- joyfully-deception-hacking-dictator)

Create a subnet

After the new subnet is created, it is displayed on the Subnets for VPC page.

Status	Subnets	Virtual Private Cloud	Location	IP Range	Public Gateway
Available	sap-test-vpc-net1	sa-p-test-vpc	Frankfurt 3	10.243.128.0/24	-
Available	sap-test-net2	sa-p-test-vpc	Frankfurt 3	10.243.129.0/24	-

Subnets for VPC page

The two virtual servers need to connect to the new network. Go back to the virtual server overview and click **New interface**.

Data volumes

Maintain your `/etc/hosts` files according to the targeted setup. The following example is for `sap-app2-vsi`.

```
$ # The following lines are desirable for IPv4 capable hosts
#127.0.0.1 sap-app2-vsi sap-app2-vsi
127.0.0.1 localhost.localdomain localhost
127.0.0.1 localhost4.localdomain4 localhost4

# The following lines are desirable for IPv6 capable hosts
::1 sap-app2-vsi sap-app2-vsi
::1 localhost.localdomain localhost
::1 localhost6.localdomain6 localhost6
10.243.128.9 sap-app2-vsi.saptest.com sap-app2-vsi
10.243.129.6 sap-app2-vsi-priv.saptest.com sap-app2-vsi-priv
10.243.128.7 sap-app-vsi.saptest.com sap-app-vsi
10.243.129.4 sap-app-vsi-priv.saptest.com sap-app-vsi-priv
```

Step 7: Preparing your storage

You need to provision two volumes on the database virtual server with a file system for the database and for the SAP installation. In addition, `/sapmnt` needs to be Network File System (NFS) exported to the application server virtual server.

The application server virtual server has only one attached 20 GB volume. You can identify the volume without looking at the resource ID.

```
$ Disk /dev/vdd: 21.5 GB, 21474836480 bytes, 41943040 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

We create a file system on the volume and mount it after you determine its `/dev/disk/by-uuid` path.

```
$ ls -als /dev/disk/by-uuid/ | grep vdd  
0 lrwxrwxrwx 1 root root 9 May 13 03:23 cf5d6692-4176-47c4-b799-039c11103fd4 -> ../../vdd
```

The resulting `/etc/fstab` entry is in the following example.

```
$ UUID=cf5d6692-4176-47c4-b799-039c11103fd4 /usr/sap xfs defaults 0 0
```

You need to create the mount point and mount it.

```
$ [root@sap-app-vsi ~]# mkdir /usr/sap  
[root@sap-app-vsi ~]# mount -a
```

On the database virtual server, you need to create three file systems. One for the RDBMS installation and two for `/usr/sap` and `/sapmnt`. Both attached volumes are created the same way and display as `/dev/vdb` and `/dev/vde`. In our example, we split the first file system in two partitions.

```
$ [root@sap-app2-vsi ~]# /sbin/fdisk /dev/vdb  
Welcome to fdisk (util-linux 2.23.2).  
Changes will remain in memory only, until you decide to write them.  
Be careful before using the write command.  
Device does not contain a recognized partition table  
Building a new DOS disklabel with disk identifier 0x8f5f8b5e.  
Command (m for help): n  
Partition type:  
p primary (0 primary, 0 extended, 4 free)  
e extended  
Select (default p): p  
Partition number (1-4, default 1): 1  
First sector (2048-419430399, default 2048):  
Using default value 2048  
Last sector, +sectors or +size{K,M,G} (2048-419430399, default 419430399): +100G  
Partition 1 of type Linux and of size 100 GiB is set  
Command (m for help): n  
Partition type:  
p primary (1 primary, 0 extended, 3 free)  
e extended  
Select (default p): p  
Partition number (2-4, default 2):  
First sector (209717248-419430399, default 209717248):  
Using default value 209717248  
Last sector, +sectors or +size{K,M,G} (209717248-419430399, default 419430399):  
Using default value 419430399  
Partition 2 of type Linux and of size 100 GiB is set  
Command (m for help): w  
The partition table has been altered!  
Calling ioctl() to re-read partition table.  
Syncing disks.
```

Create the three file systems (output isn't shown in this example).

```
$ [root@sap-app2-vsi ~]# mkfs.xfs /dev/vdb1  
[root@sap-app2-vsi ~]# mkfs.xfs /dev/vdb2  
[root@sap-app2-vsi ~]# mkfs.xfs /dev/vde  
[root@sap-app2-vsi ~]# mkdir /usr/sap /sapmnt /db2
```

Again, you need to determine the `/dev/disk/by-uuid` paths, as previously shown, and maintain `/etc/fstab` entries. As a final step, you need to set up the NFS to install SAP.

1. Install the NFS utilities on both virtual servers.

```
$ [root@sap-app-vsi ~]# yum install nfs-utils
```

```
$ [root@sap-app2-vsi ~]# yum install nfs-utils
```

2. Start the NFS server on the database virtual server.

```
$ [root@sap-app2-vsi ~]# systemctl enable nfs-server  
[root@sap-app2-vsi ~]# systemctl start nfs-server
```

3. Use NFS to export /sapmnt and /usr/sap/trans from the database server to the application server by adding the required entry to /etc(exports of the database server:

```
$ /sapmnt/C10 10.243.129.0/24(rw,no_root_squash,sync,no_subtree_check)  
/usr/sap/trans 10.17.139.0/24(rw,no_root_squash,sync,no_subtree_check)
```

You need to adapt the subnet in the previous example to your actual IP range and subnet mask. Replace the value **C10** with the SAP System ID for your SAP system. **C10** is a sample value. You must create the directory before you export it.

4. Run on the following command from the command line.

```
$ [root@sap-app2-vsi ~]# mkdir /sapmnt/C10  
[root@sap-app2-vsi ~]# mkdir -p /usr/sap/trans  
[root@sap-app2-vsi ~]# exportfs -a
```

5. Mount the NFS share on the application server by adding the following entry to its **/etc/fstab** and mount the application server from the command line by using the following command.

```
$ [root@sap-app-vsi ~]# vi /etc/fstab  
...  
sap-app2-vsi-priv:/sapmnt/C10 /sapmnt/C10 nfs defaults 0 0  
sap-app2-vsi-priv:/usr/sap/trans /usr/sap/trans nfs defaults 0 0
```

6. Create and mount the target directory.

```
$ [root@sap-app-vsi ~]# mkdir /sapmnt/C10  
[root@sap-app-vsi ~]# mkdir /usr/sap/trans  
[root@sap-app-vsi ~]# mount /sapmnt/C10  
[root@sap-app-vsi ~]# mount /usr/sap/trans
```

Your servers are now prepared to host the components of a distributed SAP installation. For more information about more installation preparations, see [Downloading and installing SAP software and applications](#).

Step 8: Installing your SAP landscape

RPM package prerequisites

An SAP installation requires that certain prerequisites are met regarding the packages that are installed on the OS and the OS daemons that are running. See the latest installation guides and support notes from SAP for an up-to-date list of these prerequisites. Currently, the following extra packages are required for an SAP NetWeaver installation: - **compat-sap-c++-7**: Achieves compatibility of the C++ runtime with the compilers that are used by SAP - **uuidd**: Maintains OS support for the creation of UUIDs - **csh**: C shell support for the OS

1. Follow [SAP note 2195019](#) and install package **compat-sap-c++-7**. Create a specific soft-link, which is required by the SAP binary files.

```
$ [root@sap-app-vsi ~]# yum install compat-sap-c++-7  
...  
[root@sap-app-vsi tmp]# mkdir -p /usr/sap/lib  
[root@sap-app-vsi tmp]# ln -s /opt/rh/SAP/lib64/compat-sap-c++-7.so /usr/sap/lib/libstdc++.so.6
```

2. Check if uuid daemon (uuidd) is installed. If it's not, install and start it.

```
$ [root@sap-app-vsi ~]# rpm -qa | grep uuidd  
[root@sap-app-vsi ~]# yum install uuidd  
[root@sap-app-vsi ~]# systemctl enable uuidd  
[root@sap-app-vsi ~]# systemctl start uuidd
```

3. Install the tcsh package required for C shell support

```
$ [root@sap-app-vsi ~]# yum install tcsh
```

Installing the IBM Cloud Metrics Collector for SAP

SAP requires the installation of the IBM Cloud Metrics Collector for SAP to analyze your infrastructure if a support case is submitted. Install the collector by using the instructions in [IBM Cloud Metrics Collector for SAP](#).

Downloading your SAP software

Log in to SAP for Me [Download Software](#) and download the required digital versatile discs (DVDs) to a local share drive and then transfer the DVDs to your provisioned server. Alternative option, download the SAP Software Download Manager, install it on your target server and directly download the DVD images to the server. For more information about the SAP Software Download Manager, see [SAP Download Manager](#).

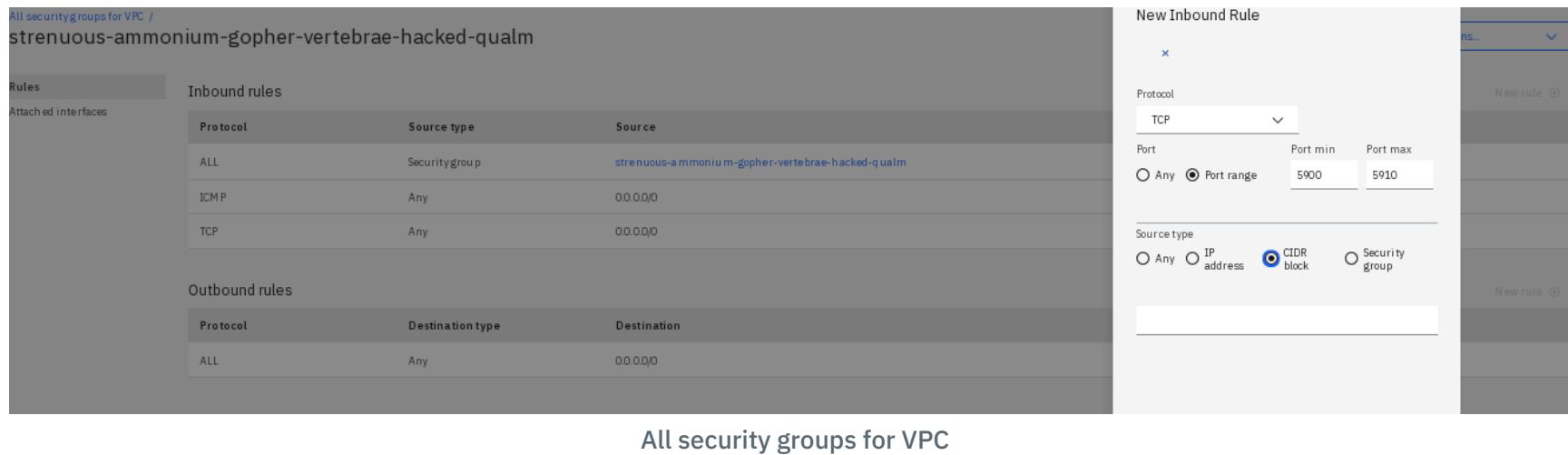
 **Note:** You need an S-User ID and the Download Software authorization when you download the DVDs from the SAP Service Marketplace. To request an S-User ID, see the [SAP Support Portal](#).

Preparing for SAP's Software Provisioning Manager (SWPM)

Depending on your network bandwidth and latency, you might need to run the SAP SWPM GUI remotely in a virtual network computing (VNC) session. Another option is to run GUI locally and connect it to SWPM on the target machine. For the first option, you must run X11 in your virtual server and install a VNC server and a browser. You can run the browser locally on your desktop, and connect to SWPM in the virtual server. To connect to SWPM, check the port that SWPM is listening on. SWPM displays the port during startup when it lists the access URL. The port, typically 4237, needs to open in the security group of your VPC. You need to add a **New Inbound rule** for your IP source range (or 0.0.0.0/0) and the port number. Another possibility, and even more secure, is to tunnel the port through `ssh`.

```
$ [root@sap-app-vsi ~]# ssh -L 4237:localhost:4237 <your virtual server IP>
```

-L option for local tunnels and connecting your browser to that localhost port, instead of the remote IP. Remember to add the ports that are required by your SAP application (example: ports 3200-3299, depending on your SAP NetWeaver instance number) to the security group. For more information about ports, see [SAP ports](#) for details.



Installing SAP software

After you download the installation media, follow the standard SAP installation procedure that is documented in the [SAP installation guides](#) for your SAP version and components. Also, review the corresponding SAP notes. See more detailed information about SAP NetWeaver installation that uses Db2 as the RDBMS in [Considerations about IBM Db2](#).

Relevant SAP Notes

- [SAP Note 2002167 - Red Hat Enterprise Linux 7.x: Installation and Upgrade](#).
- [SAP Note 2923773 - Linux on IBM Cloud \(IaaS\): Adaption of your SAP License](#).

SAP NetWeaver deployment to Intel Virtual Server on VPC Infrastructure that uses Windows Server

 **Note:** A Quick Study, someone who is able to learn new things quickly.

These Quick Study Tutorials provide a single sample configuration, with less detailed instructions, as an introduction for customers who prefer hands-on tasks to increase their pace of learning.

The following information provides an introduction for customers who are new to IBM Cloud® Virtual Private Cloud (VPC) environment. Two

sample configurations are provided to help you through the ordering process to the start of the SAP installation.

The first configuration sample is simple, a single node 128 GB, 32 vCPU virtual server instance (VSI). The second is an advanced configuration of two nodes by adding a second VSI to the landscape. The sample layouts might not be your preferred layout. The purpose of this guidance is to show you two possibilities if you are not experienced with the Windows® operating system or with VPC.

Although we want to start quickly, you first must be able to log in to IBM Cloud and make sure that you have access to important SAP resources.



Note: This tutorial contains instructions to complete the deployment - a detailed explanation of the navigation through the IBM Cloud console and all available options that you can use, you find in the topic [Deploying your infrastructure](#).

Step 1: Securing Access

Security is one of the biggest concerns when you run your business-critical applications in a cloud environment. To secure your connection to your IBM® Virtual Servers, a public SSH key can be uploaded to your account, per region. These public keys are deployed to your VSIs to allow access to them.



Tip: Before you continue, create an SSH public key that you can upload later to the region of your choice when you are creating the VSI. Follow the steps that are [documented here](#). Store your public and private key on your client computer - usually, in Linux® environments it is located in the `~/.ssh` folder.

You use security groups to restrict access to and from IP ranges, protocols, and ports. The default security group that is deployed with your sample VPC can suffice. However, you might have to add extra ports for exceptions to the access restrictions, such as the SAP Software Provisioning Manager and for the ports that are being used by your SAP NetWeaver based application.

Step 2: Creating an IBM Cloud VPC and subnet

IBM Cloud® compute resources are kept in a global region within a VPC. Use the following steps to create a VPC and its subnet.

1. Log in to the [IBM Cloud console](#) with your unique credentials.
2. Click **Menu icon** > **VPC Infrastructure** > **Network** > **VPCs**
3. Click **Create**.
4. Enter a unique **Name** for the VPC, for example, `sap-test-vpc`.
5. Select a **Resource group**. Use resource groups to organize your account resources for access control and billing purposes. **Leave the value default**.
6. *Optional: Tags.* Enter tags to help you organize and find your resources. For example, `sap quick guide`.
7. Select whether the **Default security group** allows inbound SSH and ping traffic to VSIs in this VPC. **Leave the value default**.
8. *Optional: Classic access.* Select whether you want to enable your VPC to access classic infrastructure resources. **Leave the value default**.
9. *Optional: Default address prefixes.* If you do disable this option, the **New subnet for VPC** section will be hidden, and will require manual definition after the VPC is created. **Leave the value default**.

New subnet for VPC

1. Enter a unique **Name** for the VPC subnet, for example, `sap-test-net`.
2. Select a **Resource group** for the subnet. **Leave the value default**.
3. Select a **Location** for the subnet. The location consists of a region and a zone.



Tip: The region that you select is used as the region of the VPC. All additional resources that you create in this VPC are created in the selected region.

4. Enter an **Address prefix**, **Number of addresses**, and an **IP range** for the subnet. **Leave the value default**.
5. *Optional: Public gateway.* **Leave the value default**.
6. Click **Create virtual private cloud** on the right.

Step 3: Creating a Virtual Server Instance

Use the following steps to create a virtual server instance.

1. Click **Virtual server instances > New instance**.
2. Enter a unique **Name** for the virtual server, for example, *sap-wdb*. The name that you enter becomes the hostname.



Important: SAP hostnames must consist of a maximum of 13 alpha-numeric characters. See [SAP Note 611361](#) for further details.

3. Select the **Virtual private cloud** in which to attach the VSI, for example, *sap-test-vpc*.
4. Keep the **Resource group** default.
5. *Optional:* **Tags**. For example, *sap quick guide*.
6. Leave the selected **Location** in which you created your subnet
7. Select **Windows Server > 2016 Standard Edition** as the *Operating System*.
8. Click **All profiles > Balanced** and select *bx2-32x128*.

For more information about SAP-certified profiles, see [Intel Virtual Server certified profiles for SAP NetWeaver](#).

Setting an SSH key

If you uploaded your public key for the VPC's region, select it and skip to the next section (Attaching storage). Otherwise, follow these steps.

1. Click **New key**.
2. Enter a unique **Name**, for example, *sap-ssh-key*.
3. Keep the default **Resource group**.
4. The **Region** in which you created your subnets is already selected.
5. *Optional:* **Tags**. For example, *sap quick guide*.
6. Paste the **Public key**, that you created according to [the guidelines mentioned in Securing Access](#).
7. Click **Add SSH key**.
8. *Optional:* **User data**. Leave blank.

Attaching a block storage volume

To have file system space available beyond what is required by the operating system, you need to attach a block storage volume to your VSI. This storage volume is used by the application that you're installing. In this example, the application is the Relational Database Management System (RDBMS) required for an SAP NetWeaver stack.

1. Click **New volume**.
2. Enter *sap-db-vol* for **Name**.
3. Select *Custom* for **Profile**.
4. Enter *500* for **Size**.
5. Enter *10000* for **IOPS**. **Throughput** defaults to *156.25 MiBps*.
6. Keep the **Encryption** and **Auto Delete** defaults.
7. Click **Attach**.
8. Keep the **Networking** default.
9. Keep the **Network interfaces** default.
10. Click **Create virtual server instance**. After the Windows instance is provisioned and ready, you need to retrieve the *Administrator* password and connect to it.

Step 4: Connecting to your Windows VSI

To be able to connect to the Windows VSI from your client, you need the *Administrator* password and a public IP address. The password is retrieved by the IBM Cloud command-line interface (CLI) whereas the public IP address - it is called *Floating IP* - can be created with the IBM

Cloud console.

Install CLI

Before you can use the CLI to retrieve the *Administrator* password, you must [install the IBM Cloud CLI](#) and [the VPC CLI plug-in](#).

Connect to IBM Cloud with the CLI

Log in to IBM Cloud with your IBMID. If you have multiple accounts, you are prompted to select which account to use.

```
$ ibmcloud login
```

Tip: If your credentials are rejected, you might be using a federated ID. To log in with a federated ID, use the `--sso` flag. See [Logging in with a federated ID](#) for more details.

Set the target region (DC)

List the regions using command

```
$ ibmcloud regions
```

Target the region using command

```
$ ibmcloud target -r eu-de
```

Get the instance ID

```
$ ibmcloud is ins
```

Find the instance ID that is assigned to your VSI *sap-wdb*.

Retrieve the Administrator password

```
$ ibmcloud is instance-initialization-values <instance ID> --private-key @sap-ssh-key
```

Take note of the password.

Set the floating IP

To quickly access the deployed instance, you can assign a *Floating IP* to your VSI. To add this IP to your server, complete the following steps:

1. In the IBM Cloud console, go to **Menu icon**  > **VPC Infrastructure** > **Compute** > **Virtual server instances**.
2. Click the name of the Windows VSI - *sap-wdb*.
3. On the Instance details page, find the **Network interfaces** section.
4. By default, the first interface is named *eth0*.
5. Click the pencil icon to edit the primary network interface.
6. On the **Edit network interface** page, locate the **Floating IP address** field. You can select **Reserve a new floating IP** or you can select an existing floating IP address.
7. After you make your selection, click **Save**.
8. You might note the *Floating IP address* or back in the **virtual server instances list** you can click it and copy it into the clipboard.

You can now log in to the virtual instance and begin preparing it for the SAP NetWeaver workload installation.

Step 5: Preparing the virtual server instance for your workload

 **Important:** In this tutorial, we simplify the process and use sample VSI profiles, volume and pagefile sizes. In a production-ready environment, of course, you need to size the servers and the volumes according to the number of concurrent users and the expected amount of data and further parameters. Find more in the topic [Sizing process for SAP Systems](#).

Depending on the database vendor you should consult their specific documentation, recommendations and best practices how to setup the file systems. You may start here.

- [IBM Db2](#)
- [SAP MaxDB](#)
- [SAP ASE](#)

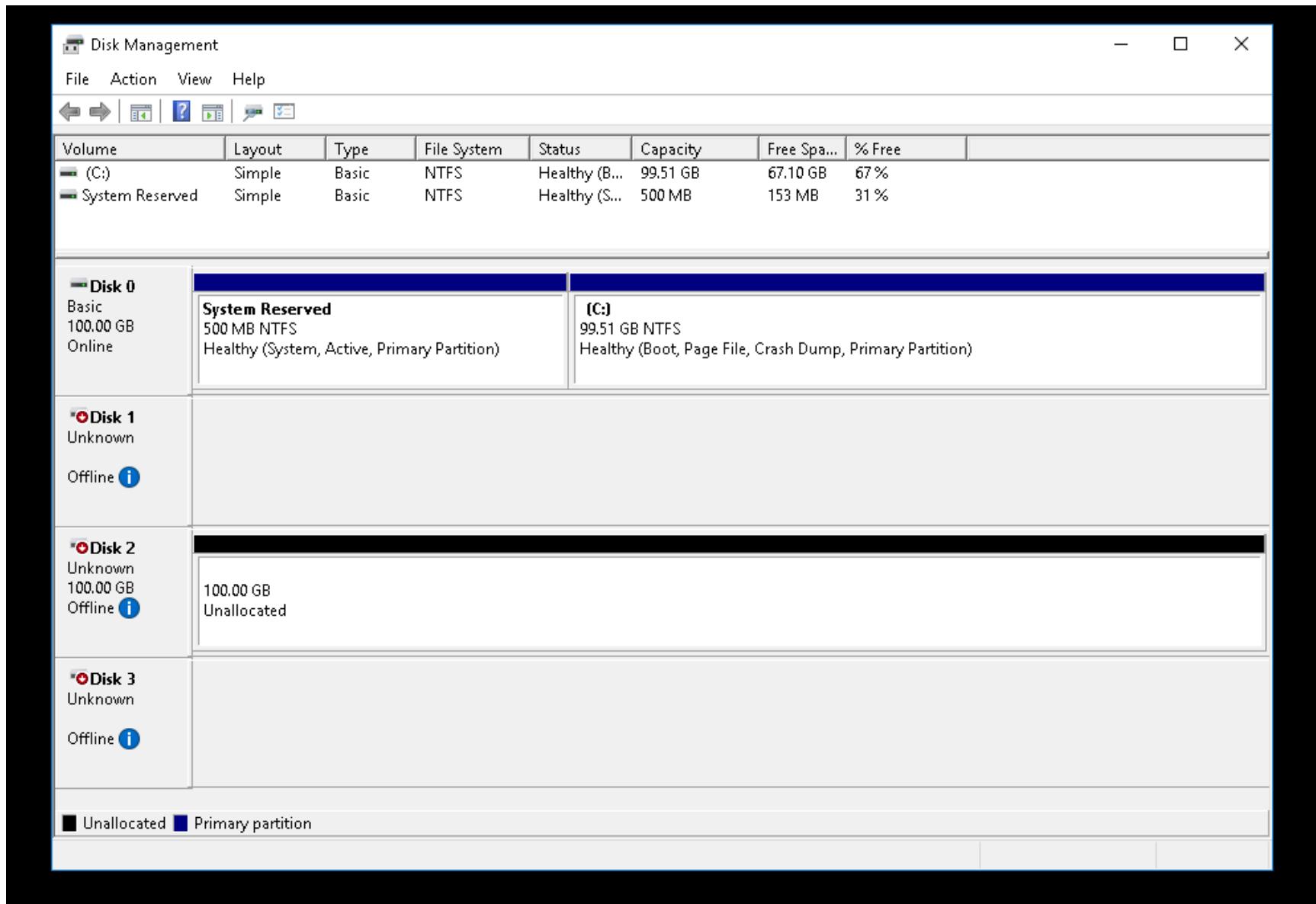
We let `sapinst`, the SAP installation program, care about the user management, the disk partitioning as well as folder and subfolder creations that are required for the SAP application and the RDBMS.

Logging in to your Windows VSI

You can access the newly created VSI with Windows Remote Desktop. Enter the *Floating IP* and the *Administrator* password that you retrieved during the steps that are described previously.

Initializing the block storage for Windows disk usage

1. Start the Windows Server **Disk Management**



Windows Server Disk Manager

1. Find the block storage - usually it is Disk 2 and shows the ordered size and the status *offline*
2. Right-click the Disk tile and select **online** from the menu
3. Again right-click the Disk tile and select **Initialize Disk** from the menu, check to make sure that the correct disk is selected, select **GPT** as the default partition style - see footnote (+) below - and click **Ok**
4. Now right-click the related tile to the right that shows *Unallocated* and select **New Simple Volume...**
5. Click **Next** twice, which retains the default value for the disk size and then specify your preferred drive letter, or leave the default and click **Next**
6. Overwrite the **Folder Name**, for example, **SAP** and leave the other default values and click **Next** - note, that **File System** **FAT32** is NOT SUPPORTED for SAP applications
7. Check the values and click **Finish**
8. After the volume has been prepared and formatted, you can find the new disk in the Windows Explorer

(+) [About partition styles - GPT and MBR.](#)

Specifying the page file

1. Start the Windows Control Panel

2. Click **System and Security** then **System**
3. Click **Advanced system settings**
4. Click the tab **Advanced** then in Section **Performance** the button **Settings...**
5. Click the tab **Advanced** then in Section **Virtual memory** the button **Change...**
6. Deselect the check mark **Automatically manage...**
7. Select drive C: and click **Custom size**
8. Enter Initial size and Maximum size **32768**, click **Set** and **Ok**

Your next step is to [download and install your SAP software and applications](#) if a single virtual server sample is sufficient for your needs.

Step 6: Installing two virtual server instances in a 3-tier setup

A more complex scenario involves installing two virtual servers. One server is the SAP NetWeaver Application Server (*sap-wapp*) and the other server (*sap-wdb*) is the database server for SAP NetWeaver. You can reuse the server *sap-wdb* that you provisioned in the previous sections and create the application server *sap-wapp* as described in sections [Creating a Virtual Server Instance](#) and [Attaching a block storage volume](#) previously, except that you use the **Balanced profile** *bx2-8x32* and 20 as **Size** for data volume *sap-app-vol*. Also, follow the steps to retrieve the *Administrator* password of the new VSI.

Both VSIs have one extra attached volume and a *Floating IP*. A smaller volume is attached to *sap-wapp*, which is the SAP primary application server (PAS). *sap-wdb* has a larger volume to host the RDBMS and the SAP Central Services (ASCS) instance.

The top screenshot shows the 'Virtual server instances' list in the IBM Cloud interface. It lists two VSIs: 'sap-app-vsi' and 'sap-app2-vsi', both powered on, located in 'sap-test-vpc', using profile 'bx 2-3 2x128', and having private IPs 10.243.128.7 and 10.243.128.9 respectively. The bottom screenshot shows the 'Block storage volumes for VPC' page for the 'sap-app2-vol2' volume. It displays volume details like name, size (200 GB), profile (10 IOPS/GB), and throughput (4688 MiBps). The 'Attached instances' section shows no instances attached to this volume. A modal window is open, titled 'Attach virtual server instance', with a dropdown menu showing 'sap-app2-vsi'. At the bottom right of the modal is a blue button labeled 'Attach volume'.

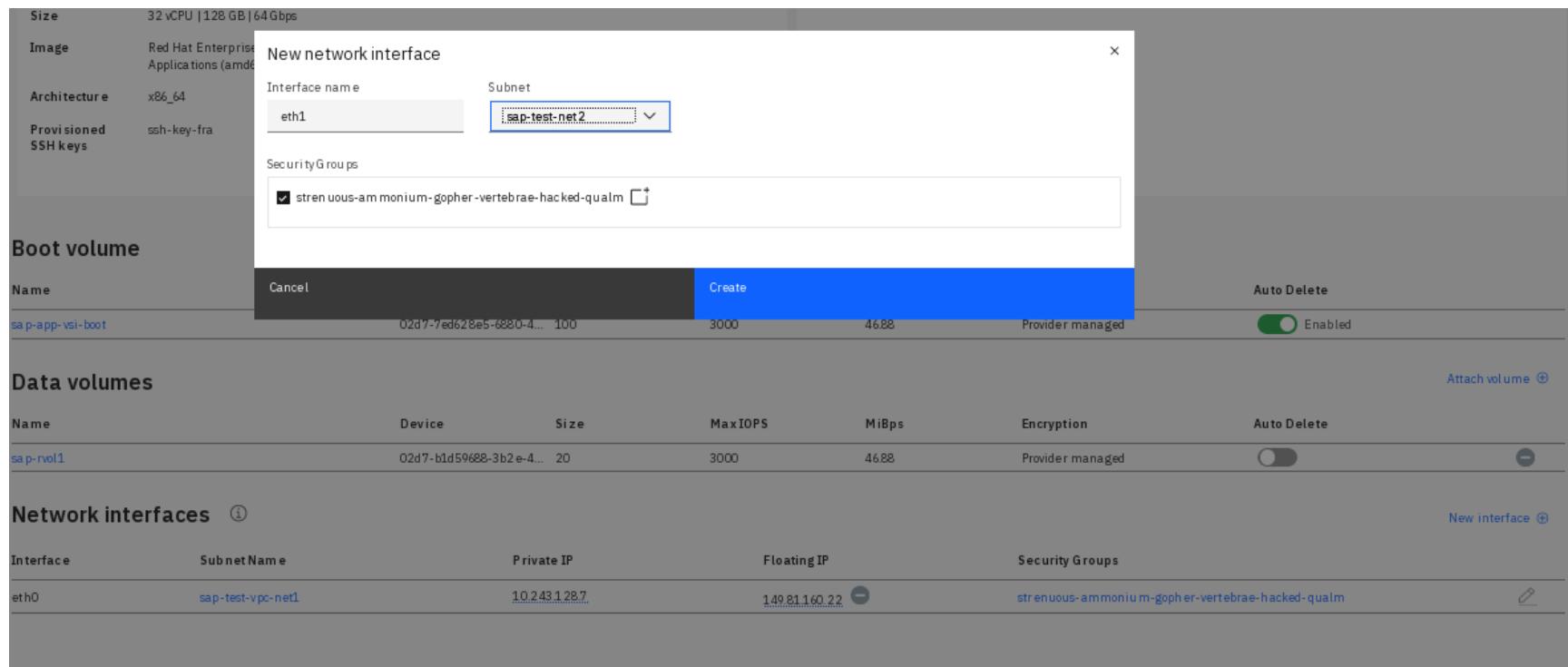
Step 7: Preparing your network

To segregate network traffic, as recommended by SAP, deploy a second subnet. One network is used for client access, the other for communication between the SAP ABAP stack and the RDBMS.

Follow the steps in the section [New subnet for VPC](#) but use the **Name** *sap-test-net2*. After the new subnet is created, it will show on the Subnets for VPC page.

The two VSIs need to connect to the new network.

1. Go to the VSIs details overview and on each click **New interface**.
2. Select **eth1** as **Interface name**.
3. Select **sap-test-net2** as **Subnet**.
4. Leave the other values default and click **Create**.



Data volumes

Maintain your **hosts** files on both servers according to the targeted setup. Usually you find it in the following path:

`C:\Windows\System32\drivers\etc\hosts`

Note: In this tutorial that installs a prototypical SAP System, we do not specify a Windows domain. Usually, if you configure a server for your company's access, you would specify the domain in the **hosts** file. During the SAP installation, you turn off the **FQDN** option and leave the domain name blank.

The following example is for the server instance `sap-wdb`.

```
$ 10.243.128.9 sap-wdb
10.243.129.6 sap-wdb-priv
10.243.128.7 sap-wapp-win
10.243.129.4 sap-wapp-priv
```

Your VSIs are now prepared to host the components of a distributed SAP installation. For more information about more installation preparations, see [Downloading and installing SAP software and applications](#).

Step 8: Installing your SAP landscape

Installing the IBM Cloud Metrics Collector for SAP

SAP requires the installation of the IBM Cloud Metrics Collector for SAP to analyze your infrastructure in the event that a support incident has been submitted. Install the collector by using the instructions in [IBM Cloud Metrics Collector for SAP](#).

Downloading your SAP software

Note: You need an S-User ID and the Download Software authorization when you download the DVD images from the SAP Service Marketplace. To request an S-USer ID, see the [SAP Support Portal](#).

Depending on your target SAP application that you are going to install you need to gather information, which SAP images you will need to download. In this tutorial, we are choosing SAP NetWeaver ABAP on Windows using IBM Db2 for the SAP Database. Therefore we find in this guide [SAP NetWeaver Installation Guide](#) all the needed information. SAP recommends to always search for the most recent versions.

Log in to SAP for Me [Download Software](#) and download the required digital versatile discs (DVDs) to a local share drive and then transfer the DVDs to your provisioned server. Alternative option, download the SAP Software Download Manager, install it on your target server and directly download the DVD images to the server. For more information about the SAP Software Download Manager, see [SAP Download Manager](#).

Preparing for SAP's Software Provisioning Manager (SWPM)

SWPM is the component that guides you through the steps to successfully prepare and complete an SAP installation. Together with the other required images you may store and unpack SWPM on an extra file share that you then can attach to several VSIs on which you want to install SAP workloads.

Installing SAP software

Follow the instructions in the [SAP NetWeaver Installation Guide](#). Also, review the corresponding SAP notes. See more detailed information about SAP NetWeaver installation that uses Db2 as the RDBMS in [Considerations about IBM Db2](#).

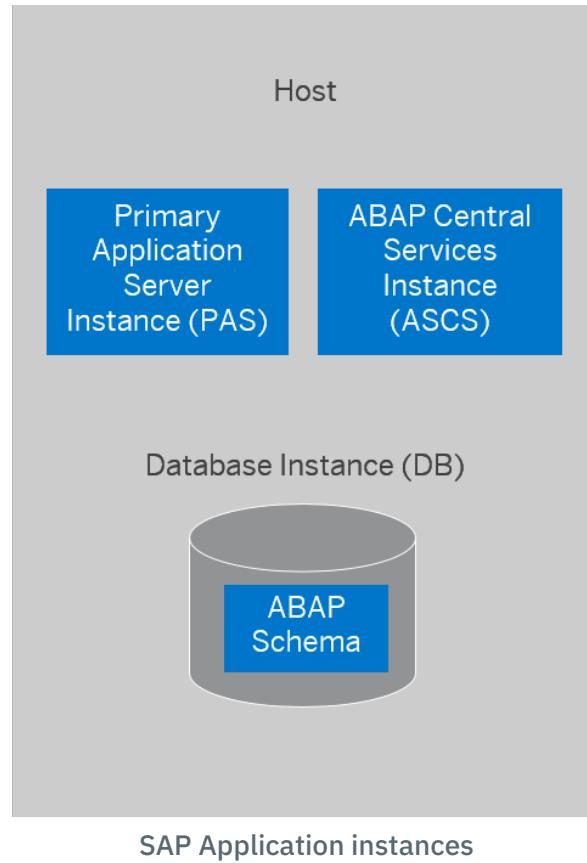


Figure 2 illustrates the basic SAP instances that will be installed to deploy the SAP NetWeaver ABAP application server onto one host. If you now want to complete the single server instance - i.e. just using VSI `sap-wdb`, you need to launch `sapinst` only one time on that server. In this case, you will first install the ABAP Central Services Instance (ASCS), then the Database Instance DB and finally the Primary Application Server (PAS).

If you go for the more complex implementation, a distributed SAP System, you will need to launch `sapinst` on `sap-wdb`, install the ASCS and the DB and then run `sapinst` on `sap-wapp` to install the PAS. Then, it is necessary that you open specific ports to allow inter-application communication between the application server and the database server. To accomplish this, you must use Windows Firewall tool.

1. Start **Windows Firewall with Advanced Security** - enter `wf.msc` in Windows search field
2. Click **Inbound Rules** then **Action** and **New rule...**
3. Click Rule Type **Port** and **Next**
4. Enter the ports that need to be opened (see below)
5. Click Action **Allow the connection** and **Next**
6. Click Profile **Public** to unselect this option and **Next**
7. Enter a name and optionally a description and click **Finish** (see below)

Example values are e.g. depending on the instance numbers that you have chosen:

Ports	Name
3000-3999	SAP
5912-5917	Db2
40000-40099	IGS
50000-50099	sapstartsrv

Port mapping



Note: In a production environment you will get more granular on the port numbers. For more information about ports, see [SAP ports](#) and the respective documentation of your database vendor for details.

If you run SAP GUI on your desktop, remember to add the ports that are required by your SAP application (example: ports 3200-3299, depending on your SAP NetWeaver instance number) to the security group.

Finding more information

Leaving now the tutorial and finding all information that you need to install your specific SAP components and versions, visit the [SAP Help Portal](#) as a starting point.

Relevant SAP Notes

- [SAP Note 2384179 - SAP Systems on Windows Server 2016](#).
- [SAP Note 2979010 - Windows on IBM Cloud \(IaaS\): Adaption of your SAP License](#).

Memory Management

- [SAP Note 88416 - Zero administration memory management for the ABAP server](#).
- [SAP Note 1518419 - Page file and virtual memory required by the SAP system](#).
- [SAP Note 2488097 - FAQ: Memory usage for the ABAP Server on Windows](#).

Troubleshooting

- [SAP Note 100972 - Windows bug check event \(blue screen\)](#).
- [SAP Note 1559353 - How to capture user dumps on Windows](#).
- [SAP Note 2015747 - How to generate Windows crash dump files](#).

SAP NetWeaver deployment to Bare Metal on Classic Infrastructure, using RHEL



Note: A Quick Study, someone who is able to learn new things quickly.

These Quick Study Tutorials provide a single sample configuration, with less detailed instructions, as an introduction for customers who prefer hands-on tasks to increase their pace of learning.

The following information provides an introduction for customers who are new to the Classic Infrastructure environment. Two sample configurations are provided to help you through the ordering process to the start of the SAP installation.

The first configuration sample is a simple, single node 32 GB RAM server with Red Hat Enterprise Linux® (RHEL). The second is an advanced two node configuration that adds a second virtual server of 192 GB RAM with Red Hat Enterprise Linux (RHEL) to the landscape.

An example of how to set up external storage, which can be applied to either sample configuration, is also provided.

The sample layouts might not be your preferred layout. The purpose of this guidance is to show two possibilities. Your installation should follow your business requirements and SAP installation documentation.

Step 1: Provisioning a 32 GB server for a single-host environment

1. Log in to the [IBM Cloud console](#) with your unique credentials.
2. Click **Create > Compute > Infrastructure > Bare Metal Server**.
3. Click **Continue**. If you can't click **Continue**, you don't have the correct permissions to create a server. Check with your system administrator about your permissions.
4. Leave **1** in the **Quantity** field.
5. Enter **e2e1270** in the **Hostname** field. Hostname is a permanent or temporary name for your servers. Click **Information** for formatting specifics.
6. Enter **mycloud.com** in the **Domain** field. Domain is the identification string that defines administrative control within the internet. Click **Information** for formatting specifics.
7. **Billing** defaults to *Monthly*. Currently, 1-year contract and 3-year contract are not available for SAP-certified servers.
8. The data centers displayed under **Location** depend on product availability within a particular data center. Select *NA East TOR01-Toronto*.
9. Click **All servers > SAP certified**.

Configuring your server

1. Select **CPU Model BI.S3.NW32 (OS Options)**. For more information about how to decipher the server names, see [Provisioning your Bare Metal Servers using the IBM Cloud console](#).

2. **RAM** defaults to a predefined value based on your server selection and cannot be changed.
3. Enter an optional public key for your **SSH key**, which you can use to log in to your server after the server is provisioned. The default is *None*.
4. Select *Red Hat* as your **Image** (OS). The default is *7.x (64 bit)*.



Note: If you're bringing your own license (BYOL) for your OS, select *No OS*. For more information, see [Bring your own license](#).

Adding storage disks

1. Under **Type**, select *RAID 10*.
2. **Disks**, **Hot Spare**, and **Disk Media** have default values. Select a **Disk size** that covers the total amount of storage you need.
3. Click the Menu icon > **Advanced configuration** and leave **Controller** cleared. Click **OK**.

Network interface

1. Select *1 Gbps Redundant Public and Private Network Uplinks* for **Uplink Port Speed**.
2. Select the values in Table 1 for the following fields:

Field	Value
Private VLAN	tor01.bcr01a.1241
Public VLAN	tor01.fcr01a.851
Private Subnet	10.114.63.64/26
Public Subnet	158.85.65.224/28

32 GB network interface values

3. Leave the default values for all other fields.
4. Review your Order Summary.
5. Click **I read and agree to the following Third-Party Service Agreements**.



Note: You can create your server, save the order as a quote to provision later, or add the order to an estimate, which might include multiple services.

6. Click **Create** to be redirected to the Checkout page after your order is verified.

You are redirected to a page with your order number. The page is your order receipt; print a copy for your records. You also receive a confirmation email with the subject *Your IBM Cloud Order ## has been approved*. The ## is your order number.

Depending on your order, server is available for use within one to four hours after your order is submitted. You can check the Device Details from the IBM Cloud console (Menu icon > Resource List > Devices) for the status of the provisioning steps. Click the **Device Name** that matches your device's Hostname and Domain to see its status.

Bring your own license

If you have your own operating system license, you install it on your Bare Metal Servers based on the vendor's instructions. For more information, see [The no OS option](#).

Access your server

A public IP is used for remote access, so you can connect to your server through an **ssh** client (for example, PuTTY on Microsoft Windows). Use the public IP address displayed in the Device List (under the **Devices** menu) for your device. The root password for your server is also displayed. Click **Show Password** to see it.

Partitioning and file systems

For the single-node example, you ordered a server with one logical disk (on RAID 1). The server has one mirrored disk with the operating

system (OS) and one large root file system equal to the total size of the disk (with some space used for `/boot`). The file system layout in this example is just one possible approach. For production use, follow the sizing information for your system as other layouts might better meet your needs or SAP requirements.

1. Create the three directories required for the SAP installation, `/sapmnt`, `/usr/sap`, and `/db2`.

```
$ [root@e2e1270 ~]# mkdir /sapmnt
[root@e2e1270 ~]# mkdir /usr/sap
[root@e2e1270 ~]# mkdir /db2
```

Your IBM Cloud® Bare Metal Servers is now ready for external storage and the installation of your SAP applications and software.

Step 2: Provisioning 192 GB and 32 GB servers for a three-tier environment

A three-tier environment is a more complex scenario using a 192 GB server as the database server and a 32 GB server as the SAP NetWeaver application server.

Ordering your SAP NetWeaver Application Server

Follow the same steps in [Provisioning a 32 GB server for a single-host environment](#) to order the SAP NetWeaver Application Server.

Ordering your Database Server

Use the following steps to order an SAP-certified server as your database server.

1. Log in to the [IBM Cloud® console](#)) with your unique credentials.
2. Click **Create resource > Compute > Bare Metal Server**.
3. Click **Continue**. If you can't click **Continue**, you don't have the correct permissions to create a server. Check with your system administrator about your permissions.
4. Leave **1** in the **Quantity** field.
5. Enter **sdb192** in the **Hostname** field. Hostname is a permanent or temporary name for your servers. Click **Information** for formatting specifics.
6. Enter **mycloud.com** in the **Domain** field. Domain is the identification string that defines administrative control within the internet. Click **Information** for formatting specifics.
7. **Billing** defaults to *Monthly*. Currently, 1-year contract and 3-year contract are not available for SAP-certified servers.
8. The data centers displayed under **Location** depend on product availability within a particular data center. Select **NA East, TOR01-Toronto**.
9. Click **All servers > SAP certified**.

Configuring your Database Server

Use the following steps to configure your database server and OS.

1. Select **CPU Model BI.S3.NW192 (OS Options)**. For more information about how to decipher the server names, see [Provisioning your Bare Metal Servers using the IBM Cloud console](#).
2. **RAM** defaults to a predefined value based on your server selection and cannot be changed.
3. Enter an optional public key for **SSH key**, which you can use to log in to your server after the server is provisioned. The default is **None**.
4. Select **Red Hat** as your **Image** (OS). The default is **7.x (64 bit)**.



Note: If you're bringing your own license (BYOL) for your OS, select **No OS** as your image. For more information, see [Bring your own license](#).

Adding storage disks

Use the following steps to add a second 2 TB SATA drive to your database server.

1. For **Disk 1**, click the Menu icon > **Advanced configuration** > and verify that Primary disk partition** is set to the default of **Windows Basic**. Click **OK**.
2. Click **Add new**.

3. **Disks, Hot Spare**, and **Disk Media** have default values. Select a **Disk Size** that covers the total amount of storage you need.

Setting up the network interface

Use the following steps to set up the network interface for your database server.

1. Select *1 Gbps Redundant Public & Private Network Uplinks* for **Uplink Port Speed**.
2. Select the values in Table 1 for the following fields:



Note: Make sure the network interface values for your database server match the values of your application server.

Field	Value
Private VLAN	tor01.bcr01a.1241
Public VLAN	tor01.fcr01a.851
Private Subnet	10.114.63.64/26
Public Subnet	158.85.65.224/28

192 GB network interface values

3. Leave the default values for all other fields.
4. Review your Order Summary.
5. Select **I read and agree to the following Third-Party Service Agreements**.



Note: You can create your server, save the order as a quote to provision later, or add the order to an estimate, which might include multiple services.

6. Click **Create** to be redirected to the Checkout page after your order is verified.

You are redirected to a page with your order number. The page is your receipt; print the page for your records. You also receive a confirmation email with the subject *Your IBM Cloud Order ## has been approved*. The ## is your order number.

Depending on your order, the server is available for use within one to four hours after the order is submitted. You can check Device Details from the IBM Cloud console (Menu icon > Resource List > Devices) for the status of the provisioning steps. Click the **Device Name** that matches your given Hostname and Domain to see its status.

Bring your own license

If you have your own operating system license, you install it on your Bare Metal Servers based on the vendor's instructions. For more information, see [The no OS option](#).

Access your server

A public IP is used for remote access, so you can connect to your server through an client (for example, PuTTY on Microsoft Windows). Use the public IP address displayed in the Device List (**Classic Infrastructure > Devices**) for your device. The root password for your server is also displayed. Click **Show Password** to see it.

Partitioning and file systems

For the three-tier example, a 192 GB database server with one logical disk (on RAID10) and a 32 GB application server with one logical disk (on RAID 1) were ordered. Both servers come with one large root file system that is equal to the total size of disk (with some space that is used for .

For the 32 GB server, create the file system. The file systems and are created on the database server. The Network File System (NFS) is exported from the database server, which also hosts the Advanced Business Application Programming (ABAP) SAP Central Service [(A)SCS] instance.

The following file system layout is one possible approach. For production use, you might follow the sizing information for your system as other

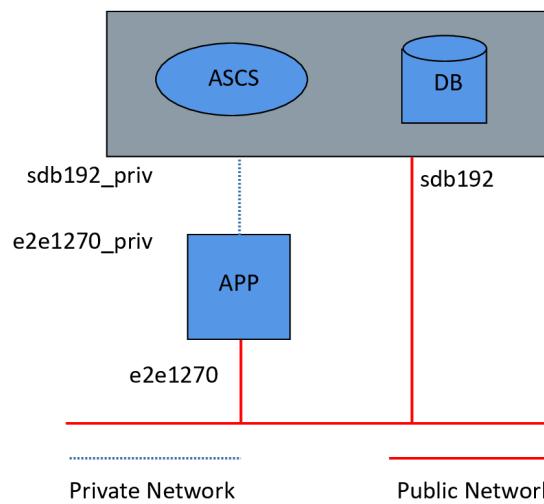
layouts might better meet your needs or SAP requirements, or you might use quotas.

Use the following commands to create the required directories for installing the SAP software, `/sapmnt`, `/usr/sap`, and `/db2`:

```
$ [root@sdb192 ~]# mkdir /sapmnt  
[root@sdb192 ~]# mkdir /usr/sap  
[root@sdb192 ~]# mkdir /db2
```

Preparing your network for a three-tier setup

If you are planning to install a three-tier setup, the network needs to be set up correctly. In the example, a 192 GB database server (named "sdb192") and a 32 GB application server (named "e2e1270") are deployed. The database server also hosts the (A)SCS instance. Adding the IP addresses on the private network to your `/etc/hosts` helps with the upcoming steps and ensures that SAP internal network traffic goes through the right network.



Sample of three-tier setup

Use the following steps to establish your network.

1. Log in to the servers and find their private network configuration.

```
$ [root@sdb192 ~]# ifconfig bond0  
bond0  Link encap:Ethernet HWaddr 0C:C4:7A:66:2D:A8  
      inet addr:10.17.139.35 Bcast:10.17.139.63 Mask:255.255.255.192  
      inet6 addr: fe80::ec4:7aff:fe66:2da8/64 Scope:Link  
        UP BROADCAST RUNNING MASTER MULTICAST MTU:1500 Metric:1  
        RX packets:128080 errors:0 dropped:0 overruns:0 frame:0  
        TX packets:25491 errors:0 dropped:0 overruns:0 carrier:0  
        collisions:0 txqueuelen:0  
        RX bytes:19137850 (18.2 MiB) TX bytes:3426015 (3.2 MiB)
```

```
$ [root@sdb192 ~]# ifconfig bond1  
bond1  Link encap:Ethernet HWaddr 0C:C4:7A:66:2D:A9  
      inet addr:208.43.211.118 Bcast:208.43.211.127 Mask:255.255.255.224  
      inet6 addr: fe80::ec4:7aff:fe66:2da9/64 Scope:Link  
        UP BROADCAST RUNNING MASTER MULTICAST MTU:1500 Metric:1  
        RX packets:289610 errors:0 dropped:0 overruns:0 frame:0  
        TX packets:109371 errors:0 dropped:0 overruns:0 carrier:0  
        collisions:0 txqueuelen:0  
        RX bytes:31216160 (29.7 MiB) TX bytes:18591947 (17.7 MiB)
```

In the three-tier example, 10.17.139.35 is the private IP address of the database server; it is from one of the IP address ranges from RFC 1597. You can determine the IP address of the application server, too, and add both IP addresses to both servers' `/etc/hosts`.

```
$ [root@sdb192 ~]# cat /etc/hosts
```

```
127.0.0.1 localhost.localdomain localhost
208.43.211.118 e2e2690.saptest.com e2e2690

10.17.139.35    sdb192-priv
10.17.139.46    e2e1270-priv
```

Add the last two lines on `e2e1270`, too.

Installing NFS software

1. Install NFS software `nfs-utils` on both servers.

```
$ [root@sdb192 ~]# yum install nfs-utils
```

Make sure you start and register the `rpcbind` and NFS service on the database server.

```
$ [root@sdb192 ~]# service rpcbind start
[root@sdb192 ~]# chkconfig nfs on
[root@sdb192 ~]# service nfs start
```

Using NFS to export

1. Use NFS to export `/sapmnt` and `/usr/sap/trans` from the database server to the application server by adding the required entry to `/etc/exports` of the database server.

```
$ /sapmnt/C10 10.17.139.46(rw,no_root_squash,sync,no_subtree_check)
/usr/sap/trans 10.17.139.46(rw,no_root_squash,sync,no_subtree_check)
```

The sample value `C10` needs to be replaced with the SAP System ID for your SAP system. You must create the directory before you export it. Run the following commands from the command line of the database server:

```
$ [root@sdb192 ~]# mkdir /sapmnt/C10
[root@sdb192 ~]# mkdir -p /usr/sap/trans
[root@sdb192 ~]# exportfs -a
```

Mounting the NFS share

1. Mount the NFS share on the application server by adding the following entry to its `/etc/fstab` and mount it from the command line.

```
$ sdb192-priv:/sapmnt/C10 /sapmnt/C10 nfs defaults 0 0
sdb192-priv:/usr/sap/trans /usr/sap/trans nfs defaults 0 0
```

2. Create the target directories on the application server and mount them.

```
$ [root@e2e1270 ~]# mkdir -p /sapmnt/C10
[root@e2e1270 ~]# mkdir /usr/sap/trans
[root@e2e1270 ~]# mount /sapmnt/C10
[root@e2e1270 ~]# mount /usr/sap/trans
```

Your servers are now prepared to host the components of a distributed SAP installation.

Step 3: Adding external storage to your server

External storage can be added to your provisioned server or servers. You can use the external storage as a backup device, or use as a snapshot to quickly restore your database in a test environment. For the three-tier example, block storage is used for both archiving database log files and online and offline database backups. The fastest block storage (10 IOPS per GB) was selected to help assure a minimum backup time. Slower block storage might be sufficient for your needs. For more information about IBM Cloud® Block Storage for Classic, see [Getting started with Block Storage](#).

IBM Cloud storage LUNS can be provisioned with two options - Endurance and Performance. Endurance tiers feature pre-defined performance levels and other features, such as [snapshot](#) and replication. A custom Performance environment is built with allocated input/output operations per second (IOPS) in the range 100 - 1,000.

Setting up external storage

1. Log in to the [IBM Cloud console](#) with your unique credentials.
2. Expand the Menu icon  and select *Classic Infrastructure*.
3. Select *Storage > Block Storage > Order Block Storage*.
4. Select the specifics for your storage needs. Table 1 contains recommended values, including 10 IOPS/GB for a demanding database workload.

Field	Value
Location	US South, DAL10
Billing Method	Monthly (default)
Size	1000 GB
Endurance (IOPS tiers)	10 IOPS/GB
Snapshot space	0 GB
OS Type	Linux (default)

Recommended values for block storage

5. Review the Order Summary.
6. Select **I have read and agree to the terms and conditions listed below**.
7. Click **Create**.

Authorizing host

1. Select **Storage > Block Storage**.
2. Highlight your LUN and expand the Action menu  and select **Authorize Host**.
3. Select *Bare Metal Server* for **Device Type**.
4. Click **Hardware** to load available devices and select the hostname of your database server.
5. Click **Save**.
6. Check the status of your provisioned storage under **Devices > (select your device) > Storage** tab.
7. Note the **Target Address** and iSCSI Qualified Name (**IQN**) for your server (iSCSI initiator), and the **username** and **password** for authorization with the iSCSI server. You need that information in the following steps.



Tip: More provisioning information can be found under [Ordering Block Storage through the Console](#).

Follow the steps in [Connecting to MPIO iSCSI LUNS on Microsoft Windows](#) to make your storage accessible from your provisioned server.

Making storage multipath

In the sample deployment, you retrieved the following data from the **Storage** tab: * Target IP: 10.2.62.78 * IQN: iqn.2005-05.com.softlayer:SL01SU276540-H896345 * User: SL01SU276540-H896345 * Password: EtJ79F4RA33dXm2q

1. Enter the following based on the retrieved information:

```
$ [root@sdb192 ~]# cat /etc/iscsi/initiatorname.iscsi
InitiatorName=iqn.2005-05.com.softlayer:SL01SU276540-H896345
```

An existing entry might have to be replaced in `/etc/iscsi/initiatorname.iscsi`.

2. Add the following lines to the end of `/etc/iscsi/iscsid.conf`:

```
$ [root@sdb192 ~]# tail /etc/iscsi/iscsid.conf
# it continue to respond to R2Ts. To enable this, uncomment this line
# node.session.iscsi.FastAbort = No
node.session.auth.authmethod = CHAP
```

```

node.session.auth.username = SL01SU276540-H896345
node.session.auth.password = EtJ79F4RA33dXm2q
discovery.sendtargets.auth.authmethod = CHAP
discovery.sendtargets.auth.username = SL01SU276540-H896345
discovery.sendtargets.auth.password = EtJ79F4RA33dXm2q

```

3. Replace the `username` and `password` values in step 2 with the values that you noted during step 5 of *Authorizing hosts*.
4. Discover the iSCSI target by entering the following lines.

```

$ [root@sdb192 ~]# iscsiadm -m discovery -t sendtargets -p "10.2.62.78"
10.2.62.78:3260,1031 iqn.1992-08.com.netapp:tor0101
10.2.62.87:3260,1032 iqn.1992-08.com.netapp:tor0101

```

5. Set the host to automatically log in to the iSCSI array.

```
$ [root@sdb192 ~]# iscsiadm -m node -L automatic
```

6. Install and start the multipath daemon.

```

$ [root@sdb192 ~]# yum install device-mapper-multipath
...
[root@sdb192 ~]# chkconfig multipathd on
[root@sdb192 ~]# service multipathd start

```

7. Complete all the commands in [Connecting to iSCSI LUNS on Linux](#) so another LUN appears in the multipath output.

```

$ [root@sdb192 ~]# multipath -ll
...
3600a098038303452543f464142755a42 dm-9 NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1 alua' wp=rw
|--- policy='round-robin 0' prio=50 status=active
| `-- 10:0:0:169 sde 8:64 active ready running
`--- policy='round-robin 0' prio=10 status=enabled
`- 9:0:0:169 sdf 8:80 active ready running
...

```

You can now use the multipath device as you would use any disk device. A device path appears under `/dev/mapper/3600a098038303452543f464142755a42`.

Take the sample `/etc/multipath.conf` from the [example multipath.conf](#) and create it on your server. Any copied special characters, DOS-like carriage returns, line-feed entries might lead to unexpected behavior. Make sure that you have an ASCII Unix file after you copy the contents.

Adapt the multipath block from `/etc/multipath.conf` to create an alias of the path to access the device under `/dev/mapper/mpath1`.

```

$ multipaths {
    multipath {
        wwid 3600a098038303452543f464142755a42
        alias mpath1
    }
}

```

1. Restart `multipathd`. You can now create the `/backup` file system and mount on the block device.

```

$ [root@sdb192 ~]# service multipathd restart
[root@sdb192 ~]# mkfs.ext4 /dev/mapper/mpath1
[root@sdb192 ~]# mkdir /backup

```

1. Check the file systems on both servers. Your output should be similar to the following output.

```

$ [root@e2e1270 ~]# df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/sda3        879G  1,5G  833G   1% /
tmpfs            16G     0   16G   0% /dev/shm
/dev/sda1       248M   63M  173M  27% /boot

```

```
/dev/sdb2          849G 201M 805G 1% /usr/sap
db192-priv:/usr/sap/trans
    165G 59M 157G 1% /usr/sap/trans
db192-priv:/sapmnt/C10
    165G 59M 157G 1% /sapmnt/C10
```

```
$ [root@sdb192 ~]# df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/sda3        549G  2,3G  519G  1% /
tmpfs           127G     0  127G  0% /dev/shm
/dev/sda1        248M   63M  173M 27% /boot
/dev/mapper/mpath1 493G   70M  468G 1% /backup
/dev/mapper/datavg-datalv
    1,2T  71M  1,1T  1% /db2
/dev/mapper/datavg-saplv
    165G  60M  157G 1% /usr/sap
/dev/mapper/datavg-sapmntlv
    165G  60M  157G 1% /sapmnt
```

If you install an SAP NetWeaver-based SAP application on IBM Db2, you must create subdirectories under `/backup` owned by the database admin user (db2SID) for full backups and archived log files. To automatically archive the log files, set `LOGMETH1` in your IBM Db2 SaaS database. Refer to the [IBM Db2 SaaS documentation](#)) for details.

Step 4: Installing your SAP landscape

Prerequisite: Installing RPM packages

An SAP installation requires certain prerequisites for the packages that are installed on the OS and the OS daemons that are running. Refer to the latest [installation guides](#)). Click **Access downloads** under **Installations & Upgrades**. This requires an SAP S-user ID. Also, refer to the latest [support notes](#)) (requires an SAP S-user ID) from SAP for an up-to-date list of these prerequisites.

Two more packages need to be installed:

- `compat-sap-c++`: Generally achieves compatibility of the C++ runtime with the compilers that are used by SAP. Because Red Hat Enterprise Linux for SAP Business Application 7.X was selected as the OS for both the 32 GB application server and the 192 GB database server, you use `compat-sap-c++-7`.
- `uuidd`: Maintains OS support for the creation of UUIDs.

Checking if `uuidd` is installed

1. Check whether `uuid` daemon (`uuidd`) is installed. If it is not, install and start it.

```
$ [root@sdb192 ~]# rpm -qa | grep uuidd
[root@sdb192 ~]# yum install uuidd
[root@sdb192 ~]# chkconfig uuidd on
[root@sdb192 ~]# service uuidd start
```

Installing package `compat-sap-c++-7`

1. Follow [SAP Note 2195019](#)) and install package `compat-sap-c++-7` and create a specific soft-link, which is required by the SAP binaries. Check the release-specific SAP Notes for the product you are installing to determine whether the library is required.

```
$ [root@sdb192 ~]# yum install compat-sap-c++-7-7.2.1-2.e17_4.x86_64.rpm
...
[root@sdb192 ~]# mkdir -p /usr/sap/lib
[root@sdb192 ~]# ln -s /opt/rh/SAP/lib64/compat-sap-c++.so /usr/sap/lib/libstdc++.so.6
```

Downloading your SAP software

Log in to the [SAP Support Portal](#)), click **Download Software**, and download the required DVDs to a local share drive. Transfer the files to your provisioned server. Another option is to download the [SAP Software Download Manager](#)), install it on your target server and directly download the DVD images to the server.

Preparing for SAP's SWPM GUI

Depending on your network bandwidth and latency, you might want to run the SAP Software Provisioning Manager (SWPM) graphical user

interface (GUI) remotely in a virtual network computing (VNC) session. Another option is to have the GUI running locally and connect to SWPM on the target machine. Use the [SWPM documentation](#) if you decide to run the GUI locally.

The following steps outline running the SWPM GUI remotely in a virtual network computing (VNC) session. This option installs a VNC server, which might not be inline with hardening your operating system; ensure that you are meeting your security measures. Refer to [VNC documentation](#) for an overview on its functions if you are not familiar with it.

1. Use the following commands to install a VNC server.

```
$ [root@sdb192 ~]# yum install tigervnc-server
```

2. Use the following command to install the X11 window manager, `twm`, which is included in the Linux distribution.

```
$ [root@sdb192 ~]# yum install twm
```

3. Install a terminal emulator, for example, `xterm`.

```
$ [root@sdb192 ~]# yum install xterm
```

4. Start the VNC server from the command line.

```
$ [root@sdb192 ~]# vncserver
```

You now require a VNC client program. Multiple implementations are available for all operating systems at no cost. Typically, you need port 590X (where X is the number of the servers that are running, starting at 1) to be accessible from your client.

You might have to start an xterm from the background menu of twm. You can start SWPM (sapinst) from the xterm.

Installing SAP software

After you download the installation media, follow the standard SAP installation procedure that is documented in the SAP installation guide for your SAP version and components, and the corresponding SAP Notes.

You can start SAP SWPM from the xterm, and run the installation steps.

Installing the SAP software in a three-tier environment

Follow the steps in SAP's SWPM for a three-tier setup.

1. Select **Distributed System** and install the ASCS and the database on the database server.
2. Install the Application Server ABAP on the application server. Be sure to use the private addresses for the ASCS and the database hostnames during installation of the application server.

The use of the private addresses and hostnames assures that network traffic between the application server and ASCS, or database, passes through the private network and not through the public network.

Step 5: Sample multipath.conf

The following sample multipath.conf is for Red Hat 7.X and NetApp-based iSCSI LUNs.

```
$ defaults {  
    user_friendly_names no  
    max_fds max  
    flush_on_last_del yes  
    queue_without_daemon no  
    dev_loss_tmo infinity  
    fast_io_fail_tmo 5  
}
```

All data under blacklist must be specific to your system.

```
$ blacklist {  
    wwid "SAdaptec*"  
    devnode "^hd[a-z]"  
    devnode "^(ram|raw|loop|fd|md|dm-|sr|scd|st)[0-9]*"  
    devnode "^cciss.*"
```

```

}
devices {
    device {
        vendor "NETAPP"
        product "LUN"
        path_grouping_policy group_by_prio
        features "3 queue_if_no_path pg_init_retries 50"
        prio "alua"
        path_checker tur
        fallback immediate
        path_selector "round-robin 0"
        hardware_handler "1 alua"
        rr_weight uniform
        rr_min_io 128
    }
}

```

Sample multipath.conf multipaths extension for ‘human readable’ device paths:

```

$ multipaths {
multipath {
wwid XXXXXXXXZZZ
alias pathname
}
}

```

SAP NetWeaver deployment to Bare Metal on Classic Infrastructure, when you are using Windows Server



Note: A Quick Study, someone who is able to learn new things quickly.

These Quick Study Tutorials provide a single sample configuration, with less detailed instructions, as an introduction for customers who prefer hands-on tasks to increase their pace of learning.

The following information provides an introduction for customers who are new to the Classic Infrastructure environment. Two sample configurations are provided to help you through the ordering process to the start of the SAP installation.

The first configuration sample is a simple, single node 32 GB RAM server with Windows Server. The second is an advanced two-node configuration that adds a second virtual server of 192 GB RAM with Windows Server to the landscape.

The third sample is an example of how to set up external storage, which can be applied to either sample configuration.

The sample layouts might match your preferred layout. The purpose of the tutorial is to show two possibilities. Your installation should follow your business requirements and SAP installation documentation.

Step 1: Provisioning a 32 GB server for a single-host environment

1. Log in to the [IBM Cloud console](#) with your unique credentials.
2. Click **Create resource > Compute > Infrastructure > Bare Metal Server**.
3. Click **Continue**. If you can't click **Continue**, you don't have the correct permissions to create a server. Check with your system administrator about your permissions.
4. Leave **1** in the **Quantity** field.
5. Enter **e2e1270** in the **Hostname** field. Hostname is a permanent or temporary name for your servers. Click **Information** for formatting specifics.
6. Enter **mycloud.com** in the **Domain** field. Domain is the identification string that defines administrative control within the internet. Click **Information** for formatting specifics.
7. **Billing** defaults to *Monthly*. Currently, 1-year contract and 3-year contract are not available for SAP-certified servers.
8. The data centers displayed under **Location** depend on product availability within a particular data center. Leave the default **Location** of **NA South DAL10-Dallas**.
9. Click **All servers > SAP certified**.

Configuring your server

Select your SAP-certified server and OS.

1. Select **CPU Model BI.S3.NW32 (OS Options)**. For more information about deciphering the server names, see [Provisioning your Bare Metal Servers using the IBM Cloud console](#).
2. **RAM** defaults to a predefined value based on your server selection and cannot be changed.
3. Enter an optional public key for your **SSH key**, which you can use to log in to your server after provisioning is done. The default is **None**.
4. Choose *Microsoft* as your **Image** (OS) and select *2016 Standard (64 bit)-HVM*.



Note: If you're bringing your own license (BYOL) for your OS, select **No OS**. For more information, see [Bring your own license](#).

Adding storage disks

1. Under **Type**, select *RAID 10*.
2. **Disks**, **Hot Spare**, and **Disk Media** have default values that are based on your selection. Select a **Disk Size** that covers the total amount of storage you need.
3. Click the Menu icon > **Advanced configuration** and leave **Controller** cleared. Click **OK**.

Network interface

1. Select *1 Gbps Redundant Public and Private Network Uplinks* for **Uplink Port Speed**.
2. Select the values in Table 1 for the following fields:

Field	Value
Private VLAN	dal10.bcr01a.981
Public VLAN	dal10.fcr01a.926
Private Subnet	10.177.119.192/26
Public Subnet	169.46.15.96/27

32 GB network interface values

3. Leave the default values for all other fields.
4. Review your Order Summary.
5. Select **I read and agree to the following Third-Party Service Agreements**.



Note: You can create your server, save the order as a quote to provision later, or add the order an estimate, which might include multiple services.

6. Click **Create** to be redirected to the Checkout page after your order is verified.

You are redirected to a page with your order number. Print the page because it is your receipt. You also receive a confirmation email with the subject *Your IBM Cloud Order ## has been approved*. The ## is your order number.

Depending on your order, the server is available for use within one to four hours after the order is submitted. You can check Device Details from the IBM Cloud console (Menu icon > Resource List > Devices) for the status of the provisioning steps. Click the **Device Name** that matches your device's hostname and domain to see its status.

Bring your own license

If you have your own operating system license, you install it on your Bare Metal Servers based on the vendor's instructions. For more information, see [The no OS option](#).

Access your server

Use a public IP for remote access so that you can connect to your server through a Remote Desktop (RDP) client (for example, Microsoft Windows' MSTSC). The public IP address is displayed in the Device List for your device. The administrator password for your server is also displayed. Click **Show Password** to see the password.

Partitioning and file systems

For the single-node example, a server with one logical disk (on RAID 1) was ordered. The operating system (OS) has one mirrored disk, with one large file system equal to the total size of the ordered disk.

The server does not require any further installation steps for storage.

Step 2: Provisioning 192 GB and 32 GB servers for a three-tier environment

A three-tier environment is a more complex scenario that uses a 192 GB server as the database server and a 32 GB server as the SAP NetWeaver application server.

Ordering your SAP NetWeaver Application Server

Follow the steps in the [Provisioning a 32 GB server for a single-host environment](#) to order the SAP NetWeaver Application Server.

Ordering your Database Server

Use the following steps to order an SAP-certified server as your database server.

1. Log in to the [IBM Cloud console](#) with your unique credentials.
2. Click **Create resource > Compute > Infrastructure > Bare Metal Server**.
3. Click **Continue**. If you can't click **Continue**, you don't have the correct permissions to create a server. Check with your system administrator about your permissions.
4. Leave **1** in the **Quantity** field.
5. Enter **sdb192** in the **Hostname** field. Hostname is a permanent or temporary name for your servers. Click **Information** for formatting specifics.
6. Enter **mycloud.com** in the **Domain** field. Domain is the identification string that defines administrative control within the internet. Click **Information** for formatting specifics.
7. **Billing** defaults to *Monthly*. Currently, 1-year contract and 3-year contract are not available for SAP-certified servers.
8. The data centers displayed under **Location** depend on product availability within a particular data center. Leave the default **Location** of *NA South DAL10-Dallas*.
9. Click **All servers > SAP certified**.

Configuring your Database Server

Use the following steps to configure your database server and its OS.

1. Select **CPU Model BI.S3.NW192 (OS Options)**. For more information about deciphering the server names, see [Provisioning your Bare Metal Servers using the IBM Cloud console](#).
2. **RAM** defaults to a predefined value based on your server selection and cannot be changed.
3. Enter an optional public key for your **SSH key**, which you can use to log in to your server after provisioning is done. The default is *None*.
4. Choose **Microsoft** as your **Image** (OS), and select *2016 Standard (64 bit)-HVM*.



Note: If you're bringing your own license (BYOL) for your OS, select **No OS**. For more information, see [Bring your own license](#).

Adding storage disks

Use the following steps to add a 2 TB SATA drive for your database server.

1. For **Disk 1**, click the Menu icon > **Advanced configuration** and verify that **Primary disk partition** is set to the default of *Windows Basic*. Click **OK**.
2. Click **Add new**.
3. **Disks**, **Hot Spare**, and **Disk Media** have default values. Select a **Disk Size** that covers the total amount of storage you need.

Setting up the network interface

Use the following steps to set up the network interface for your database server.

1. Select **1 Gbps Redundant Public and Private Network Uplinks** for **Uplink Port Speed**.

2. Select the values in Table 1 for the following fields:



Note: Make sure the network interface values for your database server match the values for your application server.

Field	Value
Private VLAN	dal10.bcr01a.981
Public VLAN	dal10.fcr01a.926
Private Subnet	10.177.119.192/26
Public Subnet	169.46.15.96/27

192 GB network interface values

3. Leave the default values for all other fields.
4. Review your Order Summary.
5. Select **I read and agree to the following Third-Party Service Agreements**.



Note: You can create your server, save the order as a quote to provision later, or add the order to an estimate, which might include multiple services.

6. Click **Create** to be redirected to the Checkout page after your order is verified.

You are redirected to a page with your order number. Print the page because it is your receipt. You also receive a confirmation email with the subject *Your IBM Cloud Order ## has been approved*. The ## is your order number.

Depending on your order, the server is available for use within one to four hours after the order is submitted. You can check Device Details from the IBM Cloud console (Menu icon > Resource List > Devices) for the status of the provisioning steps. Click the **Device Name** that matches your given hostname and Domain to see its status.

Bring your own license

If you have your own operating system license, you install it on your Bare Metal Servers based on the vendor's instructions. For more information, see [The no OS option](#).

Access your server

Use a public IP for remote access so that you can connect to your servers through a Remote Desktop (RDP) client (for example, Windows' MSTSC). The public IP addresses are displayed in the Device List (under the Device menu) for your device. The root passwords for your servers are also displayed. Click **Show Password** to see the passwords.

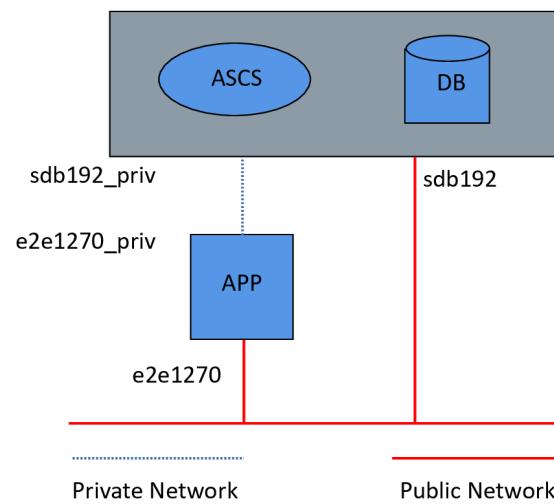
Partitioning and file systems

For the three-tier example, a 192 GB database server with one logical disk (on RAID10) and a 32 GB application server with one logical disk (on RAID 1) were ordered. Both servers come with one large file system equal to the total size of disks.

The server does not require any further installation steps for storage.

Preparing your network for a three-tier setup

If you are installing a three-tier setup, you need to prepare the network setup. For the sample setup, a 192 GB database server (named "sdb192") and a 32 GB application server (named "e2e1270") are deployed. The database server also hosts the ABAP SAP Central Services (ASCS) instance. Adding the IPs on the private network to your hosts file helps with the upcoming steps and ensures that SAP internal network traffic goes through the right network.



Sample of three-tier setup

The network setup of the deployed servers that are outlined in Figure 1 is found under Network Connections in Microsoft Windows. In the sample setup, `10.17.139.35` is the private IP of the database server that is found under Network Connections - Private Network-Teamed, and is one of the IP ranges from RFC 1597. You can determine the IP of the application server, too, and add both IPs to both servers' `host files` under `C:\Windows\System32\drivers\etc`.

In the IBM Cloud® console, you can find the private IP of the database server under Menu icon > Resource List > Devices. Select the applicable device and the IP address is displayed in the respective column.

Step 3: Adding external storage to your server

External storage can be added to your provisioned server, or servers. You can use the external storage as a backup device, or as a snapshot to quickly restore your database in a test environment. In the example, block storage is used for both archiving log files of the database and online and offline backups for the database. The fastest block storage (10 IOPS per GB) was selected to help assure a minimum backup time. Slower block storage might be sufficient for your needs. For more information about IBM Cloud® Block Storage for Classic, see [Getting started with Block Storage](#).

IBM Cloud storage LUNS can be provisioned with two options - Endurance and Performance. Endurance tiers feature pre-defined performance levels and other features, such as [snapshot](#) and replication. A custom Performance environment is built with allocated input/output operations per second (IOPS) in the range 100 - 1,000.

Setting up external storage

1. Log in to the [IBM Cloud console](#) with your unique credentials.
2. Expand the Menu icon and select **Classic Infrastructure**.
3. Select **Storage > Block Storage > Order Block Storage**.
4. Select the specifics for your storage needs. Table 1 contains recommended values, including 10 IOPS/GB for a demanding database workload.

Field	Value
Location	US South, DAL10
Billing Method	Monthly (default)
Size	1000 GB
Endurance (IOPS tiers)	10 IOPS/GB
Snapshot space	0 GB

OS Type	Windows 2008+
Recommended values for block storage	
5. Review the Order Summary.	
6. Select I have read and agree to the terms and conditions listed below .	

Authorizing host

1. Select **Storage > Block Storage**.
2. Highlight your LUN and expand the Action menu  and select **Authorize Host**.
3. Select a **Device Type** of *Bare Metal Server*.
4. Click **Hardware** to load available devices and select the hostname of your database server.
5. Click **Save**.



Tip: More provisioning information can be found under [Ordering Block Storage through the Console](#).

Follow the steps in [Connecting to MPIO iSCSI LUNS on Microsoft Windows](#) to connect your block storage to your database server by using the data from the example. Follow the steps carefully; they lead to a new “offline” disk available for your Windows server.

You can now bring the disk online and initialize it.

Step 4: Installing your SAP landscape

Downloading your SAP software

You need an SAP S-user ID and Download Authorization to download the DVDs. For more information about the SAP S-user ID, see [How to set up an S-user ID](#).

1. Log in to the [SAP Support Portal](#), click **Download Software**, and download the required DVDs to a local share drive.
2. Transfer the files to your provisioned server.

Another option is to download the [SAP Software Download Manager](#), install it on your target server, and directly download the DVD images to the server.

Installing SAP software



Note: This example is for downloading the applicable SAP NetWeaver software. You may or might not be using SAP Netweaver 7.5.

After you download the installation media, follow the standard SAP installation procedure that is documented in the SAP installation guide for your SAP version and components, and the corresponding SAP Notes. For more information, see [SAP Installation Guide](#) (search for the guides based on the Windows OS) and [SAP Notes](#). SAP Notes requires an SAP S-user ID.

1. Open the root folder of your SWPM-DVD or of your installation DVD as Administrator, and run `sapinst`. The Welcome to SAP Installation page is displayed.
2. Select **SAP NetWeaver 7.5 > IBM DB2 for Linux, Unix, and Windows > SAP Systems > Application Server ABAP**.
3. Open **Distributed System** and run **ASCS Instance** and **Database Instance** on the database server.
4. Verify that `sapinst` successfully shared folders `\usr\sap\trans` and `\sapmnt` after the ASCS Instance is installed for the next step to work.
5. Run **Primary Application Server Instance** on the application server. Be sure to use the private addresses for the ASCS and the database hostnames during installation of the application server. Using private addresses ensures that network traffic between the application server and ASCS, or database, path through the private network and not through the public network.

You can now run your SAP installation according to the SAP installation instructions.

VPC infrastructure integration scenarios

Accessing File Storage for VPC from IBM Power Virtual Server instances

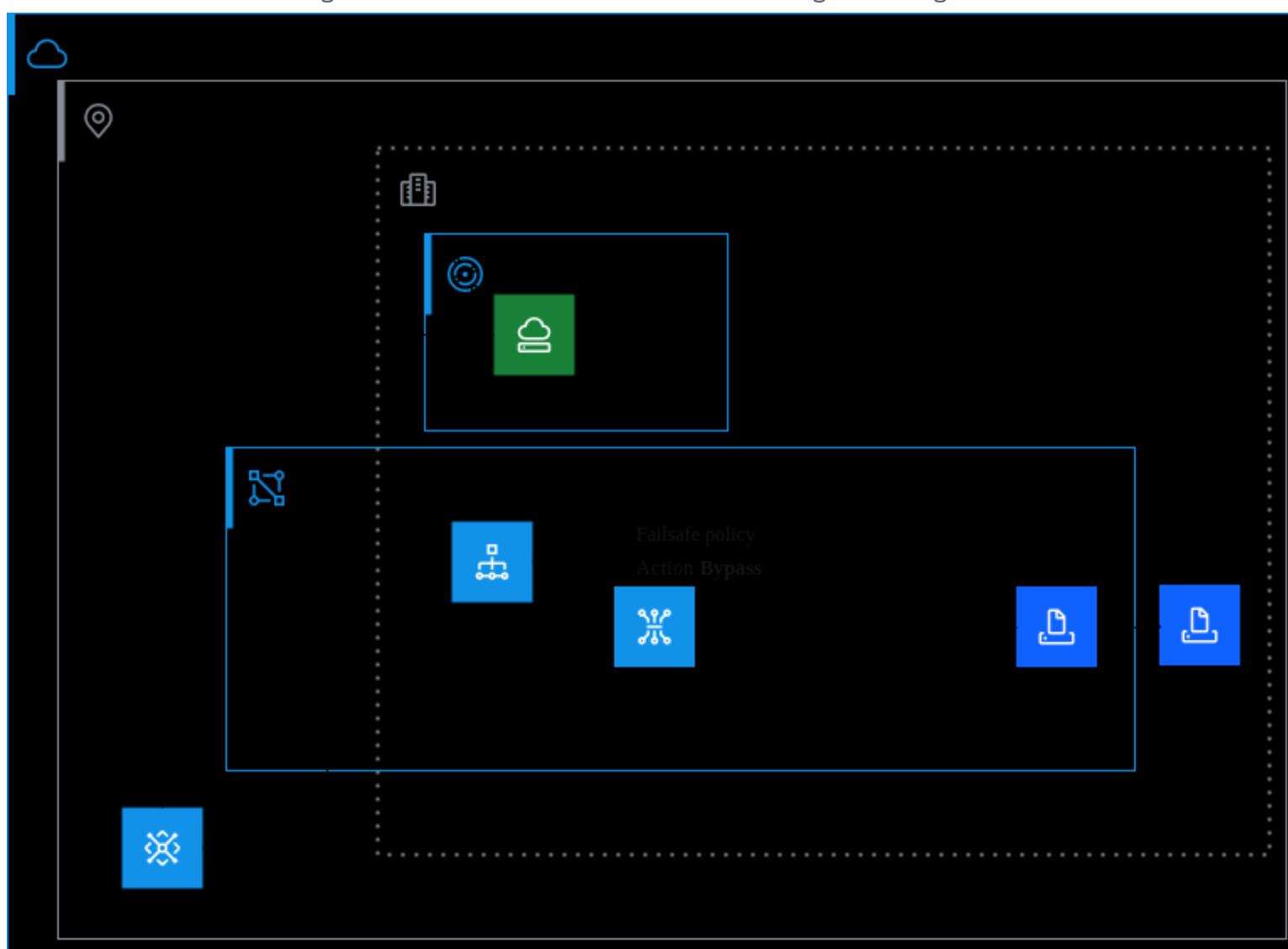
Tip: This tutorial might incur costs. Use the [Cost Estimator](#) to generate a cost estimate based on your projected usage.

In this tutorial, you learn how to mount a file share on an IBM Power Virtual Server server instance. You cannot directly mount a file storage share on IBM Power Virtual Server instances and must instead use a path through a network load balancer (NLB). You create a file storage share and a mount target in IBM VPC. You create a network load balancer with routing mode, and a route table in IBM VPC. Then, you mount the file storage share on the virtual server instance in IBM Power Virtual Server.

The following architecture overview diagram illustrates this scenario.

The virtual server instance in IBM Power Virtual Server sends a request through a transit gateway to the file storage share. According to the rule in the routing table of the VPC, the network traffic to the file storage share is directed to the network load balancer. The network load balancer has *Routing_mode* enabled. It bypasses a back-end pool and sends requests directly to the destination IP address. The file storage share responds and the response is sent directly to the virtual server instance in IBM Power Virtual Server. The network load balancer (NLB) with routing mode has two IP addresses (active and standby). When a failover occurs, the route mode updates all routing rules that are created for the VPC with a `next_hop` of the standby IP. Both the active IP and the standby IP are used during the lifetime of an NLB with route mode.

A diagram that shows the architecture for accessing File Storage for VPC.



Before you begin

- [Create a VPC](#) or use an existing one.
- Create a subnet in the VPC for your preferred zone.
- Create an IBM Power Virtual Server workspace in the IBM Cloud region.
- Create a Transit Gateway and attach the VPC subnet and the IBM Power Virtual Server workspace to the Transit Gateway.
- Check the user permissions. Make sure that your user account has permissions to create and manage VPC resources. See [Granting user permissions for VPC resources](#).
- Use or create an SSH key to connect to the virtual server instances. If you don't have an SSH key, see [Getting started with SSH keys](#).

Step 1: Creating a security group and a file storage share

Creating a security group to allow NFS V4 traffic

Create a security group and configure inbound rules for the SSH (22) and NFS (2049) ports.

1. Browse to [Security groups for VPC](#) and click **Create**.
2. Verify or set the **Geography** and **Region** fields.
3. Enter `nfs-server-sg` for the **Name**.
4. Select the same **Resource group** as the VPC resource group.
5. Select your VPC in the **Virtual private cloud** list.
6. Add the **Inbound rules** as shown in the following table.

Protocol	Port range	Source type	Destination type
TCP	22-22	Any	Any
TCP	2049-2049	Any	Any

Inbound rules

7. Add the **Outbound rules** as shown in the following table, then click **Create security group**.

Protocol	Port	Destination type	Source type
TCP	Any	Any	Any
UDP	Any	Any	Any

Outbound rules

Provisioning a file storage share

1. Browse to [File storage shares for VPC](#).
2. Click **Create > Create file share**.
3. In the **Location** section, select the same **Geography**, **Region**, and **Zone** as the virtual private cloud.
4. Enter `nfs-server` in the **Name** field. Select the same **Resource group** as the VPC resource group.
5. In the **Size** section, enter the **Storage size** in GB.
6. Enter a **Max IOPS** value.
7. In the **Mount target access mode** section, select **Security groups**.
8. In the **Mount targets (optional)** section, click **Create**.
 - Enter `nfs-server-mount-target` in the **Mount target name** field.
 - Select your **VPC**.
 - In the **Network interfaces** section, click the pencil icon on the new interface.
 - Verify the selected subnet and click **Next**.
 - In the **Security groups** section, check the `nfs-server-sg` security group, clear the **VPC default** security group, and click **Next**.
 - Click **Next** a few times to get to the **Review** section, then click **Save**.
 - Back on the **Create mount target screen**, click **Next**.
 - Click **Next** in the **Encryption** step.
 - In the **Review** step, click **Create**.
9. Click **Create file share** to provision the file storage and the mount target.

Gathering the file storage IP address and mount path information

1. Browse to [File storage shares for VPC](#).
2. Click the **Name** `nfs-server`.
3. In the **Mount targets** section, click the **Name** of the mount target in the VPC to view the mount target details.
4. Make a note of the **primary IP** and the **Mount path**.

Later, the **Destination** parameter in the VPC route entry is set to the **Primary IP** of the file storage share. The **Mount path** parameter is used as an argument to the `mount` command on the IBM Power Virtual Server instance.

Step 2: Creating the private network load balancer with routing mode

Creating the service-to-service authentication policy

To support routing mode, you must first create a *service-to-service* authentication policy for your NLB.

1. Log in to [IBM Access Management](#).
2. Click **Authorizations**, then click **Create**.
3. Select **This account** for **Source account** and click **Next**.
4. Select **VPC Infrastructure Services** for **Service** and click **Next**.
5. Select **Specific resources > Resource Type > Load Balancer for VPC** for the scope access and click **Next**.
6. Select **VPC Infrastructure Services** for the target service and click **Next**.
7. Select **Specific resources > Resource Type > Virtual Private Cloud** for the scope access and click **Next**.
8. Select the **Editor** checkbox to grant the Editor access role.
9. Click **Authorize**.

Creating the network load balancer

1. Browse to the [Load balancers for VPC](#) page and click **Create**.
2. Select **Network Load Balancer (NLB)** as the **Load balancer type**.
3. In the **Location** section, select the same **Geography** and **Region** that is used for the virtual private cloud.
4. Enter `nfs-server-nlb` in the **Name** field.
5. Select the same **Resource group** as the VPC resource group.
6. Select your VPC in the **Virtual private cloud** list.
7. Select the **Subnet**.
8. Check **Private** in the **Type** section.
9. Set **Routing mode** to **On** to create a network load balancer with routing mode.
10. In the **Back-end pools** section, click **Create pool**. Set the parameters to the following values.
 - **Name:** `nfs-server-fwd-pool`
 - **Pool protocol:** `TCP`
 - **Session stickiness:** `None`
 - **Method:** `Round robin`
 - Click **Create**.
11. In the **Front-end listeners** section, click **Create listener**. Select your **Back-end pool** and click **Save**.
12. In the **Security Groups** sections, check the `nfs-server-sg` security group, and clear the default security group.
13. Click **Create load balancer** to provision the load balancer.

 **Important:** As part of the process, you create a back-end pool. However, you cannot define the back-end pool `Failsafe policy` directly, and it must be updated in the next step.

Updating the network load balancer failsafe policy

Update the `Failsafe policy` for the `nfs-server-fwd-pool` back-end pool. The network load balancer then bypasses the back-end pool and sends requests directly to the destination IPs.

1. Browse to [Load balancers for VPC](#).
2. Click the load balancer `nfs-server-nlb`.

3. Click the **Back-end pools** tab and select the pool `nfs-server-fwd-pool`.
4. Click `nfs-server-fwd-pool` and then **Edit**.
5. In the **Failsave policy** section, select **Bypass** as the **Action**.
6. Click **Save**.

Collecting the private IP addresses of the load balancer

1. Browse to [Load balancers for VPC](#).
2. Click `nfs-server-nlb`.
3. In the **Load balancer details - Private IPs** section, make a note of the first IP address entry in the list.

Later, the **Next hop** parameter in the VPC route entry is set to the active **Private IP** address of the load balancer.

Step 3: Creating a routing table and routes for VPC

Creating a routing table

Customize the **Ingress routes** to route incoming traffic from external sources such as the IBM Cloud Transit Gateway.



Note: Only one custom routing table is associated with an ingress source. If an ingress routing table exists for the IBM Cloud Transit Gateway source, add the **route** to that table.

1. Browse to [Routing tables for VPC](#).
2. Click **Create**.
3. In the **Location** section, select the same **Geography** and **Region** that is used for the virtual private cloud.
4. Enter `nfs-server-routing` in the **Name** field.
5. Select your VPC in the **Virtual private cloud** list.
6. Enable the **Transit gateway** flag in the **Traffic source (optional)** section.
7. Click **Create routing table** to provision the routing table.

Creating a route

1. Browse to [Routing tables for VPC](#).
2. Click the name `nfs-server-routing`.
3. Click **Create**.
4. Select the zone for your route in the **Zone** field.
5. Enter `nfs-server` in the **Name** field.
6. Using CIDR notation, enter the primary IP address of the file share as **Destination CIDR**.
7. Select **Deliver** as the **Action**.
8. Enter the `IP address of the network load balancer` as the **Next hop (IP address)**.
9. Click **Save** to add the route to the table.

Step 4: Mounting the file share on the IBM Power Virtual Server instance

Log on as the `root` user to the server instance in IBM Power Virtual Server where you want to mount the file share.

1. Install the NFS client packages on the instance.

```
$ dnf install nfs-utils
```

2. Create a directory for the mount point.

```
$ mkdir <mount_point>
```

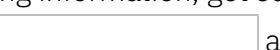
3. Mount the remote file share.

```
$ mount -t nfs4 -o <options> <host:/mount_target> <mount_point>
```

See the following example.

```
mkdir /mnt/test  
mount -t nfs4 -o rw,sec=sys 10.30.40.5:/73a1ff96_4861_4463_aa09_8c8128b8e277fsf /mnt/test
```

Navigating the IBM Cloud console

The [IBM Cloud® console](#) is the user interface that you use to manage all your IBM Cloud resources. You can create a free account, log in, access documentation, access the catalog, view pricing information, get support, or check the status of IBM Cloud components. After you log in, the menu bar contains a **Navigation Menu** icon  and more links.

Using the console

When you log in to IBM Cloud, your dashboard is displayed, which shows widgets that summarize the status of your account. If you're interested in customizing your dashboard, see [Working with scoped dashboards](#).

Use the following options to navigate to general areas of the console:

Browse available products

Use the **Catalog** link to explore over 350 products that offer options for compute, networking, security management, end-to-end developer solutions, and more. Use the tabs to filter the catalog to quickly access *deployable architectures*, IBM products, Cloud essentials, and more.

Find help when you need it

Click the **Help** icon  > **Docs** to access the product documentation.

Get support when something's not working as expected

Click the **Help** icon  > **Support center** to go to the [Support Center](#) page.

Manage account preferences and more

From the **Manage** menu, you can access your account, billing and usage, and Identity and Access Management options.

Quickly access a browser-based shell environment

Click the **IBM Cloud Shell** icon  to open a browser-based shell environment that you can use to work with your IBM Cloud resources.

Estimate costs for your cloud deployments

Click the **Cost estimator** icon  to open the cost estimator.

Stay up to date with notifications

Click the **Notifications** icon  to view and control all incidents, maintenance, and announcements that are likely to affect your account.

Customize your profile and more

Click the **Avatar** icon  to access your profile, guided tours, console theme options, and more.

In addition to the console, [command-line interfaces \(CLIs\)](#), APIs, and SDKs are available for interacting with your cloud account and resources. [Terraform](#) support is also available through use of the IBM Cloud Provider plug-in for managing cloud resources at enterprise scale through templates and scripting.

Can't find what you're looking for?

The IBM Cloud platform recently consolidated services and features to provide you with a more simplified and customized experience. Services and areas of the console are now unified into the following hubs: Infrastructure, Containers, Automation, Databases, Observability, and Security. The goal of these changes is to bundle together related services to make it easier to find, deploy, and use them. Use our mapping and guidance to see what's changed in the IBM Cloud catalog and console navigation to find what you're looking for.

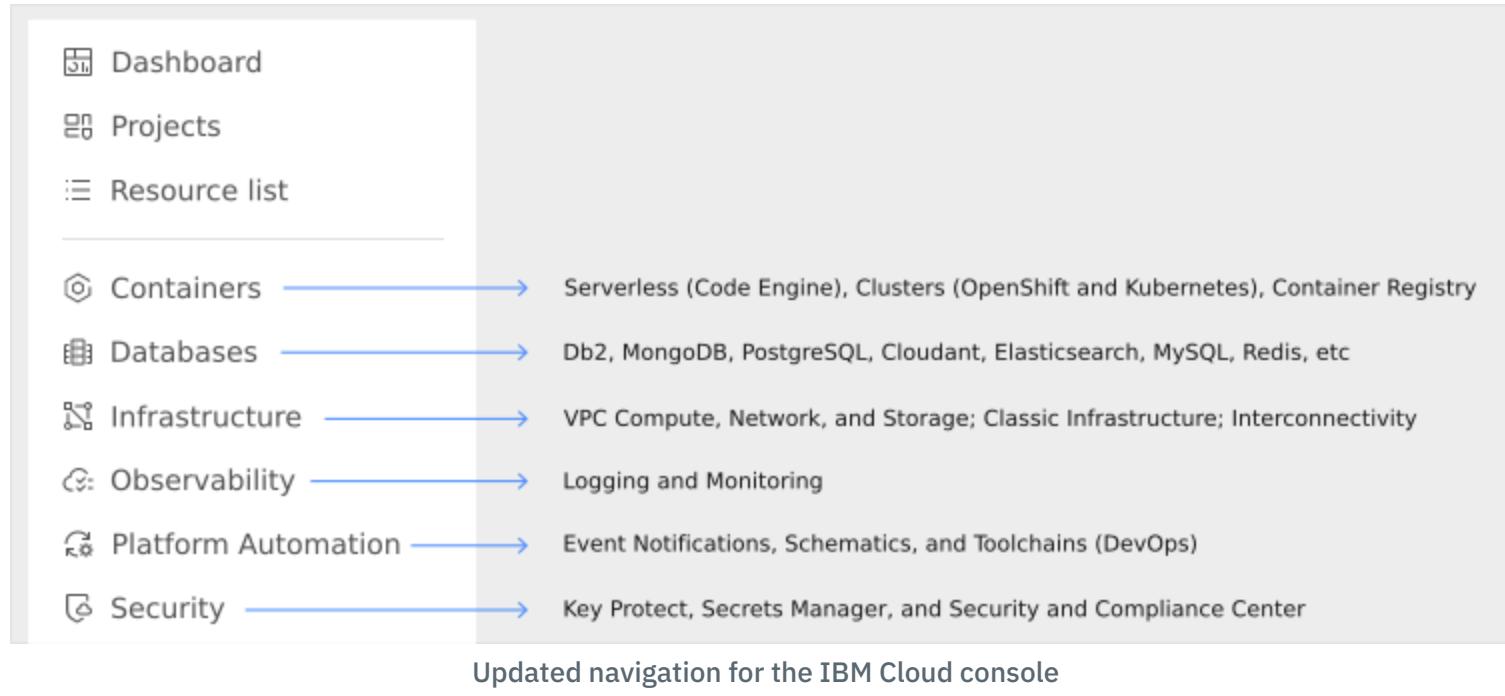
Streamlined and dynamic IBM Cloud catalog

In addition to the new navigation changes, we updated the discoverability and management of our catalog. The new IBM Cloud catalog makes it easy to discover IBM products such as managed services, preconfigured software, professional services, and even partner services. You can navigate by using the new tabs in the catalog to explore what each category consists of.

- Get your job done more efficiently with expertly-designed solutions. Cloud essentials is your main source for exploring related products that are tailored to specific industries in a cohesive way.

- Use deployable architectures to understand how pre-built compositions of products work together to help solve common business problems. Deployable architectures accelerate your innovation and reduce risk across complex enterprise workloads. Industry solutions with configurations that previously took months to achieve are now available within hours.

Simplified access to your workloads



From the **Navigation Menu** [Navigation Menu], you can access areas of IBM Cloud that are focused on specific use cases and industries. Use the following options to explore the menu:

Containers

The previous **Kubernetes**, **OpenShift**, **Code Engine**, and **Container Registry** menu options are now nested within **Containers**.

Databases

All of your database needs are now centralized into one location. From **Databases**, you can create and manage relational databases (Databases for MySQL, Db2, Databases for PostgreSQL, and Databases for EDB); auxiliary databases (IBM Db2 Warehouse SaaS, Databases for etcd, and Databases for Redis); and non-relational databases (Databases for Elasticsearch, Databases for MongoDB, and IBM Cloudant).

Infrastructure

The previous **Classic Infrastructure**, **VPC Infrastructure**, **Power Virtual Server**, and **Interconnectivity** menu options are now nested within **Infrastructure**.

Observability

The **Observability** option still provides access to **Logging**, **Monitoring**, and **Activity tracking**.

Platform Automation

The previous **DevOps** and **Schematics** options are now nested within **Platform Automation**, along with Event Notifications.

Security

Security and Compliance Center is now integrated with IBM Key Protect and Secrets Manager and can be accessed from the **Security** menu option.

Provisioning SAP HANA and SAP NetWeaver

Intel Virtual Server in VPC

Planning your deployment

Make sure that you are already familiar with the fundamental components and options that are provided by IBM Cloud Classic Infrastructure for SAP. Before you start with the deployment of servers, make sure that you also read the Get Started section.

Intel Optane persistent memory (PMem) is available on the Bare Metal servers. You have three memory options for PMem on the Bare Metal servers, 1.5 TB, 3.0 TB, and 6.0 TB. Which option you choose depends on the:

- Application that you want to run, for example BW or BW/4 HANA.
- SAP sizing, which determines the amount of memory and CPU that you need.

Network and storage configuration, disaster recovery, high availability, backups, and system replication are all configured and managed as part of the Bare Metal provisioning and operation.

The 'Must-Reads' before you start deploying

To ensure that your first deployment is a success, review the information in Provisioning SAP HANA and SAP NetWeaver [Planning your deployment](#)

Other useful documents

See the respective topics in the *Get Started* section for the following information:

- [SAP HANA design considerations for High Availability and Disaster Recovery \(HA/DR\)](#)
- [SAP HANA backups - Storage impacts on Recovery Time Objective \(RTO\)](#)
- [SAP NetWeaver design considerations for High Availability configuration](#)

VPC with Additional Application Server (AAS) ABAP on Linux for SAP HANA

You can use Terraform scripts to create a single-tier VPC and create the AAS to HANA and AnyDB infrastructure on the VPC. The Terraform scripts use the VPC information that you provide and then call the Ansible playbook to create the SAP architecture on the specified VPC.

Terraform on IBM Cloud® enables predictable and consistent provisioning of IBM Cloud Virtual Private Cloud (VPC) infrastructure resources so that you can rapidly build complex, cloud environments. IBM Cloud VPC infrastructure consists of SAP certified hardware that uses Intel® Xeon CPUs and more Intel® technologies.

You have two deployment methods to choose from:

- Terraform scripts that run from the CLI on your bastion server.
- Schematics user interface accessed from your cloud dashboard menu.

You can create SAP AAS NetWeaver 7.x on the SAP HANA-based ABAP stack.

SAP solution implemented

Many SAP enterprise solutions are built on the SAP platform (SAP NetWeaver) including:

- SAP HANA as Primary Persistence for SAP NetWeaver-based applications
- SAP Business Suite applications (ERP, CRM, and SCM, and other applications),
- SAP Business Warehouse (BW), and
- Other SAP enterprise solutions

SAP NetWeaver has two distinct aspects, ABAP and Java. Many applications that are built on the SAP NetWeaver's ABAP or Java (or both) application servers run on SAP DB owned HANA and ASE Sybase either in AnyDB platforms (MSSQL, Oracle, and Db2).

Technical interfaces are available for applications that are built on the SAP NetWeaver AS ABAP and AS Java to run on SAP HANA and AnyDB. However, specific development enablement is normally required for each application to ensure that it runs optimally on the SAP HANA. SAP Business Suite applications (ERP, CRM, SCM, and other applications), SAP Business Warehouse (BW), and other SAP NetWeaver-based applications were modified to run on SAP HANA and have many advantages. Also, various components and complimentary applications that are built on SAP NetWeaver can also run on SAP HANA or AnyDB by using the provided SAP NetWeaver DB interfaces.

The SAP HANA as primary persistence for SAP NetWeaver-based applications scenario has one restriction: SAP NetWeaver ABAP and Java application servers must run on separate hardware servers from the SAP HANA hardware.

What is created

The scripts automate the virtual infrastructure resources, provisioning the processes for the SAP architecture in an existing VPC with a distributed environment. SAP AAS NetWeaver 7.x (HANA or ASE SYB) application server on a distinct VSI VPC system and SAP HANA DB on a dedicated server type VSI VPC box are provisioned. The scripts work in two phases.

During the first phase of [Automate SAP bastion server – SAP media storage repository](#), the following virtual infrastructure resources based on the components from the existing VPC created by the bastion server are:

- 1 VPC where the virtual server instance is provisioned.
- 1 security group. The rules for this security group are:
 - Allow inbound DNS traffic (port 53).
 - Allow inbound SSH traffic (TCP port 22).
 - Allow all outbound traffic from the virtual server instance.
 - Allow all traffic in the security group.
- 1 subnet to enable the networking in your VPC.
- 2 virtual server instances with SAP certified storage and network configurations.
- 1 floating IP address used to access your VPC virtual server instance over the public network.

During the second phase, the Ansible Playbooks is called and the SAP architecture is installed for both dedicated virtual server instance (VSI) SAP application; VSI system and dedicated SAP HANA VSI box. The SAP architecture that is deployed on the SAP NetWeaver 7.x release is a stand-alone dedicated SAP HANA 2.0 box release. For more information about this architecture, see [Automating SAP HANA stand-alone virtual server instance on IBM Cloud® VPC by using Terraform and Ansible](#).

You can provision only one instance of the service per IBM Cloud region.

Schematics deployment

When you run the scripts with the Schematics interface, you:

- Enter the workspace information.
- Enter the GitHub path for the chosen solution either on NetWeaver AAS for HANA.
- Modify the parameters in the Schematics interface. They are the same parameters as the `input.auto.tfvars` file that you use with the cli.

Virtual server instance configuration

Following are the supported operating system images for SAP NetWeaver primary application server:

- ibm-redhat-8-4-amd64-sap-applications-2
- ibm-redhat-8-6-amd64-sap-applications-2
- ibm-sles-15-3-amd64-sap-applications-2
- ibm-sles-15-4-amd64-sap-applications-3

Following are the supported operating system images for SAP HANA database:

- ibm-redhat-8-4-amd64-sap-hana-2
- ibm-redhat-8-6-amd64-sap-hana-2
- ibm-sles-15-3-amd64-sap-hana-2
- ibm-sles-15-4-amd64-sap-hana-1

For both server instances there are:

- Two SSH keys are configured to access SSH as `root`.
- Three storage volumes as described in the `input.auto.tfvars` file.

What is created for anydb

The scripts use the information that you provide for an existing VPC and deploy AAS to SAP HANA or AnyDB on a different host than CI (SAP Central Instance) VSI host. For more information about this architecture, see [SAP NetWeaver 7.x on UNIX with HANA or AnyDB on IBM Cloud VPC on IBM Cloud VPC](#). You specify the information for the VPC to use in the `input.auto.tfvars` file.

The scripts call the Ansible Playbooks to install the SAP architecture.

Script files

The configuration and script files are provided on GitHub. Each supported interface for the SAP solution installation has its own folder in the GitHub repository:

- [GitHub repository for Terraform – AAS HANA](#)

Terraform interface

To run the Terraform script, you modify:

- The `input.auto.tfvars` file to specify the existing VPC resources for your solution. Specify the variables for the existing VPC:
 - VPC name
 - Security group
 - Subnet
 - Hostname
 - Profile
 - Image
 - Up to two SSH keys

You can change the default SAP system configuration settings to match your solution. You can also specify the location where you downloaded the SAP kits.

The IBM Cloud Provider plug-in for Terraform on IBM Cloud uses these configuration files to install AAS to SAP HANA and AnyDB on the specified VPC in your IBM Cloud account.

Support

There are no warranties of any kind, and there is no service or technical support available for these materials from IBM®. As a recommended practice, review carefully any materials that you download from this site before using them on a live system.

Though the materials provided herein are not supported by the IBM® Service organization, your comments are welcomed by the developers, who reserve the right to revise, readapt or remove the materials at any time. To report a problem, or provide suggestions or comments, open a GitHub issue.

Before you begin

Before you use the scripts in the bastion cli:

- Set up your account to access the VPC. Make sure that your account is [upgraded to a paid account](#).
- If you have not already, create a Bastion server to store the SAP kits. For more information, see [Automate SAP bastion server - SAP media storage repository](#).
- Download the SAP kits from the SAP Portal to your Deployment Server. Make note of the download locations. Ansible decompresses the files. For more information, see the [readme](#) file.
- [Create or retrieve an IBM Cloud API key](#). The API key is used to authenticate with the IBM Cloud platform and to determine your permissions for IBM Cloud services.
- [Create or retrieve your SSH key ID](#). You need the 40-digit UUID for the SSH key, not the SSH key name.
- Terraform should already be installed on the bastion server that you deployed. For more information, see [Bastion server for SAP deployment](#).
- (Optional - Catalog Tile) create secrets for your credentials and passwords by using the [Secrets Manager](#).

Deploying SAP AAS NetWeaver 7.x on HANA by using the Schematics user interface

Use these steps to configure the SAP Additional Application Server (AAS) NetWeaver with HANA or AnyDB on your existing VPC by using the Schematics interface. The script takes 2 - 3 hours to complete.

1. From the IBM Cloud menu, select **Schematics**.
2. Click **Create** workspace.
3. On the **Specify template** page:
 - Enter the URL for the Schematics interface.

- Select the **Terraform version** that is listed in the readme file.
 - Click **Next**.
4. On the **workspace details** page:
- Enter a name for the workspace.
 - Select a **Resource group**.
 - Select a **Location** for your workspace. The workspace location does not have to match the resource location.
 - Select **Next**.
5. Select **Create** to create your workspace.
6. On the workspace settings page, in the input variables section, review the default input variables and provide values that match your solution.
- For a more detailed description of each parameter, check the GitHub repo [AAS HANA readme](#) file, chapter “Input parameter file”. Also, make sure to mark the parameters that contain sensitive information like passwords, API, and ssh private keys as “sensitive”. These parameters are marked as “sensitive” in the readme file, under “Input parameter file”.
7. On the workspace settings page, click **Generate plan**. Wait for the plan to complete.
8. Click **View log** to review the log files of your terraform execution plan.
9. Apply your Terraform template by clicking **Apply plan**.
10. Review the log file to ensure that no errors occur during the provisioning, modification, or deletion process.

Deploying SAP AAS NetWeaver (ABAP) on HANA with the Deployable Architecture tile interface

Use these steps to configure the SAP AAS NetWeaver (ABAP) on HANA on your existing VPC by using the catalog tile interface. The script takes 2 - 3 hours to complete.

1. From the IBM Cloud catalog, select **VPC with Additional Application Server ABAP on Linux for SAP HANA** on HANA tile. The **Create** tab opens for VPC with Additional Application Server ABAP on Linux for SAP HANA. For more information about this deployment, see the About tab or the readme file link.
2. Select the latest version.
3. Select **VPC with Additional Application Server ABAP on Linux for SAP HANA on Deployable Architecture tile** variation.
4. Click **Review deployment** options:
 - **Add to project** to add this deployment to an IBM Cloud project and combine it with other deployments. IBM Cloud projects include several more pipeline steps before deployment, including deployment validation, cost calculation, compliance verification, and approval process.
 - **Create from the CLI** to get the CLI command. With this command you can trigger the deployment from the CLI.
 - **Work with code** to embed the code into other terraform deployments.
 - **Deploy with IBM Cloud Schematics** to trigger the deployment process directly.
5. Select **Deploy with IBM Cloud Schematics**.
6. Add the input parameters for this installation. There are 3 categories of parameters:
 - **Workspace** - These parameters define the workspace that is automatically created in Schematics:
 - Enter a name for the workspace or use the default name.
 - The Resource Group used to create resources. Use default or create a Resource Group.
 - Select a location to create your Schematics workspace. The workspace location need not match the resource location.
 - **Required input variables** - Review the default input variables and provide values that match your solution. These parameters are specific to your deployment. For more detailed information, see the [Readme file](#).

Parameter	Description
BASTION_FLOATING_IP	Required only for Schematics Deployments. The Floating IP from the Bastion Server.

HOSTNAME	The hostname for the VSI. The hostname should be up to 13 characters as required by SAP. For more information on the rules regarding hostnames for SAP systems, check SAP Note 611361: Hostnames of SAP ABAP Platform servers
REGION	The cloud region to deploy the solution. The regions and zones for VPC are listed here . Review supported locations in IBM Cloud Schematics here . Sample value: eu-de.
RESOURCE_GROUP	The name of an existing Resource Group for VSIs and Volumes resources. Default value: "Default". The list of Resource Groups is available here .
SECURITY_GROUP	The name of an existing Security group. The list of security groups is available here .
SSH_KEYS	The list of SSH Keys UUIDs that are allowed to SSH as root to the VSI can contain one or more IDs. The list of SSH Keys is available here . Sample input (use your own SSH UUIDs from IBM Cloud){: external}: ["r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a", "r010-3fcfd9fe7-d4a7-41ce-8bb3-d96e936b2c7e"]
SUBNET	The name of an existing subnet. The list of subnets is available here .
VPC	The name of an existing VPC. The list of VPCs is available here .
ZONE	The cloud zone where to deploy the solution. Sample value: eu-de-2.
ibmcloud_api_key	IBM Cloud API key (Sensitive* value).
private_ssh_key	Required only for Schematics Deployments - Input your id_rsa private key pair content in OpenSSH format (Sensitive* value). This private key should be used only during the terraform provisioning and it is recommended to be changed after the SAP deployment.
hdb_instance_number	The instance number of the SAP HANA database server.
sap_aas_instance_number	Technical identifier for the internal processes of the additional application server.
sap_ascs_instance_number	Technical identifier for the internal processes of ASCS.
sap_ci_host	IP address of the existing SAP Central Instance.
sap_ci_hostname	The hostname of the existing SAP Central Instance.
sap_ci_instance_number	Technical identifier for the internal processes of the Central Instance.
sap_sid	The SAP system ID identifies the entire SAP system.
sap_main_password	Common password for all users that are created during the installation (See Obs*).

Required Variables

- **Optional variables** - Review and update the optional input variables. The Ansible scripts expect the SAP kits to be in the default locations listed. For more information, see the [Readme file - Input Parameters](#).

Parameter	Description
ID_RSA_FILE_PATH	The file path for private_ssh_key is automatically generated by default. If it is changed, it must contain the relative path from Git repo folders. Default value: "ansible/id_rsa".
IMAGE	The OS image used for the VSI. A list of images is available here .
PROFILE	The profile used for the VSI. A list of profiles is available here . For more information about supported DB/OS and IBM Gen 2 Virtual Server Instances (VSI), check SAP Note 2927211: SAP Applications on IBM Virtual Private Cloud .

VOL1	Volume 1 Size - The size for the disks in GB that are to be attached to the VSI and used by SAP.
VOL2	Volume 2 Size - The size for the disks in GB that are to be attached to the VSI and used by SAP.
kit_sapcar_file	Path to the sapcar binary, as downloaded from SAP Support Portal.
kit_swpm_file	Path to the SWPM archive (SAR), as downloaded from SAP Support Portal.
kit_saphostagent_file	Path to the SAP Host Agent archive (SAR), as downloaded from SAP Support Portal.
kit_hdbclient_file	Path to the HANA DB client archive (SAR), as downloaded from SAP Support Portal.

Optional Variables

7. Accept the license agreement.
8. Select **Deploy**. The deployment starts and you are directed to the Schematics page that displays the script log files for you to monitor the deployment progress.

Creating the infrastructure using Terraform with the bastion server CLI

Use these steps to configure the IBM Cloud Provider plug-in and use Terraform to install SAP AAS to SAP HANA and AnyDB on your existing VPC on an already deployed SAP NetWeaver 7.X with SAP HANA 2.0 or ASE SYB as a Central Instance.

The script takes 1 - 2 hours to complete.

1. Access the bastion server cli.
2. Clone the solution repository and change to the folder.

ASE SYB 16 Clone the solution repository from <https://github.com/IBM-Cloud/sap-aas-abap-ase-syb> and cd to the sap-aas-abap-ase-syb/cli folder.

```
$ git clone https://github.com/IBM-Cloud/sap-aas-abap-ase-syb
cd sap-aas-abap-ase-syb/cli/
```

SAP HANA 2.0: Clone the solution repository from <https://github.com/IBM-Cloud/sap-abap-hana-aas> and cd to the sap-abap-hana-aas folder.

```
$ git clone https://github.com/IBM-Cloud/sap-abap-hana-aas.git
cd sap-abap-hana-aas/
```

3. Modify the `input.auto.tfvars` file to specify the information for the existing VPC, your region, zone, networking component names, hostname for the AAS VSI,profile, and image. You need your 40-digit SSH key ID for this file. The second SSH key is optional. For more options for profile, see [Instance Profiles](#). For more options, see [Images](#). For descriptions of the variables, see the [readme](#) file.

The VSI OS images that are supported for this solution for Netweaver Additional Application Server are:

- ibm-redhat-8-4-amd64-sap-applications-2
- ibm-redhat-8-6-amd64-sap-applications-2
- ibm-sles-15-3-amd64-sap-applications-2
- ibm-sles-15-4-amd64-sap-applications-4

```
$ # Infra VPC variables for ASE SYB
REGION    = "eu-de"
ZONE      = "eu-de-2"
VPC       = "ic4sap"                      # EXISTING Security group name
SECURITY_GROUP = "ic4sap-securitygroup"     # EXISTING Security group name
RESOURCE_GROUP = "wes-automation"
SUBNET    = "ic4sap-subnet"                 # EXISTING Subnet name
SSH_KEYS   = [ "r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a" , "r010-3fcfd9fe7-d4a7-41ce-8bb3-
d96e936b2c7e" ]

# SAP AAS VSI variables:
```

```

HOSTNAME = "sapnwase-as01"
PROFILE = "bx2-4x16"
IMAGE = "ibm-redhat-8-4-amd64-sap-applications-2

$ # Infra VPC variables for ABAP HANA
REGION      = "eu-de"
ZONE        = "eu-de-2"
VPC          = "ic4sap" # EXISTING Security group name
SECURITY_GROUP = "ic4sap-securitygroup" # EXISTING Security group name
RESOURCE_GROUP = "wes-automation"
SUBNET       = "ic4sap-subnet" # EXISTING Subnet name
SSH_KEYS     = [ "r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a" , "r010-3fc9fe7-d4a7-41ce-8bb3-d96e936b2c7e" ]
ID_RSA_FILE_PATH = "ansible/id_rsa"

# SAP AAS variables:
HOSTNAME = "sapnwapp"
PROFILE = "bx2-4x16"
IMAGE = "ibm-redhat-8-6-amd64-sap-applications-2"

```

4. Customize your SAP system configuration. In the same file, input.auto.tfvars, edit the SAP system configuration variables that are passed to the Ansible automated deployment. For descriptions of the variables, see the [readme](#) file.

```

$ # SAP system configuration - for ASE SYB
sap_sid = "NWD"
sap_ci_host = "10.243.132.10"
sap_ci_hostname = "sapnwase"
sap_ci_instance_number = "00"
sap_asc_s_instance_number = "01"
sap_aas_instance_number = "00"

# Kits paths
kit_sapcar_file = "/storage/NW75SYB/SAPCAR_1010-70006178.EXE"
kit_swpm_file = "/storage/NW75SYB/SWPM10SP31_7-20009701.SAR"
kit_saphotagent_file = "/storage/NW75SYB/SAPHOSTAGENT51_51-20009394.SAR"

```

```

$ # SAP system configuration - for ABAP HANA
sap_sid = "NWD"
sap_ci_host = "10.243.132.10"
sap_ci_hostname = "sapnwapp01"
sap_ci_instance_number = "00"
sap_asc_s_instance_number = "01"
hdb_instance_number = "00"
sap_aas_instance_number = "00"

# Kits paths
kit_sapcar_file = "/storage/NW75HDB/SAPCAR_1010-70006178.EXE"
kit_swpm_file = "/storage/NW75HDB/SWPM10SP31_7-20009701.SAR"
kit_saphotagent_file = "/storage/NW75HDB/SAPHOSTAGENT51_51-20009394.SAR"
kit_hdbclient_file = "/storage/NW75HDB/IMDB_CLIENT20_009_28-80002082.SAR"

```

Ansible decompresses the rest of the SAP kit files. For more information, see the [readme](#) file.

5. Initialize the Terraform CLI.

```
terraform init
```

6. Create a Terraform execution plan. The Terraform execution plan summarizes all the actions that are done to create the virtual private cloud instance in your account.

```
terraform plan plan1
```

Enter an SAP main password and your API key.

The SAP main password must be 10 - 14 characters long and contain at least one digit (0-9). It can contain only the following characters: a-z, A-Z, 0-9, @, #, \$, . *This password cannot contain exclamation points '!'. The password must not start with a digit or an underscore ().*

7. Verify that the plan shows all of the resources that you want to create and that the names and values are correct. If the plan needs to be adjusted, edit the input.auto.tfvars file to correct resources and run terraform plan again.
8. Apply the saved plan.

```
$ terraform apply "plan1"
```

The virtual private cloud and components are created and you see output similar to the `terraform plan` output.

9. Add the SAP credentials and the virtual server instance IP to the SAP GUI. For more information about the SAP GUI, see [SAP GUI](#).

Next steps

If you need to rename your resources after they are created, modify the input.auto.tfvars file to change the names and run `terraform plan` and `terraform apply` again. Do not use the IBM Cloud Dashboard and user interface to modify your VPC after it is created. The Terraform scripts create a complete solution and selectively modifying resources with the user interface might cause unexpected results.

If you need to remove the SAP Netweaver 7.X on HANA or AnyDB installation, go to your project folder and run `terraform destroy`. The `terraform destroy` command does not remove the VPC in this scenario because the VPC was created before these Terraform scripts were run.

Related information

For more information about Terraform on IBM Cloud, see [Getting started with Terraform on IBM Cloud](#).

For more information about using Terraform for creating only a VPC for SAP, without the SAP architecture, see [Creating single-tier virtual private cloud for SAP by using Terraform](#).

SAP One Support Notes that apply to this document:

- [SAP Note 84555 - Windows Server, Linux®, and UNIX: Certified hardware](#)
- [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#)
- [SAP Note 2923773 - Linux® on IBM Cloud \(IaaS\): Adaption of your SAP license](#)
- [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#)
- [SAP Note 2369910 - SAP Software on Linux®: General information](#)
- [SAP Note 171380 - Released IBM hardware \(Intel processors\) and IBM cloud services offers](#)
- [SAP Note 1380654 - SAP support in IaaS environments](#)

This document is referenced by:

- [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#)
- [SAP Note 2588225 - SAP on IBM Cloud: Protect against speculative execution vulnerabilities](#)
- [SAP Note 1380654 - SAP support in IaaS environments](#)
- [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#)

Using IBM Metrics Collector for SAP (IMCS) on Linux

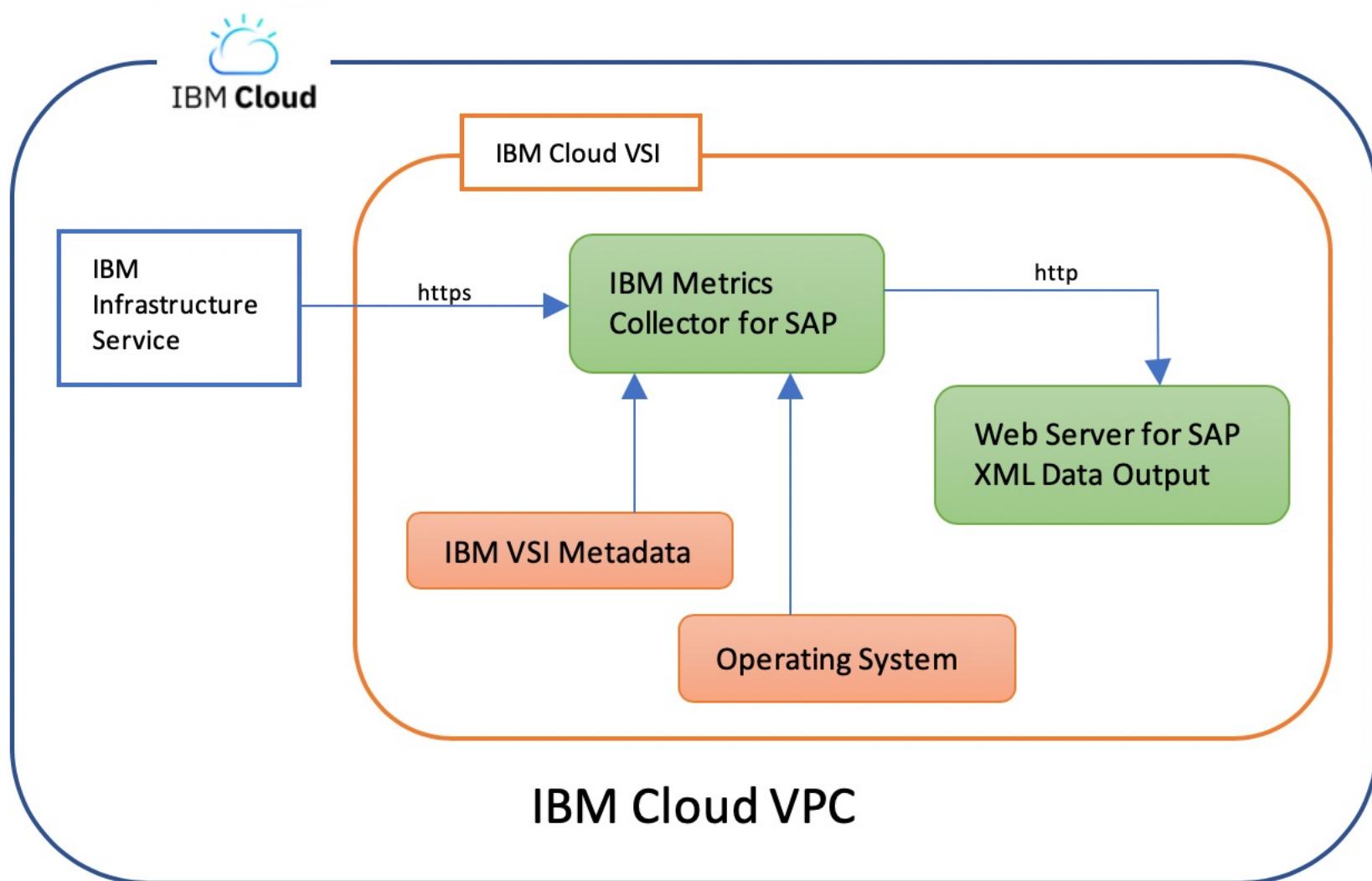


Note: The IBM® Metrics Collector for SAP (IMCS) on Linux® is a requirement by SAP Support for IBM Cloud® Virtual Private Cloud Infrastructure only when SAP workloads are running on the virtual server instance (VSI).

The IMCS collects performance-related data from IBM Cloud® Virtual Servers for Virtual Private Cloud for SAP. The SAP Support team uses the collected metric data to monitor, troubleshoot, and improve performance of business transactions. Use the following information to help with installing, configuring, and troubleshooting the IBM Metrics Collector for SAP on Linux.

Before you begin

You need to successfully create an IBM Cloud® Virtual Private Cloud and Virtual Servers for VPC by using the appropriate catalog image for SAP. Check [SAP Note 2927211](#) to make sure that the selected operating system is supported by SAP. The Metrics Collector runs specifically on Virtual Servers for VPC to gather required SAP metrics. Figure 1 outlines the data sources that are used by IBM Metrics Collector for SAP.



Data sources for IBM Metrics Collector for SAP

Getting an IBM Cloud API key

You need an IBM Cloud API key for IMCS to successfully collect all required metrics. The API key grants view access to IBM Cloud infrastructure services. You can install IMCS without an API key. However, some metrics are missing and the virtual server is not supported by SAP.

For a list of missing metrics, see [Additional Information](#).

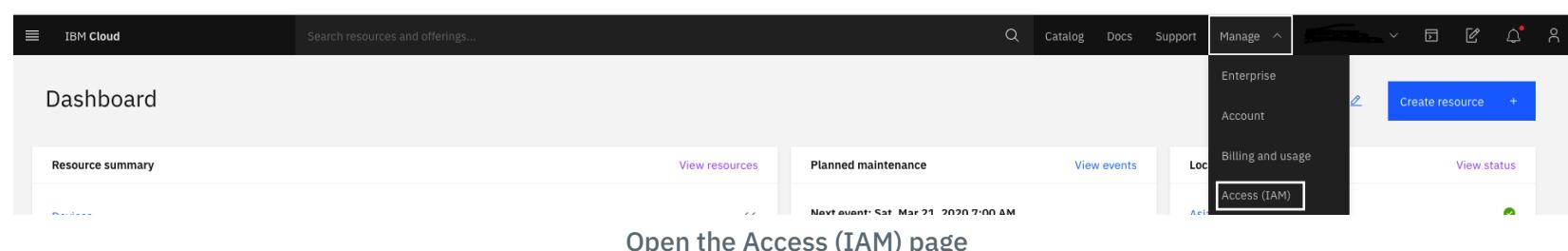
Note: You need to create only one Service ID and one API Key per Account. You can use the same Service ID and API Key for all the Metric Collectors that are installed in the virtual server that is associated to the Account.

Creating a Service ID

You need to first create a Service ID and then the related API key. Use the following steps to create a Service ID.

1. Sign in to the [IBM Cloud console](#) and click **Manage > Access (IAM)**.

Figure 2. Open the Access (IAM) page



2. Click **Services IDs > Create**.
3. Enter a **Name** and **Description** for the Service ID and click **Create**. You can assign the Access Policy after your Service ID is created.
4. Click **Access Policies > Assign Access**.
5. Click **IAM Services** for **Assign Service ID additional access**.
6. Select **VPC Infrastructure service** for **What type of access do you want to assign?**
7. Leave the default **Account** for in
8. Leave **All resource types** for **Resource type** and click **Viewer** for **Platform Access**.
9. Click **Add > Assign**. The VPC Infrastructure Service policy is assigned to your Service ID.

Creating an API Key for the Service ID.

Use the following steps to create an API Key for the new Service ID.

1. Select **Service IDs** and your newly created Service ID
2. Click the tab **Access Policy** and verify that the **VPC Infrastructure Service** is listed as an Access Policy. If not repeat steps 4-9.
3. Click the next tab **API keys > Create**.
4. Enter a **Name** and **Description** for the key and click **Create**.
5. Click **Copy** or **Download** your API key to save it.



Important: This is the only opportunity to access the API Key's data. You cannot view this API key again, so you cannot retrieve it later.

Installing the IBM Metrics Collector for SAP on Linux

The IMCS is a daemon or service that automatically starts as soon as it is installed and requires an API key. It collects metrics from the metadata of the virtual server, IBM Cloud infrastructure services, runtime data about resources, such as CPU, memory, network, and disk. The metrics are aggregated and displayed through the web server for SAP customers. SAPOS COL uses the XML output of this web server.



Important: The IMCS uses port 18181 to display the metrics. Make sure that **port 18181** is not used by any other application. For more information about checking port availability, see [Troubleshooting](#).



Note: The commands that are listed in this section were run on a Red Hat virtual server instance. If you have a SUSE virtual server, you can follow the same steps but you will see a slightly different user interface.

Use the following steps to download the IMCS.

1. [Download the IMCS](#).
2. Select the appropriate **tar.gz** file. In most cases, use the current version. Connect as **guest**.
3. Save the file to your internal Downloads folder and click **OK**.
4. Move or copy the IMCS **tar.gz** file to your VPC virtual server instance.
5. Extract the file and open the extracted folder.

```
$ tar -xvf sap-metrics-collector-v1.3.tar.gz  
cd sap
```

6. Run the **install-linux.sh** file.

```
$ ./install-linux.sh
```

7. Paste your API key when prompted. If you don't have an API key, see [Getting an IBM Cloud API key](#).
8. Check to make sure that the IMCS is running after the installation is complete. The service status displays **active** when it is ready.

```
$ sudo systemctl is-active sap-metrics-collector
```

Verifying data collection

After the installation completes and the service is started, it can take time for the IMCS begins collecting metrics. Wait at least 2 minutes after the installation before you expect full and accurate metrics.

1. Run the following **curl** command for your localhost address to see your metrics:

```
$ curl http://localhost:18181/sap/metrics
```

```
<metrics>  
  <metric category="config" context="vm" device-id="" last-refresh="1607451781" refresh-interval="0"  
    type="string" unit="none">  
    <name>Data Provider Version</name>  
    <value>1.3</value>
```

```
</metric>
<metric category="config" context="host" device-id="" last-refresh="1607451781" refresh-interval="0"
type="string" unit="none">
<name>Cloud Provider</name>
<value>IBM Cloud</value>
</metric>
<metric category="config" context="vm" device-id="" last-refresh="1607451781" refresh-interval="0"
type="string" unit="none">
<name>Instance Type</name>
<value>bx2-8x32</value>
</metric>
<metric category="config" context="host" device-id="" last-refresh="1607451781" refresh-interval="0"
type="string" unit="none">
<name>Virtualization Solution</name>
<value>KVM</value>
</metric>
.
.
.

</metrics>
```



Note: You might experience a delay before your data is available.

Troubleshooting

Use the following troubleshooting tips for IMCS.

Uninstalling the Metrics Collector

1. Run the following command to uninstall IMCS if you have any issues during the installation process. Then, reinstall it.

```
$ ./uninstall-linux.sh
```

```
Removing IBM Metric Collector for SAP...
Successfully removed IBM Metric Collector for SAP.
```

No metrics reported when you run the curl command

No reported metrics message is often due to the port not assigned to SAP Metrics Collector. It needs port **18181** available for **localhost**. If you have any other applications that use the port, you must close the applications.

1. Use the following command to see whether the port is assigned to another application.

```
$ nmap -sT -O localhost
```

```
Starting Nmap 6.40 ( http://nmap.org ) at (date and time)
Nmap scan report for localhost (your localhost address)
Host is up (0.0s latency).
Other addresses for localhost (not scanned): (localhost addresses)
rDNS record for (localhost): sap-mc-redhat
Not shown: (number of) closed ports
PORT      STATE SERVICE
(port)/tcp open  ssh
(port)/tcp open  smtp
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.7 3.9
Network Distance: 0 hops
```

nmap not found

You can install **nmap** on your system by using the appropriate package manager like **yum** or **apt-get**.

- Command for Red Hat: **yum install nmap**
- Command for SUSE: **zypper install nmap**

Additional information

If you don't have an IBM Cloud API key, the IMCS can't collect all of the metrics that are required by SAP, which include

- Network Adapter Mapping - replaced with local MAC ID.
- Network Adapter Bandwidth - Port Speed - defaults to 0.
- Disk Volume Mapping - replaced with Volume Attachment ID.
- Disk Guaranteed IOPS - defaults to 0.

 **Important:** You must provide an API key so that all metrics can be collected. Otherwise, this virtual server is not fully supported by SAP.

Using IBM Metrics Collector for SAP (IMCS) on Windows

 **Note:** The IBM® Metrics Collector for SAP (IMCS) on Windows is a requirement by SAP Support for IBM Cloud® Virtual Private Cloud Infrastructure only when SAP workloads are running on the virtual server instance (VSI).

Getting an IBM Cloud API key

You need an IBM Cloud API key for IMCS to successfully collect all required metrics. The API key grants view access to IBM Cloud infrastructure services. You can install IMCS without an API key. However, some metrics are missing and the virtual server is not supported by SAP.

For a list of missing metrics, see [Additional Information](#).

 **Note:** You need to create only one Service ID and one API Key per Account. You can use the same Service ID and API Key for all the Metric Collectors that are installed in the virtual server that is associated to the Account.

Creating a Service ID

You need to first create a Service ID and then the related API key. Use the following steps to create a Service ID.

1. Sign in to the [IBM Cloud console](#) and click **Manage > Access (IAM)**.
2. Click **Services IDs > Create**.
3. Enter a **Name** and **Description** for the Service ID and click **Create**. You can assign the Access Policy after your Service ID is created.
4. Click **Access Policies > Assign Access**.
5. Click **IAM Services** for **Assign Service ID additional access**.
6. Select **VPC Infrastructure service** for **What type of access do you want to assign?**
7. Select **All resource groups** for **in**.
8. Leave the default **Account** for **in**.
9. Leave **All resource types** for **Resource type** and click **Viewer** for **Platform Access**.
10. Click **Add > Assign**. The VPC Infrastructure Service policy is assigned to your Service ID.

Creating an API Key for the Service ID.

Use the following steps to create an API Key for the new Service ID.

1. Select **Service IDs** and your newly created Service ID
2. Click the tab **Access Policy** and verify that the **VPC Infrastructure Service** is listed as an Access Policy. If not repeat steps 4-9.
3. Click the next tab **API keys > Create**.
4. Enter a **Name** and **Description** for the key and click **Create**.
5. Click **Copy** or **Download** your API key to save it.

 **Important:** Now is the only opportunity to access the API Key data. You cannot view this API key again, so you cannot retrieve it later.

Installing the IBM Metrics Collector for SAP on Windows

The IMCS is a service that automatically starts after the installation and requires an API key. It collects metrics from the metadata of the virtual server, IBM Cloud infrastructure services, runtime data about resources, such as CPU, memory, network, and disk. The metrics are aggregated and displayed through the web server for SAP customers. SAPOS COL uses the XML output of this web server.

Important: The IMCS uses port 18181 to show the metrics. Make sure that port **18181** is not used by any other application. For more information on how to check port availability, see [Troubleshooting](#).

Note: The commands that are listed in this section were run in Windows PowerShell 5.1.

Use the following steps to download the IMCS.

1. [Download the IMCS](#).
 2. Select the appropriate .zip. In most cases, use the current version. Connect as **guest**.
 3. Save the file to your internal Downloads folder and click **OK**.
 4. Move or copy the IMCS .zip file to your VPC virtual server instance.
 5. Extract the file and open the extracted folder.
 6. Run the `install-metric-collector.ps1` file. Right-click on the file and select 'Run with Powershell', or run the following command on the power shell:

```
$ .\install-metric-collector.ps1
```

```
$ Get-Service Telegraf
Status      Name               DisplayName
-----      --
Running     Telegraf          Telegraf Data Collector Service
```

Verifying data collection

After the installation completes and the service is started, it can take time for the IMCS begins collecting metrics. Wait at least 2 minutes after the installation before you expect full and accurate metrics.

1. Open the browser of your choice.
 2. Open the following link: <http://localhost:18181/sap/metrics>

```
<metrics>
  <metric category="config" context="vm" device-id="" last-refresh="1607451781" refresh-interval="0"
type="string" unit="none">
    <name>Data Provider Version</name>
    <value>1.3</value>
  </metric>
  <metric category="config" context="host" device-id="" last-refresh="1607451781" refresh-interval="0"
type="string" unit="none">
    <name>Cloud Provider</name>
    <value>IBM Cloud</value>
  </metric>
  <metric category="config" context="vm" device-id="" last-refresh="1607451781" refresh-interval="0"
type="string" unit="none">
    <name>Instance Type</name>
    <value>bx2-8x32</value>
  </metric>
  <metric category="config" context="host" device-id="" last-refresh="1607451781" refresh-interval="0"
type="string" unit="none">
    <name>Virtualization Solution</name>
    <value>KVM</value>
  </metric>
.
```

```
</metrics>
```

You might experience a delay before your data is available. { :note }

Troubleshooting

Use the following troubleshooting tips for IMCS.

Uninstalling the Metrics Collector

- Run the following command to uninstall IMCS if you have any issues during the installation process. Then, reinstall it.

```
$ .\uninstall-metric-collector.ps1
```

```
Are you sure you want to uninstall Metric Collector for SAP? (Default is No)
( y / n ) : y
Continuing uninstalling metric collector...
Removed scheduled task: IBM Metric Collector for SAP Updater
Successfully Uninstalled Metric Collector
```

No metrics reported when you open the link

No reported metrics is often due to the port not assigned to SAP Metrics Collector. It needs port **18181** available for **localhost**. If you have any other applications using the port, you must close the applications/owning process.

- Use the following command to see whether the port is assigned to another application.

```
$ Get-NetTCPConnection -State listen
```

LocalAddress	LocalPort	RemoteAddress	RemotePort	State	AppliedSetting	OwningProcess
::	49685	::	0	Listen		704
::	49670	::	0	Listen		688
::	49668	::	0	Listen		1840
::	49667	::	0	Listen		1004
::	49666	::	0	Listen		1004
::	49665	::	0	Listen		336
::	49664	::	0	Listen		568
::	47001	::	0	Listen		4
::	5985	::	0	Listen		4
::	3389	::	0	Listen		996
::	445	::	0	Listen		4
::	135	::	0	Listen		852
0.0.0.0	49685	0.0.0.0	0	Listen		704
0.0.0.0	49670	0.0.0.0	0	Listen		688
0.0.0.0	49668	0.0.0.0	0	Listen		1840
0.0.0.0	49667	0.0.0.0	0	Listen		1004
0.0.0.0	49666	0.0.0.0	0	Listen		1004
0.0.0.0	49665	0.0.0.0	0	Listen		336
0.0.0.0	49664	0.0.0.0	0	Listen		568
0.0.0.0	3389	0.0.0.0	0	Listen		996
10.245.128.5	139	0.0.0.0	0	Listen		4
0.0.0.0	135	0.0.0.0	0	Listen		852

Ports that are used by applications

Additional information

If you don't have an IBM Cloud API key, the IMCS can't collect all of the metrics that are required by SAP, which include

- Network Adapter Mapping - replaced with local MAC ID.
- Network Adapter Bandwidth - Port Speed - defaults to 0.
- Disk Volume Mapping - replaced with Volume Attachment ID.
- Disk Guaranteed IOPS - defaults to 0.

⚠ Important: You must provide an API key so that all metrics can be collected. Otherwise, this virtual server is not fully supported by SAP.

Intel Bare Metal in VPC

Planning your deployment

Make sure that you are already familiar with the fundamental components and options that are provided by IBM Cloud Classic Infrastructure for SAP. Before you start with the deployment of servers, make sure that you also read the Get Started section.

Intel Optane persistent memory (PMem) is available on the Bare Metal servers. You have three memory options for PMem on the Bare Metal servers, 1.5 TB, 3.0 TB, and 6.0 TB. Which option you choose depends on the:

- Application that you want to run, for example BW or BW/4 HANA.
- SAP sizing, which determines the amount of memory and CPU that you need.

Network and storage configuration, disaster recovery, high availability, backups, and system replication are all configured and managed as part of the Bare Metal provisioning and operation.

The 'Must-Reads' before you start deploying

To ensure that your first deployment is a success, review the information in Provisioning SAP HANA and SAP NetWeaver [Planning your deployment](#)

Other useful documents

See the respective topics in the *Get Started* section for the following information:

- [SAP HANA design considerations for High Availability and Disaster Recovery \(HA/DR\)](#)
- [SAP HANA backups - Storage impacts on Recovery Time Objective \(RTO\)](#)
- [SAP NetWeaver design considerations for High Availability configuration](#)

VPC with Additional Application Server (AAS) ABAP on Linux for SAP HANA

You can use Terraform scripts to create a single-tier VPC and create the AAS to HANA and AnyDB infrastructure on the VPC. The Terraform scripts use the VPC information that you provide and then call the Ansible playbook to create the SAP architecture on the specified VPC.

Terraform on IBM Cloud® enables predictable and consistent provisioning of IBM Cloud Virtual Private Cloud (VPC) infrastructure resources so that you can rapidly build complex, cloud environments. IBM Cloud VPC infrastructure consists of SAP certified hardware that uses Intel® Xeon CPUs and more Intel® technologies.

You have two deployment methods to choose from:

- Terraform scripts that run from the CLI on your bastion server.
- Schematics user interface accessed from your cloud dashboard menu.

You can create SAP AAS NetWeaver 7.x on the SAP HANA-based ABAP stack.

SAP solution implemented

Many SAP enterprise solutions are built on the SAP platform (SAP NetWeaver) including:

- SAP HANA as Primary Persistence for SAP NetWeaver-based applications
- SAP Business Suite applications (ERP, CRM, and SCM, and other applications),
- SAP Business Warehouse (BW), and
- Other SAP enterprise solutions

SAP NetWeaver has two distinct aspects, ABAP and Java. Many applications that are built on the SAP NetWeaver's ABAP or Java (or both) application servers run on SAP DB owned HANA and ASE Sybase either in AnyDB platforms (MSSQL, Oracle, and Db2).

Technical interfaces are available for applications that are built on the SAP NetWeaver AS ABAP and AS Java to run on SAP HANA and AnyDB. However, specific development enablement is normally required for each application to ensure that it runs optimally on the SAP HANA. SAP Business Suite applications (ERP, CRM, SCM, and other applications), SAP Business Warehouse (BW), and other SAP NetWeaver-based applications were modified to run on SAP HANA and have many advantages. Also, various components and complimentary applications that are built on SAP NetWeaver can also run on SAP HANA or AnyDB by using the provided SAP NetWeaver DB interfaces.

The SAP HANA as primary persistence for SAP NetWeaver-based applications scenario has one restriction: SAP NetWeaver ABAP and Java application servers must run on separate hardware servers from the SAP HANA hardware.

What is created

The scripts automate the virtual infrastructure resources, provisioning the processes for the SAP architecture in an existing VPC with a distributed environment. SAP AAS NetWeaver 7.x (HANA or ASE SYB) application server on a distinct VSI VPC system and SAP HANA DB on a dedicated server type VSI VPC box are provisioned. The scripts work in two phases.

During the first phase of [Automate SAP bastion server – SAP media storage repository](#), the following virtual infrastructure resources based on the components from the existing VPC created by the bastion server are:

- 1 VPC where the virtual server instance is provisioned.
- 1 security group. The rules for this security group are:
 - Allow inbound DNS traffic (port 53).
 - Allow inbound SSH traffic (TCP port 22).
 - Allow all outbound traffic from the virtual server instance.
 - Allow all traffic in the security group.
- 1 subnet to enable the networking in your VPC.
- 2 virtual server instances with SAP certified storage and network configurations.
- 1 floating IP address used to access your VPC virtual server instance over the public network.

During the second phase, the Ansible Playbooks is called and the SAP architecture is installed for both dedicated virtual server instance (VSI) SAP application; VSI system and dedicated SAP HANA VSI box. The SAP architecture that is deployed on the SAP NetWeaver 7.x release is a stand-alone dedicated SAP HANA 2.0 box release. For more information about this architecture, see [Automating SAP HANA stand-alone virtual server instance on IBM Cloud® VPC by using Terraform and Ansible](#).

You can provision only one instance of the service per IBM Cloud region.

Schematics deployment

When you run the scripts with the Schematics interface, you:

- Enter the workspace information.
- Enter the GitHub path for the chosen solution either on NetWeaver AAS for HANA.
- Modify the parameters in the Schematics interface. They are the same parameters as the `input.auto.tfvars` file that you use with the cli.

Virtual server instance configuration

Following are the supported operating system images for SAP NetWeaver primary application server:

- ibm-redhat-8-4-amd64-sap-applications-2
- ibm-redhat-8-6-amd64-sap-applications-2
- ibm-sles-15-3-amd64-sap-applications-2
- ibm-sles-15-4-amd64-sap-applications-3

Following are the supported operating system images for SAP HANA database:

- ibm-redhat-8-4-amd64-sap-hana-2
- ibm-redhat-8-6-amd64-sap-hana-2
- ibm-sles-15-3-amd64-sap-hana-2
- ibm-sles-15-4-amd64-sap-hana-1

For both server instances there are:

- Two SSH keys are configured to access SSH as `root`.
- Three storage volumes as described in the `input.auto.tfvars` file.

What is created for anydb

The scripts use the information that you provide for an existing VPC and deploy AAS to SAP HANA or AnyDB on a different host than CI (SAP Central Instance) VSI host. For more information about this architecture, see [SAP NetWeaver 7.x on UNIX with HANA or AnyDB on IBM Cloud VPC on IBM Cloud VPC](#). You specify the information for the VPC to use in the `input.auto.tfvars` file.

The scripts call the Ansible Playbooks to install the SAP architecture.

Script files

The configuration and script files are provided on GitHub. Each supported interface for the SAP solution installation has its own folder in the GitHub repository:

- [GitHub repository for Terraform – AAS HANA](#)

Terraform interface

To run the Terraform script, you modify:

- The `input.auto.tfvars` file to specify the existing VPC resources for your solution. Specify the variables for the existing VPC:
 - VPC name
 - Security group
 - Subnet
 - Hostname
 - Profile
 - Image
 - Up to two SSH keys

You can change the default SAP system configuration settings to match your solution. You can also specify the location where you downloaded the SAP kits.

The IBM Cloud Provider plug-in for Terraform on IBM Cloud uses these configuration files to install AAS to SAP HANA and AnyDB on the specified VPC in your IBM Cloud account.

Support

There are no warranties of any kind, and there is no service or technical support available for these materials from IBM®. As a recommended practice, review carefully any materials that you download from this site before using them on a live system.

Though the materials provided herein are not supported by the IBM® Service organization, your comments are welcomed by the developers, who reserve the right to revise, readapt or remove the materials at any time. To report a problem, or provide suggestions or comments, open a GitHub issue.

Before you begin

Before you use the scripts in the bastion cli:

- Set up your account to access the VPC. Make sure that your account is [upgraded to a paid account](#).
- If you have not already, create a Bastion server to store the SAP kits. For more information, see [Automate SAP bastion server - SAP media storage repository](#).
- Download the SAP kits from the SAP Portal to your Deployment Server. Make note of the download locations. Ansible decompresses the files. For more information, see the [readme](#) file.
- [Create or retrieve an IBM Cloud API key](#). The API key is used to authenticate with the IBM Cloud platform and to determine your permissions for IBM Cloud services.
- [Create or retrieve your SSH key ID](#). You need the 40-digit UUID for the SSH key, not the SSH key name.
- Terraform should already be installed on the bastion server that you deployed. For more information, see [Bastion server for SAP deployment](#).
- (Optional - Catalog Tile) create secrets for your credentials and passwords by using the [Secrets Manager](#).

Deploying SAP AAS NetWeaver 7.x on HANA by using the Schematics user interface

Use these steps to configure the SAP Additional Application Server (AAS) NetWeaver with HANA or AnyDB on your existing VPC by using the Schematics interface. The script takes 2 - 3 hours to complete.

1. From the IBM Cloud menu, select **Schematics**.
2. Click **Create** workspace.
3. On the **Specify template** page:
 - Enter the URL for the Schematics interface.

- Select the **Terraform version** that is listed in the readme file.
 - Click **Next**.
4. On the **workspace details** page:
- Enter a name for the workspace.
 - Select a **Resource group**.
 - Select a **Location** for your workspace. The workspace location does not have to match the resource location.
 - Select **Next**.
5. Select **Create** to create your workspace.
6. On the workspace settings page, in the input variables section, review the default input variables and provide values that match your solution.
- For a more detailed description of each parameter, check the GitHub repo [AAS HANA readme](#) file, chapter “Input parameter file”. Also, make sure to mark the parameters that contain sensitive information like passwords, API, and ssh private keys as “sensitive”. These parameters are marked as “sensitive” in the readme file, under “Input parameter file”.
7. On the workspace settings page, click **Generate plan**. Wait for the plan to complete.
8. Click **View log** to review the log files of your terraform execution plan.
9. Apply your Terraform template by clicking **Apply plan**.
10. Review the log file to ensure that no errors occur during the provisioning, modification, or deletion process.

Deploying SAP AAS NetWeaver (ABAP) on HANA with the Deployable Architecture tile interface

Use these steps to configure the SAP AAS NetWeaver (ABAP) on HANA on your existing VPC by using the catalog tile interface. The script takes 2 - 3 hours to complete.

1. From the IBM Cloud catalog, select **VPC with Additional Application Server ABAP on Linux for SAP HANA** on HANA tile. The **Create** tab opens for VPC with Additional Application Server ABAP on Linux for SAP HANA. For more information about this deployment, see the About tab or the readme file link.
2. Select the latest version.
3. Select **VPC with Additional Application Server ABAP on Linux for SAP HANA on Deployable Architecture tile** variation.
4. Click **Review deployment** options:
 - **Add to project** to add this deployment to an IBM Cloud project and combine it with other deployments. IBM Cloud projects include several more pipeline steps before deployment, including deployment validation, cost calculation, compliance verification, and approval process.
 - **Create from the CLI** to get the CLI command. With this command you can trigger the deployment from the CLI.
 - **Work with code** to embed the code into other terraform deployments.
 - **Deploy with IBM Cloud Schematics** to trigger the deployment process directly.
5. Select **Deploy with IBM Cloud Schematics**.
6. Add the input parameters for this installation. There are 3 categories of parameters:
 - **Workspace** - These parameters define the workspace that is automatically created in Schematics:
 - Enter a name for the workspace or use the default name.
 - The Resource Group used to create resources. Use default or create a Resource Group.
 - Select a location to create your Schematics workspace. The workspace location need not match the resource location.
 - **Required input variables** - Review the default input variables and provide values that match your solution. These parameters are specific to your deployment. For more detailed information, see the [Readme file](#).

Parameter	Description
BASTION_FLOATING_IP	Required only for Schematics Deployments. The Floating IP from the Bastion Server.

HOSTNAME	The hostname for the VSI. The hostname should be up to 13 characters as required by SAP. For more information on the rules regarding hostnames for SAP systems, check SAP Note 611361: Hostnames of SAP ABAP Platform servers
REGION	The cloud region to deploy the solution. The regions and zones for VPC are listed here . Review supported locations in IBM Cloud Schematics here . Sample value: eu-de.
RESOURCE_GROUP	The name of an existing Resource Group for VSIs and Volumes resources. Default value: "Default". The list of Resource Groups is available here .
SECURITY_GROUP	The name of an existing Security group. The list of security groups is available here .
SSH_KEYS	The list of SSH Keys UUIDs that are allowed to SSH as root to the VSI can contain one or more IDs. The list of SSH Keys is available here . Sample input (use your own SSH UUIDs from IBM Cloud){: external}[: ["r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a", "r010-3fcfd9fe7-d4a7-41ce-8bb3-d96e936b2c7e"]]
SUBNET	The name of an existing subnet. The list of subnets is available here .
VPC	The name of an existing VPC. The list of VPCs is available here .
ZONE	The cloud zone where to deploy the solution. Sample value: eu-de-2.
ibmcloud_api_key	IBM Cloud API key (Sensitive* value).
private_ssh_key	Required only for Schematics Deployments - Input your id_rsa private key pair content in OpenSSH format (Sensitive* value). This private key should be used only during the terraform provisioning and it is recommended to be changed after the SAP deployment.
hdb_instance_number	The instance number of the SAP HANA database server.
sap_aas_instance_number	Technical identifier for the internal processes of the additional application server.
sap_ascs_instance_number	Technical identifier for the internal processes of ASCS.
sap_ci_host	IP address of the existing SAP Central Instance.
sap_ci_hostname	The hostname of the existing SAP Central Instance.
sap_ci_instance_number	Technical identifier for the internal processes of the Central Instance.
sap_sid	The SAP system ID identifies the entire SAP system.
sap_main_password	Common password for all users that are created during the installation (See Obs*).

Required Variables

- **Optional variables** - Review and update the optional input variables. The Ansible scripts expect the SAP kits to be in the default locations listed. For more information, see the [Readme file - Input Parameters](#).

Parameter	Description
ID_RSA_FILE_PATH	The file path for private_ssh_key is automatically generated by default. If it is changed, it must contain the relative path from Git repo folders. Default value: "ansible/id_rsa".
IMAGE	The OS image used for the VSI. A list of images is available here .
PROFILE	The profile used for the VSI. A list of profiles is available here . For more information about supported DB/OS and IBM Gen 2 Virtual Server Instances (VSI), check SAP Note 2927211: SAP Applications on IBM Virtual Private Cloud .

VOL1	Volume 1 Size - The size for the disks in GB that are to be attached to the VSI and used by SAP.
VOL2	Volume 2 Size - The size for the disks in GB that are to be attached to the VSI and used by SAP.
kit_sapcar_file	Path to the sapcar binary, as downloaded from SAP Support Portal.
kit_swpm_file	Path to the SWPM archive (SAR), as downloaded from SAP Support Portal.
kit_saphostagent_file	Path to the SAP Host Agent archive (SAR), as downloaded from SAP Support Portal.
kit_hdbclient_file	Path to the HANA DB client archive (SAR), as downloaded from SAP Support Portal.

Optional Variables

7. Accept the license agreement.
8. Select **Deploy**. The deployment starts and you are directed to the Schematics page that displays the script log files for you to monitor the deployment progress.

Creating the infrastructure using Terraform with the bastion server CLI

Use these steps to configure the IBM Cloud Provider plug-in and use Terraform to install SAP AAS to SAP HANA and AnyDB on your existing VPC on an already deployed SAP NetWeaver 7.X with SAP HANA 2.0 or ASE SYB as a Central Instance.

The script takes 1 - 2 hours to complete.

1. Access the bastion server cli.
2. Clone the solution repository and change to the folder.

ASE SYB 16 Clone the solution repository from <https://github.com/IBM-Cloud/sap-aas-abap-ase-syb> and cd to the sap-aas-abap-ase-syb/cli folder.

```
$ git clone https://github.com/IBM-Cloud/sap-aas-abap-ase-syb
cd sap-aas-abap-ase-syb/cli/
```

SAP HANA 2.0: Clone the solution repository from <https://github.com/IBM-Cloud/sap-abap-hana-aas> and cd to the sap-abap-hana-aas folder.

```
$ git clone https://github.com/IBM-Cloud/sap-abap-hana-aas.git
cd sap-abap-hana-aas/
```

3. Modify the `input.auto.tfvars` file to specify the information for the existing VPC, your region, zone, networking component names, hostname for the AAS VSI,profile, and image. You need your 40-digit SSH key ID for this file. The second SSH key is optional. For more options for profile, see [Instance Profiles](#). For more options, see [Images](#). For descriptions of the variables, see the [readme](#) file.

The VSI OS images that are supported for this solution for Netweaver Additional Application Server are:

- ibm-redhat-8-4-amd64-sap-applications-2
- ibm-redhat-8-6-amd64-sap-applications-2
- ibm-sles-15-3-amd64-sap-applications-2
- ibm-sles-15-4-amd64-sap-applications-4

```
$ # Infra VPC variables for ASE SYB
REGION    = "eu-de"
ZONE      = "eu-de-2"
VPC       = "ic4sap"                      # EXISTING Security group name
SECURITY_GROUP = "ic4sap-securitygroup"    # EXISTING Security group name
RESOURCE_GROUP = "wes-automation"
SUBNET    = "ic4sap-subnet"                 # EXISTING Subnet name
SSH_KEYS   = [ "r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a" , "r010-3fcfd9fe7-d4a7-41ce-8bb3-
d96e936b2c7e" ]

# SAP AAS VSI variables:
```

```

HOSTNAME = "sapnwase-as01"
PROFILE = "bx2-4x16"
IMAGE = "ibm-redhat-8-4-amd64-sap-applications-2

$ # Infra VPC variables for ABAP HANA
REGION      = "eu-de"
ZONE        = "eu-de-2"
VPC          = "ic4sap" # EXISTING Security group name
SECURITY_GROUP = "ic4sap-securitygroup" # EXISTING Security group name
RESOURCE_GROUP = "wes-automation"
SUBNET       = "ic4sap-subnet" # EXISTING Subnet name
SSH_KEYS     = [ "r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a" , "r010-3fc9fe7-d4a7-41ce-8bb3-d96e936b2c7e" ]
ID_RSA_FILE_PATH = "ansible/id_rsa"

# SAP AAS variables:
HOSTNAME = "sapnwapp"
PROFILE = "bx2-4x16"
IMAGE = "ibm-redhat-8-6-amd64-sap-applications-2"

```

4. Customize your SAP system configuration. In the same file, input.auto.tfvars, edit the SAP system configuration variables that are passed to the Ansible automated deployment. For descriptions of the variables, see the [readme](#) file.

```

$ # SAP system configuration - for ASE SYB
sap_sid = "NWD"
sap_ci_host = "10.243.132.10"
sap_ci_hostname = "sapnwase"
sap_ci_instance_number = "00"
sap_asc_s_instance_number = "01"
sap_aas_instance_number = "00"

# Kits paths
kit_sapcar_file = "/storage/NW75SYB/SAPCAR_1010-70006178.EXE"
kit_swpm_file = "/storage/NW75SYB/SWPM10SP31_7-20009701.SAR"
kit_saphotagent_file = "/storage/NW75SYB/SAPHOSTAGENT51_51-20009394.SAR"

```

```

$ # SAP system configuration - for ABAP HANA
sap_sid = "NWD"
sap_ci_host = "10.243.132.10"
sap_ci_hostname = "sapnwapp01"
sap_ci_instance_number = "00"
sap_asc_s_instance_number = "01"
hdb_instance_number = "00"
sap_aas_instance_number = "00"

# Kits paths
kit_sapcar_file = "/storage/NW75HDB/SAPCAR_1010-70006178.EXE"
kit_swpm_file = "/storage/NW75HDB/SWPM10SP31_7-20009701.SAR"
kit_saphotagent_file = "/storage/NW75HDB/SAPHOSTAGENT51_51-20009394.SAR"
kit_hdbclient_file = "/storage/NW75HDB/IMDB_CLIENT20_009_28-80002082.SAR"

```

Ansible decompresses the rest of the SAP kit files. For more information, see the [readme](#) file.

5. Initialize the Terraform CLI.

```
terraform init
```

6. Create a Terraform execution plan. The Terraform execution plan summarizes all the actions that are done to create the virtual private cloud instance in your account.

```
terraform plan plan1
```

Enter an SAP main password and your API key.

The SAP main password must be 10 - 14 characters long and contain at least one digit (0-9). It can contain only the following characters: a-z, A-Z, 0-9, @, #, \$, . *This password cannot contain exclamation points '!'. The password must not start with a digit or an underscore ().*

7. Verify that the plan shows all of the resources that you want to create and that the names and values are correct. If the plan needs to be adjusted, edit the input.auto.tfvars file to correct resources and run terraform plan again.
8. Apply the saved plan.

```
$ terraform apply "plan1"
```

The virtual private cloud and components are created and you see output similar to the `terraform plan` output.

9. Add the SAP credentials and the virtual server instance IP to the SAP GUI. For more information about the SAP GUI, see [SAP GUI](#).

Next steps

If you need to rename your resources after they are created, modify the input.auto.tfvars file to change the names and run `terraform plan` and `terraform apply` again. Do not use the IBM Cloud Dashboard and user interface to modify your VPC after it is created. The Terraform scripts create a complete solution and selectively modifying resources with the user interface might cause unexpected results.

If you need to remove the SAP Netweaver 7.X on HANA or AnyDB installation, go to your project folder and run `terraform destroy`. The `terraform destroy` command does not remove the VPC in this scenario because the VPC was created before these Terraform scripts were run.

Related information

For more information about Terraform on IBM Cloud, see [Getting started with Terraform on IBM Cloud](#).

For more information about using Terraform for creating only a VPC for SAP, without the SAP architecture, see [Creating single-tier virtual private cloud for SAP by using Terraform](#).

SAP One Support Notes that apply to this document:

- [SAP Note 84555 - Windows Server, Linux®, and UNIX: Certified hardware](#)
- [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#)
- [SAP Note 2923773 - Linux® on IBM Cloud \(IaaS\): Adaption of your SAP license](#)
- [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#)
- [SAP Note 2369910 - SAP Software on Linux®: General information](#)
- [SAP Note 171380 - Released IBM hardware \(Intel processors\) and IBM cloud services offers](#)
- [SAP Note 1380654 - SAP support in IaaS environments](#)

This document is referenced by:

- [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#)
- [SAP Note 2588225 - SAP on IBM Cloud: Protect against speculative execution vulnerabilities](#)
- [SAP Note 1380654 - SAP support in IaaS environments](#)
- [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#)

Intel Bare Metal in Classic

Planning your deployment

Make sure that you are already familiar with the fundamental components and options that are provided by IBM Cloud Classic Infrastructure for SAP. Before you start with the deployment of servers, make sure that you also read the Get Started section.

Intel Optane persistent memory (PMem) is available on the Bare Metal servers. You have three memory options for PMem on the Bare Metal servers, 1.5 TB, 3.0 TB, and 6.0 TB. Which option you choose depends on the:

- Application that you want to run, for example BW or BW/4 HANA.
- SAP sizing, which determines the amount of memory and CPU that you need.

Network and storage configuration, disaster recovery, high availability, backups, and system replication are all configured and managed as part of the Bare Metal provisioning and operation.

The 'Must-Reads' before you start deploying

To ensure that your first deployment is a success, review the information in Provisioning SAP HANA and SAP NetWeaver [Planning your deployment](#)

Other useful documents

See the respective topics in the *Get Started* section for the following information:

- [SAP HANA design considerations for High Availability and Disaster Recovery \(HA/DR\)](#)
- [SAP HANA backups - Storage impacts on Recovery Time Objective \(RTO\)](#)
- [SAP NetWeaver design considerations for High Availability configuration](#)

VPC with Additional Application Server (AAS) ABAP on Linux for SAP HANA

You can use Terraform scripts to create a single-tier VPC and create the AAS to HANA and AnyDB infrastructure on the VPC. The Terraform scripts use the VPC information that you provide and then call the Ansible playbook to create the SAP architecture on the specified VPC.

Terraform on IBM Cloud® enables predictable and consistent provisioning of IBM Cloud Virtual Private Cloud (VPC) infrastructure resources so that you can rapidly build complex, cloud environments. IBM Cloud VPC infrastructure consists of SAP certified hardware that uses Intel® Xeon CPUs and more Intel® technologies.

You have two deployment methods to choose from:

- Terraform scripts that run from the CLI on your bastion server.
- Schematics user interface accessed from your cloud dashboard menu.

You can create SAP AAS NetWeaver 7.x on the SAP HANA-based ABAP stack.

SAP solution implemented

Many SAP enterprise solutions are built on the SAP platform (SAP NetWeaver) including:

- SAP HANA as Primary Persistence for SAP NetWeaver-based applications
- SAP Business Suite applications (ERP, CRM, and SCM, and other applications),
- SAP Business Warehouse (BW), and
- Other SAP enterprise solutions

SAP NetWeaver has two distinct aspects, ABAP and Java. Many applications that are built on the SAP NetWeaver's ABAP or Java (or both) application servers run on SAP DB owned HANA and ASE Sybase either in AnyDB platforms (MSSQL, Oracle, and Db2).

Technical interfaces are available for applications that are built on the SAP NetWeaver AS ABAP and AS Java to run on SAP HANA and AnyDB. However, specific development enablement is normally required for each application to ensure that it runs optimally on the SAP HANA. SAP Business Suite applications (ERP, CRM, SCM, and other applications), SAP Business Warehouse (BW), and other SAP NetWeaver-based applications were modified to run on SAP HANA and have many advantages. Also, various components and complimentary applications that are built on SAP NetWeaver can also run on SAP HANA or AnyDB by using the provided SAP NetWeaver DB interfaces.

The SAP HANA as primary persistence for SAP NetWeaver-based applications scenario has one restriction: SAP NetWeaver ABAP and Java application servers must run on separate hardware servers from the SAP HANA hardware.

What is created

The scripts automate the virtual infrastructure resources, provisioning the processes for the SAP architecture in an existing VPC with a distributed environment. SAP AAS NetWeaver 7.x (HANA or ASE SYB) application server on a distinct VSI VPC system and SAP HANA DB on a dedicated server type VSI VPC box are provisioned. The scripts work in two phases.

During the first phase of [Automate SAP bastion server – SAP media storage repository](#), the following virtual infrastructure resources based on the components from the existing VPC created by the bastion server are:

- 1 VPC where the virtual server instance is provisioned.
- 1 security group. The rules for this security group are:
 - Allow inbound DNS traffic (port 53).
 - Allow inbound SSH traffic (TCP port 22).
 - Allow all outbound traffic from the virtual server instance.
 - Allow all traffic in the security group.
- 1 subnet to enable the networking in your VPC.
- 2 virtual server instances with SAP certified storage and network configurations.
- 1 floating IP address used to access your VPC virtual server instance over the public network.

During the second phase, the Ansible Playbooks is called and the SAP architecture is installed for both dedicated virtual server instance (VSI) SAP application; VSI system and dedicated SAP HANA VSI box. The SAP architecture that is deployed on the SAP NetWeaver 7.x release is a stand-alone dedicated SAP HANA 2.0 box release. For more information about this architecture, see [Automating SAP HANA stand-alone virtual server instance on IBM Cloud® VPC by using Terraform and Ansible](#).

You can provision only one instance of the service per IBM Cloud region.

Schematics deployment

When you run the scripts with the Schematics interface, you:

- Enter the workspace information.
- Enter the GitHub path for the chosen solution either on NetWeaver AAS for HANA.
- Modify the parameters in the Schematics interface. They are the same parameters as the `input.auto.tfvars` file that you use with the cli.

Virtual server instance configuration

Following are the supported operating system images for SAP NetWeaver primary application server:

- ibm-redhat-8-4-amd64-sap-applications-2
- ibm-redhat-8-6-amd64-sap-applications-2
- ibm-sles-15-3-amd64-sap-applications-2
- ibm-sles-15-4-amd64-sap-applications-3

Following are the supported operating system images for SAP HANA database:

- ibm-redhat-8-4-amd64-sap-hana-2
- ibm-redhat-8-6-amd64-sap-hana-2
- ibm-sles-15-3-amd64-sap-hana-2
- ibm-sles-15-4-amd64-sap-hana-1

For both server instances there are:

- Two SSH keys are configured to access SSH as `root`.
- Three storage volumes as described in the `input.auto.tfvars` file.

What is created for anydb

The scripts use the information that you provide for an existing VPC and deploy AAS to SAP HANA or AnyDB on a different host than CI (SAP Central Instance) VSI host. For more information about this architecture, see [SAP NetWeaver 7.x on UNIX with HANA or AnyDB on IBM Cloud VPC on IBM Cloud VPC](#). You specify the information for the VPC to use in the `input.auto.tfvars` file.

The scripts call the Ansible Playbooks to install the SAP architecture.

Script files

The configuration and script files are provided on GitHub. Each supported interface for the SAP solution installation has its own folder in the GitHub repository:

- [GitHub repository for Terraform – AAS HANA](#)

Terraform interface

To run the Terraform script, you modify:

- The `input.auto.tfvars` file to specify the existing VPC resources for your solution. Specify the variables for the existing VPC:
 - VPC name
 - Security group
 - Subnet
 - Hostname
 - Profile
 - Image
 - Up to two SSH keys

You can change the default SAP system configuration settings to match your solution. You can also specify the location where you downloaded the SAP kits.

The IBM Cloud Provider plug-in for Terraform on IBM Cloud uses these configuration files to install AAS to SAP HANA and AnyDB on the specified VPC in your IBM Cloud account.

Support

There are no warranties of any kind, and there is no service or technical support available for these materials from IBM®. As a recommended practice, review carefully any materials that you download from this site before using them on a live system.

Though the materials provided herein are not supported by the IBM® Service organization, your comments are welcomed by the developers, who reserve the right to revise, readapt or remove the materials at any time. To report a problem, or provide suggestions or comments, open a GitHub issue.

Before you begin

Before you use the scripts in the bastion cli:

- Set up your account to access the VPC. Make sure that your account is [upgraded to a paid account](#).
- If you have not already, create a Bastion server to store the SAP kits. For more information, see [Automate SAP bastion server - SAP media storage repository](#).
- Download the SAP kits from the SAP Portal to your Deployment Server. Make note of the download locations. Ansible decompresses the files. For more information, see the [readme](#) file.
- [Create or retrieve an IBM Cloud API key](#). The API key is used to authenticate with the IBM Cloud platform and to determine your permissions for IBM Cloud services.
- [Create or retrieve your SSH key ID](#). You need the 40-digit UUID for the SSH key, not the SSH key name.
- Terraform should already be installed on the bastion server that you deployed. For more information, see [Bastion server for SAP deployment](#).
- (Optional - Catalog Tile) create secrets for your credentials and passwords by using the [Secrets Manager](#).

Deploying SAP AAS NetWeaver 7.x on HANA by using the Schematics user interface

Use these steps to configure the SAP Additional Application Server (AAS) NetWeaver with HANA or AnyDB on your existing VPC by using the Schematics interface. The script takes 2 - 3 hours to complete.

1. From the IBM Cloud menu, select **Schematics**.
2. Click **Create** workspace.
3. On the **Specify template** page:
 - Enter the URL for the Schematics interface.

- Select the **Terraform version** that is listed in the readme file.
 - Click **Next**.
4. On the **workspace details** page:
- Enter a name for the workspace.
 - Select a **Resource group**.
 - Select a **Location** for your workspace. The workspace location does not have to match the resource location.
 - Select **Next**.
5. Select **Create** to create your workspace.
6. On the workspace settings page, in the input variables section, review the default input variables and provide values that match your solution.
- For a more detailed description of each parameter, check the GitHub repo [AAS HANA readme](#) file, chapter “Input parameter file”. Also, make sure to mark the parameters that contain sensitive information like passwords, API, and ssh private keys as “sensitive”. These parameters are marked as “sensitive” in the readme file, under “Input parameter file”.
7. On the workspace settings page, click **Generate plan**. Wait for the plan to complete.
8. Click **View log** to review the log files of your terraform execution plan.
9. Apply your Terraform template by clicking **Apply plan**.
10. Review the log file to ensure that no errors occur during the provisioning, modification, or deletion process.

Deploying SAP AAS NetWeaver (ABAP) on HANA with the Deployable Architecture tile interface

Use these steps to configure the SAP AAS NetWeaver (ABAP) on HANA on your existing VPC by using the catalog tile interface. The script takes 2 - 3 hours to complete.

1. From the IBM Cloud catalog, select **VPC with Additional Application Server ABAP on Linux for SAP HANA** on HANA tile. The **Create** tab opens for VPC with Additional Application Server ABAP on Linux for SAP HANA. For more information about this deployment, see the About tab or the readme file link.
2. Select the latest version.
3. Select **VPC with Additional Application Server ABAP on Linux for SAP HANA on Deployable Architecture tile** variation.
4. Click **Review deployment** options:
 - **Add to project** to add this deployment to an IBM Cloud project and combine it with other deployments. IBM Cloud projects include several more pipeline steps before deployment, including deployment validation, cost calculation, compliance verification, and approval process.
 - **Create from the CLI** to get the CLI command. With this command you can trigger the deployment from the CLI.
 - **Work with code** to embed the code into other terraform deployments.
 - **Deploy with IBM Cloud Schematics** to trigger the deployment process directly.
5. Select **Deploy with IBM Cloud Schematics**.
6. Add the input parameters for this installation. There are 3 categories of parameters:
 - **Workspace** - These parameters define the workspace that is automatically created in Schematics:
 - Enter a name for the workspace or use the default name.
 - The Resource Group used to create resources. Use default or create a Resource Group.
 - Select a location to create your Schematics workspace. The workspace location need not match the resource location.
 - **Required input variables** - Review the default input variables and provide values that match your solution. These parameters are specific to your deployment. For more detailed information, see the [Readme file](#).

Parameter	Description
BASTION_FLOATING_IP	Required only for Schematics Deployments. The Floating IP from the Bastion Server.

HOSTNAME	The hostname for the VSI. The hostname should be up to 13 characters as required by SAP. For more information on the rules regarding hostnames for SAP systems, check SAP Note 611361: Hostnames of SAP ABAP Platform servers
REGION	The cloud region to deploy the solution. The regions and zones for VPC are listed here . Review supported locations in IBM Cloud Schematics here . Sample value: eu-de.
RESOURCE_GROUP	The name of an existing Resource Group for VSIs and Volumes resources. Default value: "Default". The list of Resource Groups is available here .
SECURITY_GROUP	The name of an existing Security group. The list of security groups is available here .
SSH_KEYS	The list of SSH Keys UUIDs that are allowed to SSH as root to the VSI can contain one or more IDs. The list of SSH Keys is available here . Sample input (use your own SSH UUIDs from IBM Cloud){: external}: ["r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a", "r010-3fcfd9fe7-d4a7-41ce-8bb3-d96e936b2c7e"]
SUBNET	The name of an existing subnet. The list of subnets is available here .
VPC	The name of an existing VPC. The list of VPCs is available here .
ZONE	The cloud zone where to deploy the solution. Sample value: eu-de-2.
ibmcloud_api_key	IBM Cloud API key (Sensitive* value).
private_ssh_key	Required only for Schematics Deployments - Input your id_rsa private key pair content in OpenSSH format (Sensitive* value). This private key should be used only during the terraform provisioning and it is recommended to be changed after the SAP deployment.
hdb_instance_number	The instance number of the SAP HANA database server.
sap_aas_instance_number	Technical identifier for the internal processes of the additional application server.
sap_asci_instance_number	Technical identifier for the internal processes of ASCS.
sap_ci_host	IP address of the existing SAP Central Instance.
sap_ci_hostname	The hostname of the existing SAP Central Instance.
sap_ci_instance_number	Technical identifier for the internal processes of the Central Instance.
sap_sid	The SAP system ID identifies the entire SAP system.
sap_main_password	Common password for all users that are created during the installation (See Obs*).

Required Variables

- **Optional variables** - Review and update the optional input variables. The Ansible scripts expect the SAP kits to be in the default locations listed. For more information, see the [Readme file - Input Parameters](#).

Parameter	Description
ID_RSA_FILE_PATH	The file path for private_ssh_key is automatically generated by default. If it is changed, it must contain the relative path from Git repo folders. Default value: "ansible/id_rsa".
IMAGE	The OS image used for the VSI. A list of images is available here .
PROFILE	The profile used for the VSI. A list of profiles is available here . For more information about supported DB/OS and IBM Gen 2 Virtual Server Instances (VSI), check SAP Note 2927211: SAP Applications on IBM Virtual Private Cloud .

VOL1	Volume 1 Size - The size for the disks in GB that are to be attached to the VSI and used by SAP.
VOL2	Volume 2 Size - The size for the disks in GB that are to be attached to the VSI and used by SAP.
kit_sapcar_file	Path to the sapcar binary, as downloaded from SAP Support Portal.
kit_swpm_file	Path to the SWPM archive (SAR), as downloaded from SAP Support Portal.
kit_saphostagent_file	Path to the SAP Host Agent archive (SAR), as downloaded from SAP Support Portal.
kit_hdbclient_file	Path to the HANA DB client archive (SAR), as downloaded from SAP Support Portal.

Optional Variables

7. Accept the license agreement.
8. Select **Deploy**. The deployment starts and you are directed to the Schematics page that displays the script log files for you to monitor the deployment progress.

Creating the infrastructure using Terraform with the bastion server CLI

Use these steps to configure the IBM Cloud Provider plug-in and use Terraform to install SAP AAS to SAP HANA and AnyDB on your existing VPC on an already deployed SAP NetWeaver 7.X with SAP HANA 2.0 or ASE SYB as a Central Instance.

The script takes 1 - 2 hours to complete.

1. Access the bastion server cli.
2. Clone the solution repository and change to the folder.

ASE SYB 16 Clone the solution repository from <https://github.com/IBM-Cloud/sap-aas-abap-ase-syb> and cd to the sap-aas-abap-ase-syb/cli folder.

```
$ git clone https://github.com/IBM-Cloud/sap-aas-abap-ase-syb
cd sap-aas-abap-ase-syb/cli/
```

SAP HANA 2.0: Clone the solution repository from <https://github.com/IBM-Cloud/sap-abap-hana-aas> and cd to the sap-abap-hana-aas folder.

```
$ git clone https://github.com/IBM-Cloud/sap-abap-hana-aas.git
cd sap-abap-hana-aas/
```

3. Modify the `input.auto.tfvars` file to specify the information for the existing VPC, your region, zone, networking component names, hostname for the AAS VSI,profile, and image. You need your 40-digit SSH key ID for this file. The second SSH key is optional. For more options for profile, see [Instance Profiles](#). For more options, see [Images](#). For descriptions of the variables, see the [readme](#) file.

The VSI OS images that are supported for this solution for Netweaver Additional Application Server are:

- ibm-redhat-8-4-amd64-sap-applications-2
- ibm-redhat-8-6-amd64-sap-applications-2
- ibm-sles-15-3-amd64-sap-applications-2
- ibm-sles-15-4-amd64-sap-applications-4

```
$ # Infra VPC variables for ASE SYB
REGION    = "eu-de"
ZONE      = "eu-de-2"
VPC       = "ic4sap"                      # EXISTING Security group name
SECURITY_GROUP = "ic4sap-securitygroup"     # EXISTING Security group name
RESOURCE_GROUP = "wes-automation"
SUBNET    = "ic4sap-subnet"                 # EXISTING Subnet name
SSH_KEYS   = [ "r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a" , "r010-3fcfd9fe7-d4a7-41ce-8bb3-
d96e936b2c7e" ]

# SAP AAS VSI variables:
```

```

HOSTNAME = "sapnwase-as01"
PROFILE = "bx2-4x16"
IMAGE = "ibm-redhat-8-4-amd64-sap-applications-2

$ # Infra VPC variables for ABAP HANA
REGION      = "eu-de"
ZONE        = "eu-de-2"
VPC          = "ic4sap" # EXISTING Security group name
SECURITY_GROUP = "ic4sap-securitygroup" # EXISTING Security group name
RESOURCE_GROUP = "wes-automation"
SUBNET       = "ic4sap-subnet" # EXISTING Subnet name
SSH_KEYS     = [ "r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a" , "r010-3fc9fe7-d4a7-41ce-8bb3-d96e936b2c7e" ]
ID_RSA_FILE_PATH = "ansible/id_rsa"

# SAP AAS variables:
HOSTNAME = "sapnwapp"
PROFILE = "bx2-4x16"
IMAGE = "ibm-redhat-8-6-amd64-sap-applications-2"

```

4. Customize your SAP system configuration. In the same file, input.auto.tfvars, edit the SAP system configuration variables that are passed to the Ansible automated deployment. For descriptions of the variables, see the [readme](#) file.

```

$ # SAP system configuration - for ASE SYB
sap_sid = "NWD"
sap_ci_host = "10.243.132.10"
sap_ci_hostname = "sapnwase"
sap_ci_instance_number = "00"
sap_asc_s_instance_number = "01"
sap_aas_instance_number = "00"

# Kits paths
kit_sapcar_file = "/storage/NW75SYB/SAPCAR_1010-70006178.EXE"
kit_swpm_file = "/storage/NW75SYB/SWPM10SP31_7-20009701.SAR"
kit_saphotagent_file = "/storage/NW75SYB/SAPHOSTAGENT51_51-20009394.SAR"

```

```

$ # SAP system configuration - for ABAP HANA
sap_sid = "NWD"
sap_ci_host = "10.243.132.10"
sap_ci_hostname = "sapnwapp01"
sap_ci_instance_number = "00"
sap_asc_s_instance_number = "01"
hdb_instance_number = "00"
sap_aas_instance_number = "00"

# Kits paths
kit_sapcar_file = "/storage/NW75HDB/SAPCAR_1010-70006178.EXE"
kit_swpm_file = "/storage/NW75HDB/SWPM10SP31_7-20009701.SAR"
kit_saphotagent_file = "/storage/NW75HDB/SAPHOSTAGENT51_51-20009394.SAR"
kit_hdbclient_file = "/storage/NW75HDB/IMDB_CLIENT20_009_28-80002082.SAR"

```

Ansible decompresses the rest of the SAP kit files. For more information, see the [readme](#) file.

5. Initialize the Terraform CLI.

```
terraform init
```

6. Create a Terraform execution plan. The Terraform execution plan summarizes all the actions that are done to create the virtual private cloud instance in your account.

```
terraform plan plan1
```

Enter an SAP main password and your API key.

The SAP main password must be 10 - 14 characters long and contain at least one digit (0-9). It can contain only the following characters: a-z, A-Z, 0-9, @, #, \$, . *This password cannot contain exclamation points '!'. The password must not start with a digit or an underscore ().*

7. Verify that the plan shows all of the resources that you want to create and that the names and values are correct. If the plan needs to be adjusted, edit the input.auto.tfvars file to correct resources and run terraform plan again.
8. Apply the saved plan.

```
$ terraform apply "plan1"
```

The virtual private cloud and components are created and you see output similar to the `terraform plan` output.

9. Add the SAP credentials and the virtual server instance IP to the SAP GUI. For more information about the SAP GUI, see [SAP GUI](#).

Next steps

If you need to rename your resources after they are created, modify the input.auto.tfvars file to change the names and run `terraform plan` and `terraform apply` again. Do not use the IBM Cloud Dashboard and user interface to modify your VPC after it is created. The Terraform scripts create a complete solution and selectively modifying resources with the user interface might cause unexpected results.

If you need to remove the SAP Netweaver 7.X on HANA or AnyDB installation, go to your project folder and run `terraform destroy`. The `terraform destroy` command does not remove the VPC in this scenario because the VPC was created before these Terraform scripts were run.

Related information

For more information about Terraform on IBM Cloud, see [Getting started with Terraform on IBM Cloud](#).

For more information about using Terraform for creating only a VPC for SAP, without the SAP architecture, see [Creating single-tier virtual private cloud for SAP by using Terraform](#).

SAP One Support Notes that apply to this document:

- [SAP Note 84555 - Windows Server, Linux®, and UNIX: Certified hardware](#)
- [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#)
- [SAP Note 2923773 - Linux® on IBM Cloud \(IaaS\): Adaption of your SAP license](#)
- [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#)
- [SAP Note 2369910 - SAP Software on Linux®: General information](#)
- [SAP Note 171380 - Released IBM hardware \(Intel processors\) and IBM cloud services offers](#)
- [SAP Note 1380654 - SAP support in IaaS environments](#)

This document is referenced by:

- [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#)
- [SAP Note 2588225 - SAP on IBM Cloud: Protect against speculative execution vulnerabilities](#)
- [SAP Note 1380654 - SAP support in IaaS environments](#)
- [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#)

Intel Bare Metal with Intel Optane DC PMEM in Classic

Planning your deployment

Make sure that you are already familiar with the fundamental components and options that are provided by IBM Cloud Classic Infrastructure for SAP. Before you start with the deployment of servers, make sure that you also read the Get Started section.

Intel Optane persistent memory (PMem) is available on the Bare Metal servers. You have three memory options for PMem on the Bare Metal servers, 1.5 TB, 3.0 TB, and 6.0 TB. Which option you choose depends on the:

- Application that you want to run, for example BW or BW/4 HANA.
- SAP sizing, which determines the amount of memory and CPU that you need.

Network and storage configuration, disaster recovery, high availability, backups, and system replication are all configured and managed as part of the Bare Metal provisioning and operation.

The 'Must-Reads' before you start deploying

To ensure that your first deployment is a success, review the information in Provisioning SAP HANA and SAP NetWeaver [Planning your deployment](#)

Other useful documents

See the respective topics in the *Get Started* section for the following information:

- [SAP HANA design considerations for High Availability and Disaster Recovery \(HA/DR\)](#)
- [SAP HANA backups - Storage impacts on Recovery Time Objective \(RTO\)](#)
- [SAP NetWeaver design considerations for High Availability configuration](#)

VPC with Additional Application Server (AAS) ABAP on Linux for SAP HANA

You can use Terraform scripts to create a single-tier VPC and create the AAS to HANA and AnyDB infrastructure on the VPC. The Terraform scripts use the VPC information that you provide and then call the Ansible playbook to create the SAP architecture on the specified VPC.

Terraform on IBM Cloud® enables predictable and consistent provisioning of IBM Cloud Virtual Private Cloud (VPC) infrastructure resources so that you can rapidly build complex, cloud environments. IBM Cloud VPC infrastructure consists of SAP certified hardware that uses Intel® Xeon CPUs and more Intel® technologies.

You have two deployment methods to choose from:

- Terraform scripts that run from the CLI on your bastion server.
- Schematics user interface accessed from your cloud dashboard menu.

You can create SAP AAS NetWeaver 7.x on the SAP HANA-based ABAP stack.

SAP solution implemented

Many SAP enterprise solutions are built on the SAP platform (SAP NetWeaver) including:

- SAP HANA as Primary Persistence for SAP NetWeaver-based applications
- SAP Business Suite applications (ERP, CRM, and SCM, and other applications),
- SAP Business Warehouse (BW), and
- Other SAP enterprise solutions

SAP NetWeaver has two distinct aspects, ABAP and Java. Many applications that are built on the SAP NetWeaver's ABAP or Java (or both) application servers run on SAP DB owned HANA and ASE Sybase either in AnyDB platforms (MSSQL, Oracle, and Db2).

Technical interfaces are available for applications that are built on the SAP NetWeaver AS ABAP and AS Java to run on SAP HANA and AnyDB. However, specific development enablement is normally required for each application to ensure that it runs optimally on the SAP HANA. SAP Business Suite applications (ERP, CRM, SCM, and other applications), SAP Business Warehouse (BW), and other SAP NetWeaver-based applications were modified to run on SAP HANA and have many advantages. Also, various components and complimentary applications that are built on SAP NetWeaver can also run on SAP HANA or AnyDB by using the provided SAP NetWeaver DB interfaces.

The SAP HANA as primary persistence for SAP NetWeaver-based applications scenario has one restriction: SAP NetWeaver ABAP and Java application servers must run on separate hardware servers from the SAP HANA hardware.

What is created

The scripts automate the virtual infrastructure resources, provisioning the processes for the SAP architecture in an existing VPC with a distributed environment. SAP AAS NetWeaver 7.x (HANA or ASE SYB) application server on a distinct VSI VPC system and SAP HANA DB on a dedicated server type VSI VPC box are provisioned. The scripts work in two phases.

During the first phase of [Automate SAP bastion server – SAP media storage repository](#), the following virtual infrastructure resources based on the components from the existing VPC created by the bastion server are:

- 1 VPC where the virtual server instance is provisioned.
- 1 security group. The rules for this security group are:
 - Allow inbound DNS traffic (port 53).
 - Allow inbound SSH traffic (TCP port 22).
 - Allow all outbound traffic from the virtual server instance.
 - Allow all traffic in the security group.
- 1 subnet to enable the networking in your VPC.
- 2 virtual server instances with SAP certified storage and network configurations.
- 1 floating IP address used to access your VPC virtual server instance over the public network.

During the second phase, the Ansible Playbooks is called and the SAP architecture is installed for both dedicated virtual server instance (VSI) SAP application; VSI system and dedicated SAP HANA VSI box. The SAP architecture that is deployed on the SAP NetWeaver 7.x release is a stand-alone dedicated SAP HANA 2.0 box release. For more information about this architecture, see [Automating SAP HANA stand-alone virtual server instance on IBM Cloud® VPC by using Terraform and Ansible](#).

You can provision only one instance of the service per IBM Cloud region.

Schematics deployment

When you run the scripts with the Schematics interface, you:

- Enter the workspace information.
- Enter the GitHub path for the chosen solution either on NetWeaver AAS for HANA.
- Modify the parameters in the Schematics interface. They are the same parameters as the `input.auto.tfvars` file that you use with the cli.

Virtual server instance configuration

Following are the supported operating system images for SAP NetWeaver primary application server:

- ibm-redhat-8-4-amd64-sap-applications-2
- ibm-redhat-8-6-amd64-sap-applications-2
- ibm-sles-15-3-amd64-sap-applications-2
- ibm-sles-15-4-amd64-sap-applications-3

Following are the supported operating system images for SAP HANA database:

- ibm-redhat-8-4-amd64-sap-hana-2
- ibm-redhat-8-6-amd64-sap-hana-2
- ibm-sles-15-3-amd64-sap-hana-2
- ibm-sles-15-4-amd64-sap-hana-1

For both server instances there are:

- Two SSH keys are configured to access SSH as `root`.
- Three storage volumes as described in the `input.auto.tfvars` file.

What is created for anydb

The scripts use the information that you provide for an existing VPC and deploy AAS to SAP HANA or AnyDB on a different host than CI (SAP Central Instance) VSI host. For more information about this architecture, see [SAP NetWeaver 7.x on UNIX with HANA or AnyDB on IBM Cloud VPC on IBM Cloud VPC](#). You specify the information for the VPC to use in the `input.auto.tfvars` file.

The scripts call the Ansible Playbooks to install the SAP architecture.

Script files

The configuration and script files are provided on GitHub. Each supported interface for the SAP solution installation has its own folder in the GitHub repository:

- [GitHub repository for Terraform – AAS HANA](#)

Terraform interface

To run the Terraform script, you modify:

- The `input.auto.tfvars` file to specify the existing VPC resources for your solution. Specify the variables for the existing VPC:
 - VPC name
 - Security group
 - Subnet
 - Hostname
 - Profile
 - Image
 - Up to two SSH keys

You can change the default SAP system configuration settings to match your solution. You can also specify the location where you downloaded the SAP kits.

The IBM Cloud Provider plug-in for Terraform on IBM Cloud uses these configuration files to install AAS to SAP HANA and AnyDB on the specified VPC in your IBM Cloud account.

Support

There are no warranties of any kind, and there is no service or technical support available for these materials from IBM®. As a recommended practice, review carefully any materials that you download from this site before using them on a live system.

Though the materials provided herein are not supported by the IBM® Service organization, your comments are welcomed by the developers, who reserve the right to revise, readapt or remove the materials at any time. To report a problem, or provide suggestions or comments, open a GitHub issue.

Before you begin

Before you use the scripts in the bastion cli:

- Set up your account to access the VPC. Make sure that your account is [upgraded to a paid account](#).
- If you have not already, create a Bastion server to store the SAP kits. For more information, see [Automate SAP bastion server - SAP media storage repository](#).
- Download the SAP kits from the SAP Portal to your Deployment Server. Make note of the download locations. Ansible decompresses the files. For more information, see the [readme](#) file.
- [Create or retrieve an IBM Cloud API key](#). The API key is used to authenticate with the IBM Cloud platform and to determine your permissions for IBM Cloud services.
- [Create or retrieve your SSH key ID](#). You need the 40-digit UUID for the SSH key, not the SSH key name.
- Terraform should already be installed on the bastion server that you deployed. For more information, see [Bastion server for SAP deployment](#).
- (Optional - Catalog Tile) create secrets for your credentials and passwords by using the [Secrets Manager](#).

Deploying SAP AAS NetWeaver 7.x on HANA by using the Schematics user interface

Use these steps to configure the SAP Additional Application Server (AAS) NetWeaver with HANA or AnyDB on your existing VPC by using the Schematics interface. The script takes 2 - 3 hours to complete.

1. From the IBM Cloud menu, select **Schematics**.
2. Click **Create** workspace.
3. On the **Specify template** page:
 - Enter the URL for the Schematics interface.

- Select the **Terraform version** that is listed in the readme file.
 - Click **Next**.
4. On the **workspace details** page:
- Enter a name for the workspace.
 - Select a **Resource group**.
 - Select a **Location** for your workspace. The workspace location does not have to match the resource location.
 - Select **Next**.
5. Select **Create** to create your workspace.
6. On the workspace settings page, in the input variables section, review the default input variables and provide values that match your solution.
- For a more detailed description of each parameter, check the GitHub repo [AAS HANA readme](#) file, chapter “Input parameter file”. Also, make sure to mark the parameters that contain sensitive information like passwords, API, and ssh private keys as “sensitive”. These parameters are marked as “sensitive” in the readme file, under “Input parameter file”.
7. On the workspace settings page, click **Generate plan**. Wait for the plan to complete.
8. Click **View log** to review the log files of your terraform execution plan.
9. Apply your Terraform template by clicking **Apply plan**.
10. Review the log file to ensure that no errors occur during the provisioning, modification, or deletion process.

Deploying SAP AAS NetWeaver (ABAP) on HANA with the Deployable Architecture tile interface

Use these steps to configure the SAP AAS NetWeaver (ABAP) on HANA on your existing VPC by using the catalog tile interface. The script takes 2 - 3 hours to complete.

1. From the IBM Cloud catalog, select **VPC with Additional Application Server ABAP on Linux for SAP HANA** on HANA tile. The **Create** tab opens for VPC with Additional Application Server ABAP on Linux for SAP HANA. For more information about this deployment, see the About tab or the readme file link.
2. Select the latest version.
3. Select **VPC with Additional Application Server ABAP on Linux for SAP HANA on Deployable Architecture tile** variation.
4. Click **Review deployment** options:
 - **Add to project** to add this deployment to an IBM Cloud project and combine it with other deployments. IBM Cloud projects include several more pipeline steps before deployment, including deployment validation, cost calculation, compliance verification, and approval process.
 - **Create from the CLI** to get the CLI command. With this command you can trigger the deployment from the CLI.
 - **Work with code** to embed the code into other terraform deployments.
 - **Deploy with IBM Cloud Schematics** to trigger the deployment process directly.
5. Select **Deploy with IBM Cloud Schematics**.
6. Add the input parameters for this installation. There are 3 categories of parameters:
 - **Workspace** - These parameters define the workspace that is automatically created in Schematics:
 - Enter a name for the workspace or use the default name.
 - The Resource Group used to create resources. Use default or create a Resource Group.
 - Select a location to create your Schematics workspace. The workspace location need not match the resource location.
 - **Required input variables** - Review the default input variables and provide values that match your solution. These parameters are specific to your deployment. For more detailed information, see the [Readme file](#).

Parameter	Description
BASTION_FLOATING_IP	Required only for Schematics Deployments. The Floating IP from the Bastion Server.

HOSTNAME	The hostname for the VSI. The hostname should be up to 13 characters as required by SAP. For more information on the rules regarding hostnames for SAP systems, check SAP Note 611361: Hostnames of SAP ABAP Platform servers
REGION	The cloud region to deploy the solution. The regions and zones for VPC are listed here . Review supported locations in IBM Cloud Schematics here . Sample value: eu-de.
RESOURCE_GROUP	The name of an existing Resource Group for VSIs and Volumes resources. Default value: "Default". The list of Resource Groups is available here .
SECURITY_GROUP	The name of an existing Security group. The list of security groups is available here .
SSH_KEYS	The list of SSH Keys UUIDs that are allowed to SSH as root to the VSI can contain one or more IDs. The list of SSH Keys is available here . Sample input (use your own SSH UUIDs from IBM Cloud){: external}: ["r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a", "r010-3fcfd9fe7-d4a7-41ce-8bb3-d96e936b2c7e"]
SUBNET	The name of an existing subnet. The list of subnets is available here .
VPC	The name of an existing VPC. The list of VPCs is available here .
ZONE	The cloud zone where to deploy the solution. Sample value: eu-de-2.
ibmcloud_api_key	IBM Cloud API key (Sensitive* value).
private_ssh_key	Required only for Schematics Deployments - Input your id_rsa private key pair content in OpenSSH format (Sensitive* value). This private key should be used only during the terraform provisioning and it is recommended to be changed after the SAP deployment.
hdb_instance_number	The instance number of the SAP HANA database server.
sap_aas_instance_number	Technical identifier for the internal processes of the additional application server.
sap_asci_instance_number	Technical identifier for the internal processes of ASCS.
sap_ci_host	IP address of the existing SAP Central Instance.
sap_ci_hostname	The hostname of the existing SAP Central Instance.
sap_ci_instance_number	Technical identifier for the internal processes of the Central Instance.
sap_sid	The SAP system ID identifies the entire SAP system.
sap_main_password	Common password for all users that are created during the installation (See Obs*).

Required Variables

- **Optional variables** - Review and update the optional input variables. The Ansible scripts expect the SAP kits to be in the default locations listed. For more information, see the [Readme file - Input Parameters](#).

Parameter	Description
ID_RSA_FILE_PATH	The file path for private_ssh_key is automatically generated by default. If it is changed, it must contain the relative path from Git repo folders. Default value: "ansible/id_rsa".
IMAGE	The OS image used for the VSI. A list of images is available here .
PROFILE	The profile used for the VSI. A list of profiles is available here . For more information about supported DB/OS and IBM Gen 2 Virtual Server Instances (VSI), check SAP Note 2927211: SAP Applications on IBM Virtual Private Cloud .

VOL1	Volume 1 Size - The size for the disks in GB that are to be attached to the VSI and used by SAP.
VOL2	Volume 2 Size - The size for the disks in GB that are to be attached to the VSI and used by SAP.
kit_sapcar_file	Path to the sapcar binary, as downloaded from SAP Support Portal.
kit_swpm_file	Path to the SWPM archive (SAR), as downloaded from SAP Support Portal.
kit_saphostagent_file	Path to the SAP Host Agent archive (SAR), as downloaded from SAP Support Portal.
kit_hdbclient_file	Path to the HANA DB client archive (SAR), as downloaded from SAP Support Portal.

Optional Variables

7. Accept the license agreement.
8. Select **Deploy**. The deployment starts and you are directed to the Schematics page that displays the script log files for you to monitor the deployment progress.

Creating the infrastructure using Terraform with the bastion server CLI

Use these steps to configure the IBM Cloud Provider plug-in and use Terraform to install SAP AAS to SAP HANA and AnyDB on your existing VPC on an already deployed SAP NetWeaver 7.X with SAP HANA 2.0 or ASE SYB as a Central Instance.

The script takes 1 - 2 hours to complete.

1. Access the bastion server cli.
2. Clone the solution repository and change to the folder.

ASE SYB 16 Clone the solution repository from <https://github.com/IBM-Cloud/sap-aas-abap-ase-syb> and cd to the sap-aas-abap-ase-syb/cli folder.

```
$ git clone https://github.com/IBM-Cloud/sap-aas-abap-ase-syb
cd sap-aas-abap-ase-syb/cli/
```

SAP HANA 2.0: Clone the solution repository from <https://github.com/IBM-Cloud/sap-abap-hana-aas> and cd to the sap-abap-hana-aas folder.

```
$ git clone https://github.com/IBM-Cloud/sap-abap-hana-aas.git
cd sap-abap-hana-aas/
```

3. Modify the `input.auto.tfvars` file to specify the information for the existing VPC, your region, zone, networking component names, hostname for the AAS VSI,profile, and image. You need your 40-digit SSH key ID for this file. The second SSH key is optional. For more options for profile, see [Instance Profiles](#). For more options, see [Images](#). For descriptions of the variables, see the [readme](#) file.

The VSI OS images that are supported for this solution for Netweaver Additional Application Server are:

- ibm-redhat-8-4-amd64-sap-applications-2
- ibm-redhat-8-6-amd64-sap-applications-2
- ibm-sles-15-3-amd64-sap-applications-2
- ibm-sles-15-4-amd64-sap-applications-4

```
$ # Infra VPC variables for ASE SYB
REGION    = "eu-de"
ZONE      = "eu-de-2"
VPC       = "ic4sap"                      # EXISTING Security group name
SECURITY_GROUP = "ic4sap-securitygroup"     # EXISTING Security group name
RESOURCE_GROUP = "wes-automation"
SUBNET    = "ic4sap-subnet"                 # EXISTING Subnet name
SSH_KEYS   = [ "r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a" , "r010-3fcfd9fe7-d4a7-41ce-8bb3-
d96e936b2c7e" ]

# SAP AAS VSI variables:
```

```

HOSTNAME = "sapnwase-as01"
PROFILE = "bx2-4x16"
IMAGE = "ibm-redhat-8-4-amd64-sap-applications-2

$ # Infra VPC variables for ABAP HANA
REGION      = "eu-de"
ZONE        = "eu-de-2"
VPC          = "ic4sap" # EXISTING Security group name
SECURITY_GROUP = "ic4sap-securitygroup" # EXISTING Security group name
RESOURCE_GROUP = "wes-automation"
SUBNET       = "ic4sap-subnet" # EXISTING Subnet name
SSH_KEYS     = [ "r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a" , "r010-3fc9fe7-d4a7-41ce-8bb3-d96e936b2c7e" ]
ID_RSA_FILE_PATH = "ansible/id_rsa"

# SAP AAS variables:
HOSTNAME = "sapnwapp"
PROFILE = "bx2-4x16"
IMAGE = "ibm-redhat-8-6-amd64-sap-applications-2"

```

4. Customize your SAP system configuration. In the same file, input.auto.tfvars, edit the SAP system configuration variables that are passed to the Ansible automated deployment. For descriptions of the variables, see the [readme](#) file.

```

$ # SAP system configuration - for ASE SYB
sap_sid = "NWD"
sap_ci_host = "10.243.132.10"
sap_ci_hostname = "sapnwase"
sap_ci_instance_number = "00"
sap_asc_s_instance_number = "01"
sap_aas_instance_number = "00"

# Kits paths
kit_sapcar_file = "/storage/NW75SYB/SAPCAR_1010-70006178.EXE"
kit_swpm_file = "/storage/NW75SYB/SWPM10SP31_7-20009701.SAR"
kit_saphotagent_file = "/storage/NW75SYB/SAPHOSTAGENT51_51-20009394.SAR"

```

```

$ # SAP system configuration - for ABAP HANA
sap_sid = "NWD"
sap_ci_host = "10.243.132.10"
sap_ci_hostname = "sapnwapp01"
sap_ci_instance_number = "00"
sap_asc_s_instance_number = "01"
hdb_instance_number = "00"
sap_aas_instance_number = "00"

# Kits paths
kit_sapcar_file = "/storage/NW75HDB/SAPCAR_1010-70006178.EXE"
kit_swpm_file = "/storage/NW75HDB/SWPM10SP31_7-20009701.SAR"
kit_saphotagent_file = "/storage/NW75HDB/SAPHOSTAGENT51_51-20009394.SAR"
kit_hdbclient_file = "/storage/NW75HDB/IMDB_CLIENT20_009_28-80002082.SAR"

```

Ansible decompresses the rest of the SAP kit files. For more information, see the [readme](#) file.

5. Initialize the Terraform CLI.

```
terraform init
```

6. Create a Terraform execution plan. The Terraform execution plan summarizes all the actions that are done to create the virtual private cloud instance in your account.

```
terraform plan plan1
```

Enter an SAP main password and your API key.

The SAP main password must be 10 - 14 characters long and contain at least one digit (0-9). It can contain only the following characters: a-z, A-Z, 0-9, @, #, \$, . *This password cannot contain exclamation points '!'. The password must not start with a digit or an underscore ().*

7. Verify that the plan shows all of the resources that you want to create and that the names and values are correct. If the plan needs to be adjusted, edit the input.auto.tfvars file to correct resources and run terraform plan again.
8. Apply the saved plan.

```
$ terraform apply "plan1"
```

The virtual private cloud and components are created and you see output similar to the `terraform plan` output.

9. Add the SAP credentials and the virtual server instance IP to the SAP GUI. For more information about the SAP GUI, see [SAP GUI](#).

Next steps

If you need to rename your resources after they are created, modify the input.auto.tfvars file to change the names and run `terraform plan` and `terraform apply` again. Do not use the IBM Cloud Dashboard and user interface to modify your VPC after it is created. The Terraform scripts create a complete solution and selectively modifying resources with the user interface might cause unexpected results.

If you need to remove the SAP Netweaver 7.X on HANA or AnyDB installation, go to your project folder and run `terraform destroy`. The `terraform destroy` command does not remove the VPC in this scenario because the VPC was created before these Terraform scripts were run.

Related information

For more information about Terraform on IBM Cloud, see [Getting started with Terraform on IBM Cloud](#).

For more information about using Terraform for creating only a VPC for SAP, without the SAP architecture, see [Creating single-tier virtual private cloud for SAP by using Terraform](#).

SAP One Support Notes that apply to this document:

- [SAP Note 84555 - Windows Server, Linux®, and UNIX: Certified hardware](#)
- [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#)
- [SAP Note 2923773 - Linux® on IBM Cloud \(IaaS\): Adaption of your SAP license](#)
- [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#)
- [SAP Note 2369910 - SAP Software on Linux®: General information](#)
- [SAP Note 171380 - Released IBM hardware \(Intel processors\) and IBM cloud services offers](#)
- [SAP Note 1380654 - SAP support in IaaS environments](#)

This document is referenced by:

- [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#)
- [SAP Note 2588225 - SAP on IBM Cloud: Protect against speculative execution vulnerabilities](#)
- [SAP Note 1380654 - SAP support in IaaS environments](#)
- [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#)

VMware SDDC in Classic

Planning your deployment

Make sure that you are already familiar with the fundamental components and options that are provided by IBM Cloud Classic Infrastructure for SAP. Before you start with the deployment of servers, make sure that you also read the Get Started section.

Intel Optane persistent memory (PMem) is available on the Bare Metal servers. You have three memory options for PMem on the Bare Metal servers, 1.5 TB, 3.0 TB, and 6.0 TB. Which option you choose depends on the:

- Application that you want to run, for example BW or BW/4 HANA.
- SAP sizing, which determines the amount of memory and CPU that you need.

Network and storage configuration, disaster recovery, high availability, backups, and system replication are all configured and managed as part of the Bare Metal provisioning and operation.

The 'Must-Reads' before you start deploying

To ensure that your first deployment is a success, review the information in Provisioning SAP HANA and SAP NetWeaver [Planning your deployment](#)

Other useful documents

See the respective topics in the *Get Started* section for the following information:

- [SAP HANA design considerations for High Availability and Disaster Recovery \(HA/DR\)](#)
- [SAP HANA backups - Storage impacts on Recovery Time Objective \(RTO\)](#)
- [SAP NetWeaver design considerations for High Availability configuration](#)

VPC with Additional Application Server (AAS) ABAP on Linux for SAP HANA

You can use Terraform scripts to create a single-tier VPC and create the AAS to HANA and AnyDB infrastructure on the VPC. The Terraform scripts use the VPC information that you provide and then call the Ansible playbook to create the SAP architecture on the specified VPC.

Terraform on IBM Cloud® enables predictable and consistent provisioning of IBM Cloud Virtual Private Cloud (VPC) infrastructure resources so that you can rapidly build complex, cloud environments. IBM Cloud VPC infrastructure consists of SAP certified hardware that uses Intel® Xeon CPUs and more Intel® technologies.

You have two deployment methods to choose from:

- Terraform scripts that run from the CLI on your bastion server.
- Schematics user interface accessed from your cloud dashboard menu.

You can create SAP AAS NetWeaver 7.x on the SAP HANA-based ABAP stack.

SAP solution implemented

Many SAP enterprise solutions are built on the SAP platform (SAP NetWeaver) including:

- SAP HANA as Primary Persistence for SAP NetWeaver-based applications
- SAP Business Suite applications (ERP, CRM, and SCM, and other applications),
- SAP Business Warehouse (BW), and
- Other SAP enterprise solutions

SAP NetWeaver has two distinct aspects, ABAP and Java. Many applications that are built on the SAP NetWeaver's ABAP or Java (or both) application servers run on SAP DB owned HANA and ASE Sybase either in AnyDB platforms (MSSQL, Oracle, and Db2).

Technical interfaces are available for applications that are built on the SAP NetWeaver AS ABAP and AS Java to run on SAP HANA and AnyDB. However, specific development enablement is normally required for each application to ensure that it runs optimally on the SAP HANA. SAP Business Suite applications (ERP, CRM, SCM, and other applications), SAP Business Warehouse (BW), and other SAP NetWeaver-based applications were modified to run on SAP HANA and have many advantages. Also, various components and complimentary applications that are built on SAP NetWeaver can also run on SAP HANA or AnyDB by using the provided SAP NetWeaver DB interfaces.

The SAP HANA as primary persistence for SAP NetWeaver-based applications scenario has one restriction: SAP NetWeaver ABAP and Java application servers must run on separate hardware servers from the SAP HANA hardware.

What is created

The scripts automate the virtual infrastructure resources, provisioning the processes for the SAP architecture in an existing VPC with a distributed environment. SAP AAS NetWeaver 7.x (HANA or ASE SYB) application server on a distinct VSI VPC system and SAP HANA DB on a dedicated server type VSI VPC box are provisioned. The scripts work in two phases.

During the first phase of [Automate SAP bastion server – SAP media storage repository](#), the following virtual infrastructure resources based on the components from the existing VPC created by the bastion server are:

- 1 VPC where the virtual server instance is provisioned.
- 1 security group. The rules for this security group are:
 - Allow inbound DNS traffic (port 53).
 - Allow inbound SSH traffic (TCP port 22).
 - Allow all outbound traffic from the virtual server instance.
 - Allow all traffic in the security group.
- 1 subnet to enable the networking in your VPC.
- 2 virtual server instances with SAP certified storage and network configurations.
- 1 floating IP address used to access your VPC virtual server instance over the public network.

During the second phase, the Ansible Playbooks is called and the SAP architecture is installed for both dedicated virtual server instance (VSI) SAP application; VSI system and dedicated SAP HANA VSI box. The SAP architecture that is deployed on the SAP NetWeaver 7.x release is a stand-alone dedicated SAP HANA 2.0 box release. For more information about this architecture, see [Automating SAP HANA stand-alone virtual server instance on IBM Cloud® VPC by using Terraform and Ansible](#).

You can provision only one instance of the service per IBM Cloud region.

Schematics deployment

When you run the scripts with the Schematics interface, you:

- Enter the workspace information.
- Enter the GitHub path for the chosen solution either on NetWeaver AAS for HANA.
- Modify the parameters in the Schematics interface. They are the same parameters as the `input.auto.tfvars` file that you use with the cli.

Virtual server instance configuration

Following are the supported operating system images for SAP NetWeaver primary application server:

- ibm-redhat-8-4-amd64-sap-applications-2
- ibm-redhat-8-6-amd64-sap-applications-2
- ibm-sles-15-3-amd64-sap-applications-2
- ibm-sles-15-4-amd64-sap-applications-3

Following are the supported operating system images for SAP HANA database:

- ibm-redhat-8-4-amd64-sap-hana-2
- ibm-redhat-8-6-amd64-sap-hana-2
- ibm-sles-15-3-amd64-sap-hana-2
- ibm-sles-15-4-amd64-sap-hana-1

For both server instances there are:

- Two SSH keys are configured to access SSH as `root`.
- Three storage volumes as described in the `input.auto.tfvars` file.

What is created for anydb

The scripts use the information that you provide for an existing VPC and deploy AAS to SAP HANA or AnyDB on a different host than CI (SAP Central Instance) VSI host. For more information about this architecture, see [SAP NetWeaver 7.x on UNIX with HANA or AnyDB on IBM Cloud VPC on IBM Cloud VPC](#). You specify the information for the VPC to use in the `input.auto.tfvars` file.

The scripts call the Ansible Playbooks to install the SAP architecture.

Script files

The configuration and script files are provided on GitHub. Each supported interface for the SAP solution installation has its own folder in the GitHub repository:

- [GitHub repository for Terraform – AAS HANA](#)

Terraform interface

To run the Terraform script, you modify:

- The `input.auto.tfvars` file to specify the existing VPC resources for your solution. Specify the variables for the existing VPC:
 - VPC name
 - Security group
 - Subnet
 - Hostname
 - Profile
 - Image
 - Up to two SSH keys

You can change the default SAP system configuration settings to match your solution. You can also specify the location where you downloaded the SAP kits.

The IBM Cloud Provider plug-in for Terraform on IBM Cloud uses these configuration files to install AAS to SAP HANA and AnyDB on the specified VPC in your IBM Cloud account.

Support

There are no warranties of any kind, and there is no service or technical support available for these materials from IBM®. As a recommended practice, review carefully any materials that you download from this site before using them on a live system.

Though the materials provided herein are not supported by the IBM® Service organization, your comments are welcomed by the developers, who reserve the right to revise, readapt or remove the materials at any time. To report a problem, or provide suggestions or comments, open a GitHub issue.

Before you begin

Before you use the scripts in the bastion cli:

- Set up your account to access the VPC. Make sure that your account is [upgraded to a paid account](#).
- If you have not already, create a Bastion server to store the SAP kits. For more information, see [Automate SAP bastion server - SAP media storage repository](#).
- Download the SAP kits from the SAP Portal to your Deployment Server. Make note of the download locations. Ansible decompresses the files. For more information, see the [readme](#) file.
- [Create or retrieve an IBM Cloud API key](#). The API key is used to authenticate with the IBM Cloud platform and to determine your permissions for IBM Cloud services.
- [Create or retrieve your SSH key ID](#). You need the 40-digit UUID for the SSH key, not the SSH key name.
- Terraform should already be installed on the bastion server that you deployed. For more information, see [Bastion server for SAP deployment](#).
- (Optional - Catalog Tile) create secrets for your credentials and passwords by using the [Secrets Manager](#).

Deploying SAP AAS NetWeaver 7.x on HANA by using the Schematics user interface

Use these steps to configure the SAP Additional Application Server (AAS) NetWeaver with HANA or AnyDB on your existing VPC by using the Schematics interface. The script takes 2 - 3 hours to complete.

1. From the IBM Cloud menu, select **Schematics**.
2. Click **Create** workspace.
3. On the **Specify template** page:
 - Enter the URL for the Schematics interface.

- Select the **Terraform version** that is listed in the readme file.
 - Click **Next**.
4. On the **workspace details** page:
- Enter a name for the workspace.
 - Select a **Resource group**.
 - Select a **Location** for your workspace. The workspace location does not have to match the resource location.
 - Select **Next**.
5. Select **Create** to create your workspace.
6. On the workspace settings page, in the input variables section, review the default input variables and provide values that match your solution.
- For a more detailed description of each parameter, check the GitHub repo [AAS HANA readme](#) file, chapter “Input parameter file”. Also, make sure to mark the parameters that contain sensitive information like passwords, API, and ssh private keys as “sensitive”. These parameters are marked as “sensitive” in the readme file, under “Input parameter file”.
7. On the workspace settings page, click **Generate plan**. Wait for the plan to complete.
8. Click **View log** to review the log files of your terraform execution plan.
9. Apply your Terraform template by clicking **Apply plan**.
10. Review the log file to ensure that no errors occur during the provisioning, modification, or deletion process.

Deploying SAP AAS NetWeaver (ABAP) on HANA with the Deployable Architecture tile interface

Use these steps to configure the SAP AAS NetWeaver (ABAP) on HANA on your existing VPC by using the catalog tile interface. The script takes 2 - 3 hours to complete.

1. From the IBM Cloud catalog, select **VPC with Additional Application Server ABAP on Linux for SAP HANA** on HANA tile. The **Create** tab opens for VPC with Additional Application Server ABAP on Linux for SAP HANA. For more information about this deployment, see the About tab or the readme file link.
2. Select the latest version.
3. Select **VPC with Additional Application Server ABAP on Linux for SAP HANA on Deployable Architecture tile** variation.
4. Click **Review deployment** options:
 - **Add to project** to add this deployment to an IBM Cloud project and combine it with other deployments. IBM Cloud projects include several more pipeline steps before deployment, including deployment validation, cost calculation, compliance verification, and approval process.
 - **Create from the CLI** to get the CLI command. With this command you can trigger the deployment from the CLI.
 - **Work with code** to embed the code into other terraform deployments.
 - **Deploy with IBM Cloud Schematics** to trigger the deployment process directly.
5. Select **Deploy with IBM Cloud Schematics**.
6. Add the input parameters for this installation. There are 3 categories of parameters:
 - **Workspace** - These parameters define the workspace that is automatically created in Schematics:
 - Enter a name for the workspace or use the default name.
 - The Resource Group used to create resources. Use default or create a Resource Group.
 - Select a location to create your Schematics workspace. The workspace location need not match the resource location.
 - **Required input variables** - Review the default input variables and provide values that match your solution. These parameters are specific to your deployment. For more detailed information, see the [Readme file](#).

Parameter	Description
BASTION_FLOATING_IP	Required only for Schematics Deployments. The Floating IP from the Bastion Server.

HOSTNAME	The hostname for the VSI. The hostname should be up to 13 characters as required by SAP. For more information on the rules regarding hostnames for SAP systems, check SAP Note 611361: Hostnames of SAP ABAP Platform servers
REGION	The cloud region to deploy the solution. The regions and zones for VPC are listed here . Review supported locations in IBM Cloud Schematics here . Sample value: eu-de.
RESOURCE_GROUP	The name of an existing Resource Group for VSIs and Volumes resources. Default value: "Default". The list of Resource Groups is available here .
SECURITY_GROUP	The name of an existing Security group. The list of security groups is available here .
SSH_KEYS	The list of SSH Keys UUIDs that are allowed to SSH as root to the VSI can contain one or more IDs. The list of SSH Keys is available here . Sample input (use your own SSH UUIDs from IBM Cloud){: external}: ["r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a", "r010-3fcfd9fe7-d4a7-41ce-8bb3-d96e936b2c7e"]
SUBNET	The name of an existing subnet. The list of subnets is available here .
VPC	The name of an existing VPC. The list of VPCs is available here .
ZONE	The cloud zone where to deploy the solution. Sample value: eu-de-2.
ibmcloud_api_key	IBM Cloud API key (Sensitive* value).
private_ssh_key	Required only for Schematics Deployments - Input your id_rsa private key pair content in OpenSSH format (Sensitive* value). This private key should be used only during the terraform provisioning and it is recommended to be changed after the SAP deployment.
hdb_instance_number	The instance number of the SAP HANA database server.
sap_aas_instance_number	Technical identifier for the internal processes of the additional application server.
sap_ascs_instance_number	Technical identifier for the internal processes of ASCS.
sap_ci_host	IP address of the existing SAP Central Instance.
sap_ci_hostname	The hostname of the existing SAP Central Instance.
sap_ci_instance_number	Technical identifier for the internal processes of the Central Instance.
sap_sid	The SAP system ID identifies the entire SAP system.
sap_main_password	Common password for all users that are created during the installation (See Obs*).

Required Variables

- **Optional variables** - Review and update the optional input variables. The Ansible scripts expect the SAP kits to be in the default locations listed. For more information, see the [Readme file - Input Parameters](#).

Parameter	Description
ID_RSA_FILE_PATH	The file path for private_ssh_key is automatically generated by default. If it is changed, it must contain the relative path from Git repo folders. Default value: "ansible/id_rsa".
IMAGE	The OS image used for the VSI. A list of images is available here .
PROFILE	The profile used for the VSI. A list of profiles is available here . For more information about supported DB/OS and IBM Gen 2 Virtual Server Instances (VSI), check SAP Note 2927211: SAP Applications on IBM Virtual Private Cloud .

VOL1	Volume 1 Size - The size for the disks in GB that are to be attached to the VSI and used by SAP.
VOL2	Volume 2 Size - The size for the disks in GB that are to be attached to the VSI and used by SAP.
kit_sapcar_file	Path to the sapcar binary, as downloaded from SAP Support Portal.
kit_swpm_file	Path to the SWPM archive (SAR), as downloaded from SAP Support Portal.
kit_saphostagent_file	Path to the SAP Host Agent archive (SAR), as downloaded from SAP Support Portal.
kit_hdbclient_file	Path to the HANA DB client archive (SAR), as downloaded from SAP Support Portal.

Optional Variables

7. Accept the license agreement.
8. Select **Deploy**. The deployment starts and you are directed to the Schematics page that displays the script log files for you to monitor the deployment progress.

Creating the infrastructure using Terraform with the bastion server CLI

Use these steps to configure the IBM Cloud Provider plug-in and use Terraform to install SAP AAS to SAP HANA and AnyDB on your existing VPC on an already deployed SAP NetWeaver 7.X with SAP HANA 2.0 or ASE SYB as a Central Instance.

The script takes 1 - 2 hours to complete.

1. Access the bastion server cli.
2. Clone the solution repository and change to the folder.

ASE SYB 16 Clone the solution repository from <https://github.com/IBM-Cloud/sap-aas-abap-ase-syb> and cd to the sap-aas-abap-ase-syb/cli folder.

```
$ git clone https://github.com/IBM-Cloud/sap-aas-abap-ase-syb
cd sap-aas-abap-ase-syb/cli/
```

SAP HANA 2.0: Clone the solution repository from <https://github.com/IBM-Cloud/sap-abap-hana-aas> and cd to the sap-abap-hana-aas folder.

```
$ git clone https://github.com/IBM-Cloud/sap-abap-hana-aas.git
cd sap-abap-hana-aas/
```

3. Modify the `input.auto.tfvars` file to specify the information for the existing VPC, your region, zone, networking component names, hostname for the AAS VSI,profile, and image. You need your 40-digit SSH key ID for this file. The second SSH key is optional. For more options for profile, see [Instance Profiles](#). For more options, see [Images](#). For descriptions of the variables, see the [readme](#) file.

The VSI OS images that are supported for this solution for Netweaver Additional Application Server are:

- ibm-redhat-8-4-amd64-sap-applications-2
- ibm-redhat-8-6-amd64-sap-applications-2
- ibm-sles-15-3-amd64-sap-applications-2
- ibm-sles-15-4-amd64-sap-applications-4

```
$ # Infra VPC variables for ASE SYB
REGION    = "eu-de"
ZONE      = "eu-de-2"
VPC        = "ic4sap"                      # EXISTING Security group name
SECURITY_GROUP = "ic4sap-securitygroup"      # EXISTING Security group name
RESOURCE_GROUP = "wes-automation"
SUBNET     = "ic4sap-subnet"                  # EXISTING Subnet name
SSH_KEYS   = [ "r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a" , "r010-3fcfd9fe7-d4a7-41ce-8bb3-
d96e936b2c7e" ]

# SAP AAS VSI variables:
```

```

HOSTNAME = "sapnwase-as01"
PROFILE = "bx2-4x16"
IMAGE = "ibm-redhat-8-4-amd64-sap-applications-2

$ # Infra VPC variables for ABAP HANA
REGION      = "eu-de"
ZONE        = "eu-de-2"
VPC          = "ic4sap" # EXISTING Security group name
SECURITY_GROUP = "ic4sap-securitygroup" # EXISTING Security group name
RESOURCE_GROUP = "wes-automation"
SUBNET       = "ic4sap-subnet" # EXISTING Subnet name
SSH_KEYS     = [ "r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a" , "r010-3fc9fe7-d4a7-41ce-8bb3-d96e936b2c7e" ]
ID_RSA_FILE_PATH = "ansible/id_rsa"

# SAP AAS variables:
HOSTNAME = "sapnwapp"
PROFILE = "bx2-4x16"
IMAGE = "ibm-redhat-8-6-amd64-sap-applications-2"

```

4. Customize your SAP system configuration. In the same file, input.auto.tfvars, edit the SAP system configuration variables that are passed to the Ansible automated deployment. For descriptions of the variables, see the [readme](#) file.

```

$ # SAP system configuration - for ASE SYB
sap_sid = "NWD"
sap_ci_host = "10.243.132.10"
sap_ci_hostname = "sapnwase"
sap_ci_instance_number = "00"
sap_asc_s_instance_number = "01"
sap_aas_instance_number = "00"

# Kits paths
kit_sapcar_file = "/storage/NW75SYB/SAPCAR_1010-70006178.EXE"
kit_swpm_file = "/storage/NW75SYB/SWPM10SP31_7-20009701.SAR"
kit_saphotagent_file = "/storage/NW75SYB/SAPHOSTAGENT51_51-20009394.SAR"

```

```

$ # SAP system configuration - for ABAP HANA
sap_sid = "NWD"
sap_ci_host = "10.243.132.10"
sap_ci_hostname = "sapnwapp01"
sap_ci_instance_number = "00"
sap_asc_s_instance_number = "01"
hdb_instance_number = "00"
sap_aas_instance_number = "00"

# Kits paths
kit_sapcar_file = "/storage/NW75HDB/SAPCAR_1010-70006178.EXE"
kit_swpm_file = "/storage/NW75HDB/SWPM10SP31_7-20009701.SAR"
kit_saphotagent_file = "/storage/NW75HDB/SAPHOSTAGENT51_51-20009394.SAR"
kit_hdbclient_file = "/storage/NW75HDB/IMDB_CLIENT20_009_28-80002082.SAR"

```

Ansible decompresses the rest of the SAP kit files. For more information, see the [readme](#) file.

5. Initialize the Terraform CLI.

```
terraform init
```

6. Create a Terraform execution plan. The Terraform execution plan summarizes all the actions that are done to create the virtual private cloud instance in your account.

```
terraform plan plan1
```

Enter an SAP main password and your API key.

The SAP main password must be 10 - 14 characters long and contain at least one digit (0-9). It can contain only the following characters: a-z, A-Z, 0-9, @, #, \$, . *This password cannot contain exclamation points '!'. The password must not start with a digit or an underscore ().*

7. Verify that the plan shows all of the resources that you want to create and that the names and values are correct. If the plan needs to be adjusted, edit the input.auto.tfvars file to correct resources and run terraform plan again.
8. Apply the saved plan.

```
$ terraform apply "plan1"
```

The virtual private cloud and components are created and you see output similar to the `terraform plan` output.

9. Add the SAP credentials and the virtual server instance IP to the SAP GUI. For more information about the SAP GUI, see [SAP GUI](#).

Next steps

If you need to rename your resources after they are created, modify the `input.auto.tfvars` file to change the names and run `terraform plan` and `terraform apply` again. Do not use the IBM Cloud Dashboard and user interface to modify your VPC after it is created. The Terraform scripts create a complete solution and selectively modifying resources with the user interface might cause unexpected results.

If you need to remove the SAP Netweaver 7.X on HANA or AnyDB installation, go to your project folder and run `terraform destroy`. The `terraform destroy` command does not remove the VPC in this scenario because the VPC was created before these Terraform scripts were run.

Related information

For more information about Terraform on IBM Cloud, see [Getting started with Terraform on IBM Cloud](#).

For more information about using Terraform for creating only a VPC for SAP, without the SAP architecture, see [Creating single-tier virtual private cloud for SAP by using Terraform](#).

SAP One Support Notes that apply to this document:

- [SAP Note 84555 - Windows Server, Linux®, and UNIX: Certified hardware](#)
- [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#)
- [SAP Note 2923773 - Linux® on IBM Cloud \(IaaS\): Adaption of your SAP license](#)
- [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#)
- [SAP Note 2369910 - SAP Software on Linux®: General information](#)
- [SAP Note 171380 - Released IBM hardware \(Intel processors\) and IBM cloud services offers](#)
- [SAP Note 1380654 - SAP support in IaaS environments](#)

This document is referenced by:

- [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#)
- [SAP Note 2588225 - SAP on IBM Cloud: Protect against speculative execution vulnerabilities](#)
- [SAP Note 1380654 - SAP support in IaaS environments](#)
- [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#)

Power Virtual Server instances

Planning your deployment

Make sure that you are already familiar with the fundamental components and options that are provided by IBM Cloud Classic Infrastructure for SAP. Before you start with the deployment of servers, make sure that you also read the Get Started section.

Intel Optane persistent memory (PMem) is available on the Bare Metal servers. You have three memory options for PMem on the Bare Metal servers, 1.5 TB, 3.0 TB, and 6.0 TB. Which option you choose depends on the:

- Application that you want to run, for example BW or BW/4 HANA.
- SAP sizing, which determines the amount of memory and CPU that you need.

Network and storage configuration, disaster recovery, high availability, backups, and system replication are all configured and managed as part of the Bare Metal provisioning and operation.

The 'Must-Reads' before you start deploying

To ensure that your first deployment is a success, review the information in Provisioning SAP HANA and SAP NetWeaver [Planning your deployment](#)

Other useful documents

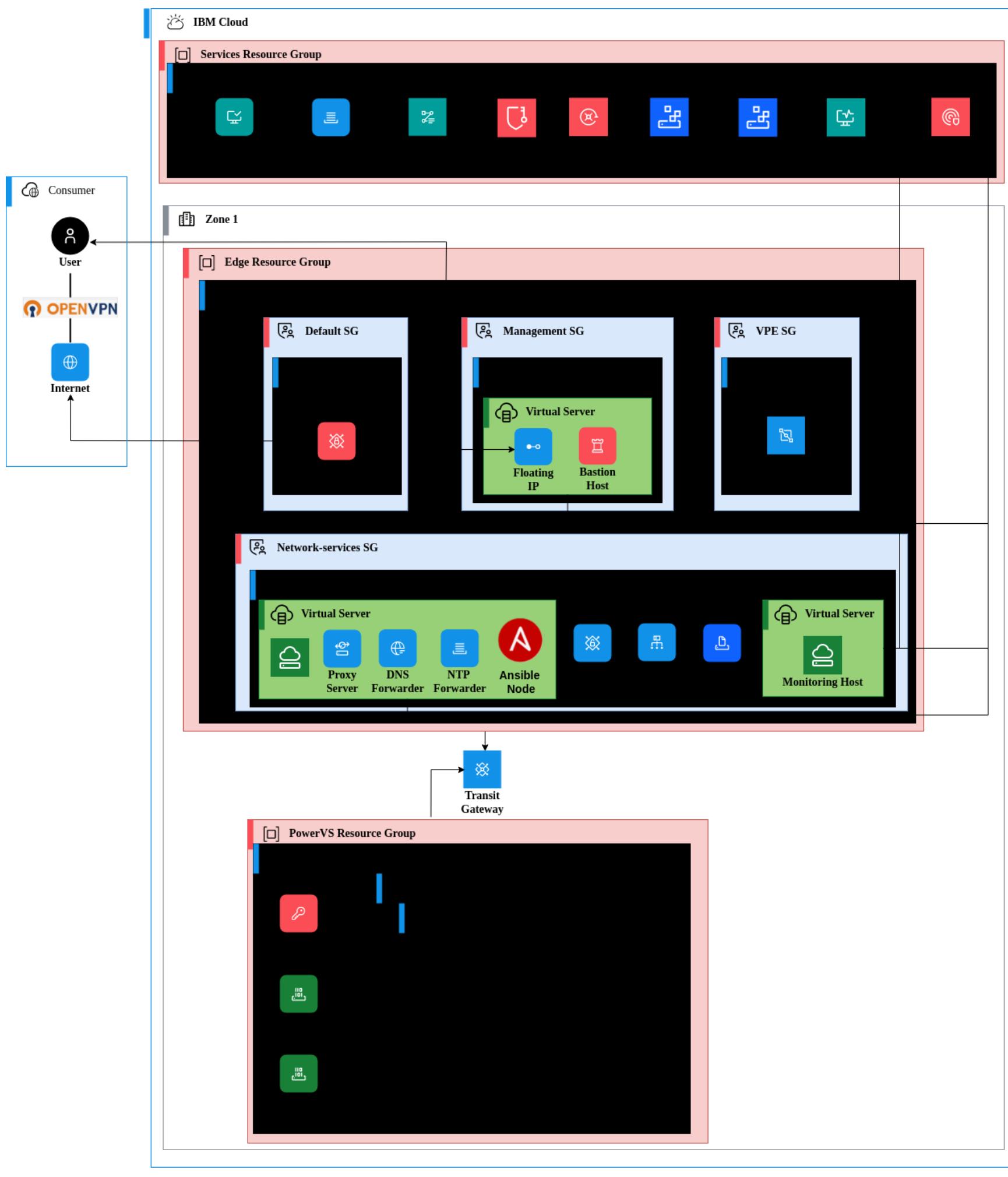
See the respective topics in the *Get Started* section for the following information:

- [SAP HANA design considerations for High Availability and Disaster Recovery \(HA/DR\)](#)
- [SAP HANA backups - Storage impacts on Recovery Time Objective \(RTO\)](#)
- [SAP NetWeaver design considerations for High Availability configuration](#)

Deploying IBM Cloud VPC infrastructure for Power Virtual Server SAP workloads

As a best practice for SAP that runs on IBM® Power® Virtual Server, one IBM Cloud VPC is created and two virtual server instances are deployed and configured.

- **Access host that is deployed in edge VPC** is used for the management access to the landscape.
- **Host for network management services that are deployed in edge VPC** provides certain network services to the Power Virtual Server instances, like proxy forwarding, NFS, DNS, NTP and monitoring services.



VPC landing zone for SAP on Power Virtual Server

Deploying IBM Cloud VPC for management services

IBM Cloud VPC for management services is a **mandatory** component in the SAP on Power Virtual Server best practices. This service hosts the access hosts to the environment.

- Set up Virtual Private Cloud for management services. For more information, see [Creating a VPC and subnet](#).
- Take care about the default network prefix. We recommend reducing the default network prefix, so it does not overlap between all your IBM Cloud VPC services.
- Optionally, attach a public gateway to the subnet. With this option, every Virtual Server Instance in the subnet can communicate with the internet. An alternative is to use a floating IP address on virtual system instance instead and enable internet for the instances. The [table](#) gives an overview on segregation of networks used.

Deploying access host in edge VPC

Access host is a **mandatory** component in the SAP on Power Virtual Server best practices. By this virtual server instance, the floating IP address is activated. You can then log in to the environment by using SSH. You need to set up a VPN access as a separate step and disable the floating IP address for a more secure environment. Use the following steps to deploy the access host.

1. Create ACL rules for Edge VPC as described [here](#)

2. Create security groups for management services, network services and IBM Cloud services as described [here](#). For more information, see [Configuring the security group for the instance](#). Specify following rules.
3. Create a virtual server instance with a Linux operating system. For more information, see [Creating a virtual server instance](#).
 - You can select any available Linux image, but you need to use the same operating system release for all of the virtual server instances in the landscape. We verify the setup with newest versions of Red Hat Enterprise Linux (starting with RHEL 8.4) and of Suse Linux Enterprise Server (starting with SLES 15 SP3).
 - You don't have limitations as to which Compute profile, SAP certification, or storage and network performance is used. You can use the smallest profile with 2 virtual CPUs and with 4 GB memory.
4. Attach the right security group (management-sg security group) to the virtual server instance that you created in the previous step. Detach the default security group.
5. Enable the floating IP address on the access host. For more information, see [Reserving a floating IP address](#).
6. After instance status changes to **Running**, verify that you can successfully log in on the access host.

Tip: We recommend that you use two extra SSH client parameters to get a more reliable SSH connection: `ServerAliveInterval=60` and `ServerAliveCountMax=600`. If you use a nondefault path to your SSH key, you must specify it by following SSH client parameter: `-i <path to your SSH private key>`.

SSH command example:

```
$ ssh -A -o ServerAliveInterval=60 -o ServerAliveCountMax=600 root@<access_host_floating_ip>
```

Deploying network services host in edge VPC

Host for internet services is a mandatory component in the SAP on Power Virtual Server best practices. This virtual server instance hosts mandatory proxy server, NTP and DNS services. It is also configured as central Ansible Node. Use the following steps to deploy a host for basic network management services.

 **Note:** The following example setup uses open ports for standard SQUID proxy server that is provided by Linux distributions. If you use another proxy software or custom configurations, setup might vary.

1. Provision a virtual service instance with Linux. For more information, see [Creating a virtual server instance](#).
 - You can choose any of available Linux distributions. We recommend that you use the same OS release for all virtual server instances in the landscape. We verify the setup with the newest versions of Red Hat Enterprise Linux (starting with RHEL 8.4) and of Suse Linux Enterprise Server (starting with SLES 15 SP3).
 - One of the profiles with 2 or 4 virtual CPUs and with 4 GB or 8 GB of memory would be sufficient in general. If you have stronger performance requirements, by using SQUID cache, you can choose a profile with more virtual CPUs or memory.
 - We recommend that you attach extra storage to the instance, locate SAP installation files on this separate disk, and export them over NFS. The disk size must be large enough to host all the data from IBM Cloud Object Storage that is relevant for all the installations and setups.
2. Attach the right security group to the virtual server instance (network-services-sg security group) that you created in the previous step. Detach the default security group.
3. After some time, instance becomes status 'running'.

Verify that you can successfully log in to the **host for network services over the access host**. The floating IP address of the access host is specified as `ProxyCommand` parameter of your ssh command.

Tip: We recommend that you use two extra SSH client parameters for a more reliable SSH connection: `ServerAliveInterval=60` and `ServerAliveCountMax=600`. If you use a nondefault path to your SSH key, you must specify it by following SSH client parameter: `-i <path_to_your_SSH_private_key>`.

SSH command example (host for network services over the access host):

```
$ ssh -A -o ServerAliveInterval=60 -o ServerAliveCountMax=600 -o ProxyCommand=\"ssh -W %h:%p root@<access_host_floating_ip>\" root@<network_services_host_private_ip>
```

Configure the network management services on the Intel virtual server instances in IBM Cloud

VPC

The following setup example demonstrates usage of SQUID proxy server, NFS server, NTP forwarder, IBM Cloud DNS service, or DNS forwarder for your private DNS server. Setup of central user management (LDAP) is not covered here.

Setup SQUID proxy server

1. Ensure all required ports in the security group in IBM Cloud VPC for edge services that are used by host for internet services are open. The needed ports are configured for internet services. Required ports for SQUID proxy are used by Power Virtual Server services. For more information, see [Creating a proxy](#).
2. Log in to the network services instance. SSH command example:

```
$ ssh -A -o ServerAliveInterval=60 -o ServerAliveCountMax=600 -o ProxyCommand=\"ssh -W %h:%p root@<access_host_floating_ip>\\" root@<network_services_host_private_ip>\\"
```

3. Ensure that the squid software is available. On SUSE: `zypper update -y; zypper install -y squid`. On RHEL: `yum update -y; yum install epel-release; yum install -y squid`.
4. Modify the SQUID configuration and add the rules relevant for OS update registration of virtual instances that run in Power Virtual Server. For more information, see [proxy configuration documentation](#).
5. Enable and restart SQUID service: `systemctl stop squid; systemctl start squid; systemctl enable squid`.

Setup SQUID proxy server -- Ansible

To perform the previous steps through ansible automation, download ansible-galaxy collection `ibm.power_linux_sap`.

```
$ ansible-galaxy collection install ibm.power_linux_sap
```

After the ansible collection is installed, to set up proxy, update the variable file `playbook/vars/sample-variables-configure-network-services-host.yml`

```
$ server_config: {  
    squid: { enable: true }  
}
```

After the file is updated, run the following ansible-playbook command.

```
$ ansible-playbook --connection=local -i \"localhost,\" playbook/sample-configure-network-services-host.yml
```

This ansible execution ensures that the squid proxy server is configured on host for network services.

Setting up NFS server for SAP installation files

1. Ensure all required ports in the security group in IBM Cloud VPC for network services that are used by host for private services are open. The needed ports are configured for private services. Required ports for NFS server are: 111 (TCP and UDP) and 2049 (TCP and UDP).
2. Log in to the network services instance. SSH command example:

```
$ ssh -A -o ServerAliveInterval=60 -o ServerAliveCountMax=600 -o ProxyCommand=\"ssh -W %h:%p root@<access_host_floating_ip>\\" root@<network_services_host_private_ip>\\"
```

3. Make sure that the required NFS software is available. On SUSE: `zypper update -y; zypper install -y nfs-utils`. On RHEL: `yum update -y; yum install epel-release; yum install -y nfs-utils`.
4. Create a directory where NFS is mounted and export it.
5. Start NFS service and verify that the directory is exported. Use command `showmount -e`.
6. Make sure that the awscli software is available. This software is used later to download the software from S3 storage (IBM Cloud Object Storage). On SUSE: `zypper update -y; zypper install -y aws-cli`. On RHEL: `yum update -y; yum install epel-release; yum install -y awscli`.

Setting up NFS server for SAP installation files -- Ansible

To perform the previous steps through ansible automation, download ansible-galaxy collection `ibm.power_linux_sap`.

```
$ ansible-galaxy collection install ibm.power_linux_sap
```

After the ansible collection is installed, update the variable file `playbook/vars/sample-variables-configure-network-services-host.yml` to set up NFS.

```
$ server_config: {  
    nfs: { enable: true, nfs_directory: "/NFS;/hana/software" }  
}
```

After file is updated, run the following ansible-playbook command.

```
$ ansible-playbook --connection=local -i \"localhost,\" playbooks/sample-configure-network-services-host.yml
```

This ansible execution makes sure that the host for network services acts as an NFS server.

Setting up NTP proxy and forwarder

1. Ensure all required ports in the security group in IBM Cloud VPC for network services that are used by host for private services are open.
The needed ports are configured for private services. Required port for NTP forwarder is: 123 (TCP).
2. Log in to the network services instance. SSH command example:

```
$ ssh -A -o ServerAliveInterval=60 -o ServerAliveCountMax=600 -o ProxyCommand=\"ssh -W %h:%p root@\  
<access_host_floating_ip\>\\" root@<network_services_host_private_ip\>\\"
```

3. Make sure that the required NTP software is available. On SUSE: `zypper update -y; zypper install -y chrony`. On RHEL: `yum update -y; yum install epel-release; yum install -y chrony`.
4. Modify file '/etc/chrony.conf' and add following lines. Replace `\<pvs_mgmt_cidr\>` with Power Virtual Server management CIDR block (network segment)

```
$ local stratum 10  
manual  
allow \<pvs_mgmt_cidr\>
```

5. Enable and start chrony service: `systemctl stop chronyd; systemctl start chronyd; systemctl enable chronyd;`.

Setup NTP proxy or forwarder -- Ansible

To perform previous steps through ansible automation, download ansible-galaxy collection `ibm.power_linux_sap`.

```
$ ansible-galaxy collection install ibm.power_linux_sap
```

After the ansible collection is installed, to set up NTP, update the variable file `playbook/vars/sample-variables-configure-network-services-host.yml`.

```
$ server_config: {  
    ntp: { enable: true }  
}
```

After the file is updated, run the following ansible-playbook command.

```
$ ansible-playbook --connection=local -i \"localhost,\" playbooks/sample-configure-network-services-host.yml
```

This ansible execution ensures that the NTP proxy is configured on the host for network services.

Setting up IBM Cloud-native DNS service (DNS option 1)

You can use IBM Cloud DNS service that is directly reachable from IBM Power Virtual Servers over custom resolver. For more information, see the following links.

- [Setting up an instance](#)
- [Managing DNS zones](#)
- [Managing permitted networks](#)

- [Managing DNS records](#)
- [Configuring custom resolver](#).

Specify VPE subnet of IBM Cloud VPC for network services as location in the resolver.

Make sure that all required ports in the security group in IBM Cloud VPC for network services that are used by host for private services are open. The needed ports are configured for private services. Required port for DNS is: 53 (TCP and UDP). As result, you get a private IP address that you can specify in Power® Virtual Server instances as DNS endpoints by private subnet configuration. These IP addresses are entered into `/etc/resolv.conf` in the operating system.

Setting up DNS forwarder (DNS option 2)

If you use your own DNS service, its IP must be reachable from VPC for network services. If the IP is not directly reachable from IBM Power Systems Virtual Servers, a DNS forwarder on the host for critical management services is required. Use the following steps to complete the configuration:

1. Make sure that all required ports in the security group in IBM Cloud VPC for network services that are used by host for private services are open. The needed ports are configured for private services. Required port for DNS is: 53 (TCP and UDP).

2. Log in to the private services instance. You can use the following SSH command example:

```
$ ssh -A -o ServerAliveInterval=60 -o ServerAliveCountMax=600 -o ProxyCommand=\"ssh -W %h:%p root@\
<access_host_floating_ip\>\\" root@<network_services_host_private_ip\>
```

3. Make sure that the required DNS software is available. On SUSE: `zypper update -y; zypper install -y bind`. On RHEL: `yum update -y; yum install epel-release; yum install -y bind`.

4. Modify file `/etc/named.conf`:

- Add the following lines at the beginning of the file direct after the starting comment (before the `options` section starts). Replace `\<pvs_mgmt_cidr\>` with Power Virtual Server management CIDR block (network segment)

```
$ acl allowed_clients {
localhost;
10.10.0.0/16;
};
```

- Add the following lines at the beginning of the `options` section. Both 161.26.0.x IPs are the IBM Cloud DNS servers. 9.9.9.9 IP is the IBM public DNS server IP. Replace or extend this IP list with DNS servers of your choice.

```
$ forwarders {
161.26.0.7;
161.26.0.8;
9.9.9.9;
};
recursion yes;
allow-query { allowed_clients; };
forward only;
```

5. Enable and start DNS service: `systemctl stop named; systemctl start named; systemctl enable named;`.

Setup DNS forwarder (DNS option 2) -- Ansible

To perform the previous steps through ansible automation, download ansible-galaxy collection `ibm.power_linux_sap`.

```
$ ansible-galaxy collection install ibm.power_linux_sap
```

After the ansible collection is installed, to set up proxy, update the variable file `playbook/vars/sample-variables-configure-network-services-host.yml`

```
$ server_config: {
  dns: { enable: false, dns_servers: "161.26.0.7; 161.26.0.8; 9.9.9.9;" }
}
```

After the file is updated, run the following ansible-playbook command.

```
$ ansible-playbook --connection=local -i "localhost," playbooks/sample-configure-network-services-host.yml
```

This ansible execution ensures that the DNS forwarder services are configured on Power Virtual Server.

Optional steps on IBM Cloud VPC for other services

To create other VPC resources, such as load balancer, and other resources, see [Using the IBM Cloud console to create VPC resources](#).

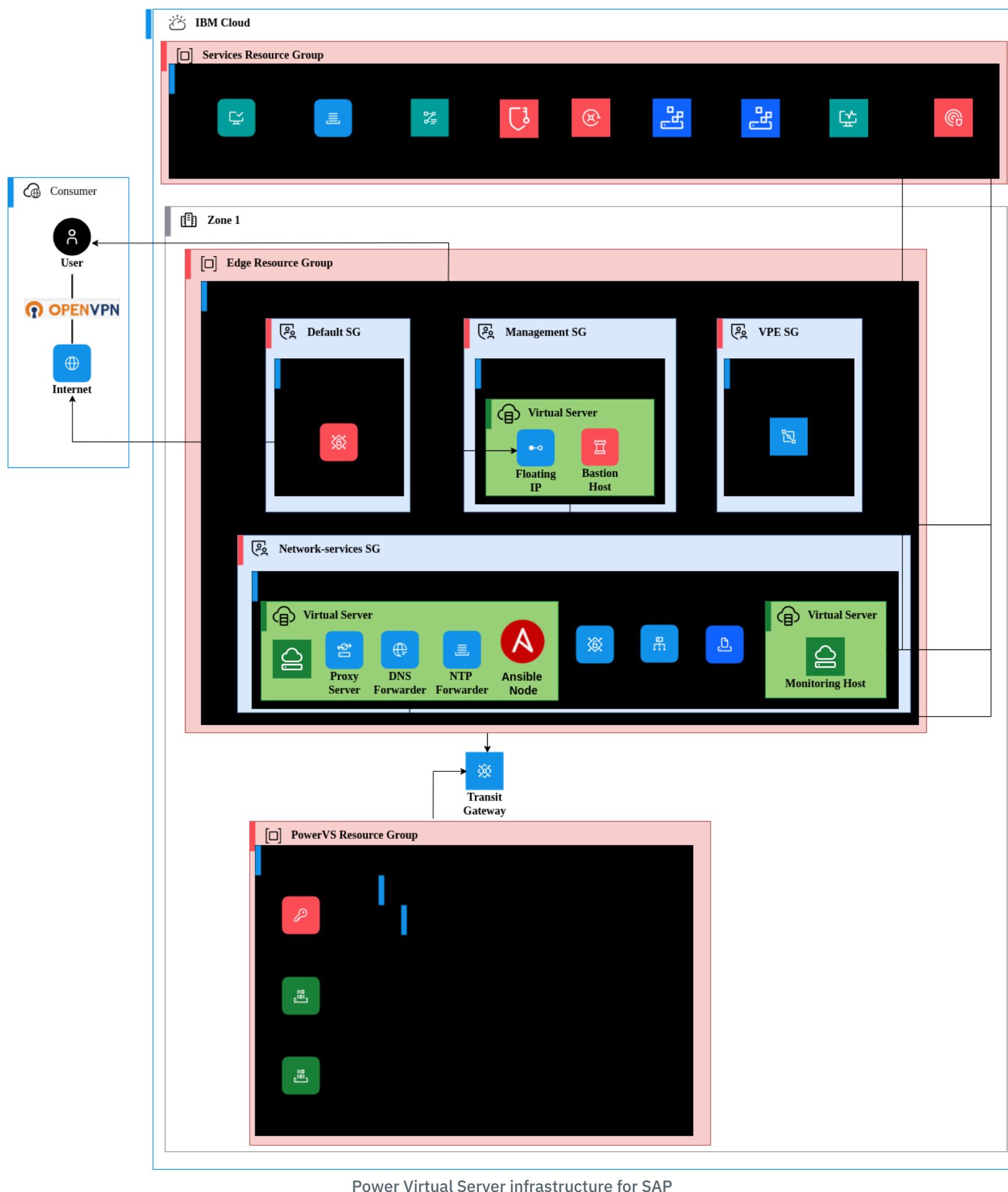
Terraform automation - Deploying the VPC landing zone for Power Virtual Server

All the above steps are automated using terraform and ansible and is available as a Deployable Architecture Solution in IBM Cloud Catalog. To configure and deploy check the [link](#) for further details.

Deploying Power Virtual Server infrastructure

For SAP workloads that run on IBM® Power® Virtual Server, one workspace for Power Virtual Server is deployed.

The following diagram shows deployed components.



Deploying a Power Virtual Server

Workspaces for Power Virtual Server host all the SAP instances that don't require direct internet access. All SAP NetWeaver and SAP HANA instances are deployed in the workspace for Power Virtual Server. To create and configure this service, use the following steps.

1. Deploy a new workspace for Power Virtual Server in the same region where your IBM Cloud edge VPC is. For more information, see [Creating a Power Systems Virtual Server workspace](#).
2. Upload your SSH public key to the workspace. SSH keys are distributed across all the workspaces that are in your account, so you generate the SSH key one time.
 - Go to **SSH keys**, click **Create SSH key**, provide a unique name, and press **Add SSH key**.
3. In the workspace, create a management and backup private networks. For more information, see [Configuring and adding a private network subnet](#).
4. Connect the Power Virtual Server workspace to the transit gateway as described [here](#). You can now ping gateway IBM Power Virtual Server private networks IP addresses from the access host deployed in VPC.

Terraform automation - Deploying the VPC landing zone for Power Virtual Server

All the above steps are automated using terraform and ansible and is available as a Deployable Architecture Solution in IBM Cloud Catalog. To configure and deploy check the [link](#) for further details.

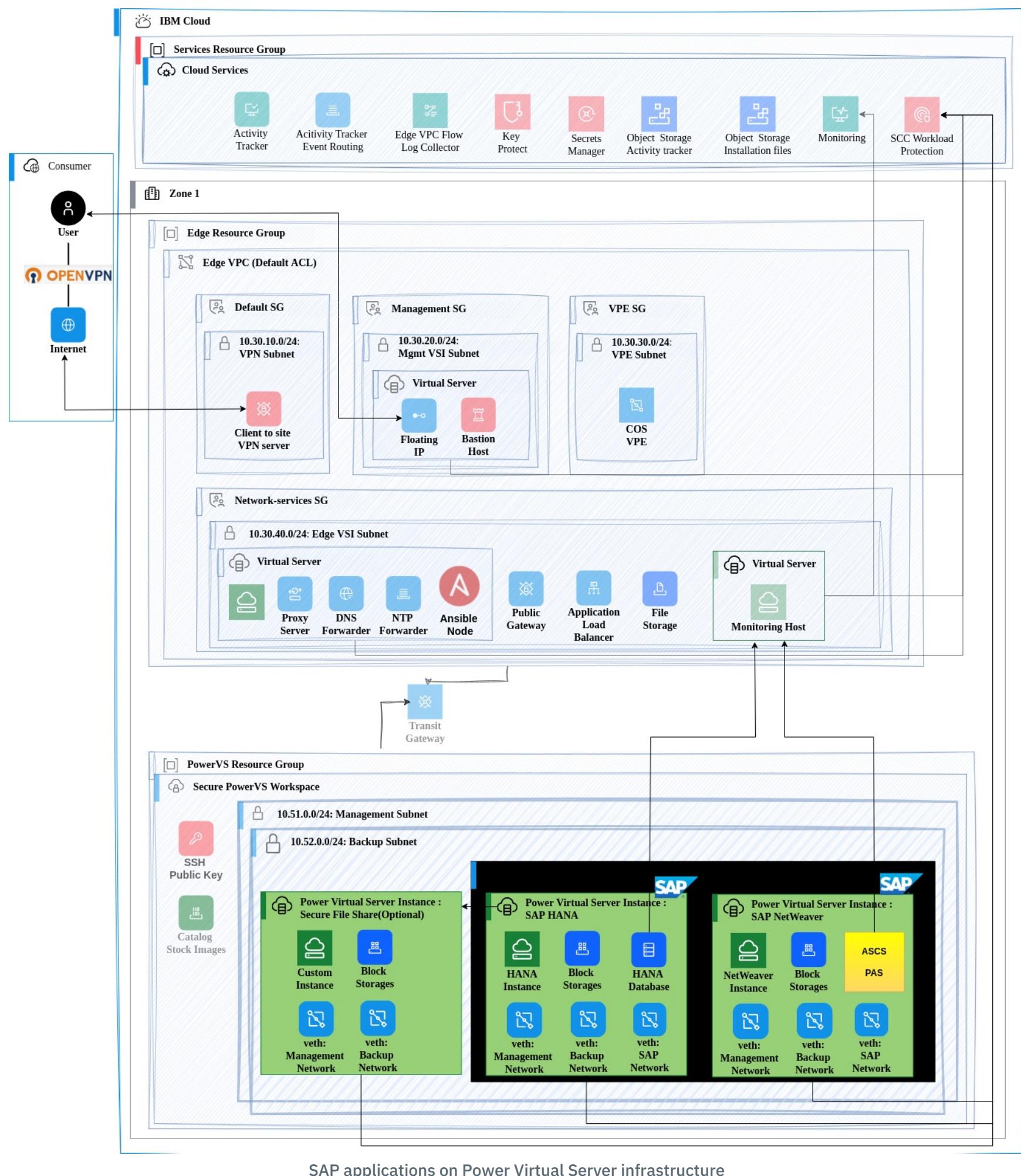
Deploying SAP applications on Power Virtual Server

The following information explains how to deploy Power Virtual Server instances for SAP HANA database and SAP application server (NetWeaver) on Red Hat Enterprise Linux (RHEL) and SUSE Linux Enterprise Server (SLES).

An infrastructure, that was deployed on IBM Cloud® and runs on IBM® Power® Virtual Server consists of the following components:

- A separate private network for SAP system.
- A Power Virtual Server instance for shared file systems.
- A Power Virtual Server instance for SAP HANA.
- A Power Virtual Server instance for SAP NetWeaver (on Linux).
- An operating system, such as RHEL or SLES, that is configured to use management services that are configured on IBM Cloud® Virtual Private Cloud (SQUID proxy, NFS, NTP, DNS).
- A registered RHEL or SLES operating systems (OS) with IBM provided subscription, which includes SAP-specific network performance tuning, file system setup, and packages.

The following diagram shows SAP applications already deployed on Power Virtual Server infrastructure.



SAP applications on Power Virtual Server infrastructure

Deploying a separate private network for SAP systems

For each SAP system that you deploy, create a separate private network for communication between the virtual server instances. Follow [Configuring a private network subnet](#) to configure a separate private network for the SAP system.

Deploying Power Virtual Server instances for SAP on IBM Cloud®

It is recommended to perform a memory sizing of SAP applications before deploying them on Power Virtual Server instances. See the [Sizing process for SAP Systems](#) and [IBM Power Virtual Server certified profiles for SAP HANA](#).

Before deploying of Power Virtual Server instances, you should be aware of the various options for choosing an operating system (OS) image, that is based on a subscription. The available subscription alternatives are:

- **IBM provided subscription**, where IBM Cloud® provides a full subscription to IBM stock OS images, such as RHEL and SLES, Linux® for SAP applications (RHEL and SLES for SAP workloads), AIX, and IBM i.
- **Client supplied subscription**, where you use your own subscription with IBM stock OS images or custom images. This feature is called "Bring Your Own License" (BYOL). Custom images are imported by users as boot images into Power Virtual Server. Therefore, if you plan to use your own subscription, select the OS image that has a suffix of -BYOL under the "Client supplied subscription" when deploying Power Virtual Server instances in the step [Deploying an Power Virtual Server instance for SAP HANA](#).



Note: For deploying and setting up the Power Virtual Server instances for SAP applications, we focus on the **IBM provided subscription** for Red Hat Enterprise Linux (RHEL) and SUSE Linux Enterprise Server (SLES) images.

More details about the subscription for RHEL and SLES could be found in [Using RHEL within the Power Virtual Server](#) and [Using SLES within IBM Power Virtual Server](#).

IBM Cloud® for SAP provides SAP-certified infrastructure to run SAP workloads, which includes the following operating systems with OS images under **IBM provided subscription**:

- Linux® for SAP HANA: Red Hat Enterprise Linux for SAP HANA and SUSE Linux Enterprise Server for SAP HANA. The images have a **SAP** suffix.
- Linux® for SAP application server (NetWeaver): Red Hat Enterprise Linux for SAP NetWeaver and SUSE Linux Enterprise Server for SAP NetWeaver. The images have a **NETWEAVER** suffix.



Important: Pay attention to the choice of operating system. Linux® OS is not the same as Linux® for SAP applications. Linux® OS does not have specific pre-configured settings for SAP workloads.

See more details about Linux® versions for SAP applications in [OS for IBM Power Virtual Servers](#).

It is recommended to perform a memory sizing of SAP applications before deploying them on Power Virtual Server instances. See the [Sizing process for SAP Systems](#) and [IBM Power Virtual Server certified profiles for SAP HANA](#).

Deploying an Power Virtual Server instance for SAP HANA

1. To deploy an Power Virtual Server instance for SAP HANA database, select a previously created workspace from the list of [Workspaces](#) on the left navigation page.
2. Click **Virtual server instances** on the left page.
3. Create a new instance, click **Create instance** on the right side.
4. In the **General** section, make the following selections:

Field	Details
Instance name	Enter a unique name for the instance.
Number of instances	Enter '1'.
Add to server placement group	Optional and can be skipped.
Add to a shared processor pool	Optional and can be skipped.
Virtual server pinning	Optional, can be set to None as default selection.
SSH key	Choose an existing SSH key that was created previously.

Table 1. SAP HANA general selections

5. In the **Boot image** section, make the following selections:

Field	Details
Operating system	Select the IBM provided subscription 'Linux for SAP (HANA)'. See the explanation of differences in the section Deploying Power Virtual Server instances for SAP on IBM Cloud®
Image	Select an operating system and a version. Make sure that you use the same operating system and version for all deployments.
Tier	Choose a tier that best meets your needs, for more information, see Storage tiers .
Storage pool	Select the storage pool that you need.

Advanced configurations	Enable toggle buttons to support more settings.
-------------------------	---

Table 2. SAP HANA boot image selections

6. In the **Profile** section, make the following selection:
 - Select a profile that meets your needs. For more information, see [SAP HANA profiles](#).
7. In the **Storage volumes** section, make the following selection:
 - For SAP HANA, the attached volumes are on different storage tiers 'Tier 1' and 'Tier 3'. You can't mix storage tiers during the instance creation process, so you need to attach storage volumes later. Leave this list empty.
8. In the **Networking** section, make the following selections:
 - Leave **Public networks** deactivated.
 - Attach both private networks (management and backup) and any separate private networks. Enter the IP addresses as entered in the DNS configuration for the corresponding host names. If the IP addresses are assigned dynamically, you need to adapt the DNS entries for the host names of this system.

It takes some time for the Power Virtual Server instance for SAP HANA to become available. When the deployment is completed, you can log in to the instance via the VPC access host. Use the SSH command below to login as `root` user to the virtual server instance:

```
$ ssh -A -o ServerAliveInterval=60 -o ServerAliveCountMax=600 -o ProxyCommand="ssh -W %h:%p
root@<ACCESS_HOST_FLOATING_IP>" root@<HANA_PVS_IP>
```

`ACCESS_HOST_FLOATING_IP` is a public IP address of a jump host, `HANA_PVS_IP` is the virtual server instance IP address in the management subnet.

An alternative solution for connecting to the VPC instance is to use a VPN server. See more details in the tutorial [Connect by using a client-to-site VPN](#).

Deploying an Power Virtual Server instance for SAP NetWeaver

To deploy an Power Virtual Server instance for SAP NetWeaver, go to your [workspace for Power Virtual Server](#) and create an Power Virtual Server instance as described in [Configuring a Power Virtual Server instance](#). Use the information in [Deploying SAP HANA on Power Virtual Server](#) to complete the configuration for **General**, **Profile**, **Storage volumes**, **Networking** sections. For the **Boot image** section, specify the IBM provided subscription 'Linux for SAP (NetWeaver)' selection.

After creating an Power Virtual Server instance for SAP NetWeaver, wait for the instance to become active. Then log on to the SAP NetWeaver instance by using the following SSH command:

```
$ ssh -A -o ServerAliveInterval=60 -o ServerAliveCountMax=600 -o ProxyCommand="ssh -W %h:%p
root@<ACCESS_HOST_FLOATING_IP>" root@<NETWEAVER_PVS_IP>
```

`ACCESS_HOST_FLOATING_IP` is a public IP address of a jump host, `NETWEAVER_PVS_IP` is the virtual server instance IP address in the management subnet.

Alternatively, connect by using a VPN client, as described in the tutorial [Connect by using a client-to-site VPN](#).

Deploying an optional Power Virtual Server instance for SAP shared file systems

Each deployment of an SAP NetWeaver-based application server, contains file systems that are shared between multiple application server instances. It is a good practice to set up a separate virtual service instance for the shared file systems. A single Power Virtual Server shared file systems instance can be used by multiple SAP systems. Your security requirements determine how many Power Virtual Server shared file systems instances you might need.

To deploy an Power Virtual Server instance for shared file systems, use the Workspace where the SAP HANA and SAP NetWeaver instances were created. Create a shared file system as described in [Configuring a Power Virtual Server instance](#).

After deploying the Power Virtual Server instance for shared file systems, you can use it as Network File System (NFS) storage, where an NFS server will run. How to set up the NFS server is described in the [Deploying an NFS server](#) for [RHEL](#) and [Sharing file systems with NFS](#) for [SLES](#).

Creating extra storage volumes for SAP HANA Power Virtual Server

Modify Power Virtual Server SAP HANA instance and attach extra storage volumes as described in [Managing your storage volumes](#).

In accordance with the SAP sizing guidelines, you should add the following volumes:

- A storage volume for SAP HANA shared file system with a size of MIN (1 x RAM; 1 TB). Storage tier "Tier 3" is sufficient. The "Shareable" switch should remain "off".
- Four or more equal-size storage volumes for SAP HANA log file system with size MIN (1/2xRAM; 512 GB). Divide the file system size by the number of volumes to determine the size for each storage volume. Select "Tier 1", "Tier 0", or "Fixed IOPS Tier" as the storage tier. Ensure that your configuration provides a total of at least 12,000 IOPS (input/output operations per second). The "Shareable" flag should remain "off".
- Four or more equal-sized storage volumes for the SAP HANA data file system with a size of 1.5 times the RAM. Divide the file system size by the number of volumes to determine the size for each storage volume. Select "Tier 1" or "Tier 0" as the storage tier. Ensure that your configuration provides a total of at least 8,000 IOPS (input/output operations per second). The "Shareable" flag should remain "off".
- An extra storage volume for other data (such as "/usr/sap" file system). The Storage tier "Tier 3" is sufficient. The "Shareable" flag should remain "off".
- You can add more volumes for backup or export.

Continue with the configuration of Power Virtual Server instances for SAP applications, which can be done by manual or automated setup. You can choose one of the following setup sections:

- [Configuring Power Virtual Server instances manually](#).
- [Configuring Power Virtual Server instances by using Ansible automation playbooks](#).

Configuring Power Virtual Server instances manually

Complete the following steps on your Power Virtual Server instances.

Checking IBM subscription for an operating system image

To ensure that the OS subscription is set up correctly, check for a subscription by running:

RHEL :

```
$ subscription-manager release
```

```
$ subscription-manager list
```

```
$ yum repolist
```

Optional:

```
$ subscription-manager status
```

SLES :

```
$ SUSEConnect --status
```

RHEL and **SLES** :

Enable the IBM Power Tools repository using:

```
$ /opt/ibm/lop/configure
```

check if repo is enabled:

RHEL :

```
$ yum repolist enabled
```

SLES :

```
$ zypper lr
```

Then run a system update. This will also update the installed Power Tools.

RHEL :

```
$ yum -y update
```

SLES :

```
$ zypper update -y
```

Configuring a proxy endpoint

To use proxy and cache services for HTTP, FTP, and other popular network protocols, you must export a `SQUID_PROXY_SERVER` proxy endpoint. Run the following commands to export a `SQUID_PROXY_SERVER` proxy endpoint:

```
$ export http_proxy=http://<SQUID_PROXY_SERVER>:3128
export https_proxy=https://<SQUID_PROXY_SERVER>:3128
export HTTP_PROXY=http://<SQUID_PROXY_SERVER>:3128
export HTTPS_PROXY=https://<SQUID_PROXY_SERVER>:3128
```

To keep these exported variables persistent across multiple sessions, these entries must be added to `/etc/bash.bashrc` (on SLES) or `/etc/bashrc` (on RHEL). These files ensure that new sessions use the exported variables as environment variables.

Configuring a NTP client

If an NTP server is already configured, you must install the chrony package by using the following command.

RHEL :

```
$ yum install -y chrony
```

SLES :

```
$ zypper install -y chrony
```

Check the status of chrony service:

```
$ systemctl status chronyd
```

Adapt the `chrony.conf` configuration according to the description in the section [Setting up chrony for a system in an isolated network](#).

The following is a sample configuration for `/etc/chrony.conf`:

```
server <NTP_SERVER_IP> iburst
driftfile /var/lib/chrony/drift
makestep 1.0 3
rtcsync
logdir /var/log/chrony
```

Then, restart the `chronyd` service on the node.

```
$ systemctl restart chronyd.service
```

Configuring a DNS client

The public Domain Name Service (DNS) servers of IBM Cloud are configured as default, there is no need to modify the DNS configuration for them. If you create a private DNS server for your environment, you must configure it after the Power Virtual Server instance is created.

Configuring an NFS client

Use the following steps to manually configure an NFS client.

1. Install the `nfs-client` package and enable the NFS client by using the `systemctl` command.

■ **RHEL** :

```
$ yum install -y nfs-utils
```

■ **SLES** :

```
$ zypper install -y nfs-utils
```

2. To enable NFS client service, use the following command.

```
$ systemctl start nfs-client
```

3. After the NFS client service starts, you can mount the shared NFS directory by using the `mount` command.

```
$ mount -t nfs4 -o sec=sys <NFS_SERVER_IP>:<NFS_DIRECTORY_PATH>
```

`NFS_SERVER_IP` is an IP address of a loadbalancer, `NFS_DIRECTORY_PATH` is the path of the NFS file storage share.

Creating file systems manually

For shared SAP file systems, you must create a file system to store SAP data and distribute them to all SAP instances. You can use extra file systems for other purposes.

For an SAP NetWeaver instance, you must create a file system to store instance-specific data.

Three file systems are required to install SAP HANA: data, log, and shared. According to the default installation catalog, these file systems are `/hana/data`, `/hana/log` and `/hana/shared`, but you can customize the file system names. You might also need file systems for other purposes (`/usr/sap` directory). The `/hana/data` and `/hana/log` file systems are striped across four or eight disks, depending on the number of volumes that you created. `/hana/shared` and all other file systems are non-striped 1-disk file systems.

Perform a disk discovery by running the following script:

```
$ /usr/bin/rescan-scsi-bus.sh -a -c -v
```

Newly discovered disks are listed with their details.

To identify the Word Wide Names (WWNs) that will be used to set up storage volumes, run:

```
$ multipath -ll
```

The output of the `multipath -ll` command corresponds to the World Wide Names that are also listed on the IBM Cloud® console. Log on to the IBM Cloud® console and go to the [Storage volumes](#), select a workspace and a Virtual server instance where storage volumes are defined. You might notice that the WWNs on the IBM Cloud® are in uppercase, while they are in lowercase in the operating system.

To create a file system, use the `/hana/data` example that is described below. The same procedure is repeated for `/hana/log` and `/hana/shared` and all other file systems. For example, a storage volume named `dm-6` has a WWN of `600507681381021420000000000a7a8` and a size of 60G. The `3` at the beginning is ignored. The device name is needed to create a logical volume and a volume group.

```
multipath -ll
3600507681381021420000000000a72d dm-0 IBM,2145
size=100G features='1 queue_if_no_path' hwhandler='1 alua' wp=rw
|-- policy='service-time 0' prio=50 status=active
|- 1:0:1:0 sdj 8:144 active ready running
|- 2:0:1:0 sdab 65:176 active ready running
|- 3:0:1:0 sdat 66:208 active ready running
`- 4:0:1:0 sdbl 67:240 active ready running
`-- policy='service-time 0' prio=10 status=enabled
|- 1:0:0:0 sda 8:0 active ready running
|- 2:0:0:0 sds 65:32 active ready running
|- 3:0:0:0 sdak 66:64 active ready running
`- 4:0:0:0 sdcb 67:96 active ready running
3600507681381021420000000000a7a8 dm-6 IBM,2145
```

```

size=60G features='1 queue_if_no_path' hwhandler='1 alua' wp=rw
|-- policy='service-time 0' prio=50 status=active
| |- 1:0:1:4 sdn 8:208 active ready running
| |- 2:0:1:4 sdaf 65:240 active ready running
| |- 3:0:1:4 sdax 67:16 active ready running
| `-- 4:0:1:4 sdbp 68:48 active ready running
`-- policy='service-time 0' prio=10 status=enabled
  |- 1:0:0:4 sde 8:64 active ready running
  |- 2:0:0:4 sdw 65:96 active ready running
  |- 3:0:0:4 sdao 66:128 active ready running
  `-- 4:0:0:4 sdbg 67:160 active ready running
...

```

Multipath aliases are used for this setup. Run the following commands to create the `/hana/data` file system.

Export the following variables:

```

$ export pv_size=60G
$ export lv_name=hana_data_lv
$ export vg_name=hana_data_vg
$ export mount=/hana/data

```

If you are using multipath aliases, use the following commands:

```

$ devices=$(multipath -ll | grep -B 1 $pv_size | grep dm- | awk '{print "/dev/$2"}' | tr '\n' ' ')
$ stripes=$(multipath -ll | grep -B 1 $pv_size | grep dm- | awk '{print "/dev/$2"}' | wc | awk '{print $1}')
$ pvcreate $devices
$ vgcreate ${vg_name} ${devices}
$ lvcreate -i${stripes} -I64 -l100%VG -n ${lv_name} ${vg_name}
$ mkfs.xfs /dev/mapper/${vg_name}-$lv_name
$ mkdir -p ${mount}
$ mount /dev/mapper/${vg_name}-$lv_name ${mount}

```

Run the same commands to create storage volumes for `/hana/log` and `/hana/shared`. Change `lv_name` to `hana_log_lv`, `vg_name` to `hana_log_vg` and `mount` to `/hana/log`.

Export these variables:

```

$ export lv_name=hana_log_lv
$ export vg_name=hana_log_vg
$ export mount=/hana/log

```

Use the same approach for `/hana/shared`.

⚠ Important: Make sure that the variable `pv_size` has different values for `/hana/data`, `/hana/log` and `/hana/shared`, before running the `export` command, otherwise the whole setup will not work.

If you don't use multipath aliases, replace the line starting with `devices=$(())` that is used to identify devices. Instead, use following line:
`devices=$(multipath -ll | grep -B 1 $pv_size | grep dm- | awk '{print "/dev/$2"}' | tr '\n' ' ')`

Checking the storage volumes

After you create the storage volumes, verify that they were created correctly by running the following commands:

```
$ lvscan
```

The command output shows the status of the created logical volumes (LV). The status should be active.

To check if the file system is mounted:

```
$ mount | grep hana
```

The following is a sample output of this command:

```
/dev/mapper/hana_shared_vg-hana_shared_lv on /hana/shared type xfs
(rw,relatime,seclabel,attr2,inode64,logbufs=8,logbsize=32k,noquota)
/dev/mapper/hana_log_vg-hana_log_lv on /hana/log type xfs
(rw,relatime,seclabel,attr2,inode64,logbufs=8,logbsize=64k,sunit=128,swidth=256,noquota)
/dev/mapper/hana_data_vg-hana_data_lv on /hana/data type xfs
(rw,relatime,seclabel,attr2,inode64,logbufs=8,logbsize=64k,sunit=128,swidth=512,noquota)
```

Add the file systems `/hana/data`, `/hana/log` and `/hana/shared` to the file systems table `/etc/fstab`, unless there is already an entry for each of them.

```
$ cat /etc/fstab
```

Sample output:

```
...
/dev/mapper/datavg-datalv /hana/data xfs defaults,nofail 0 0
/dev/mapper/logvg-loglv /hana/log xfs defaults,nofail 0 0
/dev/mapper/sharedvg-sharedlv /hana/shared xfs defaults,nofail 0 0
```

On RHEL 8.8 and RHEL 8.10 please run the following command as a workaround to prevent the logical volumes from becoming inactive after reboot:

```
$ dracut --force --verbose
```

It might be necessary to reboot the operating system. Then check that the LV setup is still correct and proceed to the [Preparing for SAP Installation](#) section.

Configuring Power Virtual Server instances by using Ansible automation playbooks

To configure Power Virtual Server instances for SAP applications, use Ansible automation playbooks on both [RHEL](#) and [SLES](#). Download and install the `ibm.power_linux_sap` Ansible Galaxy collection:

```
$ ansible-galaxy collection install ibm.power_linux_sap
```

This [Ansible Galaxy collection](#) is used on both operating systems, RHEL and SLES without changing any specific OS settings.

Configuring network management services

The `configure_network_management_services` Ansible role installs and configures a proxy endpoint, NTP, DNS, and NFS network services in a virtual server instance. For more details, see the [full role description](#) on Ansible Galaxy.

Before executing an Ansible playbook where the `configure_network_management_services` role is defined, configure the variable file in `playbooks/vars/sample-variables-configure-network-services-client.yml` by updating the downloaded sample with your own values, see an example how it might look like:

```
$ client_config:
  squid:
    enable: true
    squid_server_ip_port: "SQUID_PROXY_SERVER_IP:3128"
    no_proxy_hosts: "161.0.0.0/8"
  ntp:
```

```

enable: true
ntp_server_ip: "NTP_SERVER_IP"
nfs:
  enable: true
  nfs_server_path: "NFS_SERVER_IP:/nfs"
  nfs_client_path: "/nfs"
  opts: sec=sys,nfsvers=4.1,nofail
  fstype: nfs4
dns:
  enable: true
  dns_server_ip: "DNS_SERVER_IP"

```

A detailed description of the parameters `SQUID_PROXY_SERVER_IP`, `NTP_SERVER_IP`, `NFS_SERVER_IP`, `DNS_SERVER_IP`, that are used for the above example, can be found in the section [Edit parameters in the configuration file](#).

After updating the variable file, run the following command:

```
$ ansible-playbook --connection=local -i "localhost," playbooks/sample-configure-network-services-client.yml
```

Creating the file systems

The Ansible role, `powervs_storage_and_swap_setup` is used to create file systems for SAP HANA, SAP NetWeaver, or for a SAP shared file systems instance. This role performs tasks such as creating file systems for `/hana/data`, `/hana/log` and `/hana/shared`, mounting these file systems on provided mount points, adding an entry to `/etc/fstab` for automount on reboot, and other tasks. For more details, see the description of [powervs_storage_and_swap_setup on Ansible Galaxy](#).

Before running a playbook for a storage setup, identify the WWNs as described in the [Manually creating file systems](#) section. Add the WWNs to the `sample-variables-powervs-storage-setup.yml` variable file. For an explanation of the variable file, see the [Edit parameters in the configuration file](#) section.

Next, run an Ansible playbook to create the file systems as:

```
$ ansible-playbook --connection=local -i "localhost," playbooks/sample-powervs-storage-setup.yml
```

To see if all file systems have been created and mounted correctly, use the [Checking of storage volumes](#) section. Continue to [Preparing for SAP installation](#), if the `/hana/data`, `/hana/log`, and `/hana/shared` are mounted correctly.

Preparing for SAP software installation

Preparation for SAP software installation is required for SAP HANA and SAP NetWeaver, but is not needed on the Power Virtual Server instance for SAP shared file systems.

Configuring SLES for SAP applications

SLES

Use the saptune tool to apply recommended operating system settings for SAP HANA or SAP NetWeaver on SUSE Linux® Enterprise Server. On IBM Power Systems Virtual Servers, the same SUSE Linux® Enterprise Server image is used for SAP NetWeaver and SAP HANA.

The following workflow shows how you can use the saptune tool to apply the SAP solution to your server. For more information about saptune, see [SAP Note 1275776 - Linux: Preparing SLES for SAP environments](#).

1. Verify that the package status is current.

```
$ zypper info saptune
```

2. Verify that the saptune version is at least 3.

```
$ saptune version
```

3. List all available solutions. Numbered entries represent integrated SAP Notes for each of the solutions.

```
$ saptune solution list
```

4. Get an overview of saptune options.

```
$ saptune --help
```

5. Enable and start the saptune.service. This command also disables sapconf and tuned, which isn't used since saptune version 3.

```
$ saptune service takeover
```

6. Simulate the changes before applying them (optional).

For SAP HANA:

```
$ saptune solution simulate HANA
```

For SAP NetWeaver:

```
$ saptune solution simulate NETWEAVER
```

7. Apply the saptune solution.

For SAP HANA:

```
$ saptune solution apply HANA
```

For SAP NetWeaver:

```
$ saptune solution apply NETWEAVER
```

8. Check the saptune status.

```
$ saptune status
```

9. Verify if the saptune is set up correctly.

```
$ saptune check
```

Configuring RHEL for SAP applications

RHEL

RHEL System Roles for SAP are a collection of Ansible roles that help you configure a RHEL system for installing SAP HANA or SAP NetWeaver. Ansible roles for SAP configuration are distributed and updated directly by Red Hat, so the task performed and parameters required might vary depending on the version of the `rhel-system-roles-sap` package. The RHEL image that is provided by IBM includes the Ansible execution engine, SAP-related system roles, and the Ansible execution files.



Note: Starting with `rhel-system-roles-sap-3.2.0-1.el8_4`, the role names have changed. The `/root/sap-preconfigure.yml`, `/root/sap-netweaver.yml`, and `/root/sap-hana.yml` files in the OS images for RHEL 8.1 or RHEL 8.4 must be adapted. For more information, see [following Red Hat article](#).

Previous role name	New role name
sap-preconfigure	sap_general_preconfigure
sap-netweaver-preconfigure	sap_netweaver_preconfigure
sap-hana-preconfigure	sap_hana_preconfigure

Table 3. RHEL System Roles

The RHEL system roles for setting up SAP application are available in the root directory.

Use the following command to prepare the operating system for an SAP HANA workload.

- For RHEL 8.4 and previous versions:

```
$ ansible-playbook /root/sap-hana.yml
```

- For RHEL versions RHEL 8.6 and greater:

```
$ ansible-playbook -i /root/inventory /root/sap-hana.yml
```

Use the following command to prepare the operating system for an SAP NetWeaver workload.

- For RHEL 8.4 and previous versions:

```
$ ansible-playbook /root/sap-netweaver.yml
```

- For RHEL versions RHEL 8.6 and greater:

```
$ ansible-playbook -i /root/inventory /root/sap-netweaver.yml
```

For more information about customizing the operating system, see the following documentation.

- [SAP Note 2772999 "Red Hat Enterprise Linux 8.x: Installation and Configuration"](#)
- [SAP Note 2777782 "SAP HANA DB: Recommended OS Settings for RHEL8"](#)
- [SAP Note 2382421 "Optimizing the Network Configuration on HANA- and OS-Level"](#)
- [Red Hat Enterprise Linux System Roles for SAP](#)

Configuring jumbo frames

Jumbo frames should be enabled by setting `MTU='9000'`.

RHEL

In the `/etc/sysconfig/network-scripts` directory, check that the `ifcfg-env0`, `ifcfg-env2`, `ifcfg-env(...)` files contain the `MTU='9000'` parameter.

SLES

In the `/etc/sysconfig/network` directory, check the content of the files such as `ifcfg-eth0`, `ifcfg-eth1`, etc.

Checking the NUMA layout

Check that the CPU and memory placement is optimized for SAP HANA by running the `chk numa lpm.py` script. The `chk numa lpm.py` script performs the following actions.

- Checks the nonuniform memory access (NUMA) layout according to SAP HANA rules. The script verifies that there are no cores without memory and that the memory distribution between the cores doesn't exceed a margin of 50%. In the first case, the script generates an error; in the second case, the script generates a warning.
- Checks if a Live Partition Mobility (LPM) operation has been performed. After LPM, the NUMA layout might be different from the configuration at boot time. The script searches the system log for the last LPM operation. A warning is generated if there has been an LPM operation since the last system boot.

1. Check the information in [SAP Note 2923962](#).
2. Download the `chk numa lpm.py` script that is attached to this SAP Note and copy it to your Power Virtual Server instance.
3. Set executable permissions for the script:

```
$ chmod +x ./chk numa lpm.py
```

4. Run the script:

```
$ ./chk numa lpm.py
```

Next Steps

Your infrastructure is now ready to install the SAP software.

Custom OS image build process on RHEL for SAP solutions on IBM® Power® Virtual Server

The following information describes how to build a custom operating system (OS) image on Red Hat Enterprise Linux (RHEL) for SAP software on IBM® Power® Virtual Server.

Custom OS image build requirements

Complete the following requirements before you start the image build process:

- Create an [IBM Cloud account](#) and obtain the necessary credentials to deploy an image build server on Power Virtual Server. Details about identity and access management (IAM) are described in [Managing identity and access management \(IAM\) for IBM® Power® Virtual Server](#).
- Ensure that you have access to IBM Cloud Object Storage so that you can upload a base image. See [Getting started with IBM Cloud Object Storage](#) for information on how to get started.
- Download the Red Hat Enterprise Linux 9 KVM Guest Image [rhel-9.4-ppc64le-kvm.qcow2](#) from [Red Hat Enterprise Linux for Power little endian](#).



Note: The following guidance for building a custom OS image is based on RHEL 9.4 OS image.

- Create an image build server, where you configure an image build environment and build an OS image. It consists of an Power Virtual Server instance running RHEL 9.2 (RHEL9-SP2-SAP-NETWEAVER) or higher RHEL version, with the additional storage volume of 200 GByte. There are two methods how to set up the image build server:
 - For a manual approach, refer to the detailed information in [Getting started with Power Virtual Server](#) and [Creating an IBM Power Virtual Server](#).
 - For an automated approach, refer to the [Power Virtual Server with VPC Landing Zone](#) deployment guide.

Setup a build image environment

The following steps describe how to set up a build server environment for image creation.

1. Log in to your build server and check its registration status by executing the following command.

```
$ subscription-manager status
```

2. Update RHEL OS packages.

3. Check and adjust proxy settings for a build environment. Configure temporary HTTPS proxy settings by using your Proxy IP address or URL. If you deployed the automated Power Virtual Server with VPC landing zone from IBM Cloud catalog, use this proxy address <http://10.30.40.7:3128/> for your configuration.

```
$ export https_proxy="http://10.30.40.7:3128/" || die "Set HTTPS proxy failed (rc $?)"
```

4. Create a '/data' directory and export an environment variable that points to it.

```
$ mkdir -p /data
```

```
$ export MOUNT_PATH=/data
```

5. Attach an additional storage volume with a capacity of 200 GB and create the [/data](#) file system.

- Run the multipath command to identify the available storage volumes and their World Wide Names (WWNs). Ensure that the command output only shows one 200 GB storage volume. Otherwise, creating the file system will not work properly..

```
$ multipath -ll
```

- Export the following variables for physical and logical volumes, a volume group, and a mount directory.

```
$ export PV_SIZE=200G
```

```
$ export LV_NAME=image_lv
```

```
$ export VG_NAME=image_vg
```

- Create the physical and logical volumes.

```
$ devices=$(multipath -ll | grep -B 1 $PV_SIZE | grep dm- | awk '{print "/dev/".$2}' | tr '\n' ' ')
```

```
$ stripes=$(multipath -ll | grep -B 1 $PV_SIZE | grep dm- | awk '{print "/dev/".$2}' | wc | awk '{print $1}')
```

```
$ pvcreate $devices
```

```
$ vgcreate ${VG_NAME} ${devices}
```

```
$ lvcreate -i${stripes} -I64 -l100%VG -n ${LV_NAME} ${VG_NAME}
```

```
$ mkfs.xfs /dev/mapper/${VG_NAME}-$({LV_NAME})
```

- Check if the created logical volume is active.

```
$ lvscan
```

- Mount the file system.

```
$ mount -t xfs -o defaults,nofail --source /dev/mapper/${VG_NAME}-$({LV_NAME}) --target ${MOUNT_PATH}
```

- Add the file system to the `/etc/fstab` file.

```
$ echo "/dev/mapper/${VG_NAME}-$({LV_NAME}) ${MOUNT_PATH} xfs defaults,nofail 0 0" >> /etc/fstab
```

- Ensure that the file system is present in the list of all mounted file systems.

```
$ df -h
```

6. Create the directory `/data/image` where the base image is saved.

7. Copy the image `rhel-9.4-ppc64le-kvm.qcow2` to `/data/image`.

8. Create the `/data/tmp` directory, in which a temporary image is saved during the build process.

9. Complete the following tasks to configure the build server. Use the `dnf` RHEL package manager.

- Install the `xfsprogs` and `lvm2` system packages.
- Install the `make`, `git`, `libgcrypt-devel` and `go-toolset` development packages.
- Install the `qemu-img` and `cloud-utils-growpart` packages.
- Configure a proxy by adding your proxy host in the file `~root/.bashrc`.

```
export https_proxy='<your_https_proxy>'
```

10. Configure the NBD module to load at boot time by adding the following lines to the file `/etc/modules-load.d/nbd.conf`.

```
nbd
options nbd max_part=8
```

11. Download the `pvsadm` tool from the [latest release of pvsadm-linux-ppc64le](#) GitHub repository. Save it in the file named `/usr/local/bin/pvsadm` and change the mode to `0755`. For more details about the tool, refer to [pvsadm tool](#).

Building a custom OS image

The build process of a custom OS image for IBM Cloud PowerVS consists of the following tasks.

1. Check that the Red Hat Satellite subscription credentials are valid.

2. Create an empty file named `image-prep.template` and use it as the image preparation template .
3. The following tasks contain the shell commands that are needed for building a customized image. Add these commands to the template `image-prep.template`. The commands update the base OS image during image creation with the `pvsadm` tool to create the final SAP-ready OS image. The command order is important and should not be changed.

- Copy the following lines, including error handling, to be used as the template header.

```
#!/usr/bin/env bash
set -o errexit
set -o nounset
set -o pipefail

die() {
    echo -e "\n${1}"
    set +o errexit
    set +o nounset
    exit 1
}
```

- Add a temporary name server.

```
$ echo "nameserver 9.9.9.9" >> /etc/resolv.conf \
|| die "Add nameserver failed (rc $?)"
```

- Create a work directory `/tmp/work` and export it as an environmental variable.

```
$ mkdir -p /tmp/work || die "Create work directory failed (rc $?)"
```

```
$ export WORK_DIR=/tmp/work
```

- Create the 25GB swap file, add permissions and check that it has been created correctly.

```
$ fallocate -l 25G /swapfile || die "allocate swapfile failed (rc $?)"
```

```
$ chmod 600 /swapfile || die "chmod swapfile failed (rc $?)"
```

```
$ mkswap /swapfile || die "mkswap swapfile failed (rc $?)"
```

```
$ swapon /swapfile || die "swapon swapfile failed (rc $?)"
```

```
$ swapon --show
```

```
$ echo "/swapfile swap swap defaults 0 0" >> /etc/fstab || die "update fstab with swapfile failed (rc $?)"
```

```
$ echo "swapon -s"
```

- Subscribe to Red Hat Satellite and enable the SAP repositories. Use your own values for the subscription user name, password and release version.

```
$ subscription-manager register \
--force --auto-attach \
--username=<SUBSCRIPTION_USER> \
--password=<SUBSCRIPTION_PASSWORD> \
--release=<OS_VERSION> \
|| die "Register subscription failed (rc $?)"
```

```
$ subscription-manager repos \
--disable="*" \
--enable="rhel-9-for-$(uname -m)-baseos-e4s-rpms" \
--enable="rhel-9-for-$(uname -m)-appstream-e4s-rpms" \
--enable="rhel-9-for-$(uname -m)-sap-solutions-e4s-rpms" \
--enable="rhel-9-for-$(uname -m)-sap-netweaver-e4s-rpms" \
--enable="rhel-9-for-$(uname -m)-highavailability-e4s-rpms"\
```

```
--enable="codeready-builder-for-rhel-9-$(uname -m)-rpms" \
|| die "Repository configuration failed (rc $?)"
```

- Install a package group server.

```
$ dnf -y group install server \
|| die "Installing server group packages failed (rc $?)"
```

- Install the system packages.

```
$ dnf -y install \
cloud-init \
device-mapper-multipath \
libcrypt-compat \
glibc-langpack-en \
|| die "Install system packages failed (rc $?)"
```

- Update `grub2`.

```
$ dnf -y reinstall grub2-common \
|| die "Reinstall system package failed (rc $?)"
```

```
$ dnf -y update grub2 \
|| die "Update grub2 package failed (rc $?)"
```

- Install Ansible and the Red Hat system roles for SAP.

```
$ dnf -y install ansible-core rhel-system-roles rhel-system-roles-sap \
|| die "Install Ansible and RH System Roles failed (rc $?)"
```

- Enable the EPEL repository.

```
$ dnf -y install "https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm" \
|| die "Installation EPEL configuration failed (rc $?)"
```

- Configure the IBM Power [tools repository](#).

```
$ dnf -y install "https://public.dhe.ibm.com/software/server/POWER/Linux/yum/download/ibm-power-repo-
latest.noarch.rpm" \
|| die "Installation IBM Power Tools configuration failed (rc $?)"
```

```
$ echo 'y' | (/opt/ibm/lop/configure \
|| die "Power Tools configuration failed (rc $?)")
```

- Install the IBM Power tools and disable the repository.

```
$ dnf config-manager --set-disabled Advance_Toolchain \
|| die "Disable Advance Toolchain repository failed (rc $?)"
```

```
$ dnf -y install ibm-power-managed-rhel9 \
|| die "Install IBM Power Tools failed (rc $?)"
```

```
$ dnf config-manager --set-disabled IBM_Power_Tools \
|| die "Disable IBM Power Tools repository failed (rc $?)"
```

- Updating OS.

```
$ dnf -y update || die "OS update failed (rc $?)"
```

- Remove the EPEL repository.

```
$ dnf -y remove epel-release \
|| die "Uninstall EPEL configuration failed (rc $?)"
```

- Unregister from the Red Hat Satellite server.

```
$ subscription-manager unregister \
|| die "Unregister subscription failed (rc $?)"

$ subscription-manager clean \
|| die "Clean subscription failed (rc $?)"
```

- Change the cryptographic policy (disable SHA1/CBC).

```
$ echo -e "cipher@ssh = -*~CBC\n" \
> /etc/crypto-policies/policies/modules/NO-CBC.pmod \
|| die "Create of CBC disabling file failed (rc $?)"

$ update-crypto-policies --set DEFAULT:NO-SHA1:NO-CBC \
|| die "Update of cryptografic policy failed (rc $?)"
```

- Create a basic multipath configuration.

```
$ echo -e "defaults {\n \
    user_friendly_names no\n \
    find_multipaths smart\n}\n" \
> /etc/multipath.conf \
|| die "Create multipath configuration failed (rc $?)"
```

- Define an Ansible inventory.

```
$ echo -e "localhost ansible_connection=local\n" > /root/inventory \
|| die "Create Ansible inventory file failed (rc $?)"
```

- Create Ansible yml-files for SAP HANA and NetWeaver.

```
cat <<EOF > /root/sap-hana.yml \
|| die "Create SAP HANA Ansible file failed (rc $?)"
- hosts: localhost
  vars:
    sap_hana_preconfigure_min_rhel_release_check: false
    sap_hana_preconfigure_install_ibm_power_tools: false
    sap_hana_preconfigure_add_ibm_power_repo: false
  connection: local
  roles:
    - redhat.sap_install.sap_general_preconfigure
    - redhat.sap_install.sap_hana_preconfigure
EOF
```

```
cat <<EOF > /root/sap-netweaver.yml \
|| die "Create SAP NetWeaver Ansible file failed (rc $?)"
- hosts: localhost
  connection: local
  roles:
    - redhat.sap_install.sap_general_preconfigure
    - redhat.sap_install.sap_netweaver_preconfigure
EOF
```

```
cat <<EOF > /root/sap-preconfigure.yml \
|| die "Create SAP preconfiguration Ansible file failed (rc $?)"
- hosts: localhost
  connection: local
  roles:
    - redhat.sap_install.sap_general_preconfigure
EOF
```

- Change the default kernel parameter in the file [/etc/sysctl.conf](#).

```
cat <<EOF >> /etc/sysctl.conf \
```

```

|| die "Change of kernel parameter failed (rc $?)"
net.core.rmem_max = 56623104
net.core.wmem_max = 56623104
net.ipv4.tcp_rmem = 65536 262088 56623104
net.ipv4.tcp_wmem = 65536 262088 56623104
net.ipv4.tcp_mem = 56623104 56623104 56623104
EOF

```

- Enable Receive Flow Steering (RFS) on ibmveth devices, adjust the file `/etc/udev/rules.d/70-ibmveth-rfs.rules`.

```

cat <<EOF >> /etc/udev/rules.d/70-ibmveth-rfs.rules \
|| die "Create udev rule for RFS failed (rc $?)"
# Enable Receive Flow Steering (RFS) on ibmveth devices
SUBSYSTEM=="net",ACTION=="add",DRIVERS=="ibmveth",RUN{program}+="/bin/bash -c 'echo 32768 >
/sys/\$DEVPATH/queues/rx-0/rps_flow_cnt';"
EOF

```

Enable the Receive Flow Steering (RFS) in the file `/etc/sysctl.d/95-enable-rfs.conf`.

```

cat <<EOF >> /etc/sysctl.d/95-enable-rfs.conf \
|| die "Create kernel parameter file for RFS failed (rc $?)"
# Enable Receive Flow Steering (RFS)
net.core.rps_sock_flow_entries=32768
EOF

```

- Configure the SSH daemon.

```

$ sed -i \
-e 's/^(\#\!)\\?PermitRootLogin .*/PermitRootLogin yes/g' \
-e 's/^(\#\!)\\?PasswordAuthentication .*/PasswordAuthentication no/g' \
-e 's/^(\#\!)\\?MaxStartups .*/MaxStartups 10:30:60/g' \
/etc/ssh/sshd_config \
|| die "Failed SSH daemon configuration (rc $?)"

```

- Adapt GRUB.

- Check that the PReP partition exists and update it.

```

prep_partition=$(fdisk -l | grep -i ppc | grep -i loop | awk '{print $1}')

# Check if a PReP partition was found
if [ -z "$prep_partition" ]; then
    echo "No PReP partition found with /dev/loop."
    exit 1
else
    echo "PReP partition found: $prep_partition"
fi

```

- Install `grub2` on the PReP partition.

```

$ grub2-install "$prep_partition" \
|| die "Install GRUB update failed (rc $?)"

```

- Execute the bootlist command.

```

$ bootlist -m normal -o || die "Setting boot list failed (rc $?)"

```

- Change the GRUB default timeout option.

```

$ sed -i \
-e 's/GRUB_TIMEOUT=.*/GRUB_TIMEOUT=20/' \
/etc/default/grub || die "Fail to change default GRUB options (rc $?)"

```

- Update the GRUB configuration.

```

$ grubby --update-kernel=ALL \

```

```
--remove-args="net.ifnames=0" \
--args="console=tty0 console=hvc0,115200n8 crashkernel=2G-4G:384M,4G-16G:512M,16G-64G:1G,64G-128G:2G,128G-:4G rd.shell rd.debug rd.driver.pre=dm_multipath log_buf_len=1M elevator=none" \
|| die "GRUB cmdline configuration update failed (rc $?)"
```

- Enable multipath for all kernels.

```
$ echo -e 'force_drivers+=" dm-multipath "\n' >/etc/dracut.conf.d/10-mp.conf \
|| die "Create of multipath include file for dracut failed (rc $?)"
```

```
dracut --regenerate-all --force \
|| die "Regenerate of initramfs images failed (rc $?)"
for kernel in $(rpm -q kernel | sort -V | sed 's/kernel-//'); do
    dracut --kver ${kernel} --force --add multipath --include /etc/multipath\
/etc/multipath --include /etc/multipath.conf /etc/multipath.conf \
|| die "Generate initramfs of ${kernel} failed (rc $?)"
done
```

- Generate the GRUB configuration.

```
$ grub2-mkconfig -o /boot/grub2/grub.cfg \
|| die "Generate GRUB configuration failed (rc $?)"
```

- Remove the temporary name server.

```
$ sed -i '/nameserver 9.9.9.9/d' /etc/resolv.conf \
|| die "Remove nameserver failed (rc $?)"
```

- Enable SELinux relabeling on the next boot.

```
$ touch /.autorelabel || die "Create relabel file failed (rc $?)"
```

- Delete the root user password.

```
$ usermod -p '!' root || die "Delete root password failed (rc $?)"
```

- Clean up the file system.

```
$ rm -rf /etc/sysconfig/network-scripts/ifcfg-eth*
```

```
$ rm -rf /tmp/work
```

```
$ rm -rf /root/.ssh
```

```
$ rm -rf /etc/pki/entitlement/
```

```
$ rm -rf /setup.sh
```

- Deleting command history.

```
$ history -c
```

4. Before running the `pvsadm` tool, make sure that local swapping on a build server is disabled. Otherwise, the error `mkswap: error: /swapfile is mounted; will not make swapspace` occurs while executing `pvsadm`. To disable swapping, run the following command.

```
$ swapoff -a
```

5. Use the `pvsadm` image build tool with the `qcov2ova` command to convert the qcov2 image to the OVA format. Set your own customized values for the command flags according to their input formats. See the description of the flags below.

```
--image-name <string>      Name of the resultant OVA image
```

```

--image-url <string> URL or absolute local file path to the qcow2 image
--image-dist <string> Image Distribution(supported: rhel, centos, coreos)
--target-disk-size <int> Size (in GB) of the target disk volume where OVA will be copied (default 120)
--rhn-user <string> RedHat Subscription username. Required when Image distribution is rhel
--rhn-password <string> RedHat Subscription password. Required when Image distribution is rhel
--os-password <string> Root user password, will auto-generate the 12 bits password(applicable only for redhat and cento distro)
--temp-dir <string> Scratch space to use for OVA generation
--prep-template <string> Image preparation script template

```

For instance, use the `rhel-9.4-ppc64le-image` as a new OS image name, `rhel-9.4-ppc64le-kvm.qcow2` is the base OS image located in `/data/image`, so the absolute local path for the qcow2 image is `/data/image/rhel-9.4-ppc64le-kvm.qcow2`, and the image distribution is `rhel`. Adjust the image and target disk sizes according to your requirements, 120 GB is set as the default value for the target disk volume. An image preparation script template is `image-prep.template`, and the name of the script is customizable as well. To simplify running the `pvsadm` image build tool, you can set up environment variables as well.

```

export IMAGE_NAME=rhel-9.4-ppc64le-image
export QCOW2_IMAGE_PATH=/data/image/rhel-9.4-ppc64le-kvm.qcow2
export IMAGE_SIZE=100
export TARGET_DISK_SIZE=100
export SUBSCRIPTION_USER=<RedHat subscription username>
export SUBSCRIPTION_PASSWORD=<RedHat Subscription password>
export IMAGE_BUILD_DIRECTORY=/data/tmp
export IMAGE_PREP_SCRIPT=image-prep.template

```

```

$ pvsadm image qcowsova --image-name ${IMAGE_NAME} \
    --image-url ${QCOW2_IMAGE_PATH} \
    --image-dist rhel \
    --image-size ${IMAGE_SIZE} --target-disk-size ${TARGET_DISK_SIZE} \
    --rhn-user ${SUBSCRIPTION_USER} \
    --rhn-password ${SUBSCRIPTION_PASSWORD} \
    --temp-dir ${IMAGE_BUILD_DIRECTORY} \
    --prep-template ${IMAGE_PREP_SCRIPT}

```

The `pvsadm` tool has a help menu with detailed descriptions of usage, commands and flags. Run the following command to access the help menu.

```
$ pvsadm --help
```

6. Upload the custom-created OS image to Cloud Object Storage (COS).

Importing OS image in the Power Virtual Server workspace

To import your custom boot image, see the guidance for [Importing a boot image](#).

Creating an Power Virtual Server instance from the new imported OS image

To provision a new Power Virtual Server instance follow the steps that are described in [Using a custom boot image to provision a new instance](#).

Terraform for SAP solutions on Intel VPC

Terraform deployment templates

IBM provides several templates with scripts to deploy different SAP NetWeaver and SAP HANA architectures:

- [Deploying SAP bastion server – SAP media storage repository](#)
- [Deploying single-tier VPC for SAP on IBM Cloud VPC \(Terraform\)](#)
- [Deploying SAP AnyDB \(non-SAP HANA\) 2-tier and 3-tier distributed architecture on IBM Cloud VPC \(Terraform\)](#)
- SAP NetWeaver and Db2 single-tier on IBM Cloud VPC
 - [Overview SAP workload deployment on IBM Cloud® Virtual Private Cloud \(VPC\) \(Terraform and Ansible\)](#)
 - [Deploying SAP NetWeaver 7.x and Db2 on an existing IBM Cloud VPC \(Terraform and Ansible\)](#)
- SAP NetWeaver and Db2 3-tier on IBM Cloud VPC
 - [Overview SAP workload deployment on IBM Cloud Virtual Private Cloud \(VPC\) \(Terraform and Ansible\)](#)
 - [Deploying SAP NetWeaver 7.x and Db2 on 3-tier IBM Cloud VPC \(Terraform and Ansible\)](#)
- SAP HANA stand-alone VSI on IBM Cloud VPC
 - [Background for automating SAP HANA stand-alone virtual server instance on IBM Cloud VPC](#)
 - [Deploying SAP HANA stand-alone virtual server instance on IBM Cloud VPC \(Terraform\)](#)
- SAP NetWeaver and ASE SYB on IBM Cloud VPC
 - [Introduction to SAP NetWeaver and ASE SYB](#)
 - [Deploying SAP NetWeaver 7.x and ASE SYB on an existing IBM Cloud VPC \(Terraform and Ansible\)](#)
- SAP AAS for SAP HANA and AnyDB on IBM Cloud VPC
 - [Introduction to IBM Cloud VPC and Additional Application Server \(AAS\) to HANA and AnyDB](#)
 - [Deploying Additional Application Server \(AAS\) to SAP HANA and AnyDB on an existing IBM Cloud VPC \(Terraform\)](#)
- SAP S/4HANA HA deployment on IBM Cloud VPC
 - [Overview for deploying SAP workload HA deployment on IBM Cloud Virtual Private Cloud \(VPC\) \(Terraform and Ansible\)](#)
 - [Deploying SAP workload S/4HANA HA deployment on IBM Cloud VPC \(Terraform and Ansible\)](#)
- SAP HANA DB backup to Cloud Object Storage
 - [Introduction to IBM Cloud VPC and HANA db backup automation on Cloud Object Storage](#)
 - [Deploying SAP HANA db backup to Cloud Object Storage on existing IBM Cloud VPC \(Terraform\)](#)
- [Deploying SAP S/4HANA on 3-tier IBM Cloud VPC \(Terraform and Ansible\)](#)
- SAP BW/4HANA 3-tier on IBM Cloud VPC
 - [Overview SAP workload deployment on IBM Cloud Virtual Private Cloud \(VPC\) with Terraform and Ansible](#)
 - [Deploying SAP BW/4HANA on 3-tier IBM Cloud VPC \(Terraform and Ansible\)](#)
- [Deploying SAP NetWeaver 7.x and SAP HANA 3-tier distributed architecture on IBM Cloud VPC \(Terraform and Ansible\)](#)

Deploying the SAP bastion server – SAP media storage repository

This topic describes how to do an automated deployment of SAP bastion and storage setup on Red Hat Enterprise Linux 8.4. It shows how to deploy an IBM Cloud Virtual Private Cloud (VPC) with a bastion host with secure remote SSH access. In SAP Terraform and Ansible deployments, the bastion host is used to give external administrative access to the other servers and applications. The bastion server is accessed through the Floating IP. The bastion server includes a customizable security group and subnet to enable access to the same region zones on its dedicated SAP/DBs and the VSI's IPs and ports. The floating IP also allows the bastion host access to the internet so the sap and DB kits can be downloaded. Also, a dedicated client-to-site VPN solution will be created automatically to provide direct access to the private IP address for future SAP servers, using an OpenVPN software client.

Before you decide which SAP automated solution you want to deploy in IBM Cloud VPC, run the bastion server automated deployment. You need to specify the amount of dedicated storage that is needed to download and store the SAP kits. The SAP kits are used to deploy wanted SAP solution from the IBM Cloud VPC automated SAP solutions pool. The bastion server in IBM Cloud is primarily used for SAP solution deployment. It can be used as a Jump Host, for example, to maintain and administer all SAP solutions within its respective IBM Cloud VPC region.

Each customer is given an SAP S-user that reflects their contractual details with SAP, including:

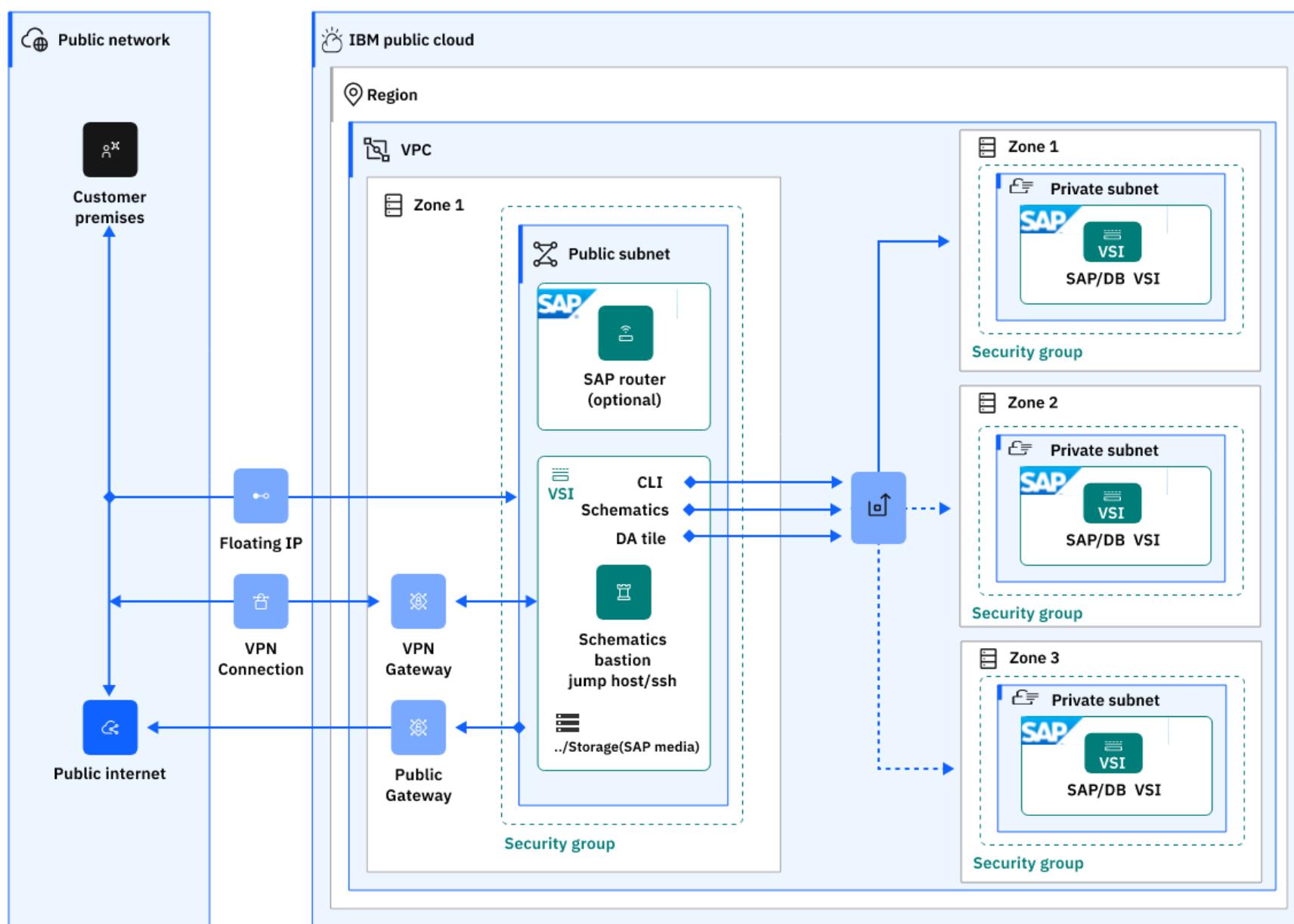
- SAP support
- SAP Notes

- System maintenance
- Generate and maintain SAP and DB licenses
- Migrations keys

It is the customers responsibility to download and prepare the necessary SAP kits from [SAP launchpad support](#) and store them on the dedicated and customizable storage. The SAP kits are used during automated deployment when Ansible is called.

Solution implemented

The Bastion server is used for remote software installation by using Terraform remote-exec and Ansible playbooks run by Schematics.



The Terraform modules implement a 'reasonable' set of best practices for bastion host configuration only. Your own Organization might have more requirements that you must apply before the deployment.

It contains:

- Terraform scripts for deploying a VPC, Subnet, Security Group with default and custom rules, a VSI with a volume, a Secrets Manager service instance and a VPN client-to-site solution.
- Bash scripts to install the prerequisites for SAP BASTION&STORAGE VSI and other SAP solutions.

VPC Configuration

The Security Rules are:

- Allow all traffic in the Security group
- Allow all outbound traffic
- Allow inbound DNS traffic (UDP port 53)
- Allow inbound SSH traffic (TCP port 22)
- Option to Allow inbound TCP traffic with a custom port or a range of ports.

VSI Configuration

The VSI is configured with Red Hat Enterprise Linux 8.4 (amd64), has a minimal of two SSH keys that are configured to be accessed by the root user and one storage volume.

VPN Configuration

For the VPN solution, a Secrets Manager instance will be provisioned. Two secrets are provisioned, the server certificate and the client certificate; both will be used during the VPN creation and also to generate the `ovpn` file for the connection. You can see these secrets under the Secrets Managers page > Secrets and select **View secret** option.

The VPN server will have a dedicated Security Group. The Security Group will open the UDP port 443 for all source IP addresses. This can be later customized according to the customers needs.

A rule is added for the bastion's Security Group to allow all the traffic from the VPN's Security Group. Later, if other Security Groups are added to the VPC and you want to allow access to their attached resources through the VPN connection, then the same rule should be configured for those as well.

The automation script will generate on the bastion server an ovpn profile file for your OpenVPN client. You need to download from the bastion and import in your OpenVPN client.

Software configuration

- Terraform - an open source infrastructure as code software tool created by HashiCorp.
- Ansible - an open source software provisioning and configuration management tool.
- The IBM Cloud Command Line Interface provides commands for managing resources in IBM Cloud.

Bastion input variables

Parameter	Description
IBMCLOUD_API_KEY	IBM Cloud API key (Sensitive* value).
PRIVATE_SSH_KEY	The id_rsa private key content from your local system (Sensitive* value).
REGION	The cloud region to deploy the resources. For more information about regions and zones for VPC, see Locations . Review the supported locations in IBM Cloud Schematics that are listed in Locations and endpoints . Sample value: eu-de.
ZONE	The cloud zone where to deploy the solution. Sample value: eu-de-2.
VPC_EXISTS	Specify whether the chosen VPC exists (enter 'yes' or 'no'). If you choose 'no', the VPC is created.
SUBNET_EXISTS	Specify whether the chosen SUBNET/SECURITYGROUP exist (use 'yes' or 'no'). If you choose 'no', a SUBNET/SECURITYGROUP with OPEN PORTS is created in the specified VPC.
ADD_OPEN_PORTS_IN_NEW_SUBNET	Create a new port/s only if a NEW SUBNET is created, use 'yes' or 'no'.
OPEN_PORT_MINIMUM (Required, Integer)	The TCP port range that includes the minimum value. Valid values are 1 - 65535.
OPEN_PORT_MAXIMUM (Required, Integer)	The TCP port range that includes the maximum value. Valid values are 1 - 65535.
VPC	The name of the VPC. View the list of available VPCs on the IBM Cloud Console Virtual private clouds page.
SUBNET	The name of the Subnet. View the list of available Subnets on the IBM Cloud Console [Subnets] (https://cloud.ibm.com/infrastructure/network/subnets){: external} page.
SECURITYGROUP	The name of the Security Group. View the list of available Security Groups on the IBM Cloud Console Security groups for VPC page.
HOSTNAME	The hostname for the VSI. The hostname must have up to 13 characters.

PROFILE	The profile used for the VSI. For more information about profiles, see Instance profiles . Default value: "bx2-2x8".
IMAGE	The OS image used for the VSI. For more information about available images, see Virtual server images . Default value: ibm-redhat-8-4-minimal-amd64-1.
SSH_KEYS	List of SSH Key IDs that are allowed to SSH as <code>root</code> to the VSI. This can contain one or more IDs. View the list of available SSH Keys on the IBM Cloud Console SSH keys for VPC page. Sample input (use your own SSH IDs from IBM Cloud) ["r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a", "r010-3fc9fe7-d4a7-41ce-8bb3-d96e936b2c7e"]
VOL1 [number]	The size for the disk in GB to be attached to the BASTION VSI as storage for the SAP deployment kits. The mount point for the new volume is: "/storage". Default value: 100 GB.
VPN_CREATE	Specifies if you want a VPN solution to be added to your bastion setup. If 'yes' a VPN solution will be automatically deployed for you, allowing you access to the private ip addressing space of your VPC.
VPN_PREFIX	The prefix to use for the VPN-related elements. The prefix set under this variable will be added to the Secrets Manager instance created, also used as a prefix for the VPN's Security Group and it will be used as a name for the VPN server created.
VPN_NETWORK_PORT_PROTOCOL	The protocol to be used for the VPN solution. (must be either 'tcp' or 'udp')
VPN_NETWORK_PORT_NUMBER	The port number to be used for the VPN solution. (must be between 1 and 65535)
SM_PLAN	The pricing plan to be used for the Secrets Manager instance, provided as a plan ID. Use 869c191a-3c2a-4faf-98be-18d48f95ba1f for trial or 7713c3a8-3be8-4a9a-81bb-ee822fcaac3d for standard.
VPN_CLIENT_IP_POOL	Optional variable to specify the CIDR for VPN client IP pool space. This is the IP space that will be used by systems connecting with the VPN. You should only need to change this if you have a conflict with your local network.
DESTROY_BASTION_SERVER_VSI	For the initial deployment, should remain set to false. After the initial deployment, in case there is a wish to destroy the Deployment Server (Bastion Server) VSI, but preserve the rest of the Cloud resources (VPC, Subnet, Security Group, and VPN Solution), in Schematics, the value must be set to true and then the changes must be applied by pressing the "Apply plan" button.

Sensitive* - The variable value is not displayed in your workspace details after it is stored. Make sure to select **Sensitive** on the Settings page for all fields marked "Sensitive".



Note: VOL1 [number] variable represents the defined customer size of the storage that is needed to store downloaded SAP kits before you run the automated SAP deployment. The storage size can be customized when you deploy the bastion SAP VPC and VSI. The default storage that is allocated is 100 GB.

Before you begin

1. To complete this procedure, you need a general understanding of IBM Cloud VPC and VSIs. To run the example in IBM Cloud Schematics, you need an IBM Cloud account. The deployed resources are chargeable.
2. [Create or retrieve an IBM Cloud API key](#). The API key is used to authenticate with the IBM Cloud platform and to determine your permissions for IBM Cloud services.
3. Be sure that you have the [required IBM Cloud IAM permissions](#) to create and work with VPC infrastructure and you are [assigned the correct permissions](#) to create the workspace and deploy resources.
4. [Generate an SSH key](#). The SSH key is required to access the provisioned VPC virtual server instances through the bastion host. After you create your SSH key, make sure to [upload this SSH key to your IBM Cloud account](#), in the VPC region and resource group where you want to deploy the bastion server.

- Verify that you can access the URL used for this solution [Automation script for SAP solutions using a BASTION & STORAGE setup deployment through Terraform and IBM Schematics](#).
- [Create an IAM service-to-service authorization for your VPN server and IBM Cloud Secrets Manager](#). This will allow the client-to-site VPN service to access and use the secrets created under the Secrets Manager instance.

Procedure

- From the IBM Cloud menu, select [Schematics](#).
- Click Create workspace.
- On the **Specify template** page:
 - Enter the URL of bastion setup folder.
 - Select the **Terraform version**.
 - Click Next.
- On the Workspace details page:
 - Enter a name for the workspace.
 - Select a **Resource group**.
 - Select a **Location** for your workspace. The workspace location does not have to match the resource location.
 - Select Next.
- Select **Create** to create your workspace.
- On the workspace **Settings** page, in the Input variables section, review the default input variables and provide values that match your solution:
 - Your API key
 - Your private SSH key from your local system.
 - The ID for the SSH key that you created and uploaded to IBM Cloud
 - The Region for your resources
 - The Zone for your resources
 - Whether to use an existing VPC or create one
 - Whether to use an existing subnet
 - Whether to create new port only when a new subnet is created
 - TCP port range, minimum and maximum
 - VPC name
 - Subnet name
 - Security group name
 - Hostname
 - Profile
 - Image
 - Minimal recommended disk sizes.
 - Click Save changes.
- On the workspace Settings page, click **Generate plan**. Wait for the plan to complete.
- Click **View log** to review the log files of your Terraform execution plan.
- Apply your Terraform template by clicking **Apply plan**.
- Review the log file to make sure that no errors occurred during the provisioning, modification, or deletion process.
- At the end of the log is information that you need to deploy different SAP products and databases. Copy and save this information for your deployments. For example:

```
$ 2024/09/16 12:01:08 Terraform refresh | FLOATING_IP = "xxx.xxx.xxx.xxx"
2024/09/16 12:01:08 Terraform refresh | HOSTNAME = "myhost"
2024/09/16 12:01:08 Terraform refresh | OVPN_FILE = "/root/OpenVPN.ovpn"
2024/09/16 12:01:08 Terraform refresh | PRIVATE_IP = "xxx.xxx.xxx.xxx"
```

```
2024/09/16 12:01:08 Terraform refresh | REGION = "eu-de"
2024/09/16 12:01:08 Terraform refresh | SECURITY_GROUP = "secgrp-myhost"
2024/09/16 12:01:08 Terraform refresh | SUBNET = [
2024/09/16 12:01:08 Terraform refresh |   "myvpc-subnet-1",
2024/09/16 12:01:08 Terraform refresh |   "myvpc-subnet-2",
2024/09/16 12:01:08 Terraform refresh |   "myvpc-subnet-3",
2024/09/16 12:01:08 Terraform refresh | VPC = "myvpc"
2024/09/16 12:01:08 Terraform refresh | VPN_HOSTNAME = "xxxxxx.eu-der vpn-server.appdomain.cloud"
```

12. Your OpenVPN client profile file is on the bastion server under `OVPN_FILE` path displayed in the output. Copy the file and share with the required users. Import this file in your OpenVPN client. Once the OpenVPN client connects, you are able to reach the private IP addressing space of the bastion server.



Note: This automation is offered at no cost; however, the provisioned infrastructure comes at cost.

Creating single-tier VPC for SAP

Terraform on IBM Cloud® enables predictable and consistent provisioning of IBM Cloud VPC infrastructure resources so that you can rapidly build complex, cloud environments. IBM Cloud VPC infrastructure consists of SAP certified hardware using Intel® Xeon CPUs and additional Intel® technologies.

For more information about Terraform on IBM Cloud®, see [Terraform on IBM Cloud getting started tutorial](#).

To create resources with Terraform, you use Terraform configuration files that describe the IBM Cloud resources that you need and how you want to configure them. Based on your configuration, Terraform creates an execution plan and describes the actions that need to be run to create the resources. You can review the execution plan, change it, or run the plan. When you change your configuration, Terraform on IBM Cloud can determine what changed and create incremental execution plans that you can apply to your existing IBM Cloud resources.

Script files

The configuration and script files are provided on the GitHub repository <https://github.com/IBM-Cloud/sap-infra-anydb-single/tree/main>.

For single-tier virtual private cloud on SAP, you modify the `input.auto.tfvars` file to customize the resources for your solution. You specify zones, resource names, and SSH keys.

All of the other configuration files are provided and do not need to be modified.

The IBM Cloud Provider plug-in for Terraform on IBM Cloud uses these configuration files to provision a VPC in your IBM Cloud account.

What is created

A VPC is a private space in IBM Cloud where you can run an isolated environment with custom network policies. The variables that you define are used by the scripts to provision the following virtual private cloud infrastructure resources for you:

- 1 VPC where you provision your virtual server instance
- 1 security group and rules for this security group to allow DNS and SSH connections to your virtual server instance and all outbound traffic
- 1 subnet to enable networking in your VPC
- 1 virtual server instance
- 2 storage volumes, 1 for swap and 1 for data

Support

There are no warranties of any kind, and there is no service or technical support available for these materials from IBM®. As a recommended practice, review carefully any materials that you download from this site before using them on a live system.

Though the materials provided herein are not supported by the IBM Service organization, your comments are welcomed by the developers, who reserve the right to revise, re-adapt or remove the materials at any time. To report a problem, or provide suggestions or comments, open a GitHub issue.

Before you begin

[Create or retrieve an IBM Cloud API key](#). The API key is used to authenticate with the IBM Cloud platform and to determine your permissions

for IBM Cloud services.

[Create or retrieve your SSH key ID](#). You need the 40-digit UUID for the SSH key, not the SSH key name.

Procedure

Use these steps to configure the IBM Cloud Provider Plug-in and use Terraform to create a VPC for SAP.

1. If you do not have Terraform installed, [Install the Terraform CLI and the IBM Cloud Provider plug-in](#).

If you are using Terraform 0.13 and higher, you do not need to install the IBM Cloud Provider Plug-in. You modify the configuration files provided on the single-tier VPC for SAP GitHub repository to specify the plug-in version to use.

If you are using Terraform 1.12.x and earlier, follow these IBM Cloud Provider Plug-in [installation instructions](#). Do not configure the plug-in.

Do not do any IBM Cloud Provider Plug-in configuration because those files are provided for you.

2. Create a project folder in the Terraform installation folder, and change directory to your project folder.

```
mkdir myproject && cd myproject
```

3. Copy the files from <https://github.com/IBM-Cloud/sap-infra-anydb-single/tree/main> to the project folder that you created in the Terraform installation directory.

4. Edit the `input.auto.tfvars` file to customize your solution. Modify the file to specify your zone, VPC component names, profile, and image. You need your 40-digit SSH key ID for this file. The second SSH key is optional. For more options for profile, see [Instance Profiles](#). For more options for image, see [Images](#).

```
$ ZONE      = "eu-de-1"
VPC        = "test-vpc"
SECURITYGROUP = "test-securitygroup"
SUBNET     = "test-subnet"
HOSTNAME   = "test-vsi"
PROFILE    = "bx2-4x16"
IMAGE      = "ibm-redhat-8-6-amd64-sap-applications-4"
SSH_KEYS  = [ "<SSH Key ID 1>" , "<SSH Key ID 2>" ]
SWAP      = "16"
VOL1      = "10"
```

5. Initialize the Terraform CLI.

```
$ terraform init
```

6. Create a Terraform execution plan. The Terraform execution plan summarizes all the actions that are done to create the VPC instance in your account.

```
$ terraform plan
```

7. Verify that the plan shows all of the resources that you want to create and that the names and values are correct. If the plan needs to be adjusted, edit the `input.auto.tfvars` file to correct resources and run `terraform plan` again.

8. Create the VPC for SAP instance and IAM access policy in IBM Cloud.

```
$ terraform apply
```

The VPC and components are created and you see output similar to the terraform plan output.



Note: This automation is offered at no cost; however, the provisioned infrastructure comes at cost.

Next steps

If you need to rename your resources after they are created, modify the `input.auto.tfvars` file to change the names and run `terraform plan` and `terraform apply` again. Do not use the IBM Cloud Dashboard and user interface to modify your VPC after it is created. The Terraform scripts create a complete solution and selectively modifying resources with the user interface might cause unexpected results.

If you need to remove your VPC, go to your project folder and run `terraform destroy`.

Deploying SAP AnyDB (non-SAP HANA) 2-tier and 3-tier distributed architecture on IBM Cloud® VPC (Terraform)

Terraform on IBM Cloud® enables predictable and consistent provisioning of IBM Cloud VPC infrastructure resources so that you can rapidly build complex, cloud environments. IBM Cloud VPC infrastructure consists of SAP certified hardware using Intel Xeon CPUs and additional Intel technologies.

For more information about Terraform on IBM Cloud, see [Terraform on IBM Cloud getting started tutorial](#).

To create resources with Terraform, you use Terraform configuration files that describe the IBM Cloud resources that you need and how you want to configure them. Based on your configuration, Terraform creates an execution plan and describes the actions that need to be run to create the resources. You can review the execution plan, change it, or run the plan. When you change your configuration, Terraform on IBM Cloud can determine what changed and create incremental execution plans that you can apply to your existing IBM Cloud resources.

Script files

The configuration and script files are provided on the GitHub repository <https://github.com/IBM-Cloud/sap-infra-anydb-distributed>.

For 2-tier and 3-tier VPC for SAP, you modify the `input.auto.tfvars` file to customize the resources for your solution. You specify zones, resource names, and SSH keys.

All of the other configuration files are provided and do not need to be modified.

The IBM Cloud Provider plug-in for Terraform on IBM Cloud uses these configuration files to provision a VPC in your IBM Cloud account.

What is created

A VPC is a private space in IBM Cloud where you can run an isolated environment with custom network policies. The variables that you define are used by the scripts to provision the following VPC infrastructure resources for you:

- 1 VPC where you provision your virtual server instance.
- 1 security group and rules for this security group to allow DNS and SSH connections to your virtual server instance and all outbound traffic.
- 1 subnet to enable networking in your VPC.
- 2 virtual server instances (1 SAP App VSI and 1 DB(anydb) instance server VSI).
- 2 storage volumes, 1 for swap and 1 for data for SAP app VSI and 4 storage 1 x SWAP and 3 x DATA volumes for DB VSI.

The VSIs are configured with Red Hat Enterprise Linux 8.x for SAP Applications (amd64) and Suse Enterprise Linux 15 (amd64) and they have at least one SSH key that are configured to access as root user. The VSIs have the following storage volumes:

DB virtual server instance disks: • 1x 40 GB disk with 10 IOPS / GB - SWAP • 1 x 32 GB disk with 10 IOPS / GB - DATA (DB LOG) • 1x 64 GB disk with 10 IOPS / GB - DATA (DB ARCHIVE LOG) • 1 x 128/256 GB disk with 10 IOPS / GB – DATA

SAP app virtual server instance disks: • 1x 40 GB disk with 10 IOPS / GB - SWAP • 1 x 128 GB disk with 10 IOPS / GB – DATA

Support

There are no warranties of any kind, and there is no service or technical support available for these materials from IBM®. As a recommended practice, review carefully any materials that you download from this site before using them on a live system.

Though the materials provided herein are not supported by the IBM Service organization, your comments are welcomed by the developers, who reserve the right to revise, re-adapt or remove the materials at any time. To report a problem, or provide suggestions or comments, open a GitHub issue.

Before you begin

1. If you do not have Terraform installed, [Install the Terraform CLI and the IBM Cloud Provider plug-in](#).

If you are using Terraform 0.13 and higher, you do not need to install the IBM Cloud Provider Plug-in. You modify the configuration files provided on the 1-Tier VPC for SAP GitHub repository to specify the plug-in version to use.

If you are using Terraform 1.12.x and earlier, follow these IBM Cloud Provider Plug-in [installation instructions](#). Do not configure the plug-

in.

Do not do any IBM Cloud Provider Plug-in configuration because those files are provided for you.

2. [Create or retrieve an IBM Cloud API key](#). The API key is used to authenticate with the IBM Cloud platform and to determine your permissions for IBM Cloud services.
3. [Create or retrieve your SSH key ID](#). You need the 40-digit UUID for the SSH key, not the SSH key name.

Procedure

Use these steps to configure the IBM Cloud Provider Plug-in and use Terraform to create a VPC for SAP.

1. Create a project folder in the Terraform installation folder, and change directory to your project folder.

```
mkdir myproject && cd myproject
```

2. Copy the files from <https://github.com/IBM-Cloud/sap-infra-anydb-distributed/tree/main> to the project folder that you created in the Terraform installation directory.
3. Edit the `input.auto.tfvars` file to customize your solution. Modify the file to specify your VPC name, subnet, security group, hostname, profile, image, SSH keys, and disk sizes. You must modify:

- VPC - Unique VPC name.
- SECURITYGROUP - Change ic4sap to the VPC name.
- SUBNET - Change ic4sap to the VPC name.
- DB/APP HOSTNAME - Enter a hostname up to 13 characters. For more information, see the README file.

For disk sizes, volumes are created with the required size and are attached to the VSIs. The size for the volumes is defined as a list in the VOLUME_SIZES variable with each value specifying capacity for a volume in GB.

You need your 40-digit SSH key ID for this file. The second SSH key is optional.

For more options for profile, see [Instance Profiles](#). For more options for image, see [Images](#).

```
# General VPC variables:  
REGION      = "eu-de" # default value  
ZONE        = "eu-de-2" # default value  
VPC         = "ic4sap"  
SECURITYGROUP = "ic4sap-securitygroup"  
SUBNET       = "ic4sap-subnet"  
SSH_KEYS     = [ "r010-57bf315-f9e5-46bf-bf61-d87a24a9ce7a" , "r010-3fc9fe7-d4a7-41ce-8bb3-d96e936b2c7e" ]  
DB_PROFILE   = "bx2-4x16"  
APP_PROFILE  = "bx2-4x16"  
DB_IMAGE     = "ibm-redhat-8-6-amd64-sap-applications-4"  
APP_IMAGE    = "ibm-redhat-8-6-amd64-sap-applications-4"  
  
# SAP Database VSI variables:  
DB_HOSTNAME = "ep12db"  
DB_VOLUME_SIZES = [ "40" , "32" , "64" , "128" ]  
  
# SAP APPS VSI variables:  
APP_HOSTNAME = "ep12app" # default value  
APP_VOLUME_SIZES= [ "40" , "128" ]
```

Parameter	Description
REGION	The cloud region where the solution is deployed. The regions and zones for VPC are listed here .
ZONE	The cloud zone where the solution is deployed.
VPC	The name of the VPC. The list of VPCs is available here .
SECURITYGROUP	The name of the Security Group. The list of Security Groups is available here

SUBNET	The name of the Subnet. The list of Subnets is available here
DB_PROFILE	The profile used for the VSI. A list of profiles is available here.
APP_PROFILE	The profile used for the VSI. A list of profiles is available here.
DB_IMAGE	The OS image used for the VSI. A list of images is available here .
APP_IMAGE	The OS image used for the VSI. A list of images is available here .
SSH_KEYS	List of SSH Keys IDs that are allowed to SSH as root to the VSI. Can contain one or more IDs. The list of SSH Keys is available here .
[DB/APP]_HOSTNAME	The hostname for the VSI. The hostname must have up to 13 characters as required by SAP. For more information about rules regarding hostnames for SAP systems, see SAP Note 611361 - Hostnames of SAP ABAP Platform servers .

4. Initialize the Terraform CLI.

```
$ terraform init
```

5. Create a Terraform execution plan. The Terraform execution plan summarizes all the actions that are done to create the VPC instance in your account.

```
$ terraform init
```

6. Verify that the plan shows all of the resources that you want to create and that the names and values are correct. If the plan needs to be adjusted, edit the `input.auto.tfvars` file to correct resources and run `terraform plan` again.

7. Create the VPC for SAP instance and IAM access policy in IBM Cloud.

```
$ terraform apply
```

The VPC and components are created and you see output similar to the terraform plan output.



Note: This automation is offered at no cost; however, the provisioned infrastructure comes at cost.

Next steps

If you need to rename your resources after they are created, modify the `input.auto.tfvars` file to change the names and run `terraform plan` and `terraform apply` again. Do not use the IBM Cloud Dashboard and user interface to modify your VPC after it is created. The Terraform scripts create a complete solution and selectively modifying resources with the user interface might cause unexpected results.

If you need to remove your VPC, go to your project folder and run `terraform destroy`.

SAP NetWeaver and Db2 2-tier in VPC

Automating SAP workload HA deployment on IBM Cloud VPC with Terraform and Ansible

You can use Terraform to automate IBM Cloud® VPC provisioning. The VPC provisioned includes virtual server instances with high network performance. The VPC infrastructure contains various Infrastructure-as-a-Service (IaaS) offerings, including virtual servers. After the VPC is provisioned, the scripts use the Ansible Playbooks to install the SAP system.

IBM Cloud VPC introduction

VPC is a public cloud offering that an enterprise uses to establish its own private cloud-like computing environment on shared [public cloud](#) infrastructure. VPC gives an enterprise the ability to define and control a virtual network that is logically isolated from all other public cloud tenants, creating a private and secure place on the public cloud.

Imagine that a cloud provider's infrastructure is a residential apartment building and multiple families live inside. A public cloud tenant is a kind of sharing an apartment with a few roommates. In contrast, having a VPC is like having your own private condominium; no one else has the key, and no one can enter the space without your permission.

VPC's logical isolation is implemented by using virtual network functions and security features that give the enterprise customer granular control over which IP addresses or applications can access particular resources. It is analogous to the "friends-only" or "public/private" controls on social media accounts used to restrict who can or can't see your otherwise public posts.

With IBM Cloud VPC, you can use the UI, CLI, and API to manually provision virtual server instances for VPC with high network performance. VPC infrastructure contains various Infrastructure-as-a-Service (IaaS) offerings including virtual servers for VPC.

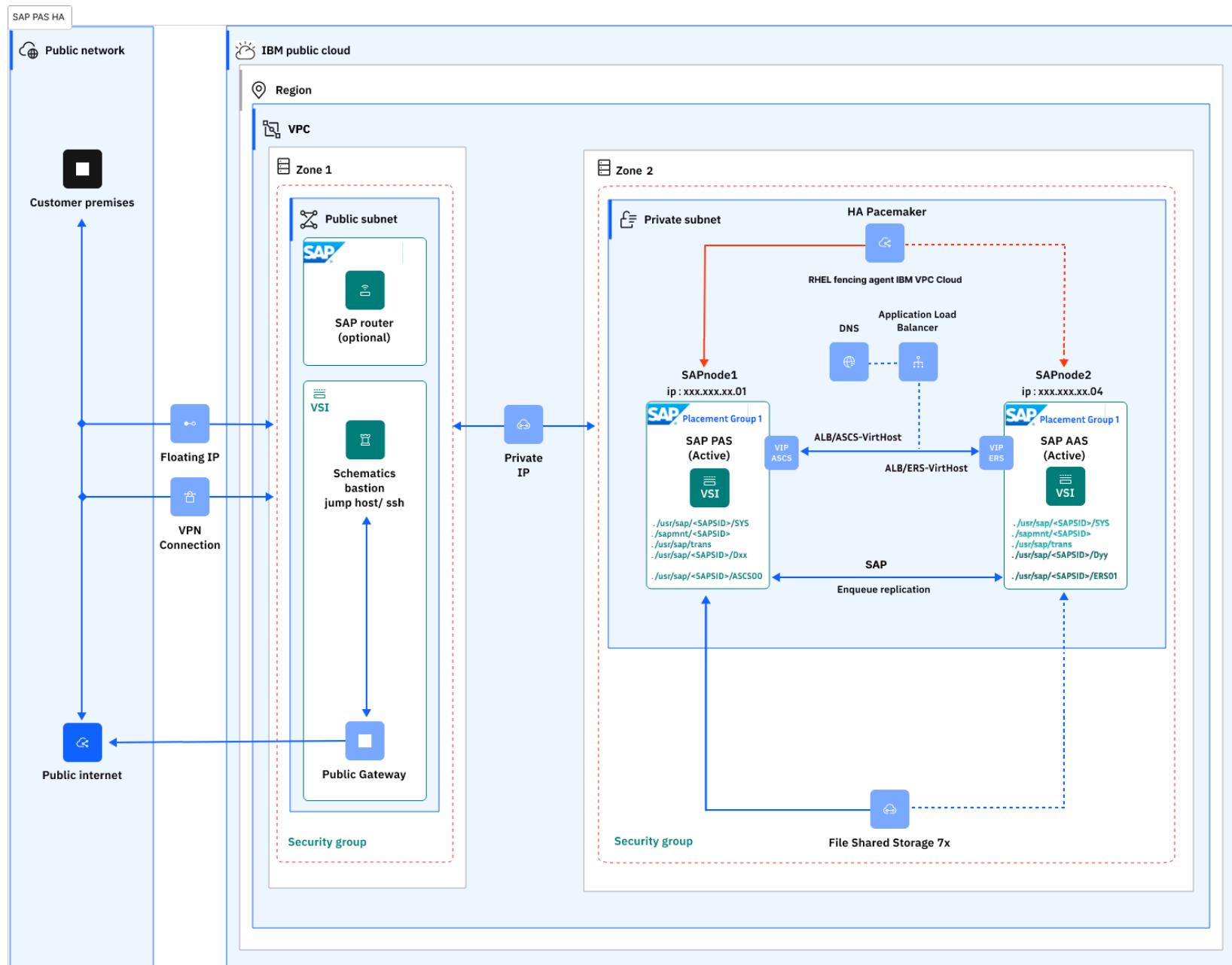
Use the following information to understand a simple use-case for planning, creating, and configuring resources for your VPC, and learn more about VPC overviews and VPC tutorials. For more information about the VPC, see [Getting started with Virtual Private Cloud \(VPC\)](#).

SAP products architecture on IBM Cloud VPC

A [Virtual Private Cloud \(VPC\)](#) contains one of the most secure and reliable cloud environments for SAP applications within your own VPC with virtual server instances. This represents an Infrastructure-as-a-Service (IaaS){: external} within IBM Cloud that offers all the benefits of isolated, secure, and flexible virtual cloud infrastructure from IBM. In comparison, the IBM Cloud classic infrastructure virtual servers offering uses virtual instances with native and VLAN networking to communicate with each other within a data center; however, the instances are restricted in one well-working pod by using subnet and VLAN networking as a gap scale up of virtual resources should rely between the pods. The IBM Cloud VPC network orchestrator layer concept eliminates the pod boundaries and restrictions, so this new concept handles all the networking for every virtual instance running within VPC across regions and zones.

Highly available system for SAP NetWeaver on IBM Cloud VPC

In a Highly Available (HA) system, every instance can run on a separate IBM Cloud virtual server instance. The cluster HA configuration for the SAP application server consists of two virtual server instances, each of them located in the same zone within the region by using placement groups. Placement groups assure that both cluster resources and cloud resources are also located in different compute nodes as specified in the following placement groups section:



SAP HA for SAP applications cluster nodes PAS (Active) and AAS (Active)

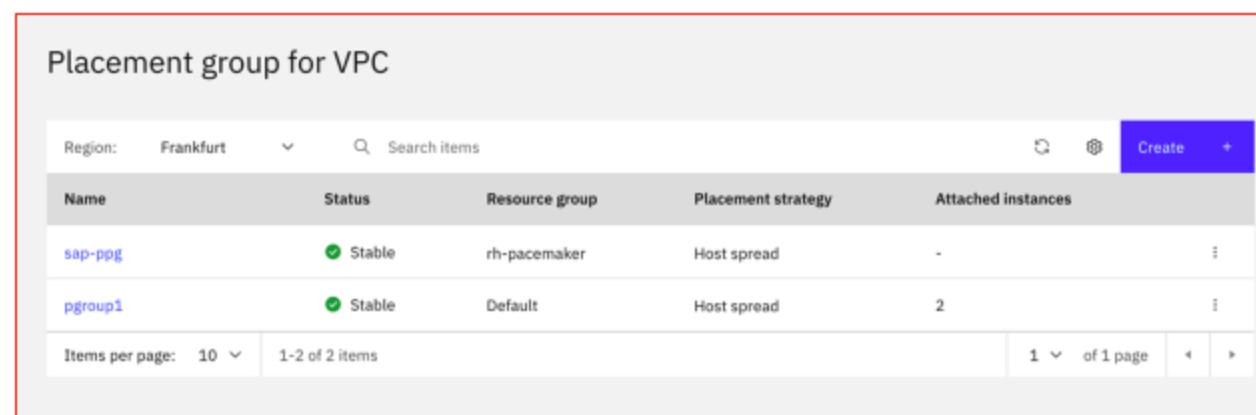
Placement groups on IBM Cloud VPC for SAP HA architecture

Placement Groups (PG) for VPC have two different anti-affinity strategies for high availability. By using the placement strategies, you minimize the chance of service disruption with virtual server instances that are placed on different hosts or into an infrastructure with separate power and network supplies.

The design of placement groups for IBM Cloud virtual servers solves this issue. Placement groups give a measure of control over the host on which a new public virtual server is placed. In this release, a “spread” rule is implemented, which means that the virtual servers within a placement group are spread onto different hosts. You can build a highly available application within a data center and know that your virtual servers are isolated from each other.

Placement groups with the spread rule are available to create in selected IBM Cloud data centers. After a spread rule is created, you can provision a virtual server into that group and ensure that it is not on the same host as any of your other virtual servers. This feature comes with no cost.

You can create your placement group and assign up to four new virtual server instances. With the spread rule, each of your virtual servers are provisioned on different physical hosts. In the following configuration example, the “Power Spread” option is used:



Placement groups host spread

Placement group for VPC					
Name	Status	Resource group	Placement strategy	Attached instances	
sapha-poc	Stable	wes-ic4sap-resourcegroup	Power spread	4	⋮
Items per page: 10 1 item 1 of 1 page ⋮					

Placement groups power spread

Following are the SAP instances that are required for HA scenario:

- ABAP SAP Central Services (ASCS) instance - contains the ABAP message server and the ABAP enqueue server.
- Enqueue Replication Server (ERS) instance for the ASCS instance.
- Database instance
- Primary Application Server (PAS) instance on node 1.
- Additional Application Server (AAS) instance on node 2.



Note: It is recommended to run both the ASCS instance and the ERS instance in a switchover cluster infrastructure.

IBM Cloud File Storage for VPC for SAP HA architecture

[IBM Cloud File Storage for VPC](#) technology is used to make the SAP directories available to the SAP system. The technologies of choice are NFS, shared disks, and cluster file system. If you have decided to use the HA solution for your SAP system, make sure that you properly address the HA requirements of the SAP file systems in your SAP environment.

File shares for VPC								
Name	Status	Resource groups	Location	Mount targets	Size	Replication role	Encryption type	
usrsap-as1-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	⋮
usrsap-as2-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	⋮
usrsap-sapscs-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	⋮
usrsap-sapers-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	⋮
usrsap-sapmnt-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	⋮
usrsap-sapsys-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	⋮
usrsap-trans-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	80 GB	None	Provider managed	⋮

File shares for VPC

- File shares that are mounted as NFS permanent file systems on both cluster nodes for SAP HA application:
 - `/usr/sap/<SAPSID>/SYS`
 - `/sapmnt<SAPSID>`
 - `/usr/sap/trans`
- Cluster-managed file systems for SAP HA application: ASCS
 - `/usr/sap/<SAPSID>/ASCS00`
 - `/usr/sap/<SAPSID>/ERS01`
- Permanent NFS mount on SAP HA application node 1 PAS instance:
 - `/usr/sap/<SAPSID>/Dxx`
- Permanent NFS mount on SAP HA application node 2 dialog instance:
 - `/usr/sap/<SAPSID>/Dyy`

Prerequisites

You need to install the hardware (hosts, disks, and network) and decide how to distribute the database, SAP instances, and if required, the Network File System (NFS) server over the cluster nodes.

Context

Following are the types of SAP directories:

- Physically shared directories: `/<sapmnt>/<SAPSID>` and `/usr/sap/trans`

- Logically shared directories that are bound to a node, such as `/usr/sap`, with the following local directories:
 - `/usr/sap/<SAPSID>`
 - `/usr/sap/<SAPSID>/SYS`
 - `/usr/sap/hostctrl`
- Local directories that contain the SAP instances such as `/usr/sap/<SAPSID>/ASCS<Instance_Number>`
- The global transport directory may reside on a separate SAP transport host as a standard three systems transport layer configuration.

You need at least two nodes and a shared file system for distributed ASCS and ERS instances. The assumption is that the rest of the components are distributed on other nodes.

ASCS and ERS installation

In order for the ASCS and ERS instances to be able to move from one node to the other, they need to be installed on a shared file system and use virtual hostnames based on the virtual IP.

In this VPC-based SAP HA solution, the shared file system that is required by the cluster is replaced by the NFS-mounted file storage, and the virtual IP is replaced by the Application Load Balancer for VPC (ALB).

In this scenario, three ALBs are used, one for each Single Point of Failure (SPOF) component in order to replace the virtual IP requirement: ALB for ASCS, ALB for ERS, and ALB for ASE Sybase. Each ALB is configured as a backend for the corresponding cluster servers and redirects all of the communication that is received on the front-end ports to the active server in the backend pool.

Load balancers for VPC						
Region:	Frankfurt	▼	<input type="text"/> poc	X		
Name	Status	Family	Resource group	Type	Hostname	Location
db-alb-hana-poc	Active	Application	wes-ic4sap-resourcegroup	Private	20bdd130-eu-de.lb.appdomain.cloud	Frankfurt
sap-alb-ers-poc	Active	Application	wes-ic4sap-resourcegroup	Private	3941d983-eu-de.lb.appdomain.cloud	Frankfurt
sap-alb-ascs-poc	Active	Application	wes-ic4sap-resourcegroup	Private	56a9190d-eu-de.lb.appdomain.cloud	Frankfurt

Application load balancer management of HA IPs mechanism

Private application load balancer

A [private application load balancer](#) is accessible through your private subnets that you configured to create the load balancer.

Similar to a public application load balancer, your private application load balancer service instance is assigned an FQDN; however, this domain name is registered with one or more private IP addresses.

IBM Cloud operations change the number and value of your assigned private IP addresses over time, based on maintenance and scaling activities. The backend virtual server instances that host your application must run in the same region and under the same VPC.

Use the assigned ALB FQDN to send traffic to the private application load balancer to avoid connectivity problems to your applications during system maintenance or scaling down activities.

Each ALB sends traffic to the cluster node where the application (ASCS, ERS, ASE Sybase DB) is running. During the cluster failover, the ALB redirects all the traffic to the new node where the resources are up and running.



Note: DNS-as-a-Service (DNSaaS) is the management IBM Cloud VPC DNS service of HA and FQDN (IPs) mechanism.



Note: The ALB has a default of 50 seconds for client and server timeout, so after 50 seconds of inactivity, the connection is closed. To support SAP connections through ALB and not lose connection after 50 seconds, you need to request a change this value to a minimum of 300 seconds (client-side idle connection = minimum 300s and server-side idle connection = minimum 300s). To request this change, open a support ticket. This is an account-wide change that affects all of the ALBs in your account. For more information, see [Connection timeouts](#).

DNS Services with VPC

[IBM Cloud DNS Services](#) provide private DNS to VPC users. Private DNS zones are resolvable only on IBM Cloud and from explicitly [permitted networks](#) in an account. To get started, create a DNS Services instance by using the IBM Cloud console.

DNS Services allows you to:

- Create the private DNS zones that are collections for holding the domain names.
- Create the DNS resource records under these DNS zones.
- Specify the access controls used for the DNS resolution of resource records on a zone-wide level.

DNS Services also maintains its own worldwide set of DNS resolvers. Instances that are provisioned under IBM Cloud on an IBM Cloud network can use resource records that are configured through IBM Cloud DNS Services by querying DNS Services resolvers.

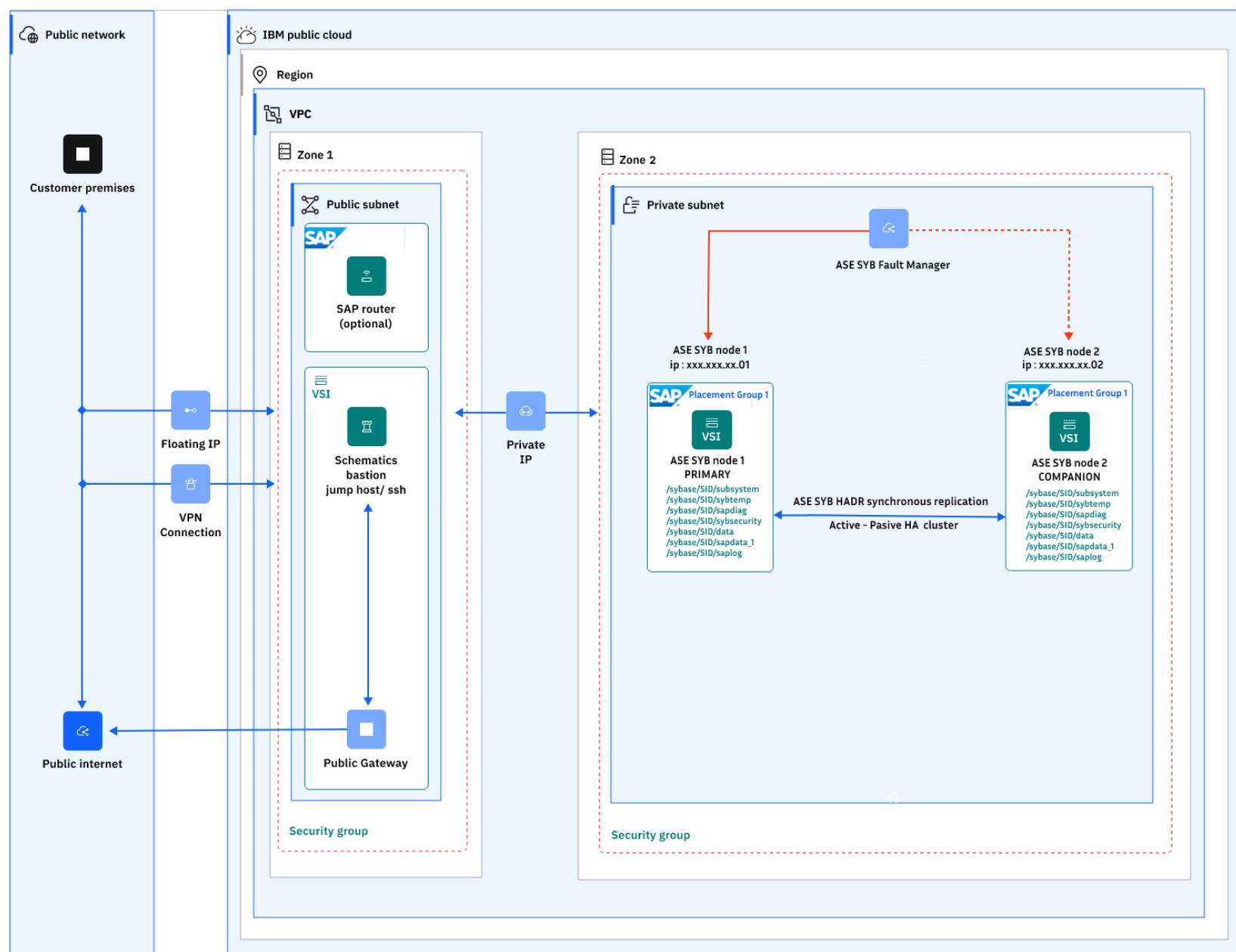
Resource records and zones that are configured through DNS Services are:

- Separated from the wider public DNS, and their publicly accessible records.
- Hidden from the system outside of and not part of the IBM Cloud private network.
- Accessible only from the system that you authorize on the IBM Cloud private network.
- Resolvable only via the resolvers provided by the service.

The DNS service maps the FQDN of each ALB to the virtual hostnames of the ASCS, ERS, and ASE Sybase that are used by SAP applications.

Type	Name	Value	TTL
CNAME	dbpochana	is an alias of 20bdd130-eu-de.lb.appdomain.cloud	12 hr
CNAME	sappocers	is an alias of 3941d983-eu-de.lb.appdomain.cloud	12 hr
CNAME	sappocases	is an alias of 56a9190d-eu-de.lb.appdomain.cloud	12 hr

Highly available system for SAP ASE Sybase database with HADR system



SAP HA for ASE Sybase DB instances cluster nodes primary (Active) and Secondary (Companion)

At the most basic level, a standard HA ASE Sybase cluster in an active(primary)-passive(companion) configuration has two nodes: one is the primary node and the other is the standby node. This means that the primary node is actively serving the active SAP DB instances (Primary and Companion), while the standby node is waiting to jump in if there is any failure.

The cluster is set with a virtual hostname IP (hostname is mapped to the FQDN of the ASE Sybase ALB through DNS, which is the same as

explained previously for SAP ASCS and ERS instances). Application instances (PAS and AAS) are used on the SAP profiles to call that particular component. The cluster assigns the virtual IP to the active node and uses a heartbeat monitor to confirm the availability of the components. If the primary node stops responding, it triggers the automatic failover mechanism that calls the standby node to step up to become the primary node. The ALB detects the change, redirects the traffic to the new active node, and assigns the virtual IP to it, restoring the component availability. Once fixed, the failed node comes online as a standby node.

SAP Sybase HADR system supports synchronous replication

The SAP Sybase HADR system supports synchronous replication between the primary and standby servers for high availability. An active-active setup is a two-node configuration where both nodes in the cluster include SAP ASE managing independent workloads, capable of taking over each others workload in the event of a failure.

The SAP ASE server that takes over the workload is called a secondary companion, and the SAP ASE server that fails is called the primary companion. Together they are companion servers. This movement from one node to another is called failover. After the primary companion is ready to resume its workload, it is moved back to its original node. This movement is called a failback.

When a system fails over, clients that are connected to the primary companion and use the failover property automatically reestablish their network connections to the secondary companion. You must tune your operating system to successfully manage both servers during fail over. See your operating system documentation for information about configuring your system for high availability. An SAP ASE configured for failover in an active-active setup can be shut down using the shutdown command only after you have suspended SAP ASE from the companion configuration, at both the server level and the platform level.

The always-on option in a High Availability and Disaster Recovery (HADR) system consists of two SAP ASE servers:

- Primary on which all transaction processing takes place.
- Warm standby (referred to as a "standby server" in DR mode, and as a "companion" in HA mode) for the primary server, and contains copies of designated databases from the primary server.



Note: The HADR feature that is shipped with SAP ASE version 16.0 SP02 supports only a single-companion server.

Some high-availability solutions (for example, the SAP Adaptive Server Enterprise Cluster Edition) share or use common resources between nodes. However, the HADR system is a "shared nothing" configuration, each node has separate resources including disks.

In an HADR system, servers are separate entities and data is replicated from the primary server to the companion server. If the primary server fails, a companion server is promoted to the role of primary server either manually or automatically. Once the promotion is complete, clients can reconnect to the new primary server, and see all committed data, including data that was committed on the previous primary server.

Servers can be separated geographically, which makes an HADR system capable of withstanding the loss of an entire computing facility.



Note: The HADR system includes an embedded SAP Replication Server, which synchronizes the databases between the primary and companion servers. SAP ASE uses the Replication Management Agent (RMA) to communicate with Replication Server and SAP Replication Server uses Open Client connectivity to communicate with the companion SAP ASE.

The Replication Agent detects any data changes made on the primary server and sends them to the primary SAP Replication Server. In the figure above, the unidirectional arrows indicate that, although both SAP Replication Servers are configured, only one direction is enabled at a time.

The HADR system supports synchronous replication between the primary and standby servers for high availability so the two servers can keep in sync with Zero Data Loss (ZDL). This requires a network link that is fast enough between the primary and standby server so that synchronous replication can keep up with the primary servers workload. Generally, this means that the network latency is approximately the same speed as the local disk IO speed, a few (fewer than 10) milliseconds. Anything longer than a few milliseconds may result in a slower response to write operations at the primary.

The HADR system supports asynchronous replication between the primary and standby servers for disaster recovery. The primary and standby servers by using asynchronous replication can be geographically distant, meaning they can have a slower network link. With asynchronous replication, Replication Agent Thread captures the primary servers workload, which is delivered asynchronously to SAP Replication Server. The SAP Replication Server applies these workload change to the companion server.

The most fundamental service that is offered by the HADR system is the failover; planned or unplanned from the primary to the companion server, which allows maintenance activity to occur on the old primary server, while applications continue on the new primary.

The HADR system provides protection in the event of a disaster. If the primary server is lost, the companion server can be used as a replacement. Client applications can switch to the companion server, and the companion server is quickly available for users. If the SAP Replication Server was in synchronous mode before the failure of the primary server, the Fault Manager automatically initiates failover with

zero data loss.

Fault Manager installation on the SAP ASCS node

The required parameters are asked during the installation process to create a profile for the fault manager and then adds it to the instance start profile. It is also possible to run the installation by using an existing profile: `sybdbfm install pf=<SYBHA.PFL>` In this case, the installation process will only ask for profile parameters missing in the profile.



Note: Fault manger is integrated with ASCS on same SAP PAS/AAS cluster (start/stop/move together).

There may be some data loss if the SAP Replication Server was in asynchronous mode and you must use manual intervention to failover for disaster recovery.

Connection attempts to the companion server without the necessary privileges are silently redirected to the primary companion via the login redirection mechanism, which is supported by Connectivity libraries. If login redirection is not enabled, client connections fail and are disconnected.

The SAP ASE HADR option installs the below components:

- SAP ASE
- SAP Replication Server
- Replication Management Agent (RMA)
- SAP Host Agent
- Fault Manager
- SAP ASE Cockpit



Note: This automation is offered at no cost; however, the provisioned infrastructure comes at cost.

VPC with Additional Application Server (AAS) ABAP on Linux for SAP HANA

You can use Terraform scripts to create a single-tier VPC and create the AAS to HANA and AnyDB infrastructure on the VPC. The Terraform scripts use the VPC information that you provide and then call the Ansible playbook to create the SAP architecture on the specified VPC. Terraform on IBM Cloud® enables predictable and consistent provisioning of IBM Cloud Virtual Private Cloud (VPC) infrastructure resources so that you can rapidly build complex, cloud environments. IBM Cloud VPC infrastructure consists of SAP certified hardware that uses Intel® Xeon CPUs and more Intel® technologies.

You have two deployment methods to choose from:

- Terraform scripts that run from the CLI on your bastion server.
- Schematics user interface accessed from your cloud dashboard menu.

You can create SAP AAS NetWeaver 7.x on the SAP HANA-based ABAP stack.

SAP solution implemented

Many SAP enterprise solutions are built on the SAP platform (SAP NetWeaver) including:

- SAP HANA as Primary Persistence for SAP NetWeaver-based applications
- SAP Business Suite applications (ERP, CRM, and SCM, and other applications),
- SAP Business Warehouse (BW), and
- Other SAP enterprise solutions

SAP NetWeaver has two distinct aspects, ABAP and Java. Many applications that are built on the SAP NetWeaver's ABAP or Java (or both) application servers run on SAP DB owned HANA and ASE Sybase either in AnyDB platforms (MSSQL, Oracle, and Db2).

Technical interfaces are available for applications that are built on the SAP NetWeaver AS ABAP and AS Java to run on SAP HANA and AnyDB. However, specific development enablement is normally required for each application to ensure that it runs optimally on the SAP HANA. SAP Business Suite applications (ERP, CRM, SCM, and other applications), SAP Business Warehouse (BW), and other SAP NetWeaver-based applications were modified to run on SAP HANA and have many advantages. Also, various components and complimentary applications that are built on SAP NetWeaver can also run on SAP HANA or AnyDB by using the provided SAP NetWeaver DB interfaces.

The SAP HANA as primary persistence for SAP NetWeaver-based applications scenario has one restriction: SAP NetWeaver ABAP and Java

application servers must run on separate hardware servers from the SAP HANA hardware.

What is created

The scripts automate the virtual infrastructure resources, provisioning the processes for the SAP architecture in an existing VPC with a distributed environment. SAP AAS NetWeaver 7.x (HANA or ASE SYB) application server on a distinct VSI VPC system and SAP HANA DB on a dedicated server type VSI VPC box are provisioned. The scripts work in two phases.

During the first phase of [Automate SAP bastion server – SAP media storage repository](#), the following virtual infrastructure resources based on the components from the existing VPC created by the bastion server are:

- 1 VPC where the virtual server instance is provisioned.
- 1 security group. The rules for this security group are:
 - Allow inbound DNS traffic (port 53).
 - Allow inbound SSH traffic (TCP port 22).
 - Allow all outbound traffic from the virtual server instance.
 - Allow all traffic in the security group.
- 1 subnet to enable the networking in your VPC.
- 2 virtual server instances with SAP certified storage and network configurations.
- 1 floating IP address used to access your VPC virtual server instance over the public network.

During the second phase, the Ansible Playbooks is called and the SAP architecture is installed for both dedicated virtual server instance (VSI) SAP application; VSI system and dedicated SAP HANA VSI box. The SAP architecture that is deployed on the SAP NetWeaver 7.x release is a stand-alone dedicated SAP HANA 2.0 box release. For more information about this architecture, see [Automating SAP HANA stand-alone virtual server instance on IBM Cloud® VPC by using Terraform and Ansible](#).

You can provision only one instance of the service per IBM Cloud region.

Schematics deployment

When you run the scripts with the Schematics interface, you:

- Enter the workspace information.
- Enter the GitHub path for the chosen solution either on NetWeaver AAS for HANA.
- Modify the parameters in the Schematics interface. They are the same parameters as the `input.auto.tfvars` file that you use with the cli.

Virtual server instance configuration

Following are the supported operating system images for SAP NetWeaver primary application server:

- ibm-redhat-8-4-amd64-sap-applications-2
- ibm-redhat-8-6-amd64-sap-applications-2
- ibm-sles-15-3-amd64-sap-applications-2
- ibm-sles-15-4-amd64-sap-applications-3

Following are the supported operating system images for SAP HANA database:

- ibm-redhat-8-4-amd64-sap-hana-2
- ibm-redhat-8-6-amd64-sap-hana-2
- ibm-sles-15-3-amd64-sap-hana-2
- ibm-sles-15-4-amd64-sap-hana-1

For both server instances there are:

- Two SSH keys are configured to access SSH as `root`.
- Three storage volumes as described in the `input.auto.tfvars` file.

What is created for anydb

The scripts use the information that you provide for an existing VPC and deploy AAS to SAP HANA or AnyDB on a different host than CI (SAP Central Instance) VSI host. For more information about this architecture, see [SAP NetWeaver 7.x on UNIX with HANA or AnyDB on IBM Cloud](#)

[VPC on IBM Cloud VPC](#). You specify the information for the VPC to use in the `input.auto.tfvars` file.

The scripts call the Ansible Playbooks to install the SAP architecture.

Script files

The configuration and script files are provided on GitHub. Each supported interface for the SAP solution installation has its own folder in the GitHub repository:

- [GitHub repository for Terraform – AAS HANA](#)

Terraform interface

To run the Terraform script, you modify:

- The `input.auto.tfvars` file to specify the existing VPC resources for your solution. Specify the variables for the existing VPC:
 - VPC name
 - Security group
 - Subnet
 - Hostname
 - Profile
 - Image
 - Up to two SSH keys

You can change the default SAP system configuration settings to match your solution. You can also specify the location where you downloaded the SAP kits.

The IBM Cloud Provider plug-in for Terraform on IBM Cloud uses these configuration files to install AAS to SAP HANA and AnyDB on the specified VPC in your IBM Cloud account.

Support

There are no warranties of any kind, and there is no service or technical support available for these materials from IBM®. As a recommended practice, review carefully any materials that you download from this site before using them on a live system.

Though the materials provided herein are not supported by the IBM® Service organization, your comments are welcomed by the developers, who reserve the right to revise, readapt or remove the materials at any time. To report a problem, or provide suggestions or comments, open a GitHub issue.

Before you begin

Before you use the scripts in the bastion cli:

- Set up your account to access the VPC. Make sure that your account is [upgraded to a paid account](#).
- If you have not already, create a Bastion server to store the SAP kits. For more information, see [Automate SAP bastion server - SAP media storage repository](#).
- Download the SAP kits from the SAP Portal to your Deployment Server. Make note of the download locations. Ansible decompresses the files. For more information, see the [readme](#) file.
- [Create or retrieve an IBM Cloud API key](#). The API key is used to authenticate with the IBM Cloud platform and to determine your permissions for IBM Cloud services.
- [Create or retrieve your SSH key ID](#). You need the 40-digit UUID for the SSH key, not the SSH key name.
- Terraform should already be installed on the bastion server that you deployed. For more information, see [Bastion server for SAP deployment](#).
- (Optional - Catalog Tile) create secrets for your credentials and passwords by using the [Secrets Manager](#).

Deploying SAP AAS NetWeaver 7.x on HANA by using the Schematics user interface

Use these steps to configure the SAP Additional Application Server (AAS) NetWeaver with HANA or AnyDB on your existing VPC by using the Schematics interface. The script takes 2 - 3 hours to complete.

1. From the IBM Cloud menu, select **Schematics**.
2. Click **Create** workspace.

3. On the **Specify template** page:
 - Enter the URL for the Schematics interface.
 - Select the **Terraform version** that is listed in the readme file.
 - Click **Next**.
4. On the **workspace details** page:
 - Enter a name for the workspace.
 - Select a **Resource group**.
 - Select a **Location** for your workspace. The workspace location does not have to match the resource location.
 - Select **Next**.
5. Select **Create** to create your workspace.
6. On the workspace settings page, in the input variables section, review the default input variables and provide values that match your solution.
 For a more detailed description of each parameter, check the GitHub repo [AAS HANA readme](#) file, chapter "Input parameter file". Also, make sure to mark the parameters that contain sensitive information like passwords, API, and ssh private keys as "sensitive". These parameters are marked as "sensitive" in the readme file, under "Input parameter file".
7. On the workspace settings page, click **Generate plan**. Wait for the plan to complete.
8. Click **View log** to review the log files of your terraform execution plan.
9. Apply your Terraform template by clicking **Apply plan**.
10. Review the log file to ensure that no errors occur during the provisioning, modification, or deletion process.

Deploying SAP AAS NetWeaver (ABAP) on HANA with the Deployable Architecture tile interface

Use these steps to configure the SAP AAS NetWeaver (ABAP) on HANA on your existing VPC by using the catalog tile interface. The script takes 2 - 3 hours to complete.

1. From the IBM Cloud catalog, select **VPC with Additional Application Server ABAP on Linux for SAP HANA** on HANA tile. The **Create** tab opens for VPC with Additional Application Server ABAP on Linux for SAP HANA. For more information about this deployment, see the About tab or the readme file link.
2. Select the latest version.
3. Select **VPC with Additional Application Server ABAP on Linux for SAP HANA on Deployable Architecture tile** variation.
4. Click **Review deployment** options:
 - **Add to project** to add this deployment to an IBM Cloud project and combine it with other deployments. IBM Cloud projects include several more pipeline steps before deployment, including deployment validation, cost calculation, compliance verification, and approval process.
 - **Create from the CLI** to get the CLI command. With this command you can trigger the deployment from the CLI.
 - **Work with code** to embed the code into other terraform deployments.
 - **Deploy with IBM Cloud Schematics** to trigger the deployment process directly.
5. Select **Deploy with IBM Cloud Schematics**.
6. Add the input parameters for this installation. There are 3 categories of parameters:
 - **Workspace** - These parameters define the workspace that is automatically created in Schematics:
 - Enter a name for the workspace or use the default name.
 - The Resource Group used to create resources. Use default or create a Resource Group.
 - Select a location to create your Schematics workspace. The workspace location need not match the resource location.
 - **Required input variables** - Review the default input variables and provide values that match your solution. These parameters are specific to your deployment. For more detailed information, see the [Readme file](#).

Parameter	Description
BASTION_FLOATING_IP	Required only for Schematics Deployments. The Floating IP from the Bastion Server.

HOSTNAME	The hostname for the VSI. The hostname should be up to 13 characters as required by SAP. For more information on the rules regarding hostnames for SAP systems, check SAP Note 611361: Hostnames of SAP ABAP Platform servers
REGION	The cloud region to deploy the solution. The regions and zones for VPC are listed here . Review supported locations in IBM Cloud Schematics here . Sample value: eu-de.
RESOURCE_GROUP	The name of an existing Resource Group for VSIs and Volumes resources. Default value: "Default". The list of Resource Groups is available here .
SECURITY_GROUP	The name of an existing Security group. The list of security groups is available here .
SSH_KEYS	The list of SSH Keys UUIDs that are allowed to SSH as root to the VSI can contain one or more IDs. The list of SSH Keys is available here . Sample input (use your own SSH UUIDs from IBM Cloud){: external}: ["r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a", "r010-3fcfd9fe7-d4a7-41ce-8bb3-d96e936b2c7e"]
SUBNET	The name of an existing subnet. The list of subnets is available here .
VPC	The name of an existing VPC. The list of VPCs is available here .
ZONE	The cloud zone where to deploy the solution. Sample value: eu-de-2.
ibmcloud_api_key	IBM Cloud API key (Sensitive* value).
private_ssh_key	Required only for Schematics Deployments - Input your id_rsa private key pair content in OpenSSH format (Sensitive* value). This private key should be used only during the terraform provisioning and it is recommended to be changed after the SAP deployment.
hdb_instance_number	The instance number of the SAP HANA database server.
sap_aas_instance_number	Technical identifier for the internal processes of the additional application server.
sap_asci_instance_number	Technical identifier for the internal processes of ASCS.
sap_ci_host	IP address of the existing SAP Central Instance.
sap_ci_hostname	The hostname of the existing SAP Central Instance.
sap_ci_instance_number	Technical identifier for the internal processes of the Central Instance.
sap_sid	The SAP system ID identifies the entire SAP system.
sap_main_password	Common password for all users that are created during the installation (See Obs*).

Required Variables

- **Optional variables** - Review and update the optional input variables. The Ansible scripts expect the SAP kits to be in the default locations listed. For more information, see the [Readme file - Input Parameters](#).

Parameter	Description
ID_RSA_FILE_PATH	The file path for private_ssh_key is automatically generated by default. If it is changed, it must contain the relative path from Git repo folders. Default value: "ansible/id_rsa".
IMAGE	The OS image used for the VSI. A list of images is available here .
PROFILE	The profile used for the VSI. A list of profiles is available here . For more information about supported DB/OS and IBM Gen 2 Virtual Server Instances (VSI), check SAP Note 2927211: SAP Applications on IBM Virtual Private Cloud .

VOL1	Volume 1 Size - The size for the disks in GB that are to be attached to the VSI and used by SAP.
VOL2	Volume 2 Size - The size for the disks in GB that are to be attached to the VSI and used by SAP.
kit_sapcar_file	Path to the sapcar binary, as downloaded from SAP Support Portal.
kit_swpm_file	Path to the SWPM archive (SAR), as downloaded from SAP Support Portal.
kit_saphostagent_file	Path to the SAP Host Agent archive (SAR), as downloaded from SAP Support Portal.
kit_hdbclient_file	Path to the HANA DB client archive (SAR), as downloaded from SAP Support Portal.

Optional Variables

7. Accept the license agreement.
8. Select **Deploy**. The deployment starts and you are directed to the Schematics page that displays the script log files for you to monitor the deployment progress.

Creating the infrastructure using Terraform with the bastion server CLI

Use these steps to configure the IBM Cloud Provider plug-in and use Terraform to install SAP AAS to SAP HANA and AnyDB on your existing VPC on an already deployed SAP NetWeaver 7.X with SAP HANA 2.0 or ASE SYB as a Central Instance.

The script takes 1 - 2 hours to complete.

1. Access the bastion server cli.
2. Clone the solution repository and change to the folder.

ASE SYB 16 Clone the solution repository from <https://github.com/IBM-Cloud/sap-aas-abap-ase-syb> and cd to the sap-aas-abap-ase-syb/cli folder.

```
$ git clone https://github.com/IBM-Cloud/sap-aas-abap-ase-syb
cd sap-aas-abap-ase-syb/cli/
```

SAP HANA 2.0: Clone the solution repository from <https://github.com/IBM-Cloud/sap-abap-hana-aas> and cd to the sap-abap-hana-aas folder.

```
$ git clone https://github.com/IBM-Cloud/sap-abap-hana-aas.git
cd sap-abap-hana-aas/
```

3. Modify the `input.auto.tfvars` file to specify the information for the existing VPC, your region, zone, networking component names, hostname for the AAS VSI,profile, and image. You need your 40-digit SSH key ID for this file. The second SSH key is optional. For more options for profile, see [Instance Profiles](#). For more options, see [Images](#). For descriptions of the variables, see the [readme](#) file.

The VSI OS images that are supported for this solution for Netweaver Additional Application Server are:

- ibm-redhat-8-4-amd64-sap-applications-2
- ibm-redhat-8-6-amd64-sap-applications-2
- ibm-sles-15-3-amd64-sap-applications-2
- ibm-sles-15-4-amd64-sap-applications-4

```
$ # Infra VPC variables for ASE SYB
REGION    = "eu-de"
ZONE      = "eu-de-2"
VPC       = "ic4sap"                      # EXISTING Security group name
SECURITY_GROUP = "ic4sap-securitygroup"     # EXISTING Security group name
RESOURCE_GROUP = "wes-automation"
SUBNET    = "ic4sap-subnet"                 # EXISTING Subnet name
SSH_KEYS   = [ "r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a" , "r010-3fcfd9fe7-d4a7-41ce-8bb3-
d96e936b2c7e" ]

# SAP AAS VSI variables:
```

```

HOSTNAME = "sapnwase-as01"
PROFILE = "bx2-4x16"
IMAGE = "ibm-redhat-8-4-amd64-sap-applications-2

$ # Infra VPC variables for ABAP HANA
REGION      = "eu-de"
ZONE        = "eu-de-2"
VPC          = "ic4sap" # EXISTING Security group name
SECURITY_GROUP = "ic4sap-securitygroup" # EXISTING Security group name
RESOURCE_GROUP = "wes-automation"
SUBNET       = "ic4sap-subnet" # EXISTING Subnet name
SSH_KEYS     = [ "r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a" , "r010-3fc9fe7-d4a7-41ce-8bb3-d96e936b2c7e" ]
ID_RSA_FILE_PATH = "ansible/id_rsa"

# SAP AAS variables:
HOSTNAME = "sapnwapp"
PROFILE = "bx2-4x16"
IMAGE = "ibm-redhat-8-6-amd64-sap-applications-2"

```

4. Customize your SAP system configuration. In the same file, input.auto.tfvars, edit the SAP system configuration variables that are passed to the Ansible automated deployment. For descriptions of the variables, see the [readme](#) file.

```

$ # SAP system configuration - for ASE SYB
sap_sid = "NWD"
sap_ci_host = "10.243.132.10"
sap_ci_hostname = "sapnwase"
sap_ci_instance_number = "00"
sap_asc_s_instance_number = "01"
sap_aas_instance_number = "00"

# Kits paths
kit_sapcar_file = "/storage/NW75SYB/SAPCAR_1010-70006178.EXE"
kit_swpm_file = "/storage/NW75SYB/SWPM10SP31_7-20009701.SAR"
kit_saphotagent_file = "/storage/NW75SYB/SAPHOSTAGENT51_51-20009394.SAR"

```

```

$ # SAP system configuration - for ABAP HANA
sap_sid = "NWD"
sap_ci_host = "10.243.132.10"
sap_ci_hostname = "sapnwapp01"
sap_ci_instance_number = "00"
sap_asc_s_instance_number = "01"
hdb_instance_number = "00"
sap_aas_instance_number = "00"

# Kits paths
kit_sapcar_file = "/storage/NW75HDB/SAPCAR_1010-70006178.EXE"
kit_swpm_file = "/storage/NW75HDB/SWPM10SP31_7-20009701.SAR"
kit_saphotagent_file = "/storage/NW75HDB/SAPHOSTAGENT51_51-20009394.SAR"
kit_hdbclient_file = "/storage/NW75HDB/IMDB_CLIENT20_009_28-80002082.SAR"

```

Ansible decompresses the rest of the SAP kit files. For more information, see the [readme](#) file.

5. Initialize the Terraform CLI.

```
terraform init
```

6. Create a Terraform execution plan. The Terraform execution plan summarizes all the actions that are done to create the virtual private cloud instance in your account.

```
terraform plan plan1
```

Enter an SAP main password and your API key.

The SAP main password must be 10 - 14 characters long and contain at least one digit (0-9). It can contain only the following characters: a-z, A-Z, 0-9, @, #, \$, . *This password cannot contain exclamation points '!'. The password must not start with a digit or an underscore ().*

7. Verify that the plan shows all of the resources that you want to create and that the names and values are correct. If the plan needs to be adjusted, edit the input.auto.tfvars file to correct resources and run terraform plan again.
8. Apply the saved plan.

```
$ terraform apply "plan1"
```

The virtual private cloud and components are created and you see output similar to the `terraform plan` output.

9. Add the SAP credentials and the virtual server instance IP to the SAP GUI. For more information about the SAP GUI, see [SAP GUI](#).

Next steps

If you need to rename your resources after they are created, modify the `input.auto.tfvars` file to change the names and run `terraform plan` and `terraform apply` again. Do not use the IBM Cloud Dashboard and user interface to modify your VPC after it is created. The Terraform scripts create a complete solution and selectively modifying resources with the user interface might cause unexpected results.

If you need to remove the SAP Netweaver 7.X on HANA or AnyDB installation, go to your project folder and run `terraform destroy`. The `terraform destroy` command does not remove the VPC in this scenario because the VPC was created before these Terraform scripts were run.

Related information

For more information about Terraform on IBM Cloud, see [Getting started with Terraform on IBM Cloud](#).

For more information about using Terraform for creating only a VPC for SAP, without the SAP architecture, see [Creating single-tier virtual private cloud for SAP by using Terraform](#).

SAP One Support Notes that apply to this document:

- [SAP Note 84555 - Windows Server, Linux®, and UNIX: Certified hardware](#)
- [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#)
- [SAP Note 2923773 - Linux® on IBM Cloud \(IaaS\): Adaption of your SAP license](#)
- [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#)
- [SAP Note 2369910 - SAP Software on Linux®: General information](#)
- [SAP Note 171380 - Released IBM hardware \(Intel processors\) and IBM cloud services offers](#)
- [SAP Note 1380654 - SAP support in IaaS environments](#)

This document is referenced by:

- [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#)
- [SAP Note 2588225 - SAP on IBM Cloud: Protect against speculative execution vulnerabilities](#)
- [SAP Note 1380654 - SAP support in IaaS environments](#)
- [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#)

SAP NetWeaver and Db2 3-tier in VPC

Automating SAP workload HA deployment on IBM Cloud VPC with Terraform and Ansible

You can use Terraform to automate IBM Cloud® VPC provisioning. The VPC provisioned includes virtual server instances with high network performance. The VPC infrastructure contains various Infrastructure-as-a-Service (IaaS) offerings, including virtual servers. After the VPC is provisioned, the scripts use the Ansible Playbooks to install the SAP system.

IBM Cloud VPC introduction

VPC is a public cloud offering that an enterprise uses to establish its own private cloud-like computing environment on shared [public cloud](#) infrastructure. VPC gives an enterprise the ability to define and control a virtual network that is logically isolated from all other public cloud tenants, creating a private and secure place on the public cloud.

Imagine that a cloud provider's infrastructure is a residential apartment building and multiple families live inside. A public cloud tenant is a kind of sharing an apartment with a few roommates. In contrast, having a VPC is like having your own private condominium; no one else has the key, and no one can enter the space without your permission.

VPC's logical isolation is implemented by using virtual network functions and security features that give the enterprise customer granular control over which IP addresses or applications can access particular resources. It is analogous to the "friends-only" or "public/private" controls on social media accounts used to restrict who can or can't see your otherwise public posts.

With IBM Cloud VPC, you can use the UI, CLI, and API to manually provision virtual server instances for VPC with high network performance. VPC infrastructure contains various Infrastructure-as-a-Service (IaaS) offerings including virtual servers for VPC.

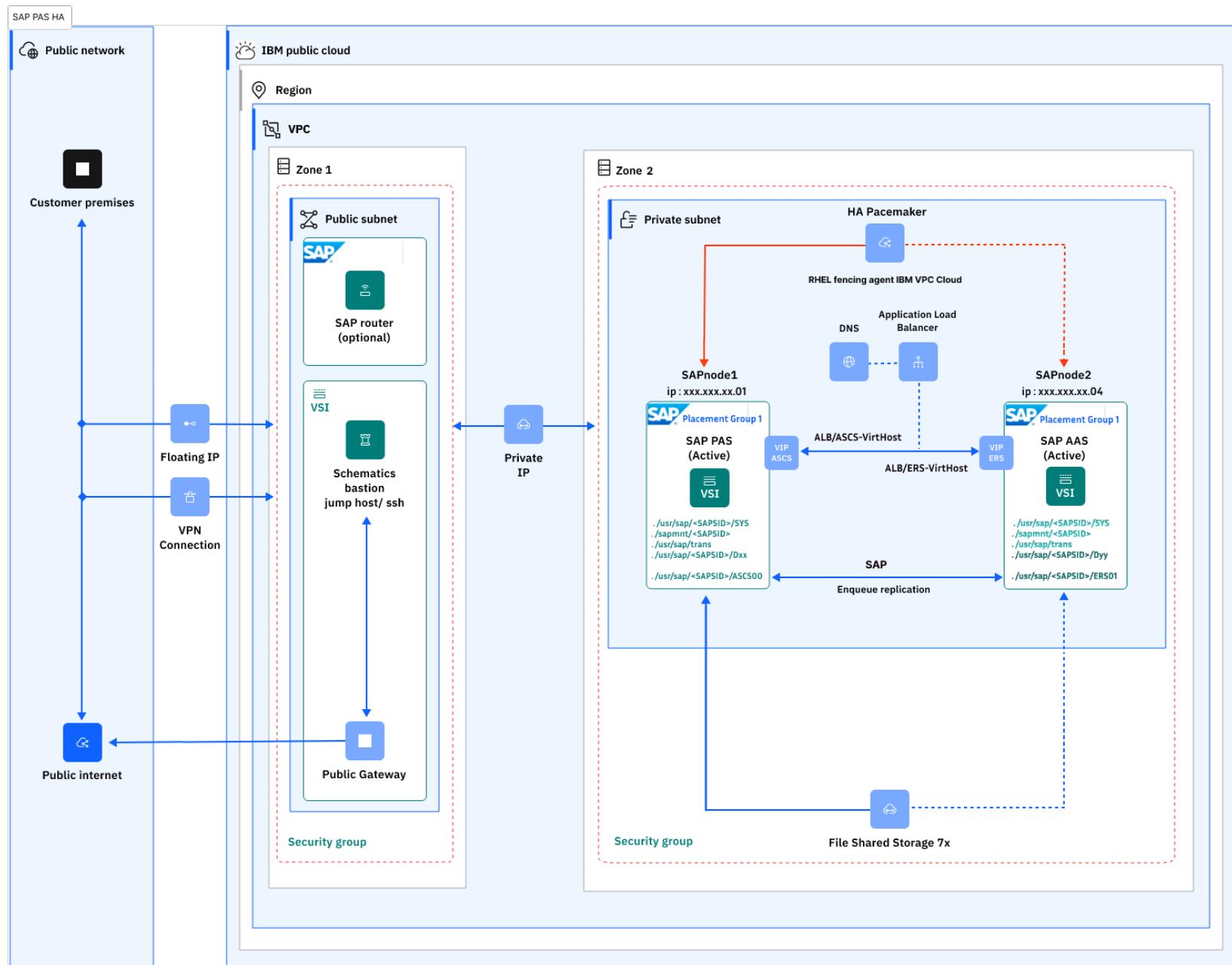
Use the following information to understand a simple use-case for planning, creating, and configuring resources for your VPC, and learn more about VPC overviews and VPC tutorials. For more information about the VPC, see [Getting started with Virtual Private Cloud \(VPC\)](#).

SAP products architecture on IBM Cloud VPC

A [Virtual Private Cloud \(VPC\)](#) contains one of the most secure and reliable cloud environments for SAP applications within your own VPC with virtual server instances. This represents an Infrastructure-as-a-Service (IaaS){: external} within IBM Cloud that offers all the benefits of isolated, secure, and flexible virtual cloud infrastructure from IBM. In comparison, the IBM Cloud classic infrastructure virtual servers offering uses virtual instances with native and VLAN networking to communicate with each other within a data center; however, the instances are restricted in one well-working pod by using subnet and VLAN networking as a gap scale up of virtual resources should rely between the pods. The IBM Cloud VPC network orchestrator layer concept eliminates the pod boundaries and restrictions, so this new concept handles all the networking for every virtual instance running within VPC across regions and zones.

Highly available system for SAP NetWeaver on IBM Cloud VPC

In a Highly Available (HA) system, every instance can run on a separate IBM Cloud virtual server instance. The cluster HA configuration for the SAP application server consists of two virtual server instances, each of them located in the same zone within the region by using placement groups. Placement groups assure that both cluster resources and cloud resources are also located in different compute nodes as specified in the following placement groups section:



SAP HA for SAP applications cluster nodes PAS (Active) and AAS (Active)

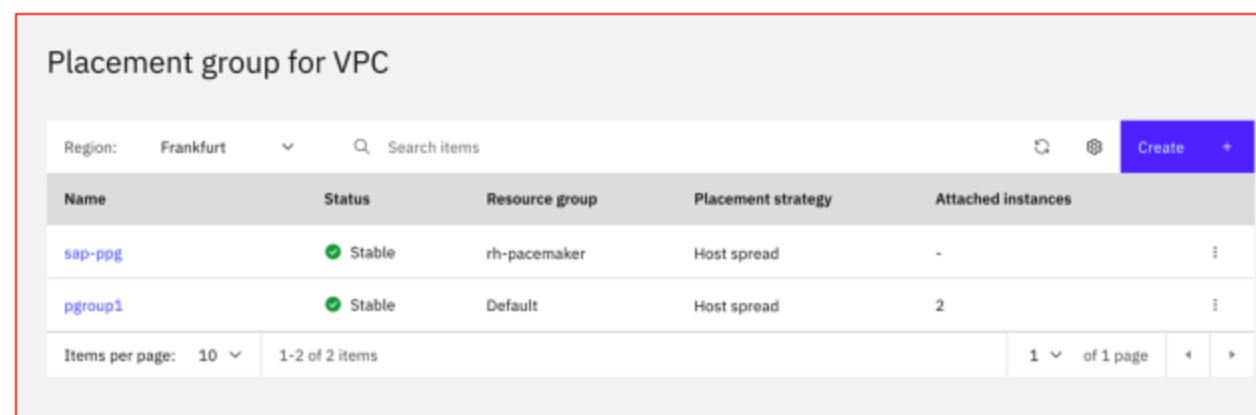
Placement groups on IBM Cloud VPC for SAP HA architecture

Placement Groups (PG) for VPC have two different anti-affinity strategies for high availability. By using the placement strategies, you minimize the chance of service disruption with virtual server instances that are placed on different hosts or into an infrastructure with separate power and network supplies.

The design of placement groups for IBM Cloud virtual servers solves this issue. Placement groups give a measure of control over the host on which a new public virtual server is placed. In this release, a “spread” rule is implemented, which means that the virtual servers within a placement group are spread onto different hosts. You can build a highly available application within a data center and know that your virtual servers are isolated from each other.

Placement groups with the spread rule are available to create in selected IBM Cloud data centers. After a spread rule is created, you can provision a virtual server into that group and ensure that it is not on the same host as any of your other virtual servers. This feature comes with no cost.

You can create your placement group and assign up to four new virtual server instances. With the spread rule, each of your virtual servers are provisioned on different physical hosts. In the following configuration example, the “Power Spread” option is used:



Placement groups host spread

Placement group for VPC					
Name	Status	Resource group	Placement strategy	Attached instances	
sapha-poc	Stable	wes-ic4sap-resourcegroup	Power spread	4	
Items per page: 10 1 item 1 of 1 page					

Placement groups power spread

Following are the SAP instances that are required for HA scenario:

- ABAP SAP Central Services (ASCS) instance - contains the ABAP message server and the ABAP enqueue server.
- Enqueue Replication Server (ERS) instance for the ASCS instance.
- Database instance
- Primary Application Server (PAS) instance on node 1.
- Additional Application Server (AAS) instance on node 2.



Note: It is recommended to run both the ASCS instance and the ERS instance in a switchover cluster infrastructure.

IBM Cloud File Storage for VPC for SAP HA architecture

[IBM Cloud File Storage for VPC](#) technology is used to make the SAP directories available to the SAP system. The technologies of choice are NFS, shared disks, and cluster file system. If you have decided to use the HA solution for your SAP system, make sure that you properly address the HA requirements of the SAP file systems in your SAP environment.

File shares for VPC								
Name	Status	Resource groups	Location	Mount targets	Size	Replication role	Encryption type	
usrsap-as1-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-as2-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-sapscs-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-sapers-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-sapmnt-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-sapsys-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-trans-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	80 GB	None	Provider managed	

File shares for VPC

- File shares that are mounted as NFS permanent file systems on both cluster nodes for SAP HA application:
 - `/usr/sap/<SAPSID>/SYS`
 - `/sapmnt<SAPSID>`
 - `/usr/sap/trans`
- Cluster-managed file systems for SAP HA application: ASCS
 - `/usr/sap/<SAPSID>/ASCS00`
 - `/usr/sap/<SAPSID>/ERS01`
- Permanent NFS mount on SAP HA application node 1 PAS instance:
 - `/usr/sap/<SAPSID>/Dxx`
- Permanent NFS mount on SAP HA application node 2 dialog instance:
 - `/usr/sap/<SAPSID>/Dyy`

Prerequisites

You need to install the hardware (hosts, disks, and network) and decide how to distribute the database, SAP instances, and if required, the Network File System (NFS) server over the cluster nodes.

Context

Following are the types of SAP directories:

- Physically shared directories: `/<sapmnt>/<SAPSID>` and `/usr/sap/trans`

- Logically shared directories that are bound to a node, such as `/usr/sap`, with the following local directories:
 - `/usr/sap/<SAPSID>`
 - `/usr/sap/<SAPSID>/SYS`
 - `/usr/sap/hostctrl`
- Local directories that contain the SAP instances such as `/usr/sap/<SAPSID>/ASCS<Instance_Number>`
- The global transport directory may reside on a separate SAP transport host as a standard three systems transport layer configuration.

You need at least two nodes and a shared file system for distributed ASCS and ERS instances. The assumption is that the rest of the components are distributed on other nodes.

ASCS and ERS installation

In order for the ASCS and ERS instances to be able to move from one node to the other, they need to be installed on a shared file system and use virtual hostnames based on the virtual IP.

In this VPC-based SAP HA solution, the shared file system that is required by the cluster is replaced by the NFS-mounted file storage, and the virtual IP is replaced by the Application Load Balancer for VPC (ALB).

In this scenario, three ALBs are used, one for each Single Point of Failure (SPOF) component in order to replace the virtual IP requirement: ALB for ASCS, ALB for ERS, and ALB for ASE Sybase. Each ALB is configured as a backend for the corresponding cluster servers and redirects all of the communication that is received on the front-end ports to the active server in the backend pool.

Load balancers for VPC						
Region:	Frankfurt	▼	<input type="text"/> poc	X		
Name	Status	Family	Resource group	Type	Hostname	Location
db-alb-hana-poc	Active	Application	wes-ic4sap-resourcegroup	Private	20bdd130-eu-de.lb.appdomain.cloud	Frankfurt
sap-alb-ers-poc	Active	Application	wes-ic4sap-resourcegroup	Private	3941d983-eu-de.lb.appdomain.cloud	Frankfurt
sap-alb-ascs-poc	Active	Application	wes-ic4sap-resourcegroup	Private	56a9190d-eu-de.lb.appdomain.cloud	Frankfurt

Application load balancer management of HA IPs mechanism

Private application load balancer

A [private application load balancer](#) is accessible through your private subnets that you configured to create the load balancer.

Similar to a public application load balancer, your private application load balancer service instance is assigned an FQDN; however, this domain name is registered with one or more private IP addresses.

IBM Cloud operations change the number and value of your assigned private IP addresses over time, based on maintenance and scaling activities. The backend virtual server instances that host your application must run in the same region and under the same VPC.

Use the assigned ALB FQDN to send traffic to the private application load balancer to avoid connectivity problems to your applications during system maintenance or scaling down activities.

Each ALB sends traffic to the cluster node where the application (ASCS, ERS, ASE Sybase DB) is running. During the cluster failover, the ALB redirects all the traffic to the new node where the resources are up and running.



Note: DNS-as-a-Service (DNSaaS) is the management IBM Cloud VPC DNS service of HA and FQDN (IPs) mechanism.



Note: The ALB has a default of 50 seconds for client and server timeout, so after 50 seconds of inactivity, the connection is closed. To support SAP connections through ALB and not lose connection after 50 seconds, you need to request a change this value to a minimum of 300 seconds (client-side idle connection = minimum 300s and server-side idle connection = minimum 300s). To request this change, open a support ticket. This is an account-wide change that affects all of the ALBs in your account. For more information, see [Connection timeouts](#).

DNS Services with VPC

[IBM Cloud DNS Services](#) provide private DNS to VPC users. Private DNS zones are resolvable only on IBM Cloud and from explicitly [permitted networks](#) in an account. To get started, create a DNS Services instance by using the IBM Cloud console.

DNS Services allows you to:

- Create the private DNS zones that are collections for holding the domain names.
- Create the DNS resource records under these DNS zones.
- Specify the access controls used for the DNS resolution of resource records on a zone-wide level.

DNS Services also maintains its own worldwide set of DNS resolvers. Instances that are provisioned under IBM Cloud on an IBM Cloud network can use resource records that are configured through IBM Cloud DNS Services by querying DNS Services resolvers.

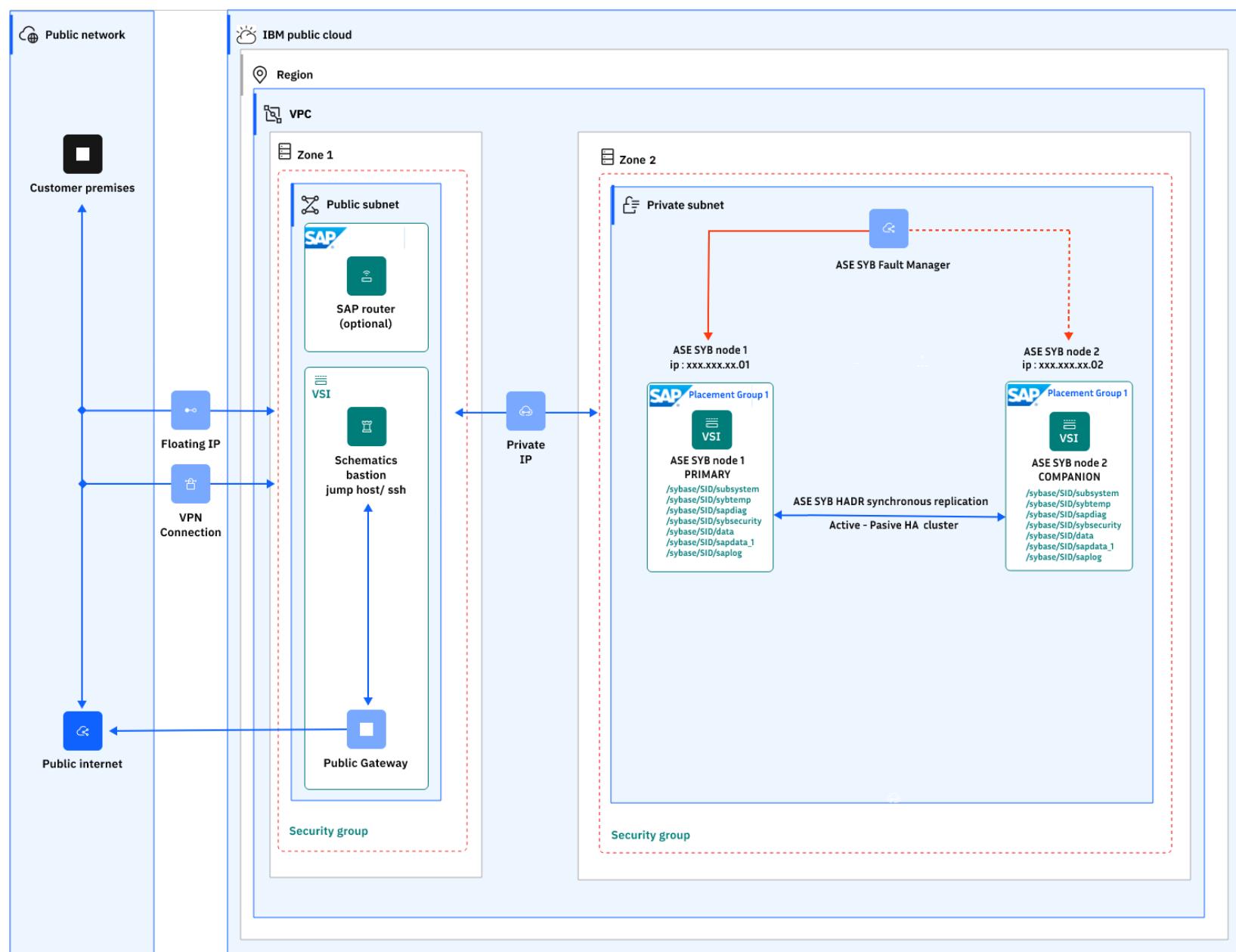
Resource records and zones that are configured through DNS Services are:

- Separated from the wider public DNS, and their publicly accessible records.
- Hidden from the system outside of and not part of the IBM Cloud private network.
- Accessible only from the system that you authorize on the IBM Cloud private network.
- Resolvable only via the resolvers provided by the service.

The DNS service maps the FQDN of each ALB to the virtual hostnames of the ASCS, ERS, and ASE Sybase that are used by SAP applications.

Type	Name	Value	TTL
CNAME	dbpochana	is an alias of 20bdd130-eu-de.lb.appdomain.cloud	12 hr
CNAME	sappocers	is an alias of 3941d983-eu-de.lb.appdomain.cloud	12 hr
CNAME	sappocases	is an alias of 56a9190d-eu-de.lb.appdomain.cloud	12 hr

Highly available system for SAP ASE Sybase database with HADR system



SAP HA for ASE Sybase DB instances cluster nodes primary (Active) and Secondary (Companion)

At the most basic level, a standard HA ASE Sybase cluster in an active(primary)-passive(companion) configuration has two nodes: one is the primary node and the other is the standby node. This means that the primary node is actively serving the active SAP DB instances (Primary and Companion), while the standby node is waiting to jump in if there is any failure.

The cluster is set with a virtual hostname IP (hostname is mapped to the FQDN of the ASE Sybase ALB through DNS, which is the same as

explained previously for SAP ASCS and ERS instances). Application instances (PAS and AAS) are used on the SAP profiles to call that particular component. The cluster assigns the virtual IP to the active node and uses a heartbeat monitor to confirm the availability of the components. If the primary node stops responding, it triggers the automatic failover mechanism that calls the standby node to step up to become the primary node. The ALB detects the change, redirects the traffic to the new active node, and assigns the virtual IP to it, restoring the component availability. Once fixed, the failed node comes online as a standby node.

SAP Sybase HADR system supports synchronous replication

The SAP Sybase HADR system supports synchronous replication between the primary and standby servers for high availability. An active-active setup is a two-node configuration where both nodes in the cluster include SAP ASE managing independent workloads, capable of taking over each others workload in the event of a failure.

The SAP ASE server that takes over the workload is called a secondary companion, and the SAP ASE server that fails is called the primary companion. Together they are companion servers. This movement from one node to another is called failover. After the primary companion is ready to resume its workload, it is moved back to its original node. This movement is called a failback.

When a system fails over, clients that are connected to the primary companion and use the failover property automatically reestablish their network connections to the secondary companion. You must tune your operating system to successfully manage both servers during fail over. See your operating system documentation for information about configuring your system for high availability. An SAP ASE configured for failover in an active-active setup can be shut down using the shutdown command only after you have suspended SAP ASE from the companion configuration, at both the server level and the platform level.

The always-on option in a High Availability and Disaster Recovery (HADR) system consists of two SAP ASE servers:

- Primary on which all transaction processing takes place.
- Warm standby (referred to as a "standby server" in DR mode, and as a "companion" in HA mode) for the primary server, and contains copies of designated databases from the primary server.



Note: The HADR feature that is shipped with SAP ASE version 16.0 SP02 supports only a single-companion server.

Some high-availability solutions (for example, the SAP Adaptive Server Enterprise Cluster Edition) share or use common resources between nodes. However, the HADR system is a "shared nothing" configuration, each node has separate resources including disks.

In an HADR system, servers are separate entities and data is replicated from the primary server to the companion server. If the primary server fails, a companion server is promoted to the role of primary server either manually or automatically. Once the promotion is complete, clients can reconnect to the new primary server, and see all committed data, including data that was committed on the previous primary server.

Servers can be separated geographically, which makes an HADR system capable of withstanding the loss of an entire computing facility.



Note: The HADR system includes an embedded SAP Replication Server, which synchronizes the databases between the primary and companion servers. SAP ASE uses the Replication Management Agent (RMA) to communicate with Replication Server and SAP Replication Server uses Open Client connectivity to communicate with the companion SAP ASE.

The Replication Agent detects any data changes made on the primary server and sends them to the primary SAP Replication Server. In the figure above, the unidirectional arrows indicate that, although both SAP Replication Servers are configured, only one direction is enabled at a time.

The HADR system supports synchronous replication between the primary and standby servers for high availability so the two servers can keep in sync with Zero Data Loss (ZDL). This requires a network link that is fast enough between the primary and standby server so that synchronous replication can keep up with the primary servers workload. Generally, this means that the network latency is approximately the same speed as the local disk IO speed, a few (fewer than 10) milliseconds. Anything longer than a few milliseconds may result in a slower response to write operations at the primary.

The HADR system supports asynchronous replication between the primary and standby servers for disaster recovery. The primary and standby servers by using asynchronous replication can be geographically distant, meaning they can have a slower network link. With asynchronous replication, Replication Agent Thread captures the primary servers workload, which is delivered asynchronously to SAP Replication Server. The SAP Replication Server applies these workload change to the companion server.

The most fundamental service that is offered by the HADR system is the failover; planned or unplanned from the primary to the companion server, which allows maintenance activity to occur on the old primary server, while applications continue on the new primary.

The HADR system provides protection in the event of a disaster. If the primary server is lost, the companion server can be used as a replacement. Client applications can switch to the companion server, and the companion server is quickly available for users. If the SAP Replication Server was in synchronous mode before the failure of the primary server, the Fault Manager automatically initiates failover with

zero data loss.

Fault Manager installation on the SAP ASCS node

The required parameters are asked during the installation process to create a profile for the fault manager and then adds it to the instance start profile. It is also possible to run the installation by using an existing profile: `sybdbfm install pf=<SYBHA.PFL>` In this case, the installation process will only ask for profile parameters missing in the profile.



Note: Fault manger is integrated with ASCS on same SAP PAS/AAS cluster (start/stop/move together).

There may be some data loss if the SAP Replication Server was in asynchronous mode and you must use manual intervention to failover for disaster recovery.

Connection attempts to the companion server without the necessary privileges are silently redirected to the primary companion via the login redirection mechanism, which is supported by Connectivity libraries. If login redirection is not enabled, client connections fail and are disconnected.

The SAP ASE HADR option installs the below components:

- SAP ASE
- SAP Replication Server
- Replication Management Agent (RMA)
- SAP Host Agent
- Fault Manager
- SAP ASE Cockpit



Note: This automation is offered at no cost; however, the provisioned infrastructure comes at cost.

VPC with Additional Application Server (AAS) ABAP on Linux for SAP HANA

You can use Terraform scripts to create a single-tier VPC and create the AAS to HANA and AnyDB infrastructure on the VPC. The Terraform scripts use the VPC information that you provide and then call the Ansible playbook to create the SAP architecture on the specified VPC. Terraform on IBM Cloud® enables predictable and consistent provisioning of IBM Cloud Virtual Private Cloud (VPC) infrastructure resources so that you can rapidly build complex, cloud environments. IBM Cloud VPC infrastructure consists of SAP certified hardware that uses Intel® Xeon CPUs and more Intel® technologies.

You have two deployment methods to choose from:

- Terraform scripts that run from the CLI on your bastion server.
- Schematics user interface accessed from your cloud dashboard menu.

You can create SAP AAS NetWeaver 7.x on the SAP HANA-based ABAP stack.

SAP solution implemented

Many SAP enterprise solutions are built on the SAP platform (SAP NetWeaver) including:

- SAP HANA as Primary Persistence for SAP NetWeaver-based applications
- SAP Business Suite applications (ERP, CRM, and SCM, and other applications),
- SAP Business Warehouse (BW), and
- Other SAP enterprise solutions

SAP NetWeaver has two distinct aspects, ABAP and Java. Many applications that are built on the SAP NetWeaver's ABAP or Java (or both) application servers run on SAP DB owned HANA and ASE Sybase either in AnyDB platforms (MSSQL, Oracle, and Db2).

Technical interfaces are available for applications that are built on the SAP NetWeaver AS ABAP and AS Java to run on SAP HANA and AnyDB. However, specific development enablement is normally required for each application to ensure that it runs optimally on the SAP HANA. SAP Business Suite applications (ERP, CRM, SCM, and other applications), SAP Business Warehouse (BW), and other SAP NetWeaver-based applications were modified to run on SAP HANA and have many advantages. Also, various components and complimentary applications that are built on SAP NetWeaver can also run on SAP HANA or AnyDB by using the provided SAP NetWeaver DB interfaces.

The SAP HANA as primary persistence for SAP NetWeaver-based applications scenario has one restriction: SAP NetWeaver ABAP and Java

application servers must run on separate hardware servers from the SAP HANA hardware.

What is created

The scripts automate the virtual infrastructure resources, provisioning the processes for the SAP architecture in an existing VPC with a distributed environment. SAP AAS NetWeaver 7.x (HANA or ASE SYB) application server on a distinct VSI VPC system and SAP HANA DB on a dedicated server type VSI VPC box are provisioned. The scripts work in two phases.

During the first phase of [Automate SAP bastion server – SAP media storage repository](#), the following virtual infrastructure resources based on the components from the existing VPC created by the bastion server are:

- 1 VPC where the virtual server instance is provisioned.
- 1 security group. The rules for this security group are:
 - Allow inbound DNS traffic (port 53).
 - Allow inbound SSH traffic (TCP port 22).
 - Allow all outbound traffic from the virtual server instance.
 - Allow all traffic in the security group.
- 1 subnet to enable the networking in your VPC.
- 2 virtual server instances with SAP certified storage and network configurations.
- 1 floating IP address used to access your VPC virtual server instance over the public network.

During the second phase, the Ansible Playbooks is called and the SAP architecture is installed for both dedicated virtual server instance (VSI) SAP application; VSI system and dedicated SAP HANA VSI box. The SAP architecture that is deployed on the SAP NetWeaver 7.x release is a stand-alone dedicated SAP HANA 2.0 box release. For more information about this architecture, see [Automating SAP HANA stand-alone virtual server instance on IBM Cloud® VPC by using Terraform and Ansible](#).

You can provision only one instance of the service per IBM Cloud region.

Schematics deployment

When you run the scripts with the Schematics interface, you:

- Enter the workspace information.
- Enter the GitHub path for the chosen solution either on NetWeaver AAS for HANA.
- Modify the parameters in the Schematics interface. They are the same parameters as the `input.auto.tfvars` file that you use with the cli.

Virtual server instance configuration

Following are the supported operating system images for SAP NetWeaver primary application server:

- ibm-redhat-8-4-amd64-sap-applications-2
- ibm-redhat-8-6-amd64-sap-applications-2
- ibm-sles-15-3-amd64-sap-applications-2
- ibm-sles-15-4-amd64-sap-applications-3

Following are the supported operating system images for SAP HANA database:

- ibm-redhat-8-4-amd64-sap-hana-2
- ibm-redhat-8-6-amd64-sap-hana-2
- ibm-sles-15-3-amd64-sap-hana-2
- ibm-sles-15-4-amd64-sap-hana-1

For both server instances there are:

- Two SSH keys are configured to access SSH as `root`.
- Three storage volumes as described in the `input.auto.tfvars` file.

What is created for anydb

The scripts use the information that you provide for an existing VPC and deploy AAS to SAP HANA or AnyDB on a different host than CI (SAP Central Instance) VSI host. For more information about this architecture, see [SAP NetWeaver 7.x on UNIX with HANA or AnyDB on IBM Cloud](#)

[VPC on IBM Cloud VPC](#). You specify the information for the VPC to use in the `input.auto.tfvars` file.

The scripts call the Ansible Playbooks to install the SAP architecture.

Script files

The configuration and script files are provided on GitHub. Each supported interface for the SAP solution installation has its own folder in the GitHub repository:

- [GitHub repository for Terraform – AAS HANA](#)

Terraform interface

To run the Terraform script, you modify:

- The `input.auto.tfvars` file to specify the existing VPC resources for your solution. Specify the variables for the existing VPC:
 - VPC name
 - Security group
 - Subnet
 - Hostname
 - Profile
 - Image
 - Up to two SSH keys

You can change the default SAP system configuration settings to match your solution. You can also specify the location where you downloaded the SAP kits.

The IBM Cloud Provider plug-in for Terraform on IBM Cloud uses these configuration files to install AAS to SAP HANA and AnyDB on the specified VPC in your IBM Cloud account.

Support

There are no warranties of any kind, and there is no service or technical support available for these materials from IBM®. As a recommended practice, review carefully any materials that you download from this site before using them on a live system.

Though the materials provided herein are not supported by the IBM® Service organization, your comments are welcomed by the developers, who reserve the right to revise, readapt or remove the materials at any time. To report a problem, or provide suggestions or comments, open a GitHub issue.

Before you begin

Before you use the scripts in the bastion cli:

- Set up your account to access the VPC. Make sure that your account is [upgraded to a paid account](#).
- If you have not already, create a Bastion server to store the SAP kits. For more information, see [Automate SAP bastion server - SAP media storage repository](#).
- Download the SAP kits from the SAP Portal to your Deployment Server. Make note of the download locations. Ansible decompresses the files. For more information, see the [readme](#) file.
- [Create or retrieve an IBM Cloud API key](#). The API key is used to authenticate with the IBM Cloud platform and to determine your permissions for IBM Cloud services.
- [Create or retrieve your SSH key ID](#). You need the 40-digit UUID for the SSH key, not the SSH key name.
- Terraform should already be installed on the bastion server that you deployed. For more information, see [Bastion server for SAP deployment](#).
- (Optional - Catalog Tile) create secrets for your credentials and passwords by using the [Secrets Manager](#).

Deploying SAP AAS NetWeaver 7.x on HANA by using the Schematics user interface

Use these steps to configure the SAP Additional Application Server (AAS) NetWeaver with HANA or AnyDB on your existing VPC by using the Schematics interface. The script takes 2 - 3 hours to complete.

1. From the IBM Cloud menu, select **Schematics**.
2. Click **Create** workspace.

3. On the **Specify template** page:
 - Enter the URL for the Schematics interface.
 - Select the **Terraform version** that is listed in the readme file.
 - Click **Next**.
4. On the **workspace details** page:
 - Enter a name for the workspace.
 - Select a **Resource group**.
 - Select a **Location** for your workspace. The workspace location does not have to match the resource location.
 - Select **Next**.
5. Select **Create** to create your workspace.
6. On the workspace settings page, in the input variables section, review the default input variables and provide values that match your solution.
 For a more detailed description of each parameter, check the GitHub repo [AAS HANA readme](#) file, chapter "Input parameter file". Also, make sure to mark the parameters that contain sensitive information like passwords, API, and ssh private keys as "sensitive". These parameters are marked as "sensitive" in the readme file, under "Input parameter file".
7. On the workspace settings page, click **Generate plan**. Wait for the plan to complete.
8. Click **View log** to review the log files of your terraform execution plan.
9. Apply your Terraform template by clicking **Apply plan**.
10. Review the log file to ensure that no errors occur during the provisioning, modification, or deletion process.

Deploying SAP AAS NetWeaver (ABAP) on HANA with the Deployable Architecture tile interface

Use these steps to configure the SAP AAS NetWeaver (ABAP) on HANA on your existing VPC by using the catalog tile interface. The script takes 2 - 3 hours to complete.

1. From the IBM Cloud catalog, select **VPC with Additional Application Server ABAP on Linux for SAP HANA** on HANA tile. The **Create** tab opens for VPC with Additional Application Server ABAP on Linux for SAP HANA. For more information about this deployment, see the About tab or the readme file link.
2. Select the latest version.
3. Select **VPC with Additional Application Server ABAP on Linux for SAP HANA on Deployable Architecture tile** variation.
4. Click **Review deployment** options:
 - **Add to project** to add this deployment to an IBM Cloud project and combine it with other deployments. IBM Cloud projects include several more pipeline steps before deployment, including deployment validation, cost calculation, compliance verification, and approval process.
 - **Create from the CLI** to get the CLI command. With this command you can trigger the deployment from the CLI.
 - **Work with code** to embed the code into other terraform deployments.
 - **Deploy with IBM Cloud Schematics** to trigger the deployment process directly.
5. Select **Deploy with IBM Cloud Schematics**.
6. Add the input parameters for this installation. There are 3 categories of parameters:
 - **Workspace** - These parameters define the workspace that is automatically created in Schematics:
 - Enter a name for the workspace or use the default name.
 - The Resource Group used to create resources. Use default or create a Resource Group.
 - Select a location to create your Schematics workspace. The workspace location need not match the resource location.
 - **Required input variables** - Review the default input variables and provide values that match your solution. These parameters are specific to your deployment. For more detailed information, see the [Readme file](#).

Parameter	Description
BASTION_FLOATING_IP	Required only for Schematics Deployments. The Floating IP from the Bastion Server.

HOSTNAME	The hostname for the VSI. The hostname should be up to 13 characters as required by SAP. For more information on the rules regarding hostnames for SAP systems, check SAP Note 611361: Hostnames of SAP ABAP Platform servers
REGION	The cloud region to deploy the solution. The regions and zones for VPC are listed here . Review supported locations in IBM Cloud Schematics here . Sample value: eu-de.
RESOURCE_GROUP	The name of an existing Resource Group for VSIs and Volumes resources. Default value: "Default". The list of Resource Groups is available here .
SECURITY_GROUP	The name of an existing Security group. The list of security groups is available here .
SSH_KEYS	The list of SSH Keys UUIDs that are allowed to SSH as root to the VSI can contain one or more IDs. The list of SSH Keys is available here . Sample input (use your own SSH UUIDs from IBM Cloud){: external}: ["r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a", "r010-3fcfd9fe7-d4a7-41ce-8bb3-d96e936b2c7e"]
SUBNET	The name of an existing subnet. The list of subnets is available here .
VPC	The name of an existing VPC. The list of VPCs is available here .
ZONE	The cloud zone where to deploy the solution. Sample value: eu-de-2.
ibmcloud_api_key	IBM Cloud API key (Sensitive* value).
private_ssh_key	Required only for Schematics Deployments - Input your id_rsa private key pair content in OpenSSH format (Sensitive* value). This private key should be used only during the terraform provisioning and it is recommended to be changed after the SAP deployment.
hdb_instance_number	The instance number of the SAP HANA database server.
sap_aas_instance_number	Technical identifier for the internal processes of the additional application server.
sap_ascs_instance_number	Technical identifier for the internal processes of ASCS.
sap_ci_host	IP address of the existing SAP Central Instance.
sap_ci_hostname	The hostname of the existing SAP Central Instance.
sap_ci_instance_number	Technical identifier for the internal processes of the Central Instance.
sap_sid	The SAP system ID identifies the entire SAP system.
sap_main_password	Common password for all users that are created during the installation (See Obs*).

Required Variables

- **Optional variables** - Review and update the optional input variables. The Ansible scripts expect the SAP kits to be in the default locations listed. For more information, see the [Readme file - Input Parameters](#).

Parameter	Description
ID_RSA_FILE_PATH	The file path for private_ssh_key is automatically generated by default. If it is changed, it must contain the relative path from Git repo folders. Default value: "ansible/id_rsa".
IMAGE	The OS image used for the VSI. A list of images is available here .
PROFILE	The profile used for the VSI. A list of profiles is available here . For more information about supported DB/OS and IBM Gen 2 Virtual Server Instances (VSI), check SAP Note 2927211: SAP Applications on IBM Virtual Private Cloud .

VOL1	Volume 1 Size - The size for the disks in GB that are to be attached to the VSI and used by SAP.
VOL2	Volume 2 Size - The size for the disks in GB that are to be attached to the VSI and used by SAP.
kit_sapcar_file	Path to the sapcar binary, as downloaded from SAP Support Portal.
kit_swpm_file	Path to the SWPM archive (SAR), as downloaded from SAP Support Portal.
kit_saphostagent_file	Path to the SAP Host Agent archive (SAR), as downloaded from SAP Support Portal.
kit_hdbclient_file	Path to the HANA DB client archive (SAR), as downloaded from SAP Support Portal.

Optional Variables

7. Accept the license agreement.
8. Select **Deploy**. The deployment starts and you are directed to the Schematics page that displays the script log files for you to monitor the deployment progress.

Creating the infrastructure using Terraform with the bastion server CLI

Use these steps to configure the IBM Cloud Provider plug-in and use Terraform to install SAP AAS to SAP HANA and AnyDB on your existing VPC on an already deployed SAP NetWeaver 7.X with SAP HANA 2.0 or ASE SYB as a Central Instance.

The script takes 1 - 2 hours to complete.

1. Access the bastion server cli.
2. Clone the solution repository and change to the folder.

ASE SYB 16 Clone the solution repository from <https://github.com/IBM-Cloud/sap-aas-abap-ase-syb> and cd to the sap-aas-abap-ase-syb/cli folder.

```
$ git clone https://github.com/IBM-Cloud/sap-aas-abap-ase-syb
cd sap-aas-abap-ase-syb/cli/
```

SAP HANA 2.0: Clone the solution repository from <https://github.com/IBM-Cloud/sap-abap-hana-aas> and cd to the sap-abap-hana-aas folder.

```
$ git clone https://github.com/IBM-Cloud/sap-abap-hana-aas.git
cd sap-abap-hana-aas/
```

3. Modify the `input.auto.tfvars` file to specify the information for the existing VPC, your region, zone, networking component names, hostname for the AAS VSI,profile, and image. You need your 40-digit SSH key ID for this file. The second SSH key is optional. For more options for profile, see [Instance Profiles](#). For more options, see [Images](#). For descriptions of the variables, see the [readme](#) file.

The VSI OS images that are supported for this solution for Netweaver Additional Application Server are:

- ibm-redhat-8-4-amd64-sap-applications-2
- ibm-redhat-8-6-amd64-sap-applications-2
- ibm-sles-15-3-amd64-sap-applications-2
- ibm-sles-15-4-amd64-sap-applications-4

```
$ # Infra VPC variables for ASE SYB
REGION    = "eu-de"
ZONE      = "eu-de-2"
VPC       = "ic4sap"                      # EXISTING Security group name
SECURITY_GROUP = "ic4sap-securitygroup"     # EXISTING Security group name
RESOURCE_GROUP = "wes-automation"
SUBNET    = "ic4sap-subnet"                 # EXISTING Subnet name
SSH_KEYS   = [ "r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a" , "r010-3fcfd9fe7-d4a7-41ce-8bb3-
d96e936b2c7e" ]

# SAP AAS VSI variables:
```

```

HOSTNAME = "sapnwase-as01"
PROFILE = "bx2-4x16"
IMAGE = "ibm-redhat-8-4-amd64-sap-applications-2

$ # Infra VPC variables for ABAP HANA
REGION      = "eu-de"
ZONE        = "eu-de-2"
VPC          = "ic4sap" # EXISTING Security group name
SECURITY_GROUP = "ic4sap-securitygroup" # EXISTING Security group name
RESOURCE_GROUP = "wes-automation"
SUBNET       = "ic4sap-subnet" # EXISTING Subnet name
SSH_KEYS     = [ "r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a" , "r010-3fc9fe7-d4a7-41ce-8bb3-d96e936b2c7e" ]
ID_RSA_FILE_PATH = "ansible/id_rsa"

# SAP AAS variables:
HOSTNAME = "sapnwapp"
PROFILE = "bx2-4x16"
IMAGE = "ibm-redhat-8-6-amd64-sap-applications-2"

```

4. Customize your SAP system configuration. In the same file, input.auto.tfvars, edit the SAP system configuration variables that are passed to the Ansible automated deployment. For descriptions of the variables, see the [readme](#) file.

```

$ # SAP system configuration - for ASE SYB
sap_sid = "NWD"
sap_ci_host = "10.243.132.10"
sap_ci_hostname = "sapnwase"
sap_ci_instance_number = "00"
sap_asc_s_instance_number = "01"
sap_aas_instance_number = "00"

# Kits paths
kit_sapcar_file = "/storage/NW75SYB/SAPCAR_1010-70006178.EXE"
kit_swpm_file = "/storage/NW75SYB/SWPM10SP31_7-20009701.SAR"
kit_saphotagent_file = "/storage/NW75SYB/SAPHOSTAGENT51_51-20009394.SAR"

```

```

$ # SAP system configuration - for ABAP HANA
sap_sid = "NWD"
sap_ci_host = "10.243.132.10"
sap_ci_hostname = "sapnwapp01"
sap_ci_instance_number = "00"
sap_asc_s_instance_number = "01"
hdb_instance_number = "00"
sap_aas_instance_number = "00"

# Kits paths
kit_sapcar_file = "/storage/NW75HDB/SAPCAR_1010-70006178.EXE"
kit_swpm_file = "/storage/NW75HDB/SWPM10SP31_7-20009701.SAR"
kit_saphotagent_file = "/storage/NW75HDB/SAPHOSTAGENT51_51-20009394.SAR"
kit_hdbclient_file = "/storage/NW75HDB/IMDB_CLIENT20_009_28-80002082.SAR"

```

Ansible decompresses the rest of the SAP kit files. For more information, see the [readme](#) file.

5. Initialize the Terraform CLI.

```
terraform init
```

6. Create a Terraform execution plan. The Terraform execution plan summarizes all the actions that are done to create the virtual private cloud instance in your account.

```
terraform plan plan1
```

Enter an SAP main password and your API key.

The SAP main password must be 10 - 14 characters long and contain at least one digit (0-9). It can contain only the following characters: a-z, A-Z, 0-9, @, #, \$, . *This password cannot contain exclamation points '!'. The password must not start with a digit or an underscore ().*

7. Verify that the plan shows all of the resources that you want to create and that the names and values are correct. If the plan needs to be adjusted, edit the input.auto.tfvars file to correct resources and run terraform plan again.
8. Apply the saved plan.

```
$ terraform apply "plan1"
```

The virtual private cloud and components are created and you see output similar to the `terraform plan` output.

9. Add the SAP credentials and the virtual server instance IP to the SAP GUI. For more information about the SAP GUI, see [SAP GUI](#).

Next steps

If you need to rename your resources after they are created, modify the `input.auto.tfvars` file to change the names and run `terraform plan` and `terraform apply` again. Do not use the IBM Cloud Dashboard and user interface to modify your VPC after it is created. The Terraform scripts create a complete solution and selectively modifying resources with the user interface might cause unexpected results.

If you need to remove the SAP Netweaver 7.X on HANA or AnyDB installation, go to your project folder and run `terraform destroy`. The `terraform destroy` command does not remove the VPC in this scenario because the VPC was created before these Terraform scripts were run.

Related information

For more information about Terraform on IBM Cloud, see [Getting started with Terraform on IBM Cloud](#).

For more information about using Terraform for creating only a VPC for SAP, without the SAP architecture, see [Creating single-tier virtual private cloud for SAP by using Terraform](#).

SAP One Support Notes that apply to this document:

- [SAP Note 84555 - Windows Server, Linux®, and UNIX: Certified hardware](#)
- [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#)
- [SAP Note 2923773 - Linux® on IBM Cloud \(IaaS\): Adaption of your SAP license](#)
- [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#)
- [SAP Note 2369910 - SAP Software on Linux®: General information](#)
- [SAP Note 171380 - Released IBM hardware \(Intel processors\) and IBM cloud services offers](#)
- [SAP Note 1380654 - SAP support in IaaS environments](#)

This document is referenced by:

- [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#)
- [SAP Note 2588225 - SAP on IBM Cloud: Protect against speculative execution vulnerabilities](#)
- [SAP Note 1380654 - SAP support in IaaS environments](#)
- [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#)

SAP HANA stand-alone VSI in VPC

Automating SAP workload HA deployment on IBM Cloud VPC with Terraform and Ansible

You can use Terraform to automate IBM Cloud® VPC provisioning. The VPC provisioned includes virtual server instances with high network performance. The VPC infrastructure contains various Infrastructure-as-a-Service (IaaS) offerings, including virtual servers. After the VPC is provisioned, the scripts use the Ansible Playbooks to install the SAP system.

IBM Cloud VPC introduction

VPC is a public cloud offering that an enterprise uses to establish its own private cloud-like computing environment on shared [public cloud](#) infrastructure. VPC gives an enterprise the ability to define and control a virtual network that is logically isolated from all other public cloud tenants, creating a private and secure place on the public cloud.

Imagine that a cloud provider's infrastructure is a residential apartment building and multiple families live inside. A public cloud tenant is a kind of sharing an apartment with a few roommates. In contrast, having a VPC is like having your own private condominium; no one else has the key, and no one can enter the space without your permission.

VPC's logical isolation is implemented by using virtual network functions and security features that give the enterprise customer granular control over which IP addresses or applications can access particular resources. It is analogous to the "friends-only" or "public/private" controls on social media accounts used to restrict who can or can't see your otherwise public posts.

With IBM Cloud VPC, you can use the UI, CLI, and API to manually provision virtual server instances for VPC with high network performance. VPC infrastructure contains various Infrastructure-as-a-Service (IaaS) offerings including virtual servers for VPC.

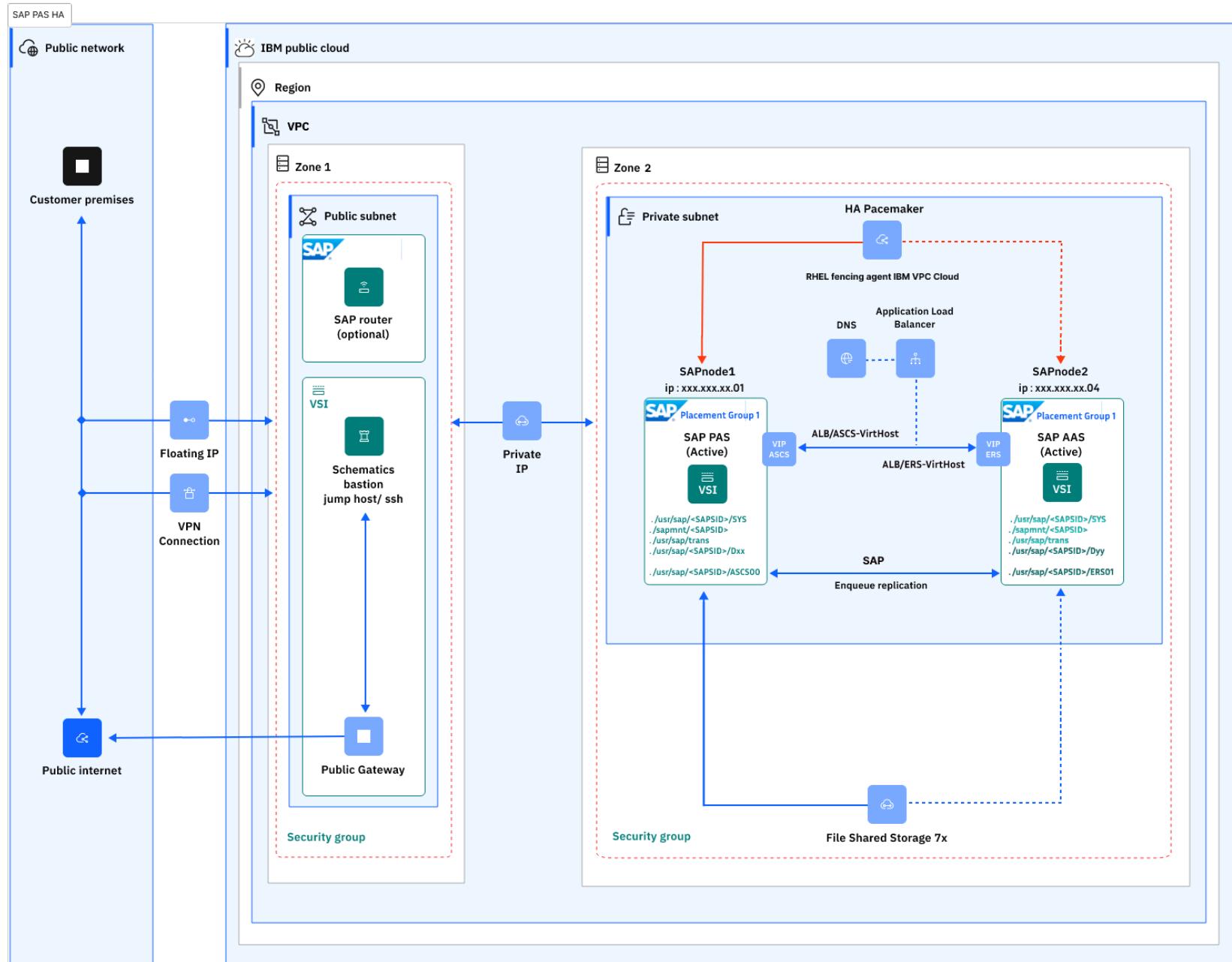
Use the following information to understand a simple use-case for planning, creating, and configuring resources for your VPC, and learn more about VPC overviews and VPC tutorials. For more information about the VPC, see [Getting started with Virtual Private Cloud \(VPC\)](#).

SAP products architecture on IBM Cloud VPC

A [Virtual Private Cloud \(VPC\)](#) contains one of the most secure and reliable cloud environments for SAP applications within your own VPC with virtual server instances. This represents an Infrastructure-as-a-Service (IaaS){: external} within IBM Cloud that offers all the benefits of isolated, secure, and flexible virtual cloud infrastructure from IBM. In comparison, the IBM Cloud classic infrastructure virtual servers offering uses virtual instances with native and VLAN networking to communicate with each other within a data center; however, the instances are restricted in one well-working pod by using subnet and VLAN networking as a gap scale up of virtual resources should rely between the pods. The IBM Cloud VPC network orchestrator layer concept eliminates the pod boundaries and restrictions, so this new concept handles all the networking for every virtual instance running within VPC across regions and zones.

Highly available system for SAP NetWeaver on IBM Cloud VPC

In a Highly Available (HA) system, every instance can run on a separate IBM Cloud virtual server instance. The cluster HA configuration for the SAP application server consists of two virtual server instances, each of them located in the same zone within the region by using placement groups. Placement groups assure that both cluster resources and cloud resources are also located in different compute nodes as specified in the following placement groups section:



SAP HA for SAP applications cluster nodes PAS (Active) and AAS (Active)

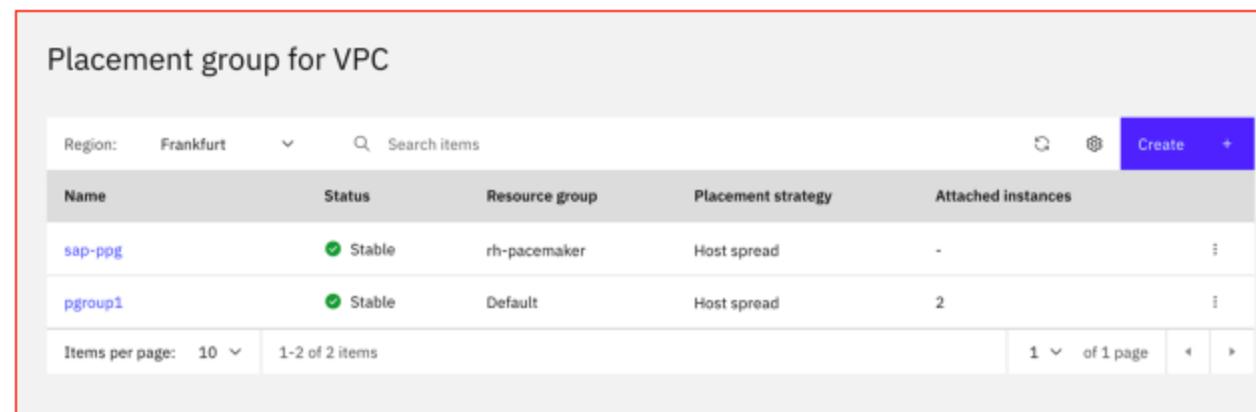
Placement groups on IBM Cloud VPC for SAP HA architecture

Placement Groups (PG) for VPC have two different anti-affinity strategies for high availability. By using the placement strategies, you minimize the chance of service disruption with virtual server instances that are placed on different hosts or into an infrastructure with separate power and network supplies.

The design of placement groups for IBM Cloud virtual servers solves this issue. Placement groups give a measure of control over the host on which a new public virtual server is placed. In this release, a “spread” rule is implemented, which means that the virtual servers within a placement group are spread onto different hosts. You can build a highly available application within a data center and know that your virtual servers are isolated from each other.

Placement groups with the spread rule are available to create in selected IBM Cloud data centers. After a spread rule is created, you can provision a virtual server into that group and ensure that it is not on the same host as any of your other virtual servers. This feature comes with no cost.

You can create your placement group and assign up to four new virtual server instances. With the spread rule, each of your virtual servers are provisioned on different physical hosts. In the following configuration example, the “Power Spread” option is used:



Placement groups host spread

Placement group for VPC					
Name	Status	Resource group	Placement strategy	Attached instances	
sapha-poc	Stable	wes-ic4sap-resourcegroup	Power spread	4	⋮
Items per page: 10 1 item 1 of 1 page ⋮					

Placement groups power spread

Following are the SAP instances that are required for HA scenario:

- ABAP SAP Central Services (ASCS) instance - contains the ABAP message server and the ABAP enqueue server.
- Enqueue Replication Server (ERS) instance for the ASCS instance.
- Database instance
- Primary Application Server (PAS) instance on node 1.
- Additional Application Server (AAS) instance on node 2.



Note: It is recommended to run both the ASCS instance and the ERS instance in a switchover cluster infrastructure.

IBM Cloud File Storage for VPC for SAP HA architecture

[IBM Cloud File Storage for VPC](#) technology is used to make the SAP directories available to the SAP system. The technologies of choice are NFS, shared disks, and cluster file system. If you have decided to use the HA solution for your SAP system, make sure that you properly address the HA requirements of the SAP file systems in your SAP environment.

File shares for VPC								
Name	Status	Resource groups	Location	Mount targets	Size	Replication role	Encryption type	
usrsap-as1-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	⋮
usrsap-as2-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	⋮
usrsap-sapsacs-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	⋮
usrsap-sapers-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	⋮
usrsap-sapmnt-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	⋮
usrsap-sapsys-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	⋮
usrsap-trans-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	80 GB	None	Provider managed	⋮

File shares for VPC

- File shares that are mounted as NFS permanent file systems on both cluster nodes for SAP HA application:
 - `/usr/sap/<SAPSID>/SYS`
 - `/sapmnt<SAPSID>`
 - `/usr/sap/trans`
- Cluster-managed file systems for SAP HA application: ASCS
 - `/usr/sap/<SAPSID>/ASCS00`
 - `/usr/sap/<SAPSID>/ERS01`
- Permanent NFS mount on SAP HA application node 1 PAS instance:
 - `/usr/sap/<SAPSID>/Dxx`
- Permanent NFS mount on SAP HA application node 2 dialog instance:
 - `/usr/sap/<SAPSID>/Dyy`

Prerequisites

You need to install the hardware (hosts, disks, and network) and decide how to distribute the database, SAP instances, and if required, the Network File System (NFS) server over the cluster nodes.

Context

Following are the types of SAP directories:

- Physically shared directories: `/<sapmnt>/<SAPSID>` and `/usr/sap/trans`

- Logically shared directories that are bound to a node, such as `/usr/sap`, with the following local directories:
 - `/usr/sap/<SAPSID>`
 - `/usr/sap/<SAPSID>/SYS`
 - `/usr/sap/hostctrl`
- Local directories that contain the SAP instances such as `/usr/sap/<SAPSID>/ASCS<Instance_Number>`
- The global transport directory may reside on a separate SAP transport host as a standard three systems transport layer configuration.

You need at least two nodes and a shared file system for distributed ASCS and ERS instances. The assumption is that the rest of the components are distributed on other nodes.

ASCS and ERS installation

In order for the ASCS and ERS instances to be able to move from one node to the other, they need to be installed on a shared file system and use virtual hostnames based on the virtual IP.

In this VPC-based SAP HA solution, the shared file system that is required by the cluster is replaced by the NFS-mounted file storage, and the virtual IP is replaced by the Application Load Balancer for VPC (ALB).

In this scenario, three ALBs are used, one for each Single Point of Failure (SPOF) component in order to replace the virtual IP requirement: ALB for ASCS, ALB for ERS, and ALB for ASE Sybase. Each ALB is configured as a backend for the corresponding cluster servers and redirects all of the communication that is received on the front-end ports to the active server in the backend pool.

Load balancers for VPC						
Region:	Frankfurt	▼	<input type="text"/> poc	X		
Name	Status	Family	Resource group	Type	Hostname	Location
db-alb-hana-poc	Active	Application	wes-ic4sap-resourcegroup	Private	20bdd130-eu-de.lb.appdomain.cloud	Frankfurt
sap-alb-ers-poc	Active	Application	wes-ic4sap-resourcegroup	Private	3941d983-eu-de.lb.appdomain.cloud	Frankfurt
sap-alb-ascs-poc	Active	Application	wes-ic4sap-resourcegroup	Private	56a9190d-eu-de.lb.appdomain.cloud	Frankfurt

Application load balancer management of HA IPs mechanism

Private application load balancer

A [private application load balancer](#) is accessible through your private subnets that you configured to create the load balancer.

Similar to a public application load balancer, your private application load balancer service instance is assigned an FQDN; however, this domain name is registered with one or more private IP addresses.

IBM Cloud operations change the number and value of your assigned private IP addresses over time, based on maintenance and scaling activities. The backend virtual server instances that host your application must run in the same region and under the same VPC.

Use the assigned ALB FQDN to send traffic to the private application load balancer to avoid connectivity problems to your applications during system maintenance or scaling down activities.

Each ALB sends traffic to the cluster node where the application (ASCS, ERS, ASE Sybase DB) is running. During the cluster failover, the ALB redirects all the traffic to the new node where the resources are up and running.



Note: DNS-as-a-Service (DNSaaS) is the management IBM Cloud VPC DNS service of HA and FQDN (IPs) mechanism.



Note: The ALB has a default of 50 seconds for client and server timeout, so after 50 seconds of inactivity, the connection is closed. To support SAP connections through ALB and not lose connection after 50 seconds, you need to request a change this value to a minimum of 300 seconds (client-side idle connection = minimum 300s and server-side idle connection = minimum 300s). To request this change, open a support ticket. This is an account-wide change that affects all of the ALBs in your account. For more information, see [Connection timeouts](#).

DNS Services with VPC

[IBM Cloud DNS Services](#) provide private DNS to VPC users. Private DNS zones are resolvable only on IBM Cloud and from explicitly [permitted networks](#) in an account. To get started, create a DNS Services instance by using the IBM Cloud console.

DNS Services allows you to:

- Create the private DNS zones that are collections for holding the domain names.
- Create the DNS resource records under these DNS zones.
- Specify the access controls used for the DNS resolution of resource records on a zone-wide level.

DNS Services also maintains its own worldwide set of DNS resolvers. Instances that are provisioned under IBM Cloud on an IBM Cloud network can use resource records that are configured through IBM Cloud DNS Services by querying DNS Services resolvers.

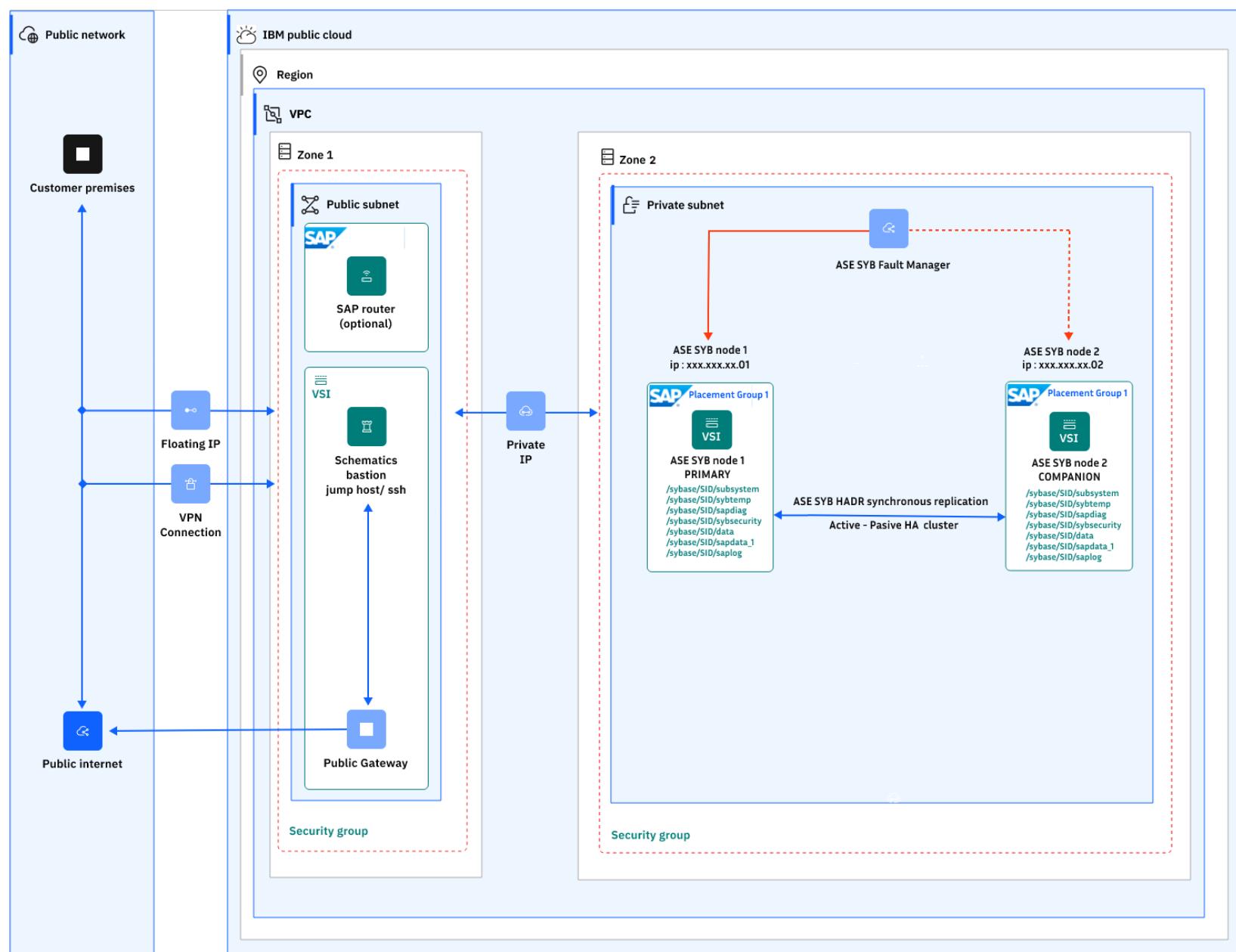
Resource records and zones that are configured through DNS Services are:

- Separated from the wider public DNS, and their publicly accessible records.
- Hidden from the system outside of and not part of the IBM Cloud private network.
- Accessible only from the system that you authorize on the IBM Cloud private network.
- Resolvable only via the resolvers provided by the service.

The DNS service maps the FQDN of each ALB to the virtual hostnames of the ASCS, ERS, and ASE Sybase that are used by SAP applications.

Type	Name	Value	TTL
CNAME	dbpochana	is an alias of 20bdd130-eu-de.lb.appdomain.cloud	12 hr
CNAME	sappocers	is an alias of 3941d983-eu-de.lb.appdomain.cloud	12 hr
CNAME	sappocases	is an alias of 56a9190d-eu-de.lb.appdomain.cloud	12 hr

Highly available system for SAP ASE Sybase database with HADR system



SAP HA for ASE Sybase DB instances cluster nodes primary (Active) and Secondary (Companion)

At the most basic level, a standard HA ASE Sybase cluster in an active(primary)-passive(companion) configuration has two nodes: one is the primary node and the other is the standby node. This means that the primary node is actively serving the active SAP DB instances (Primary and Companion), while the standby node is waiting to jump in if there is any failure.

The cluster is set with a virtual hostname IP (hostname is mapped to the FQDN of the ASE Sybase ALB through DNS, which is the same as

explained previously for SAP ASCS and ERS instances). Application instances (PAS and AAS) are used on the SAP profiles to call that particular component. The cluster assigns the virtual IP to the active node and uses a heartbeat monitor to confirm the availability of the components. If the primary node stops responding, it triggers the automatic failover mechanism that calls the standby node to step up to become the primary node. The ALB detects the change, redirects the traffic to the new active node, and assigns the virtual IP to it, restoring the component availability. Once fixed, the failed node comes online as a standby node.

SAP Sybase HADR system supports synchronous replication

The SAP Sybase HADR system supports synchronous replication between the primary and standby servers for high availability. An active-active setup is a two-node configuration where both nodes in the cluster include SAP ASE managing independent workloads, capable of taking over each others workload in the event of a failure.

The SAP ASE server that takes over the workload is called a secondary companion, and the SAP ASE server that fails is called the primary companion. Together they are companion servers. This movement from one node to another is called failover. After the primary companion is ready to resume its workload, it is moved back to its original node. This movement is called a failback.

When a system fails over, clients that are connected to the primary companion and use the failover property automatically reestablish their network connections to the secondary companion. You must tune your operating system to successfully manage both servers during fail over. See your operating system documentation for information about configuring your system for high availability. An SAP ASE configured for failover in an active-active setup can be shut down using the shutdown command only after you have suspended SAP ASE from the companion configuration, at both the server level and the platform level.

The always-on option in a High Availability and Disaster Recovery (HADR) system consists of two SAP ASE servers:

- Primary on which all transaction processing takes place.
- Warm standby (referred to as a "standby server" in DR mode, and as a "companion" in HA mode) for the primary server, and contains copies of designated databases from the primary server.



Note: The HADR feature that is shipped with SAP ASE version 16.0 SP02 supports only a single-companion server.

Some high-availability solutions (for example, the SAP Adaptive Server Enterprise Cluster Edition) share or use common resources between nodes. However, the HADR system is a "shared nothing" configuration, each node has separate resources including disks.

In an HADR system, servers are separate entities and data is replicated from the primary server to the companion server. If the primary server fails, a companion server is promoted to the role of primary server either manually or automatically. Once the promotion is complete, clients can reconnect to the new primary server, and see all committed data, including data that was committed on the previous primary server.

Servers can be separated geographically, which makes an HADR system capable of withstanding the loss of an entire computing facility.



Note: The HADR system includes an embedded SAP Replication Server, which synchronizes the databases between the primary and companion servers. SAP ASE uses the Replication Management Agent (RMA) to communicate with Replication Server and SAP Replication Server uses Open Client connectivity to communicate with the companion SAP ASE.

The Replication Agent detects any data changes made on the primary server and sends them to the primary SAP Replication Server. In the figure above, the unidirectional arrows indicate that, although both SAP Replication Servers are configured, only one direction is enabled at a time.

The HADR system supports synchronous replication between the primary and standby servers for high availability so the two servers can keep in sync with Zero Data Loss (ZDL). This requires a network link that is fast enough between the primary and standby server so that synchronous replication can keep up with the primary servers workload. Generally, this means that the network latency is approximately the same speed as the local disk IO speed, a few (fewer than 10) milliseconds. Anything longer than a few milliseconds may result in a slower response to write operations at the primary.

The HADR system supports asynchronous replication between the primary and standby servers for disaster recovery. The primary and standby servers by using asynchronous replication can be geographically distant, meaning they can have a slower network link. With asynchronous replication, Replication Agent Thread captures the primary servers workload, which is delivered asynchronously to SAP Replication Server. The SAP Replication Server applies these workload change to the companion server.

The most fundamental service that is offered by the HADR system is the failover; planned or unplanned from the primary to the companion server, which allows maintenance activity to occur on the old primary server, while applications continue on the new primary.

The HADR system provides protection in the event of a disaster. If the primary server is lost, the companion server can be used as a replacement. Client applications can switch to the companion server, and the companion server is quickly available for users. If the SAP Replication Server was in synchronous mode before the failure of the primary server, the Fault Manager automatically initiates failover with

zero data loss.

Fault Manager installation on the SAP ASCS node

The required parameters are asked during the installation process to create a profile for the fault manager and then adds it to the instance start profile. It is also possible to run the installation by using an existing profile: `sybdbfm install pf=<SYBHA.PFL>` In this case, the installation process will only ask for profile parameters missing in the profile.



Note: Fault manger is integrated with ASCS on same SAP PAS/AAS cluster (start/stop/move together).

There may be some data loss if the SAP Replication Server was in asynchronous mode and you must use manual intervention to failover for disaster recovery.

Connection attempts to the companion server without the necessary privileges are silently redirected to the primary companion via the login redirection mechanism, which is supported by Connectivity libraries. If login redirection is not enabled, client connections fail and are disconnected.

The SAP ASE HADR option installs the below components:

- SAP ASE
- SAP Replication Server
- Replication Management Agent (RMA)
- SAP Host Agent
- Fault Manager
- SAP ASE Cockpit



Note: This automation is offered at no cost; however, the provisioned infrastructure comes at cost.

VPC with Additional Application Server (AAS) ABAP on Linux for SAP HANA

You can use Terraform scripts to create a single-tier VPC and create the AAS to HANA and AnyDB infrastructure on the VPC. The Terraform scripts use the VPC information that you provide and then call the Ansible playbook to create the SAP architecture on the specified VPC. Terraform on IBM Cloud® enables predictable and consistent provisioning of IBM Cloud Virtual Private Cloud (VPC) infrastructure resources so that you can rapidly build complex, cloud environments. IBM Cloud VPC infrastructure consists of SAP certified hardware that uses Intel® Xeon CPUs and more Intel® technologies.

You have two deployment methods to choose from:

- Terraform scripts that run from the CLI on your bastion server.
- Schematics user interface accessed from your cloud dashboard menu.

You can create SAP AAS NetWeaver 7.x on the SAP HANA-based ABAP stack.

SAP solution implemented

Many SAP enterprise solutions are built on the SAP platform (SAP NetWeaver) including:

- SAP HANA as Primary Persistence for SAP NetWeaver-based applications
- SAP Business Suite applications (ERP, CRM, and SCM, and other applications),
- SAP Business Warehouse (BW), and
- Other SAP enterprise solutions

SAP NetWeaver has two distinct aspects, ABAP and Java. Many applications that are built on the SAP NetWeaver's ABAP or Java (or both) application servers run on SAP DB owned HANA and ASE Sybase either in AnyDB platforms (MSSQL, Oracle, and Db2).

Technical interfaces are available for applications that are built on the SAP NetWeaver AS ABAP and AS Java to run on SAP HANA and AnyDB. However, specific development enablement is normally required for each application to ensure that it runs optimally on the SAP HANA. SAP Business Suite applications (ERP, CRM, SCM, and other applications), SAP Business Warehouse (BW), and other SAP NetWeaver-based applications were modified to run on SAP HANA and have many advantages. Also, various components and complimentary applications that are built on SAP NetWeaver can also run on SAP HANA or AnyDB by using the provided SAP NetWeaver DB interfaces.

The SAP HANA as primary persistence for SAP NetWeaver-based applications scenario has one restriction: SAP NetWeaver ABAP and Java

application servers must run on separate hardware servers from the SAP HANA hardware.

What is created

The scripts automate the virtual infrastructure resources, provisioning the processes for the SAP architecture in an existing VPC with a distributed environment. SAP AAS NetWeaver 7.x (HANA or ASE SYB) application server on a distinct VSI VPC system and SAP HANA DB on a dedicated server type VSI VPC box are provisioned. The scripts work in two phases.

During the first phase of [Automate SAP bastion server – SAP media storage repository](#), the following virtual infrastructure resources based on the components from the existing VPC created by the bastion server are:

- 1 VPC where the virtual server instance is provisioned.
- 1 security group. The rules for this security group are:
 - Allow inbound DNS traffic (port 53).
 - Allow inbound SSH traffic (TCP port 22).
 - Allow all outbound traffic from the virtual server instance.
 - Allow all traffic in the security group.
- 1 subnet to enable the networking in your VPC.
- 2 virtual server instances with SAP certified storage and network configurations.
- 1 floating IP address used to access your VPC virtual server instance over the public network.

During the second phase, the Ansible Playbooks is called and the SAP architecture is installed for both dedicated virtual server instance (VSI) SAP application; VSI system and dedicated SAP HANA VSI box. The SAP architecture that is deployed on the SAP NetWeaver 7.x release is a stand-alone dedicated SAP HANA 2.0 box release. For more information about this architecture, see [Automating SAP HANA stand-alone virtual server instance on IBM Cloud® VPC by using Terraform and Ansible](#).

You can provision only one instance of the service per IBM Cloud region.

Schematics deployment

When you run the scripts with the Schematics interface, you:

- Enter the workspace information.
- Enter the GitHub path for the chosen solution either on NetWeaver AAS for HANA.
- Modify the parameters in the Schematics interface. They are the same parameters as the `input.auto.tfvars` file that you use with the cli.

Virtual server instance configuration

Following are the supported operating system images for SAP NetWeaver primary application server:

- ibm-redhat-8-4-amd64-sap-applications-2
- ibm-redhat-8-6-amd64-sap-applications-2
- ibm-sles-15-3-amd64-sap-applications-2
- ibm-sles-15-4-amd64-sap-applications-3

Following are the supported operating system images for SAP HANA database:

- ibm-redhat-8-4-amd64-sap-hana-2
- ibm-redhat-8-6-amd64-sap-hana-2
- ibm-sles-15-3-amd64-sap-hana-2
- ibm-sles-15-4-amd64-sap-hana-1

For both server instances there are:

- Two SSH keys are configured to access SSH as `root`.
- Three storage volumes as described in the `input.auto.tfvars` file.

What is created for anydb

The scripts use the information that you provide for an existing VPC and deploy AAS to SAP HANA or AnyDB on a different host than CI (SAP Central Instance) VSI host. For more information about this architecture, see [SAP NetWeaver 7.x on UNIX with HANA or AnyDB on IBM Cloud](#)

[VPC on IBM Cloud VPC](#). You specify the information for the VPC to use in the `input.auto.tfvars` file.

The scripts call the Ansible Playbooks to install the SAP architecture.

Script files

The configuration and script files are provided on GitHub. Each supported interface for the SAP solution installation has its own folder in the GitHub repository:

- [GitHub repository for Terraform – AAS HANA](#)

Terraform interface

To run the Terraform script, you modify:

- The `input.auto.tfvars` file to specify the existing VPC resources for your solution. Specify the variables for the existing VPC:
 - VPC name
 - Security group
 - Subnet
 - Hostname
 - Profile
 - Image
 - Up to two SSH keys

You can change the default SAP system configuration settings to match your solution. You can also specify the location where you downloaded the SAP kits.

The IBM Cloud Provider plug-in for Terraform on IBM Cloud uses these configuration files to install AAS to SAP HANA and AnyDB on the specified VPC in your IBM Cloud account.

Support

There are no warranties of any kind, and there is no service or technical support available for these materials from IBM®. As a recommended practice, review carefully any materials that you download from this site before using them on a live system.

Though the materials provided herein are not supported by the IBM® Service organization, your comments are welcomed by the developers, who reserve the right to revise, readapt or remove the materials at any time. To report a problem, or provide suggestions or comments, open a GitHub issue.

Before you begin

Before you use the scripts in the bastion cli:

- Set up your account to access the VPC. Make sure that your account is [upgraded to a paid account](#).
- If you have not already, create a Bastion server to store the SAP kits. For more information, see [Automate SAP bastion server - SAP media storage repository](#).
- Download the SAP kits from the SAP Portal to your Deployment Server. Make note of the download locations. Ansible decompresses the files. For more information, see the [readme](#) file.
- [Create or retrieve an IBM Cloud API key](#). The API key is used to authenticate with the IBM Cloud platform and to determine your permissions for IBM Cloud services.
- [Create or retrieve your SSH key ID](#). You need the 40-digit UUID for the SSH key, not the SSH key name.
- Terraform should already be installed on the bastion server that you deployed. For more information, see [Bastion server for SAP deployment](#).
- (Optional - Catalog Tile) create secrets for your credentials and passwords by using the [Secrets Manager](#).

Deploying SAP AAS NetWeaver 7.x on HANA by using the Schematics user interface

Use these steps to configure the SAP Additional Application Server (AAS) NetWeaver with HANA or AnyDB on your existing VPC by using the Schematics interface. The script takes 2 - 3 hours to complete.

1. From the IBM Cloud menu, select **Schematics**.
2. Click **Create** workspace.

3. On the **Specify template** page:
 - Enter the URL for the Schematics interface.
 - Select the **Terraform version** that is listed in the readme file.
 - Click **Next**.
4. On the **workspace details** page:
 - Enter a name for the workspace.
 - Select a **Resource group**.
 - Select a **Location** for your workspace. The workspace location does not have to match the resource location.
 - Select **Next**.
5. Select **Create** to create your workspace.
6. On the workspace settings page, in the input variables section, review the default input variables and provide values that match your solution.

For a more detailed description of each parameter, check the GitHub repo [AAS HANA readme](#) file, chapter “Input parameter file”. Also, make sure to mark the parameters that contain sensitive information like passwords, API, and ssh private keys as “sensitive”. These parameters are marked as “sensitive” in the readme file, under “Input parameter file”.
7. On the workspace settings page, click **Generate plan**. Wait for the plan to complete.
8. Click **View log** to review the log files of your terraform execution plan.
9. Apply your Terraform template by clicking **Apply plan**.
10. Review the log file to ensure that no errors occur during the provisioning, modification, or deletion process.

Deploying SAP AAS NetWeaver (ABAP) on HANA with the Deployable Architecture tile interface

Use these steps to configure the SAP AAS NetWeaver (ABAP) on HANA on your existing VPC by using the catalog tile interface. The script takes 2 - 3 hours to complete.

1. From the IBM Cloud catalog, select **VPC with Additional Application Server ABAP on Linux for SAP HANA** on HANA tile. The **Create** tab opens for VPC with Additional Application Server ABAP on Linux for SAP HANA. For more information about this deployment, see the About tab or the readme file link.
2. Select the latest version.
3. Select **VPC with Additional Application Server ABAP on Linux for SAP HANA on Deployable Architecture tile** variation.
4. Click **Review deployment** options:
 - **Add to project** to add this deployment to an IBM Cloud project and combine it with other deployments. IBM Cloud projects include several more pipeline steps before deployment, including deployment validation, cost calculation, compliance verification, and approval process.
 - **Create from the CLI** to get the CLI command. With this command you can trigger the deployment from the CLI.
 - **Work with code** to embed the code into other terraform deployments.
 - **Deploy with IBM Cloud Schematics** to trigger the deployment process directly.
5. Select **Deploy with IBM Cloud Schematics**.
6. Add the input parameters for this installation. There are 3 categories of parameters:
 - **Workspace** - These parameters define the workspace that is automatically created in Schematics:
 - Enter a name for the workspace or use the default name.
 - The Resource Group used to create resources. Use default or create a Resource Group.
 - Select a location to create your Schematics workspace. The workspace location need not match the resource location.
 - **Required input variables** - Review the default input variables and provide values that match your solution. These parameters are specific to your deployment. For more detailed information, see the [Readme file](#).

Parameter	Description
BASTION_FLOATING_IP	Required only for Schematics Deployments. The Floating IP from the Bastion Server.

HOSTNAME	The hostname for the VSI. The hostname should be up to 13 characters as required by SAP. For more information on the rules regarding hostnames for SAP systems, check SAP Note 611361: Hostnames of SAP ABAP Platform servers
REGION	The cloud region to deploy the solution. The regions and zones for VPC are listed here . Review supported locations in IBM Cloud Schematics here . Sample value: eu-de.
RESOURCE_GROUP	The name of an existing Resource Group for VSIs and Volumes resources. Default value: "Default". The list of Resource Groups is available here .
SECURITY_GROUP	The name of an existing Security group. The list of security groups is available here .
SSH_KEYS	The list of SSH Keys UUIDs that are allowed to SSH as root to the VSI can contain one or more IDs. The list of SSH Keys is available here . Sample input (use your own SSH UUIDs from IBM Cloud){: external}: ["r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a", "r010-3fcfd9fe7-d4a7-41ce-8bb3-d96e936b2c7e"]
SUBNET	The name of an existing subnet. The list of subnets is available here .
VPC	The name of an existing VPC. The list of VPCs is available here .
ZONE	The cloud zone where to deploy the solution. Sample value: eu-de-2.
ibmcloud_api_key	IBM Cloud API key (Sensitive* value).
private_ssh_key	Required only for Schematics Deployments - Input your id_rsa private key pair content in OpenSSH format (Sensitive* value). This private key should be used only during the terraform provisioning and it is recommended to be changed after the SAP deployment.
hdb_instance_number	The instance number of the SAP HANA database server.
sap_aas_instance_number	Technical identifier for the internal processes of the additional application server.
sap_ascs_instance_number	Technical identifier for the internal processes of ASCS.
sap_ci_host	IP address of the existing SAP Central Instance.
sap_ci_hostname	The hostname of the existing SAP Central Instance.
sap_ci_instance_number	Technical identifier for the internal processes of the Central Instance.
sap_sid	The SAP system ID identifies the entire SAP system.
sap_main_password	Common password for all users that are created during the installation (See Obs*).

Required Variables

- **Optional variables** - Review and update the optional input variables. The Ansible scripts expect the SAP kits to be in the default locations listed. For more information, see the [Readme file - Input Parameters](#).

Parameter	Description
ID_RSA_FILE_PATH	The file path for private_ssh_key is automatically generated by default. If it is changed, it must contain the relative path from Git repo folders. Default value: "ansible/id_rsa".
IMAGE	The OS image used for the VSI. A list of images is available here .
PROFILE	The profile used for the VSI. A list of profiles is available here . For more information about supported DB/OS and IBM Gen 2 Virtual Server Instances (VSI), check SAP Note 2927211: SAP Applications on IBM Virtual Private Cloud .

VOL1	Volume 1 Size - The size for the disks in GB that are to be attached to the VSI and used by SAP.
VOL2	Volume 2 Size - The size for the disks in GB that are to be attached to the VSI and used by SAP.
kit_sapcar_file	Path to the sapcar binary, as downloaded from SAP Support Portal.
kit_swpm_file	Path to the SWPM archive (SAR), as downloaded from SAP Support Portal.
kit_saphostagent_file	Path to the SAP Host Agent archive (SAR), as downloaded from SAP Support Portal.
kit_hdbclient_file	Path to the HANA DB client archive (SAR), as downloaded from SAP Support Portal.

Optional Variables

7. Accept the license agreement.
8. Select **Deploy**. The deployment starts and you are directed to the Schematics page that displays the script log files for you to monitor the deployment progress.

Creating the infrastructure using Terraform with the bastion server CLI

Use these steps to configure the IBM Cloud Provider plug-in and use Terraform to install SAP AAS to SAP HANA and AnyDB on your existing VPC on an already deployed SAP NetWeaver 7.X with SAP HANA 2.0 or ASE SYB as a Central Instance.

The script takes 1 - 2 hours to complete.

1. Access the bastion server cli.
2. Clone the solution repository and change to the folder.

ASE SYB 16 Clone the solution repository from <https://github.com/IBM-Cloud/sap-aas-abap-ase-syb> and cd to the sap-aas-abap-ase-syb/cli folder.

```
$ git clone https://github.com/IBM-Cloud/sap-aas-abap-ase-syb
cd sap-aas-abap-ase-syb/cli/
```

SAP HANA 2.0: Clone the solution repository from <https://github.com/IBM-Cloud/sap-abap-hana-aas> and cd to the sap-abap-hana-aas folder.

```
$ git clone https://github.com/IBM-Cloud/sap-abap-hana-aas.git
cd sap-abap-hana-aas/
```

3. Modify the `input.auto.tfvars` file to specify the information for the existing VPC, your region, zone, networking component names, hostname for the AAS VSI,profile, and image. You need your 40-digit SSH key ID for this file. The second SSH key is optional. For more options for profile, see [Instance Profiles](#). For more options, see [Images](#). For descriptions of the variables, see the [readme](#) file.

The VSI OS images that are supported for this solution for Netweaver Additional Application Server are:

- ibm-redhat-8-4-amd64-sap-applications-2
- ibm-redhat-8-6-amd64-sap-applications-2
- ibm-sles-15-3-amd64-sap-applications-2
- ibm-sles-15-4-amd64-sap-applications-4

```
$ # Infra VPC variables for ASE SYB
REGION    = "eu-de"
ZONE      = "eu-de-2"
VPC       = "ic4sap"                      # EXISTING Security group name
SECURITY_GROUP = "ic4sap-securitygroup"     # EXISTING Security group name
RESOURCE_GROUP = "wes-automation"
SUBNET    = "ic4sap-subnet"                 # EXISTING Subnet name
SSH_KEYS   = [ "r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a" , "r010-3fcfd9fe7-d4a7-41ce-8bb3-
d96e936b2c7e" ]

# SAP AAS VSI variables:
```

```

HOSTNAME = "sapnwase-as01"
PROFILE = "bx2-4x16"
IMAGE = "ibm-redhat-8-4-amd64-sap-applications-2

$ # Infra VPC variables for ABAP HANA
REGION      = "eu-de"
ZONE        = "eu-de-2"
VPC          = "ic4sap" # EXISTING Security group name
SECURITY_GROUP = "ic4sap-securitygroup" # EXISTING Security group name
RESOURCE_GROUP = "wes-automation"
SUBNET       = "ic4sap-subnet" # EXISTING Subnet name
SSH_KEYS     = [ "r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a" , "r010-3fc9fe7-d4a7-41ce-8bb3-d96e936b2c7e" ]
ID_RSA_FILE_PATH = "ansible/id_rsa"

# SAP AAS variables:
HOSTNAME = "sapnwapp"
PROFILE = "bx2-4x16"
IMAGE = "ibm-redhat-8-6-amd64-sap-applications-2"

```

4. Customize your SAP system configuration. In the same file, input.auto.tfvars, edit the SAP system configuration variables that are passed to the Ansible automated deployment. For descriptions of the variables, see the [readme](#) file.

```

$ # SAP system configuration - for ASE SYB
sap_sid = "NWD"
sap_ci_host = "10.243.132.10"
sap_ci_hostname = "sapnwase"
sap_ci_instance_number = "00"
sap_asc_s_instance_number = "01"
sap_aas_instance_number = "00"

# Kits paths
kit_sapcar_file = "/storage/NW75SYB/SAPCAR_1010-70006178.EXE"
kit_swpm_file = "/storage/NW75SYB/SWPM10SP31_7-20009701.SAR"
kit_saphotagent_file = "/storage/NW75SYB/SAPHOSTAGENT51_51-20009394.SAR"

```

```

$ # SAP system configuration - for ABAP HANA
sap_sid = "NWD"
sap_ci_host = "10.243.132.10"
sap_ci_hostname = "sapnwapp01"
sap_ci_instance_number = "00"
sap_asc_s_instance_number = "01"
hdb_instance_number = "00"
sap_aas_instance_number = "00"

# Kits paths
kit_sapcar_file = "/storage/NW75HDB/SAPCAR_1010-70006178.EXE"
kit_swpm_file = "/storage/NW75HDB/SWPM10SP31_7-20009701.SAR"
kit_saphotagent_file = "/storage/NW75HDB/SAPHOSTAGENT51_51-20009394.SAR"
kit_hdbclient_file = "/storage/NW75HDB/IMDB_CLIENT20_009_28-80002082.SAR"

```

Ansible decompresses the rest of the SAP kit files. For more information, see the [readme](#) file.

5. Initialize the Terraform CLI.

```
terraform init
```

6. Create a Terraform execution plan. The Terraform execution plan summarizes all the actions that are done to create the virtual private cloud instance in your account.

```
terraform plan plan1
```

Enter an SAP main password and your API key.

The SAP main password must be 10 - 14 characters long and contain at least one digit (0-9). It can contain only the following characters: a-z, A-Z, 0-9, @, #, \$, . *This password cannot contain exclamation points '!'. The password must not start with a digit or an underscore ().*

7. Verify that the plan shows all of the resources that you want to create and that the names and values are correct. If the plan needs to be adjusted, edit the input.auto.tfvars file to correct resources and run terraform plan again.
8. Apply the saved plan.

```
$ terraform apply "plan1"
```

The virtual private cloud and components are created and you see output similar to the `terraform plan` output.

9. Add the SAP credentials and the virtual server instance IP to the SAP GUI. For more information about the SAP GUI, see [SAP GUI](#).

Next steps

If you need to rename your resources after they are created, modify the input.auto.tfvars file to change the names and run `terraform plan` and `terraform apply` again. Do not use the IBM Cloud Dashboard and user interface to modify your VPC after it is created. The Terraform scripts create a complete solution and selectively modifying resources with the user interface might cause unexpected results.

If you need to remove the SAP Netweaver 7.X on HANA or AnyDB installation, go to your project folder and run `terraform destroy`. The `terraform destroy` command does not remove the VPC in this scenario because the VPC was created before these Terraform scripts were run.

Related information

For more information about Terraform on IBM Cloud, see [Getting started with Terraform on IBM Cloud](#).

For more information about using Terraform for creating only a VPC for SAP, without the SAP architecture, see [Creating single-tier virtual private cloud for SAP by using Terraform](#).

SAP One Support Notes that apply to this document:

- [SAP Note 84555 - Windows Server, Linux®, and UNIX: Certified hardware](#)
- [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#)
- [SAP Note 2923773 - Linux® on IBM Cloud \(IaaS\): Adaption of your SAP license](#)
- [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#)
- [SAP Note 2369910 - SAP Software on Linux®: General information](#)
- [SAP Note 171380 - Released IBM hardware \(Intel processors\) and IBM cloud services offers](#)
- [SAP Note 1380654 - SAP support in IaaS environments](#)

This document is referenced by:

- [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#)
- [SAP Note 2588225 - SAP on IBM Cloud: Protect against speculative execution vulnerabilities](#)
- [SAP Note 1380654 - SAP support in IaaS environments](#)
- [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#)

SAP AAS for SAP HANA and AnyDB in VPC

Automating SAP workload HA deployment on IBM Cloud VPC with Terraform and Ansible

You can use Terraform to automate IBM Cloud® VPC provisioning. The VPC provisioned includes virtual server instances with high network performance. The VPC infrastructure contains various Infrastructure-as-a-Service (IaaS) offerings, including virtual servers. After the VPC is provisioned, the scripts use the Ansible Playbooks to install the SAP system.

IBM Cloud VPC introduction

VPC is a public cloud offering that an enterprise uses to establish its own private cloud-like computing environment on shared [public cloud](#) infrastructure. VPC gives an enterprise the ability to define and control a virtual network that is logically isolated from all other public cloud tenants, creating a private and secure place on the public cloud.

Imagine that a cloud provider's infrastructure is a residential apartment building and multiple families live inside. A public cloud tenant is a kind of sharing an apartment with a few roommates. In contrast, having a VPC is like having your own private condominium; no one else has the key, and no one can enter the space without your permission.

VPC's logical isolation is implemented by using virtual network functions and security features that give the enterprise customer granular control over which IP addresses or applications can access particular resources. It is analogous to the "friends-only" or "public/private" controls on social media accounts used to restrict who can or can't see your otherwise public posts.

With IBM Cloud VPC, you can use the UI, CLI, and API to manually provision virtual server instances for VPC with high network performance. VPC infrastructure contains various Infrastructure-as-a-Service (IaaS) offerings including virtual servers for VPC.

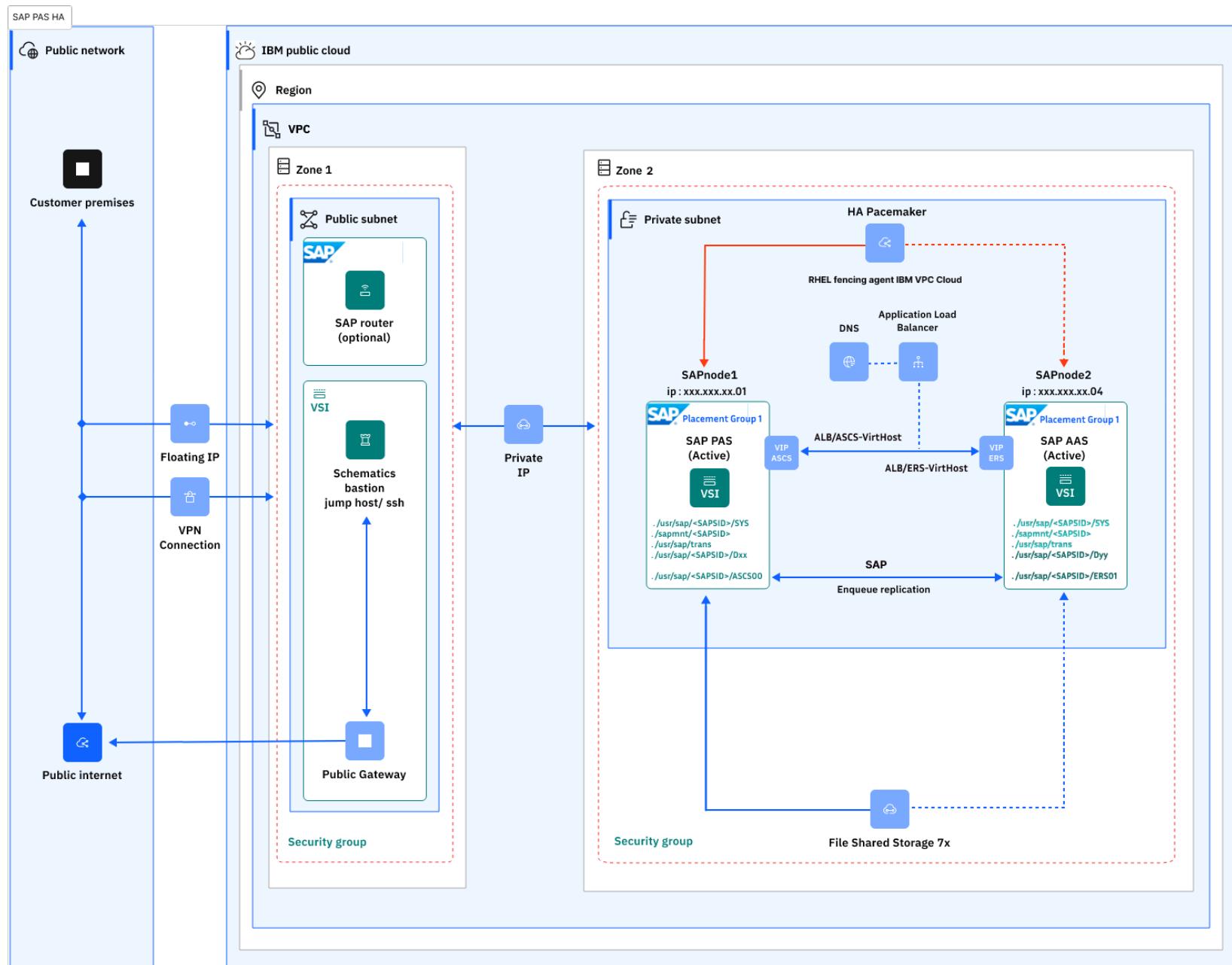
Use the following information to understand a simple use-case for planning, creating, and configuring resources for your VPC, and learn more about VPC overviews and VPC tutorials. For more information about the VPC, see [Getting started with Virtual Private Cloud \(VPC\)](#).

SAP products architecture on IBM Cloud VPC

A [Virtual Private Cloud \(VPC\)](#) contains one of the most secure and reliable cloud environments for SAP applications within your own VPC with virtual server instances. This represents an Infrastructure-as-a-Service (IaaS){: external} within IBM Cloud that offers all the benefits of isolated, secure, and flexible virtual cloud infrastructure from IBM. In comparison, the IBM Cloud classic infrastructure virtual servers offering uses virtual instances with native and VLAN networking to communicate with each other within a data center; however, the instances are restricted in one well-working pod by using subnet and VLAN networking as a gap scale up of virtual resources should rely between the pods. The IBM Cloud VPC network orchestrator layer concept eliminates the pod boundaries and restrictions, so this new concept handles all the networking for every virtual instance running within VPC across regions and zones.

Highly available system for SAP NetWeaver on IBM Cloud VPC

In a Highly Available (HA) system, every instance can run on a separate IBM Cloud virtual server instance. The cluster HA configuration for the SAP application server consists of two virtual server instances, each of them located in the same zone within the region by using placement groups. Placement groups assure that both cluster resources and cloud resources are also located in different compute nodes as specified in the following placement groups section:



SAP HA for SAP applications cluster nodes PAS (Active) and AAS (Active)

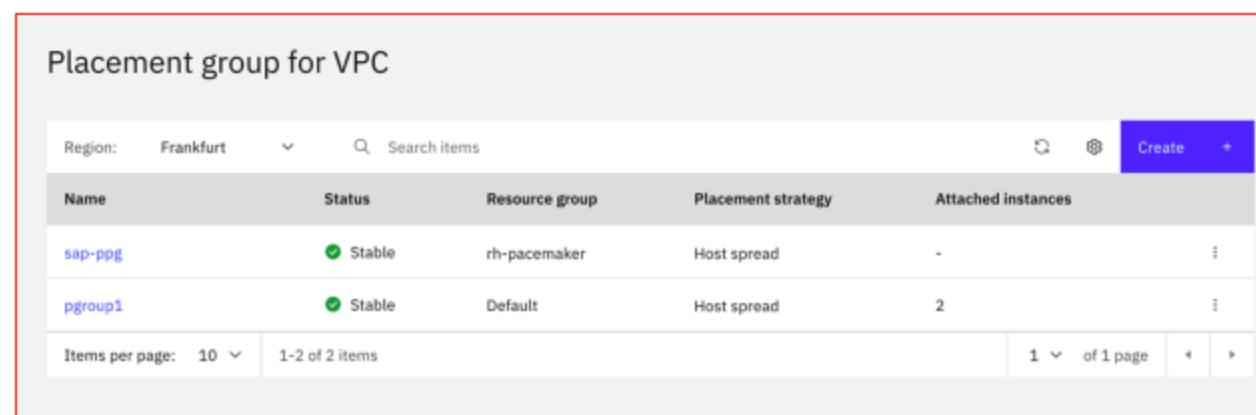
Placement groups on IBM Cloud VPC for SAP HA architecture

Placement Groups (PG) for VPC have two different anti-affinity strategies for high availability. By using the placement strategies, you minimize the chance of service disruption with virtual server instances that are placed on different hosts or into an infrastructure with separate power and network supplies.

The design of placement groups for IBM Cloud virtual servers solves this issue. Placement groups give a measure of control over the host on which a new public virtual server is placed. In this release, a “spread” rule is implemented, which means that the virtual servers within a placement group are spread onto different hosts. You can build a highly available application within a data center and know that your virtual servers are isolated from each other.

Placement groups with the spread rule are available to create in selected IBM Cloud data centers. After a spread rule is created, you can provision a virtual server into that group and ensure that it is not on the same host as any of your other virtual servers. This feature comes with no cost.

You can create your placement group and assign up to four new virtual server instances. With the spread rule, each of your virtual servers are provisioned on different physical hosts. In the following configuration example, the “Power Spread” option is used:



Placement groups host spread

Placement group for VPC					
Name	Status	Resource group	Placement strategy	Attached instances	
sapha-poc	Stable	wes-ic4sap-resourcegroup	Power spread	4	
Items per page: 10 1 item 1 of 1 page					

Placement groups power spread

Following are the SAP instances that are required for HA scenario:

- ABAP SAP Central Services (ASCS) instance - contains the ABAP message server and the ABAP enqueue server.
- Enqueue Replication Server (ERS) instance for the ASCS instance.
- Database instance
- Primary Application Server (PAS) instance on node 1.
- Additional Application Server (AAS) instance on node 2.



Note: It is recommended to run both the ASCS instance and the ERS instance in a switchover cluster infrastructure.

IBM Cloud File Storage for VPC for SAP HA architecture

[IBM Cloud File Storage for VPC](#) technology is used to make the SAP directories available to the SAP system. The technologies of choice are NFS, shared disks, and cluster file system. If you have decided to use the HA solution for your SAP system, make sure that you properly address the HA requirements of the SAP file systems in your SAP environment.

File shares for VPC								
Name	Status	Resource groups	Location	Mount targets	Size	Replication role	Encryption type	
usrsap-as1-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-as2-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-sapscs-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-sapers-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-sapmnt-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-sapsys-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-trans-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	80 GB	None	Provider managed	

File shares for VPC

- File shares that are mounted as NFS permanent file systems on both cluster nodes for SAP HA application:
 - `/usr/sap/<SAPSID>/SYS`
 - `/sapmnt<SAPSID>`
 - `/usr/sap/trans`
- Cluster-managed file systems for SAP HA application: ASCS
 - `/usr/sap/<SAPSID>/ASCS00`
 - `/usr/sap/<SAPSID>/ERS01`
- Permanent NFS mount on SAP HA application node 1 PAS instance:
 - `/usr/sap/<SAPSID>/Dxx`
- Permanent NFS mount on SAP HA application node 2 dialog instance:
 - `/usr/sap/<SAPSID>/Dyy`

Prerequisites

You need to install the hardware (hosts, disks, and network) and decide how to distribute the database, SAP instances, and if required, the Network File System (NFS) server over the cluster nodes.

Context

Following are the types of SAP directories:

- Physically shared directories: `/<sapmnt>/<SAPSID>` and `/usr/sap/trans`

- Logically shared directories that are bound to a node, such as `/usr/sap`, with the following local directories:
 - `/usr/sap/<SAPSID>`
 - `/usr/sap/<SAPSID>/SYS`
 - `/usr/sap/hostctrl`
- Local directories that contain the SAP instances such as `/usr/sap/<SAPSID>/ASCS<Instance_Number>`
- The global transport directory may reside on a separate SAP transport host as a standard three systems transport layer configuration.

You need at least two nodes and a shared file system for distributed ASCS and ERS instances. The assumption is that the rest of the components are distributed on other nodes.

ASCS and ERS installation

In order for the ASCS and ERS instances to be able to move from one node to the other, they need to be installed on a shared file system and use virtual hostnames based on the virtual IP.

In this VPC-based SAP HA solution, the shared file system that is required by the cluster is replaced by the NFS-mounted file storage, and the virtual IP is replaced by the Application Load Balancer for VPC (ALB).

In this scenario, three ALBs are used, one for each Single Point of Failure (SPOF) component in order to replace the virtual IP requirement: ALB for ASCS, ALB for ERS, and ALB for ASE Sybase. Each ALB is configured as a backend for the corresponding cluster servers and redirects all of the communication that is received on the front-end ports to the active server in the backend pool.

Load balancers for VPC						
Region:	Frankfurt	▼	<input type="text"/> poc	X		
Name	Status	Family	Resource group	Type	Hostname	Location
db-alb-hana-poc	Active	Application	wes-ic4sap-resourcegroup	Private	20bdd130-eu-de.lb.appdomain.cloud	Frankfurt
sap-alb-ers-poc	Active	Application	wes-ic4sap-resourcegroup	Private	3941d983-eu-de.lb.appdomain.cloud	Frankfurt
sap-alb-ascs-poc	Active	Application	wes-ic4sap-resourcegroup	Private	56a9190d-eu-de.lb.appdomain.cloud	Frankfurt

Application load balancer management of HA IPs mechanism

Private application load balancer

A [private application load balancer](#) is accessible through your private subnets that you configured to create the load balancer.

Similar to a public application load balancer, your private application load balancer service instance is assigned an FQDN; however, this domain name is registered with one or more private IP addresses.

IBM Cloud operations change the number and value of your assigned private IP addresses over time, based on maintenance and scaling activities. The backend virtual server instances that host your application must run in the same region and under the same VPC.

Use the assigned ALB FQDN to send traffic to the private application load balancer to avoid connectivity problems to your applications during system maintenance or scaling down activities.

Each ALB sends traffic to the cluster node where the application (ASCS, ERS, ASE Sybase DB) is running. During the cluster failover, the ALB redirects all the traffic to the new node where the resources are up and running.



Note: DNS-as-a-Service (DNSaaS) is the management IBM Cloud VPC DNS service of HA and FQDN (IPs) mechanism.



Note: The ALB has a default of 50 seconds for client and server timeout, so after 50 seconds of inactivity, the connection is closed. To support SAP connections through ALB and not lose connection after 50 seconds, you need to request a change this value to a minimum of 300 seconds (client-side idle connection = minimum 300s and server-side idle connection = minimum 300s). To request this change, open a support ticket. This is an account-wide change that affects all of the ALBs in your account. For more information, see [Connection timeouts](#).

DNS Services with VPC

[IBM Cloud DNS Services](#) provide private DNS to VPC users. Private DNS zones are resolvable only on IBM Cloud and from explicitly [permitted networks](#) in an account. To get started, create a DNS Services instance by using the IBM Cloud console.

DNS Services allows you to:

- Create the private DNS zones that are collections for holding the domain names.
- Create the DNS resource records under these DNS zones.
- Specify the access controls used for the DNS resolution of resource records on a zone-wide level.

DNS Services also maintains its own worldwide set of DNS resolvers. Instances that are provisioned under IBM Cloud on an IBM Cloud network can use resource records that are configured through IBM Cloud DNS Services by querying DNS Services resolvers.

Resource records and zones that are configured through DNS Services are:

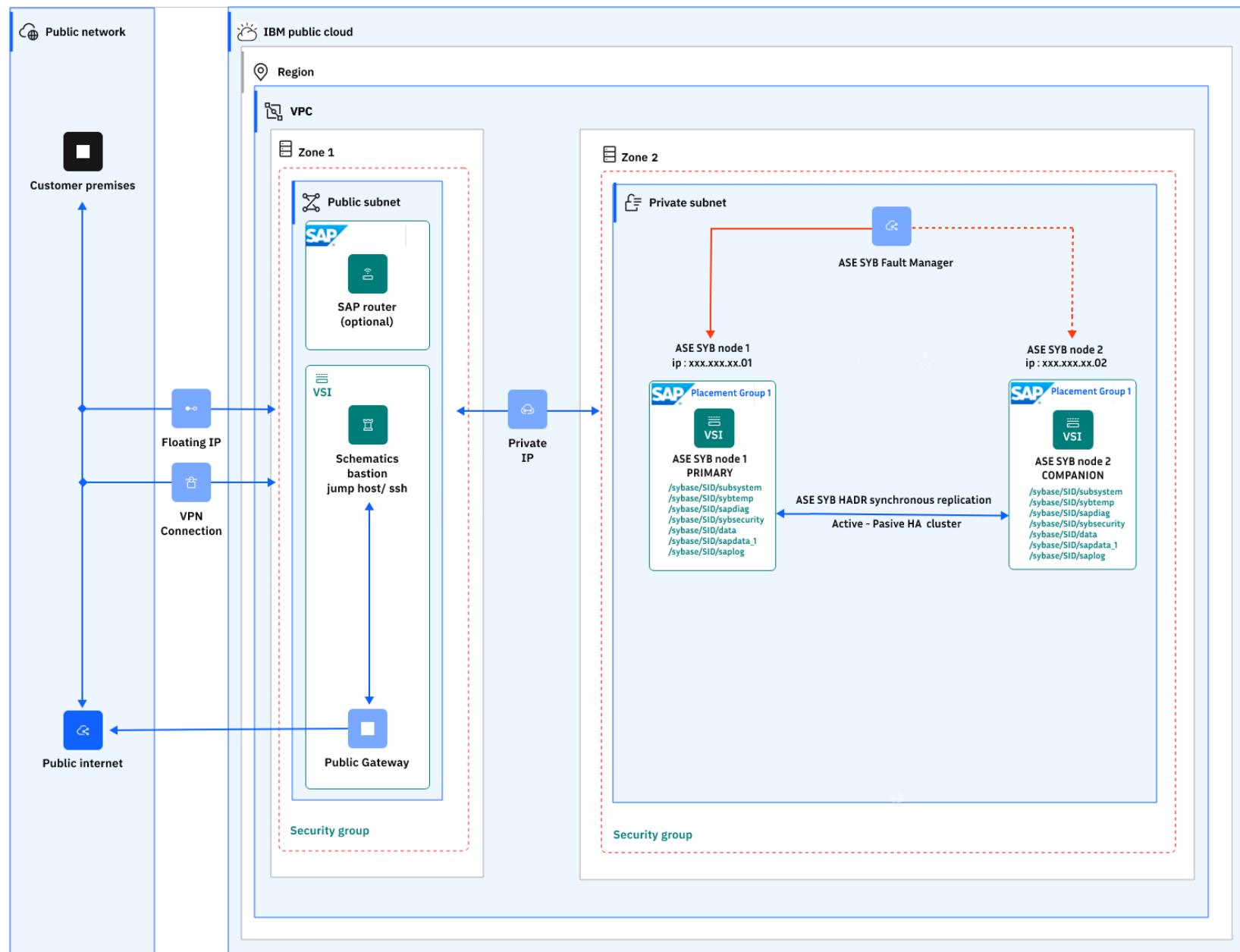
- Separated from the wider public DNS, and their publicly accessible records.
- Hidden from the system outside of and not part of the IBM Cloud private network.
- Accessible only from the system that you authorize on the IBM Cloud private network.
- Resolvable only via the resolvers provided by the service.

The DNS service maps the FQDN of each ALB to the virtual hostnames of the ASCS, ERS, and ASE Sybase that are used by SAP applications.

Type	Name	Value	TTL
CNAME	dbpochana	is an alias of 20bdd130-eu-de.lb.appdomain.cloud	12 hr
CNAME	sappocers	is an alias of 3941d983-eu-de.lb.appdomain.cloud	12 hr
CNAME	sappocases	is an alias of 56a9190d-eu-de.lb.appdomain.cloud	12 hr

DNS records

Highly available system for SAP ASE Sybase database with HADR system



SAP HA for ASE Sybase DB instances cluster nodes primary (Active) and Secondary (Companion)

At the most basic level, a standard HA ASE Sybase cluster in an active(primary)-passive(companion) configuration has two nodes: one is the primary node and the other is the standby node. This means that the primary node is actively serving the active SAP DB instances (Primary and Companion), while the standby node is waiting to jump in if there is any failure.

The cluster is set with a virtual hostname IP (hostname is mapped to the FQDN of the ASE Sybase ALB through DNS, which is the same as

explained previously for SAP ASCS and ERS instances). Application instances (PAS and AAS) are used on the SAP profiles to call that particular component. The cluster assigns the virtual IP to the active node and uses a heartbeat monitor to confirm the availability of the components. If the primary node stops responding, it triggers the automatic failover mechanism that calls the standby node to step up to become the primary node. The ALB detects the change, redirects the traffic to the new active node, and assigns the virtual IP to it, restoring the component availability. Once fixed, the failed node comes online as a standby node.

SAP Sybase HADR system supports synchronous replication

The SAP Sybase HADR system supports synchronous replication between the primary and standby servers for high availability. An active-active setup is a two-node configuration where both nodes in the cluster include SAP ASE managing independent workloads, capable of taking over each others workload in the event of a failure.

The SAP ASE server that takes over the workload is called a secondary companion, and the SAP ASE server that fails is called the primary companion. Together they are companion servers. This movement from one node to another is called failover. After the primary companion is ready to resume its workload, it is moved back to its original node. This movement is called a failback.

When a system fails over, clients that are connected to the primary companion and use the failover property automatically reestablish their network connections to the secondary companion. You must tune your operating system to successfully manage both servers during fail over. See your operating system documentation for information about configuring your system for high availability. An SAP ASE configured for failover in an active-active setup can be shut down using the shutdown command only after you have suspended SAP ASE from the companion configuration, at both the server level and the platform level.

The always-on option in a High Availability and Disaster Recovery (HADR) system consists of two SAP ASE servers:

- Primary on which all transaction processing takes place.
- Warm standby (referred to as a "standby server" in DR mode, and as a "companion" in HA mode) for the primary server, and contains copies of designated databases from the primary server.



Note: The HADR feature that is shipped with SAP ASE version 16.0 SP02 supports only a single-companion server.

Some high-availability solutions (for example, the SAP Adaptive Server Enterprise Cluster Edition) share or use common resources between nodes. However, the HADR system is a "shared nothing" configuration, each node has separate resources including disks.

In an HADR system, servers are separate entities and data is replicated from the primary server to the companion server. If the primary server fails, a companion server is promoted to the role of primary server either manually or automatically. Once the promotion is complete, clients can reconnect to the new primary server, and see all committed data, including data that was committed on the previous primary server.

Servers can be separated geographically, which makes an HADR system capable of withstanding the loss of an entire computing facility.



Note: The HADR system includes an embedded SAP Replication Server, which synchronizes the databases between the primary and companion servers. SAP ASE uses the Replication Management Agent (RMA) to communicate with Replication Server and SAP Replication Server uses Open Client connectivity to communicate with the companion SAP ASE.

The Replication Agent detects any data changes made on the primary server and sends them to the primary SAP Replication Server. In the figure above, the unidirectional arrows indicate that, although both SAP Replication Servers are configured, only one direction is enabled at a time.

The HADR system supports synchronous replication between the primary and standby servers for high availability so the two servers can keep in sync with Zero Data Loss (ZDL). This requires a network link that is fast enough between the primary and standby server so that synchronous replication can keep up with the primary servers workload. Generally, this means that the network latency is approximately the same speed as the local disk IO speed, a few (fewer than 10) milliseconds. Anything longer than a few milliseconds may result in a slower response to write operations at the primary.

The HADR system supports asynchronous replication between the primary and standby servers for disaster recovery. The primary and standby servers by using asynchronous replication can be geographically distant, meaning they can have a slower network link. With asynchronous replication, Replication Agent Thread captures the primary servers workload, which is delivered asynchronously to SAP Replication Server. The SAP Replication Server applies these workload change to the companion server.

The most fundamental service that is offered by the HADR system is the failover; planned or unplanned from the primary to the companion server, which allows maintenance activity to occur on the old primary server, while applications continue on the new primary.

The HADR system provides protection in the event of a disaster. If the primary server is lost, the companion server can be used as a replacement. Client applications can switch to the companion server, and the companion server is quickly available for users. If the SAP Replication Server was in synchronous mode before the failure of the primary server, the Fault Manager automatically initiates failover with

zero data loss.

Fault Manager installation on the SAP ASCS node

The required parameters are asked during the installation process to create a profile for the fault manager and then adds it to the instance start profile. It is also possible to run the installation by using an existing profile: `sybdbfm install pf=<SYBHA.PFL>` In this case, the installation process will only ask for profile parameters missing in the profile.



Note: Fault manger is integrated with ASCS on same SAP PAS/AAS cluster (start/stop/move together).

There may be some data loss if the SAP Replication Server was in asynchronous mode and you must use manual intervention to failover for disaster recovery.

Connection attempts to the companion server without the necessary privileges are silently redirected to the primary companion via the login redirection mechanism, which is supported by Connectivity libraries. If login redirection is not enabled, client connections fail and are disconnected.

The SAP ASE HADR option installs the below components:

- SAP ASE
- SAP Replication Server
- Replication Management Agent (RMA)
- SAP Host Agent
- Fault Manager
- SAP ASE Cockpit



Note: This automation is offered at no cost; however, the provisioned infrastructure comes at cost.

VPC with Additional Application Server (AAS) ABAP on Linux for SAP HANA

You can use Terraform scripts to create a single-tier VPC and create the AAS to HANA and AnyDB infrastructure on the VPC. The Terraform scripts use the VPC information that you provide and then call the Ansible playbook to create the SAP architecture on the specified VPC. Terraform on IBM Cloud® enables predictable and consistent provisioning of IBM Cloud Virtual Private Cloud (VPC) infrastructure resources so that you can rapidly build complex, cloud environments. IBM Cloud VPC infrastructure consists of SAP certified hardware that uses Intel® Xeon CPUs and more Intel® technologies.

You have two deployment methods to choose from:

- Terraform scripts that run from the CLI on your bastion server.
- Schematics user interface accessed from your cloud dashboard menu.

You can create SAP AAS NetWeaver 7.x on the SAP HANA-based ABAP stack.

SAP solution implemented

Many SAP enterprise solutions are built on the SAP platform (SAP NetWeaver) including:

- SAP HANA as Primary Persistence for SAP NetWeaver-based applications
- SAP Business Suite applications (ERP, CRM, and SCM, and other applications),
- SAP Business Warehouse (BW), and
- Other SAP enterprise solutions

SAP NetWeaver has two distinct aspects, ABAP and Java. Many applications that are built on the SAP NetWeaver's ABAP or Java (or both) application servers run on SAP DB owned HANA and ASE Sybase either in AnyDB platforms (MSSQL, Oracle, and Db2).

Technical interfaces are available for applications that are built on the SAP NetWeaver AS ABAP and AS Java to run on SAP HANA and AnyDB. However, specific development enablement is normally required for each application to ensure that it runs optimally on the SAP HANA. SAP Business Suite applications (ERP, CRM, SCM, and other applications), SAP Business Warehouse (BW), and other SAP NetWeaver-based applications were modified to run on SAP HANA and have many advantages. Also, various components and complimentary applications that are built on SAP NetWeaver can also run on SAP HANA or AnyDB by using the provided SAP NetWeaver DB interfaces.

The SAP HANA as primary persistence for SAP NetWeaver-based applications scenario has one restriction: SAP NetWeaver ABAP and Java

application servers must run on separate hardware servers from the SAP HANA hardware.

What is created

The scripts automate the virtual infrastructure resources, provisioning the processes for the SAP architecture in an existing VPC with a distributed environment. SAP AAS NetWeaver 7.x (HANA or ASE SYB) application server on a distinct VSI VPC system and SAP HANA DB on a dedicated server type VSI VPC box are provisioned. The scripts work in two phases.

During the first phase of [Automate SAP bastion server – SAP media storage repository](#), the following virtual infrastructure resources based on the components from the existing VPC created by the bastion server are:

- 1 VPC where the virtual server instance is provisioned.
- 1 security group. The rules for this security group are:
 - Allow inbound DNS traffic (port 53).
 - Allow inbound SSH traffic (TCP port 22).
 - Allow all outbound traffic from the virtual server instance.
 - Allow all traffic in the security group.
- 1 subnet to enable the networking in your VPC.
- 2 virtual server instances with SAP certified storage and network configurations.
- 1 floating IP address used to access your VPC virtual server instance over the public network.

During the second phase, the Ansible Playbooks is called and the SAP architecture is installed for both dedicated virtual server instance (VSI) SAP application; VSI system and dedicated SAP HANA VSI box. The SAP architecture that is deployed on the SAP NetWeaver 7.x release is a stand-alone dedicated SAP HANA 2.0 box release. For more information about this architecture, see [Automating SAP HANA stand-alone virtual server instance on IBM Cloud® VPC by using Terraform and Ansible](#).

You can provision only one instance of the service per IBM Cloud region.

Schematics deployment

When you run the scripts with the Schematics interface, you:

- Enter the workspace information.
- Enter the GitHub path for the chosen solution either on NetWeaver AAS for HANA.
- Modify the parameters in the Schematics interface. They are the same parameters as the `input.auto.tfvars` file that you use with the cli.

Virtual server instance configuration

Following are the supported operating system images for SAP NetWeaver primary application server:

- ibm-redhat-8-4-amd64-sap-applications-2
- ibm-redhat-8-6-amd64-sap-applications-2
- ibm-sles-15-3-amd64-sap-applications-2
- ibm-sles-15-4-amd64-sap-applications-3

Following are the supported operating system images for SAP HANA database:

- ibm-redhat-8-4-amd64-sap-hana-2
- ibm-redhat-8-6-amd64-sap-hana-2
- ibm-sles-15-3-amd64-sap-hana-2
- ibm-sles-15-4-amd64-sap-hana-1

For both server instances there are:

- Two SSH keys are configured to access SSH as `root`.
- Three storage volumes as described in the `input.auto.tfvars` file.

What is created for anydb

The scripts use the information that you provide for an existing VPC and deploy AAS to SAP HANA or AnyDB on a different host than CI (SAP Central Instance) VSI host. For more information about this architecture, see [SAP NetWeaver 7.x on UNIX with HANA or AnyDB on IBM Cloud](#)

[VPC on IBM Cloud VPC](#). You specify the information for the VPC to use in the `input.auto.tfvars` file.

The scripts call the Ansible Playbooks to install the SAP architecture.

Script files

The configuration and script files are provided on GitHub. Each supported interface for the SAP solution installation has its own folder in the GitHub repository:

- [GitHub repository for Terraform – AAS HANA](#)

Terraform interface

To run the Terraform script, you modify:

- The `input.auto.tfvars` file to specify the existing VPC resources for your solution. Specify the variables for the existing VPC:
 - VPC name
 - Security group
 - Subnet
 - Hostname
 - Profile
 - Image
 - Up to two SSH keys

You can change the default SAP system configuration settings to match your solution. You can also specify the location where you downloaded the SAP kits.

The IBM Cloud Provider plug-in for Terraform on IBM Cloud uses these configuration files to install AAS to SAP HANA and AnyDB on the specified VPC in your IBM Cloud account.

Support

There are no warranties of any kind, and there is no service or technical support available for these materials from IBM®. As a recommended practice, review carefully any materials that you download from this site before using them on a live system.

Though the materials provided herein are not supported by the IBM® Service organization, your comments are welcomed by the developers, who reserve the right to revise, readapt or remove the materials at any time. To report a problem, or provide suggestions or comments, open a GitHub issue.

Before you begin

Before you use the scripts in the bastion cli:

- Set up your account to access the VPC. Make sure that your account is [upgraded to a paid account](#).
- If you have not already, create a Bastion server to store the SAP kits. For more information, see [Automate SAP bastion server - SAP media storage repository](#).
- Download the SAP kits from the SAP Portal to your Deployment Server. Make note of the download locations. Ansible decompresses the files. For more information, see the [readme](#) file.
- [Create or retrieve an IBM Cloud API key](#). The API key is used to authenticate with the IBM Cloud platform and to determine your permissions for IBM Cloud services.
- [Create or retrieve your SSH key ID](#). You need the 40-digit UUID for the SSH key, not the SSH key name.
- Terraform should already be installed on the bastion server that you deployed. For more information, see [Bastion server for SAP deployment](#).
- (Optional - Catalog Tile) create secrets for your credentials and passwords by using the [Secrets Manager](#).

Deploying SAP AAS NetWeaver 7.x on HANA by using the Schematics user interface

Use these steps to configure the SAP Additional Application Server (AAS) NetWeaver with HANA or AnyDB on your existing VPC by using the Schematics interface. The script takes 2 - 3 hours to complete.

1. From the IBM Cloud menu, select **Schematics**.
2. Click **Create** workspace.

3. On the **Specify template** page:
 - Enter the URL for the Schematics interface.
 - Select the **Terraform version** that is listed in the readme file.
 - Click **Next**.
4. On the **workspace details** page:
 - Enter a name for the workspace.
 - Select a **Resource group**.
 - Select a **Location** for your workspace. The workspace location does not have to match the resource location.
 - Select **Next**.
5. Select **Create** to create your workspace.
6. On the workspace settings page, in the input variables section, review the default input variables and provide values that match your solution.
 For a more detailed description of each parameter, check the GitHub repo [AAS HANA readme](#) file, chapter "Input parameter file". Also, make sure to mark the parameters that contain sensitive information like passwords, API, and ssh private keys as "sensitive". These parameters are marked as "sensitive" in the readme file, under "Input parameter file".
7. On the workspace settings page, click **Generate plan**. Wait for the plan to complete.
8. Click **View log** to review the log files of your terraform execution plan.
9. Apply your Terraform template by clicking **Apply plan**.
10. Review the log file to ensure that no errors occur during the provisioning, modification, or deletion process.

Deploying SAP AAS NetWeaver (ABAP) on HANA with the Deployable Architecture tile interface

Use these steps to configure the SAP AAS NetWeaver (ABAP) on HANA on your existing VPC by using the catalog tile interface. The script takes 2 - 3 hours to complete.

1. From the IBM Cloud catalog, select **VPC with Additional Application Server ABAP on Linux for SAP HANA** on HANA tile. The **Create** tab opens for VPC with Additional Application Server ABAP on Linux for SAP HANA. For more information about this deployment, see the About tab or the readme file link.
2. Select the latest version.
3. Select **VPC with Additional Application Server ABAP on Linux for SAP HANA on Deployable Architecture tile** variation.
4. Click **Review deployment** options:
 - **Add to project** to add this deployment to an IBM Cloud project and combine it with other deployments. IBM Cloud projects include several more pipeline steps before deployment, including deployment validation, cost calculation, compliance verification, and approval process.
 - **Create from the CLI** to get the CLI command. With this command you can trigger the deployment from the CLI.
 - **Work with code** to embed the code into other terraform deployments.
 - **Deploy with IBM Cloud Schematics** to trigger the deployment process directly.
5. Select **Deploy with IBM Cloud Schematics**.
6. Add the input parameters for this installation. There are 3 categories of parameters:
 - **Workspace** - These parameters define the workspace that is automatically created in Schematics:
 - Enter a name for the workspace or use the default name.
 - The Resource Group used to create resources. Use default or create a Resource Group.
 - Select a location to create your Schematics workspace. The workspace location need not match the resource location.
 - **Required input variables** - Review the default input variables and provide values that match your solution. These parameters are specific to your deployment. For more detailed information, see the [Readme file](#).

Parameter	Description
BASTION_FLOATING_IP	Required only for Schematics Deployments. The Floating IP from the Bastion Server.

HOSTNAME	The hostname for the VSI. The hostname should be up to 13 characters as required by SAP. For more information on the rules regarding hostnames for SAP systems, check SAP Note 611361: Hostnames of SAP ABAP Platform servers
REGION	The cloud region to deploy the solution. The regions and zones for VPC are listed here . Review supported locations in IBM Cloud Schematics here . Sample value: eu-de.
RESOURCE_GROUP	The name of an existing Resource Group for VSIs and Volumes resources. Default value: "Default". The list of Resource Groups is available here .
SECURITY_GROUP	The name of an existing Security group. The list of security groups is available here .
SSH_KEYS	The list of SSH Keys UUIDs that are allowed to SSH as root to the VSI can contain one or more IDs. The list of SSH Keys is available here . Sample input (use your own SSH UUIDs from IBM Cloud){: external}: ["r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a", "r010-3fcfd9fe7-d4a7-41ce-8bb3-d96e936b2c7e"]
SUBNET	The name of an existing subnet. The list of subnets is available here .
VPC	The name of an existing VPC. The list of VPCs is available here .
ZONE	The cloud zone where to deploy the solution. Sample value: eu-de-2.
ibmcloud_api_key	IBM Cloud API key (Sensitive* value).
private_ssh_key	Required only for Schematics Deployments - Input your id_rsa private key pair content in OpenSSH format (Sensitive* value). This private key should be used only during the terraform provisioning and it is recommended to be changed after the SAP deployment.
hdb_instance_number	The instance number of the SAP HANA database server.
sap_aas_instance_number	Technical identifier for the internal processes of the additional application server.
sap_asci_instance_number	Technical identifier for the internal processes of ASCS.
sap_ci_host	IP address of the existing SAP Central Instance.
sap_ci_hostname	The hostname of the existing SAP Central Instance.
sap_ci_instance_number	Technical identifier for the internal processes of the Central Instance.
sap_sid	The SAP system ID identifies the entire SAP system.
sap_main_password	Common password for all users that are created during the installation (See Obs*).

Required Variables

- **Optional variables** - Review and update the optional input variables. The Ansible scripts expect the SAP kits to be in the default locations listed. For more information, see the [Readme file - Input Parameters](#).

Parameter	Description
ID_RSA_FILE_PATH	The file path for private_ssh_key is automatically generated by default. If it is changed, it must contain the relative path from Git repo folders. Default value: "ansible/id_rsa".
IMAGE	The OS image used for the VSI. A list of images is available here .
PROFILE	The profile used for the VSI. A list of profiles is available here . For more information about supported DB/OS and IBM Gen 2 Virtual Server Instances (VSI), check SAP Note 2927211: SAP Applications on IBM Virtual Private Cloud .

VOL1	Volume 1 Size - The size for the disks in GB that are to be attached to the VSI and used by SAP.
VOL2	Volume 2 Size - The size for the disks in GB that are to be attached to the VSI and used by SAP.
kit_sapcar_file	Path to the sapcar binary, as downloaded from SAP Support Portal.
kit_swpm_file	Path to the SWPM archive (SAR), as downloaded from SAP Support Portal.
kit_saphostagent_file	Path to the SAP Host Agent archive (SAR), as downloaded from SAP Support Portal.
kit_hdbclient_file	Path to the HANA DB client archive (SAR), as downloaded from SAP Support Portal.

Optional Variables

7. Accept the license agreement.
8. Select **Deploy**. The deployment starts and you are directed to the Schematics page that displays the script log files for you to monitor the deployment progress.

Creating the infrastructure using Terraform with the bastion server CLI

Use these steps to configure the IBM Cloud Provider plug-in and use Terraform to install SAP AAS to SAP HANA and AnyDB on your existing VPC on an already deployed SAP NetWeaver 7.X with SAP HANA 2.0 or ASE SYB as a Central Instance.

The script takes 1 - 2 hours to complete.

1. Access the bastion server cli.
2. Clone the solution repository and change to the folder.

ASE SYB 16 Clone the solution repository from <https://github.com/IBM-Cloud/sap-aas-abap-ase-syb> and cd to the sap-aas-abap-ase-syb/cli folder.

```
$ git clone https://github.com/IBM-Cloud/sap-aas-abap-ase-syb
cd sap-aas-abap-ase-syb/cli/
```

SAP HANA 2.0: Clone the solution repository from <https://github.com/IBM-Cloud/sap-abap-hana-aas> and cd to the sap-abap-hana-aas folder.

```
$ git clone https://github.com/IBM-Cloud/sap-abap-hana-aas.git
cd sap-abap-hana-aas/
```

3. Modify the `input.auto.tfvars` file to specify the information for the existing VPC, your region, zone, networking component names, hostname for the AAS VSI,profile, and image. You need your 40-digit SSH key ID for this file. The second SSH key is optional. For more options for profile, see [Instance Profiles](#). For more options, see [Images](#). For descriptions of the variables, see the [readme](#) file.

The VSI OS images that are supported for this solution for Netweaver Additional Application Server are:

- ibm-redhat-8-4-amd64-sap-applications-2
- ibm-redhat-8-6-amd64-sap-applications-2
- ibm-sles-15-3-amd64-sap-applications-2
- ibm-sles-15-4-amd64-sap-applications-4

```
$ # Infra VPC variables for ASE SYB
REGION    = "eu-de"
ZONE      = "eu-de-2"
VPC       = "ic4sap"                      # EXISTING Security group name
SECURITY_GROUP = "ic4sap-securitygroup"     # EXISTING Security group name
RESOURCE_GROUP = "wes-automation"
SUBNET    = "ic4sap-subnet"                 # EXISTING Subnet name
SSH_KEYS   = [ "r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a" , "r010-3fcfd9fe7-d4a7-41ce-8bb3-
d96e936b2c7e" ]

# SAP AAS VSI variables:
```

```

HOSTNAME = "sapnwase-as01"
PROFILE = "bx2-4x16"
IMAGE = "ibm-redhat-8-4-amd64-sap-applications-2

$ # Infra VPC variables for ABAP HANA
REGION      = "eu-de"
ZONE        = "eu-de-2"
VPC          = "ic4sap" # EXISTING Security group name
SECURITY_GROUP = "ic4sap-securitygroup" # EXISTING Security group name
RESOURCE_GROUP = "wes-automation"
SUBNET       = "ic4sap-subnet" # EXISTING Subnet name
SSH_KEYS     = [ "r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a" , "r010-3fc9fe7-d4a7-41ce-8bb3-d96e936b2c7e" ]
ID_RSA_FILE_PATH = "ansible/id_rsa"

# SAP AAS variables:
HOSTNAME = "sapnwapp"
PROFILE = "bx2-4x16"
IMAGE = "ibm-redhat-8-6-amd64-sap-applications-2"

```

4. Customize your SAP system configuration. In the same file, input.auto.tfvars, edit the SAP system configuration variables that are passed to the Ansible automated deployment. For descriptions of the variables, see the [readme](#) file.

```

$ # SAP system configuration - for ASE SYB
sap_sid = "NWD"
sap_ci_host = "10.243.132.10"
sap_ci_hostname = "sapnwase"
sap_ci_instance_number = "00"
sap_asc_s_instance_number = "01"
sap_aas_instance_number = "00"

# Kits paths
kit_sapcar_file = "/storage/NW75SYB/SAPCAR_1010-70006178.EXE"
kit_swpm_file = "/storage/NW75SYB/SWPM10SP31_7-20009701.SAR"
kit_saphotagent_file = "/storage/NW75SYB/SAPHOSTAGENT51_51-20009394.SAR"

```

```

$ # SAP system configuration - for ABAP HANA
sap_sid = "NWD"
sap_ci_host = "10.243.132.10"
sap_ci_hostname = "sapnwapp01"
sap_ci_instance_number = "00"
sap_asc_s_instance_number = "01"
hdb_instance_number = "00"
sap_aas_instance_number = "00"

# Kits paths
kit_sapcar_file = "/storage/NW75HDB/SAPCAR_1010-70006178.EXE"
kit_swpm_file = "/storage/NW75HDB/SWPM10SP31_7-20009701.SAR"
kit_saphotagent_file = "/storage/NW75HDB/SAPHOSTAGENT51_51-20009394.SAR"
kit_hdbclient_file = "/storage/NW75HDB/IMDB_CLIENT20_009_28-80002082.SAR"

```

Ansible decompresses the rest of the SAP kit files. For more information, see the [readme](#) file.

5. Initialize the Terraform CLI.

```
terraform init
```

6. Create a Terraform execution plan. The Terraform execution plan summarizes all the actions that are done to create the virtual private cloud instance in your account.

```
terraform plan plan1
```

Enter an SAP main password and your API key.

The SAP main password must be 10 - 14 characters long and contain at least one digit (0-9). It can contain only the following characters: a-z, A-Z, 0-9, @, #, \$, . *This password cannot contain exclamation points '!'. The password must not start with a digit or an underscore ().*

7. Verify that the plan shows all of the resources that you want to create and that the names and values are correct. If the plan needs to be adjusted, edit the input.auto.tfvars file to correct resources and run terraform plan again.
8. Apply the saved plan.

```
$ terraform apply "plan1"
```

The virtual private cloud and components are created and you see output similar to the `terraform plan` output.

9. Add the SAP credentials and the virtual server instance IP to the SAP GUI. For more information about the SAP GUI, see [SAP GUI](#).

Next steps

If you need to rename your resources after they are created, modify the `input.auto.tfvars` file to change the names and run `terraform plan` and `terraform apply` again. Do not use the IBM Cloud Dashboard and user interface to modify your VPC after it is created. The Terraform scripts create a complete solution and selectively modifying resources with the user interface might cause unexpected results.

If you need to remove the SAP Netweaver 7.X on HANA or AnyDB installation, go to your project folder and run `terraform destroy`. The `terraform destroy` command does not remove the VPC in this scenario because the VPC was created before these Terraform scripts were run.

Related information

For more information about Terraform on IBM Cloud, see [Getting started with Terraform on IBM Cloud](#).

For more information about using Terraform for creating only a VPC for SAP, without the SAP architecture, see [Creating single-tier virtual private cloud for SAP by using Terraform](#).

SAP One Support Notes that apply to this document:

- [SAP Note 84555 - Windows Server, Linux®, and UNIX: Certified hardware](#)
- [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#)
- [SAP Note 2923773 - Linux® on IBM Cloud \(IaaS\): Adaption of your SAP license](#)
- [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#)
- [SAP Note 2369910 - SAP Software on Linux®: General information](#)
- [SAP Note 171380 - Released IBM hardware \(Intel processors\) and IBM cloud services offers](#)
- [SAP Note 1380654 - SAP support in IaaS environments](#)

This document is referenced by:

- [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#)
- [SAP Note 2588225 - SAP on IBM Cloud: Protect against speculative execution vulnerabilities](#)
- [SAP Note 1380654 - SAP support in IaaS environments](#)
- [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#)

SAP NetWeaver and SAP ASE in VPC

Automating SAP workload HA deployment on IBM Cloud VPC with Terraform and Ansible

You can use Terraform to automate IBM Cloud® VPC provisioning. The VPC provisioned includes virtual server instances with high network performance. The VPC infrastructure contains various Infrastructure-as-a-Service (IaaS) offerings, including virtual servers. After the VPC is provisioned, the scripts use the Ansible Playbooks to install the SAP system.

IBM Cloud VPC introduction

VPC is a public cloud offering that an enterprise uses to establish its own private cloud-like computing environment on shared [public cloud](#) infrastructure. VPC gives an enterprise the ability to define and control a virtual network that is logically isolated from all other public cloud tenants, creating a private and secure place on the public cloud.

Imagine that a cloud provider's infrastructure is a residential apartment building and multiple families live inside. A public cloud tenant is a kind of sharing an apartment with a few roommates. In contrast, having a VPC is like having your own private condominium; no one else has the key, and no one can enter the space without your permission.

VPC's logical isolation is implemented by using virtual network functions and security features that give the enterprise customer granular control over which IP addresses or applications can access particular resources. It is analogous to the "friends-only" or "public/private" controls on social media accounts used to restrict who can or can't see your otherwise public posts.

With IBM Cloud VPC, you can use the UI, CLI, and API to manually provision virtual server instances for VPC with high network performance. VPC infrastructure contains various Infrastructure-as-a-Service (IaaS) offerings including virtual servers for VPC.

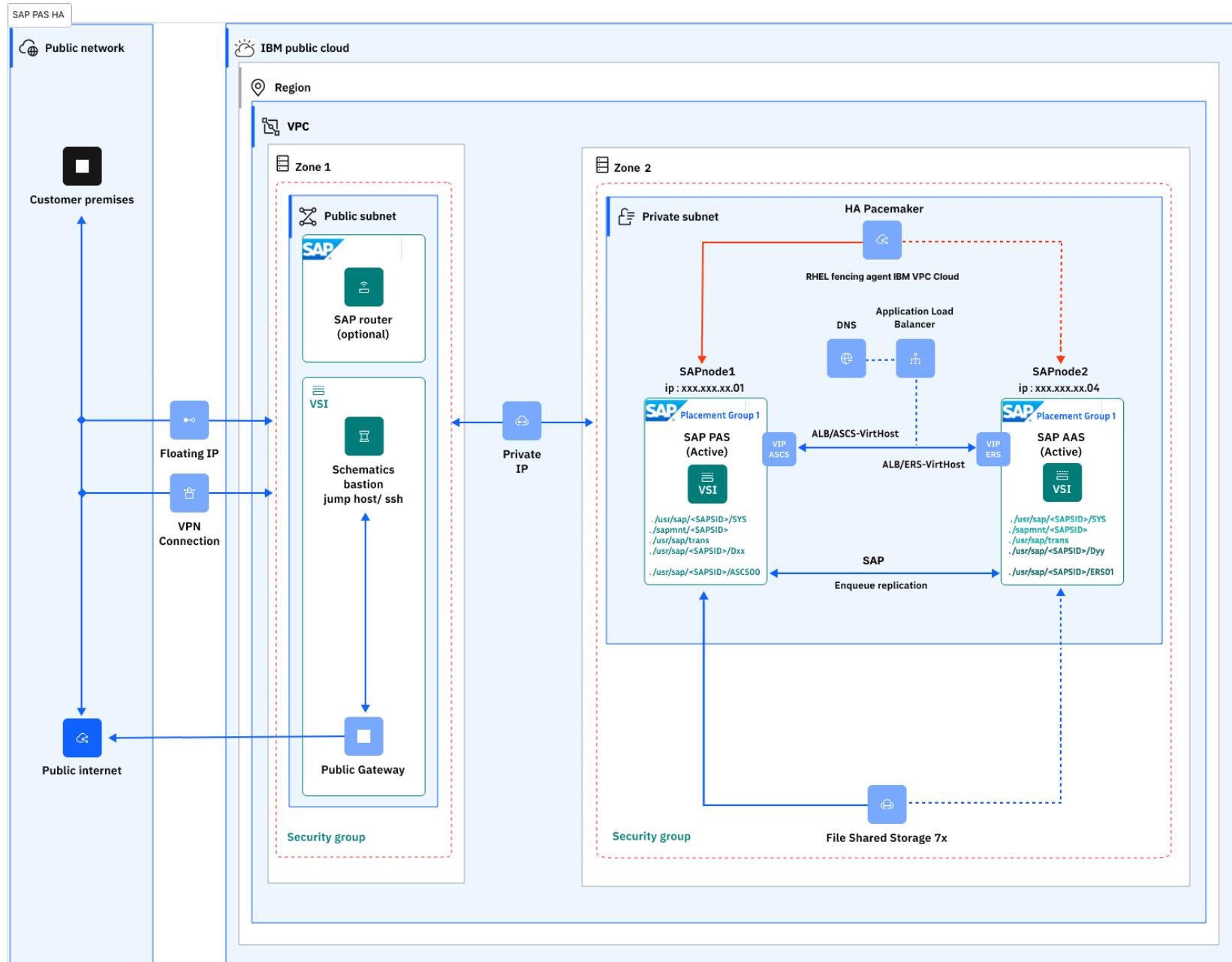
Use the following information to understand a simple use-case for planning, creating, and configuring resources for your VPC, and learn more about VPC overviews and VPC tutorials. For more information about the VPC, see [Getting started with Virtual Private Cloud \(VPC\)](#).

SAP products architecture on IBM Cloud VPC

A [Virtual Private Cloud \(VPC\)](#) contains one of the most secure and reliable cloud environments for SAP applications within your own VPC with virtual server instances. This represents an Infrastructure-as-a-Service (IaaS){: external} within IBM Cloud that offers all the benefits of isolated, secure, and flexible virtual cloud infrastructure from IBM. In comparison, the IBM Cloud classic infrastructure virtual servers offering uses virtual instances with native and VLAN networking to communicate with each other within a data center; however, the instances are restricted in one well-working pod by using subnet and VLAN networking as a gap scale up of virtual resources should rely between the pods. The IBM Cloud VPC network orchestrator layer concept eliminates the pod boundaries and restrictions, so this new concept handles all the networking for every virtual instance running within VPC across regions and zones.

Highly available system for SAP NetWeaver on IBM Cloud VPC

In a Highly Available (HA) system, every instance can run on a separate IBM Cloud virtual server instance. The cluster HA configuration for the SAP application server consists of two virtual server instances, each of them located in the same zone within the region by using placement groups. Placement groups assure that both cluster resources and cloud resources are also located in different compute nodes as specified in the following placement groups section:



SAP HA for SAP applications cluster nodes PAS (Active) and AAS (Active)

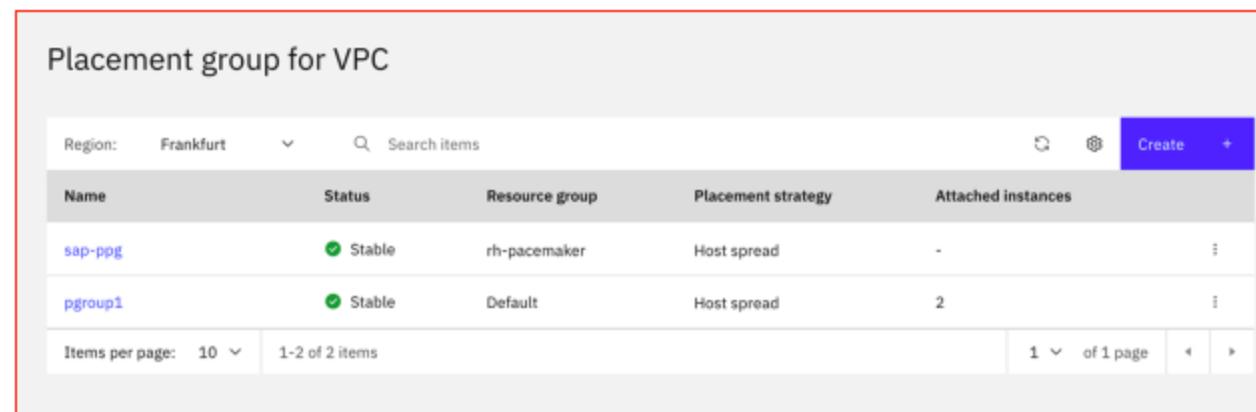
Placement groups on IBM Cloud VPC for SAP HA architecture

Placement Groups (PG) for VPC have two different anti-affinity strategies for high availability. By using the placement strategies, you minimize the chance of service disruption with virtual server instances that are placed on different hosts or into an infrastructure with separate power and network supplies.

The design of placement groups for IBM Cloud virtual servers solves this issue. Placement groups give a measure of control over the host on which a new public virtual server is placed. In this release, a “spread” rule is implemented, which means that the virtual servers within a placement group are spread onto different hosts. You can build a highly available application within a data center and know that your virtual servers are isolated from each other.

Placement groups with the spread rule are available to create in selected IBM Cloud data centers. After a spread rule is created, you can provision a virtual server into that group and ensure that it is not on the same host as any of your other virtual servers. This feature comes with no cost.

You can create your placement group and assign up to four new virtual server instances. With the spread rule, each of your virtual servers are provisioned on different physical hosts. In the following configuration example, the “Power Spread” option is used:



Placement groups host spread

Placement group for VPC					
Name	Status	Resource group	Placement strategy	Attached instances	
sapha-poc	Stable	wes-ic4sap-resourcegroup	Power spread	4	
Items per page: 10 1 item 1 of 1 page					

Placement groups power spread

Following are the SAP instances that are required for HA scenario:

- ABAP SAP Central Services (ASCS) instance - contains the ABAP message server and the ABAP enqueue server.
- Enqueue Replication Server (ERS) instance for the ASCS instance.
- Database instance
- Primary Application Server (PAS) instance on node 1.
- Additional Application Server (AAS) instance on node 2.



Note: It is recommended to run both the ASCS instance and the ERS instance in a switchover cluster infrastructure.

IBM Cloud File Storage for VPC for SAP HA architecture

[IBM Cloud File Storage for VPC](#) technology is used to make the SAP directories available to the SAP system. The technologies of choice are NFS, shared disks, and cluster file system. If you have decided to use the HA solution for your SAP system, make sure that you properly address the HA requirements of the SAP file systems in your SAP environment.

File shares for VPC								
Name	Status	Resource groups	Location	Mount targets	Size	Replication role	Encryption type	
usrsap-as1-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-as2-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-sapscs-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-sapers-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-sapmnt-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-sapsys-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-trans-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	80 GB	None	Provider managed	

File shares for VPC

- File shares that are mounted as NFS permanent file systems on both cluster nodes for SAP HA application:
 - `/usr/sap/<SAPSID>/SYS`
 - `/sapmnt<SAPSID>`
 - `/usr/sap/trans`
- Cluster-managed file systems for SAP HA application: ASCS
 - `/usr/sap/<SAPSID>/ASCS00`
 - `/usr/sap/<SAPSID>/ERS01`
- Permanent NFS mount on SAP HA application node 1 PAS instance:
 - `/usr/sap/<SAPSID>/Dxx`
- Permanent NFS mount on SAP HA application node 2 dialog instance:
 - `/usr/sap/<SAPSID>/Dyy`

Prerequisites

You need to install the hardware (hosts, disks, and network) and decide how to distribute the database, SAP instances, and if required, the Network File System (NFS) server over the cluster nodes.

Context

Following are the types of SAP directories:

- Physically shared directories: `/<sapmnt>/<SAPSID>` and `/usr/sap/trans`

- Logically shared directories that are bound to a node, such as `/usr/sap`, with the following local directories:
 - `/usr/sap/<SAPSID>`
 - `/usr/sap/<SAPSID>/SYS`
 - `/usr/sap/hostctrl`
- Local directories that contain the SAP instances such as `/usr/sap/<SAPSID>/ASCS<Instance_Number>`
- The global transport directory may reside on a separate SAP transport host as a standard three systems transport layer configuration.

You need at least two nodes and a shared file system for distributed ASCS and ERS instances. The assumption is that the rest of the components are distributed on other nodes.

ASCS and ERS installation

In order for the ASCS and ERS instances to be able to move from one node to the other, they need to be installed on a shared file system and use virtual hostnames based on the virtual IP.

In this VPC-based SAP HA solution, the shared file system that is required by the cluster is replaced by the NFS-mounted file storage, and the virtual IP is replaced by the Application Load Balancer for VPC (ALB).

In this scenario, three ALBs are used, one for each Single Point of Failure (SPOF) component in order to replace the virtual IP requirement: ALB for ASCS, ALB for ERS, and ALB for ASE Sybase. Each ALB is configured as a backend for the corresponding cluster servers and redirects all of the communication that is received on the front-end ports to the active server in the backend pool.

Load balancers for VPC						
Region:	Frankfurt	▼	<input type="text"/> poc	X		
Name	Status	Family	Resource group	Type	Hostname	Location
db-alb-hana-poc	Active	Application	wes-ic4sap-resourcegroup	Private	20bdd130-eu-de.lb.appdomain.cloud	Frankfurt
sap-alb-ers-poc	Active	Application	wes-ic4sap-resourcegroup	Private	3941d983-eu-de.lb.appdomain.cloud	Frankfurt
sap-alb-ascs-poc	Active	Application	wes-ic4sap-resourcegroup	Private	56a9190d-eu-de.lb.appdomain.cloud	Frankfurt

Application load balancer management of HA IPs mechanism

Private application load balancer

A [private application load balancer](#) is accessible through your private subnets that you configured to create the load balancer.

Similar to a public application load balancer, your private application load balancer service instance is assigned an FQDN; however, this domain name is registered with one or more private IP addresses.

IBM Cloud operations change the number and value of your assigned private IP addresses over time, based on maintenance and scaling activities. The backend virtual server instances that host your application must run in the same region and under the same VPC.

Use the assigned ALB FQDN to send traffic to the private application load balancer to avoid connectivity problems to your applications during system maintenance or scaling down activities.

Each ALB sends traffic to the cluster node where the application (ASCS, ERS, ASE Sybase DB) is running. During the cluster failover, the ALB redirects all the traffic to the new node where the resources are up and running.



Note: DNS-as-a-Service (DNSaaS) is the management IBM Cloud VPC DNS service of HA and FQDN (IPs) mechanism.



Note: The ALB has a default of 50 seconds for client and server timeout, so after 50 seconds of inactivity, the connection is closed. To support SAP connections through ALB and not lose connection after 50 seconds, you need to request a change this value to a minimum of 300 seconds (client-side idle connection = minimum 300s and server-side idle connection = minimum 300s). To request this change, open a support ticket. This is an account-wide change that affects all of the ALBs in your account. For more information, see [Connection timeouts](#).

DNS Services with VPC

[IBM Cloud DNS Services](#) provide private DNS to VPC users. Private DNS zones are resolvable only on IBM Cloud and from explicitly [permitted networks](#) in an account. To get started, create a DNS Services instance by using the IBM Cloud console.

DNS Services allows you to:

- Create the private DNS zones that are collections for holding the domain names.
- Create the DNS resource records under these DNS zones.
- Specify the access controls used for the DNS resolution of resource records on a zone-wide level.

DNS Services also maintains its own worldwide set of DNS resolvers. Instances that are provisioned under IBM Cloud on an IBM Cloud network can use resource records that are configured through IBM Cloud DNS Services by querying DNS Services resolvers.

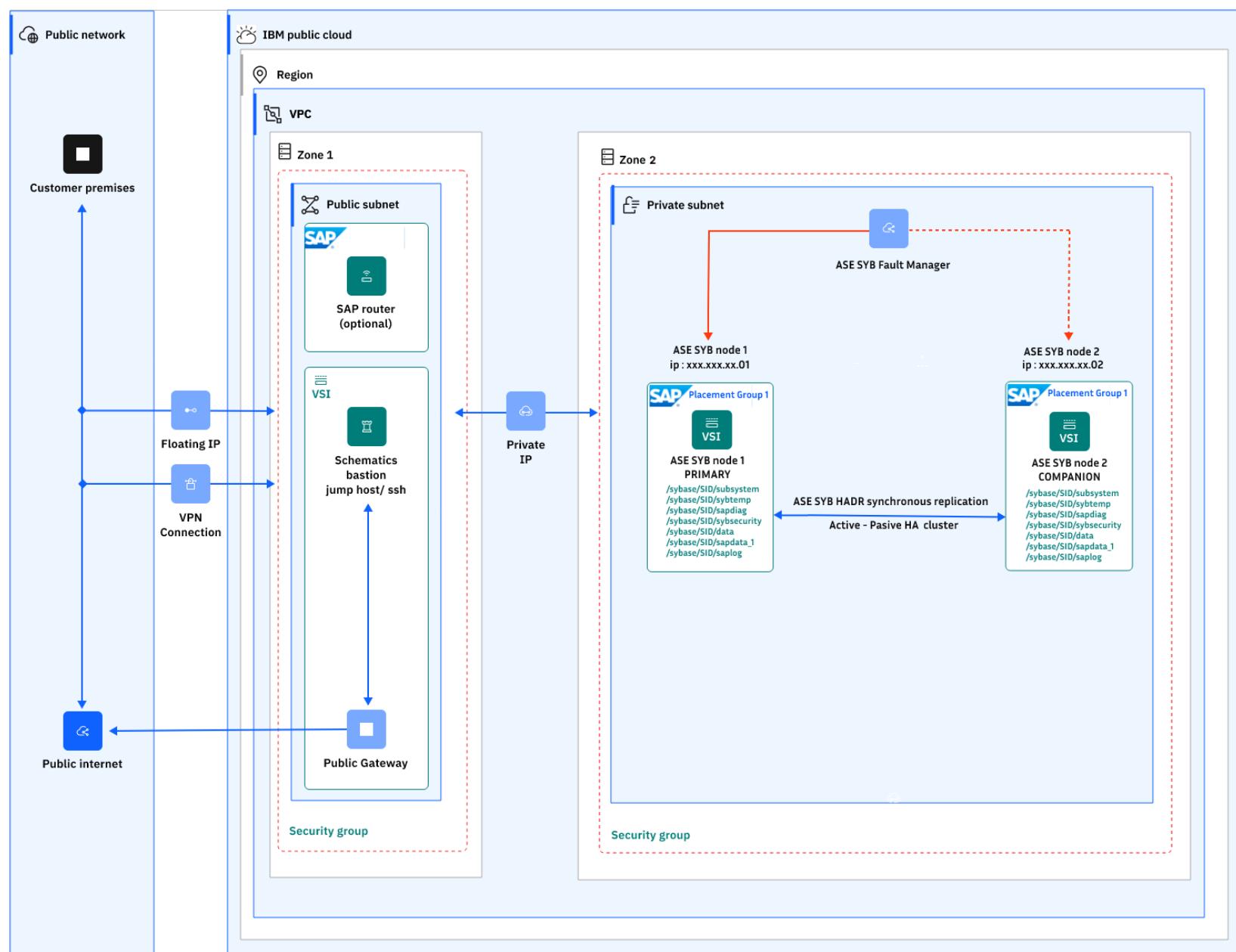
Resource records and zones that are configured through DNS Services are:

- Separated from the wider public DNS, and their publicly accessible records.
- Hidden from the system outside of and not part of the IBM Cloud private network.
- Accessible only from the system that you authorize on the IBM Cloud private network.
- Resolvable only via the resolvers provided by the service.

The DNS service maps the FQDN of each ALB to the virtual hostnames of the ASCS, ERS, and ASE Sybase that are used by SAP applications.

Type	Name	Value	TTL
CNAME	dbpochana	is an alias of 20bdd130-eu-de.lb.appdomain.cloud	12 hr
CNAME	sappocers	is an alias of 3941d983-eu-de.lb.appdomain.cloud	12 hr
CNAME	sappocases	is an alias of 56a9190d-eu-de.lb.appdomain.cloud	12 hr

Highly available system for SAP ASE Sybase database with HADR system



SAP HA for ASE Sybase DB instances cluster nodes primary (Active) and Secondary (Companion)

At the most basic level, a standard HA ASE Sybase cluster in an active(primary)-passive(companion) configuration has two nodes: one is the primary node and the other is the standby node. This means that the primary node is actively serving the active SAP DB instances (Primary and Companion), while the standby node is waiting to jump in if there is any failure.

The cluster is set with a virtual hostname IP (hostname is mapped to the FQDN of the ASE Sybase ALB through DNS, which is the same as

explained previously for SAP ASCS and ERS instances). Application instances (PAS and AAS) are used on the SAP profiles to call that particular component. The cluster assigns the virtual IP to the active node and uses a heartbeat monitor to confirm the availability of the components. If the primary node stops responding, it triggers the automatic failover mechanism that calls the standby node to step up to become the primary node. The ALB detects the change, redirects the traffic to the new active node, and assigns the virtual IP to it, restoring the component availability. Once fixed, the failed node comes online as a standby node.

SAP Sybase HADR system supports synchronous replication

The SAP Sybase HADR system supports synchronous replication between the primary and standby servers for high availability. An active-active setup is a two-node configuration where both nodes in the cluster include SAP ASE managing independent workloads, capable of taking over each others workload in the event of a failure.

The SAP ASE server that takes over the workload is called a secondary companion, and the SAP ASE server that fails is called the primary companion. Together they are companion servers. This movement from one node to another is called failover. After the primary companion is ready to resume its workload, it is moved back to its original node. This movement is called a failback.

When a system fails over, clients that are connected to the primary companion and use the failover property automatically reestablish their network connections to the secondary companion. You must tune your operating system to successfully manage both servers during fail over. See your operating system documentation for information about configuring your system for high availability. An SAP ASE configured for failover in an active-active setup can be shut down using the shutdown command only after you have suspended SAP ASE from the companion configuration, at both the server level and the platform level.

The always-on option in a High Availability and Disaster Recovery (HADR) system consists of two SAP ASE servers:

- Primary on which all transaction processing takes place.
- Warm standby (referred to as a "standby server" in DR mode, and as a "companion" in HA mode) for the primary server, and contains copies of designated databases from the primary server.



Note: The HADR feature that is shipped with SAP ASE version 16.0 SP02 supports only a single-companion server.

Some high-availability solutions (for example, the SAP Adaptive Server Enterprise Cluster Edition) share or use common resources between nodes. However, the HADR system is a "shared nothing" configuration, each node has separate resources including disks.

In an HADR system, servers are separate entities and data is replicated from the primary server to the companion server. If the primary server fails, a companion server is promoted to the role of primary server either manually or automatically. Once the promotion is complete, clients can reconnect to the new primary server, and see all committed data, including data that was committed on the previous primary server.

Servers can be separated geographically, which makes an HADR system capable of withstanding the loss of an entire computing facility.



Note: The HADR system includes an embedded SAP Replication Server, which synchronizes the databases between the primary and companion servers. SAP ASE uses the Replication Management Agent (RMA) to communicate with Replication Server and SAP Replication Server uses Open Client connectivity to communicate with the companion SAP ASE.

The Replication Agent detects any data changes made on the primary server and sends them to the primary SAP Replication Server. In the figure above, the unidirectional arrows indicate that, although both SAP Replication Servers are configured, only one direction is enabled at a time.

The HADR system supports synchronous replication between the primary and standby servers for high availability so the two servers can keep in sync with Zero Data Loss (ZDL). This requires a network link that is fast enough between the primary and standby server so that synchronous replication can keep up with the primary servers workload. Generally, this means that the network latency is approximately the same speed as the local disk IO speed, a few (fewer than 10) milliseconds. Anything longer than a few milliseconds may result in a slower response to write operations at the primary.

The HADR system supports asynchronous replication between the primary and standby servers for disaster recovery. The primary and standby servers by using asynchronous replication can be geographically distant, meaning they can have a slower network link. With asynchronous replication, Replication Agent Thread captures the primary servers workload, which is delivered asynchronously to SAP Replication Server. The SAP Replication Server applies these workload change to the companion server.

The most fundamental service that is offered by the HADR system is the failover; planned or unplanned from the primary to the companion server, which allows maintenance activity to occur on the old primary server, while applications continue on the new primary.

The HADR system provides protection in the event of a disaster. If the primary server is lost, the companion server can be used as a replacement. Client applications can switch to the companion server, and the companion server is quickly available for users. If the SAP Replication Server was in synchronous mode before the failure of the primary server, the Fault Manager automatically initiates failover with

zero data loss.

Fault Manager installation on the SAP ASCS node

The required parameters are asked during the installation process to create a profile for the fault manager and then adds it to the instance start profile. It is also possible to run the installation by using an existing profile: `sybdbfm install pf=<SYBHA.PFL>` In this case, the installation process will only ask for profile parameters missing in the profile.



Note: Fault manger is integrated with ASCS on same SAP PAS/AAS cluster (start/stop/move together).

There may be some data loss if the SAP Replication Server was in asynchronous mode and you must use manual intervention to failover for disaster recovery.

Connection attempts to the companion server without the necessary privileges are silently redirected to the primary companion via the login redirection mechanism, which is supported by Connectivity libraries. If login redirection is not enabled, client connections fail and are disconnected.

The SAP ASE HADR option installs the below components:

- SAP ASE
- SAP Replication Server
- Replication Management Agent (RMA)
- SAP Host Agent
- Fault Manager
- SAP ASE Cockpit



Note: This automation is offered at no cost; however, the provisioned infrastructure comes at cost.

VPC with Additional Application Server (AAS) ABAP on Linux for SAP HANA

You can use Terraform scripts to create a single-tier VPC and create the AAS to HANA and AnyDB infrastructure on the VPC. The Terraform scripts use the VPC information that you provide and then call the Ansible playbook to create the SAP architecture on the specified VPC. Terraform on IBM Cloud® enables predictable and consistent provisioning of IBM Cloud Virtual Private Cloud (VPC) infrastructure resources so that you can rapidly build complex, cloud environments. IBM Cloud VPC infrastructure consists of SAP certified hardware that uses Intel® Xeon CPUs and more Intel® technologies.

You have two deployment methods to choose from:

- Terraform scripts that run from the CLI on your bastion server.
- Schematics user interface accessed from your cloud dashboard menu.

You can create SAP AAS NetWeaver 7.x on the SAP HANA-based ABAP stack.

SAP solution implemented

Many SAP enterprise solutions are built on the SAP platform (SAP NetWeaver) including:

- SAP HANA as Primary Persistence for SAP NetWeaver-based applications
- SAP Business Suite applications (ERP, CRM, and SCM, and other applications),
- SAP Business Warehouse (BW), and
- Other SAP enterprise solutions

SAP NetWeaver has two distinct aspects, ABAP and Java. Many applications that are built on the SAP NetWeaver's ABAP or Java (or both) application servers run on SAP DB owned HANA and ASE Sybase either in AnyDB platforms (MSSQL, Oracle, and Db2).

Technical interfaces are available for applications that are built on the SAP NetWeaver AS ABAP and AS Java to run on SAP HANA and AnyDB. However, specific development enablement is normally required for each application to ensure that it runs optimally on the SAP HANA. SAP Business Suite applications (ERP, CRM, SCM, and other applications), SAP Business Warehouse (BW), and other SAP NetWeaver-based applications were modified to run on SAP HANA and have many advantages. Also, various components and complimentary applications that are built on SAP NetWeaver can also run on SAP HANA or AnyDB by using the provided SAP NetWeaver DB interfaces.

The SAP HANA as primary persistence for SAP NetWeaver-based applications scenario has one restriction: SAP NetWeaver ABAP and Java

application servers must run on separate hardware servers from the SAP HANA hardware.

What is created

The scripts automate the virtual infrastructure resources, provisioning the processes for the SAP architecture in an existing VPC with a distributed environment. SAP AAS NetWeaver 7.x (HANA or ASE SYB) application server on a distinct VSI VPC system and SAP HANA DB on a dedicated server type VSI VPC box are provisioned. The scripts work in two phases.

During the first phase of [Automate SAP bastion server – SAP media storage repository](#), the following virtual infrastructure resources based on the components from the existing VPC created by the bastion server are:

- 1 VPC where the virtual server instance is provisioned.
- 1 security group. The rules for this security group are:
 - Allow inbound DNS traffic (port 53).
 - Allow inbound SSH traffic (TCP port 22).
 - Allow all outbound traffic from the virtual server instance.
 - Allow all traffic in the security group.
- 1 subnet to enable the networking in your VPC.
- 2 virtual server instances with SAP certified storage and network configurations.
- 1 floating IP address used to access your VPC virtual server instance over the public network.

During the second phase, the Ansible Playbooks is called and the SAP architecture is installed for both dedicated virtual server instance (VSI) SAP application; VSI system and dedicated SAP HANA VSI box. The SAP architecture that is deployed on the SAP NetWeaver 7.x release is a stand-alone dedicated SAP HANA 2.0 box release. For more information about this architecture, see [Automating SAP HANA stand-alone virtual server instance on IBM Cloud® VPC by using Terraform and Ansible](#).

You can provision only one instance of the service per IBM Cloud region.

Schematics deployment

When you run the scripts with the Schematics interface, you:

- Enter the workspace information.
- Enter the GitHub path for the chosen solution either on NetWeaver AAS for HANA.
- Modify the parameters in the Schematics interface. They are the same parameters as the `input.auto.tfvars` file that you use with the cli.

Virtual server instance configuration

Following are the supported operating system images for SAP NetWeaver primary application server:

- ibm-redhat-8-4-amd64-sap-applications-2
- ibm-redhat-8-6-amd64-sap-applications-2
- ibm-sles-15-3-amd64-sap-applications-2
- ibm-sles-15-4-amd64-sap-applications-3

Following are the supported operating system images for SAP HANA database:

- ibm-redhat-8-4-amd64-sap-hana-2
- ibm-redhat-8-6-amd64-sap-hana-2
- ibm-sles-15-3-amd64-sap-hana-2
- ibm-sles-15-4-amd64-sap-hana-1

For both server instances there are:

- Two SSH keys are configured to access SSH as `root`.
- Three storage volumes as described in the `input.auto.tfvars` file.

What is created for anydb

The scripts use the information that you provide for an existing VPC and deploy AAS to SAP HANA or AnyDB on a different host than CI (SAP Central Instance) VSI host. For more information about this architecture, see [SAP NetWeaver 7.x on UNIX with HANA or AnyDB on IBM Cloud](#)

[VPC on IBM Cloud VPC](#). You specify the information for the VPC to use in the `input.auto.tfvars` file.

The scripts call the Ansible Playbooks to install the SAP architecture.

Script files

The configuration and script files are provided on GitHub. Each supported interface for the SAP solution installation has its own folder in the GitHub repository:

- [GitHub repository for Terraform – AAS HANA](#)

Terraform interface

To run the Terraform script, you modify:

- The `input.auto.tfvars` file to specify the existing VPC resources for your solution. Specify the variables for the existing VPC:
 - VPC name
 - Security group
 - Subnet
 - Hostname
 - Profile
 - Image
 - Up to two SSH keys

You can change the default SAP system configuration settings to match your solution. You can also specify the location where you downloaded the SAP kits.

The IBM Cloud Provider plug-in for Terraform on IBM Cloud uses these configuration files to install AAS to SAP HANA and AnyDB on the specified VPC in your IBM Cloud account.

Support

There are no warranties of any kind, and there is no service or technical support available for these materials from IBM®. As a recommended practice, review carefully any materials that you download from this site before using them on a live system.

Though the materials provided herein are not supported by the IBM® Service organization, your comments are welcomed by the developers, who reserve the right to revise, readapt or remove the materials at any time. To report a problem, or provide suggestions or comments, open a GitHub issue.

Before you begin

Before you use the scripts in the bastion cli:

- Set up your account to access the VPC. Make sure that your account is [upgraded to a paid account](#).
- If you have not already, create a Bastion server to store the SAP kits. For more information, see [Automate SAP bastion server - SAP media storage repository](#).
- Download the SAP kits from the SAP Portal to your Deployment Server. Make note of the download locations. Ansible decompresses the files. For more information, see the [readme](#) file.
- [Create or retrieve an IBM Cloud API key](#). The API key is used to authenticate with the IBM Cloud platform and to determine your permissions for IBM Cloud services.
- [Create or retrieve your SSH key ID](#). You need the 40-digit UUID for the SSH key, not the SSH key name.
- Terraform should already be installed on the bastion server that you deployed. For more information, see [Bastion server for SAP deployment](#).
- (Optional - Catalog Tile) create secrets for your credentials and passwords by using the [Secrets Manager](#).

Deploying SAP AAS NetWeaver 7.x on HANA by using the Schematics user interface

Use these steps to configure the SAP Additional Application Server (AAS) NetWeaver with HANA or AnyDB on your existing VPC by using the Schematics interface. The script takes 2 - 3 hours to complete.

1. From the IBM Cloud menu, select **Schematics**.
2. Click **Create** workspace.

3. On the **Specify template** page:
 - Enter the URL for the Schematics interface.
 - Select the **Terraform version** that is listed in the readme file.
 - Click **Next**.
4. On the **workspace details** page:
 - Enter a name for the workspace.
 - Select a **Resource group**.
 - Select a **Location** for your workspace. The workspace location does not have to match the resource location.
 - Select **Next**.
5. Select **Create** to create your workspace.
6. On the workspace settings page, in the input variables section, review the default input variables and provide values that match your solution.
 For a more detailed description of each parameter, check the GitHub repo [AAS HANA readme](#) file, chapter "Input parameter file". Also, make sure to mark the parameters that contain sensitive information like passwords, API, and ssh private keys as "sensitive". These parameters are marked as "sensitive" in the readme file, under "Input parameter file".
7. On the workspace settings page, click **Generate plan**. Wait for the plan to complete.
8. Click **View log** to review the log files of your terraform execution plan.
9. Apply your Terraform template by clicking **Apply plan**.
10. Review the log file to ensure that no errors occur during the provisioning, modification, or deletion process.

Deploying SAP AAS NetWeaver (ABAP) on HANA with the Deployable Architecture tile interface

Use these steps to configure the SAP AAS NetWeaver (ABAP) on HANA on your existing VPC by using the catalog tile interface. The script takes 2 - 3 hours to complete.

1. From the IBM Cloud catalog, select **VPC with Additional Application Server ABAP on Linux for SAP HANA** on HANA tile. The **Create** tab opens for VPC with Additional Application Server ABAP on Linux for SAP HANA. For more information about this deployment, see the About tab or the readme file link.
2. Select the latest version.
3. Select **VPC with Additional Application Server ABAP on Linux for SAP HANA on Deployable Architecture tile** variation.
4. Click **Review deployment** options:
 - **Add to project** to add this deployment to an IBM Cloud project and combine it with other deployments. IBM Cloud projects include several more pipeline steps before deployment, including deployment validation, cost calculation, compliance verification, and approval process.
 - **Create from the CLI** to get the CLI command. With this command you can trigger the deployment from the CLI.
 - **Work with code** to embed the code into other terraform deployments.
 - **Deploy with IBM Cloud Schematics** to trigger the deployment process directly.
5. Select **Deploy with IBM Cloud Schematics**.
6. Add the input parameters for this installation. There are 3 categories of parameters:
 - **Workspace** - These parameters define the workspace that is automatically created in Schematics:
 - Enter a name for the workspace or use the default name.
 - The Resource Group used to create resources. Use default or create a Resource Group.
 - Select a location to create your Schematics workspace. The workspace location need not match the resource location.
 - **Required input variables** - Review the default input variables and provide values that match your solution. These parameters are specific to your deployment. For more detailed information, see the [Readme file](#).

Parameter	Description
BASTION_FLOATING_IP	Required only for Schematics Deployments. The Floating IP from the Bastion Server.

HOSTNAME	The hostname for the VSI. The hostname should be up to 13 characters as required by SAP. For more information on the rules regarding hostnames for SAP systems, check SAP Note 611361: Hostnames of SAP ABAP Platform servers
REGION	The cloud region to deploy the solution. The regions and zones for VPC are listed here . Review supported locations in IBM Cloud Schematics here . Sample value: eu-de.
RESOURCE_GROUP	The name of an existing Resource Group for VSIs and Volumes resources. Default value: "Default". The list of Resource Groups is available here .
SECURITY_GROUP	The name of an existing Security group. The list of security groups is available here .
SSH_KEYS	The list of SSH Keys UUIDs that are allowed to SSH as root to the VSI can contain one or more IDs. The list of SSH Keys is available here . Sample input (use your own SSH UUIDs from IBM Cloud){: external}: ["r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a", "r010-3fcfd9fe7-d4a7-41ce-8bb3-d96e936b2c7e"]
SUBNET	The name of an existing subnet. The list of subnets is available here .
VPC	The name of an existing VPC. The list of VPCs is available here .
ZONE	The cloud zone where to deploy the solution. Sample value: eu-de-2.
ibmcloud_api_key	IBM Cloud API key (Sensitive* value).
private_ssh_key	Required only for Schematics Deployments - Input your id_rsa private key pair content in OpenSSH format (Sensitive* value). This private key should be used only during the terraform provisioning and it is recommended to be changed after the SAP deployment.
hdb_instance_number	The instance number of the SAP HANA database server.
sap_aas_instance_number	Technical identifier for the internal processes of the additional application server.
sap_asci_instance_number	Technical identifier for the internal processes of ASCS.
sap_ci_host	IP address of the existing SAP Central Instance.
sap_ci_hostname	The hostname of the existing SAP Central Instance.
sap_ci_instance_number	Technical identifier for the internal processes of the Central Instance.
sap_sid	The SAP system ID identifies the entire SAP system.
sap_main_password	Common password for all users that are created during the installation (See Obs*).

Required Variables

- **Optional variables** - Review and update the optional input variables. The Ansible scripts expect the SAP kits to be in the default locations listed. For more information, see the [Readme file - Input Parameters](#).

Parameter	Description
ID_RSA_FILE_PATH	The file path for private_ssh_key is automatically generated by default. If it is changed, it must contain the relative path from Git repo folders. Default value: "ansible/id_rsa".
IMAGE	The OS image used for the VSI. A list of images is available here .
PROFILE	The profile used for the VSI. A list of profiles is available here . For more information about supported DB/OS and IBM Gen 2 Virtual Server Instances (VSI), check SAP Note 2927211: SAP Applications on IBM Virtual Private Cloud .

VOL1	Volume 1 Size - The size for the disks in GB that are to be attached to the VSI and used by SAP.
VOL2	Volume 2 Size - The size for the disks in GB that are to be attached to the VSI and used by SAP.
kit_sapcar_file	Path to the sapcar binary, as downloaded from SAP Support Portal.
kit_swpm_file	Path to the SWPM archive (SAR), as downloaded from SAP Support Portal.
kit_saphostagent_file	Path to the SAP Host Agent archive (SAR), as downloaded from SAP Support Portal.
kit_hdbclient_file	Path to the HANA DB client archive (SAR), as downloaded from SAP Support Portal.

Optional Variables

7. Accept the license agreement.
8. Select **Deploy**. The deployment starts and you are directed to the Schematics page that displays the script log files for you to monitor the deployment progress.

Creating the infrastructure using Terraform with the bastion server CLI

Use these steps to configure the IBM Cloud Provider plug-in and use Terraform to install SAP AAS to SAP HANA and AnyDB on your existing VPC on an already deployed SAP NetWeaver 7.X with SAP HANA 2.0 or ASE SYB as a Central Instance.

The script takes 1 - 2 hours to complete.

1. Access the bastion server cli.
2. Clone the solution repository and change to the folder.

ASE SYB 16 Clone the solution repository from <https://github.com/IBM-Cloud/sap-aas-abap-ase-syb> and cd to the sap-aas-abap-ase-syb/cli folder.

```
$ git clone https://github.com/IBM-Cloud/sap-aas-abap-ase-syb
cd sap-aas-abap-ase-syb/cli/
```

SAP HANA 2.0: Clone the solution repository from <https://github.com/IBM-Cloud/sap-abap-hana-aas> and cd to the sap-abap-hana-aas folder.

```
$ git clone https://github.com/IBM-Cloud/sap-abap-hana-aas.git
cd sap-abap-hana-aas/
```

3. Modify the `input.auto.tfvars` file to specify the information for the existing VPC, your region, zone, networking component names, hostname for the AAS VSI,profile, and image. You need your 40-digit SSH key ID for this file. The second SSH key is optional. For more options for profile, see [Instance Profiles](#). For more options, see [Images](#). For descriptions of the variables, see the [readme](#) file.

The VSI OS images that are supported for this solution for Netweaver Additional Application Server are:

- ibm-redhat-8-4-amd64-sap-applications-2
- ibm-redhat-8-6-amd64-sap-applications-2
- ibm-sles-15-3-amd64-sap-applications-2
- ibm-sles-15-4-amd64-sap-applications-4

```
$ # Infra VPC variables for ASE SYB
REGION    = "eu-de"
ZONE      = "eu-de-2"
VPC       = "ic4sap"                      # EXISTING Security group name
SECURITY_GROUP = "ic4sap-securitygroup"     # EXISTING Security group name
RESOURCE_GROUP = "wes-automation"
SUBNET    = "ic4sap-subnet"                 # EXISTING Subnet name
SSH_KEYS   = [ "r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a" , "r010-3fcfd9fe7-d4a7-41ce-8bb3-
d96e936b2c7e" ]

# SAP AAS VSI variables:
```

```

HOSTNAME = "sapnwase-as01"
PROFILE = "bx2-4x16"
IMAGE = "ibm-redhat-8-4-amd64-sap-applications-2

$ # Infra VPC variables for ABAP HANA
REGION      = "eu-de"
ZONE        = "eu-de-2"
VPC          = "ic4sap" # EXISTING Security group name
SECURITY_GROUP = "ic4sap-securitygroup" # EXISTING Security group name
RESOURCE_GROUP = "wes-automation"
SUBNET       = "ic4sap-subnet" # EXISTING Subnet name
SSH_KEYS     = [ "r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a" , "r010-3fc9fe7-d4a7-41ce-8bb3-d96e936b2c7e" ]
ID_RSA_FILE_PATH = "ansible/id_rsa"

# SAP AAS variables:
HOSTNAME = "sapnwapp"
PROFILE = "bx2-4x16"
IMAGE = "ibm-redhat-8-6-amd64-sap-applications-2"

```

4. Customize your SAP system configuration. In the same file, input.auto.tfvars, edit the SAP system configuration variables that are passed to the Ansible automated deployment. For descriptions of the variables, see the [readme](#) file.

```

$ # SAP system configuration - for ASE SYB
sap_sid = "NWD"
sap_ci_host = "10.243.132.10"
sap_ci_hostname = "sapnwase"
sap_ci_instance_number = "00"
sap_asc_s_instance_number = "01"
sap_aas_instance_number = "00"

# Kits paths
kit_sapcar_file = "/storage/NW75SYB/SAPCAR_1010-70006178.EXE"
kit_swpm_file = "/storage/NW75SYB/SWPM10SP31_7-20009701.SAR"
kit_saphotagent_file = "/storage/NW75SYB/SAPHOSTAGENT51_51-20009394.SAR"

```

```

$ # SAP system configuration - for ABAP HANA
sap_sid = "NWD"
sap_ci_host = "10.243.132.10"
sap_ci_hostname = "sapnwapp01"
sap_ci_instance_number = "00"
sap_asc_s_instance_number = "01"
hdb_instance_number = "00"
sap_aas_instance_number = "00"

# Kits paths
kit_sapcar_file = "/storage/NW75HDB/SAPCAR_1010-70006178.EXE"
kit_swpm_file = "/storage/NW75HDB/SWPM10SP31_7-20009701.SAR"
kit_saphotagent_file = "/storage/NW75HDB/SAPHOSTAGENT51_51-20009394.SAR"
kit_hdbclient_file = "/storage/NW75HDB/IMDB_CLIENT20_009_28-80002082.SAR"

```

Ansible decompresses the rest of the SAP kit files. For more information, see the [readme](#) file.

5. Initialize the Terraform CLI.

```
terraform init
```

6. Create a Terraform execution plan. The Terraform execution plan summarizes all the actions that are done to create the virtual private cloud instance in your account.

```
terraform plan plan1
```

Enter an SAP main password and your API key.

The SAP main password must be 10 - 14 characters long and contain at least one digit (0-9). It can contain only the following characters: a-z, A-Z, 0-9, @, #, \$, . *This password cannot contain exclamation points '!'. The password must not start with a digit or an underscore ().*

7. Verify that the plan shows all of the resources that you want to create and that the names and values are correct. If the plan needs to be adjusted, edit the input.auto.tfvars file to correct resources and run terraform plan again.
8. Apply the saved plan.

```
$ terraform apply "plan1"
```

The virtual private cloud and components are created and you see output similar to the `terraform plan` output.

9. Add the SAP credentials and the virtual server instance IP to the SAP GUI. For more information about the SAP GUI, see [SAP GUI](#).

Next steps

If you need to rename your resources after they are created, modify the `input.auto.tfvars` file to change the names and run `terraform plan` and `terraform apply` again. Do not use the IBM Cloud Dashboard and user interface to modify your VPC after it is created. The Terraform scripts create a complete solution and selectively modifying resources with the user interface might cause unexpected results.

If you need to remove the SAP Netweaver 7.X on HANA or AnyDB installation, go to your project folder and run `terraform destroy`. The `terraform destroy` command does not remove the VPC in this scenario because the VPC was created before these Terraform scripts were run.

Related information

For more information about Terraform on IBM Cloud, see [Getting started with Terraform on IBM Cloud](#).

For more information about using Terraform for creating only a VPC for SAP, without the SAP architecture, see [Creating single-tier virtual private cloud for SAP by using Terraform](#).

SAP One Support Notes that apply to this document:

- [SAP Note 84555 - Windows Server, Linux®, and UNIX: Certified hardware](#)
- [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#)
- [SAP Note 2923773 - Linux® on IBM Cloud \(IaaS\): Adaption of your SAP license](#)
- [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#)
- [SAP Note 2369910 - SAP Software on Linux®: General information](#)
- [SAP Note 171380 - Released IBM hardware \(Intel processors\) and IBM cloud services offers](#)
- [SAP Note 1380654 - SAP support in IaaS environments](#)

This document is referenced by:

- [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#)
- [SAP Note 2588225 - SAP on IBM Cloud: Protect against speculative execution vulnerabilities](#)
- [SAP Note 1380654 - SAP support in IaaS environments](#)
- [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#)

SAP NetWeaver (ABAP) on SAP ASE HA deployment in VPC

Automating SAP workload HA deployment on IBM Cloud VPC with Terraform and Ansible

You can use Terraform to automate IBM Cloud® VPC provisioning. The VPC provisioned includes virtual server instances with high network performance. The VPC infrastructure contains various Infrastructure-as-a-Service (IaaS) offerings, including virtual servers. After the VPC is provisioned, the scripts use the Ansible Playbooks to install the SAP system.

IBM Cloud VPC introduction

VPC is a public cloud offering that an enterprise uses to establish its own private cloud-like computing environment on shared [public cloud](#) infrastructure. VPC gives an enterprise the ability to define and control a virtual network that is logically isolated from all other public cloud tenants, creating a private and secure place on the public cloud.

Imagine that a cloud provider's infrastructure is a residential apartment building and multiple families live inside. A public cloud tenant is a kind of sharing an apartment with a few roommates. In contrast, having a VPC is like having your own private condominium; no one else has the key, and no one can enter the space without your permission.

VPC's logical isolation is implemented by using virtual network functions and security features that give the enterprise customer granular control over which IP addresses or applications can access particular resources. It is analogous to the "friends-only" or "public/private" controls on social media accounts used to restrict who can or can't see your otherwise public posts.

With IBM Cloud VPC, you can use the UI, CLI, and API to manually provision virtual server instances for VPC with high network performance. VPC infrastructure contains various Infrastructure-as-a-Service (IaaS) offerings including virtual servers for VPC.

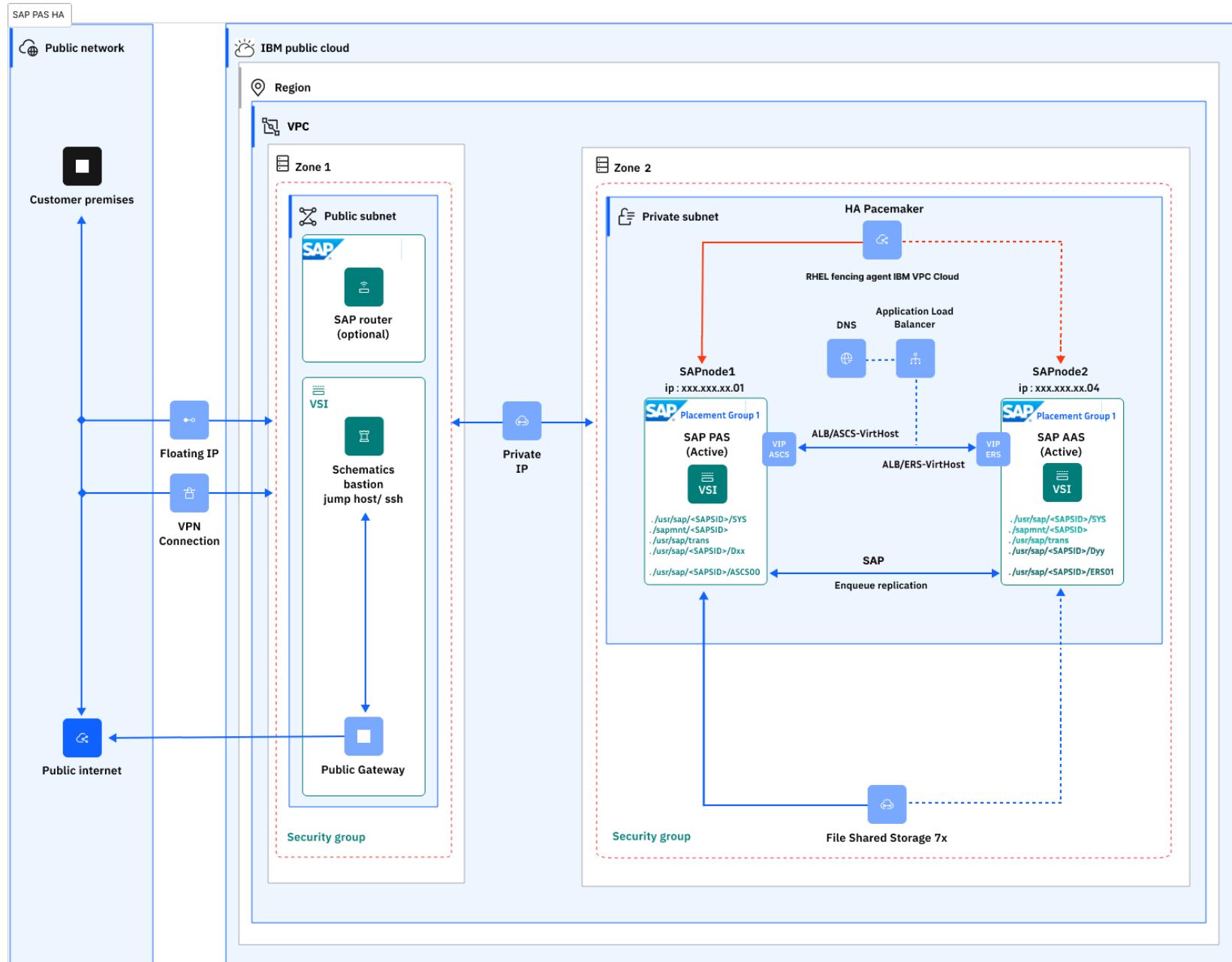
Use the following information to understand a simple use-case for planning, creating, and configuring resources for your VPC, and learn more about VPC overviews and VPC tutorials. For more information about the VPC, see [Getting started with Virtual Private Cloud \(VPC\)](#).

SAP products architecture on IBM Cloud VPC

A [Virtual Private Cloud \(VPC\)](#) contains one of the most secure and reliable cloud environments for SAP applications within your own VPC with virtual server instances. This represents an Infrastructure-as-a-Service (IaaS){: external} within IBM Cloud that offers all the benefits of isolated, secure, and flexible virtual cloud infrastructure from IBM. In comparison, the IBM Cloud classic infrastructure virtual servers offering uses virtual instances with native and VLAN networking to communicate with each other within a data center; however, the instances are restricted in one well-working pod by using subnet and VLAN networking as a gap scale up of virtual resources should rely between the pods. The IBM Cloud VPC network orchestrator layer concept eliminates the pod boundaries and restrictions, so this new concept handles all the networking for every virtual instance running within VPC across regions and zones.

Highly available system for SAP NetWeaver on IBM Cloud VPC

In a Highly Available (HA) system, every instance can run on a separate IBM Cloud virtual server instance. The cluster HA configuration for the SAP application server consists of two virtual server instances, each of them located in the same zone within the region by using placement groups. Placement groups assure that both cluster resources and cloud resources are also located in different compute nodes as specified in the following placement groups section:



SAP HA for SAP applications cluster nodes PAS (Active) and AAS (Active)

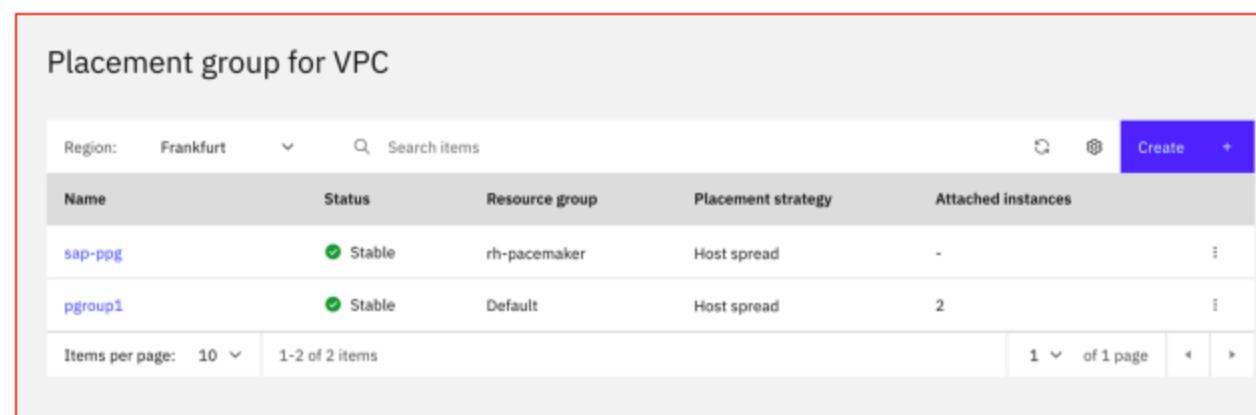
Placement groups on IBM Cloud VPC for SAP HA architecture

Placement Groups (PG) for VPC have two different anti-affinity strategies for high availability. By using the placement strategies, you minimize the chance of service disruption with virtual server instances that are placed on different hosts or into an infrastructure with separate power and network supplies.

The design of placement groups for IBM Cloud virtual servers solves this issue. Placement groups give a measure of control over the host on which a new public virtual server is placed. In this release, a “spread” rule is implemented, which means that the virtual servers within a placement group are spread onto different hosts. You can build a highly available application within a data center and know that your virtual servers are isolated from each other.

Placement groups with the spread rule are available to create in selected IBM Cloud data centers. After a spread rule is created, you can provision a virtual server into that group and ensure that it is not on the same host as any of your other virtual servers. This feature comes with no cost.

You can create your placement group and assign up to four new virtual server instances. With the spread rule, each of your virtual servers are provisioned on different physical hosts. In the following configuration example, the “Power Spread” option is used:



Placement groups host spread

Placement group for VPC					
Name	Status	Resource group	Placement strategy	Attached instances	
sapha-poc	Stable	wes-ic4sap-resourcegroup	Power spread	4	
Items per page: 10 1 item 1 of 1 page					

Placement groups power spread

Following are the SAP instances that are required for HA scenario:

- ABAP SAP Central Services (ASCS) instance - contains the ABAP message server and the ABAP enqueue server.
- Enqueue Replication Server (ERS) instance for the ASCS instance.
- Database instance
- Primary Application Server (PAS) instance on node 1.
- Additional Application Server (AAS) instance on node 2.



Note: It is recommended to run both the ASCS instance and the ERS instance in a switchover cluster infrastructure.

IBM Cloud File Storage for VPC for SAP HA architecture

[IBM Cloud File Storage for VPC](#) technology is used to make the SAP directories available to the SAP system. The technologies of choice are NFS, shared disks, and cluster file system. If you have decided to use the HA solution for your SAP system, make sure that you properly address the HA requirements of the SAP file systems in your SAP environment.

File shares for VPC								
Name	Status	Resource groups	Location	Mount targets	Size	Replication role	Encryption type	
usrsap-as1-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-as2-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-sapsacs-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-sapers-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-sapmnt-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-sapsys-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-trans-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	80 GB	None	Provider managed	

File shares for VPC

- File shares that are mounted as NFS permanent file systems on both cluster nodes for SAP HA application:
 - `/usr/sap/<SAPSID>/SYS`
 - `/sapmnt<SAPSID>`
 - `/usr/sap/trans`
- Cluster-managed file systems for SAP HA application: ASCS
 - `/usr/sap/<SAPSID>/ASCS00`
 - `/usr/sap/<SAPSID>/ERS01`
- Permanent NFS mount on SAP HA application node 1 PAS instance:
 - `/usr/sap/<SAPSID>/Dxx`
- Permanent NFS mount on SAP HA application node 2 dialog instance:
 - `/usr/sap/<SAPSID>/Dyy`

Prerequisites

You need to install the hardware (hosts, disks, and network) and decide how to distribute the database, SAP instances, and if required, the Network File System (NFS) server over the cluster nodes.

Context

Following are the types of SAP directories:

- Physically shared directories: `/<sapmnt>/<SAPSID>` and `/usr/sap/trans`

- Logically shared directories that are bound to a node, such as `/usr/sap`, with the following local directories:
 - `/usr/sap/<SAPSID>`
 - `/usr/sap/<SAPSID>/SYS`
 - `/usr/sap/hostctrl`
- Local directories that contain the SAP instances such as `/usr/sap/<SAPSID>/ASCS<Instance_Number>`
- The global transport directory may reside on a separate SAP transport host as a standard three systems transport layer configuration.

You need at least two nodes and a shared file system for distributed ASCS and ERS instances. The assumption is that the rest of the components are distributed on other nodes.

ASCS and ERS installation

In order for the ASCS and ERS instances to be able to move from one node to the other, they need to be installed on a shared file system and use virtual hostnames based on the virtual IP.

In this VPC-based SAP HA solution, the shared file system that is required by the cluster is replaced by the NFS-mounted file storage, and the virtual IP is replaced by the Application Load Balancer for VPC (ALB).

In this scenario, three ALBs are used, one for each Single Point of Failure (SPOF) component in order to replace the virtual IP requirement: ALB for ASCS, ALB for ERS, and ALB for ASE Sybase. Each ALB is configured as a backend for the corresponding cluster servers and redirects all of the communication that is received on the front-end ports to the active server in the backend pool.

Load balancers for VPC						
Region:	Frankfurt	▼	<input type="text"/> poc	X		
Name	Status	Family	Resource group	Type	Hostname	Location
db-alb-hana-poc	Active	Application	wes-ic4sap-resourcegroup	Private	20bdd130-eu-de.lb.appdomain.cloud	Frankfurt
sap-alb-ers-poc	Active	Application	wes-ic4sap-resourcegroup	Private	3941d983-eu-de.lb.appdomain.cloud	Frankfurt
sap-alb-ascs-poc	Active	Application	wes-ic4sap-resourcegroup	Private	56a9190d-eu-de.lb.appdomain.cloud	Frankfurt

Application load balancer management of HA IPs mechanism

Private application load balancer

A [private application load balancer](#) is accessible through your private subnets that you configured to create the load balancer.

Similar to a public application load balancer, your private application load balancer service instance is assigned an FQDN; however, this domain name is registered with one or more private IP addresses.

IBM Cloud operations change the number and value of your assigned private IP addresses over time, based on maintenance and scaling activities. The backend virtual server instances that host your application must run in the same region and under the same VPC.

Use the assigned ALB FQDN to send traffic to the private application load balancer to avoid connectivity problems to your applications during system maintenance or scaling down activities.

Each ALB sends traffic to the cluster node where the application (ASCS, ERS, ASE Sybase DB) is running. During the cluster failover, the ALB redirects all the traffic to the new node where the resources are up and running.



Note: DNS-as-a-Service (DNSaaS) is the management IBM Cloud VPC DNS service of HA and FQDN (IPs) mechanism.



Note: The ALB has a default of 50 seconds for client and server timeout, so after 50 seconds of inactivity, the connection is closed. To support SAP connections through ALB and not lose connection after 50 seconds, you need to request a change this value to a minimum of 300 seconds (client-side idle connection = minimum 300s and server-side idle connection = minimum 300s). To request this change, open a support ticket. This is an account-wide change that affects all of the ALBs in your account. For more information, see [Connection timeouts](#).

DNS Services with VPC

[IBM Cloud DNS Services](#) provide private DNS to VPC users. Private DNS zones are resolvable only on IBM Cloud and from explicitly [permitted networks](#) in an account. To get started, create a DNS Services instance by using the IBM Cloud console.

DNS Services allows you to:

- Create the private DNS zones that are collections for holding the domain names.
- Create the DNS resource records under these DNS zones.
- Specify the access controls used for the DNS resolution of resource records on a zone-wide level.

DNS Services also maintains its own worldwide set of DNS resolvers. Instances that are provisioned under IBM Cloud on an IBM Cloud network can use resource records that are configured through IBM Cloud DNS Services by querying DNS Services resolvers.

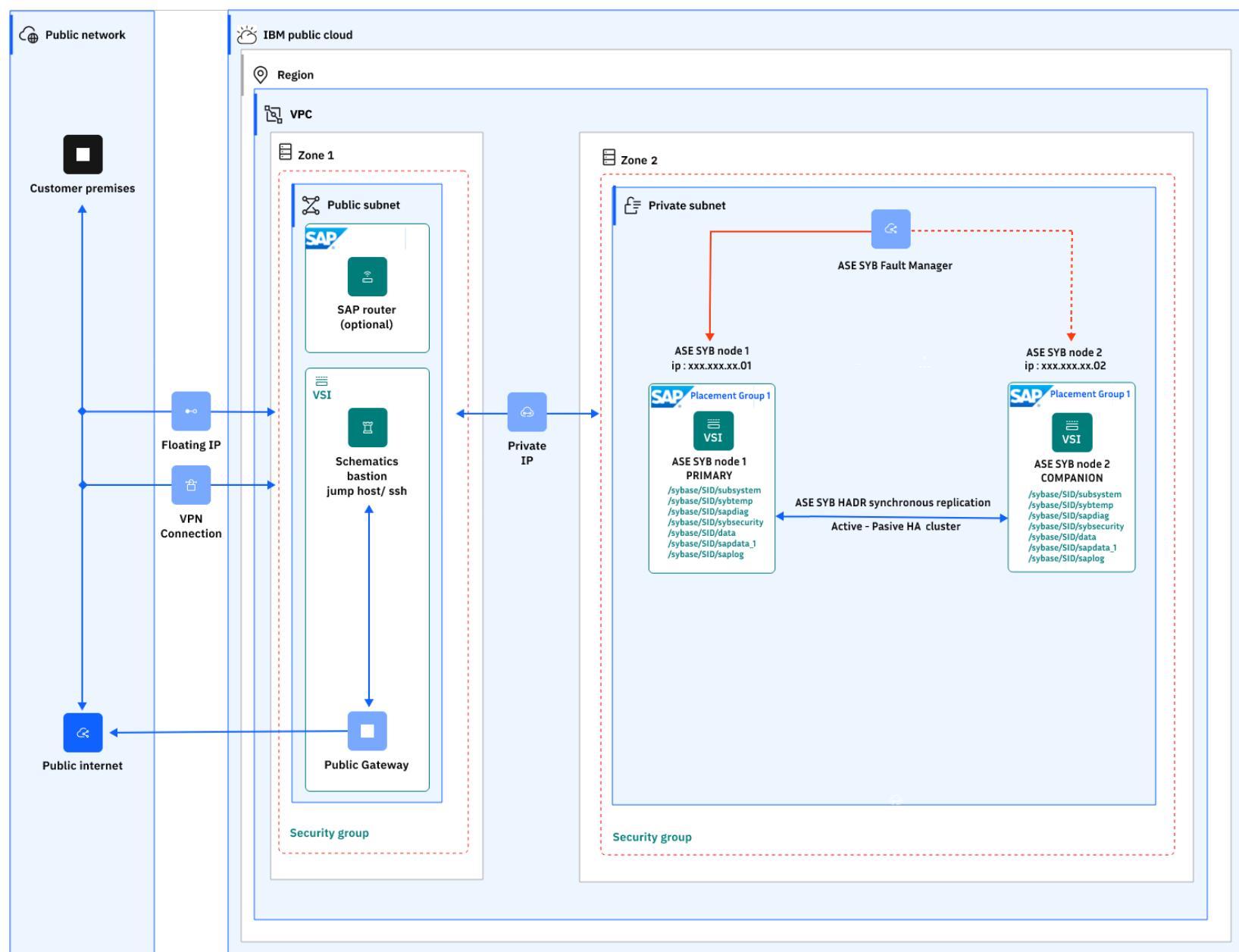
Resource records and zones that are configured through DNS Services are:

- Separated from the wider public DNS, and their publicly accessible records.
- Hidden from the system outside of and not part of the IBM Cloud private network.
- Accessible only from the system that you authorize on the IBM Cloud private network.
- Resolvable only via the resolvers provided by the service.

The DNS service maps the FQDN of each ALB to the virtual hostnames of the ASCS, ERS, and ASE Sybase that are used by SAP applications.

Type	Name	Value	TTL
CNAME	dbpochana	is an alias of 20bdd130-eu-de.lb.appdomain.cloud	12 hr
CNAME	sappocers	is an alias of 3941d983-eu-de.lb.appdomain.cloud	12 hr
CNAME	sappocases	is an alias of 56a9190d-eu-de.lb.appdomain.cloud	12 hr

Highly available system for SAP ASE Sybase database with HADR system



SAP HA for ASE Sybase DB instances cluster nodes primary (Active) and Secondary (Companion)

At the most basic level, a standard HA ASE Sybase cluster in an active(primary)-passive(companion) configuration has two nodes: one is the primary node and the other is the standby node. This means that the primary node is actively serving the active SAP DB instances (Primary and Companion), while the standby node is waiting to jump in if there is any failure.

The cluster is set with a virtual hostname IP (hostname is mapped to the FQDN of the ASE Sybase ALB through DNS, which is the same as

explained previously for SAP ASCS and ERS instances). Application instances (PAS and AAS) are used on the SAP profiles to call that particular component. The cluster assigns the virtual IP to the active node and uses a heartbeat monitor to confirm the availability of the components. If the primary node stops responding, it triggers the automatic failover mechanism that calls the standby node to step up to become the primary node. The ALB detects the change, redirects the traffic to the new active node, and assigns the virtual IP to it, restoring the component availability. Once fixed, the failed node comes online as a standby node.

SAP Sybase HADR system supports synchronous replication

The SAP Sybase HADR system supports synchronous replication between the primary and standby servers for high availability. An active-active setup is a two-node configuration where both nodes in the cluster include SAP ASE managing independent workloads, capable of taking over each others workload in the event of a failure.

The SAP ASE server that takes over the workload is called a secondary companion, and the SAP ASE server that fails is called the primary companion. Together they are companion servers. This movement from one node to another is called failover. After the primary companion is ready to resume its workload, it is moved back to its original node. This movement is called a failback.

When a system fails over, clients that are connected to the primary companion and use the failover property automatically reestablish their network connections to the secondary companion. You must tune your operating system to successfully manage both servers during fail over. See your operating system documentation for information about configuring your system for high availability. An SAP ASE configured for failover in an active-active setup can be shut down using the shutdown command only after you have suspended SAP ASE from the companion configuration, at both the server level and the platform level.

The always-on option in a High Availability and Disaster Recovery (HADR) system consists of two SAP ASE servers:

- Primary on which all transaction processing takes place.
- Warm standby (referred to as a "standby server" in DR mode, and as a "companion" in HA mode) for the primary server, and contains copies of designated databases from the primary server.



Note: The HADR feature that is shipped with SAP ASE version 16.0 SP02 supports only a single-companion server.

Some high-availability solutions (for example, the SAP Adaptive Server Enterprise Cluster Edition) share or use common resources between nodes. However, the HADR system is a "shared nothing" configuration, each node has separate resources including disks.

In an HADR system, servers are separate entities and data is replicated from the primary server to the companion server. If the primary server fails, a companion server is promoted to the role of primary server either manually or automatically. Once the promotion is complete, clients can reconnect to the new primary server, and see all committed data, including data that was committed on the previous primary server.

Servers can be separated geographically, which makes an HADR system capable of withstanding the loss of an entire computing facility.



Note: The HADR system includes an embedded SAP Replication Server, which synchronizes the databases between the primary and companion servers. SAP ASE uses the Replication Management Agent (RMA) to communicate with Replication Server and SAP Replication Server uses Open Client connectivity to communicate with the companion SAP ASE.

The Replication Agent detects any data changes made on the primary server and sends them to the primary SAP Replication Server. In the figure above, the unidirectional arrows indicate that, although both SAP Replication Servers are configured, only one direction is enabled at a time.

The HADR system supports synchronous replication between the primary and standby servers for high availability so the two servers can keep in sync with Zero Data Loss (ZDL). This requires a network link that is fast enough between the primary and standby server so that synchronous replication can keep up with the primary servers workload. Generally, this means that the network latency is approximately the same speed as the local disk IO speed, a few (fewer than 10) milliseconds. Anything longer than a few milliseconds may result in a slower response to write operations at the primary.

The HADR system supports asynchronous replication between the primary and standby servers for disaster recovery. The primary and standby servers by using asynchronous replication can be geographically distant, meaning they can have a slower network link. With asynchronous replication, Replication Agent Thread captures the primary servers workload, which is delivered asynchronously to SAP Replication Server. The SAP Replication Server applies these workload change to the companion server.

The most fundamental service that is offered by the HADR system is the failover; planned or unplanned from the primary to the companion server, which allows maintenance activity to occur on the old primary server, while applications continue on the new primary.

The HADR system provides protection in the event of a disaster. If the primary server is lost, the companion server can be used as a replacement. Client applications can switch to the companion server, and the companion server is quickly available for users. If the SAP Replication Server was in synchronous mode before the failure of the primary server, the Fault Manager automatically initiates failover with

zero data loss.

Fault Manager installation on the SAP ASCS node

The required parameters are asked during the installation process to create a profile for the fault manager and then adds it to the instance start profile. It is also possible to run the installation by using an existing profile: `sybdbfm install pf=<SYBHA.PFL>` In this case, the installation process will only ask for profile parameters missing in the profile.



Note: Fault manger is integrated with ASCS on same SAP PAS/AAS cluster (start/stop/move together).

There may be some data loss if the SAP Replication Server was in asynchronous mode and you must use manual intervention to failover for disaster recovery.

Connection attempts to the companion server without the necessary privileges are silently redirected to the primary companion via the login redirection mechanism, which is supported by Connectivity libraries. If login redirection is not enabled, client connections fail and are disconnected.

The SAP ASE HADR option installs the below components:

- SAP ASE
- SAP Replication Server
- Replication Management Agent (RMA)
- SAP Host Agent
- Fault Manager
- SAP ASE Cockpit



Note: This automation is offered at no cost; however, the provisioned infrastructure comes at cost.

VPC with Additional Application Server (AAS) ABAP on Linux for SAP HANA

You can use Terraform scripts to create a single-tier VPC and create the AAS to HANA and AnyDB infrastructure on the VPC. The Terraform scripts use the VPC information that you provide and then call the Ansible playbook to create the SAP architecture on the specified VPC. Terraform on IBM Cloud® enables predictable and consistent provisioning of IBM Cloud Virtual Private Cloud (VPC) infrastructure resources so that you can rapidly build complex, cloud environments. IBM Cloud VPC infrastructure consists of SAP certified hardware that uses Intel® Xeon CPUs and more Intel® technologies.

You have two deployment methods to choose from:

- Terraform scripts that run from the CLI on your bastion server.
- Schematics user interface accessed from your cloud dashboard menu.

You can create SAP AAS NetWeaver 7.x on the SAP HANA-based ABAP stack.

SAP solution implemented

Many SAP enterprise solutions are built on the SAP platform (SAP NetWeaver) including:

- SAP HANA as Primary Persistence for SAP NetWeaver-based applications
- SAP Business Suite applications (ERP, CRM, and SCM, and other applications),
- SAP Business Warehouse (BW), and
- Other SAP enterprise solutions

SAP NetWeaver has two distinct aspects, ABAP and Java. Many applications that are built on the SAP NetWeaver's ABAP or Java (or both) application servers run on SAP DB owned HANA and ASE Sybase either in AnyDB platforms (MSSQL, Oracle, and Db2).

Technical interfaces are available for applications that are built on the SAP NetWeaver AS ABAP and AS Java to run on SAP HANA and AnyDB. However, specific development enablement is normally required for each application to ensure that it runs optimally on the SAP HANA. SAP Business Suite applications (ERP, CRM, SCM, and other applications), SAP Business Warehouse (BW), and other SAP NetWeaver-based applications were modified to run on SAP HANA and have many advantages. Also, various components and complimentary applications that are built on SAP NetWeaver can also run on SAP HANA or AnyDB by using the provided SAP NetWeaver DB interfaces.

The SAP HANA as primary persistence for SAP NetWeaver-based applications scenario has one restriction: SAP NetWeaver ABAP and Java

application servers must run on separate hardware servers from the SAP HANA hardware.

What is created

The scripts automate the virtual infrastructure resources, provisioning the processes for the SAP architecture in an existing VPC with a distributed environment. SAP AAS NetWeaver 7.x (HANA or ASE SYB) application server on a distinct VSI VPC system and SAP HANA DB on a dedicated server type VSI VPC box are provisioned. The scripts work in two phases.

During the first phase of [Automate SAP bastion server – SAP media storage repository](#), the following virtual infrastructure resources based on the components from the existing VPC created by the bastion server are:

- 1 VPC where the virtual server instance is provisioned.
- 1 security group. The rules for this security group are:
 - Allow inbound DNS traffic (port 53).
 - Allow inbound SSH traffic (TCP port 22).
 - Allow all outbound traffic from the virtual server instance.
 - Allow all traffic in the security group.
- 1 subnet to enable the networking in your VPC.
- 2 virtual server instances with SAP certified storage and network configurations.
- 1 floating IP address used to access your VPC virtual server instance over the public network.

During the second phase, the Ansible Playbooks is called and the SAP architecture is installed for both dedicated virtual server instance (VSI) SAP application; VSI system and dedicated SAP HANA VSI box. The SAP architecture that is deployed on the SAP NetWeaver 7.x release is a stand-alone dedicated SAP HANA 2.0 box release. For more information about this architecture, see [Automating SAP HANA stand-alone virtual server instance on IBM Cloud® VPC by using Terraform and Ansible](#).

You can provision only one instance of the service per IBM Cloud region.

Schematics deployment

When you run the scripts with the Schematics interface, you:

- Enter the workspace information.
- Enter the GitHub path for the chosen solution either on NetWeaver AAS for HANA.
- Modify the parameters in the Schematics interface. They are the same parameters as the `input.auto.tfvars` file that you use with the cli.

Virtual server instance configuration

Following are the supported operating system images for SAP NetWeaver primary application server:

- ibm-redhat-8-4-amd64-sap-applications-2
- ibm-redhat-8-6-amd64-sap-applications-2
- ibm-sles-15-3-amd64-sap-applications-2
- ibm-sles-15-4-amd64-sap-applications-3

Following are the supported operating system images for SAP HANA database:

- ibm-redhat-8-4-amd64-sap-hana-2
- ibm-redhat-8-6-amd64-sap-hana-2
- ibm-sles-15-3-amd64-sap-hana-2
- ibm-sles-15-4-amd64-sap-hana-1

For both server instances there are:

- Two SSH keys are configured to access SSH as `root`.
- Three storage volumes as described in the `input.auto.tfvars` file.

What is created for anydb

The scripts use the information that you provide for an existing VPC and deploy AAS to SAP HANA or AnyDB on a different host than CI (SAP Central Instance) VSI host. For more information about this architecture, see [SAP NetWeaver 7.x on UNIX with HANA or AnyDB on IBM Cloud](#)

[VPC on IBM Cloud VPC](#). You specify the information for the VPC to use in the `input.auto.tfvars` file.

The scripts call the Ansible Playbooks to install the SAP architecture.

Script files

The configuration and script files are provided on GitHub. Each supported interface for the SAP solution installation has its own folder in the GitHub repository:

- [GitHub repository for Terraform – AAS HANA](#)

Terraform interface

To run the Terraform script, you modify:

- The `input.auto.tfvars` file to specify the existing VPC resources for your solution. Specify the variables for the existing VPC:
 - VPC name
 - Security group
 - Subnet
 - Hostname
 - Profile
 - Image
 - Up to two SSH keys

You can change the default SAP system configuration settings to match your solution. You can also specify the location where you downloaded the SAP kits.

The IBM Cloud Provider plug-in for Terraform on IBM Cloud uses these configuration files to install AAS to SAP HANA and AnyDB on the specified VPC in your IBM Cloud account.

Support

There are no warranties of any kind, and there is no service or technical support available for these materials from IBM®. As a recommended practice, review carefully any materials that you download from this site before using them on a live system.

Though the materials provided herein are not supported by the IBM® Service organization, your comments are welcomed by the developers, who reserve the right to revise, readapt or remove the materials at any time. To report a problem, or provide suggestions or comments, open a GitHub issue.

Before you begin

Before you use the scripts in the bastion cli:

- Set up your account to access the VPC. Make sure that your account is [upgraded to a paid account](#).
- If you have not already, create a Bastion server to store the SAP kits. For more information, see [Automate SAP bastion server - SAP media storage repository](#).
- Download the SAP kits from the SAP Portal to your Deployment Server. Make note of the download locations. Ansible decompresses the files. For more information, see the [readme](#) file.
- [Create or retrieve an IBM Cloud API key](#). The API key is used to authenticate with the IBM Cloud platform and to determine your permissions for IBM Cloud services.
- [Create or retrieve your SSH key ID](#). You need the 40-digit UUID for the SSH key, not the SSH key name.
- Terraform should already be installed on the bastion server that you deployed. For more information, see [Bastion server for SAP deployment](#).
- (Optional - Catalog Tile) create secrets for your credentials and passwords by using the [Secrets Manager](#).

Deploying SAP AAS NetWeaver 7.x on HANA by using the Schematics user interface

Use these steps to configure the SAP Additional Application Server (AAS) NetWeaver with HANA or AnyDB on your existing VPC by using the Schematics interface. The script takes 2 - 3 hours to complete.

1. From the IBM Cloud menu, select **Schematics**.
2. Click **Create** workspace.

3. On the **Specify template** page:
 - Enter the URL for the Schematics interface.
 - Select the **Terraform version** that is listed in the readme file.
 - Click **Next**.
4. On the **workspace details** page:
 - Enter a name for the workspace.
 - Select a **Resource group**.
 - Select a **Location** for your workspace. The workspace location does not have to match the resource location.
 - Select **Next**.
5. Select **Create** to create your workspace.
6. On the workspace settings page, in the input variables section, review the default input variables and provide values that match your solution.
 For a more detailed description of each parameter, check the GitHub repo [AAS HANA readme](#) file, chapter "Input parameter file". Also, make sure to mark the parameters that contain sensitive information like passwords, API, and ssh private keys as "sensitive". These parameters are marked as "sensitive" in the readme file, under "Input parameter file".
7. On the workspace settings page, click **Generate plan**. Wait for the plan to complete.
8. Click **View log** to review the log files of your terraform execution plan.
9. Apply your Terraform template by clicking **Apply plan**.
10. Review the log file to ensure that no errors occur during the provisioning, modification, or deletion process.

Deploying SAP AAS NetWeaver (ABAP) on HANA with the Deployable Architecture tile interface

Use these steps to configure the SAP AAS NetWeaver (ABAP) on HANA on your existing VPC by using the catalog tile interface. The script takes 2 - 3 hours to complete.

1. From the IBM Cloud catalog, select **VPC with Additional Application Server ABAP on Linux for SAP HANA** on HANA tile. The **Create** tab opens for VPC with Additional Application Server ABAP on Linux for SAP HANA. For more information about this deployment, see the About tab or the readme file link.
2. Select the latest version.
3. Select **VPC with Additional Application Server ABAP on Linux for SAP HANA on Deployable Architecture tile** variation.
4. Click **Review deployment** options:
 - **Add to project** to add this deployment to an IBM Cloud project and combine it with other deployments. IBM Cloud projects include several more pipeline steps before deployment, including deployment validation, cost calculation, compliance verification, and approval process.
 - **Create from the CLI** to get the CLI command. With this command you can trigger the deployment from the CLI.
 - **Work with code** to embed the code into other terraform deployments.
 - **Deploy with IBM Cloud Schematics** to trigger the deployment process directly.
5. Select **Deploy with IBM Cloud Schematics**.
6. Add the input parameters for this installation. There are 3 categories of parameters:
 - **Workspace** - These parameters define the workspace that is automatically created in Schematics:
 - Enter a name for the workspace or use the default name.
 - The Resource Group used to create resources. Use default or create a Resource Group.
 - Select a location to create your Schematics workspace. The workspace location need not match the resource location.
 - **Required input variables** - Review the default input variables and provide values that match your solution. These parameters are specific to your deployment. For more detailed information, see the [Readme file](#).

Parameter	Description
BASTION_FLOATING_IP	Required only for Schematics Deployments. The Floating IP from the Bastion Server.

HOSTNAME	The hostname for the VSI. The hostname should be up to 13 characters as required by SAP. For more information on the rules regarding hostnames for SAP systems, check SAP Note 611361: Hostnames of SAP ABAP Platform servers
REGION	The cloud region to deploy the solution. The regions and zones for VPC are listed here . Review supported locations in IBM Cloud Schematics here . Sample value: eu-de.
RESOURCE_GROUP	The name of an existing Resource Group for VSIs and Volumes resources. Default value: "Default". The list of Resource Groups is available here .
SECURITY_GROUP	The name of an existing Security group. The list of security groups is available here .
SSH_KEYS	The list of SSH Keys UUIDs that are allowed to SSH as root to the VSI can contain one or more IDs. The list of SSH Keys is available here . Sample input (use your own SSH UUIDs from IBM Cloud){: external}: ["r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a", "r010-3fcfd9fe7-d4a7-41ce-8bb3-d96e936b2c7e"]
SUBNET	The name of an existing subnet. The list of subnets is available here .
VPC	The name of an existing VPC. The list of VPCs is available here .
ZONE	The cloud zone where to deploy the solution. Sample value: eu-de-2.
ibmcloud_api_key	IBM Cloud API key (Sensitive* value).
private_ssh_key	Required only for Schematics Deployments - Input your id_rsa private key pair content in OpenSSH format (Sensitive* value). This private key should be used only during the terraform provisioning and it is recommended to be changed after the SAP deployment.
hdb_instance_number	The instance number of the SAP HANA database server.
sap_aas_instance_number	Technical identifier for the internal processes of the additional application server.
sap_asci_instance_number	Technical identifier for the internal processes of ASCS.
sap_ci_host	IP address of the existing SAP Central Instance.
sap_ci_hostname	The hostname of the existing SAP Central Instance.
sap_ci_instance_number	Technical identifier for the internal processes of the Central Instance.
sap_sid	The SAP system ID identifies the entire SAP system.
sap_main_password	Common password for all users that are created during the installation (See Obs*).

Required Variables

- **Optional variables** - Review and update the optional input variables. The Ansible scripts expect the SAP kits to be in the default locations listed. For more information, see the [Readme file - Input Parameters](#).

Parameter	Description
ID_RSA_FILE_PATH	The file path for private_ssh_key is automatically generated by default. If it is changed, it must contain the relative path from Git repo folders. Default value: "ansible/id_rsa".
IMAGE	The OS image used for the VSI. A list of images is available here .
PROFILE	The profile used for the VSI. A list of profiles is available here . For more information about supported DB/OS and IBM Gen 2 Virtual Server Instances (VSI), check SAP Note 2927211: SAP Applications on IBM Virtual Private Cloud .

VOL1	Volume 1 Size - The size for the disks in GB that are to be attached to the VSI and used by SAP.
VOL2	Volume 2 Size - The size for the disks in GB that are to be attached to the VSI and used by SAP.
kit_sapcar_file	Path to the sapcar binary, as downloaded from SAP Support Portal.
kit_swpm_file	Path to the SWPM archive (SAR), as downloaded from SAP Support Portal.
kit_saphostagent_file	Path to the SAP Host Agent archive (SAR), as downloaded from SAP Support Portal.
kit_hdbclient_file	Path to the HANA DB client archive (SAR), as downloaded from SAP Support Portal.

Optional Variables

7. Accept the license agreement.
8. Select **Deploy**. The deployment starts and you are directed to the Schematics page that displays the script log files for you to monitor the deployment progress.

Creating the infrastructure using Terraform with the bastion server CLI

Use these steps to configure the IBM Cloud Provider plug-in and use Terraform to install SAP AAS to SAP HANA and AnyDB on your existing VPC on an already deployed SAP NetWeaver 7.X with SAP HANA 2.0 or ASE SYB as a Central Instance.

The script takes 1 - 2 hours to complete.

1. Access the bastion server cli.
2. Clone the solution repository and change to the folder.

ASE SYB 16 Clone the solution repository from <https://github.com/IBM-Cloud/sap-aas-abap-ase-syb> and cd to the sap-aas-abap-ase-syb/cli folder.

```
$ git clone https://github.com/IBM-Cloud/sap-aas-abap-ase-syb
cd sap-aas-abap-ase-syb/cli/
```

SAP HANA 2.0: Clone the solution repository from <https://github.com/IBM-Cloud/sap-abap-hana-aas> and cd to the sap-abap-hana-aas folder.

```
$ git clone https://github.com/IBM-Cloud/sap-abap-hana-aas.git
cd sap-abap-hana-aas/
```

3. Modify the `input.auto.tfvars` file to specify the information for the existing VPC, your region, zone, networking component names, hostname for the AAS VSI,profile, and image. You need your 40-digit SSH key ID for this file. The second SSH key is optional. For more options for profile, see [Instance Profiles](#). For more options, see [Images](#). For descriptions of the variables, see the [readme](#) file.

The VSI OS images that are supported for this solution for Netweaver Additional Application Server are:

- ibm-redhat-8-4-amd64-sap-applications-2
- ibm-redhat-8-6-amd64-sap-applications-2
- ibm-sles-15-3-amd64-sap-applications-2
- ibm-sles-15-4-amd64-sap-applications-4

```
$ # Infra VPC variables for ASE SYB
REGION    = "eu-de"
ZONE      = "eu-de-2"
VPC       = "ic4sap"                      # EXISTING Security group name
SECURITY_GROUP = "ic4sap-securitygroup"     # EXISTING Security group name
RESOURCE_GROUP = "wes-automation"
SUBNET    = "ic4sap-subnet"                 # EXISTING Subnet name
SSH_KEYS   = [ "r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a" , "r010-3fcfd9fe7-d4a7-41ce-8bb3-
d96e936b2c7e" ]

# SAP AAS VSI variables:
```

```

HOSTNAME = "sapnwase-as01"
PROFILE = "bx2-4x16"
IMAGE = "ibm-redhat-8-4-amd64-sap-applications-2

$ # Infra VPC variables for ABAP HANA
REGION      = "eu-de"
ZONE        = "eu-de-2"
VPC          = "ic4sap" # EXISTING Security group name
SECURITY_GROUP = "ic4sap-securitygroup" # EXISTING Security group name
RESOURCE_GROUP = "wes-automation"
SUBNET       = "ic4sap-subnet" # EXISTING Subnet name
SSH_KEYS     = [ "r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a" , "r010-3fc9fe7-d4a7-41ce-8bb3-d96e936b2c7e" ]
ID_RSA_FILE_PATH = "ansible/id_rsa"

# SAP AAS variables:
HOSTNAME = "sapnwapp"
PROFILE = "bx2-4x16"
IMAGE = "ibm-redhat-8-6-amd64-sap-applications-2"

```

4. Customize your SAP system configuration. In the same file, input.auto.tfvars, edit the SAP system configuration variables that are passed to the Ansible automated deployment. For descriptions of the variables, see the [readme](#) file.

```

$ # SAP system configuration - for ASE SYB
sap_sid = "NWD"
sap_ci_host = "10.243.132.10"
sap_ci_hostname = "sapnwase"
sap_ci_instance_number = "00"
sap_asc_s_instance_number = "01"
sap_aas_instance_number = "00"

# Kits paths
kit_sapcar_file = "/storage/NW75SYB/SAPCAR_1010-70006178.EXE"
kit_swpm_file = "/storage/NW75SYB/SWPM10SP31_7-20009701.SAR"
kit_saphotagent_file = "/storage/NW75SYB/SAPHOSTAGENT51_51-20009394.SAR"

```

```

$ # SAP system configuration - for ABAP HANA
sap_sid = "NWD"
sap_ci_host = "10.243.132.10"
sap_ci_hostname = "sapnwapp01"
sap_ci_instance_number = "00"
sap_asc_s_instance_number = "01"
hdb_instance_number = "00"
sap_aas_instance_number = "00"

# Kits paths
kit_sapcar_file = "/storage/NW75HDB/SAPCAR_1010-70006178.EXE"
kit_swpm_file = "/storage/NW75HDB/SWPM10SP31_7-20009701.SAR"
kit_saphotagent_file = "/storage/NW75HDB/SAPHOSTAGENT51_51-20009394.SAR"
kit_hdbclient_file = "/storage/NW75HDB/IMDB_CLIENT20_009_28-80002082.SAR"

```

Ansible decompresses the rest of the SAP kit files. For more information, see the [readme](#) file.

5. Initialize the Terraform CLI.

```
terraform init
```

6. Create a Terraform execution plan. The Terraform execution plan summarizes all the actions that are done to create the virtual private cloud instance in your account.

```
terraform plan plan1
```

Enter an SAP main password and your API key.

The SAP main password must be 10 - 14 characters long and contain at least one digit (0-9). It can contain only the following characters: a-z, A-Z, 0-9, @, #, \$, . *This password cannot contain exclamation points '!'. The password must not start with a digit or an underscore ().*

7. Verify that the plan shows all of the resources that you want to create and that the names and values are correct. If the plan needs to be adjusted, edit the input.auto.tfvars file to correct resources and run terraform plan again.
8. Apply the saved plan.

```
$ terraform apply "plan1"
```

The virtual private cloud and components are created and you see output similar to the `terraform plan` output.

9. Add the SAP credentials and the virtual server instance IP to the SAP GUI. For more information about the SAP GUI, see [SAP GUI](#).

Next steps

If you need to rename your resources after they are created, modify the input.auto.tfvars file to change the names and run `terraform plan` and `terraform apply` again. Do not use the IBM Cloud Dashboard and user interface to modify your VPC after it is created. The Terraform scripts create a complete solution and selectively modifying resources with the user interface might cause unexpected results.

If you need to remove the SAP Netweaver 7.X on HANA or AnyDB installation, go to your project folder and run `terraform destroy`. The `terraform destroy` command does not remove the VPC in this scenario because the VPC was created before these Terraform scripts were run.

Related information

For more information about Terraform on IBM Cloud, see [Getting started with Terraform on IBM Cloud](#).

For more information about using Terraform for creating only a VPC for SAP, without the SAP architecture, see [Creating single-tier virtual private cloud for SAP by using Terraform](#).

SAP One Support Notes that apply to this document:

- [SAP Note 84555 - Windows Server, Linux®, and UNIX: Certified hardware](#)
- [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#)
- [SAP Note 2923773 - Linux® on IBM Cloud \(IaaS\): Adaption of your SAP license](#)
- [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#)
- [SAP Note 2369910 - SAP Software on Linux®: General information](#)
- [SAP Note 171380 - Released IBM hardware \(Intel processors\) and IBM cloud services offers](#)
- [SAP Note 1380654 - SAP support in IaaS environments](#)

This document is referenced by:

- [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#)
- [SAP Note 2588225 - SAP on IBM Cloud: Protect against speculative execution vulnerabilities](#)
- [SAP Note 1380654 - SAP support in IaaS environments](#)
- [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#)

SAP S/4HANA HA deployment in VPC

Automating SAP workload HA deployment on IBM Cloud VPC with Terraform and Ansible

You can use Terraform to automate IBM Cloud® VPC provisioning. The VPC provisioned includes virtual server instances with high network performance. The VPC infrastructure contains various Infrastructure-as-a-Service (IaaS) offerings, including virtual servers. After the VPC is provisioned, the scripts use the Ansible Playbooks to install the SAP system.

IBM Cloud VPC introduction

VPC is a public cloud offering that an enterprise uses to establish its own private cloud-like computing environment on shared [public cloud](#) infrastructure. VPC gives an enterprise the ability to define and control a virtual network that is logically isolated from all other public cloud tenants, creating a private and secure place on the public cloud.

Imagine that a cloud provider's infrastructure is a residential apartment building and multiple families live inside. A public cloud tenant is a kind of sharing an apartment with a few roommates. In contrast, having a VPC is like having your own private condominium; no one else has the key, and no one can enter the space without your permission.

VPC's logical isolation is implemented by using virtual network functions and security features that give the enterprise customer granular control over which IP addresses or applications can access particular resources. It is analogous to the "friends-only" or "public/private" controls on social media accounts used to restrict who can or can't see your otherwise public posts.

With IBM Cloud VPC, you can use the UI, CLI, and API to manually provision virtual server instances for VPC with high network performance. VPC infrastructure contains various Infrastructure-as-a-Service (IaaS) offerings including virtual servers for VPC.

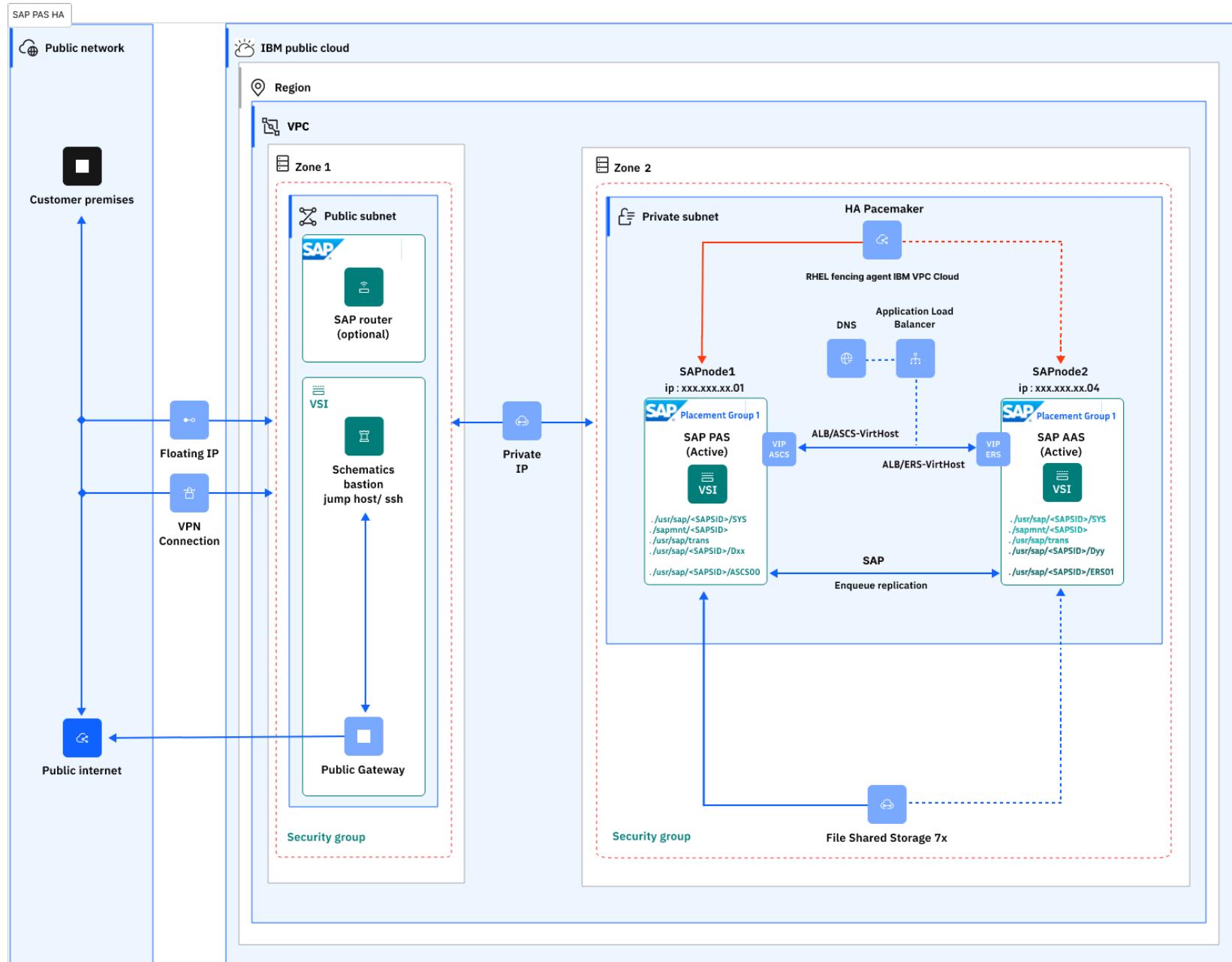
Use the following information to understand a simple use-case for planning, creating, and configuring resources for your VPC, and learn more about VPC overviews and VPC tutorials. For more information about the VPC, see [Getting started with Virtual Private Cloud \(VPC\)](#).

SAP products architecture on IBM Cloud VPC

A [Virtual Private Cloud \(VPC\)](#) contains one of the most secure and reliable cloud environments for SAP applications within your own VPC with virtual server instances. This represents an Infrastructure-as-a-Service (IaaS){: external} within IBM Cloud that offers all the benefits of isolated, secure, and flexible virtual cloud infrastructure from IBM. In comparison, the IBM Cloud classic infrastructure virtual servers offering uses virtual instances with native and VLAN networking to communicate with each other within a data center; however, the instances are restricted in one well-working pod by using subnet and VLAN networking as a gap scale up of virtual resources should rely between the pods. The IBM Cloud VPC network orchestrator layer concept eliminates the pod boundaries and restrictions, so this new concept handles all the networking for every virtual instance running within VPC across regions and zones.

Highly available system for SAP NetWeaver on IBM Cloud VPC

In a Highly Available (HA) system, every instance can run on a separate IBM Cloud virtual server instance. The cluster HA configuration for the SAP application server consists of two virtual server instances, each of them located in the same zone within the region by using placement groups. Placement groups assure that both cluster resources and cloud resources are also located in different compute nodes as specified in the following placement groups section:



SAP HA for SAP applications cluster nodes PAS (Active) and AAS (Active)

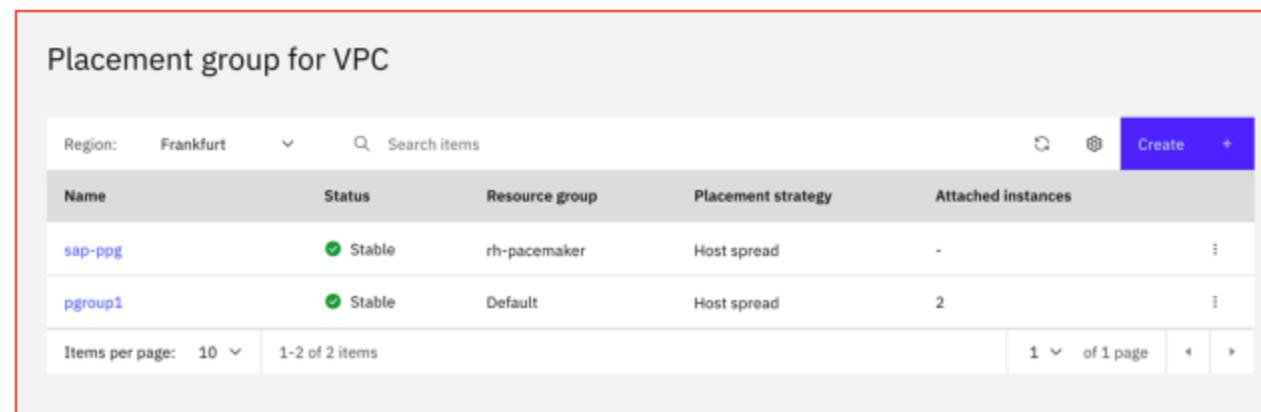
Placement groups on IBM Cloud VPC for SAP HA architecture

Placement Groups (PG) for VPC have two different anti-affinity strategies for high availability. By using the placement strategies, you minimize the chance of service disruption with virtual server instances that are placed on different hosts or into an infrastructure with separate power and network supplies.

The design of placement groups for IBM Cloud virtual servers solves this issue. Placement groups give a measure of control over the host on which a new public virtual server is placed. In this release, a “spread” rule is implemented, which means that the virtual servers within a placement group are spread onto different hosts. You can build a highly available application within a data center and know that your virtual servers are isolated from each other.

Placement groups with the spread rule are available to create in selected IBM Cloud data centers. After a spread rule is created, you can provision a virtual server into that group and ensure that it is not on the same host as any of your other virtual servers. This feature comes with no cost.

You can create your placement group and assign up to four new virtual server instances. With the spread rule, each of your virtual servers are provisioned on different physical hosts. In the following configuration example, the “Power Spread” option is used:



Placement groups host spread

Placement group for VPC					
Name	Status	Resource group	Placement strategy	Attached instances	
sapha-poc	Stable	wes-ic4sap-resourcegroup	Power spread	4	⋮
Items per page: 10 1 item 1 of 1 page ⋮					

Placement groups power spread

Following are the SAP instances that are required for HA scenario:

- ABAP SAP Central Services (ASCS) instance - contains the ABAP message server and the ABAP enqueue server.
- Enqueue Replication Server (ERS) instance for the ASCS instance.
- Database instance
- Primary Application Server (PAS) instance on node 1.
- Additional Application Server (AAS) instance on node 2.



Note: It is recommended to run both the ASCS instance and the ERS instance in a switchover cluster infrastructure.

IBM Cloud File Storage for VPC for SAP HA architecture

[IBM Cloud File Storage for VPC](#) technology is used to make the SAP directories available to the SAP system. The technologies of choice are NFS, shared disks, and cluster file system. If you have decided to use the HA solution for your SAP system, make sure that you properly address the HA requirements of the SAP file systems in your SAP environment.

File shares for VPC								
Name	Status	Resource groups	Location	Mount targets	Size	Replication role	Encryption type	
usrsap-as1-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	⋮
usrsap-as2-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	⋮
usrsap-sapsacs-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	⋮
usrsap-sapers-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	⋮
usrsap-sapmnt-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	⋮
usrsap-sapsys-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	⋮
usrsap-trans-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	80 GB	None	Provider managed	⋮

File shares for VPC

- File shares that are mounted as NFS permanent file systems on both cluster nodes for SAP HA application:
 - `/usr/sap/<SAPSID>/SYS`
 - `/sapmnt<SAPSID>`
 - `/usr/sap/trans`
- Cluster-managed file systems for SAP HA application: ASCS
 - `/usr/sap/<SAPSID>/ASCS00`
 - `/usr/sap/<SAPSID>/ERS01`
- Permanent NFS mount on SAP HA application node 1 PAS instance:
 - `/usr/sap/<SAPSID>/Dxx`
- Permanent NFS mount on SAP HA application node 2 dialog instance:
 - `/usr/sap/<SAPSID>/Dyy`

Prerequisites

You need to install the hardware (hosts, disks, and network) and decide how to distribute the database, SAP instances, and if required, the Network File System (NFS) server over the cluster nodes.

Context

Following are the types of SAP directories:

- Physically shared directories: `/<sapmnt>/<SAPSID>` and `/usr/sap/trans`

- Logically shared directories that are bound to a node, such as `/usr/sap`, with the following local directories:
 - `/usr/sap/<SAPSID>`
 - `/usr/sap/<SAPSID>/SYS`
 - `/usr/sap/hostctrl`
- Local directories that contain the SAP instances such as `/usr/sap/<SAPSID>/ASCS<Instance_Number>`
- The global transport directory may reside on a separate SAP transport host as a standard three systems transport layer configuration.

You need at least two nodes and a shared file system for distributed ASCS and ERS instances. The assumption is that the rest of the components are distributed on other nodes.

ASCS and ERS installation

In order for the ASCS and ERS instances to be able to move from one node to the other, they need to be installed on a shared file system and use virtual hostnames based on the virtual IP.

In this VPC-based SAP HA solution, the shared file system that is required by the cluster is replaced by the NFS-mounted file storage, and the virtual IP is replaced by the Application Load Balancer for VPC (ALB).

In this scenario, three ALBs are used, one for each Single Point of Failure (SPOF) component in order to replace the virtual IP requirement: ALB for ASCS, ALB for ERS, and ALB for ASE Sybase. Each ALB is configured as a backend for the corresponding cluster servers and redirects all of the communication that is received on the front-end ports to the active server in the backend pool.

Load balancers for VPC						
Region:	Frankfurt	▼	<input type="text"/> poc	X		
Name	Status	Family	Resource group	Type	Hostname	Location
db-alb-hana-poc	Active	Application	wes-ic4sap-resourcegroup	Private	20bdd130-eu-de.lb.appdomain.cloud	Frankfurt
sap-alb-ers-poc	Active	Application	wes-ic4sap-resourcegroup	Private	3941d983-eu-de.lb.appdomain.cloud	Frankfurt
sap-alb-ascs-poc	Active	Application	wes-ic4sap-resourcegroup	Private	56a9190d-eu-de.lb.appdomain.cloud	Frankfurt

Application load balancer management of HA IPs mechanism

Private application load balancer

A [private application load balancer](#) is accessible through your private subnets that you configured to create the load balancer.

Similar to a public application load balancer, your private application load balancer service instance is assigned an FQDN; however, this domain name is registered with one or more private IP addresses.

IBM Cloud operations change the number and value of your assigned private IP addresses over time, based on maintenance and scaling activities. The backend virtual server instances that host your application must run in the same region and under the same VPC.

Use the assigned ALB FQDN to send traffic to the private application load balancer to avoid connectivity problems to your applications during system maintenance or scaling down activities.

Each ALB sends traffic to the cluster node where the application (ASCS, ERS, ASE Sybase DB) is running. During the cluster failover, the ALB redirects all the traffic to the new node where the resources are up and running.



Note: DNS-as-a-Service (DNSaaS) is the management IBM Cloud VPC DNS service of HA and FQDN (IPs) mechanism.



Note: The ALB has a default of 50 seconds for client and server timeout, so after 50 seconds of inactivity, the connection is closed. To support SAP connections through ALB and not lose connection after 50 seconds, you need to request a change this value to a minimum of 300 seconds (client-side idle connection = minimum 300s and server-side idle connection = minimum 300s). To request this change, open a support ticket. This is an account-wide change that affects all of the ALBs in your account. For more information, see [Connection timeouts](#).

DNS Services with VPC

[IBM Cloud DNS Services](#) provide private DNS to VPC users. Private DNS zones are resolvable only on IBM Cloud and from explicitly [permitted networks](#) in an account. To get started, create a DNS Services instance by using the IBM Cloud console.

DNS Services allows you to:

- Create the private DNS zones that are collections for holding the domain names.
- Create the DNS resource records under these DNS zones.
- Specify the access controls used for the DNS resolution of resource records on a zone-wide level.

DNS Services also maintains its own worldwide set of DNS resolvers. Instances that are provisioned under IBM Cloud on an IBM Cloud network can use resource records that are configured through IBM Cloud DNS Services by querying DNS Services resolvers.

Resource records and zones that are configured through DNS Services are:

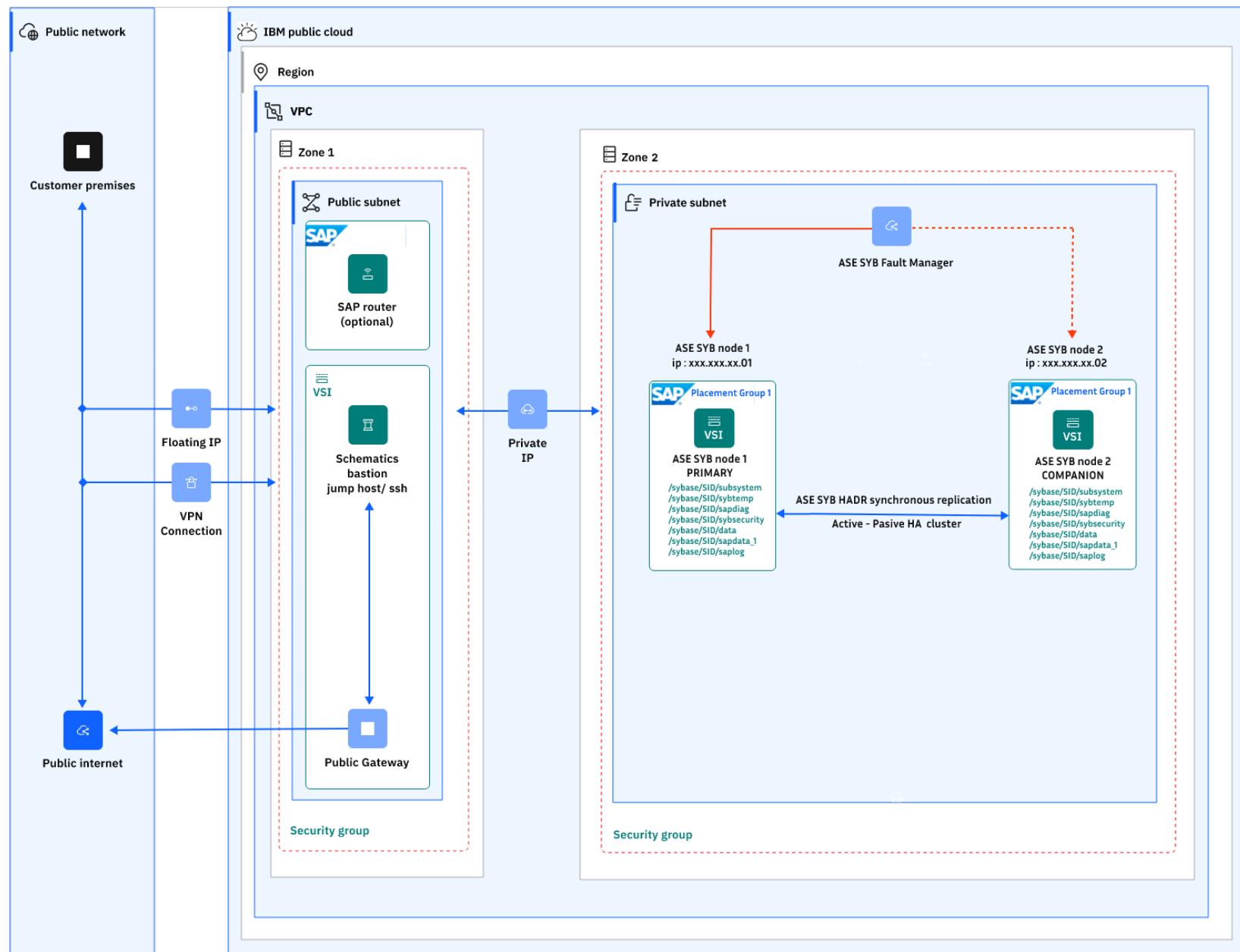
- Separated from the wider public DNS, and their publicly accessible records.
- Hidden from the system outside of and not part of the IBM Cloud private network.
- Accessible only from the system that you authorize on the IBM Cloud private network.
- Resolvable only via the resolvers provided by the service.

The DNS service maps the FQDN of each ALB to the virtual hostnames of the ASCS, ERS, and ASE Sybase that are used by SAP applications.

Type	Name	Value	TTL
CNAME	dbpochana	is an alias of 20bdd130-eu-de.lb.appdomain.cloud	12 hr
CNAME	sappocers	is an alias of 3941d983-eu-de.lb.appdomain.cloud	12 hr
CNAME	sappocases	is an alias of 56a9190d-eu-de.lb.appdomain.cloud	12 hr

DNS records

Highly available system for SAP ASE Sybase database with HADR system



SAP HA for ASE Sybase DB instances cluster nodes primary (Active) and Secondary (Companion)

At the most basic level, a standard HA ASE Sybase cluster in an active(primary)-passive(companion) configuration has two nodes: one is the primary node and the other is the standby node. This means that the primary node is actively serving the active SAP DB instances (Primary and Companion), while the standby node is waiting to jump in if there is any failure.

The cluster is set with a virtual hostname IP (hostname is mapped to the FQDN of the ASE Sybase ALB through DNS, which is the same as

explained previously for SAP ASCS and ERS instances). Application instances (PAS and AAS) are used on the SAP profiles to call that particular component. The cluster assigns the virtual IP to the active node and uses a heartbeat monitor to confirm the availability of the components. If the primary node stops responding, it triggers the automatic failover mechanism that calls the standby node to step up to become the primary node. The ALB detects the change, redirects the traffic to the new active node, and assigns the virtual IP to it, restoring the component availability. Once fixed, the failed node comes online as a standby node.

SAP Sybase HADR system supports synchronous replication

The SAP Sybase HADR system supports synchronous replication between the primary and standby servers for high availability. An active-active setup is a two-node configuration where both nodes in the cluster include SAP ASE managing independent workloads, capable of taking over each others workload in the event of a failure.

The SAP ASE server that takes over the workload is called a secondary companion, and the SAP ASE server that fails is called the primary companion. Together they are companion servers. This movement from one node to another is called failover. After the primary companion is ready to resume its workload, it is moved back to its original node. This movement is called a failback.

When a system fails over, clients that are connected to the primary companion and use the failover property automatically reestablish their network connections to the secondary companion. You must tune your operating system to successfully manage both servers during fail over. See your operating system documentation for information about configuring your system for high availability. An SAP ASE configured for failover in an active-active setup can be shut down using the shutdown command only after you have suspended SAP ASE from the companion configuration, at both the server level and the platform level.

The always-on option in a High Availability and Disaster Recovery (HADR) system consists of two SAP ASE servers:

- Primary on which all transaction processing takes place.
- Warm standby (referred to as a "standby server" in DR mode, and as a "companion" in HA mode) for the primary server, and contains copies of designated databases from the primary server.



Note: The HADR feature that is shipped with SAP ASE version 16.0 SP02 supports only a single-companion server.

Some high-availability solutions (for example, the SAP Adaptive Server Enterprise Cluster Edition) share or use common resources between nodes. However, the HADR system is a "shared nothing" configuration, each node has separate resources including disks.

In an HADR system, servers are separate entities and data is replicated from the primary server to the companion server. If the primary server fails, a companion server is promoted to the role of primary server either manually or automatically. Once the promotion is complete, clients can reconnect to the new primary server, and see all committed data, including data that was committed on the previous primary server.

Servers can be separated geographically, which makes an HADR system capable of withstanding the loss of an entire computing facility.



Note: The HADR system includes an embedded SAP Replication Server, which synchronizes the databases between the primary and companion servers. SAP ASE uses the Replication Management Agent (RMA) to communicate with Replication Server and SAP Replication Server uses Open Client connectivity to communicate with the companion SAP ASE.

The Replication Agent detects any data changes made on the primary server and sends them to the primary SAP Replication Server. In the figure above, the unidirectional arrows indicate that, although both SAP Replication Servers are configured, only one direction is enabled at a time.

The HADR system supports synchronous replication between the primary and standby servers for high availability so the two servers can keep in sync with Zero Data Loss (ZDL). This requires a network link that is fast enough between the primary and standby server so that synchronous replication can keep up with the primary servers workload. Generally, this means that the network latency is approximately the same speed as the local disk IO speed, a few (fewer than 10) milliseconds. Anything longer than a few milliseconds may result in a slower response to write operations at the primary.

The HADR system supports asynchronous replication between the primary and standby servers for disaster recovery. The primary and standby servers by using asynchronous replication can be geographically distant, meaning they can have a slower network link. With asynchronous replication, Replication Agent Thread captures the primary servers workload, which is delivered asynchronously to SAP Replication Server. The SAP Replication Server applies these workload change to the companion server.

The most fundamental service that is offered by the HADR system is the failover; planned or unplanned from the primary to the companion server, which allows maintenance activity to occur on the old primary server, while applications continue on the new primary.

The HADR system provides protection in the event of a disaster. If the primary server is lost, the companion server can be used as a replacement. Client applications can switch to the companion server, and the companion server is quickly available for users. If the SAP Replication Server was in synchronous mode before the failure of the primary server, the Fault Manager automatically initiates failover with

zero data loss.

Fault Manager installation on the SAP ASCS node

The required parameters are asked during the installation process to create a profile for the fault manager and then adds it to the instance start profile. It is also possible to run the installation by using an existing profile: `sybdbfm install pf=<SYBHA.PFL>` In this case, the installation process will only ask for profile parameters missing in the profile.



Note: Fault manger is integrated with ASCS on same SAP PAS/AAS cluster (start/stop/move together).

There may be some data loss if the SAP Replication Server was in asynchronous mode and you must use manual intervention to failover for disaster recovery.

Connection attempts to the companion server without the necessary privileges are silently redirected to the primary companion via the login redirection mechanism, which is supported by Connectivity libraries. If login redirection is not enabled, client connections fail and are disconnected.

The SAP ASE HADR option installs the below components:

- SAP ASE
- SAP Replication Server
- Replication Management Agent (RMA)
- SAP Host Agent
- Fault Manager
- SAP ASE Cockpit



Note: This automation is offered at no cost; however, the provisioned infrastructure comes at cost.

VPC with Additional Application Server (AAS) ABAP on Linux for SAP HANA

You can use Terraform scripts to create a single-tier VPC and create the AAS to HANA and AnyDB infrastructure on the VPC. The Terraform scripts use the VPC information that you provide and then call the Ansible playbook to create the SAP architecture on the specified VPC. Terraform on IBM Cloud® enables predictable and consistent provisioning of IBM Cloud Virtual Private Cloud (VPC) infrastructure resources so that you can rapidly build complex, cloud environments. IBM Cloud VPC infrastructure consists of SAP certified hardware that uses Intel® Xeon CPUs and more Intel® technologies.

You have two deployment methods to choose from:

- Terraform scripts that run from the CLI on your bastion server.
- Schematics user interface accessed from your cloud dashboard menu.

You can create SAP AAS NetWeaver 7.x on the SAP HANA-based ABAP stack.

SAP solution implemented

Many SAP enterprise solutions are built on the SAP platform (SAP NetWeaver) including:

- SAP HANA as Primary Persistence for SAP NetWeaver-based applications
- SAP Business Suite applications (ERP, CRM, and SCM, and other applications),
- SAP Business Warehouse (BW), and
- Other SAP enterprise solutions

SAP NetWeaver has two distinct aspects, ABAP and Java. Many applications that are built on the SAP NetWeaver's ABAP or Java (or both) application servers run on SAP DB owned HANA and ASE Sybase either in AnyDB platforms (MSSQL, Oracle, and Db2).

Technical interfaces are available for applications that are built on the SAP NetWeaver AS ABAP and AS Java to run on SAP HANA and AnyDB. However, specific development enablement is normally required for each application to ensure that it runs optimally on the SAP HANA. SAP Business Suite applications (ERP, CRM, SCM, and other applications), SAP Business Warehouse (BW), and other SAP NetWeaver-based applications were modified to run on SAP HANA and have many advantages. Also, various components and complimentary applications that are built on SAP NetWeaver can also run on SAP HANA or AnyDB by using the provided SAP NetWeaver DB interfaces.

The SAP HANA as primary persistence for SAP NetWeaver-based applications scenario has one restriction: SAP NetWeaver ABAP and Java

application servers must run on separate hardware servers from the SAP HANA hardware.

What is created

The scripts automate the virtual infrastructure resources, provisioning the processes for the SAP architecture in an existing VPC with a distributed environment. SAP AAS NetWeaver 7.x (HANA or ASE SYB) application server on a distinct VSI VPC system and SAP HANA DB on a dedicated server type VSI VPC box are provisioned. The scripts work in two phases.

During the first phase of [Automate SAP bastion server – SAP media storage repository](#), the following virtual infrastructure resources based on the components from the existing VPC created by the bastion server are:

- 1 VPC where the virtual server instance is provisioned.
- 1 security group. The rules for this security group are:
 - Allow inbound DNS traffic (port 53).
 - Allow inbound SSH traffic (TCP port 22).
 - Allow all outbound traffic from the virtual server instance.
 - Allow all traffic in the security group.
- 1 subnet to enable the networking in your VPC.
- 2 virtual server instances with SAP certified storage and network configurations.
- 1 floating IP address used to access your VPC virtual server instance over the public network.

During the second phase, the Ansible Playbooks is called and the SAP architecture is installed for both dedicated virtual server instance (VSI) SAP application; VSI system and dedicated SAP HANA VSI box. The SAP architecture that is deployed on the SAP NetWeaver 7.x release is a stand-alone dedicated SAP HANA 2.0 box release. For more information about this architecture, see [Automating SAP HANA stand-alone virtual server instance on IBM Cloud® VPC by using Terraform and Ansible](#).

You can provision only one instance of the service per IBM Cloud region.

Schematics deployment

When you run the scripts with the Schematics interface, you:

- Enter the workspace information.
- Enter the GitHub path for the chosen solution either on NetWeaver AAS for HANA.
- Modify the parameters in the Schematics interface. They are the same parameters as the `input.auto.tfvars` file that you use with the cli.

Virtual server instance configuration

Following are the supported operating system images for SAP NetWeaver primary application server:

- ibm-redhat-8-4-amd64-sap-applications-2
- ibm-redhat-8-6-amd64-sap-applications-2
- ibm-sles-15-3-amd64-sap-applications-2
- ibm-sles-15-4-amd64-sap-applications-3

Following are the supported operating system images for SAP HANA database:

- ibm-redhat-8-4-amd64-sap-hana-2
- ibm-redhat-8-6-amd64-sap-hana-2
- ibm-sles-15-3-amd64-sap-hana-2
- ibm-sles-15-4-amd64-sap-hana-1

For both server instances there are:

- Two SSH keys are configured to access SSH as `root`.
- Three storage volumes as described in the `input.auto.tfvars` file.

What is created for anydb

The scripts use the information that you provide for an existing VPC and deploy AAS to SAP HANA or AnyDB on a different host than CI (SAP Central Instance) VSI host. For more information about this architecture, see [SAP NetWeaver 7.x on UNIX with HANA or AnyDB on IBM Cloud](#)

[VPC on IBM Cloud VPC](#). You specify the information for the VPC to use in the `input.auto.tfvars` file.

The scripts call the Ansible Playbooks to install the SAP architecture.

Script files

The configuration and script files are provided on GitHub. Each supported interface for the SAP solution installation has its own folder in the GitHub repository:

- [GitHub repository for Terraform – AAS HANA](#)

Terraform interface

To run the Terraform script, you modify:

- The `input.auto.tfvars` file to specify the existing VPC resources for your solution. Specify the variables for the existing VPC:
 - VPC name
 - Security group
 - Subnet
 - Hostname
 - Profile
 - Image
 - Up to two SSH keys

You can change the default SAP system configuration settings to match your solution. You can also specify the location where you downloaded the SAP kits.

The IBM Cloud Provider plug-in for Terraform on IBM Cloud uses these configuration files to install AAS to SAP HANA and AnyDB on the specified VPC in your IBM Cloud account.

Support

There are no warranties of any kind, and there is no service or technical support available for these materials from IBM®. As a recommended practice, review carefully any materials that you download from this site before using them on a live system.

Though the materials provided herein are not supported by the IBM® Service organization, your comments are welcomed by the developers, who reserve the right to revise, readapt or remove the materials at any time. To report a problem, or provide suggestions or comments, open a GitHub issue.

Before you begin

Before you use the scripts in the bastion cli:

- Set up your account to access the VPC. Make sure that your account is [upgraded to a paid account](#).
- If you have not already, create a Bastion server to store the SAP kits. For more information, see [Automate SAP bastion server - SAP media storage repository](#).
- Download the SAP kits from the SAP Portal to your Deployment Server. Make note of the download locations. Ansible decompresses the files. For more information, see the [readme](#) file.
- [Create or retrieve an IBM Cloud API key](#). The API key is used to authenticate with the IBM Cloud platform and to determine your permissions for IBM Cloud services.
- [Create or retrieve your SSH key ID](#). You need the 40-digit UUID for the SSH key, not the SSH key name.
- Terraform should already be installed on the bastion server that you deployed. For more information, see [Bastion server for SAP deployment](#).
- (Optional - Catalog Tile) create secrets for your credentials and passwords by using the [Secrets Manager](#).

Deploying SAP AAS NetWeaver 7.x on HANA by using the Schematics user interface

Use these steps to configure the SAP Additional Application Server (AAS) NetWeaver with HANA or AnyDB on your existing VPC by using the Schematics interface. The script takes 2 - 3 hours to complete.

1. From the IBM Cloud menu, select **Schematics**.
2. Click **Create** workspace.

3. On the **Specify template** page:
 - Enter the URL for the Schematics interface.
 - Select the **Terraform version** that is listed in the readme file.
 - Click **Next**.
4. On the **workspace details** page:
 - Enter a name for the workspace.
 - Select a **Resource group**.
 - Select a **Location** for your workspace. The workspace location does not have to match the resource location.
 - Select **Next**.
5. Select **Create** to create your workspace.
6. On the workspace settings page, in the input variables section, review the default input variables and provide values that match your solution.
 For a more detailed description of each parameter, check the GitHub repo [AAS HANA readme](#) file, chapter "Input parameter file". Also, make sure to mark the parameters that contain sensitive information like passwords, API, and ssh private keys as "sensitive". These parameters are marked as "sensitive" in the readme file, under "Input parameter file".
7. On the workspace settings page, click **Generate plan**. Wait for the plan to complete.
8. Click **View log** to review the log files of your terraform execution plan.
9. Apply your Terraform template by clicking **Apply plan**.
10. Review the log file to ensure that no errors occur during the provisioning, modification, or deletion process.

Deploying SAP AAS NetWeaver (ABAP) on HANA with the Deployable Architecture tile interface

Use these steps to configure the SAP AAS NetWeaver (ABAP) on HANA on your existing VPC by using the catalog tile interface. The script takes 2 - 3 hours to complete.

1. From the IBM Cloud catalog, select **VPC with Additional Application Server ABAP on Linux for SAP HANA** on HANA tile. The **Create** tab opens for VPC with Additional Application Server ABAP on Linux for SAP HANA. For more information about this deployment, see the About tab or the readme file link.
2. Select the latest version.
3. Select **VPC with Additional Application Server ABAP on Linux for SAP HANA on Deployable Architecture tile** variation.
4. Click **Review deployment** options:
 - **Add to project** to add this deployment to an IBM Cloud project and combine it with other deployments. IBM Cloud projects include several more pipeline steps before deployment, including deployment validation, cost calculation, compliance verification, and approval process.
 - **Create from the CLI** to get the CLI command. With this command you can trigger the deployment from the CLI.
 - **Work with code** to embed the code into other terraform deployments.
 - **Deploy with IBM Cloud Schematics** to trigger the deployment process directly.
5. Select **Deploy with IBM Cloud Schematics**.
6. Add the input parameters for this installation. There are 3 categories of parameters:
 - **Workspace** - These parameters define the workspace that is automatically created in Schematics:
 - Enter a name for the workspace or use the default name.
 - The Resource Group used to create resources. Use default or create a Resource Group.
 - Select a location to create your Schematics workspace. The workspace location need not match the resource location.
 - **Required input variables** - Review the default input variables and provide values that match your solution. These parameters are specific to your deployment. For more detailed information, see the [Readme file](#).

Parameter	Description
BASTION_FLOATING_IP	Required only for Schematics Deployments. The Floating IP from the Bastion Server.

HOSTNAME	The hostname for the VSI. The hostname should be up to 13 characters as required by SAP. For more information on the rules regarding hostnames for SAP systems, check SAP Note 611361: Hostnames of SAP ABAP Platform servers
REGION	The cloud region to deploy the solution. The regions and zones for VPC are listed here . Review supported locations in IBM Cloud Schematics here . Sample value: eu-de.
RESOURCE_GROUP	The name of an existing Resource Group for VSIs and Volumes resources. Default value: "Default". The list of Resource Groups is available here .
SECURITY_GROUP	The name of an existing Security group. The list of security groups is available here .
SSH_KEYS	The list of SSH Keys UUIDs that are allowed to SSH as root to the VSI can contain one or more IDs. The list of SSH Keys is available here . Sample input (use your own SSH UUIDs from IBM Cloud){: external}: ["r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a", "r010-3fcfd9fe7-d4a7-41ce-8bb3-d96e936b2c7e"]
SUBNET	The name of an existing subnet. The list of subnets is available here .
VPC	The name of an existing VPC. The list of VPCs is available here .
ZONE	The cloud zone where to deploy the solution. Sample value: eu-de-2.
ibmcloud_api_key	IBM Cloud API key (Sensitive* value).
private_ssh_key	Required only for Schematics Deployments - Input your id_rsa private key pair content in OpenSSH format (Sensitive* value). This private key should be used only during the terraform provisioning and it is recommended to be changed after the SAP deployment.
hdb_instance_number	The instance number of the SAP HANA database server.
sap_aas_instance_number	Technical identifier for the internal processes of the additional application server.
sap_asci_instance_number	Technical identifier for the internal processes of ASCS.
sap_ci_host	IP address of the existing SAP Central Instance.
sap_ci_hostname	The hostname of the existing SAP Central Instance.
sap_ci_instance_number	Technical identifier for the internal processes of the Central Instance.
sap_sid	The SAP system ID identifies the entire SAP system.
sap_main_password	Common password for all users that are created during the installation (See Obs*).

Required Variables

- **Optional variables** - Review and update the optional input variables. The Ansible scripts expect the SAP kits to be in the default locations listed. For more information, see the [Readme file - Input Parameters](#).

Parameter	Description
ID_RSA_FILE_PATH	The file path for private_ssh_key is automatically generated by default. If it is changed, it must contain the relative path from Git repo folders. Default value: "ansible/id_rsa".
IMAGE	The OS image used for the VSI. A list of images is available here .
PROFILE	The profile used for the VSI. A list of profiles is available here . For more information about supported DB/OS and IBM Gen 2 Virtual Server Instances (VSI), check SAP Note 2927211: SAP Applications on IBM Virtual Private Cloud .

VOL1	Volume 1 Size - The size for the disks in GB that are to be attached to the VSI and used by SAP.
VOL2	Volume 2 Size - The size for the disks in GB that are to be attached to the VSI and used by SAP.
kit_sapcar_file	Path to the sapcar binary, as downloaded from SAP Support Portal.
kit_swpm_file	Path to the SWPM archive (SAR), as downloaded from SAP Support Portal.
kit_saphostagent_file	Path to the SAP Host Agent archive (SAR), as downloaded from SAP Support Portal.
kit_hdbclient_file	Path to the HANA DB client archive (SAR), as downloaded from SAP Support Portal.

Optional Variables

7. Accept the license agreement.
8. Select **Deploy**. The deployment starts and you are directed to the Schematics page that displays the script log files for you to monitor the deployment progress.

Creating the infrastructure using Terraform with the bastion server CLI

Use these steps to configure the IBM Cloud Provider plug-in and use Terraform to install SAP AAS to SAP HANA and AnyDB on your existing VPC on an already deployed SAP NetWeaver 7.X with SAP HANA 2.0 or ASE SYB as a Central Instance.

The script takes 1 - 2 hours to complete.

1. Access the bastion server cli.
2. Clone the solution repository and change to the folder.

ASE SYB 16 Clone the solution repository from <https://github.com/IBM-Cloud/sap-aas-abap-ase-syb> and cd to the sap-aas-abap-ase-syb/cli folder.

```
$ git clone https://github.com/IBM-Cloud/sap-aas-abap-ase-syb
cd sap-aas-abap-ase-syb/cli/
```

SAP HANA 2.0: Clone the solution repository from <https://github.com/IBM-Cloud/sap-abap-hana-aas> and cd to the sap-abap-hana-aas folder.

```
$ git clone https://github.com/IBM-Cloud/sap-abap-hana-aas.git
cd sap-abap-hana-aas/
```

3. Modify the `input.auto.tfvars` file to specify the information for the existing VPC, your region, zone, networking component names, hostname for the AAS VSI,profile, and image. You need your 40-digit SSH key ID for this file. The second SSH key is optional. For more options for profile, see [Instance Profiles](#). For more options, see [Images](#). For descriptions of the variables, see the [readme](#) file.

The VSI OS images that are supported for this solution for Netweaver Additional Application Server are:

- ibm-redhat-8-4-amd64-sap-applications-2
- ibm-redhat-8-6-amd64-sap-applications-2
- ibm-sles-15-3-amd64-sap-applications-2
- ibm-sles-15-4-amd64-sap-applications-4

```
$ # Infra VPC variables for ASE SYB
REGION    = "eu-de"
ZONE      = "eu-de-2"
VPC        = "ic4sap"                      # EXISTING Security group name
SECURITY_GROUP = "ic4sap-securitygroup"      # EXISTING Security group name
RESOURCE_GROUP = "wes-automation"
SUBNET     = "ic4sap-subnet"                  # EXISTING Subnet name
SSH_KEYS   = [ "r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a" , "r010-3fcfd9fe7-d4a7-41ce-8bb3-
d96e936b2c7e" ]

# SAP AAS VSI variables:
```

```

HOSTNAME = "sapnwase-as01"
PROFILE = "bx2-4x16"
IMAGE = "ibm-redhat-8-4-amd64-sap-applications-2

$ # Infra VPC variables for ABAP HANA
REGION      = "eu-de"
ZONE        = "eu-de-2"
VPC          = "ic4sap" # EXISTING Security group name
SECURITY_GROUP = "ic4sap-securitygroup" # EXISTING Security group name
RESOURCE_GROUP = "wes-automation"
SUBNET       = "ic4sap-subnet" # EXISTING Subnet name
SSH_KEYS     = [ "r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a" , "r010-3fc9fe7-d4a7-41ce-8bb3-d96e936b2c7e" ]
ID_RSA_FILE_PATH = "ansible/id_rsa"

# SAP AAS variables:
HOSTNAME = "sapnwapp"
PROFILE = "bx2-4x16"
IMAGE = "ibm-redhat-8-6-amd64-sap-applications-2"

```

4. Customize your SAP system configuration. In the same file, input.auto.tfvars, edit the SAP system configuration variables that are passed to the Ansible automated deployment. For descriptions of the variables, see the [readme](#) file.

```

$ # SAP system configuration - for ASE SYB
sap_sid = "NWD"
sap_ci_host = "10.243.132.10"
sap_ci_hostname = "sapnwase"
sap_ci_instance_number = "00"
sap_asc_s_instance_number = "01"
sap_aas_instance_number = "00"

# Kits paths
kit_sapcar_file = "/storage/NW75SYB/SAPCAR_1010-70006178.EXE"
kit_swpm_file = "/storage/NW75SYB/SWPM10SP31_7-20009701.SAR"
kit_saphotagent_file = "/storage/NW75SYB/SAPHOSTAGENT51_51-20009394.SAR"

```

```

$ # SAP system configuration - for ABAP HANA
sap_sid = "NWD"
sap_ci_host = "10.243.132.10"
sap_ci_hostname = "sapnwapp01"
sap_ci_instance_number = "00"
sap_asc_s_instance_number = "01"
hdb_instance_number = "00"
sap_aas_instance_number = "00"

# Kits paths
kit_sapcar_file = "/storage/NW75HDB/SAPCAR_1010-70006178.EXE"
kit_swpm_file = "/storage/NW75HDB/SWPM10SP31_7-20009701.SAR"
kit_saphotagent_file = "/storage/NW75HDB/SAPHOSTAGENT51_51-20009394.SAR"
kit_hdbclient_file = "/storage/NW75HDB/IMDB_CLIENT20_009_28-80002082.SAR"

```

Ansible decompresses the rest of the SAP kit files. For more information, see the [readme](#) file.

5. Initialize the Terraform CLI.

```
terraform init
```

6. Create a Terraform execution plan. The Terraform execution plan summarizes all the actions that are done to create the virtual private cloud instance in your account.

```
terraform plan plan1
```

Enter an SAP main password and your API key.

The SAP main password must be 10 - 14 characters long and contain at least one digit (0-9). It can contain only the following characters: a-z, A-Z, 0-9, @, #, \$, . *This password cannot contain exclamation points '!'. The password must not start with a digit or an underscore ().*

7. Verify that the plan shows all of the resources that you want to create and that the names and values are correct. If the plan needs to be adjusted, edit the input.auto.tfvars file to correct resources and run terraform plan again.
8. Apply the saved plan.

```
$ terraform apply "plan1"
```

The virtual private cloud and components are created and you see output similar to the `terraform plan` output.

9. Add the SAP credentials and the virtual server instance IP to the SAP GUI. For more information about the SAP GUI, see [SAP GUI](#).

Next steps

If you need to rename your resources after they are created, modify the `input.auto.tfvars` file to change the names and run `terraform plan` and `terraform apply` again. Do not use the IBM Cloud Dashboard and user interface to modify your VPC after it is created. The Terraform scripts create a complete solution and selectively modifying resources with the user interface might cause unexpected results.

If you need to remove the SAP Netweaver 7.X on HANA or AnyDB installation, go to your project folder and run `terraform destroy`. The `terraform destroy` command does not remove the VPC in this scenario because the VPC was created before these Terraform scripts were run.

Related information

For more information about Terraform on IBM Cloud, see [Getting started with Terraform on IBM Cloud](#).

For more information about using Terraform for creating only a VPC for SAP, without the SAP architecture, see [Creating single-tier virtual private cloud for SAP by using Terraform](#).

SAP One Support Notes that apply to this document:

- [SAP Note 84555 - Windows Server, Linux®, and UNIX: Certified hardware](#)
- [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#)
- [SAP Note 2923773 - Linux® on IBM Cloud \(IaaS\): Adaption of your SAP license](#)
- [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#)
- [SAP Note 2369910 - SAP Software on Linux®: General information](#)
- [SAP Note 171380 - Released IBM hardware \(Intel processors\) and IBM cloud services offers](#)
- [SAP Note 1380654 - SAP support in IaaS environments](#)

This document is referenced by:

- [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#)
- [SAP Note 2588225 - SAP on IBM Cloud: Protect against speculative execution vulnerabilities](#)
- [SAP Note 1380654 - SAP support in IaaS environments](#)
- [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#)

SAP NetWeaver HA deployment in VPC

Automating SAP workload HA deployment on IBM Cloud VPC with Terraform and Ansible

You can use Terraform to automate IBM Cloud® VPC provisioning. The VPC provisioned includes virtual server instances with high network performance. The VPC infrastructure contains various Infrastructure-as-a-Service (IaaS) offerings, including virtual servers. After the VPC is provisioned, the scripts use the Ansible Playbooks to install the SAP system.

IBM Cloud VPC introduction

VPC is a public cloud offering that an enterprise uses to establish its own private cloud-like computing environment on shared [public cloud](#) infrastructure. VPC gives an enterprise the ability to define and control a virtual network that is logically isolated from all other public cloud tenants, creating a private and secure place on the public cloud.

Imagine that a cloud provider's infrastructure is a residential apartment building and multiple families live inside. A public cloud tenant is a kind of sharing an apartment with a few roommates. In contrast, having a VPC is like having your own private condominium; no one else has the key, and no one can enter the space without your permission.

VPC's logical isolation is implemented by using virtual network functions and security features that give the enterprise customer granular control over which IP addresses or applications can access particular resources. It is analogous to the "friends-only" or "public/private" controls on social media accounts used to restrict who can or can't see your otherwise public posts.

With IBM Cloud VPC, you can use the UI, CLI, and API to manually provision virtual server instances for VPC with high network performance. VPC infrastructure contains various Infrastructure-as-a-Service (IaaS) offerings including virtual servers for VPC.

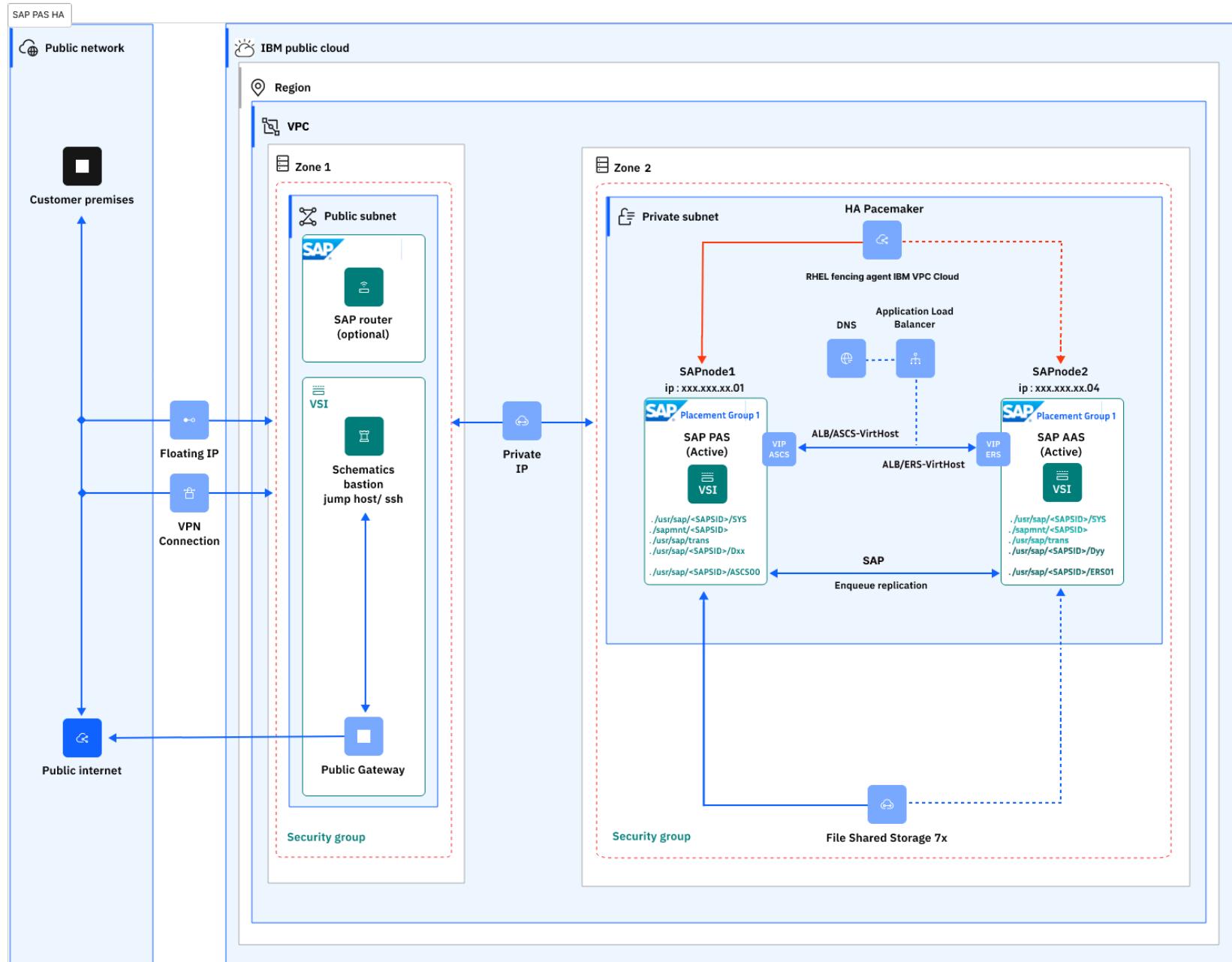
Use the following information to understand a simple use-case for planning, creating, and configuring resources for your VPC, and learn more about VPC overviews and VPC tutorials. For more information about the VPC, see [Getting started with Virtual Private Cloud \(VPC\)](#).

SAP products architecture on IBM Cloud VPC

A [Virtual Private Cloud \(VPC\)](#) contains one of the most secure and reliable cloud environments for SAP applications within your own VPC with virtual server instances. This represents an Infrastructure-as-a-Service (IaaS){: external} within IBM Cloud that offers all the benefits of isolated, secure, and flexible virtual cloud infrastructure from IBM. In comparison, the IBM Cloud classic infrastructure virtual servers offering uses virtual instances with native and VLAN networking to communicate with each other within a data center; however, the instances are restricted in one well-working pod by using subnet and VLAN networking as a gap scale up of virtual resources should rely between the pods. The IBM Cloud VPC network orchestrator layer concept eliminates the pod boundaries and restrictions, so this new concept handles all the networking for every virtual instance running within VPC across regions and zones.

Highly available system for SAP NetWeaver on IBM Cloud VPC

In a Highly Available (HA) system, every instance can run on a separate IBM Cloud virtual server instance. The cluster HA configuration for the SAP application server consists of two virtual server instances, each of them located in the same zone within the region by using placement groups. Placement groups assure that both cluster resources and cloud resources are also located in different compute nodes as specified in the following placement groups section:



SAP HA for SAP applications cluster nodes PAS (Active) and AAS (Active)

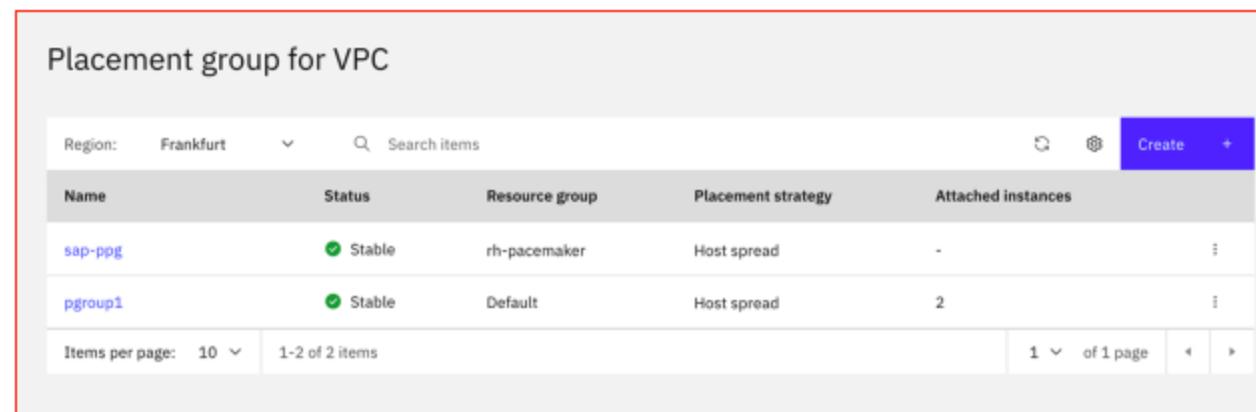
Placement groups on IBM Cloud VPC for SAP HA architecture

Placement Groups (PG) for VPC have two different anti-affinity strategies for high availability. By using the placement strategies, you minimize the chance of service disruption with virtual server instances that are placed on different hosts or into an infrastructure with separate power and network supplies.

The design of placement groups for IBM Cloud virtual servers solves this issue. Placement groups give a measure of control over the host on which a new public virtual server is placed. In this release, a “spread” rule is implemented, which means that the virtual servers within a placement group are spread onto different hosts. You can build a highly available application within a data center and know that your virtual servers are isolated from each other.

Placement groups with the spread rule are available to create in selected IBM Cloud data centers. After a spread rule is created, you can provision a virtual server into that group and ensure that it is not on the same host as any of your other virtual servers. This feature comes with no cost.

You can create your placement group and assign up to four new virtual server instances. With the spread rule, each of your virtual servers are provisioned on different physical hosts. In the following configuration example, the “Power Spread” option is used:



Placement groups host spread

Placement group for VPC					
Name	Status	Resource group	Placement strategy	Attached instances	
sapha-poc	Stable	wes-ic4sap-resourcegroup	Power spread	4	
Items per page: 10 1 item 1 of 1 page					

Placement groups power spread

Following are the SAP instances that are required for HA scenario:

- ABAP SAP Central Services (ASCS) instance - contains the ABAP message server and the ABAP enqueue server.
- Enqueue Replication Server (ERS) instance for the ASCS instance.
- Database instance
- Primary Application Server (PAS) instance on node 1.
- Additional Application Server (AAS) instance on node 2.



Note: It is recommended to run both the ASCS instance and the ERS instance in a switchover cluster infrastructure.

IBM Cloud File Storage for VPC for SAP HA architecture

[IBM Cloud File Storage for VPC](#) technology is used to make the SAP directories available to the SAP system. The technologies of choice are NFS, shared disks, and cluster file system. If you have decided to use the HA solution for your SAP system, make sure that you properly address the HA requirements of the SAP file systems in your SAP environment.

File shares for VPC								
Name	Status	Resource groups	Location	Mount targets	Size	Replication role	Encryption type	
usrsap-as1-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-as2-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-sapsacs-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-sapers-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-sapmnt-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-sapsys-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-trans-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	80 GB	None	Provider managed	

File shares for VPC

- File shares that are mounted as NFS permanent file systems on both cluster nodes for SAP HA application:
 - `/usr/sap/<SAPSID>/SYS`
 - `/sapmnt<SAPSID>`
 - `/usr/sap/trans`
- Cluster-managed file systems for SAP HA application: ASCS
 - `/usr/sap/<SAPSID>/ASCS00`
 - `/usr/sap/<SAPSID>/ERS01`
- Permanent NFS mount on SAP HA application node 1 PAS instance:
 - `/usr/sap/<SAPSID>/Dxx`
- Permanent NFS mount on SAP HA application node 2 dialog instance:
 - `/usr/sap/<SAPSID>/Dyy`

Prerequisites

You need to install the hardware (hosts, disks, and network) and decide how to distribute the database, SAP instances, and if required, the Network File System (NFS) server over the cluster nodes.

Context

Following are the types of SAP directories:

- Physically shared directories: `/<sapmnt>/<SAPSID>` and `/usr/sap/trans`

- Logically shared directories that are bound to a node, such as `/usr/sap`, with the following local directories:
 - `/usr/sap/<SAPSID>`
 - `/usr/sap/<SAPSID>/SYS`
 - `/usr/sap/hostctrl`
- Local directories that contain the SAP instances such as `/usr/sap/<SAPSID>/ASCS<Instance_Number>`
- The global transport directory may reside on a separate SAP transport host as a standard three systems transport layer configuration.

You need at least two nodes and a shared file system for distributed ASCS and ERS instances. The assumption is that the rest of the components are distributed on other nodes.

ASCS and ERS installation

In order for the ASCS and ERS instances to be able to move from one node to the other, they need to be installed on a shared file system and use virtual hostnames based on the virtual IP.

In this VPC-based SAP HA solution, the shared file system that is required by the cluster is replaced by the NFS-mounted file storage, and the virtual IP is replaced by the Application Load Balancer for VPC (ALB).

In this scenario, three ALBs are used, one for each Single Point of Failure (SPOF) component in order to replace the virtual IP requirement: ALB for ASCS, ALB for ERS, and ALB for ASE Sybase. Each ALB is configured as a backend for the corresponding cluster servers and redirects all of the communication that is received on the front-end ports to the active server in the backend pool.

Load balancers for VPC						
Region:	Frankfurt	▼	<input type="text"/> poc	X		
Name	Status	Family	Resource group	Type	Hostname	Location
db-alb-hana-poc	Active	Application	wes-ic4sap-resourcegroup	Private	20bdd130-eu-de.l b.appdomain.cloud	Frankfurt
sap-alb-ers-poc	Active	Application	wes-ic4sap-resourcegroup	Private	3941d983-eu-de.l b.appdomain.cloud	Frankfurt
sap-alb-ascs-poc	Active	Application	wes-ic4sap-resourcegroup	Private	56a9190d-eu-de.l b.appdomain.cloud	Frankfurt

Application load balancer management of HA IPs mechanism

Private application load balancer

A [private application load balancer](#) is accessible through your private subnets that you configured to create the load balancer.

Similar to a public application load balancer, your private application load balancer service instance is assigned an FQDN; however, this domain name is registered with one or more private IP addresses.

IBM Cloud operations change the number and value of your assigned private IP addresses over time, based on maintenance and scaling activities. The backend virtual server instances that host your application must run in the same region and under the same VPC.

Use the assigned ALB FQDN to send traffic to the private application load balancer to avoid connectivity problems to your applications during system maintenance or scaling down activities.

Each ALB sends traffic to the cluster node where the application (ASCS, ERS, ASE Sybase DB) is running. During the cluster failover, the ALB redirects all the traffic to the new node where the resources are up and running.



Note: DNS-as-a-Service (DNSaaS) is the management IBM Cloud VPC DNS service of HA and FQDN (IPs) mechanism.



Note: The ALB has a default of 50 seconds for client and server timeout, so after 50 seconds of inactivity, the connection is closed. To support SAP connections through ALB and not lose connection after 50 seconds, you need to request a change this value to a minimum of 300 seconds (client-side idle connection = minimum 300s and server-side idle connection = minimum 300s). To request this change, open a support ticket. This is an account-wide change that affects all of the ALBs in your account. For more information, see [Connection timeouts](#).

DNS Services with VPC

[IBM Cloud DNS Services](#) provide private DNS to VPC users. Private DNS zones are resolvable only on IBM Cloud and from explicitly [permitted networks](#) in an account. To get started, create a DNS Services instance by using the IBM Cloud console.

DNS Services allows you to:

- Create the private DNS zones that are collections for holding the domain names.
- Create the DNS resource records under these DNS zones.
- Specify the access controls used for the DNS resolution of resource records on a zone-wide level.

DNS Services also maintains its own worldwide set of DNS resolvers. Instances that are provisioned under IBM Cloud on an IBM Cloud network can use resource records that are configured through IBM Cloud DNS Services by querying DNS Services resolvers.

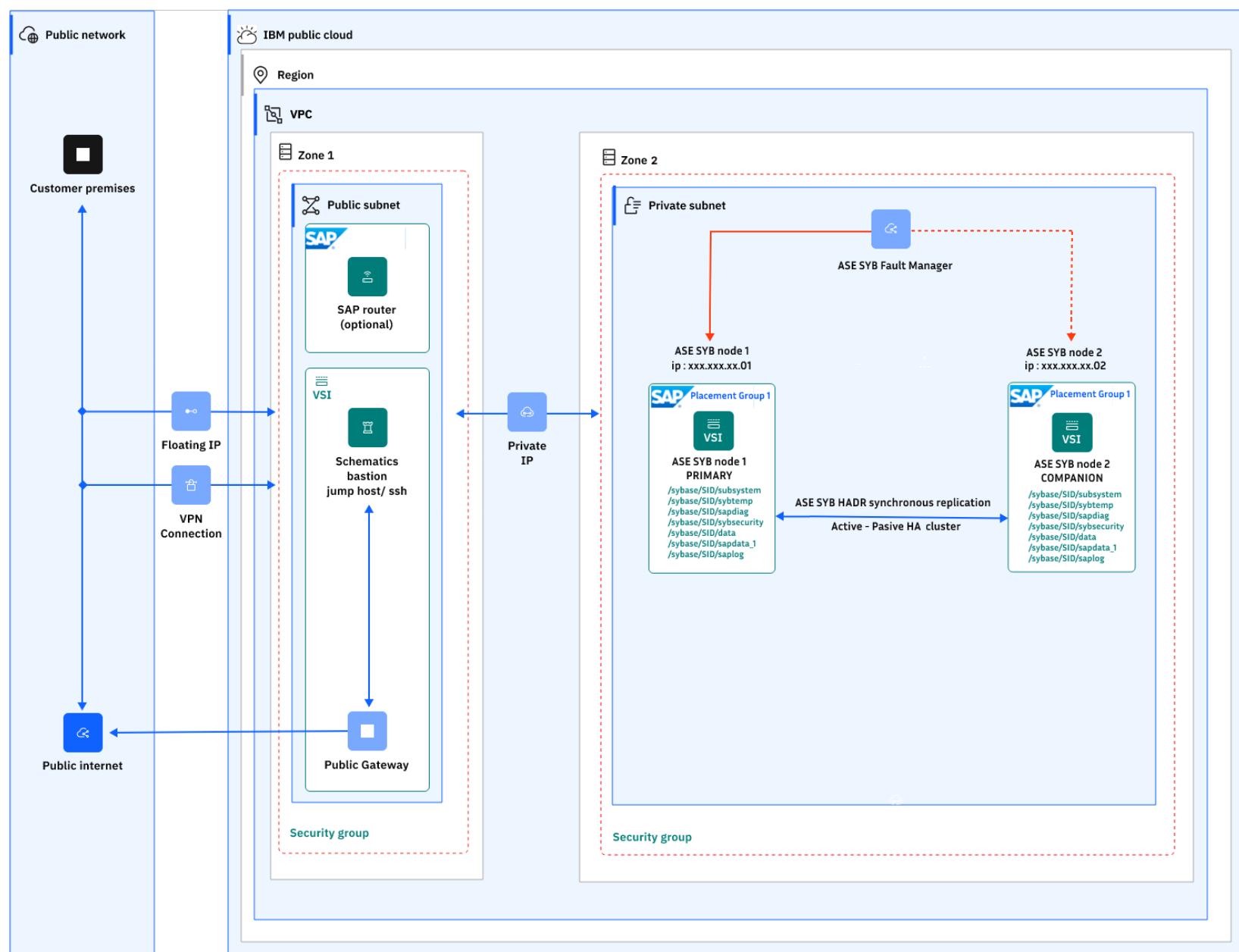
Resource records and zones that are configured through DNS Services are:

- Separated from the wider public DNS, and their publicly accessible records.
- Hidden from the system outside of and not part of the IBM Cloud private network.
- Accessible only from the system that you authorize on the IBM Cloud private network.
- Resolvable only via the resolvers provided by the service.

The DNS service maps the FQDN of each ALB to the virtual hostnames of the ASCS, ERS, and ASE Sybase that are used by SAP applications.

Type	Name	Value	TTL
CNAME	dbpochana	is an alias of 20bdd130-eu-de.lb.appdomain.cloud	12 hr
CNAME	sappocers	is an alias of 3941d983-eu-de.lb.appdomain.cloud	12 hr
CNAME	sappocases	is an alias of 56a9190d-eu-de.lb.appdomain.cloud	12 hr

Highly available system for SAP ASE Sybase database with HADR system



SAP HA for ASE Sybase DB instances cluster nodes primary (Active) and Secondary (Companion)

At the most basic level, a standard HA ASE Sybase cluster in an active(primary)-passive(companion) configuration has two nodes: one is the primary node and the other is the standby node. This means that the primary node is actively serving the active SAP DB instances (Primary and Companion), while the standby node is waiting to jump in if there is any failure.

The cluster is set with a virtual hostname IP (hostname is mapped to the FQDN of the ASE Sybase ALB through DNS, which is the same as

explained previously for SAP ASCS and ERS instances). Application instances (PAS and AAS) are used on the SAP profiles to call that particular component. The cluster assigns the virtual IP to the active node and uses a heartbeat monitor to confirm the availability of the components. If the primary node stops responding, it triggers the automatic failover mechanism that calls the standby node to step up to become the primary node. The ALB detects the change, redirects the traffic to the new active node, and assigns the virtual IP to it, restoring the component availability. Once fixed, the failed node comes online as a standby node.

SAP Sybase HADR system supports synchronous replication

The SAP Sybase HADR system supports synchronous replication between the primary and standby servers for high availability. An active-active setup is a two-node configuration where both nodes in the cluster include SAP ASE managing independent workloads, capable of taking over each others workload in the event of a failure.

The SAP ASE server that takes over the workload is called a secondary companion, and the SAP ASE server that fails is called the primary companion. Together they are companion servers. This movement from one node to another is called failover. After the primary companion is ready to resume its workload, it is moved back to its original node. This movement is called a failback.

When a system fails over, clients that are connected to the primary companion and use the failover property automatically reestablish their network connections to the secondary companion. You must tune your operating system to successfully manage both servers during fail over. See your operating system documentation for information about configuring your system for high availability. An SAP ASE configured for failover in an active-active setup can be shut down using the shutdown command only after you have suspended SAP ASE from the companion configuration, at both the server level and the platform level.

The always-on option in a High Availability and Disaster Recovery (HADR) system consists of two SAP ASE servers:

- Primary on which all transaction processing takes place.
- Warm standby (referred to as a "standby server" in DR mode, and as a "companion" in HA mode) for the primary server, and contains copies of designated databases from the primary server.



Note: The HADR feature that is shipped with SAP ASE version 16.0 SP02 supports only a single-companion server.

Some high-availability solutions (for example, the SAP Adaptive Server Enterprise Cluster Edition) share or use common resources between nodes. However, the HADR system is a "shared nothing" configuration, each node has separate resources including disks.

In an HADR system, servers are separate entities and data is replicated from the primary server to the companion server. If the primary server fails, a companion server is promoted to the role of primary server either manually or automatically. Once the promotion is complete, clients can reconnect to the new primary server, and see all committed data, including data that was committed on the previous primary server.

Servers can be separated geographically, which makes an HADR system capable of withstanding the loss of an entire computing facility.



Note: The HADR system includes an embedded SAP Replication Server, which synchronizes the databases between the primary and companion servers. SAP ASE uses the Replication Management Agent (RMA) to communicate with Replication Server and SAP Replication Server uses Open Client connectivity to communicate with the companion SAP ASE.

The Replication Agent detects any data changes made on the primary server and sends them to the primary SAP Replication Server. In the figure above, the unidirectional arrows indicate that, although both SAP Replication Servers are configured, only one direction is enabled at a time.

The HADR system supports synchronous replication between the primary and standby servers for high availability so the two servers can keep in sync with Zero Data Loss (ZDL). This requires a network link that is fast enough between the primary and standby server so that synchronous replication can keep up with the primary servers workload. Generally, this means that the network latency is approximately the same speed as the local disk IO speed, a few (fewer than 10) milliseconds. Anything longer than a few milliseconds may result in a slower response to write operations at the primary.

The HADR system supports asynchronous replication between the primary and standby servers for disaster recovery. The primary and standby servers by using asynchronous replication can be geographically distant, meaning they can have a slower network link. With asynchronous replication, Replication Agent Thread captures the primary servers workload, which is delivered asynchronously to SAP Replication Server. The SAP Replication Server applies these workload change to the companion server.

The most fundamental service that is offered by the HADR system is the failover; planned or unplanned from the primary to the companion server, which allows maintenance activity to occur on the old primary server, while applications continue on the new primary.

The HADR system provides protection in the event of a disaster. If the primary server is lost, the companion server can be used as a replacement. Client applications can switch to the companion server, and the companion server is quickly available for users. If the SAP Replication Server was in synchronous mode before the failure of the primary server, the Fault Manager automatically initiates failover with

zero data loss.

Fault Manager installation on the SAP ASCS node

The required parameters are asked during the installation process to create a profile for the fault manager and then adds it to the instance start profile. It is also possible to run the installation by using an existing profile: `sybdbfm install pf=<SYBHA.PFL>` In this case, the installation process will only ask for profile parameters missing in the profile.



Note: Fault manger is integrated with ASCS on same SAP PAS/AAS cluster (start/stop/move together).

There may be some data loss if the SAP Replication Server was in asynchronous mode and you must use manual intervention to failover for disaster recovery.

Connection attempts to the companion server without the necessary privileges are silently redirected to the primary companion via the login redirection mechanism, which is supported by Connectivity libraries. If login redirection is not enabled, client connections fail and are disconnected.

The SAP ASE HADR option installs the below components:

- SAP ASE
- SAP Replication Server
- Replication Management Agent (RMA)
- SAP Host Agent
- Fault Manager
- SAP ASE Cockpit



Note: This automation is offered at no cost; however, the provisioned infrastructure comes at cost.

VPC with Additional Application Server (AAS) ABAP on Linux for SAP HANA

You can use Terraform scripts to create a single-tier VPC and create the AAS to HANA and AnyDB infrastructure on the VPC. The Terraform scripts use the VPC information that you provide and then call the Ansible playbook to create the SAP architecture on the specified VPC. Terraform on IBM Cloud® enables predictable and consistent provisioning of IBM Cloud Virtual Private Cloud (VPC) infrastructure resources so that you can rapidly build complex, cloud environments. IBM Cloud VPC infrastructure consists of SAP certified hardware that uses Intel® Xeon CPUs and more Intel® technologies.

You have two deployment methods to choose from:

- Terraform scripts that run from the CLI on your bastion server.
- Schematics user interface accessed from your cloud dashboard menu.

You can create SAP AAS NetWeaver 7.x on the SAP HANA-based ABAP stack.

SAP solution implemented

Many SAP enterprise solutions are built on the SAP platform (SAP NetWeaver) including:

- SAP HANA as Primary Persistence for SAP NetWeaver-based applications
- SAP Business Suite applications (ERP, CRM, and SCM, and other applications),
- SAP Business Warehouse (BW), and
- Other SAP enterprise solutions

SAP NetWeaver has two distinct aspects, ABAP and Java. Many applications that are built on the SAP NetWeaver's ABAP or Java (or both) application servers run on SAP DB owned HANA and ASE Sybase either in AnyDB platforms (MSSQL, Oracle, and Db2).

Technical interfaces are available for applications that are built on the SAP NetWeaver AS ABAP and AS Java to run on SAP HANA and AnyDB. However, specific development enablement is normally required for each application to ensure that it runs optimally on the SAP HANA. SAP Business Suite applications (ERP, CRM, SCM, and other applications), SAP Business Warehouse (BW), and other SAP NetWeaver-based applications were modified to run on SAP HANA and have many advantages. Also, various components and complimentary applications that are built on SAP NetWeaver can also run on SAP HANA or AnyDB by using the provided SAP NetWeaver DB interfaces.

The SAP HANA as primary persistence for SAP NetWeaver-based applications scenario has one restriction: SAP NetWeaver ABAP and Java

application servers must run on separate hardware servers from the SAP HANA hardware.

What is created

The scripts automate the virtual infrastructure resources, provisioning the processes for the SAP architecture in an existing VPC with a distributed environment. SAP AAS NetWeaver 7.x (HANA or ASE SYB) application server on a distinct VSI VPC system and SAP HANA DB on a dedicated server type VSI VPC box are provisioned. The scripts work in two phases.

During the first phase of [Automate SAP bastion server – SAP media storage repository](#), the following virtual infrastructure resources based on the components from the existing VPC created by the bastion server are:

- 1 VPC where the virtual server instance is provisioned.
- 1 security group. The rules for this security group are:
 - Allow inbound DNS traffic (port 53).
 - Allow inbound SSH traffic (TCP port 22).
 - Allow all outbound traffic from the virtual server instance.
 - Allow all traffic in the security group.
- 1 subnet to enable the networking in your VPC.
- 2 virtual server instances with SAP certified storage and network configurations.
- 1 floating IP address used to access your VPC virtual server instance over the public network.

During the second phase, the Ansible Playbooks is called and the SAP architecture is installed for both dedicated virtual server instance (VSI) SAP application; VSI system and dedicated SAP HANA VSI box. The SAP architecture that is deployed on the SAP NetWeaver 7.x release is a stand-alone dedicated SAP HANA 2.0 box release. For more information about this architecture, see [Automating SAP HANA stand-alone virtual server instance on IBM Cloud® VPC by using Terraform and Ansible](#).

You can provision only one instance of the service per IBM Cloud region.

Schematics deployment

When you run the scripts with the Schematics interface, you:

- Enter the workspace information.
- Enter the GitHub path for the chosen solution either on NetWeaver AAS for HANA.
- Modify the parameters in the Schematics interface. They are the same parameters as the `input.auto.tfvars` file that you use with the cli.

Virtual server instance configuration

Following are the supported operating system images for SAP NetWeaver primary application server:

- ibm-redhat-8-4-amd64-sap-applications-2
- ibm-redhat-8-6-amd64-sap-applications-2
- ibm-sles-15-3-amd64-sap-applications-2
- ibm-sles-15-4-amd64-sap-applications-3

Following are the supported operating system images for SAP HANA database:

- ibm-redhat-8-4-amd64-sap-hana-2
- ibm-redhat-8-6-amd64-sap-hana-2
- ibm-sles-15-3-amd64-sap-hana-2
- ibm-sles-15-4-amd64-sap-hana-1

For both server instances there are:

- Two SSH keys are configured to access SSH as `root`.
- Three storage volumes as described in the `input.auto.tfvars` file.

What is created for anydb

The scripts use the information that you provide for an existing VPC and deploy AAS to SAP HANA or AnyDB on a different host than CI (SAP Central Instance) VSI host. For more information about this architecture, see [SAP NetWeaver 7.x on UNIX with HANA or AnyDB on IBM Cloud](#)

[VPC on IBM Cloud VPC](#). You specify the information for the VPC to use in the `input.auto.tfvars` file.

The scripts call the Ansible Playbooks to install the SAP architecture.

Script files

The configuration and script files are provided on GitHub. Each supported interface for the SAP solution installation has its own folder in the GitHub repository:

- [GitHub repository for Terraform – AAS HANA](#)

Terraform interface

To run the Terraform script, you modify:

- The `input.auto.tfvars` file to specify the existing VPC resources for your solution. Specify the variables for the existing VPC:
 - VPC name
 - Security group
 - Subnet
 - Hostname
 - Profile
 - Image
 - Up to two SSH keys

You can change the default SAP system configuration settings to match your solution. You can also specify the location where you downloaded the SAP kits.

The IBM Cloud Provider plug-in for Terraform on IBM Cloud uses these configuration files to install AAS to SAP HANA and AnyDB on the specified VPC in your IBM Cloud account.

Support

There are no warranties of any kind, and there is no service or technical support available for these materials from IBM®. As a recommended practice, review carefully any materials that you download from this site before using them on a live system.

Though the materials provided herein are not supported by the IBM® Service organization, your comments are welcomed by the developers, who reserve the right to revise, readapt or remove the materials at any time. To report a problem, or provide suggestions or comments, open a GitHub issue.

Before you begin

Before you use the scripts in the bastion cli:

- Set up your account to access the VPC. Make sure that your account is [upgraded to a paid account](#).
- If you have not already, create a Bastion server to store the SAP kits. For more information, see [Automate SAP bastion server - SAP media storage repository](#).
- Download the SAP kits from the SAP Portal to your Deployment Server. Make note of the download locations. Ansible decompresses the files. For more information, see the [readme](#) file.
- [Create or retrieve an IBM Cloud API key](#). The API key is used to authenticate with the IBM Cloud platform and to determine your permissions for IBM Cloud services.
- [Create or retrieve your SSH key ID](#). You need the 40-digit UUID for the SSH key, not the SSH key name.
- Terraform should already be installed on the bastion server that you deployed. For more information, see [Bastion server for SAP deployment](#).
- (Optional - Catalog Tile) create secrets for your credentials and passwords by using the [Secrets Manager](#).

Deploying SAP AAS NetWeaver 7.x on HANA by using the Schematics user interface

Use these steps to configure the SAP Additional Application Server (AAS) NetWeaver with HANA or AnyDB on your existing VPC by using the Schematics interface. The script takes 2 - 3 hours to complete.

1. From the IBM Cloud menu, select **Schematics**.
2. Click **Create** workspace.

3. On the **Specify template** page:
 - Enter the URL for the Schematics interface.
 - Select the **Terraform version** that is listed in the readme file.
 - Click **Next**.
4. On the **workspace details** page:
 - Enter a name for the workspace.
 - Select a **Resource group**.
 - Select a **Location** for your workspace. The workspace location does not have to match the resource location.
 - Select **Next**.
5. Select **Create** to create your workspace.
6. On the workspace settings page, in the input variables section, review the default input variables and provide values that match your solution.
 For a more detailed description of each parameter, check the GitHub repo [AAS HANA readme](#) file, chapter "Input parameter file". Also, make sure to mark the parameters that contain sensitive information like passwords, API, and ssh private keys as "sensitive". These parameters are marked as "sensitive" in the readme file, under "Input parameter file".
7. On the workspace settings page, click **Generate plan**. Wait for the plan to complete.
8. Click **View log** to review the log files of your terraform execution plan.
9. Apply your Terraform template by clicking **Apply plan**.
10. Review the log file to ensure that no errors occur during the provisioning, modification, or deletion process.

Deploying SAP AAS NetWeaver (ABAP) on HANA with the Deployable Architecture tile interface

Use these steps to configure the SAP AAS NetWeaver (ABAP) on HANA on your existing VPC by using the catalog tile interface. The script takes 2 - 3 hours to complete.

1. From the IBM Cloud catalog, select **VPC with Additional Application Server ABAP on Linux for SAP HANA** on HANA tile. The **Create** tab opens for VPC with Additional Application Server ABAP on Linux for SAP HANA. For more information about this deployment, see the About tab or the readme file link.
2. Select the latest version.
3. Select **VPC with Additional Application Server ABAP on Linux for SAP HANA on Deployable Architecture tile** variation.
4. Click **Review deployment** options:
 - **Add to project** to add this deployment to an IBM Cloud project and combine it with other deployments. IBM Cloud projects include several more pipeline steps before deployment, including deployment validation, cost calculation, compliance verification, and approval process.
 - **Create from the CLI** to get the CLI command. With this command you can trigger the deployment from the CLI.
 - **Work with code** to embed the code into other terraform deployments.
 - **Deploy with IBM Cloud Schematics** to trigger the deployment process directly.
5. Select **Deploy with IBM Cloud Schematics**.
6. Add the input parameters for this installation. There are 3 categories of parameters:
 - **Workspace** - These parameters define the workspace that is automatically created in Schematics:
 - Enter a name for the workspace or use the default name.
 - The Resource Group used to create resources. Use default or create a Resource Group.
 - Select a location to create your Schematics workspace. The workspace location need not match the resource location.
 - **Required input variables** - Review the default input variables and provide values that match your solution. These parameters are specific to your deployment. For more detailed information, see the [Readme file](#).

Parameter	Description
BASTION_FLOATING_IP	Required only for Schematics Deployments. The Floating IP from the Bastion Server.

HOSTNAME	The hostname for the VSI. The hostname should be up to 13 characters as required by SAP. For more information on the rules regarding hostnames for SAP systems, check SAP Note 611361: Hostnames of SAP ABAP Platform servers
REGION	The cloud region to deploy the solution. The regions and zones for VPC are listed here . Review supported locations in IBM Cloud Schematics here . Sample value: eu-de.
RESOURCE_GROUP	The name of an existing Resource Group for VSIs and Volumes resources. Default value: "Default". The list of Resource Groups is available here .
SECURITY_GROUP	The name of an existing Security group. The list of security groups is available here .
SSH_KEYS	The list of SSH Keys UUIDs that are allowed to SSH as root to the VSI can contain one or more IDs. The list of SSH Keys is available here . Sample input (use your own SSH UUIDs from IBM Cloud){: external}: ["r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a", "r010-3fcfd9fe7-d4a7-41ce-8bb3-d96e936b2c7e"]
SUBNET	The name of an existing subnet. The list of subnets is available here .
VPC	The name of an existing VPC. The list of VPCs is available here .
ZONE	The cloud zone where to deploy the solution. Sample value: eu-de-2.
ibmcloud_api_key	IBM Cloud API key (Sensitive* value).
private_ssh_key	Required only for Schematics Deployments - Input your id_rsa private key pair content in OpenSSH format (Sensitive* value). This private key should be used only during the terraform provisioning and it is recommended to be changed after the SAP deployment.
hdb_instance_number	The instance number of the SAP HANA database server.
sap_aas_instance_number	Technical identifier for the internal processes of the additional application server.
sap_asci_instance_number	Technical identifier for the internal processes of ASCS.
sap_ci_host	IP address of the existing SAP Central Instance.
sap_ci_hostname	The hostname of the existing SAP Central Instance.
sap_ci_instance_number	Technical identifier for the internal processes of the Central Instance.
sap_sid	The SAP system ID identifies the entire SAP system.
sap_main_password	Common password for all users that are created during the installation (See Obs*).

Required Variables

- **Optional variables** - Review and update the optional input variables. The Ansible scripts expect the SAP kits to be in the default locations listed. For more information, see the [Readme file - Input Parameters](#).

Parameter	Description
ID_RSA_FILE_PATH	The file path for private_ssh_key is automatically generated by default. If it is changed, it must contain the relative path from Git repo folders. Default value: "ansible/id_rsa".
IMAGE	The OS image used for the VSI. A list of images is available here .
PROFILE	The profile used for the VSI. A list of profiles is available here . For more information about supported DB/OS and IBM Gen 2 Virtual Server Instances (VSI), check SAP Note 2927211: SAP Applications on IBM Virtual Private Cloud .

VOL1	Volume 1 Size - The size for the disks in GB that are to be attached to the VSI and used by SAP.
VOL2	Volume 2 Size - The size for the disks in GB that are to be attached to the VSI and used by SAP.
kit_sapcar_file	Path to the sapcar binary, as downloaded from SAP Support Portal.
kit_swpm_file	Path to the SWPM archive (SAR), as downloaded from SAP Support Portal.
kit_saphostagent_file	Path to the SAP Host Agent archive (SAR), as downloaded from SAP Support Portal.
kit_hdbclient_file	Path to the HANA DB client archive (SAR), as downloaded from SAP Support Portal.

Optional Variables

7. Accept the license agreement.
8. Select **Deploy**. The deployment starts and you are directed to the Schematics page that displays the script log files for you to monitor the deployment progress.

Creating the infrastructure using Terraform with the bastion server CLI

Use these steps to configure the IBM Cloud Provider plug-in and use Terraform to install SAP AAS to SAP HANA and AnyDB on your existing VPC on an already deployed SAP NetWeaver 7.X with SAP HANA 2.0 or ASE SYB as a Central Instance.

The script takes 1 - 2 hours to complete.

1. Access the bastion server cli.
2. Clone the solution repository and change to the folder.

ASE SYB 16 Clone the solution repository from <https://github.com/IBM-Cloud/sap-aas-abap-ase-syb> and cd to the sap-aas-abap-ase-syb/cli folder.

```
$ git clone https://github.com/IBM-Cloud/sap-aas-abap-ase-syb
cd sap-aas-abap-ase-syb/cli/
```

SAP HANA 2.0: Clone the solution repository from <https://github.com/IBM-Cloud/sap-abap-hana-aas> and cd to the sap-abap-hana-aas folder.

```
$ git clone https://github.com/IBM-Cloud/sap-abap-hana-aas.git
cd sap-abap-hana-aas/
```

3. Modify the `input.auto.tfvars` file to specify the information for the existing VPC, your region, zone, networking component names, hostname for the AAS VSI,profile, and image. You need your 40-digit SSH key ID for this file. The second SSH key is optional. For more options for profile, see [Instance Profiles](#). For more options, see [Images](#). For descriptions of the variables, see the [readme](#) file.

The VSI OS images that are supported for this solution for Netweaver Additional Application Server are:

- ibm-redhat-8-4-amd64-sap-applications-2
- ibm-redhat-8-6-amd64-sap-applications-2
- ibm-sles-15-3-amd64-sap-applications-2
- ibm-sles-15-4-amd64-sap-applications-4

```
$ # Infra VPC variables for ASE SYB
REGION    = "eu-de"
ZONE      = "eu-de-2"
VPC       = "ic4sap"                      # EXISTING Security group name
SECURITY_GROUP = "ic4sap-securitygroup"     # EXISTING Security group name
RESOURCE_GROUP = "wes-automation"
SUBNET    = "ic4sap-subnet"                 # EXISTING Subnet name
SSH_KEYS   = [ "r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a" , "r010-3fcfd9fe7-d4a7-41ce-8bb3-
d96e936b2c7e" ]

# SAP AAS VSI variables:
```

```

HOSTNAME = "sapnwase-as01"
PROFILE = "bx2-4x16"
IMAGE = "ibm-redhat-8-4-amd64-sap-applications-2

$ # Infra VPC variables for ABAP HANA
REGION      = "eu-de"
ZONE        = "eu-de-2"
VPC          = "ic4sap" # EXISTING Security group name
SECURITY_GROUP = "ic4sap-securitygroup" # EXISTING Security group name
RESOURCE_GROUP = "wes-automation"
SUBNET       = "ic4sap-subnet" # EXISTING Subnet name
SSH_KEYS     = [ "r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a" , "r010-3fc9fe7-d4a7-41ce-8bb3-d96e936b2c7e" ]
ID_RSA_FILE_PATH = "ansible/id_rsa"

# SAP AAS variables:
HOSTNAME = "sapnwapp"
PROFILE = "bx2-4x16"
IMAGE = "ibm-redhat-8-6-amd64-sap-applications-2"

```

4. Customize your SAP system configuration. In the same file, input.auto.tfvars, edit the SAP system configuration variables that are passed to the Ansible automated deployment. For descriptions of the variables, see the [readme](#) file.

```

$ # SAP system configuration - for ASE SYB
sap_sid = "NWD"
sap_ci_host = "10.243.132.10"
sap_ci_hostname = "sapnwase"
sap_ci_instance_number = "00"
sap_asc_s_instance_number = "01"
sap_aas_instance_number = "00"

# Kits paths
kit_sapcar_file = "/storage/NW75SYB/SAPCAR_1010-70006178.EXE"
kit_swpm_file = "/storage/NW75SYB/SWPM10SP31_7-20009701.SAR"
kit_saphotagent_file = "/storage/NW75SYB/SAPHOSTAGENT51_51-20009394.SAR"

```

```

$ # SAP system configuration - for ABAP HANA
sap_sid = "NWD"
sap_ci_host = "10.243.132.10"
sap_ci_hostname = "sapnwapp01"
sap_ci_instance_number = "00"
sap_asc_s_instance_number = "01"
hdb_instance_number = "00"
sap_aas_instance_number = "00"

# Kits paths
kit_sapcar_file = "/storage/NW75HDB/SAPCAR_1010-70006178.EXE"
kit_swpm_file = "/storage/NW75HDB/SWPM10SP31_7-20009701.SAR"
kit_saphotagent_file = "/storage/NW75HDB/SAPHOSTAGENT51_51-20009394.SAR"
kit_hdbclient_file = "/storage/NW75HDB/IMDB_CLIENT20_009_28-80002082.SAR"

```

Ansible decompresses the rest of the SAP kit files. For more information, see the [readme](#) file.

5. Initialize the Terraform CLI.

```
terraform init
```

6. Create a Terraform execution plan. The Terraform execution plan summarizes all the actions that are done to create the virtual private cloud instance in your account.

```
terraform plan plan1
```

Enter an SAP main password and your API key.

The SAP main password must be 10 - 14 characters long and contain at least one digit (0-9). It can contain only the following characters: a-z, A-Z, 0-9, @, #, \$, . *This password cannot contain exclamation points '!'. The password must not start with a digit or an underscore ().*

7. Verify that the plan shows all of the resources that you want to create and that the names and values are correct. If the plan needs to be adjusted, edit the input.auto.tfvars file to correct resources and run terraform plan again.
8. Apply the saved plan.

```
$ terraform apply "plan1"
```

The virtual private cloud and components are created and you see output similar to the `terraform plan` output.

9. Add the SAP credentials and the virtual server instance IP to the SAP GUI. For more information about the SAP GUI, see [SAP GUI](#).

Next steps

If you need to rename your resources after they are created, modify the `input.auto.tfvars` file to change the names and run `terraform plan` and `terraform apply` again. Do not use the IBM Cloud Dashboard and user interface to modify your VPC after it is created. The Terraform scripts create a complete solution and selectively modifying resources with the user interface might cause unexpected results.

If you need to remove the SAP Netweaver 7.X on HANA or AnyDB installation, go to your project folder and run `terraform destroy`. The `terraform destroy` command does not remove the VPC in this scenario because the VPC was created before these Terraform scripts were run.

Related information

For more information about Terraform on IBM Cloud, see [Getting started with Terraform on IBM Cloud](#).

For more information about using Terraform for creating only a VPC for SAP, without the SAP architecture, see [Creating single-tier virtual private cloud for SAP by using Terraform](#).

SAP One Support Notes that apply to this document:

- [SAP Note 84555 - Windows Server, Linux®, and UNIX: Certified hardware](#)
- [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#)
- [SAP Note 2923773 - Linux® on IBM Cloud \(IaaS\): Adaption of your SAP license](#)
- [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#)
- [SAP Note 2369910 - SAP Software on Linux®: General information](#)
- [SAP Note 171380 - Released IBM hardware \(Intel processors\) and IBM cloud services offers](#)
- [SAP Note 1380654 - SAP support in IaaS environments](#)

This document is referenced by:

- [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#)
- [SAP Note 2588225 - SAP on IBM Cloud: Protect against speculative execution vulnerabilities](#)
- [SAP Note 1380654 - SAP support in IaaS environments](#)
- [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#)

SAP HANA DB backup to Cloud Object Storage

Automating SAP workload HA deployment on IBM Cloud VPC with Terraform and Ansible

You can use Terraform to automate IBM Cloud® VPC provisioning. The VPC provisioned includes virtual server instances with high network performance. The VPC infrastructure contains various Infrastructure-as-a-Service (IaaS) offerings, including virtual servers. After the VPC is provisioned, the scripts use the Ansible Playbooks to install the SAP system.

IBM Cloud VPC introduction

VPC is a public cloud offering that an enterprise uses to establish its own private cloud-like computing environment on shared [public cloud](#) infrastructure. VPC gives an enterprise the ability to define and control a virtual network that is logically isolated from all other public cloud tenants, creating a private and secure place on the public cloud.

Imagine that a cloud provider's infrastructure is a residential apartment building and multiple families live inside. A public cloud tenant is a kind of sharing an apartment with a few roommates. In contrast, having a VPC is like having your own private condominium; no one else has the key, and no one can enter the space without your permission.

VPC's logical isolation is implemented by using virtual network functions and security features that give the enterprise customer granular control over which IP addresses or applications can access particular resources. It is analogous to the "friends-only" or "public/private" controls on social media accounts used to restrict who can or can't see your otherwise public posts.

With IBM Cloud VPC, you can use the UI, CLI, and API to manually provision virtual server instances for VPC with high network performance. VPC infrastructure contains various Infrastructure-as-a-Service (IaaS) offerings including virtual servers for VPC.

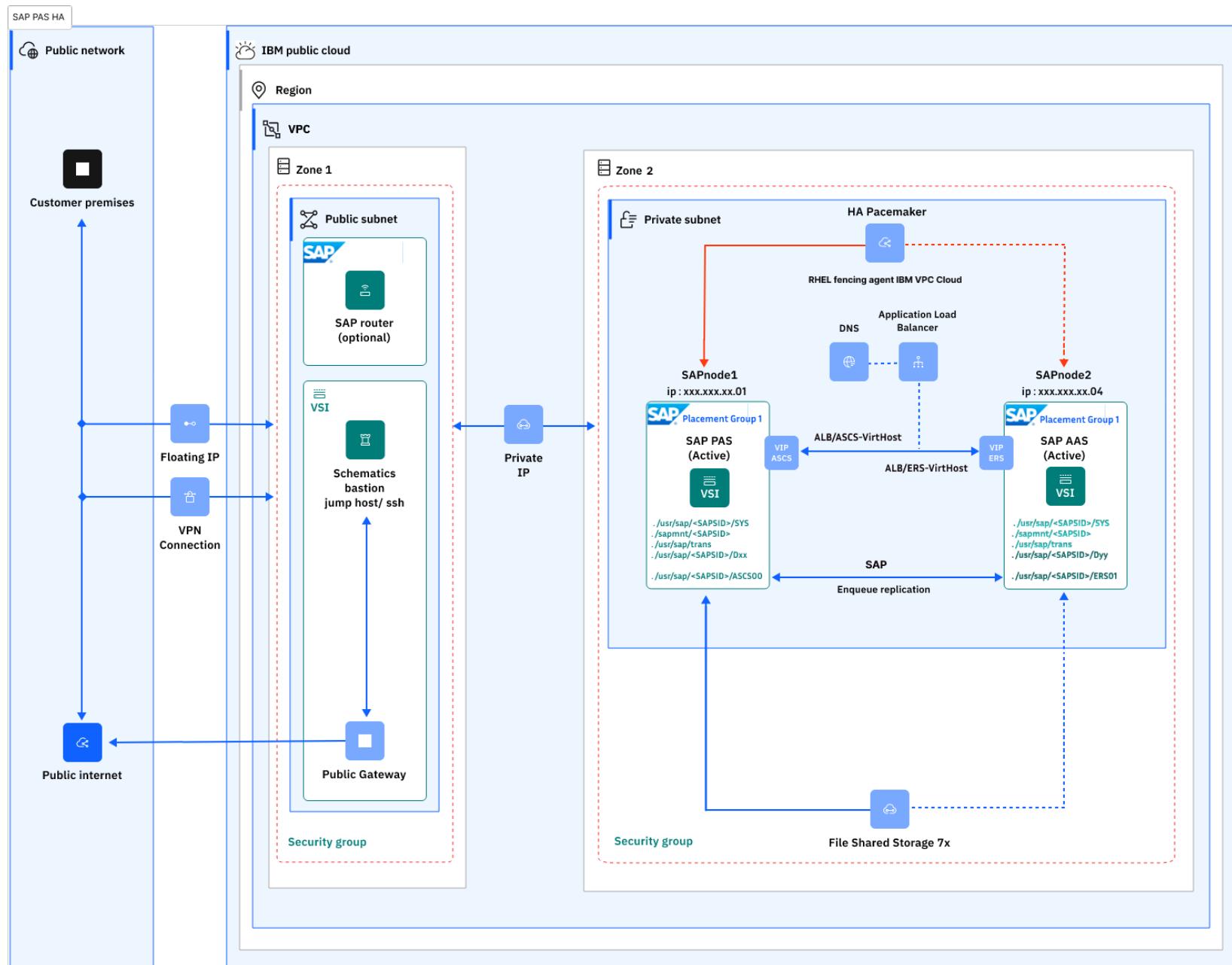
Use the following information to understand a simple use-case for planning, creating, and configuring resources for your VPC, and learn more about VPC overviews and VPC tutorials. For more information about the VPC, see [Getting started with Virtual Private Cloud \(VPC\)](#).

SAP products architecture on IBM Cloud VPC

A [Virtual Private Cloud \(VPC\)](#) contains one of the most secure and reliable cloud environments for SAP applications within your own VPC with virtual server instances. This represents an Infrastructure-as-a-Service (IaaS){: external} within IBM Cloud that offers all the benefits of isolated, secure, and flexible virtual cloud infrastructure from IBM. In comparison, the IBM Cloud classic infrastructure virtual servers offering uses virtual instances with native and VLAN networking to communicate with each other within a data center; however, the instances are restricted in one well-working pod by using subnet and VLAN networking as a gap scale up of virtual resources should rely between the pods. The IBM Cloud VPC network orchestrator layer concept eliminates the pod boundaries and restrictions, so this new concept handles all the networking for every virtual instance running within VPC across regions and zones.

Highly available system for SAP NetWeaver on IBM Cloud VPC

In a Highly Available (HA) system, every instance can run on a separate IBM Cloud virtual server instance. The cluster HA configuration for the SAP application server consists of two virtual server instances, each of them located in the same zone within the region by using placement groups. Placement groups assure that both cluster resources and cloud resources are also located in different compute nodes as specified in the following placement groups section:



SAP HA for SAP applications cluster nodes PAS (Active) and AAS (Active)

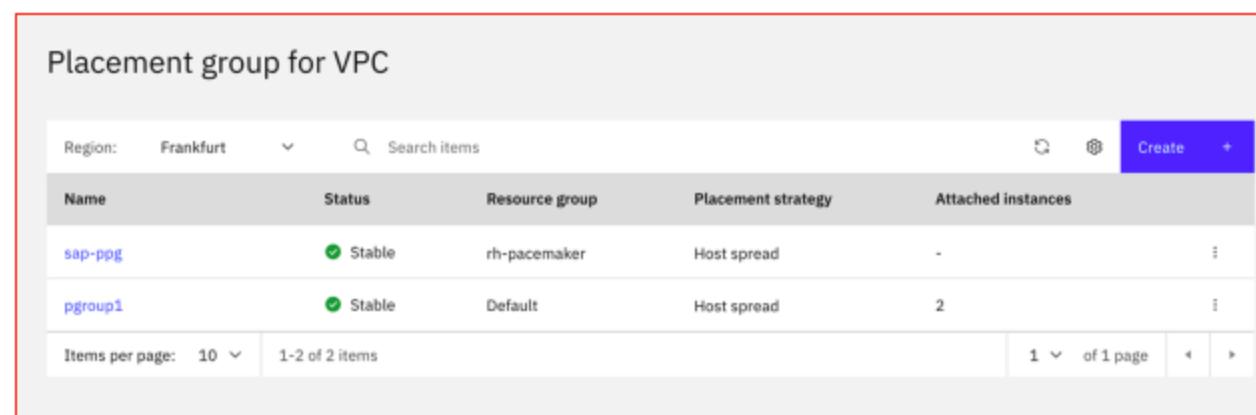
Placement groups on IBM Cloud VPC for SAP HA architecture

Placement Groups (PG) for VPC have two different anti-affinity strategies for high availability. By using the placement strategies, you minimize the chance of service disruption with virtual server instances that are placed on different hosts or into an infrastructure with separate power and network supplies.

The design of placement groups for IBM Cloud virtual servers solves this issue. Placement groups give a measure of control over the host on which a new public virtual server is placed. In this release, a “spread” rule is implemented, which means that the virtual servers within a placement group are spread onto different hosts. You can build a highly available application within a data center and know that your virtual servers are isolated from each other.

Placement groups with the spread rule are available to create in selected IBM Cloud data centers. After a spread rule is created, you can provision a virtual server into that group and ensure that it is not on the same host as any of your other virtual servers. This feature comes with no cost.

You can create your placement group and assign up to four new virtual server instances. With the spread rule, each of your virtual servers are provisioned on different physical hosts. In the following configuration example, the “Power Spread” option is used:



Placement groups host spread

Placement group for VPC					
Name	Status	Resource group	Placement strategy	Attached instances	
sapha-poc	Stable	wes-ic4sap-resourcegroup	Power spread	4	
Items per page: 10 1 item 1 of 1 page					

Placement groups power spread

Following are the SAP instances that are required for HA scenario:

- ABAP SAP Central Services (ASCS) instance - contains the ABAP message server and the ABAP enqueue server.
- Enqueue Replication Server (ERS) instance for the ASCS instance.
- Database instance
- Primary Application Server (PAS) instance on node 1.
- Additional Application Server (AAS) instance on node 2.



Note: It is recommended to run both the ASCS instance and the ERS instance in a switchover cluster infrastructure.

IBM Cloud File Storage for VPC for SAP HA architecture

[IBM Cloud File Storage for VPC](#) technology is used to make the SAP directories available to the SAP system. The technologies of choice are NFS, shared disks, and cluster file system. If you have decided to use the HA solution for your SAP system, make sure that you properly address the HA requirements of the SAP file systems in your SAP environment.

File shares for VPC								
Name	Status	Resource groups	Location	Mount targets	Size	Replication role	Encryption type	
usrsap-as1-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-as2-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-sapsacs-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-sapers-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-sapmnt-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-sapsys-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-trans-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	80 GB	None	Provider managed	

File shares for VPC

- File shares that are mounted as NFS permanent file systems on both cluster nodes for SAP HA application:
 - `/usr/sap/<SAPSID>/SYS`
 - `/sapmnt<SAPSID>`
 - `/usr/sap/trans`
- Cluster-managed file systems for SAP HA application: ASCS
 - `/usr/sap/<SAPSID>/ASCS00`
 - `/usr/sap/<SAPSID>/ERS01`
- Permanent NFS mount on SAP HA application node 1 PAS instance:
 - `/usr/sap/<SAPSID>/Dxx`
- Permanent NFS mount on SAP HA application node 2 dialog instance:
 - `/usr/sap/<SAPSID>/Dyy`

Prerequisites

You need to install the hardware (hosts, disks, and network) and decide how to distribute the database, SAP instances, and if required, the Network File System (NFS) server over the cluster nodes.

Context

Following are the types of SAP directories:

- Physically shared directories: `/<sapmnt>/<SAPSID>` and `/usr/sap/trans`

- Logically shared directories that are bound to a node, such as `/usr/sap`, with the following local directories:
 - `/usr/sap/<SAPSID>`
 - `/usr/sap/<SAPSID>/SYS`
 - `/usr/sap/hostctrl`
- Local directories that contain the SAP instances such as `/usr/sap/<SAPSID>/ASCS<Instance_Number>`
- The global transport directory may reside on a separate SAP transport host as a standard three systems transport layer configuration.

You need at least two nodes and a shared file system for distributed ASCS and ERS instances. The assumption is that the rest of the components are distributed on other nodes.

ASCS and ERS installation

In order for the ASCS and ERS instances to be able to move from one node to the other, they need to be installed on a shared file system and use virtual hostnames based on the virtual IP.

In this VPC-based SAP HA solution, the shared file system that is required by the cluster is replaced by the NFS-mounted file storage, and the virtual IP is replaced by the Application Load Balancer for VPC (ALB).

In this scenario, three ALBs are used, one for each Single Point of Failure (SPOF) component in order to replace the virtual IP requirement: ALB for ASCS, ALB for ERS, and ALB for ASE Sybase. Each ALB is configured as a backend for the corresponding cluster servers and redirects all of the communication that is received on the front-end ports to the active server in the backend pool.

Load balancers for VPC						
Region:	Frankfurt	▼	<input type="text"/> poc	X		
Name	Status	Family	Resource group	Type	Hostname	Location
db-alb-hana-poc	Active	Application	wes-ic4sap-resourcegroup	Private	20bdd130-eu-de.lb.appdomain.cloud	Frankfurt
sap-alb-ers-poc	Active	Application	wes-ic4sap-resourcegroup	Private	3941d983-eu-de.lb.appdomain.cloud	Frankfurt
sap-alb-ascs-poc	Active	Application	wes-ic4sap-resourcegroup	Private	56a9190d-eu-de.lb.appdomain.cloud	Frankfurt

Application load balancer management of HA IPs mechanism

Private application load balancer

A [private application load balancer](#) is accessible through your private subnets that you configured to create the load balancer.

Similar to a public application load balancer, your private application load balancer service instance is assigned an FQDN; however, this domain name is registered with one or more private IP addresses.

IBM Cloud operations change the number and value of your assigned private IP addresses over time, based on maintenance and scaling activities. The backend virtual server instances that host your application must run in the same region and under the same VPC.

Use the assigned ALB FQDN to send traffic to the private application load balancer to avoid connectivity problems to your applications during system maintenance or scaling down activities.

Each ALB sends traffic to the cluster node where the application (ASCS, ERS, ASE Sybase DB) is running. During the cluster failover, the ALB redirects all the traffic to the new node where the resources are up and running.



Note: DNS-as-a-Service (DNSaaS) is the management IBM Cloud VPC DNS service of HA and FQDN (IPs) mechanism.



Note: The ALB has a default of 50 seconds for client and server timeout, so after 50 seconds of inactivity, the connection is closed. To support SAP connections through ALB and not lose connection after 50 seconds, you need to request a change this value to a minimum of 300 seconds (client-side idle connection = minimum 300s and server-side idle connection = minimum 300s). To request this change, open a support ticket. This is an account-wide change that affects all of the ALBs in your account. For more information, see [Connection timeouts](#).

DNS Services with VPC

[IBM Cloud DNS Services](#) provide private DNS to VPC users. Private DNS zones are resolvable only on IBM Cloud and from explicitly [permitted networks](#) in an account. To get started, create a DNS Services instance by using the IBM Cloud console.

DNS Services allows you to:

- Create the private DNS zones that are collections for holding the domain names.
- Create the DNS resource records under these DNS zones.
- Specify the access controls used for the DNS resolution of resource records on a zone-wide level.

DNS Services also maintains its own worldwide set of DNS resolvers. Instances that are provisioned under IBM Cloud on an IBM Cloud network can use resource records that are configured through IBM Cloud DNS Services by querying DNS Services resolvers.

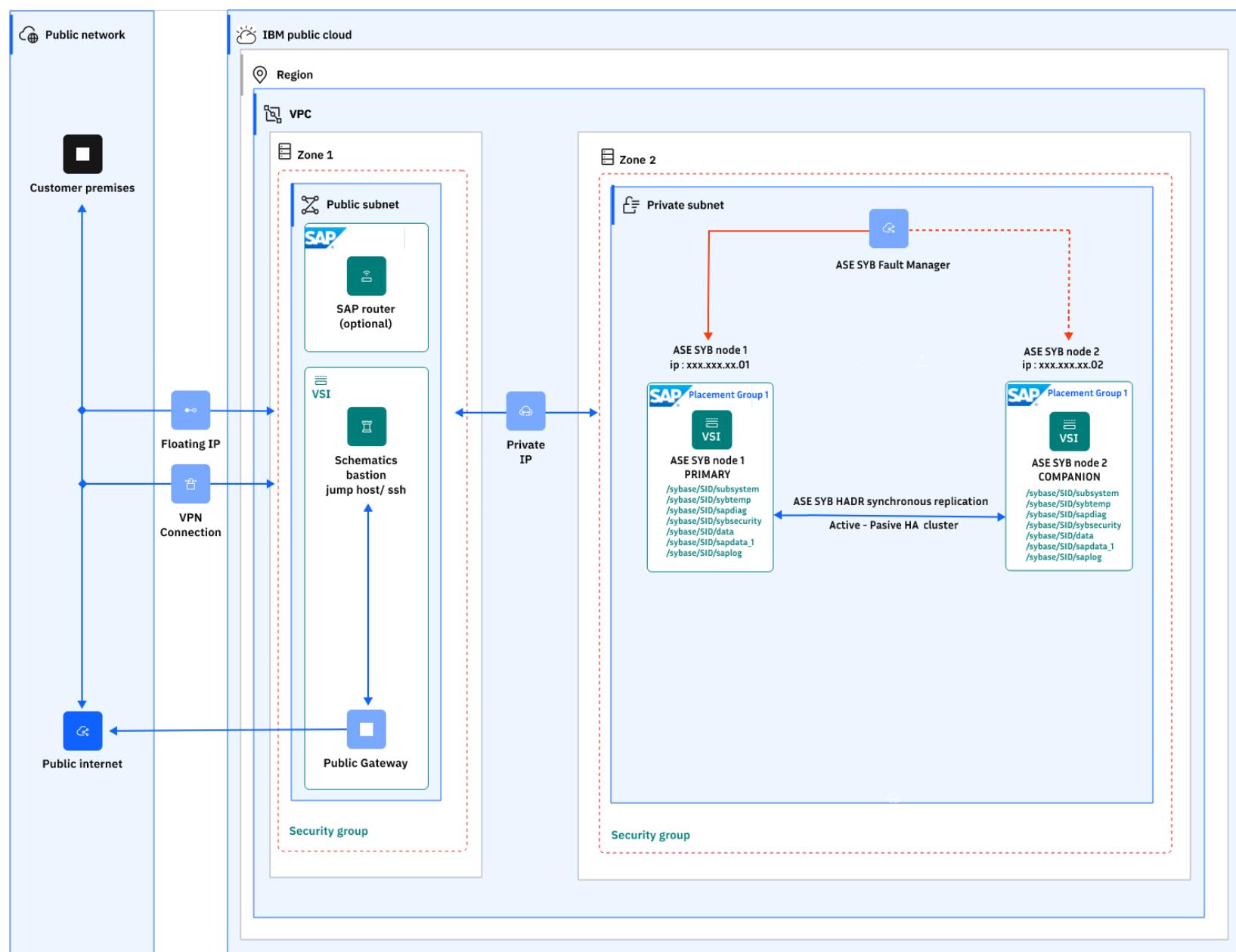
Resource records and zones that are configured through DNS Services are:

- Separated from the wider public DNS, and their publicly accessible records.
- Hidden from the system outside of and not part of the IBM Cloud private network.
- Accessible only from the system that you authorize on the IBM Cloud private network.
- Resolvable only via the resolvers provided by the service.

The DNS service maps the FQDN of each ALB to the virtual hostnames of the ASCS, ERS, and ASE Sybase that are used by SAP applications.

Type	Name	Value	TTL
CNAME	dbpochana	is an alias of 20bdd130-eu-de.lb.appdomain.cloud	12 hr
CNAME	sappocers	is an alias of 3941d983-eu-de.lb.appdomain.cloud	12 hr
CNAME	sappocases	is an alias of 56a9190d-eu-de.lb.appdomain.cloud	12 hr

Highly available system for SAP ASE Sybase database with HADR system



SAP HA for ASE Sybase DB instances cluster nodes primary (Active) and Secondary (Companion)

At the most basic level, a standard HA ASE Sybase cluster in an active(primary)-passive(companion) configuration has two nodes: one is the primary node and the other is the standby node. This means that the primary node is actively serving the active SAP DB instances (Primary and Companion), while the standby node is waiting to jump in if there is any failure.

The cluster is set with a virtual hostname IP (hostname is mapped to the FQDN of the ASE Sybase ALB through DNS, which is the same as

explained previously for SAP ASCS and ERS instances). Application instances (PAS and AAS) are used on the SAP profiles to call that particular component. The cluster assigns the virtual IP to the active node and uses a heartbeat monitor to confirm the availability of the components. If the primary node stops responding, it triggers the automatic failover mechanism that calls the standby node to step up to become the primary node. The ALB detects the change, redirects the traffic to the new active node, and assigns the virtual IP to it, restoring the component availability. Once fixed, the failed node comes online as a standby node.

SAP Sybase HADR system supports synchronous replication

The SAP Sybase HADR system supports synchronous replication between the primary and standby servers for high availability. An active-active setup is a two-node configuration where both nodes in the cluster include SAP ASE managing independent workloads, capable of taking over each others workload in the event of a failure.

The SAP ASE server that takes over the workload is called a secondary companion, and the SAP ASE server that fails is called the primary companion. Together they are companion servers. This movement from one node to another is called failover. After the primary companion is ready to resume its workload, it is moved back to its original node. This movement is called a failback.

When a system fails over, clients that are connected to the primary companion and use the failover property automatically reestablish their network connections to the secondary companion. You must tune your operating system to successfully manage both servers during fail over. See your operating system documentation for information about configuring your system for high availability. An SAP ASE configured for failover in an active-active setup can be shut down using the shutdown command only after you have suspended SAP ASE from the companion configuration, at both the server level and the platform level.

The always-on option in a High Availability and Disaster Recovery (HADR) system consists of two SAP ASE servers:

- Primary on which all transaction processing takes place.
- Warm standby (referred to as a "standby server" in DR mode, and as a "companion" in HA mode) for the primary server, and contains copies of designated databases from the primary server.



Note: The HADR feature that is shipped with SAP ASE version 16.0 SP02 supports only a single-companion server.

Some high-availability solutions (for example, the SAP Adaptive Server Enterprise Cluster Edition) share or use common resources between nodes. However, the HADR system is a "shared nothing" configuration, each node has separate resources including disks.

In an HADR system, servers are separate entities and data is replicated from the primary server to the companion server. If the primary server fails, a companion server is promoted to the role of primary server either manually or automatically. Once the promotion is complete, clients can reconnect to the new primary server, and see all committed data, including data that was committed on the previous primary server.

Servers can be separated geographically, which makes an HADR system capable of withstanding the loss of an entire computing facility.



Note: The HADR system includes an embedded SAP Replication Server, which synchronizes the databases between the primary and companion servers. SAP ASE uses the Replication Management Agent (RMA) to communicate with Replication Server and SAP Replication Server uses Open Client connectivity to communicate with the companion SAP ASE.

The Replication Agent detects any data changes made on the primary server and sends them to the primary SAP Replication Server. In the figure above, the unidirectional arrows indicate that, although both SAP Replication Servers are configured, only one direction is enabled at a time.

The HADR system supports synchronous replication between the primary and standby servers for high availability so the two servers can keep in sync with Zero Data Loss (ZDL). This requires a network link that is fast enough between the primary and standby server so that synchronous replication can keep up with the primary servers workload. Generally, this means that the network latency is approximately the same speed as the local disk IO speed, a few (fewer than 10) milliseconds. Anything longer than a few milliseconds may result in a slower response to write operations at the primary.

The HADR system supports asynchronous replication between the primary and standby servers for disaster recovery. The primary and standby servers by using asynchronous replication can be geographically distant, meaning they can have a slower network link. With asynchronous replication, Replication Agent Thread captures the primary servers workload, which is delivered asynchronously to SAP Replication Server. The SAP Replication Server applies these workload change to the companion server.

The most fundamental service that is offered by the HADR system is the failover; planned or unplanned from the primary to the companion server, which allows maintenance activity to occur on the old primary server, while applications continue on the new primary.

The HADR system provides protection in the event of a disaster. If the primary server is lost, the companion server can be used as a replacement. Client applications can switch to the companion server, and the companion server is quickly available for users. If the SAP Replication Server was in synchronous mode before the failure of the primary server, the Fault Manager automatically initiates failover with

zero data loss.

Fault Manager installation on the SAP ASCS node

The required parameters are asked during the installation process to create a profile for the fault manager and then adds it to the instance start profile. It is also possible to run the installation by using an existing profile: `sybdbfm install pf=<SYBHA.PFL>` In this case, the installation process will only ask for profile parameters missing in the profile.



Note: Fault manger is integrated with ASCS on same SAP PAS/AAS cluster (start/stop/move together).

There may be some data loss if the SAP Replication Server was in asynchronous mode and you must use manual intervention to failover for disaster recovery.

Connection attempts to the companion server without the necessary privileges are silently redirected to the primary companion via the login redirection mechanism, which is supported by Connectivity libraries. If login redirection is not enabled, client connections fail and are disconnected.

The SAP ASE HADR option installs the below components:

- SAP ASE
- SAP Replication Server
- Replication Management Agent (RMA)
- SAP Host Agent
- Fault Manager
- SAP ASE Cockpit



Note: This automation is offered at no cost; however, the provisioned infrastructure comes at cost.

VPC with Additional Application Server (AAS) ABAP on Linux for SAP HANA

You can use Terraform scripts to create a single-tier VPC and create the AAS to HANA and AnyDB infrastructure on the VPC. The Terraform scripts use the VPC information that you provide and then call the Ansible playbook to create the SAP architecture on the specified VPC. Terraform on IBM Cloud® enables predictable and consistent provisioning of IBM Cloud Virtual Private Cloud (VPC) infrastructure resources so that you can rapidly build complex, cloud environments. IBM Cloud VPC infrastructure consists of SAP certified hardware that uses Intel® Xeon CPUs and more Intel® technologies.

You have two deployment methods to choose from:

- Terraform scripts that run from the CLI on your bastion server.
- Schematics user interface accessed from your cloud dashboard menu.

You can create SAP AAS NetWeaver 7.x on the SAP HANA-based ABAP stack.

SAP solution implemented

Many SAP enterprise solutions are built on the SAP platform (SAP NetWeaver) including:

- SAP HANA as Primary Persistence for SAP NetWeaver-based applications
- SAP Business Suite applications (ERP, CRM, and SCM, and other applications),
- SAP Business Warehouse (BW), and
- Other SAP enterprise solutions

SAP NetWeaver has two distinct aspects, ABAP and Java. Many applications that are built on the SAP NetWeaver's ABAP or Java (or both) application servers run on SAP DB owned HANA and ASE Sybase either in AnyDB platforms (MSSQL, Oracle, and Db2).

Technical interfaces are available for applications that are built on the SAP NetWeaver AS ABAP and AS Java to run on SAP HANA and AnyDB. However, specific development enablement is normally required for each application to ensure that it runs optimally on the SAP HANA. SAP Business Suite applications (ERP, CRM, SCM, and other applications), SAP Business Warehouse (BW), and other SAP NetWeaver-based applications were modified to run on SAP HANA and have many advantages. Also, various components and complimentary applications that are built on SAP NetWeaver can also run on SAP HANA or AnyDB by using the provided SAP NetWeaver DB interfaces.

The SAP HANA as primary persistence for SAP NetWeaver-based applications scenario has one restriction: SAP NetWeaver ABAP and Java

application servers must run on separate hardware servers from the SAP HANA hardware.

What is created

The scripts automate the virtual infrastructure resources, provisioning the processes for the SAP architecture in an existing VPC with a distributed environment. SAP AAS NetWeaver 7.x (HANA or ASE SYB) application server on a distinct VSI VPC system and SAP HANA DB on a dedicated server type VSI VPC box are provisioned. The scripts work in two phases.

During the first phase of [Automate SAP bastion server – SAP media storage repository](#), the following virtual infrastructure resources based on the components from the existing VPC created by the bastion server are:

- 1 VPC where the virtual server instance is provisioned.
- 1 security group. The rules for this security group are:
 - Allow inbound DNS traffic (port 53).
 - Allow inbound SSH traffic (TCP port 22).
 - Allow all outbound traffic from the virtual server instance.
 - Allow all traffic in the security group.
- 1 subnet to enable the networking in your VPC.
- 2 virtual server instances with SAP certified storage and network configurations.
- 1 floating IP address used to access your VPC virtual server instance over the public network.

During the second phase, the Ansible Playbooks is called and the SAP architecture is installed for both dedicated virtual server instance (VSI) SAP application; VSI system and dedicated SAP HANA VSI box. The SAP architecture that is deployed on the SAP NetWeaver 7.x release is a stand-alone dedicated SAP HANA 2.0 box release. For more information about this architecture, see [Automating SAP HANA stand-alone virtual server instance on IBM Cloud® VPC by using Terraform and Ansible](#).

You can provision only one instance of the service per IBM Cloud region.

Schematics deployment

When you run the scripts with the Schematics interface, you:

- Enter the workspace information.
- Enter the GitHub path for the chosen solution either on NetWeaver AAS for HANA.
- Modify the parameters in the Schematics interface. They are the same parameters as the `input.auto.tfvars` file that you use with the cli.

Virtual server instance configuration

Following are the supported operating system images for SAP NetWeaver primary application server:

- ibm-redhat-8-4-amd64-sap-applications-2
- ibm-redhat-8-6-amd64-sap-applications-2
- ibm-sles-15-3-amd64-sap-applications-2
- ibm-sles-15-4-amd64-sap-applications-3

Following are the supported operating system images for SAP HANA database:

- ibm-redhat-8-4-amd64-sap-hana-2
- ibm-redhat-8-6-amd64-sap-hana-2
- ibm-sles-15-3-amd64-sap-hana-2
- ibm-sles-15-4-amd64-sap-hana-1

For both server instances there are:

- Two SSH keys are configured to access SSH as `root`.
- Three storage volumes as described in the `input.auto.tfvars` file.

What is created for anydb

The scripts use the information that you provide for an existing VPC and deploy AAS to SAP HANA or AnyDB on a different host than CI (SAP Central Instance) VSI host. For more information about this architecture, see [SAP NetWeaver 7.x on UNIX with HANA or AnyDB on IBM Cloud](#)

[VPC on IBM Cloud VPC](#). You specify the information for the VPC to use in the `input.auto.tfvars` file.

The scripts call the Ansible Playbooks to install the SAP architecture.

Script files

The configuration and script files are provided on GitHub. Each supported interface for the SAP solution installation has its own folder in the GitHub repository:

- [GitHub repository for Terraform – AAS HANA](#)

Terraform interface

To run the Terraform script, you modify:

- The `input.auto.tfvars` file to specify the existing VPC resources for your solution. Specify the variables for the existing VPC:
 - VPC name
 - Security group
 - Subnet
 - Hostname
 - Profile
 - Image
 - Up to two SSH keys

You can change the default SAP system configuration settings to match your solution. You can also specify the location where you downloaded the SAP kits.

The IBM Cloud Provider plug-in for Terraform on IBM Cloud uses these configuration files to install AAS to SAP HANA and AnyDB on the specified VPC in your IBM Cloud account.

Support

There are no warranties of any kind, and there is no service or technical support available for these materials from IBM®. As a recommended practice, review carefully any materials that you download from this site before using them on a live system.

Though the materials provided herein are not supported by the IBM® Service organization, your comments are welcomed by the developers, who reserve the right to revise, readapt or remove the materials at any time. To report a problem, or provide suggestions or comments, open a GitHub issue.

Before you begin

Before you use the scripts in the bastion cli:

- Set up your account to access the VPC. Make sure that your account is [upgraded to a paid account](#).
- If you have not already, create a Bastion server to store the SAP kits. For more information, see [Automate SAP bastion server - SAP media storage repository](#).
- Download the SAP kits from the SAP Portal to your Deployment Server. Make note of the download locations. Ansible decompresses the files. For more information, see the [readme](#) file.
- [Create or retrieve an IBM Cloud API key](#). The API key is used to authenticate with the IBM Cloud platform and to determine your permissions for IBM Cloud services.
- [Create or retrieve your SSH key ID](#). You need the 40-digit UUID for the SSH key, not the SSH key name.
- Terraform should already be installed on the bastion server that you deployed. For more information, see [Bastion server for SAP deployment](#).
- (Optional - Catalog Tile) create secrets for your credentials and passwords by using the [Secrets Manager](#).

Deploying SAP AAS NetWeaver 7.x on HANA by using the Schematics user interface

Use these steps to configure the SAP Additional Application Server (AAS) NetWeaver with HANA or AnyDB on your existing VPC by using the Schematics interface. The script takes 2 - 3 hours to complete.

1. From the IBM Cloud menu, select **Schematics**.
2. Click **Create** workspace.

3. On the **Specify template** page:
 - Enter the URL for the Schematics interface.
 - Select the **Terraform version** that is listed in the readme file.
 - Click **Next**.
4. On the **workspace details** page:
 - Enter a name for the workspace.
 - Select a **Resource group**.
 - Select a **Location** for your workspace. The workspace location does not have to match the resource location.
 - Select **Next**.
5. Select **Create** to create your workspace.
6. On the workspace settings page, in the input variables section, review the default input variables and provide values that match your solution.
 For a more detailed description of each parameter, check the GitHub repo [AAS HANA readme](#) file, chapter "Input parameter file". Also, make sure to mark the parameters that contain sensitive information like passwords, API, and ssh private keys as "sensitive". These parameters are marked as "sensitive" in the readme file, under "Input parameter file".
7. On the workspace settings page, click **Generate plan**. Wait for the plan to complete.
8. Click **View log** to review the log files of your terraform execution plan.
9. Apply your Terraform template by clicking **Apply plan**.
10. Review the log file to ensure that no errors occur during the provisioning, modification, or deletion process.

Deploying SAP AAS NetWeaver (ABAP) on HANA with the Deployable Architecture tile interface

Use these steps to configure the SAP AAS NetWeaver (ABAP) on HANA on your existing VPC by using the catalog tile interface. The script takes 2 - 3 hours to complete.

1. From the IBM Cloud catalog, select **VPC with Additional Application Server ABAP on Linux for SAP HANA** on HANA tile. The **Create** tab opens for VPC with Additional Application Server ABAP on Linux for SAP HANA. For more information about this deployment, see the About tab or the readme file link.
2. Select the latest version.
3. Select **VPC with Additional Application Server ABAP on Linux for SAP HANA on Deployable Architecture tile** variation.
4. Click **Review deployment** options:
 - **Add to project** to add this deployment to an IBM Cloud project and combine it with other deployments. IBM Cloud projects include several more pipeline steps before deployment, including deployment validation, cost calculation, compliance verification, and approval process.
 - **Create from the CLI** to get the CLI command. With this command you can trigger the deployment from the CLI.
 - **Work with code** to embed the code into other terraform deployments.
 - **Deploy with IBM Cloud Schematics** to trigger the deployment process directly.
5. Select **Deploy with IBM Cloud Schematics**.
6. Add the input parameters for this installation. There are 3 categories of parameters:
 - **Workspace** - These parameters define the workspace that is automatically created in Schematics:
 - Enter a name for the workspace or use the default name.
 - The Resource Group used to create resources. Use default or create a Resource Group.
 - Select a location to create your Schematics workspace. The workspace location need not match the resource location.
 - **Required input variables** - Review the default input variables and provide values that match your solution. These parameters are specific to your deployment. For more detailed information, see the [Readme file](#).

Parameter	Description
BASTION_FLOATING_IP	Required only for Schematics Deployments. The Floating IP from the Bastion Server.

HOSTNAME	The hostname for the VSI. The hostname should be up to 13 characters as required by SAP. For more information on the rules regarding hostnames for SAP systems, check SAP Note 611361: Hostnames of SAP ABAP Platform servers
REGION	The cloud region to deploy the solution. The regions and zones for VPC are listed here . Review supported locations in IBM Cloud Schematics here . Sample value: eu-de.
RESOURCE_GROUP	The name of an existing Resource Group for VSIs and Volumes resources. Default value: "Default". The list of Resource Groups is available here .
SECURITY_GROUP	The name of an existing Security group. The list of security groups is available here .
SSH_KEYS	The list of SSH Keys UUIDs that are allowed to SSH as root to the VSI can contain one or more IDs. The list of SSH Keys is available here . Sample input (use your own SSH UUIDs from IBM Cloud){: external}: ["r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a", "r010-3fcfd9fe7-d4a7-41ce-8bb3-d96e936b2c7e"]
SUBNET	The name of an existing subnet. The list of subnets is available here .
VPC	The name of an existing VPC. The list of VPCs is available here .
ZONE	The cloud zone where to deploy the solution. Sample value: eu-de-2.
ibmcloud_api_key	IBM Cloud API key (Sensitive* value).
private_ssh_key	Required only for Schematics Deployments - Input your id_rsa private key pair content in OpenSSH format (Sensitive* value). This private key should be used only during the terraform provisioning and it is recommended to be changed after the SAP deployment.
hdb_instance_number	The instance number of the SAP HANA database server.
sap_aas_instance_number	Technical identifier for the internal processes of the additional application server.
sap_ascs_instance_number	Technical identifier for the internal processes of ASCS.
sap_ci_host	IP address of the existing SAP Central Instance.
sap_ci_hostname	The hostname of the existing SAP Central Instance.
sap_ci_instance_number	Technical identifier for the internal processes of the Central Instance.
sap_sid	The SAP system ID identifies the entire SAP system.
sap_main_password	Common password for all users that are created during the installation (See Obs*).

Required Variables

- **Optional variables** - Review and update the optional input variables. The Ansible scripts expect the SAP kits to be in the default locations listed. For more information, see the [Readme file - Input Parameters](#).

Parameter	Description
ID_RSA_FILE_PATH	The file path for private_ssh_key is automatically generated by default. If it is changed, it must contain the relative path from Git repo folders. Default value: "ansible/id_rsa".
IMAGE	The OS image used for the VSI. A list of images is available here .
PROFILE	The profile used for the VSI. A list of profiles is available here . For more information about supported DB/OS and IBM Gen 2 Virtual Server Instances (VSI), check SAP Note 2927211: SAP Applications on IBM Virtual Private Cloud .

VOL1	Volume 1 Size - The size for the disks in GB that are to be attached to the VSI and used by SAP.
VOL2	Volume 2 Size - The size for the disks in GB that are to be attached to the VSI and used by SAP.
kit_sapcar_file	Path to the sapcar binary, as downloaded from SAP Support Portal.
kit_swpm_file	Path to the SWPM archive (SAR), as downloaded from SAP Support Portal.
kit_saphostagent_file	Path to the SAP Host Agent archive (SAR), as downloaded from SAP Support Portal.
kit_hdbclient_file	Path to the HANA DB client archive (SAR), as downloaded from SAP Support Portal.

Optional Variables

7. Accept the license agreement.
8. Select **Deploy**. The deployment starts and you are directed to the Schematics page that displays the script log files for you to monitor the deployment progress.

Creating the infrastructure using Terraform with the bastion server CLI

Use these steps to configure the IBM Cloud Provider plug-in and use Terraform to install SAP AAS to SAP HANA and AnyDB on your existing VPC on an already deployed SAP NetWeaver 7.X with SAP HANA 2.0 or ASE SYB as a Central Instance.

The script takes 1 - 2 hours to complete.

1. Access the bastion server cli.
2. Clone the solution repository and change to the folder.

ASE SYB 16 Clone the solution repository from <https://github.com/IBM-Cloud/sap-aas-abap-ase-syb> and cd to the sap-aas-abap-ase-syb/cli folder.

```
$ git clone https://github.com/IBM-Cloud/sap-aas-abap-ase-syb
cd sap-aas-abap-ase-syb/cli/
```

SAP HANA 2.0: Clone the solution repository from <https://github.com/IBM-Cloud/sap-abap-hana-aas> and cd to the sap-abap-hana-aas folder.

```
$ git clone https://github.com/IBM-Cloud/sap-abap-hana-aas.git
cd sap-abap-hana-aas/
```

3. Modify the `input.auto.tfvars` file to specify the information for the existing VPC, your region, zone, networking component names, hostname for the AAS VSI,profile, and image. You need your 40-digit SSH key ID for this file. The second SSH key is optional. For more options for profile, see [Instance Profiles](#). For more options, see [Images](#). For descriptions of the variables, see the [readme](#) file.

The VSI OS images that are supported for this solution for Netweaver Additional Application Server are:

- ibm-redhat-8-4-amd64-sap-applications-2
- ibm-redhat-8-6-amd64-sap-applications-2
- ibm-sles-15-3-amd64-sap-applications-2
- ibm-sles-15-4-amd64-sap-applications-4

```
$ # Infra VPC variables for ASE SYB
REGION    = "eu-de"
ZONE      = "eu-de-2"
VPC       = "ic4sap"                      # EXISTING Security group name
SECURITY_GROUP = "ic4sap-securitygroup"     # EXISTING Security group name
RESOURCE_GROUP = "wes-automation"
SUBNET    = "ic4sap-subnet"                 # EXISTING Subnet name
SSH_KEYS   = [ "r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a" , "r010-3fcfd9fe7-d4a7-41ce-8bb3-
d96e936b2c7e" ]

# SAP AAS VSI variables:
```

```

HOSTNAME = "sapnwase-as01"
PROFILE = "bx2-4x16"
IMAGE = "ibm-redhat-8-4-amd64-sap-applications-2

$ # Infra VPC variables for ABAP HANA
REGION      = "eu-de"
ZONE        = "eu-de-2"
VPC          = "ic4sap" # EXISTING Security group name
SECURITY_GROUP = "ic4sap-securitygroup" # EXISTING Security group name
RESOURCE_GROUP = "wes-automation"
SUBNET       = "ic4sap-subnet" # EXISTING Subnet name
SSH_KEYS     = [ "r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a" , "r010-3fc9fe7-d4a7-41ce-8bb3-d96e936b2c7e" ]
ID_RSA_FILE_PATH = "ansible/id_rsa"

# SAP AAS variables:
HOSTNAME = "sapnwapp"
PROFILE = "bx2-4x16"
IMAGE = "ibm-redhat-8-6-amd64-sap-applications-2"

```

4. Customize your SAP system configuration. In the same file, input.auto.tfvars, edit the SAP system configuration variables that are passed to the Ansible automated deployment. For descriptions of the variables, see the [readme](#) file.

```

$ # SAP system configuration - for ASE SYB
sap_sid = "NWD"
sap_ci_host = "10.243.132.10"
sap_ci_hostname = "sapnwase"
sap_ci_instance_number = "00"
sap_asc_s_instance_number = "01"
sap_aas_instance_number = "00"

# Kits paths
kit_sapcar_file = "/storage/NW75SYB/SAPCAR_1010-70006178.EXE"
kit_swpm_file = "/storage/NW75SYB/SWPM10SP31_7-20009701.SAR"
kit_saphotagent_file = "/storage/NW75SYB/SAPHOSTAGENT51_51-20009394.SAR"

```

```

$ # SAP system configuration - for ABAP HANA
sap_sid = "NWD"
sap_ci_host = "10.243.132.10"
sap_ci_hostname = "sapnwapp01"
sap_ci_instance_number = "00"
sap_asc_s_instance_number = "01"
hdb_instance_number = "00"
sap_aas_instance_number = "00"

# Kits paths
kit_sapcar_file = "/storage/NW75HDB/SAPCAR_1010-70006178.EXE"
kit_swpm_file = "/storage/NW75HDB/SWPM10SP31_7-20009701.SAR"
kit_saphotagent_file = "/storage/NW75HDB/SAPHOSTAGENT51_51-20009394.SAR"
kit_hdbclient_file = "/storage/NW75HDB/IMDB_CLIENT20_009_28-80002082.SAR"

```

Ansible decompresses the rest of the SAP kit files. For more information, see the [readme](#) file.

5. Initialize the Terraform CLI.

```
terraform init
```

6. Create a Terraform execution plan. The Terraform execution plan summarizes all the actions that are done to create the virtual private cloud instance in your account.

```
terraform plan plan1
```

Enter an SAP main password and your API key.

The SAP main password must be 10 - 14 characters long and contain at least one digit (0-9). It can contain only the following characters: a-z, A-Z, 0-9, @, #, \$, . *This password cannot contain exclamation points '!'. The password must not start with a digit or an underscore ().*

7. Verify that the plan shows all of the resources that you want to create and that the names and values are correct. If the plan needs to be adjusted, edit the input.auto.tfvars file to correct resources and run terraform plan again.
8. Apply the saved plan.

```
$ terraform apply "plan1"
```

The virtual private cloud and components are created and you see output similar to the `terraform plan` output.

9. Add the SAP credentials and the virtual server instance IP to the SAP GUI. For more information about the SAP GUI, see [SAP GUI](#).

Next steps

If you need to rename your resources after they are created, modify the input.auto.tfvars file to change the names and run `terraform plan` and `terraform apply` again. Do not use the IBM Cloud Dashboard and user interface to modify your VPC after it is created. The Terraform scripts create a complete solution and selectively modifying resources with the user interface might cause unexpected results.

If you need to remove the SAP Netweaver 7.X on HANA or AnyDB installation, go to your project folder and run `terraform destroy`. The `terraform destroy` command does not remove the VPC in this scenario because the VPC was created before these Terraform scripts were run.

Related information

For more information about Terraform on IBM Cloud, see [Getting started with Terraform on IBM Cloud](#).

For more information about using Terraform for creating only a VPC for SAP, without the SAP architecture, see [Creating single-tier virtual private cloud for SAP by using Terraform](#).

SAP One Support Notes that apply to this document:

- [SAP Note 84555 - Windows Server, Linux®, and UNIX: Certified hardware](#)
- [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#)
- [SAP Note 2923773 - Linux® on IBM Cloud \(IaaS\): Adaption of your SAP license](#)
- [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#)
- [SAP Note 2369910 - SAP Software on Linux®: General information](#)
- [SAP Note 171380 - Released IBM hardware \(Intel processors\) and IBM cloud services offers](#)
- [SAP Note 1380654 - SAP support in IaaS environments](#)

This document is referenced by:

- [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#)
- [SAP Note 2588225 - SAP on IBM Cloud: Protect against speculative execution vulnerabilities](#)
- [SAP Note 1380654 - SAP support in IaaS environments](#)
- [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#)

SAP S/4HANA workload deployment in VPC

Automating SAP workload HA deployment on IBM Cloud VPC with Terraform and Ansible

You can use Terraform to automate IBM Cloud® VPC provisioning. The VPC provisioned includes virtual server instances with high network performance. The VPC infrastructure contains various Infrastructure-as-a-Service (IaaS) offerings, including virtual servers. After the VPC is provisioned, the scripts use the Ansible Playbooks to install the SAP system.

IBM Cloud VPC introduction

VPC is a public cloud offering that an enterprise uses to establish its own private cloud-like computing environment on shared [public cloud](#) infrastructure. VPC gives an enterprise the ability to define and control a virtual network that is logically isolated from all other public cloud tenants, creating a private and secure place on the public cloud.

Imagine that a cloud provider's infrastructure is a residential apartment building and multiple families live inside. A public cloud tenant is a kind of sharing an apartment with a few roommates. In contrast, having a VPC is like having your own private condominium; no one else has the key, and no one can enter the space without your permission.

VPC's logical isolation is implemented by using virtual network functions and security features that give the enterprise customer granular control over which IP addresses or applications can access particular resources. It is analogous to the "friends-only" or "public/private" controls on social media accounts used to restrict who can or can't see your otherwise public posts.

With IBM Cloud VPC, you can use the UI, CLI, and API to manually provision virtual server instances for VPC with high network performance. VPC infrastructure contains various Infrastructure-as-a-Service (IaaS) offerings including virtual servers for VPC.

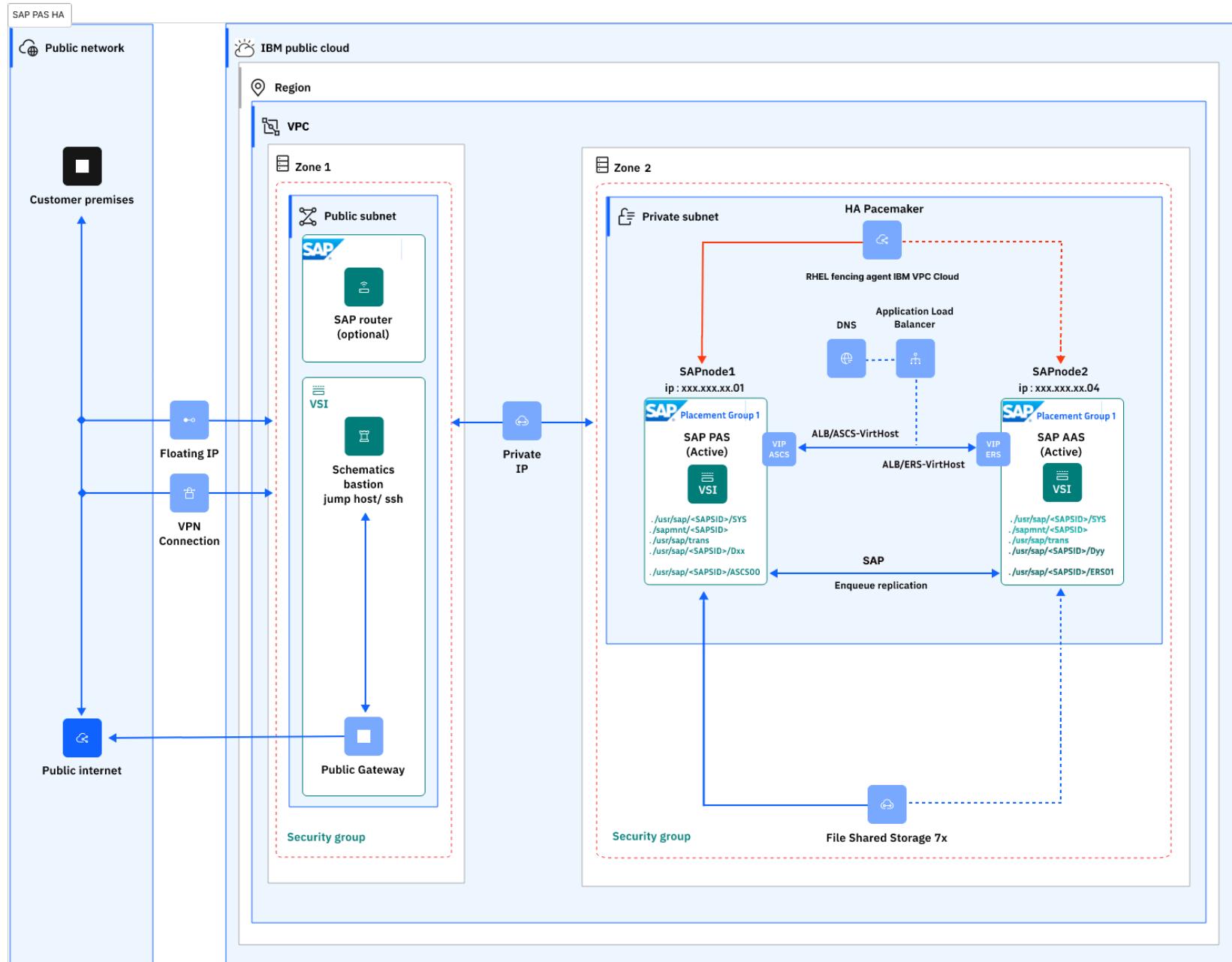
Use the following information to understand a simple use-case for planning, creating, and configuring resources for your VPC, and learn more about VPC overviews and VPC tutorials. For more information about the VPC, see [Getting started with Virtual Private Cloud \(VPC\)](#).

SAP products architecture on IBM Cloud VPC

A [Virtual Private Cloud \(VPC\)](#) contains one of the most secure and reliable cloud environments for SAP applications within your own VPC with virtual server instances. This represents an Infrastructure-as-a-Service (IaaS){: external} within IBM Cloud that offers all the benefits of isolated, secure, and flexible virtual cloud infrastructure from IBM. In comparison, the IBM Cloud classic infrastructure virtual servers offering uses virtual instances with native and VLAN networking to communicate with each other within a data center; however, the instances are restricted in one well-working pod by using subnet and VLAN networking as a gap scale up of virtual resources should rely between the pods. The IBM Cloud VPC network orchestrator layer concept eliminates the pod boundaries and restrictions, so this new concept handles all the networking for every virtual instance running within VPC across regions and zones.

Highly available system for SAP NetWeaver on IBM Cloud VPC

In a Highly Available (HA) system, every instance can run on a separate IBM Cloud virtual server instance. The cluster HA configuration for the SAP application server consists of two virtual server instances, each of them located in the same zone within the region by using placement groups. Placement groups assure that both cluster resources and cloud resources are also located in different compute nodes as specified in the following placement groups section:



SAP HA for SAP applications cluster nodes PAS (Active) and AAS (Active)

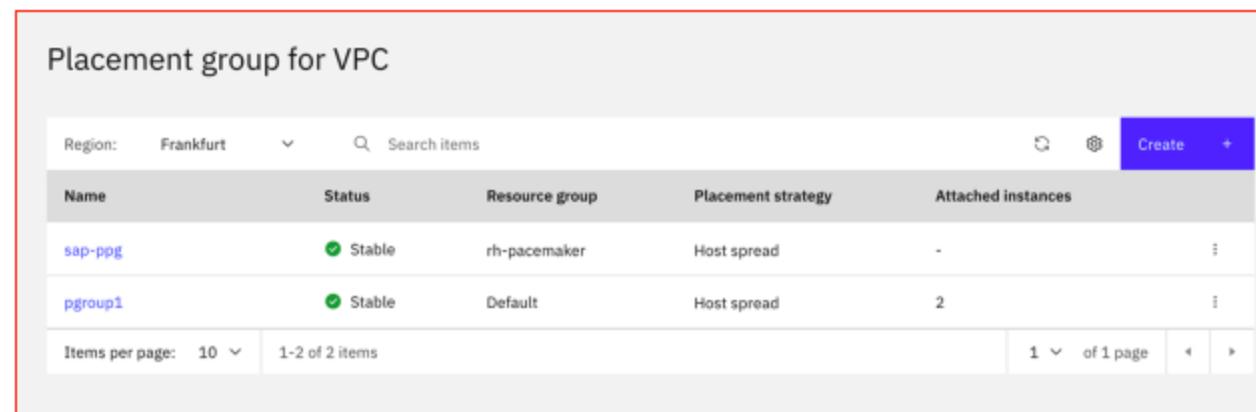
Placement groups on IBM Cloud VPC for SAP HA architecture

Placement Groups (PG) for VPC have two different anti-affinity strategies for high availability. By using the placement strategies, you minimize the chance of service disruption with virtual server instances that are placed on different hosts or into an infrastructure with separate power and network supplies.

The design of placement groups for IBM Cloud virtual servers solves this issue. Placement groups give a measure of control over the host on which a new public virtual server is placed. In this release, a “spread” rule is implemented, which means that the virtual servers within a placement group are spread onto different hosts. You can build a highly available application within a data center and know that your virtual servers are isolated from each other.

Placement groups with the spread rule are available to create in selected IBM Cloud data centers. After a spread rule is created, you can provision a virtual server into that group and ensure that it is not on the same host as any of your other virtual servers. This feature comes with no cost.

You can create your placement group and assign up to four new virtual server instances. With the spread rule, each of your virtual servers are provisioned on different physical hosts. In the following configuration example, the “Power Spread” option is used:



Placement groups host spread

Placement group for VPC					
Name	Status	Resource group	Placement strategy	Attached instances	
sapha-poc	Stable	wes-ic4sap-resourcegroup	Power spread	4	
Items per page: 10 1 item 1 of 1 page					

Placement groups power spread

Following are the SAP instances that are required for HA scenario:

- ABAP SAP Central Services (ASCS) instance - contains the ABAP message server and the ABAP enqueue server.
- Enqueue Replication Server (ERS) instance for the ASCS instance.
- Database instance
- Primary Application Server (PAS) instance on node 1.
- Additional Application Server (AAS) instance on node 2.



Note: It is recommended to run both the ASCS instance and the ERS instance in a switchover cluster infrastructure.

IBM Cloud File Storage for VPC for SAP HA architecture

[IBM Cloud File Storage for VPC](#) technology is used to make the SAP directories available to the SAP system. The technologies of choice are NFS, shared disks, and cluster file system. If you have decided to use the HA solution for your SAP system, make sure that you properly address the HA requirements of the SAP file systems in your SAP environment.

File shares for VPC								
Name	Status	Resource groups	Location	Mount targets	Size	Replication role	Encryption type	
usrsap-as1-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-as2-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-sapsacs-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-sapers-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-sapmnt-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-sapsys-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-trans-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	80 GB	None	Provider managed	

File shares for VPC

- File shares that are mounted as NFS permanent file systems on both cluster nodes for SAP HA application:
 - `/usr/sap/<SAPSID>/SYS`
 - `/sapmnt<SAPSID>`
 - `/usr/sap/trans`
- Cluster-managed file systems for SAP HA application: ASCS
 - `/usr/sap/<SAPSID>/ASCS00`
 - `/usr/sap/<SAPSID>/ERS01`
- Permanent NFS mount on SAP HA application node 1 PAS instance:
 - `/usr/sap/<SAPSID>/Dxx`
- Permanent NFS mount on SAP HA application node 2 dialog instance:
 - `/usr/sap/<SAPSID>/Dyy`

Prerequisites

You need to install the hardware (hosts, disks, and network) and decide how to distribute the database, SAP instances, and if required, the Network File System (NFS) server over the cluster nodes.

Context

Following are the types of SAP directories:

- Physically shared directories: `/<sapmnt>/<SAPSID>` and `/usr/sap/trans`

- Logically shared directories that are bound to a node, such as `/usr/sap`, with the following local directories:
 - `/usr/sap/<SAPSID>`
 - `/usr/sap/<SAPSID>/SYS`
 - `/usr/sap/hostctrl`
- Local directories that contain the SAP instances such as `/usr/sap/<SAPSID>/ASCS<Instance_Number>`
- The global transport directory may reside on a separate SAP transport host as a standard three systems transport layer configuration.

You need at least two nodes and a shared file system for distributed ASCS and ERS instances. The assumption is that the rest of the components are distributed on other nodes.

ASCS and ERS installation

In order for the ASCS and ERS instances to be able to move from one node to the other, they need to be installed on a shared file system and use virtual hostnames based on the virtual IP.

In this VPC-based SAP HA solution, the shared file system that is required by the cluster is replaced by the NFS-mounted file storage, and the virtual IP is replaced by the Application Load Balancer for VPC (ALB).

In this scenario, three ALBs are used, one for each Single Point of Failure (SPOF) component in order to replace the virtual IP requirement: ALB for ASCS, ALB for ERS, and ALB for ASE Sybase. Each ALB is configured as a backend for the corresponding cluster servers and redirects all of the communication that is received on the front-end ports to the active server in the backend pool.

Load balancers for VPC						
Region:	Frankfurt	▼	<input type="text"/> poc	X		
Name	Status	Family	Resource group	Type	Hostname	Location
db-alb-hana-poc	Active	Application	wes-ic4sap-resourcegroup	Private	20bdd130-eu-de.lb.appdomain.cloud	Frankfurt
sap-alb-ers-poc	Active	Application	wes-ic4sap-resourcegroup	Private	3941d983-eu-de.lb.appdomain.cloud	Frankfurt
sap-alb-ascs-poc	Active	Application	wes-ic4sap-resourcegroup	Private	56a9190d-eu-de.lb.appdomain.cloud	Frankfurt

Application load balancer management of HA IPs mechanism

Private application load balancer

A [private application load balancer](#) is accessible through your private subnets that you configured to create the load balancer.

Similar to a public application load balancer, your private application load balancer service instance is assigned an FQDN; however, this domain name is registered with one or more private IP addresses.

IBM Cloud operations change the number and value of your assigned private IP addresses over time, based on maintenance and scaling activities. The backend virtual server instances that host your application must run in the same region and under the same VPC.

Use the assigned ALB FQDN to send traffic to the private application load balancer to avoid connectivity problems to your applications during system maintenance or scaling down activities.

Each ALB sends traffic to the cluster node where the application (ASCS, ERS, ASE Sybase DB) is running. During the cluster failover, the ALB redirects all the traffic to the new node where the resources are up and running.



Note: DNS-as-a-Service (DNSaaS) is the management IBM Cloud VPC DNS service of HA and FQDN (IPs) mechanism.



Note: The ALB has a default of 50 seconds for client and server timeout, so after 50 seconds of inactivity, the connection is closed. To support SAP connections through ALB and not lose connection after 50 seconds, you need to request a change this value to a minimum of 300 seconds (client-side idle connection = minimum 300s and server-side idle connection = minimum 300s). To request this change, open a support ticket. This is an account-wide change that affects all of the ALBs in your account. For more information, see [Connection timeouts](#).

DNS Services with VPC

[IBM Cloud DNS Services](#) provide private DNS to VPC users. Private DNS zones are resolvable only on IBM Cloud and from explicitly [permitted networks](#) in an account. To get started, create a DNS Services instance by using the IBM Cloud console.

DNS Services allows you to:

- Create the private DNS zones that are collections for holding the domain names.
- Create the DNS resource records under these DNS zones.
- Specify the access controls used for the DNS resolution of resource records on a zone-wide level.

DNS Services also maintains its own worldwide set of DNS resolvers. Instances that are provisioned under IBM Cloud on an IBM Cloud network can use resource records that are configured through IBM Cloud DNS Services by querying DNS Services resolvers.

Resource records and zones that are configured through DNS Services are:

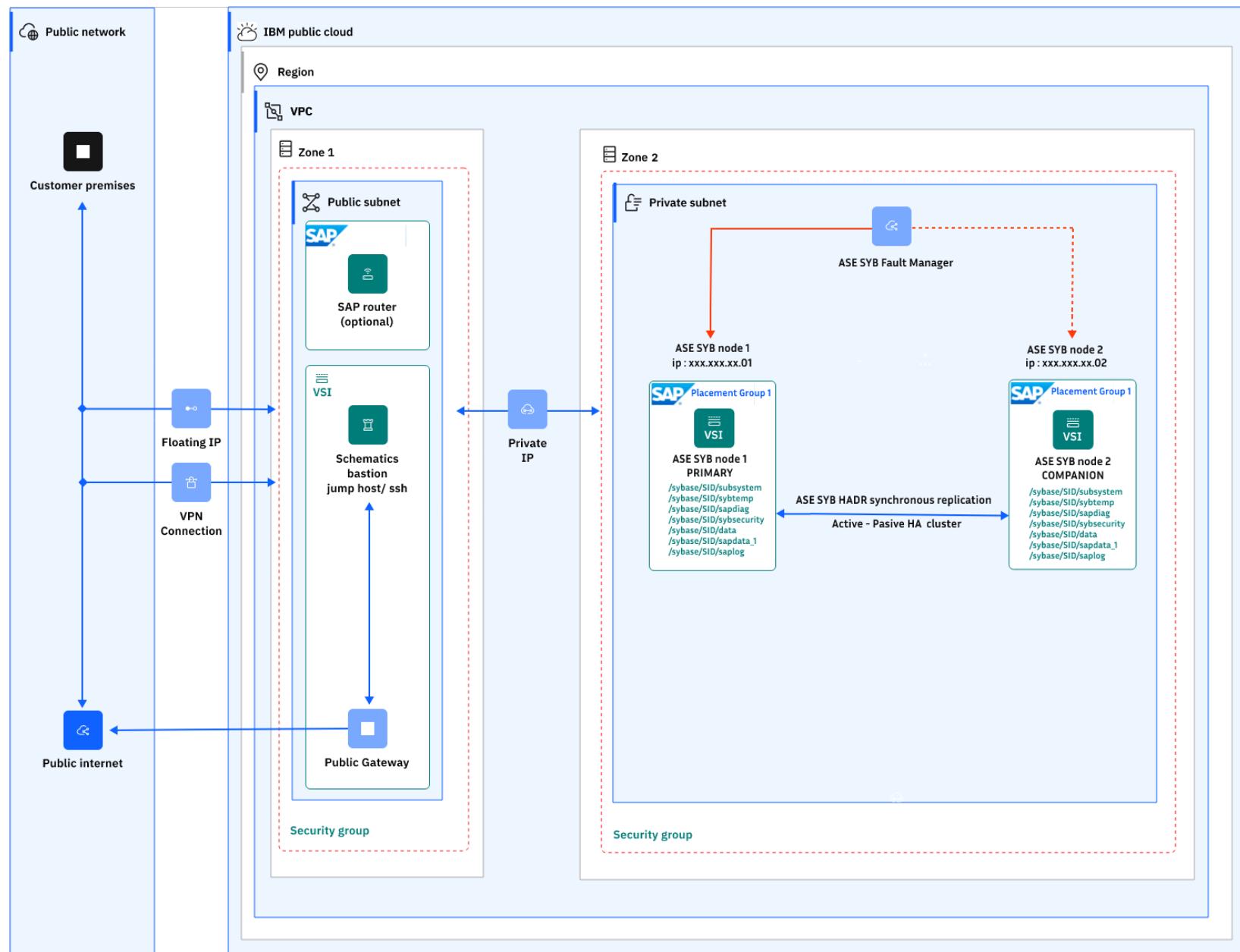
- Separated from the wider public DNS, and their publicly accessible records.
- Hidden from the system outside of and not part of the IBM Cloud private network.
- Accessible only from the system that you authorize on the IBM Cloud private network.
- Resolvable only via the resolvers provided by the service.

The DNS service maps the FQDN of each ALB to the virtual hostnames of the ASCS, ERS, and ASE Sybase that are used by SAP applications.

Type	Name	Value	TTL
CNAME	dbpochana	is an alias of 20bdd130-eu-de.lb.appdomain.cloud	12 hr
CNAME	sappocers	is an alias of 3941d983-eu-de.lb.appdomain.cloud	12 hr
CNAME	sappocases	is an alias of 56a9190d-eu-de.lb.appdomain.cloud	12 hr

DNS records

Highly available system for SAP ASE Sybase database with HADR system



SAP HA for ASE Sybase DB instances cluster nodes primary (Active) and Secondary (Companion)

At the most basic level, a standard HA ASE Sybase cluster in an active(primary)-passive(companion) configuration has two nodes: one is the primary node and the other is the standby node. This means that the primary node is actively serving the active SAP DB instances (Primary and Companion), while the standby node is waiting to jump in if there is any failure.

The cluster is set with a virtual hostname IP (hostname is mapped to the FQDN of the ASE Sybase ALB through DNS, which is the same as

explained previously for SAP ASCS and ERS instances). Application instances (PAS and AAS) are used on the SAP profiles to call that particular component. The cluster assigns the virtual IP to the active node and uses a heartbeat monitor to confirm the availability of the components. If the primary node stops responding, it triggers the automatic failover mechanism that calls the standby node to step up to become the primary node. The ALB detects the change, redirects the traffic to the new active node, and assigns the virtual IP to it, restoring the component availability. Once fixed, the failed node comes online as a standby node.

SAP Sybase HADR system supports synchronous replication

The SAP Sybase HADR system supports synchronous replication between the primary and standby servers for high availability. An active-active setup is a two-node configuration where both nodes in the cluster include SAP ASE managing independent workloads, capable of taking over each others workload in the event of a failure.

The SAP ASE server that takes over the workload is called a secondary companion, and the SAP ASE server that fails is called the primary companion. Together they are companion servers. This movement from one node to another is called failover. After the primary companion is ready to resume its workload, it is moved back to its original node. This movement is called a failback.

When a system fails over, clients that are connected to the primary companion and use the failover property automatically reestablish their network connections to the secondary companion. You must tune your operating system to successfully manage both servers during fail over. See your operating system documentation for information about configuring your system for high availability. An SAP ASE configured for failover in an active-active setup can be shut down using the shutdown command only after you have suspended SAP ASE from the companion configuration, at both the server level and the platform level.

The always-on option in a High Availability and Disaster Recovery (HADR) system consists of two SAP ASE servers:

- Primary on which all transaction processing takes place.
- Warm standby (referred to as a "standby server" in DR mode, and as a "companion" in HA mode) for the primary server, and contains copies of designated databases from the primary server.



Note: The HADR feature that is shipped with SAP ASE version 16.0 SP02 supports only a single-companion server.

Some high-availability solutions (for example, the SAP Adaptive Server Enterprise Cluster Edition) share or use common resources between nodes. However, the HADR system is a "shared nothing" configuration, each node has separate resources including disks.

In an HADR system, servers are separate entities and data is replicated from the primary server to the companion server. If the primary server fails, a companion server is promoted to the role of primary server either manually or automatically. Once the promotion is complete, clients can reconnect to the new primary server, and see all committed data, including data that was committed on the previous primary server.

Servers can be separated geographically, which makes an HADR system capable of withstanding the loss of an entire computing facility.



Note: The HADR system includes an embedded SAP Replication Server, which synchronizes the databases between the primary and companion servers. SAP ASE uses the Replication Management Agent (RMA) to communicate with Replication Server and SAP Replication Server uses Open Client connectivity to communicate with the companion SAP ASE.

The Replication Agent detects any data changes made on the primary server and sends them to the primary SAP Replication Server. In the figure above, the unidirectional arrows indicate that, although both SAP Replication Servers are configured, only one direction is enabled at a time.

The HADR system supports synchronous replication between the primary and standby servers for high availability so the two servers can keep in sync with Zero Data Loss (ZDL). This requires a network link that is fast enough between the primary and standby server so that synchronous replication can keep up with the primary servers workload. Generally, this means that the network latency is approximately the same speed as the local disk IO speed, a few (fewer than 10) milliseconds. Anything longer than a few milliseconds may result in a slower response to write operations at the primary.

The HADR system supports asynchronous replication between the primary and standby servers for disaster recovery. The primary and standby servers by using asynchronous replication can be geographically distant, meaning they can have a slower network link. With asynchronous replication, Replication Agent Thread captures the primary servers workload, which is delivered asynchronously to SAP Replication Server. The SAP Replication Server applies these workload change to the companion server.

The most fundamental service that is offered by the HADR system is the failover; planned or unplanned from the primary to the companion server, which allows maintenance activity to occur on the old primary server, while applications continue on the new primary.

The HADR system provides protection in the event of a disaster. If the primary server is lost, the companion server can be used as a replacement. Client applications can switch to the companion server, and the companion server is quickly available for users. If the SAP Replication Server was in synchronous mode before the failure of the primary server, the Fault Manager automatically initiates failover with

zero data loss.

Fault Manager installation on the SAP ASCS node

The required parameters are asked during the installation process to create a profile for the fault manager and then adds it to the instance start profile. It is also possible to run the installation by using an existing profile: `sybdbfm install pf=<SYBHA.PFL>` In this case, the installation process will only ask for profile parameters missing in the profile.



Note: Fault manger is integrated with ASCS on same SAP PAS/AAS cluster (start/stop/move together).

There may be some data loss if the SAP Replication Server was in asynchronous mode and you must use manual intervention to failover for disaster recovery.

Connection attempts to the companion server without the necessary privileges are silently redirected to the primary companion via the login redirection mechanism, which is supported by Connectivity libraries. If login redirection is not enabled, client connections fail and are disconnected.

The SAP ASE HADR option installs the below components:

- SAP ASE
- SAP Replication Server
- Replication Management Agent (RMA)
- SAP Host Agent
- Fault Manager
- SAP ASE Cockpit



Note: This automation is offered at no cost; however, the provisioned infrastructure comes at cost.

VPC with Additional Application Server (AAS) ABAP on Linux for SAP HANA

You can use Terraform scripts to create a single-tier VPC and create the AAS to HANA and AnyDB infrastructure on the VPC. The Terraform scripts use the VPC information that you provide and then call the Ansible playbook to create the SAP architecture on the specified VPC. Terraform on IBM Cloud® enables predictable and consistent provisioning of IBM Cloud Virtual Private Cloud (VPC) infrastructure resources so that you can rapidly build complex, cloud environments. IBM Cloud VPC infrastructure consists of SAP certified hardware that uses Intel® Xeon CPUs and more Intel® technologies.

You have two deployment methods to choose from:

- Terraform scripts that run from the CLI on your bastion server.
- Schematics user interface accessed from your cloud dashboard menu.

You can create SAP AAS NetWeaver 7.x on the SAP HANA-based ABAP stack.

SAP solution implemented

Many SAP enterprise solutions are built on the SAP platform (SAP NetWeaver) including:

- SAP HANA as Primary Persistence for SAP NetWeaver-based applications
- SAP Business Suite applications (ERP, CRM, and SCM, and other applications),
- SAP Business Warehouse (BW), and
- Other SAP enterprise solutions

SAP NetWeaver has two distinct aspects, ABAP and Java. Many applications that are built on the SAP NetWeaver's ABAP or Java (or both) application servers run on SAP DB owned HANA and ASE Sybase either in AnyDB platforms (MSSQL, Oracle, and Db2).

Technical interfaces are available for applications that are built on the SAP NetWeaver AS ABAP and AS Java to run on SAP HANA and AnyDB. However, specific development enablement is normally required for each application to ensure that it runs optimally on the SAP HANA. SAP Business Suite applications (ERP, CRM, SCM, and other applications), SAP Business Warehouse (BW), and other SAP NetWeaver-based applications were modified to run on SAP HANA and have many advantages. Also, various components and complimentary applications that are built on SAP NetWeaver can also run on SAP HANA or AnyDB by using the provided SAP NetWeaver DB interfaces.

The SAP HANA as primary persistence for SAP NetWeaver-based applications scenario has one restriction: SAP NetWeaver ABAP and Java

application servers must run on separate hardware servers from the SAP HANA hardware.

What is created

The scripts automate the virtual infrastructure resources, provisioning the processes for the SAP architecture in an existing VPC with a distributed environment. SAP AAS NetWeaver 7.x (HANA or ASE SYB) application server on a distinct VSI VPC system and SAP HANA DB on a dedicated server type VSI VPC box are provisioned. The scripts work in two phases.

During the first phase of [Automate SAP bastion server – SAP media storage repository](#), the following virtual infrastructure resources based on the components from the existing VPC created by the bastion server are:

- 1 VPC where the virtual server instance is provisioned.
- 1 security group. The rules for this security group are:
 - Allow inbound DNS traffic (port 53).
 - Allow inbound SSH traffic (TCP port 22).
 - Allow all outbound traffic from the virtual server instance.
 - Allow all traffic in the security group.
- 1 subnet to enable the networking in your VPC.
- 2 virtual server instances with SAP certified storage and network configurations.
- 1 floating IP address used to access your VPC virtual server instance over the public network.

During the second phase, the Ansible Playbooks is called and the SAP architecture is installed for both dedicated virtual server instance (VSI) SAP application; VSI system and dedicated SAP HANA VSI box. The SAP architecture that is deployed on the SAP NetWeaver 7.x release is a stand-alone dedicated SAP HANA 2.0 box release. For more information about this architecture, see [Automating SAP HANA stand-alone virtual server instance on IBM Cloud® VPC by using Terraform and Ansible](#).

You can provision only one instance of the service per IBM Cloud region.

Schematics deployment

When you run the scripts with the Schematics interface, you:

- Enter the workspace information.
- Enter the GitHub path for the chosen solution either on NetWeaver AAS for HANA.
- Modify the parameters in the Schematics interface. They are the same parameters as the `input.auto.tfvars` file that you use with the cli.

Virtual server instance configuration

Following are the supported operating system images for SAP NetWeaver primary application server:

- ibm-redhat-8-4-amd64-sap-applications-2
- ibm-redhat-8-6-amd64-sap-applications-2
- ibm-sles-15-3-amd64-sap-applications-2
- ibm-sles-15-4-amd64-sap-applications-3

Following are the supported operating system images for SAP HANA database:

- ibm-redhat-8-4-amd64-sap-hana-2
- ibm-redhat-8-6-amd64-sap-hana-2
- ibm-sles-15-3-amd64-sap-hana-2
- ibm-sles-15-4-amd64-sap-hana-1

For both server instances there are:

- Two SSH keys are configured to access SSH as `root`.
- Three storage volumes as described in the `input.auto.tfvars` file.

What is created for anydb

The scripts use the information that you provide for an existing VPC and deploy AAS to SAP HANA or AnyDB on a different host than CI (SAP Central Instance) VSI host. For more information about this architecture, see [SAP NetWeaver 7.x on UNIX with HANA or AnyDB on IBM Cloud](#)

[VPC on IBM Cloud VPC](#). You specify the information for the VPC to use in the `input.auto.tfvars` file.

The scripts call the Ansible Playbooks to install the SAP architecture.

Script files

The configuration and script files are provided on GitHub. Each supported interface for the SAP solution installation has its own folder in the GitHub repository:

- [GitHub repository for Terraform – AAS HANA](#)

Terraform interface

To run the Terraform script, you modify:

- The `input.auto.tfvars` file to specify the existing VPC resources for your solution. Specify the variables for the existing VPC:
 - VPC name
 - Security group
 - Subnet
 - Hostname
 - Profile
 - Image
 - Up to two SSH keys

You can change the default SAP system configuration settings to match your solution. You can also specify the location where you downloaded the SAP kits.

The IBM Cloud Provider plug-in for Terraform on IBM Cloud uses these configuration files to install AAS to SAP HANA and AnyDB on the specified VPC in your IBM Cloud account.

Support

There are no warranties of any kind, and there is no service or technical support available for these materials from IBM®. As a recommended practice, review carefully any materials that you download from this site before using them on a live system.

Though the materials provided herein are not supported by the IBM® Service organization, your comments are welcomed by the developers, who reserve the right to revise, readapt or remove the materials at any time. To report a problem, or provide suggestions or comments, open a GitHub issue.

Before you begin

Before you use the scripts in the bastion cli:

- Set up your account to access the VPC. Make sure that your account is [upgraded to a paid account](#).
- If you have not already, create a Bastion server to store the SAP kits. For more information, see [Automate SAP bastion server - SAP media storage repository](#).
- Download the SAP kits from the SAP Portal to your Deployment Server. Make note of the download locations. Ansible decompresses the files. For more information, see the [readme](#) file.
- [Create or retrieve an IBM Cloud API key](#). The API key is used to authenticate with the IBM Cloud platform and to determine your permissions for IBM Cloud services.
- [Create or retrieve your SSH key ID](#). You need the 40-digit UUID for the SSH key, not the SSH key name.
- Terraform should already be installed on the bastion server that you deployed. For more information, see [Bastion server for SAP deployment](#).
- (Optional - Catalog Tile) create secrets for your credentials and passwords by using the [Secrets Manager](#).

Deploying SAP AAS NetWeaver 7.x on HANA by using the Schematics user interface

Use these steps to configure the SAP Additional Application Server (AAS) NetWeaver with HANA or AnyDB on your existing VPC by using the Schematics interface. The script takes 2 - 3 hours to complete.

1. From the IBM Cloud menu, select **Schematics**.
2. Click **Create** workspace.

3. On the **Specify template** page:
 - Enter the URL for the Schematics interface.
 - Select the **Terraform version** that is listed in the readme file.
 - Click **Next**.
4. On the **workspace details** page:
 - Enter a name for the workspace.
 - Select a **Resource group**.
 - Select a **Location** for your workspace. The workspace location does not have to match the resource location.
 - Select **Next**.
5. Select **Create** to create your workspace.
6. On the workspace settings page, in the input variables section, review the default input variables and provide values that match your solution.
 For a more detailed description of each parameter, check the GitHub repo [AAS HANA readme](#) file, chapter "Input parameter file". Also, make sure to mark the parameters that contain sensitive information like passwords, API, and ssh private keys as "sensitive". These parameters are marked as "sensitive" in the readme file, under "Input parameter file".
7. On the workspace settings page, click **Generate plan**. Wait for the plan to complete.
8. Click **View log** to review the log files of your terraform execution plan.
9. Apply your Terraform template by clicking **Apply plan**.
10. Review the log file to ensure that no errors occur during the provisioning, modification, or deletion process.

Deploying SAP AAS NetWeaver (ABAP) on HANA with the Deployable Architecture tile interface

Use these steps to configure the SAP AAS NetWeaver (ABAP) on HANA on your existing VPC by using the catalog tile interface. The script takes 2 - 3 hours to complete.

1. From the IBM Cloud catalog, select **VPC with Additional Application Server ABAP on Linux for SAP HANA** on HANA tile. The **Create** tab opens for VPC with Additional Application Server ABAP on Linux for SAP HANA. For more information about this deployment, see the About tab or the readme file link.
2. Select the latest version.
3. Select **VPC with Additional Application Server ABAP on Linux for SAP HANA on Deployable Architecture tile** variation.
4. Click **Review deployment** options:
 - **Add to project** to add this deployment to an IBM Cloud project and combine it with other deployments. IBM Cloud projects include several more pipeline steps before deployment, including deployment validation, cost calculation, compliance verification, and approval process.
 - **Create from the CLI** to get the CLI command. With this command you can trigger the deployment from the CLI.
 - **Work with code** to embed the code into other terraform deployments.
 - **Deploy with IBM Cloud Schematics** to trigger the deployment process directly.
5. Select **Deploy with IBM Cloud Schematics**.
6. Add the input parameters for this installation. There are 3 categories of parameters:
 - **Workspace** - These parameters define the workspace that is automatically created in Schematics:
 - Enter a name for the workspace or use the default name.
 - The Resource Group used to create resources. Use default or create a Resource Group.
 - Select a location to create your Schematics workspace. The workspace location need not match the resource location.
 - **Required input variables** - Review the default input variables and provide values that match your solution. These parameters are specific to your deployment. For more detailed information, see the [Readme file](#).

Parameter	Description
BASTION_FLOATING_IP	Required only for Schematics Deployments. The Floating IP from the Bastion Server.

HOSTNAME	The hostname for the VSI. The hostname should be up to 13 characters as required by SAP. For more information on the rules regarding hostnames for SAP systems, check SAP Note 611361: Hostnames of SAP ABAP Platform servers
REGION	The cloud region to deploy the solution. The regions and zones for VPC are listed here . Review supported locations in IBM Cloud Schematics here . Sample value: eu-de.
RESOURCE_GROUP	The name of an existing Resource Group for VSIs and Volumes resources. Default value: "Default". The list of Resource Groups is available here .
SECURITY_GROUP	The name of an existing Security group. The list of security groups is available here .
SSH_KEYS	The list of SSH Keys UUIDs that are allowed to SSH as root to the VSI can contain one or more IDs. The list of SSH Keys is available here . Sample input (use your own SSH UUIDs from IBM Cloud){: external}[: ["r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a", "r010-3fcfd9fe7-d4a7-41ce-8bb3-d96e936b2c7e"]]
SUBNET	The name of an existing subnet. The list of subnets is available here .
VPC	The name of an existing VPC. The list of VPCs is available here .
ZONE	The cloud zone where to deploy the solution. Sample value: eu-de-2.
ibmcloud_api_key	IBM Cloud API key (Sensitive* value).
private_ssh_key	Required only for Schematics Deployments - Input your id_rsa private key pair content in OpenSSH format (Sensitive* value). This private key should be used only during the terraform provisioning and it is recommended to be changed after the SAP deployment.
hdb_instance_number	The instance number of the SAP HANA database server.
sap_aas_instance_number	Technical identifier for the internal processes of the additional application server.
sap_asci_instance_number	Technical identifier for the internal processes of ASCS.
sap_ci_host	IP address of the existing SAP Central Instance.
sap_ci_hostname	The hostname of the existing SAP Central Instance.
sap_ci_instance_number	Technical identifier for the internal processes of the Central Instance.
sap_sid	The SAP system ID identifies the entire SAP system.
sap_main_password	Common password for all users that are created during the installation (See Obs*).

Required Variables

- **Optional variables** - Review and update the optional input variables. The Ansible scripts expect the SAP kits to be in the default locations listed. For more information, see the [Readme file - Input Parameters](#).

Parameter	Description
ID_RSA_FILE_PATH	The file path for private_ssh_key is automatically generated by default. If it is changed, it must contain the relative path from Git repo folders. Default value: "ansible/id_rsa".
IMAGE	The OS image used for the VSI. A list of images is available here .
PROFILE	The profile used for the VSI. A list of profiles is available here . For more information about supported DB/OS and IBM Gen 2 Virtual Server Instances (VSI), check SAP Note 2927211: SAP Applications on IBM Virtual Private Cloud .

VOL1	Volume 1 Size - The size for the disks in GB that are to be attached to the VSI and used by SAP.
VOL2	Volume 2 Size - The size for the disks in GB that are to be attached to the VSI and used by SAP.
kit_sapcar_file	Path to the sapcar binary, as downloaded from SAP Support Portal.
kit_swpm_file	Path to the SWPM archive (SAR), as downloaded from SAP Support Portal.
kit_saphostagent_file	Path to the SAP Host Agent archive (SAR), as downloaded from SAP Support Portal.
kit_hdbclient_file	Path to the HANA DB client archive (SAR), as downloaded from SAP Support Portal.

Optional Variables

7. Accept the license agreement.
8. Select **Deploy**. The deployment starts and you are directed to the Schematics page that displays the script log files for you to monitor the deployment progress.

Creating the infrastructure using Terraform with the bastion server CLI

Use these steps to configure the IBM Cloud Provider plug-in and use Terraform to install SAP AAS to SAP HANA and AnyDB on your existing VPC on an already deployed SAP NetWeaver 7.X with SAP HANA 2.0 or ASE SYB as a Central Instance.

The script takes 1 - 2 hours to complete.

1. Access the bastion server cli.
2. Clone the solution repository and change to the folder.

ASE SYB 16 Clone the solution repository from <https://github.com/IBM-Cloud/sap-aas-abap-ase-syb> and cd to the sap-aas-abap-ase-syb/cli folder.

```
$ git clone https://github.com/IBM-Cloud/sap-aas-abap-ase-syb
cd sap-aas-abap-ase-syb/cli/
```

SAP HANA 2.0: Clone the solution repository from <https://github.com/IBM-Cloud/sap-abap-hana-aas> and cd to the sap-abap-hana-aas folder.

```
$ git clone https://github.com/IBM-Cloud/sap-abap-hana-aas.git
cd sap-abap-hana-aas/
```

3. Modify the `input.auto.tfvars` file to specify the information for the existing VPC, your region, zone, networking component names, hostname for the AAS VSI,profile, and image. You need your 40-digit SSH key ID for this file. The second SSH key is optional. For more options for profile, see [Instance Profiles](#). For more options, see [Images](#). For descriptions of the variables, see the [readme](#) file.

The VSI OS images that are supported for this solution for Netweaver Additional Application Server are:

- ibm-redhat-8-4-amd64-sap-applications-2
- ibm-redhat-8-6-amd64-sap-applications-2
- ibm-sles-15-3-amd64-sap-applications-2
- ibm-sles-15-4-amd64-sap-applications-4

```
$ # Infra VPC variables for ASE SYB
REGION    = "eu-de"
ZONE      = "eu-de-2"
VPC        = "ic4sap"                      # EXISTING Security group name
SECURITY_GROUP = "ic4sap-securitygroup"      # EXISTING Security group name
RESOURCE_GROUP = "wes-automation"
SUBNET     = "ic4sap-subnet"                  # EXISTING Subnet name
SSH_KEYS   = [ "r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a" , "r010-3fcfd9fe7-d4a7-41ce-8bb3-
d96e936b2c7e" ]

# SAP AAS VSI variables:
```

```

HOSTNAME = "sapnwase-as01"
PROFILE = "bx2-4x16"
IMAGE = "ibm-redhat-8-4-amd64-sap-applications-2

$ # Infra VPC variables for ABAP HANA
REGION      = "eu-de"
ZONE        = "eu-de-2"
VPC          = "ic4sap" # EXISTING Security group name
SECURITY_GROUP = "ic4sap-securitygroup" # EXISTING Security group name
RESOURCE_GROUP = "wes-automation"
SUBNET       = "ic4sap-subnet" # EXISTING Subnet name
SSH_KEYS     = [ "r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a" , "r010-3fc9fe7-d4a7-41ce-8bb3-d96e936b2c7e" ]
ID_RSA_FILE_PATH = "ansible/id_rsa"

# SAP AAS variables:
HOSTNAME = "sapnwapp"
PROFILE = "bx2-4x16"
IMAGE = "ibm-redhat-8-6-amd64-sap-applications-2"

```

4. Customize your SAP system configuration. In the same file, input.auto.tfvars, edit the SAP system configuration variables that are passed to the Ansible automated deployment. For descriptions of the variables, see the [readme](#) file.

```

$ # SAP system configuration - for ASE SYB
sap_sid = "NWD"
sap_ci_host = "10.243.132.10"
sap_ci_hostname = "sapnwase"
sap_ci_instance_number = "00"
sap_asc_s_instance_number = "01"
sap_aas_instance_number = "00"

# Kits paths
kit_sapcar_file = "/storage/NW75SYB/SAPCAR_1010-70006178.EXE"
kit_swpm_file = "/storage/NW75SYB/SWPM10SP31_7-20009701.SAR"
kit_saphotagent_file = "/storage/NW75SYB/SAPHOSTAGENT51_51-20009394.SAR"

```

```

$ # SAP system configuration - for ABAP HANA
sap_sid = "NWD"
sap_ci_host = "10.243.132.10"
sap_ci_hostname = "sapnwapp01"
sap_ci_instance_number = "00"
sap_asc_s_instance_number = "01"
hdb_instance_number = "00"
sap_aas_instance_number = "00"

# Kits paths
kit_sapcar_file = "/storage/NW75HDB/SAPCAR_1010-70006178.EXE"
kit_swpm_file = "/storage/NW75HDB/SWPM10SP31_7-20009701.SAR"
kit_saphotagent_file = "/storage/NW75HDB/SAPHOSTAGENT51_51-20009394.SAR"
kit_hdbclient_file = "/storage/NW75HDB/IMDB_CLIENT20_009_28-80002082.SAR"

```

Ansible decompresses the rest of the SAP kit files. For more information, see the [readme](#) file.

5. Initialize the Terraform CLI.

```
terraform init
```

6. Create a Terraform execution plan. The Terraform execution plan summarizes all the actions that are done to create the virtual private cloud instance in your account.

```
terraform plan plan1
```

Enter an SAP main password and your API key.

The SAP main password must be 10 - 14 characters long and contain at least one digit (0-9). It can contain only the following characters: a-z, A-Z, 0-9, @, #, \$, . *This password cannot contain exclamation points '!'. The password must not start with a digit or an underscore ().*

7. Verify that the plan shows all of the resources that you want to create and that the names and values are correct. If the plan needs to be adjusted, edit the input.auto.tfvars file to correct resources and run terraform plan again.
8. Apply the saved plan.

```
$ terraform apply "plan1"
```

The virtual private cloud and components are created and you see output similar to the `terraform plan` output.

9. Add the SAP credentials and the virtual server instance IP to the SAP GUI. For more information about the SAP GUI, see [SAP GUI](#).

Next steps

If you need to rename your resources after they are created, modify the input.auto.tfvars file to change the names and run `terraform plan` and `terraform apply` again. Do not use the IBM Cloud Dashboard and user interface to modify your VPC after it is created. The Terraform scripts create a complete solution and selectively modifying resources with the user interface might cause unexpected results.

If you need to remove the SAP Netweaver 7.X on HANA or AnyDB installation, go to your project folder and run `terraform destroy`. The `terraform destroy` command does not remove the VPC in this scenario because the VPC was created before these Terraform scripts were run.

Related information

For more information about Terraform on IBM Cloud, see [Getting started with Terraform on IBM Cloud](#).

For more information about using Terraform for creating only a VPC for SAP, without the SAP architecture, see [Creating single-tier virtual private cloud for SAP by using Terraform](#).

SAP One Support Notes that apply to this document:

- [SAP Note 84555 - Windows Server, Linux®, and UNIX: Certified hardware](#)
- [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#)
- [SAP Note 2923773 - Linux® on IBM Cloud \(IaaS\): Adaption of your SAP license](#)
- [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#)
- [SAP Note 2369910 - SAP Software on Linux®: General information](#)
- [SAP Note 171380 - Released IBM hardware \(Intel processors\) and IBM cloud services offers](#)
- [SAP Note 1380654 - SAP support in IaaS environments](#)

This document is referenced by:

- [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#)
- [SAP Note 2588225 - SAP on IBM Cloud: Protect against speculative execution vulnerabilities](#)
- [SAP Note 1380654 - SAP support in IaaS environments](#)
- [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#)

SAP HANA DB cross-region DR automation in VPC

Automating SAP workload HA deployment on IBM Cloud VPC with Terraform and Ansible

You can use Terraform to automate IBM Cloud® VPC provisioning. The VPC provisioned includes virtual server instances with high network performance. The VPC infrastructure contains various Infrastructure-as-a-Service (IaaS) offerings, including virtual servers. After the VPC is provisioned, the scripts use the Ansible Playbooks to install the SAP system.

IBM Cloud VPC introduction

VPC is a public cloud offering that an enterprise uses to establish its own private cloud-like computing environment on shared [public cloud](#) infrastructure. VPC gives an enterprise the ability to define and control a virtual network that is logically isolated from all other public cloud tenants, creating a private and secure place on the public cloud.

Imagine that a cloud provider's infrastructure is a residential apartment building and multiple families live inside. A public cloud tenant is a kind of sharing an apartment with a few roommates. In contrast, having a VPC is like having your own private condominium; no one else has the key, and no one can enter the space without your permission.

VPC's logical isolation is implemented by using virtual network functions and security features that give the enterprise customer granular control over which IP addresses or applications can access particular resources. It is analogous to the "friends-only" or "public/private" controls on social media accounts used to restrict who can or can't see your otherwise public posts.

With IBM Cloud VPC, you can use the UI, CLI, and API to manually provision virtual server instances for VPC with high network performance. VPC infrastructure contains various Infrastructure-as-a-Service (IaaS) offerings including virtual servers for VPC.

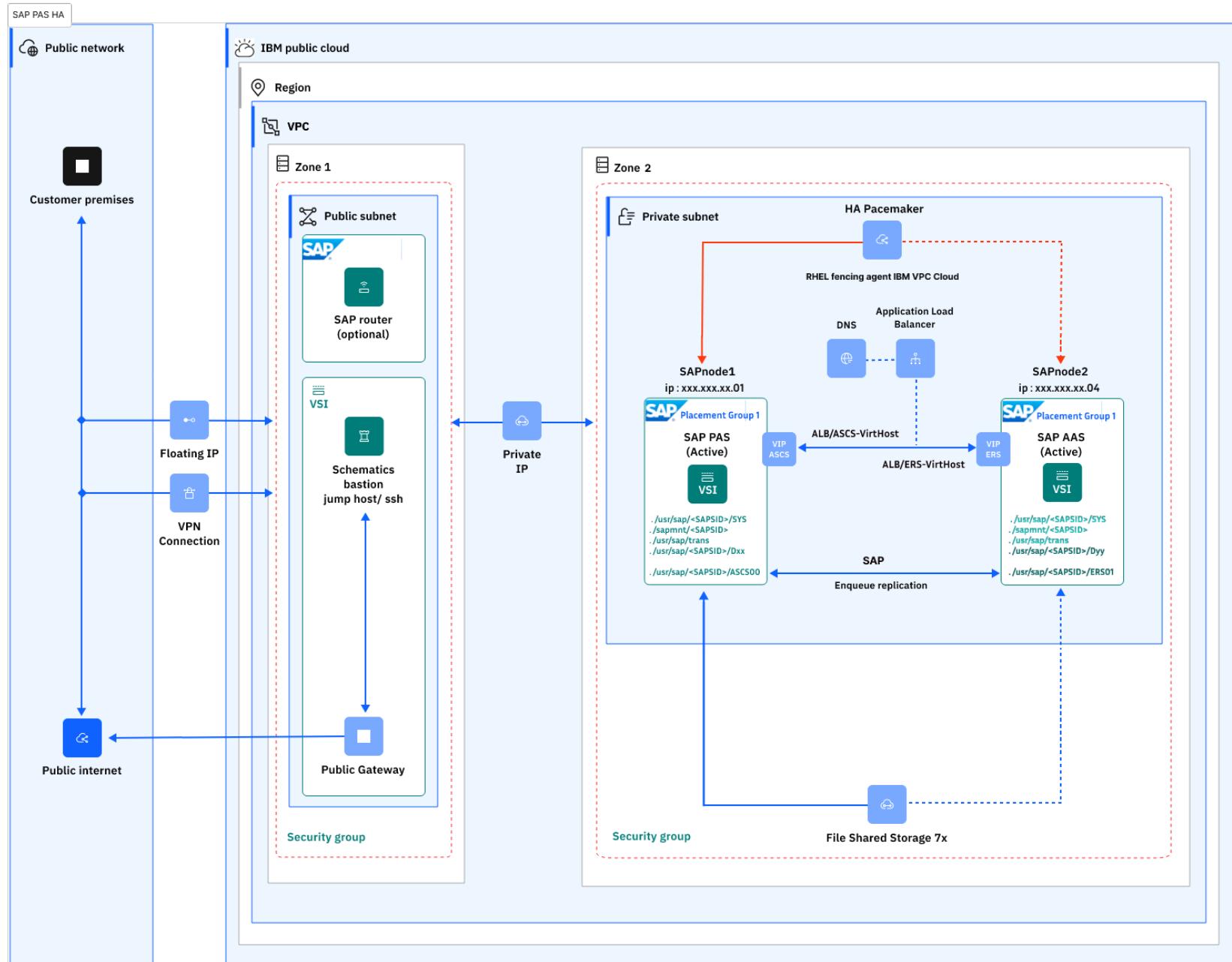
Use the following information to understand a simple use-case for planning, creating, and configuring resources for your VPC, and learn more about VPC overviews and VPC tutorials. For more information about the VPC, see [Getting started with Virtual Private Cloud \(VPC\)](#).

SAP products architecture on IBM Cloud VPC

A [Virtual Private Cloud \(VPC\)](#) contains one of the most secure and reliable cloud environments for SAP applications within your own VPC with virtual server instances. This represents an Infrastructure-as-a-Service (IaaS){: external} within IBM Cloud that offers all the benefits of isolated, secure, and flexible virtual cloud infrastructure from IBM. In comparison, the IBM Cloud classic infrastructure virtual servers offering uses virtual instances with native and VLAN networking to communicate with each other within a data center; however, the instances are restricted in one well-working pod by using subnet and VLAN networking as a gap scale up of virtual resources should rely between the pods. The IBM Cloud VPC network orchestrator layer concept eliminates the pod boundaries and restrictions, so this new concept handles all the networking for every virtual instance running within VPC across regions and zones.

Highly available system for SAP NetWeaver on IBM Cloud VPC

In a Highly Available (HA) system, every instance can run on a separate IBM Cloud virtual server instance. The cluster HA configuration for the SAP application server consists of two virtual server instances, each of them located in the same zone within the region by using placement groups. Placement groups assure that both cluster resources and cloud resources are also located in different compute nodes as specified in the following placement groups section:



SAP HA for SAP applications cluster nodes PAS (Active) and AAS (Active)

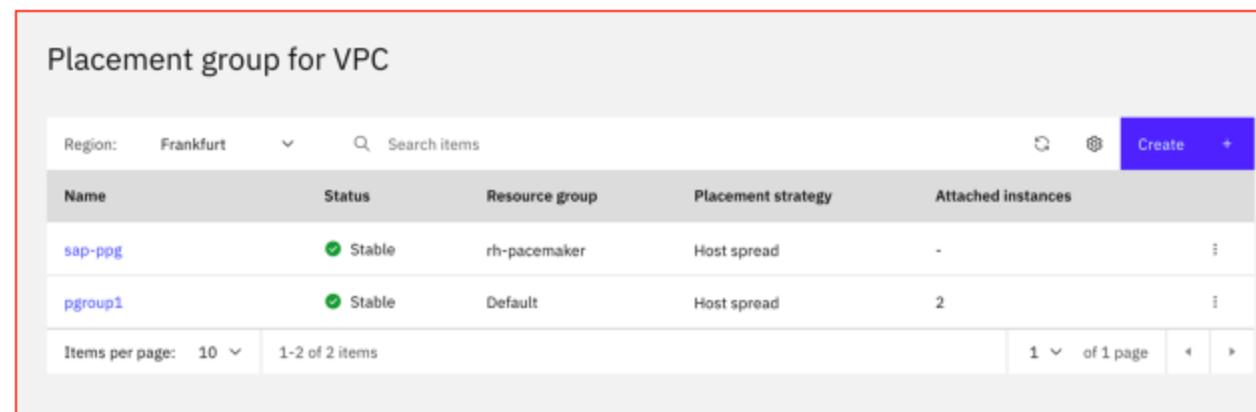
Placement groups on IBM Cloud VPC for SAP HA architecture

Placement Groups (PG) for VPC have two different anti-affinity strategies for high availability. By using the placement strategies, you minimize the chance of service disruption with virtual server instances that are placed on different hosts or into an infrastructure with separate power and network supplies.

The design of placement groups for IBM Cloud virtual servers solves this issue. Placement groups give a measure of control over the host on which a new public virtual server is placed. In this release, a “spread” rule is implemented, which means that the virtual servers within a placement group are spread onto different hosts. You can build a highly available application within a data center and know that your virtual servers are isolated from each other.

Placement groups with the spread rule are available to create in selected IBM Cloud data centers. After a spread rule is created, you can provision a virtual server into that group and ensure that it is not on the same host as any of your other virtual servers. This feature comes with no cost.

You can create your placement group and assign up to four new virtual server instances. With the spread rule, each of your virtual servers are provisioned on different physical hosts. In the following configuration example, the “Power Spread” option is used:



Placement groups host spread

Placement group for VPC					
Name	Status	Resource group	Placement strategy	Attached instances	
sapha-poc	Stable	wes-ic4sap-resourcegroup	Power spread	4	⋮
Items per page: 10 1 item 1 of 1 page ⋮					

Placement groups power spread

Following are the SAP instances that are required for HA scenario:

- ABAP SAP Central Services (ASCS) instance - contains the ABAP message server and the ABAP enqueue server.
- Enqueue Replication Server (ERS) instance for the ASCS instance.
- Database instance
- Primary Application Server (PAS) instance on node 1.
- Additional Application Server (AAS) instance on node 2.



Note: It is recommended to run both the ASCS instance and the ERS instance in a switchover cluster infrastructure.

IBM Cloud File Storage for VPC for SAP HA architecture

[IBM Cloud File Storage for VPC](#) technology is used to make the SAP directories available to the SAP system. The technologies of choice are NFS, shared disks, and cluster file system. If you have decided to use the HA solution for your SAP system, make sure that you properly address the HA requirements of the SAP file systems in your SAP environment.

File shares for VPC								
Name	Status	Resource groups	Location	Mount targets	Size	Replication role	Encryption type	
usrsap-as1-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	⋮
usrsap-as2-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	⋮
usrsap-sapsacs-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	⋮
usrsap-sapers-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	⋮
usrsap-sapmnt-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	⋮
usrsap-sapsys-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	⋮
usrsap-trans-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	80 GB	None	Provider managed	⋮

File shares for VPC

- File shares that are mounted as NFS permanent file systems on both cluster nodes for SAP HA application:
 - `/usr/sap/<SAPSID>/SYS`
 - `/sapmnt<SAPSID>`
 - `/usr/sap/trans`
- Cluster-managed file systems for SAP HA application: ASCS
 - `/usr/sap/<SAPSID>/ASCS00`
 - `/usr/sap/<SAPSID>/ERS01`
- Permanent NFS mount on SAP HA application node 1 PAS instance:
 - `/usr/sap/<SAPSID>/Dxx`
- Permanent NFS mount on SAP HA application node 2 dialog instance:
 - `/usr/sap/<SAPSID>/Dyy`

Prerequisites

You need to install the hardware (hosts, disks, and network) and decide how to distribute the database, SAP instances, and if required, the Network File System (NFS) server over the cluster nodes.

Context

Following are the types of SAP directories:

- Physically shared directories: `/<sapmnt>/<SAPSID>` and `/usr/sap/trans`

- Logically shared directories that are bound to a node, such as `/usr/sap`, with the following local directories:
 - `/usr/sap/<SAPSID>`
 - `/usr/sap/<SAPSID>/SYS`
 - `/usr/sap/hostctrl`
- Local directories that contain the SAP instances such as `/usr/sap/<SAPSID>/ASCS<Instance_Number>`
- The global transport directory may reside on a separate SAP transport host as a standard three systems transport layer configuration.

You need at least two nodes and a shared file system for distributed ASCS and ERS instances. The assumption is that the rest of the components are distributed on other nodes.

ASCS and ERS installation

In order for the ASCS and ERS instances to be able to move from one node to the other, they need to be installed on a shared file system and use virtual hostnames based on the virtual IP.

In this VPC-based SAP HA solution, the shared file system that is required by the cluster is replaced by the NFS-mounted file storage, and the virtual IP is replaced by the Application Load Balancer for VPC (ALB).

In this scenario, three ALBs are used, one for each Single Point of Failure (SPOF) component in order to replace the virtual IP requirement: ALB for ASCS, ALB for ERS, and ALB for ASE Sybase. Each ALB is configured as a backend for the corresponding cluster servers and redirects all of the communication that is received on the front-end ports to the active server in the backend pool.

Load balancers for VPC						
Region:	Frankfurt	▼	<input type="text"/> poc	X		
Name	Status	Family	Resource group	Type	Hostname	Location
db-alb-hana-poc	Active	Application	wes-ic4sap-resourcegroup	Private	20bdd130-eu-de.l b.appdomain.cloud	Frankfurt
sap-alb-ers-poc	Active	Application	wes-ic4sap-resourcegroup	Private	3941d983-eu-de.l b.appdomain.cloud	Frankfurt
sap-alb-ascs-poc	Active	Application	wes-ic4sap-resourcegroup	Private	56a9190d-eu-de.l b.appdomain.cloud	Frankfurt

Application load balancer management of HA IPs mechanism

Private application load balancer

A [private application load balancer](#) is accessible through your private subnets that you configured to create the load balancer.

Similar to a public application load balancer, your private application load balancer service instance is assigned an FQDN; however, this domain name is registered with one or more private IP addresses.

IBM Cloud operations change the number and value of your assigned private IP addresses over time, based on maintenance and scaling activities. The backend virtual server instances that host your application must run in the same region and under the same VPC.

Use the assigned ALB FQDN to send traffic to the private application load balancer to avoid connectivity problems to your applications during system maintenance or scaling down activities.

Each ALB sends traffic to the cluster node where the application (ASCS, ERS, ASE Sybase DB) is running. During the cluster failover, the ALB redirects all the traffic to the new node where the resources are up and running.



Note: DNS-as-a-Service (DNSaaS) is the management IBM Cloud VPC DNS service of HA and FQDN (IPs) mechanism.



Note: The ALB has a default of 50 seconds for client and server timeout, so after 50 seconds of inactivity, the connection is closed. To support SAP connections through ALB and not lose connection after 50 seconds, you need to request a change this value to a minimum of 300 seconds (client-side idle connection = minimum 300s and server-side idle connection = minimum 300s). To request this change, open a support ticket. This is an account-wide change that affects all of the ALBs in your account. For more information, see [Connection timeouts](#).

DNS Services with VPC

[IBM Cloud DNS Services](#) provide private DNS to VPC users. Private DNS zones are resolvable only on IBM Cloud and from explicitly [permitted networks](#) in an account. To get started, create a DNS Services instance by using the IBM Cloud console.

DNS Services allows you to:

- Create the private DNS zones that are collections for holding the domain names.
- Create the DNS resource records under these DNS zones.
- Specify the access controls used for the DNS resolution of resource records on a zone-wide level.

DNS Services also maintains its own worldwide set of DNS resolvers. Instances that are provisioned under IBM Cloud on an IBM Cloud network can use resource records that are configured through IBM Cloud DNS Services by querying DNS Services resolvers.

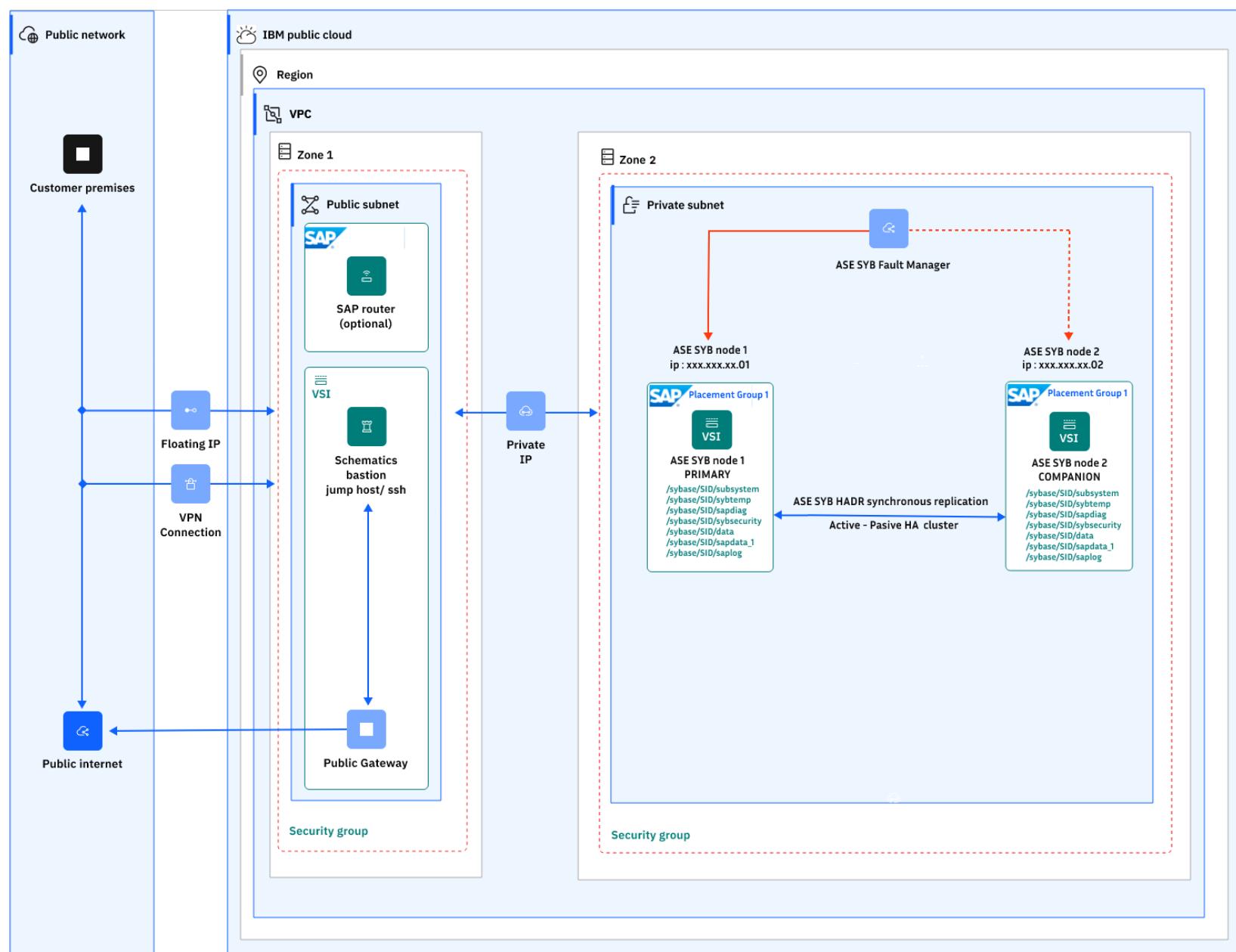
Resource records and zones that are configured through DNS Services are:

- Separated from the wider public DNS, and their publicly accessible records.
- Hidden from the system outside of and not part of the IBM Cloud private network.
- Accessible only from the system that you authorize on the IBM Cloud private network.
- Resolvable only via the resolvers provided by the service.

The DNS service maps the FQDN of each ALB to the virtual hostnames of the ASCS, ERS, and ASE Sybase that are used by SAP applications.

Type	Name	Value	TTL
CNAME	dbpochana	is an alias of 20bdd130-eu-de.lb.appdomain.cloud	12 hr
CNAME	sappocers	is an alias of 3941d983-eu-de.lb.appdomain.cloud	12 hr
CNAME	sappocases	is an alias of 56a9190d-eu-de.lb.appdomain.cloud	12 hr

Highly available system for SAP ASE Sybase database with HADR system



SAP HA for ASE Sybase DB instances cluster nodes primary (Active) and Secondary (Companion)

At the most basic level, a standard HA ASE Sybase cluster in an active(primary)-passive(companion) configuration has two nodes: one is the primary node and the other is the standby node. This means that the primary node is actively serving the active SAP DB instances (Primary and Companion), while the standby node is waiting to jump in if there is any failure.

The cluster is set with a virtual hostname IP (hostname is mapped to the FQDN of the ASE Sybase ALB through DNS, which is the same as

explained previously for SAP ASCS and ERS instances). Application instances (PAS and AAS) are used on the SAP profiles to call that particular component. The cluster assigns the virtual IP to the active node and uses a heartbeat monitor to confirm the availability of the components. If the primary node stops responding, it triggers the automatic failover mechanism that calls the standby node to step up to become the primary node. The ALB detects the change, redirects the traffic to the new active node, and assigns the virtual IP to it, restoring the component availability. Once fixed, the failed node comes online as a standby node.

SAP Sybase HADR system supports synchronous replication

The SAP Sybase HADR system supports synchronous replication between the primary and standby servers for high availability. An active-active setup is a two-node configuration where both nodes in the cluster include SAP ASE managing independent workloads, capable of taking over each others workload in the event of a failure.

The SAP ASE server that takes over the workload is called a secondary companion, and the SAP ASE server that fails is called the primary companion. Together they are companion servers. This movement from one node to another is called failover. After the primary companion is ready to resume its workload, it is moved back to its original node. This movement is called a failback.

When a system fails over, clients that are connected to the primary companion and use the failover property automatically reestablish their network connections to the secondary companion. You must tune your operating system to successfully manage both servers during fail over. See your operating system documentation for information about configuring your system for high availability. An SAP ASE configured for failover in an active-active setup can be shut down using the shutdown command only after you have suspended SAP ASE from the companion configuration, at both the server level and the platform level.

The always-on option in a High Availability and Disaster Recovery (HADR) system consists of two SAP ASE servers:

- Primary on which all transaction processing takes place.
- Warm standby (referred to as a "standby server" in DR mode, and as a "companion" in HA mode) for the primary server, and contains copies of designated databases from the primary server.



Note: The HADR feature that is shipped with SAP ASE version 16.0 SP02 supports only a single-companion server.

Some high-availability solutions (for example, the SAP Adaptive Server Enterprise Cluster Edition) share or use common resources between nodes. However, the HADR system is a "shared nothing" configuration, each node has separate resources including disks.

In an HADR system, servers are separate entities and data is replicated from the primary server to the companion server. If the primary server fails, a companion server is promoted to the role of primary server either manually or automatically. Once the promotion is complete, clients can reconnect to the new primary server, and see all committed data, including data that was committed on the previous primary server.

Servers can be separated geographically, which makes an HADR system capable of withstanding the loss of an entire computing facility.



Note: The HADR system includes an embedded SAP Replication Server, which synchronizes the databases between the primary and companion servers. SAP ASE uses the Replication Management Agent (RMA) to communicate with Replication Server and SAP Replication Server uses Open Client connectivity to communicate with the companion SAP ASE.

The Replication Agent detects any data changes made on the primary server and sends them to the primary SAP Replication Server. In the figure above, the unidirectional arrows indicate that, although both SAP Replication Servers are configured, only one direction is enabled at a time.

The HADR system supports synchronous replication between the primary and standby servers for high availability so the two servers can keep in sync with Zero Data Loss (ZDL). This requires a network link that is fast enough between the primary and standby server so that synchronous replication can keep up with the primary servers workload. Generally, this means that the network latency is approximately the same speed as the local disk IO speed, a few (fewer than 10) milliseconds. Anything longer than a few milliseconds may result in a slower response to write operations at the primary.

The HADR system supports asynchronous replication between the primary and standby servers for disaster recovery. The primary and standby servers by using asynchronous replication can be geographically distant, meaning they can have a slower network link. With asynchronous replication, Replication Agent Thread captures the primary servers workload, which is delivered asynchronously to SAP Replication Server. The SAP Replication Server applies these workload change to the companion server.

The most fundamental service that is offered by the HADR system is the failover; planned or unplanned from the primary to the companion server, which allows maintenance activity to occur on the old primary server, while applications continue on the new primary.

The HADR system provides protection in the event of a disaster. If the primary server is lost, the companion server can be used as a replacement. Client applications can switch to the companion server, and the companion server is quickly available for users. If the SAP Replication Server was in synchronous mode before the failure of the primary server, the Fault Manager automatically initiates failover with

zero data loss.

Fault Manager installation on the SAP ASCS node

The required parameters are asked during the installation process to create a profile for the fault manager and then adds it to the instance start profile. It is also possible to run the installation by using an existing profile: `sybdbfm install pf=<SYBHA.PFL>` In this case, the installation process will only ask for profile parameters missing in the profile.



Note: Fault manger is integrated with ASCS on same SAP PAS/AAS cluster (start/stop/move together).

There may be some data loss if the SAP Replication Server was in asynchronous mode and you must use manual intervention to failover for disaster recovery.

Connection attempts to the companion server without the necessary privileges are silently redirected to the primary companion via the login redirection mechanism, which is supported by Connectivity libraries. If login redirection is not enabled, client connections fail and are disconnected.

The SAP ASE HADR option installs the below components:

- SAP ASE
- SAP Replication Server
- Replication Management Agent (RMA)
- SAP Host Agent
- Fault Manager
- SAP ASE Cockpit



Note: This automation is offered at no cost; however, the provisioned infrastructure comes at cost.

VPC with Additional Application Server (AAS) ABAP on Linux for SAP HANA

You can use Terraform scripts to create a single-tier VPC and create the AAS to HANA and AnyDB infrastructure on the VPC. The Terraform scripts use the VPC information that you provide and then call the Ansible playbook to create the SAP architecture on the specified VPC. Terraform on IBM Cloud® enables predictable and consistent provisioning of IBM Cloud Virtual Private Cloud (VPC) infrastructure resources so that you can rapidly build complex, cloud environments. IBM Cloud VPC infrastructure consists of SAP certified hardware that uses Intel® Xeon CPUs and more Intel® technologies.

You have two deployment methods to choose from:

- Terraform scripts that run from the CLI on your bastion server.
- Schematics user interface accessed from your cloud dashboard menu.

You can create SAP AAS NetWeaver 7.x on the SAP HANA-based ABAP stack.

SAP solution implemented

Many SAP enterprise solutions are built on the SAP platform (SAP NetWeaver) including:

- SAP HANA as Primary Persistence for SAP NetWeaver-based applications
- SAP Business Suite applications (ERP, CRM, and SCM, and other applications),
- SAP Business Warehouse (BW), and
- Other SAP enterprise solutions

SAP NetWeaver has two distinct aspects, ABAP and Java. Many applications that are built on the SAP NetWeaver's ABAP or Java (or both) application servers run on SAP DB owned HANA and ASE Sybase either in AnyDB platforms (MSSQL, Oracle, and Db2).

Technical interfaces are available for applications that are built on the SAP NetWeaver AS ABAP and AS Java to run on SAP HANA and AnyDB. However, specific development enablement is normally required for each application to ensure that it runs optimally on the SAP HANA. SAP Business Suite applications (ERP, CRM, SCM, and other applications), SAP Business Warehouse (BW), and other SAP NetWeaver-based applications were modified to run on SAP HANA and have many advantages. Also, various components and complimentary applications that are built on SAP NetWeaver can also run on SAP HANA or AnyDB by using the provided SAP NetWeaver DB interfaces.

The SAP HANA as primary persistence for SAP NetWeaver-based applications scenario has one restriction: SAP NetWeaver ABAP and Java

application servers must run on separate hardware servers from the SAP HANA hardware.

What is created

The scripts automate the virtual infrastructure resources, provisioning the processes for the SAP architecture in an existing VPC with a distributed environment. SAP AAS NetWeaver 7.x (HANA or ASE SYB) application server on a distinct VSI VPC system and SAP HANA DB on a dedicated server type VSI VPC box are provisioned. The scripts work in two phases.

During the first phase of [Automate SAP bastion server – SAP media storage repository](#), the following virtual infrastructure resources based on the components from the existing VPC created by the bastion server are:

- 1 VPC where the virtual server instance is provisioned.
- 1 security group. The rules for this security group are:
 - Allow inbound DNS traffic (port 53).
 - Allow inbound SSH traffic (TCP port 22).
 - Allow all outbound traffic from the virtual server instance.
 - Allow all traffic in the security group.
- 1 subnet to enable the networking in your VPC.
- 2 virtual server instances with SAP certified storage and network configurations.
- 1 floating IP address used to access your VPC virtual server instance over the public network.

During the second phase, the Ansible Playbooks is called and the SAP architecture is installed for both dedicated virtual server instance (VSI) SAP application; VSI system and dedicated SAP HANA VSI box. The SAP architecture that is deployed on the SAP NetWeaver 7.x release is a stand-alone dedicated SAP HANA 2.0 box release. For more information about this architecture, see [Automating SAP HANA stand-alone virtual server instance on IBM Cloud® VPC by using Terraform and Ansible](#).

You can provision only one instance of the service per IBM Cloud region.

Schematics deployment

When you run the scripts with the Schematics interface, you:

- Enter the workspace information.
- Enter the GitHub path for the chosen solution either on NetWeaver AAS for HANA.
- Modify the parameters in the Schematics interface. They are the same parameters as the `input.auto.tfvars` file that you use with the cli.

Virtual server instance configuration

Following are the supported operating system images for SAP NetWeaver primary application server:

- ibm-redhat-8-4-amd64-sap-applications-2
- ibm-redhat-8-6-amd64-sap-applications-2
- ibm-sles-15-3-amd64-sap-applications-2
- ibm-sles-15-4-amd64-sap-applications-3

Following are the supported operating system images for SAP HANA database:

- ibm-redhat-8-4-amd64-sap-hana-2
- ibm-redhat-8-6-amd64-sap-hana-2
- ibm-sles-15-3-amd64-sap-hana-2
- ibm-sles-15-4-amd64-sap-hana-1

For both server instances there are:

- Two SSH keys are configured to access SSH as `root`.
- Three storage volumes as described in the `input.auto.tfvars` file.

What is created for anydb

The scripts use the information that you provide for an existing VPC and deploy AAS to SAP HANA or AnyDB on a different host than CI (SAP Central Instance) VSI host. For more information about this architecture, see [SAP NetWeaver 7.x on UNIX with HANA or AnyDB on IBM Cloud](#)

[VPC on IBM Cloud VPC](#). You specify the information for the VPC to use in the `input.auto.tfvars` file.

The scripts call the Ansible Playbooks to install the SAP architecture.

Script files

The configuration and script files are provided on GitHub. Each supported interface for the SAP solution installation has its own folder in the GitHub repository:

- [GitHub repository for Terraform – AAS HANA](#)

Terraform interface

To run the Terraform script, you modify:

- The `input.auto.tfvars` file to specify the existing VPC resources for your solution. Specify the variables for the existing VPC:
 - VPC name
 - Security group
 - Subnet
 - Hostname
 - Profile
 - Image
 - Up to two SSH keys

You can change the default SAP system configuration settings to match your solution. You can also specify the location where you downloaded the SAP kits.

The IBM Cloud Provider plug-in for Terraform on IBM Cloud uses these configuration files to install AAS to SAP HANA and AnyDB on the specified VPC in your IBM Cloud account.

Support

There are no warranties of any kind, and there is no service or technical support available for these materials from IBM®. As a recommended practice, review carefully any materials that you download from this site before using them on a live system.

Though the materials provided herein are not supported by the IBM® Service organization, your comments are welcomed by the developers, who reserve the right to revise, readapt or remove the materials at any time. To report a problem, or provide suggestions or comments, open a GitHub issue.

Before you begin

Before you use the scripts in the bastion cli:

- Set up your account to access the VPC. Make sure that your account is [upgraded to a paid account](#).
- If you have not already, create a Bastion server to store the SAP kits. For more information, see [Automate SAP bastion server - SAP media storage repository](#).
- Download the SAP kits from the SAP Portal to your Deployment Server. Make note of the download locations. Ansible decompresses the files. For more information, see the [readme](#) file.
- [Create or retrieve an IBM Cloud API key](#). The API key is used to authenticate with the IBM Cloud platform and to determine your permissions for IBM Cloud services.
- [Create or retrieve your SSH key ID](#). You need the 40-digit UUID for the SSH key, not the SSH key name.
- Terraform should already be installed on the bastion server that you deployed. For more information, see [Bastion server for SAP deployment](#).
- (Optional - Catalog Tile) create secrets for your credentials and passwords by using the [Secrets Manager](#).

Deploying SAP AAS NetWeaver 7.x on HANA by using the Schematics user interface

Use these steps to configure the SAP Additional Application Server (AAS) NetWeaver with HANA or AnyDB on your existing VPC by using the Schematics interface. The script takes 2 - 3 hours to complete.

1. From the IBM Cloud menu, select **Schematics**.
2. Click **Create** workspace.

3. On the **Specify template** page:
 - Enter the URL for the Schematics interface.
 - Select the **Terraform version** that is listed in the readme file.
 - Click **Next**.
4. On the **workspace details** page:
 - Enter a name for the workspace.
 - Select a **Resource group**.
 - Select a **Location** for your workspace. The workspace location does not have to match the resource location.
 - Select **Next**.
5. Select **Create** to create your workspace.
6. On the workspace settings page, in the input variables section, review the default input variables and provide values that match your solution.
 For a more detailed description of each parameter, check the GitHub repo [AAS HANA readme](#) file, chapter "Input parameter file". Also, make sure to mark the parameters that contain sensitive information like passwords, API, and ssh private keys as "sensitive". These parameters are marked as "sensitive" in the readme file, under "Input parameter file".
7. On the workspace settings page, click **Generate plan**. Wait for the plan to complete.
8. Click **View log** to review the log files of your terraform execution plan.
9. Apply your Terraform template by clicking **Apply plan**.
10. Review the log file to ensure that no errors occur during the provisioning, modification, or deletion process.

Deploying SAP AAS NetWeaver (ABAP) on HANA with the Deployable Architecture tile interface

Use these steps to configure the SAP AAS NetWeaver (ABAP) on HANA on your existing VPC by using the catalog tile interface. The script takes 2 - 3 hours to complete.

1. From the IBM Cloud catalog, select **VPC with Additional Application Server ABAP on Linux for SAP HANA** on HANA tile. The **Create** tab opens for VPC with Additional Application Server ABAP on Linux for SAP HANA. For more information about this deployment, see the About tab or the readme file link.
2. Select the latest version.
3. Select **VPC with Additional Application Server ABAP on Linux for SAP HANA on Deployable Architecture tile** variation.
4. Click **Review deployment** options:
 - **Add to project** to add this deployment to an IBM Cloud project and combine it with other deployments. IBM Cloud projects include several more pipeline steps before deployment, including deployment validation, cost calculation, compliance verification, and approval process.
 - **Create from the CLI** to get the CLI command. With this command you can trigger the deployment from the CLI.
 - **Work with code** to embed the code into other terraform deployments.
 - **Deploy with IBM Cloud Schematics** to trigger the deployment process directly.
5. Select **Deploy with IBM Cloud Schematics**.
6. Add the input parameters for this installation. There are 3 categories of parameters:
 - **Workspace** - These parameters define the workspace that is automatically created in Schematics:
 - Enter a name for the workspace or use the default name.
 - The Resource Group used to create resources. Use default or create a Resource Group.
 - Select a location to create your Schematics workspace. The workspace location need not match the resource location.
 - **Required input variables** - Review the default input variables and provide values that match your solution. These parameters are specific to your deployment. For more detailed information, see the [Readme file](#).

Parameter	Description
BASTION_FLOATING_IP	Required only for Schematics Deployments. The Floating IP from the Bastion Server.

HOSTNAME	The hostname for the VSI. The hostname should be up to 13 characters as required by SAP. For more information on the rules regarding hostnames for SAP systems, check SAP Note 611361: Hostnames of SAP ABAP Platform servers
REGION	The cloud region to deploy the solution. The regions and zones for VPC are listed here . Review supported locations in IBM Cloud Schematics here . Sample value: eu-de.
RESOURCE_GROUP	The name of an existing Resource Group for VSIs and Volumes resources. Default value: "Default". The list of Resource Groups is available here .
SECURITY_GROUP	The name of an existing Security group. The list of security groups is available here .
SSH_KEYS	The list of SSH Keys UUIDs that are allowed to SSH as root to the VSI can contain one or more IDs. The list of SSH Keys is available here . Sample input (use your own SSH UUIDs from IBM Cloud){: external}: ["r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a", "r010-3fcfd9fe7-d4a7-41ce-8bb3-d96e936b2c7e"]
SUBNET	The name of an existing subnet. The list of subnets is available here .
VPC	The name of an existing VPC. The list of VPCs is available here .
ZONE	The cloud zone where to deploy the solution. Sample value: eu-de-2.
ibmcloud_api_key	IBM Cloud API key (Sensitive* value).
private_ssh_key	Required only for Schematics Deployments - Input your id_rsa private key pair content in OpenSSH format (Sensitive* value). This private key should be used only during the terraform provisioning and it is recommended to be changed after the SAP deployment.
hdb_instance_number	The instance number of the SAP HANA database server.
sap_aas_instance_number	Technical identifier for the internal processes of the additional application server.
sap_asci_instance_number	Technical identifier for the internal processes of ASCS.
sap_ci_host	IP address of the existing SAP Central Instance.
sap_ci_hostname	The hostname of the existing SAP Central Instance.
sap_ci_instance_number	Technical identifier for the internal processes of the Central Instance.
sap_sid	The SAP system ID identifies the entire SAP system.
sap_main_password	Common password for all users that are created during the installation (See Obs*).

Required Variables

- **Optional variables** - Review and update the optional input variables. The Ansible scripts expect the SAP kits to be in the default locations listed. For more information, see the [Readme file - Input Parameters](#).

Parameter	Description
ID_RSA_FILE_PATH	The file path for private_ssh_key is automatically generated by default. If it is changed, it must contain the relative path from Git repo folders. Default value: "ansible/id_rsa".
IMAGE	The OS image used for the VSI. A list of images is available here .
PROFILE	The profile used for the VSI. A list of profiles is available here . For more information about supported DB/OS and IBM Gen 2 Virtual Server Instances (VSI), check SAP Note 2927211: SAP Applications on IBM Virtual Private Cloud .

VOL1	Volume 1 Size - The size for the disks in GB that are to be attached to the VSI and used by SAP.
VOL2	Volume 2 Size - The size for the disks in GB that are to be attached to the VSI and used by SAP.
kit_sapcar_file	Path to the sapcar binary, as downloaded from SAP Support Portal.
kit_swpm_file	Path to the SWPM archive (SAR), as downloaded from SAP Support Portal.
kit_saphostagent_file	Path to the SAP Host Agent archive (SAR), as downloaded from SAP Support Portal.
kit_hdbclient_file	Path to the HANA DB client archive (SAR), as downloaded from SAP Support Portal.

Optional Variables

7. Accept the license agreement.
8. Select **Deploy**. The deployment starts and you are directed to the Schematics page that displays the script log files for you to monitor the deployment progress.

Creating the infrastructure using Terraform with the bastion server CLI

Use these steps to configure the IBM Cloud Provider plug-in and use Terraform to install SAP AAS to SAP HANA and AnyDB on your existing VPC on an already deployed SAP NetWeaver 7.X with SAP HANA 2.0 or ASE SYB as a Central Instance.

The script takes 1 - 2 hours to complete.

1. Access the bastion server cli.
2. Clone the solution repository and change to the folder.

ASE SYB 16 Clone the solution repository from <https://github.com/IBM-Cloud/sap-aas-abap-ase-syb> and cd to the sap-aas-abap-ase-syb/cli folder.

```
$ git clone https://github.com/IBM-Cloud/sap-aas-abap-ase-syb
cd sap-aas-abap-ase-syb/cli/
```

SAP HANA 2.0: Clone the solution repository from <https://github.com/IBM-Cloud/sap-abap-hana-aas> and cd to the sap-abap-hana-aas folder.

```
$ git clone https://github.com/IBM-Cloud/sap-abap-hana-aas.git
cd sap-abap-hana-aas/
```

3. Modify the `input.auto.tfvars` file to specify the information for the existing VPC, your region, zone, networking component names, hostname for the AAS VSI,profile, and image. You need your 40-digit SSH key ID for this file. The second SSH key is optional. For more options for profile, see [Instance Profiles](#). For more options, see [Images](#). For descriptions of the variables, see the [readme](#) file.

The VSI OS images that are supported for this solution for Netweaver Additional Application Server are:

- ibm-redhat-8-4-amd64-sap-applications-2
- ibm-redhat-8-6-amd64-sap-applications-2
- ibm-sles-15-3-amd64-sap-applications-2
- ibm-sles-15-4-amd64-sap-applications-4

```
$ # Infra VPC variables for ASE SYB
REGION    = "eu-de"
ZONE      = "eu-de-2"
VPC       = "ic4sap"                      # EXISTING Security group name
SECURITY_GROUP = "ic4sap-securitygroup"     # EXISTING Security group name
RESOURCE_GROUP = "wes-automation"
SUBNET    = "ic4sap-subnet"                 # EXISTING Subnet name
SSH_KEYS   = [ "r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a" , "r010-3fcfd9fe7-d4a7-41ce-8bb3-
d96e936b2c7e" ]

# SAP AAS VSI variables:
```

```

HOSTNAME = "sapnwase-as01"
PROFILE = "bx2-4x16"
IMAGE = "ibm-redhat-8-4-amd64-sap-applications-2

$ # Infra VPC variables for ABAP HANA
REGION      = "eu-de"
ZONE        = "eu-de-2"
VPC          = "ic4sap" # EXISTING Security group name
SECURITY_GROUP = "ic4sap-securitygroup" # EXISTING Security group name
RESOURCE_GROUP = "wes-automation"
SUBNET       = "ic4sap-subnet" # EXISTING Subnet name
SSH_KEYS     = [ "r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a" , "r010-3fc9fe7-d4a7-41ce-8bb3-d96e936b2c7e" ]
ID_RSA_FILE_PATH = "ansible/id_rsa"

# SAP AAS variables:
HOSTNAME = "sapnwapp"
PROFILE = "bx2-4x16"
IMAGE = "ibm-redhat-8-6-amd64-sap-applications-2"

```

4. Customize your SAP system configuration. In the same file, input.auto.tfvars, edit the SAP system configuration variables that are passed to the Ansible automated deployment. For descriptions of the variables, see the [readme](#) file.

```

$ # SAP system configuration - for ASE SYB
sap_sid = "NWD"
sap_ci_host = "10.243.132.10"
sap_ci_hostname = "sapnwase"
sap_ci_instance_number = "00"
sap_asc_s_instance_number = "01"
sap_aas_instance_number = "00"

# Kits paths
kit_sapcar_file = "/storage/NW75SYB/SAPCAR_1010-70006178.EXE"
kit_swpm_file = "/storage/NW75SYB/SWPM10SP31_7-20009701.SAR"
kit_saphotagent_file = "/storage/NW75SYB/SAPHOSTAGENT51_51-20009394.SAR"

```

```

$ # SAP system configuration - for ABAP HANA
sap_sid = "NWD"
sap_ci_host = "10.243.132.10"
sap_ci_hostname = "sapnwapp01"
sap_ci_instance_number = "00"
sap_asc_s_instance_number = "01"
hdb_instance_number = "00"
sap_aas_instance_number = "00"

# Kits paths
kit_sapcar_file = "/storage/NW75HDB/SAPCAR_1010-70006178.EXE"
kit_swpm_file = "/storage/NW75HDB/SWPM10SP31_7-20009701.SAR"
kit_saphotagent_file = "/storage/NW75HDB/SAPHOSTAGENT51_51-20009394.SAR"
kit_hdbclient_file = "/storage/NW75HDB/IMDB_CLIENT20_009_28-80002082.SAR"

```

Ansible decompresses the rest of the SAP kit files. For more information, see the [readme](#) file.

5. Initialize the Terraform CLI.

```
terraform init
```

6. Create a Terraform execution plan. The Terraform execution plan summarizes all the actions that are done to create the virtual private cloud instance in your account.

```
terraform plan plan1
```

Enter an SAP main password and your API key.

The SAP main password must be 10 - 14 characters long and contain at least one digit (0-9). It can contain only the following characters: a-z, A-Z, 0-9, @, #, \$, . *This password cannot contain exclamation points '!'. The password must not start with a digit or an underscore ().*

7. Verify that the plan shows all of the resources that you want to create and that the names and values are correct. If the plan needs to be adjusted, edit the input.auto.tfvars file to correct resources and run terraform plan again.
8. Apply the saved plan.

```
$ terraform apply "plan1"
```

The virtual private cloud and components are created and you see output similar to the `terraform plan` output.

9. Add the SAP credentials and the virtual server instance IP to the SAP GUI. For more information about the SAP GUI, see [SAP GUI](#).

Next steps

If you need to rename your resources after they are created, modify the `input.auto.tfvars` file to change the names and run `terraform plan` and `terraform apply` again. Do not use the IBM Cloud Dashboard and user interface to modify your VPC after it is created. The Terraform scripts create a complete solution and selectively modifying resources with the user interface might cause unexpected results.

If you need to remove the SAP Netweaver 7.X on HANA or AnyDB installation, go to your project folder and run `terraform destroy`. The `terraform destroy` command does not remove the VPC in this scenario because the VPC was created before these Terraform scripts were run.

Related information

For more information about Terraform on IBM Cloud, see [Getting started with Terraform on IBM Cloud](#).

For more information about using Terraform for creating only a VPC for SAP, without the SAP architecture, see [Creating single-tier virtual private cloud for SAP by using Terraform](#).

SAP One Support Notes that apply to this document:

- [SAP Note 84555 - Windows Server, Linux®, and UNIX: Certified hardware](#)
- [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#)
- [SAP Note 2923773 - Linux® on IBM Cloud \(IaaS\): Adaption of your SAP license](#)
- [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#)
- [SAP Note 2369910 - SAP Software on Linux®: General information](#)
- [SAP Note 171380 - Released IBM hardware \(Intel processors\) and IBM cloud services offers](#)
- [SAP Note 1380654 - SAP support in IaaS environments](#)

This document is referenced by:

- [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#)
- [SAP Note 2588225 - SAP on IBM Cloud: Protect against speculative execution vulnerabilities](#)
- [SAP Note 1380654 - SAP support in IaaS environments](#)
- [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#)

SAP BW/4HANA 3-tier in VPC

Automating SAP workload HA deployment on IBM Cloud VPC with Terraform and Ansible

You can use Terraform to automate IBM Cloud® VPC provisioning. The VPC provisioned includes virtual server instances with high network performance. The VPC infrastructure contains various Infrastructure-as-a-Service (IaaS) offerings, including virtual servers. After the VPC is provisioned, the scripts use the Ansible Playbooks to install the SAP system.

IBM Cloud VPC introduction

VPC is a public cloud offering that an enterprise uses to establish its own private cloud-like computing environment on shared [public cloud](#) infrastructure. VPC gives an enterprise the ability to define and control a virtual network that is logically isolated from all other public cloud tenants, creating a private and secure place on the public cloud.

Imagine that a cloud provider's infrastructure is a residential apartment building and multiple families live inside. A public cloud tenant is a kind of sharing an apartment with a few roommates. In contrast, having a VPC is like having your own private condominium; no one else has the key, and no one can enter the space without your permission.

VPC's logical isolation is implemented by using virtual network functions and security features that give the enterprise customer granular control over which IP addresses or applications can access particular resources. It is analogous to the "friends-only" or "public/private" controls on social media accounts used to restrict who can or can't see your otherwise public posts.

With IBM Cloud VPC, you can use the UI, CLI, and API to manually provision virtual server instances for VPC with high network performance. VPC infrastructure contains various Infrastructure-as-a-Service (IaaS) offerings including virtual servers for VPC.

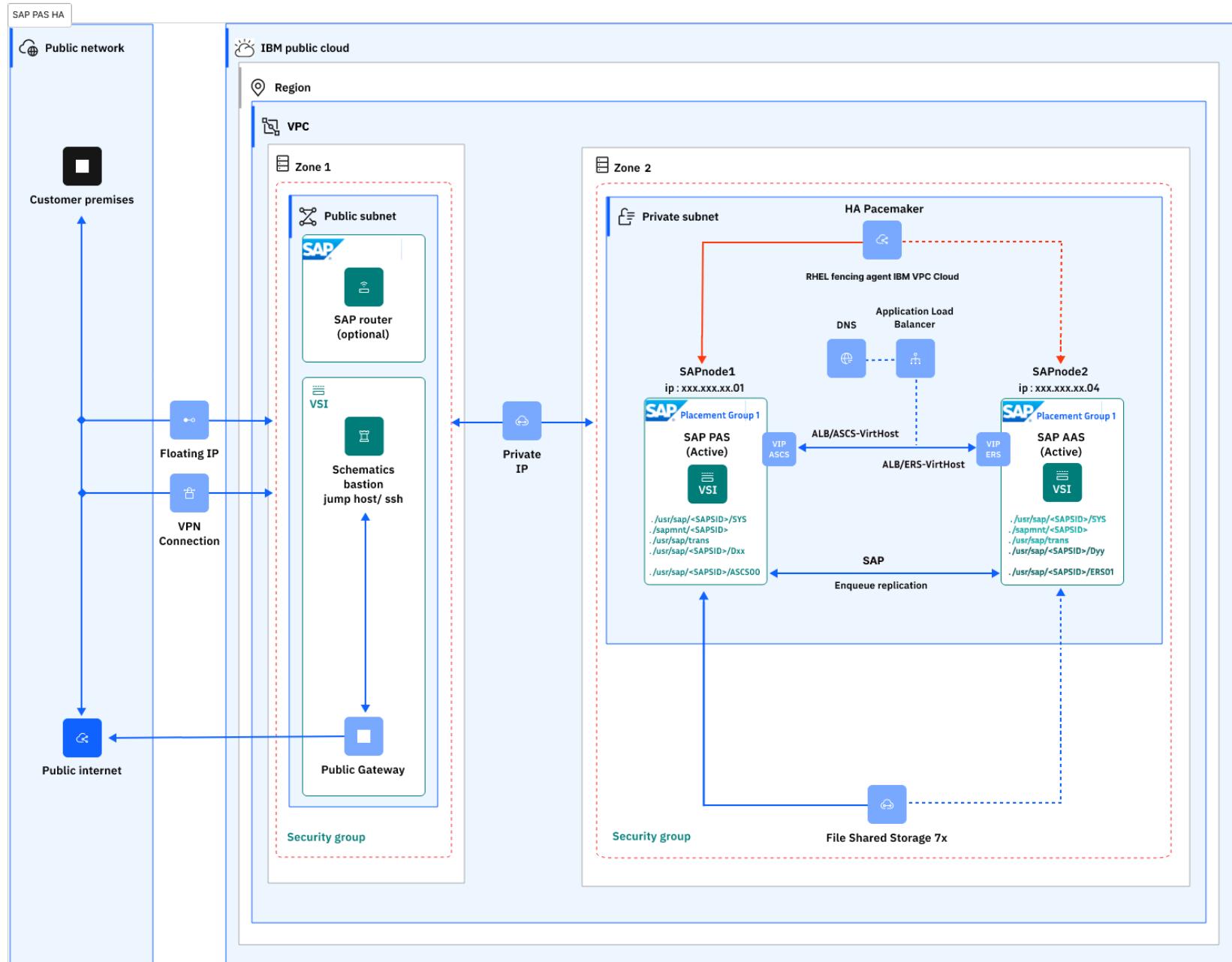
Use the following information to understand a simple use-case for planning, creating, and configuring resources for your VPC, and learn more about VPC overviews and VPC tutorials. For more information about the VPC, see [Getting started with Virtual Private Cloud \(VPC\)](#).

SAP products architecture on IBM Cloud VPC

A [Virtual Private Cloud \(VPC\)](#) contains one of the most secure and reliable cloud environments for SAP applications within your own VPC with virtual server instances. This represents an Infrastructure-as-a-Service (IaaS){: external} within IBM Cloud that offers all the benefits of isolated, secure, and flexible virtual cloud infrastructure from IBM. In comparison, the IBM Cloud classic infrastructure virtual servers offering uses virtual instances with native and VLAN networking to communicate with each other within a data center; however, the instances are restricted in one well-working pod by using subnet and VLAN networking as a gap scale up of virtual resources should rely between the pods. The IBM Cloud VPC network orchestrator layer concept eliminates the pod boundaries and restrictions, so this new concept handles all the networking for every virtual instance running within VPC across regions and zones.

Highly available system for SAP NetWeaver on IBM Cloud VPC

In a Highly Available (HA) system, every instance can run on a separate IBM Cloud virtual server instance. The cluster HA configuration for the SAP application server consists of two virtual server instances, each of them located in the same zone within the region by using placement groups. Placement groups assure that both cluster resources and cloud resources are also located in different compute nodes as specified in the following placement groups section:



SAP HA for SAP applications cluster nodes PAS (Active) and AAS (Active)

Placement groups on IBM Cloud VPC for SAP HA architecture

Placement Groups (PG) for VPC have two different anti-affinity strategies for high availability. By using the placement strategies, you minimize the chance of service disruption with virtual server instances that are placed on different hosts or into an infrastructure with separate power and network supplies.

The design of placement groups for IBM Cloud virtual servers solves this issue. Placement groups give a measure of control over the host on which a new public virtual server is placed. In this release, a “spread” rule is implemented, which means that the virtual servers within a placement group are spread onto different hosts. You can build a highly available application within a data center and know that your virtual servers are isolated from each other.

Placement groups with the spread rule are available to create in selected IBM Cloud data centers. After a spread rule is created, you can provision a virtual server into that group and ensure that it is not on the same host as any of your other virtual servers. This feature comes with no cost.

You can create your placement group and assign up to four new virtual server instances. With the spread rule, each of your virtual servers are provisioned on different physical hosts. In the following configuration example, the “Power Spread” option is used:

Name	Status	Resource group	Placement strategy	Attached instances
sap-ppg	Stable	rh-pacemaker	Host spread	0
pgroup1	Stable	Default	Host spread	2

Placement groups host spread

Placement group for VPC					
Name	Status	Resource group	Placement strategy	Attached instances	
sapha-poc	Stable	wes-ic4sap-resourcegroup	Power spread	4	
Items per page: 10 1 item 1 of 1 page					

Placement groups power spread

Following are the SAP instances that are required for HA scenario:

- ABAP SAP Central Services (ASCS) instance - contains the ABAP message server and the ABAP enqueue server.
- Enqueue Replication Server (ERS) instance for the ASCS instance.
- Database instance
- Primary Application Server (PAS) instance on node 1.
- Additional Application Server (AAS) instance on node 2.



Note: It is recommended to run both the ASCS instance and the ERS instance in a switchover cluster infrastructure.

IBM Cloud File Storage for VPC for SAP HA architecture

[IBM Cloud File Storage for VPC](#) technology is used to make the SAP directories available to the SAP system. The technologies of choice are NFS, shared disks, and cluster file system. If you have decided to use the HA solution for your SAP system, make sure that you properly address the HA requirements of the SAP file systems in your SAP environment.

File shares for VPC								
Name	Status	Resource groups	Location	Mount targets	Size	Replication role	Encryption type	
usrsap-as1-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-as2-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-sapscs-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-sapers-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-sapmnt-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-sapsys-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-trans-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	80 GB	None	Provider managed	

File shares for VPC

- File shares that are mounted as NFS permanent file systems on both cluster nodes for SAP HA application:
 - `/usr/sap/<SAPSID>/SYS`
 - `/sapmnt<SAPSID>`
 - `/usr/sap/trans`
- Cluster-managed file systems for SAP HA application: ASCS
 - `/usr/sap/<SAPSID>/ASCS00`
 - `/usr/sap/<SAPSID>/ERS01`
- Permanent NFS mount on SAP HA application node 1 PAS instance:
 - `/usr/sap/<SAPSID>/Dxx`
- Permanent NFS mount on SAP HA application node 2 dialog instance:
 - `/usr/sap/<SAPSID>/Dyy`

Prerequisites

You need to install the hardware (hosts, disks, and network) and decide how to distribute the database, SAP instances, and if required, the Network File System (NFS) server over the cluster nodes.

Context

Following are the types of SAP directories:

- Physically shared directories: `/<sapmnt>/<SAPSID>` and `/usr/sap/trans`

- Logically shared directories that are bound to a node, such as `/usr/sap`, with the following local directories:
 - `/usr/sap/<SAPSID>`
 - `/usr/sap/<SAPSID>/SYS`
 - `/usr/sap/hostctrl`
- Local directories that contain the SAP instances such as `/usr/sap/<SAPSID>/ASCS<Instance_Number>`
- The global transport directory may reside on a separate SAP transport host as a standard three systems transport layer configuration.

You need at least two nodes and a shared file system for distributed ASCS and ERS instances. The assumption is that the rest of the components are distributed on other nodes.

ASCS and ERS installation

In order for the ASCS and ERS instances to be able to move from one node to the other, they need to be installed on a shared file system and use virtual hostnames based on the virtual IP.

In this VPC-based SAP HA solution, the shared file system that is required by the cluster is replaced by the NFS-mounted file storage, and the virtual IP is replaced by the Application Load Balancer for VPC (ALB).

In this scenario, three ALBs are used, one for each Single Point of Failure (SPOF) component in order to replace the virtual IP requirement: ALB for ASCS, ALB for ERS, and ALB for ASE Sybase. Each ALB is configured as a backend for the corresponding cluster servers and redirects all of the communication that is received on the front-end ports to the active server in the backend pool.

Load balancers for VPC						
Region:	Frankfurt	▼	Search: poc	X		
Name	Status	Family	Resource group	Type	Hostname	Location
db-alb-hana-poc	Active	Application	wes-ic4sap-resourcegroup	Private	20bdd130-eu-de.lb.appdomain.cloud	Frankfurt
sap-alb-ers-poc	Active	Application	wes-ic4sap-resourcegroup	Private	3941d983-eu-de.lb.appdomain.cloud	Frankfurt
sap-alb-ascs-poc	Active	Application	wes-ic4sap-resourcegroup	Private	56a9190d-eu-de.lb.appdomain.cloud	Frankfurt

Application load balancer management of HA IPs mechanism

Private application load balancer

A [private application load balancer](#) is accessible through your private subnets that you configured to create the load balancer.

Similar to a public application load balancer, your private application load balancer service instance is assigned an FQDN; however, this domain name is registered with one or more private IP addresses.

IBM Cloud operations change the number and value of your assigned private IP addresses over time, based on maintenance and scaling activities. The backend virtual server instances that host your application must run in the same region and under the same VPC.

Use the assigned ALB FQDN to send traffic to the private application load balancer to avoid connectivity problems to your applications during system maintenance or scaling down activities.

Each ALB sends traffic to the cluster node where the application (ASCS, ERS, ASE Sybase DB) is running. During the cluster failover, the ALB redirects all the traffic to the new node where the resources are up and running.



Note: DNS-as-a-Service (DNSaaS) is the management IBM Cloud VPC DNS service of HA and FQDN (IPs) mechanism.



Note: The ALB has a default of 50 seconds for client and server timeout, so after 50 seconds of inactivity, the connection is closed. To support SAP connections through ALB and not lose connection after 50 seconds, you need to request a change this value to a minimum of 300 seconds (client-side idle connection = minimum 300s and server-side idle connection = minimum 300s). To request this change, open a support ticket. This is an account-wide change that affects all of the ALBs in your account. For more information, see [Connection timeouts](#).

DNS Services with VPC

[IBM Cloud DNS Services](#) provide private DNS to VPC users. Private DNS zones are resolvable only on IBM Cloud and from explicitly [permitted networks](#) in an account. To get started, create a DNS Services instance by using the IBM Cloud console.

DNS Services allows you to:

- Create the private DNS zones that are collections for holding the domain names.
- Create the DNS resource records under these DNS zones.
- Specify the access controls used for the DNS resolution of resource records on a zone-wide level.

DNS Services also maintains its own worldwide set of DNS resolvers. Instances that are provisioned under IBM Cloud on an IBM Cloud network can use resource records that are configured through IBM Cloud DNS Services by querying DNS Services resolvers.

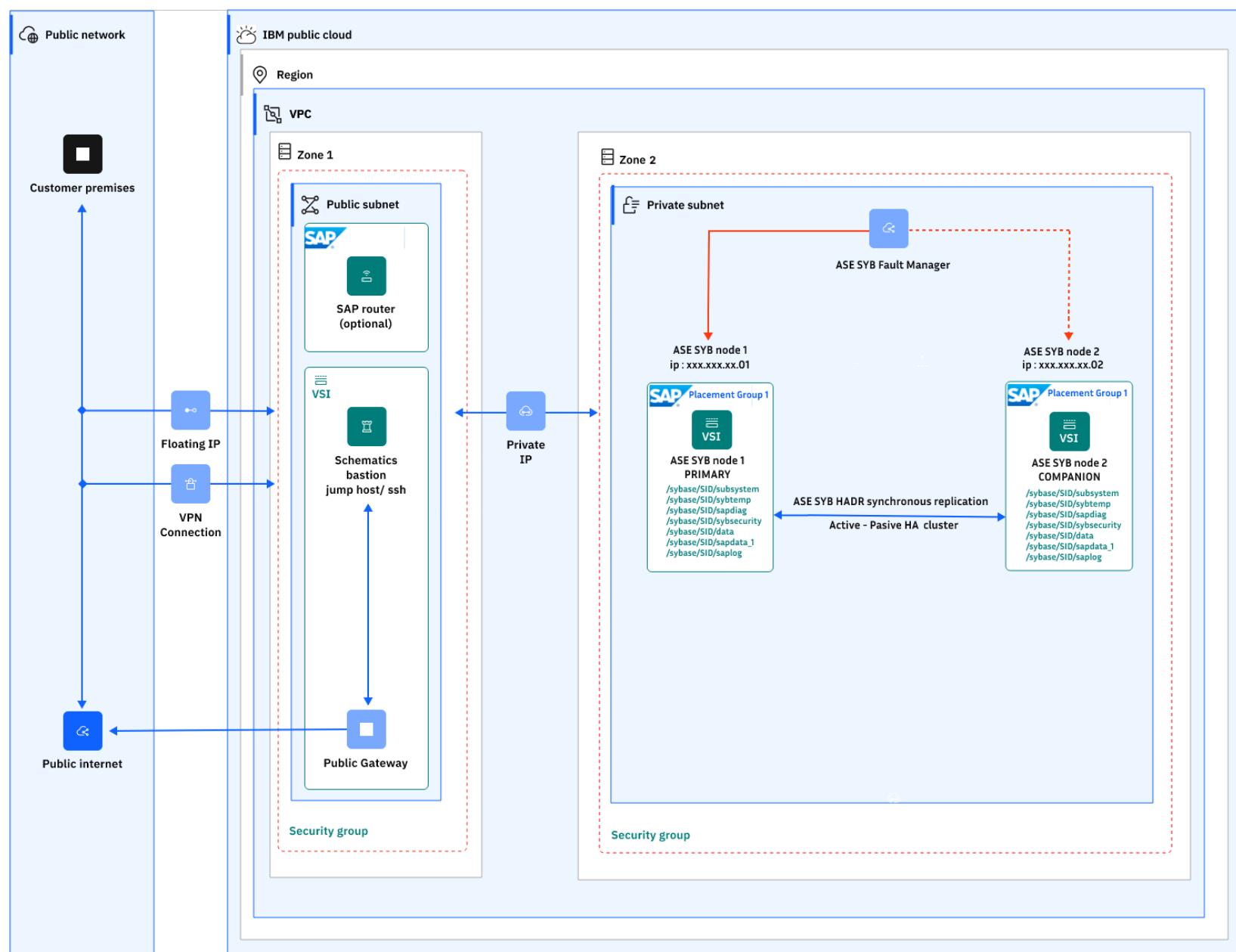
Resource records and zones that are configured through DNS Services are:

- Separated from the wider public DNS, and their publicly accessible records.
- Hidden from the system outside of and not part of the IBM Cloud private network.
- Accessible only from the system that you authorize on the IBM Cloud private network.
- Resolvable only via the resolvers provided by the service.

The DNS service maps the FQDN of each ALB to the virtual hostnames of the ASCS, ERS, and ASE Sybase that are used by SAP applications.

Type	Name	Value	TTL
CNAME	dbpochana	is an alias of 20bdd130-eu-de.lb.appdomain.cloud	12 hr
CNAME	sappocers	is an alias of 3941d983-eu-de.lb.appdomain.cloud	12 hr
CNAME	sappocases	is an alias of 56a9190d-eu-de.lb.appdomain.cloud	12 hr

Highly available system for SAP ASE Sybase database with HADR system



SAP HA for ASE Sybase DB instances cluster nodes primary (Active) and Secondary (Companion)

At the most basic level, a standard HA ASE Sybase cluster in an active(primary)-passive(companion) configuration has two nodes: one is the primary node and the other is the standby node. This means that the primary node is actively serving the active SAP DB instances (Primary and Companion), while the standby node is waiting to jump in if there is any failure.

The cluster is set with a virtual hostname IP (hostname is mapped to the FQDN of the ASE Sybase ALB through DNS, which is the same as

explained previously for SAP ASCS and ERS instances). Application instances (PAS and AAS) are used on the SAP profiles to call that particular component. The cluster assigns the virtual IP to the active node and uses a heartbeat monitor to confirm the availability of the components. If the primary node stops responding, it triggers the automatic failover mechanism that calls the standby node to step up to become the primary node. The ALB detects the change, redirects the traffic to the new active node, and assigns the virtual IP to it, restoring the component availability. Once fixed, the failed node comes online as a standby node.

SAP Sybase HADR system supports synchronous replication

The SAP Sybase HADR system supports synchronous replication between the primary and standby servers for high availability. An active-active setup is a two-node configuration where both nodes in the cluster include SAP ASE managing independent workloads, capable of taking over each others workload in the event of a failure.

The SAP ASE server that takes over the workload is called a secondary companion, and the SAP ASE server that fails is called the primary companion. Together they are companion servers. This movement from one node to another is called failover. After the primary companion is ready to resume its workload, it is moved back to its original node. This movement is called a failback.

When a system fails over, clients that are connected to the primary companion and use the failover property automatically reestablish their network connections to the secondary companion. You must tune your operating system to successfully manage both servers during fail over. See your operating system documentation for information about configuring your system for high availability. An SAP ASE configured for failover in an active-active setup can be shut down using the shutdown command only after you have suspended SAP ASE from the companion configuration, at both the server level and the platform level.

The always-on option in a High Availability and Disaster Recovery (HADR) system consists of two SAP ASE servers:

- Primary on which all transaction processing takes place.
- Warm standby (referred to as a "standby server" in DR mode, and as a "companion" in HA mode) for the primary server, and contains copies of designated databases from the primary server.



Note: The HADR feature that is shipped with SAP ASE version 16.0 SP02 supports only a single-companion server.

Some high-availability solutions (for example, the SAP Adaptive Server Enterprise Cluster Edition) share or use common resources between nodes. However, the HADR system is a "shared nothing" configuration, each node has separate resources including disks.

In an HADR system, servers are separate entities and data is replicated from the primary server to the companion server. If the primary server fails, a companion server is promoted to the role of primary server either manually or automatically. Once the promotion is complete, clients can reconnect to the new primary server, and see all committed data, including data that was committed on the previous primary server.

Servers can be separated geographically, which makes an HADR system capable of withstanding the loss of an entire computing facility.



Note: The HADR system includes an embedded SAP Replication Server, which synchronizes the databases between the primary and companion servers. SAP ASE uses the Replication Management Agent (RMA) to communicate with Replication Server and SAP Replication Server uses Open Client connectivity to communicate with the companion SAP ASE.

The Replication Agent detects any data changes made on the primary server and sends them to the primary SAP Replication Server. In the figure above, the unidirectional arrows indicate that, although both SAP Replication Servers are configured, only one direction is enabled at a time.

The HADR system supports synchronous replication between the primary and standby servers for high availability so the two servers can keep in sync with Zero Data Loss (ZDL). This requires a network link that is fast enough between the primary and standby server so that synchronous replication can keep up with the primary servers workload. Generally, this means that the network latency is approximately the same speed as the local disk IO speed, a few (fewer than 10) milliseconds. Anything longer than a few milliseconds may result in a slower response to write operations at the primary.

The HADR system supports asynchronous replication between the primary and standby servers for disaster recovery. The primary and standby servers by using asynchronous replication can be geographically distant, meaning they can have a slower network link. With asynchronous replication, Replication Agent Thread captures the primary servers workload, which is delivered asynchronously to SAP Replication Server. The SAP Replication Server applies these workload change to the companion server.

The most fundamental service that is offered by the HADR system is the failover; planned or unplanned from the primary to the companion server, which allows maintenance activity to occur on the old primary server, while applications continue on the new primary.

The HADR system provides protection in the event of a disaster. If the primary server is lost, the companion server can be used as a replacement. Client applications can switch to the companion server, and the companion server is quickly available for users. If the SAP Replication Server was in synchronous mode before the failure of the primary server, the Fault Manager automatically initiates failover with

zero data loss.

Fault Manager installation on the SAP ASCS node

The required parameters are asked during the installation process to create a profile for the fault manager and then adds it to the instance start profile. It is also possible to run the installation by using an existing profile: `sybdbfm install pf=<SYBHA.PFL>` In this case, the installation process will only ask for profile parameters missing in the profile.



Note: Fault manger is integrated with ASCS on same SAP PAS/AAS cluster (start/stop/move together).

There may be some data loss if the SAP Replication Server was in asynchronous mode and you must use manual intervention to failover for disaster recovery.

Connection attempts to the companion server without the necessary privileges are silently redirected to the primary companion via the login redirection mechanism, which is supported by Connectivity libraries. If login redirection is not enabled, client connections fail and are disconnected.

The SAP ASE HADR option installs the below components:

- SAP ASE
- SAP Replication Server
- Replication Management Agent (RMA)
- SAP Host Agent
- Fault Manager
- SAP ASE Cockpit



Note: This automation is offered at no cost; however, the provisioned infrastructure comes at cost.

VPC with Additional Application Server (AAS) ABAP on Linux for SAP HANA

You can use Terraform scripts to create a single-tier VPC and create the AAS to HANA and AnyDB infrastructure on the VPC. The Terraform scripts use the VPC information that you provide and then call the Ansible playbook to create the SAP architecture on the specified VPC. Terraform on IBM Cloud® enables predictable and consistent provisioning of IBM Cloud Virtual Private Cloud (VPC) infrastructure resources so that you can rapidly build complex, cloud environments. IBM Cloud VPC infrastructure consists of SAP certified hardware that uses Intel® Xeon CPUs and more Intel® technologies.

You have two deployment methods to choose from:

- Terraform scripts that run from the CLI on your bastion server.
- Schematics user interface accessed from your cloud dashboard menu.

You can create SAP AAS NetWeaver 7.x on the SAP HANA-based ABAP stack.

SAP solution implemented

Many SAP enterprise solutions are built on the SAP platform (SAP NetWeaver) including:

- SAP HANA as Primary Persistence for SAP NetWeaver-based applications
- SAP Business Suite applications (ERP, CRM, and SCM, and other applications),
- SAP Business Warehouse (BW), and
- Other SAP enterprise solutions

SAP NetWeaver has two distinct aspects, ABAP and Java. Many applications that are built on the SAP NetWeaver's ABAP or Java (or both) application servers run on SAP DB owned HANA and ASE Sybase either in AnyDB platforms (MSSQL, Oracle, and Db2).

Technical interfaces are available for applications that are built on the SAP NetWeaver AS ABAP and AS Java to run on SAP HANA and AnyDB. However, specific development enablement is normally required for each application to ensure that it runs optimally on the SAP HANA. SAP Business Suite applications (ERP, CRM, SCM, and other applications), SAP Business Warehouse (BW), and other SAP NetWeaver-based applications were modified to run on SAP HANA and have many advantages. Also, various components and complimentary applications that are built on SAP NetWeaver can also run on SAP HANA or AnyDB by using the provided SAP NetWeaver DB interfaces.

The SAP HANA as primary persistence for SAP NetWeaver-based applications scenario has one restriction: SAP NetWeaver ABAP and Java

application servers must run on separate hardware servers from the SAP HANA hardware.

What is created

The scripts automate the virtual infrastructure resources, provisioning the processes for the SAP architecture in an existing VPC with a distributed environment. SAP AAS NetWeaver 7.x (HANA or ASE SYB) application server on a distinct VSI VPC system and SAP HANA DB on a dedicated server type VSI VPC box are provisioned. The scripts work in two phases.

During the first phase of [Automate SAP bastion server – SAP media storage repository](#), the following virtual infrastructure resources based on the components from the existing VPC created by the bastion server are:

- 1 VPC where the virtual server instance is provisioned.
- 1 security group. The rules for this security group are:
 - Allow inbound DNS traffic (port 53).
 - Allow inbound SSH traffic (TCP port 22).
 - Allow all outbound traffic from the virtual server instance.
 - Allow all traffic in the security group.
- 1 subnet to enable the networking in your VPC.
- 2 virtual server instances with SAP certified storage and network configurations.
- 1 floating IP address used to access your VPC virtual server instance over the public network.

During the second phase, the Ansible Playbooks is called and the SAP architecture is installed for both dedicated virtual server instance (VSI) SAP application; VSI system and dedicated SAP HANA VSI box. The SAP architecture that is deployed on the SAP NetWeaver 7.x release is a stand-alone dedicated SAP HANA 2.0 box release. For more information about this architecture, see [Automating SAP HANA stand-alone virtual server instance on IBM Cloud® VPC by using Terraform and Ansible](#).

You can provision only one instance of the service per IBM Cloud region.

Schematics deployment

When you run the scripts with the Schematics interface, you:

- Enter the workspace information.
- Enter the GitHub path for the chosen solution either on NetWeaver AAS for HANA.
- Modify the parameters in the Schematics interface. They are the same parameters as the `input.auto.tfvars` file that you use with the cli.

Virtual server instance configuration

Following are the supported operating system images for SAP NetWeaver primary application server:

- ibm-redhat-8-4-amd64-sap-applications-2
- ibm-redhat-8-6-amd64-sap-applications-2
- ibm-sles-15-3-amd64-sap-applications-2
- ibm-sles-15-4-amd64-sap-applications-3

Following are the supported operating system images for SAP HANA database:

- ibm-redhat-8-4-amd64-sap-hana-2
- ibm-redhat-8-6-amd64-sap-hana-2
- ibm-sles-15-3-amd64-sap-hana-2
- ibm-sles-15-4-amd64-sap-hana-1

For both server instances there are:

- Two SSH keys are configured to access SSH as `root`.
- Three storage volumes as described in the `input.auto.tfvars` file.

What is created for anydb

The scripts use the information that you provide for an existing VPC and deploy AAS to SAP HANA or AnyDB on a different host than CI (SAP Central Instance) VSI host. For more information about this architecture, see [SAP NetWeaver 7.x on UNIX with HANA or AnyDB on IBM Cloud](#)

[VPC on IBM Cloud VPC](#). You specify the information for the VPC to use in the `input.auto.tfvars` file.

The scripts call the Ansible Playbooks to install the SAP architecture.

Script files

The configuration and script files are provided on GitHub. Each supported interface for the SAP solution installation has its own folder in the GitHub repository:

- [GitHub repository for Terraform – AAS HANA](#)

Terraform interface

To run the Terraform script, you modify:

- The `input.auto.tfvars` file to specify the existing VPC resources for your solution. Specify the variables for the existing VPC:
 - VPC name
 - Security group
 - Subnet
 - Hostname
 - Profile
 - Image
 - Up to two SSH keys

You can change the default SAP system configuration settings to match your solution. You can also specify the location where you downloaded the SAP kits.

The IBM Cloud Provider plug-in for Terraform on IBM Cloud uses these configuration files to install AAS to SAP HANA and AnyDB on the specified VPC in your IBM Cloud account.

Support

There are no warranties of any kind, and there is no service or technical support available for these materials from IBM®. As a recommended practice, review carefully any materials that you download from this site before using them on a live system.

Though the materials provided herein are not supported by the IBM® Service organization, your comments are welcomed by the developers, who reserve the right to revise, readapt or remove the materials at any time. To report a problem, or provide suggestions or comments, open a GitHub issue.

Before you begin

Before you use the scripts in the bastion cli:

- Set up your account to access the VPC. Make sure that your account is [upgraded to a paid account](#).
- If you have not already, create a Bastion server to store the SAP kits. For more information, see [Automate SAP bastion server - SAP media storage repository](#).
- Download the SAP kits from the SAP Portal to your Deployment Server. Make note of the download locations. Ansible decompresses the files. For more information, see the [readme](#) file.
- [Create or retrieve an IBM Cloud API key](#). The API key is used to authenticate with the IBM Cloud platform and to determine your permissions for IBM Cloud services.
- [Create or retrieve your SSH key ID](#). You need the 40-digit UUID for the SSH key, not the SSH key name.
- Terraform should already be installed on the bastion server that you deployed. For more information, see [Bastion server for SAP deployment](#).
- (Optional - Catalog Tile) create secrets for your credentials and passwords by using the [Secrets Manager](#).

Deploying SAP AAS NetWeaver 7.x on HANA by using the Schematics user interface

Use these steps to configure the SAP Additional Application Server (AAS) NetWeaver with HANA or AnyDB on your existing VPC by using the Schematics interface. The script takes 2 - 3 hours to complete.

1. From the IBM Cloud menu, select **Schematics**.
2. Click **Create** workspace.

3. On the **Specify template** page:
 - Enter the URL for the Schematics interface.
 - Select the **Terraform version** that is listed in the readme file.
 - Click **Next**.
4. On the **workspace details** page:
 - Enter a name for the workspace.
 - Select a **Resource group**.
 - Select a **Location** for your workspace. The workspace location does not have to match the resource location.
 - Select **Next**.
5. Select **Create** to create your workspace.
6. On the workspace settings page, in the input variables section, review the default input variables and provide values that match your solution.
 For a more detailed description of each parameter, check the GitHub repo [AAS HANA readme](#) file, chapter "Input parameter file". Also, make sure to mark the parameters that contain sensitive information like passwords, API, and ssh private keys as "sensitive". These parameters are marked as "sensitive" in the readme file, under "Input parameter file".
7. On the workspace settings page, click **Generate plan**. Wait for the plan to complete.
8. Click **View log** to review the log files of your terraform execution plan.
9. Apply your Terraform template by clicking **Apply plan**.
10. Review the log file to ensure that no errors occur during the provisioning, modification, or deletion process.

Deploying SAP AAS NetWeaver (ABAP) on HANA with the Deployable Architecture tile interface

Use these steps to configure the SAP AAS NetWeaver (ABAP) on HANA on your existing VPC by using the catalog tile interface. The script takes 2 - 3 hours to complete.

1. From the IBM Cloud catalog, select **VPC with Additional Application Server ABAP on Linux for SAP HANA** on HANA tile. The **Create** tab opens for VPC with Additional Application Server ABAP on Linux for SAP HANA. For more information about this deployment, see the About tab or the readme file link.
2. Select the latest version.
3. Select **VPC with Additional Application Server ABAP on Linux for SAP HANA on Deployable Architecture tile** variation.
4. Click **Review deployment** options:
 - **Add to project** to add this deployment to an IBM Cloud project and combine it with other deployments. IBM Cloud projects include several more pipeline steps before deployment, including deployment validation, cost calculation, compliance verification, and approval process.
 - **Create from the CLI** to get the CLI command. With this command you can trigger the deployment from the CLI.
 - **Work with code** to embed the code into other terraform deployments.
 - **Deploy with IBM Cloud Schematics** to trigger the deployment process directly.
5. Select **Deploy with IBM Cloud Schematics**.
6. Add the input parameters for this installation. There are 3 categories of parameters:
 - **Workspace** - These parameters define the workspace that is automatically created in Schematics:
 - Enter a name for the workspace or use the default name.
 - The Resource Group used to create resources. Use default or create a Resource Group.
 - Select a location to create your Schematics workspace. The workspace location need not match the resource location.
 - **Required input variables** - Review the default input variables and provide values that match your solution. These parameters are specific to your deployment. For more detailed information, see the [Readme file](#).

Parameter	Description
BASTION_FLOATING_IP	Required only for Schematics Deployments. The Floating IP from the Bastion Server.

HOSTNAME	The hostname for the VSI. The hostname should be up to 13 characters as required by SAP. For more information on the rules regarding hostnames for SAP systems, check SAP Note 611361: Hostnames of SAP ABAP Platform servers
REGION	The cloud region to deploy the solution. The regions and zones for VPC are listed here . Review supported locations in IBM Cloud Schematics here . Sample value: eu-de.
RESOURCE_GROUP	The name of an existing Resource Group for VSIs and Volumes resources. Default value: "Default". The list of Resource Groups is available here .
SECURITY_GROUP	The name of an existing Security group. The list of security groups is available here .
SSH_KEYS	The list of SSH Keys UUIDs that are allowed to SSH as root to the VSI can contain one or more IDs. The list of SSH Keys is available here . Sample input (use your own SSH UUIDs from IBM Cloud){: external}: ["r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a", "r010-3fcfd9fe7-d4a7-41ce-8bb3-d96e936b2c7e"]
SUBNET	The name of an existing subnet. The list of subnets is available here .
VPC	The name of an existing VPC. The list of VPCs is available here .
ZONE	The cloud zone where to deploy the solution. Sample value: eu-de-2.
ibmcloud_api_key	IBM Cloud API key (Sensitive* value).
private_ssh_key	Required only for Schematics Deployments - Input your id_rsa private key pair content in OpenSSH format (Sensitive* value). This private key should be used only during the terraform provisioning and it is recommended to be changed after the SAP deployment.
hdb_instance_number	The instance number of the SAP HANA database server.
sap_aas_instance_number	Technical identifier for the internal processes of the additional application server.
sap_asci_instance_number	Technical identifier for the internal processes of ASCS.
sap_ci_host	IP address of the existing SAP Central Instance.
sap_ci_hostname	The hostname of the existing SAP Central Instance.
sap_ci_instance_number	Technical identifier for the internal processes of the Central Instance.
sap_sid	The SAP system ID identifies the entire SAP system.
sap_main_password	Common password for all users that are created during the installation (See Obs*).

Required Variables

- **Optional variables** - Review and update the optional input variables. The Ansible scripts expect the SAP kits to be in the default locations listed. For more information, see the [Readme file - Input Parameters](#).

Parameter	Description
ID_RSA_FILE_PATH	The file path for private_ssh_key is automatically generated by default. If it is changed, it must contain the relative path from Git repo folders. Default value: "ansible/id_rsa".
IMAGE	The OS image used for the VSI. A list of images is available here .
PROFILE	The profile used for the VSI. A list of profiles is available here . For more information about supported DB/OS and IBM Gen 2 Virtual Server Instances (VSI), check SAP Note 2927211: SAP Applications on IBM Virtual Private Cloud .

VOL1	Volume 1 Size - The size for the disks in GB that are to be attached to the VSI and used by SAP.
VOL2	Volume 2 Size - The size for the disks in GB that are to be attached to the VSI and used by SAP.
kit_sapcar_file	Path to the sapcar binary, as downloaded from SAP Support Portal.
kit_swpm_file	Path to the SWPM archive (SAR), as downloaded from SAP Support Portal.
kit_saphostagent_file	Path to the SAP Host Agent archive (SAR), as downloaded from SAP Support Portal.
kit_hdbclient_file	Path to the HANA DB client archive (SAR), as downloaded from SAP Support Portal.

Optional Variables

7. Accept the license agreement.
8. Select **Deploy**. The deployment starts and you are directed to the Schematics page that displays the script log files for you to monitor the deployment progress.

Creating the infrastructure using Terraform with the bastion server CLI

Use these steps to configure the IBM Cloud Provider plug-in and use Terraform to install SAP AAS to SAP HANA and AnyDB on your existing VPC on an already deployed SAP NetWeaver 7.X with SAP HANA 2.0 or ASE SYB as a Central Instance.

The script takes 1 - 2 hours to complete.

1. Access the bastion server cli.
2. Clone the solution repository and change to the folder.

ASE SYB 16 Clone the solution repository from <https://github.com/IBM-Cloud/sap-aas-abap-ase-syb> and cd to the sap-aas-abap-ase-syb/cli folder.

```
$ git clone https://github.com/IBM-Cloud/sap-aas-abap-ase-syb
cd sap-aas-abap-ase-syb/cli/
```

SAP HANA 2.0: Clone the solution repository from <https://github.com/IBM-Cloud/sap-abap-hana-aas> and cd to the sap-abap-hana-aas folder.

```
$ git clone https://github.com/IBM-Cloud/sap-abap-hana-aas.git
cd sap-abap-hana-aas/
```

3. Modify the `input.auto.tfvars` file to specify the information for the existing VPC, your region, zone, networking component names, hostname for the AAS VSI,profile, and image. You need your 40-digit SSH key ID for this file. The second SSH key is optional. For more options for profile, see [Instance Profiles](#). For more options, see [Images](#). For descriptions of the variables, see the [readme](#) file.

The VSI OS images that are supported for this solution for Netweaver Additional Application Server are:

- ibm-redhat-8-4-amd64-sap-applications-2
- ibm-redhat-8-6-amd64-sap-applications-2
- ibm-sles-15-3-amd64-sap-applications-2
- ibm-sles-15-4-amd64-sap-applications-4

```
$ # Infra VPC variables for ASE SYB
REGION    = "eu-de"
ZONE      = "eu-de-2"
VPC       = "ic4sap"                      # EXISTING Security group name
SECURITY_GROUP = "ic4sap-securitygroup"     # EXISTING Security group name
RESOURCE_GROUP = "wes-automation"
SUBNET    = "ic4sap-subnet"                 # EXISTING Subnet name
SSH_KEYS   = [ "r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a" , "r010-3fcfd9fe7-d4a7-41ce-8bb3-
d96e936b2c7e" ]

# SAP AAS VSI variables:
```

```

HOSTNAME = "sapnwase-as01"
PROFILE = "bx2-4x16"
IMAGE = "ibm-redhat-8-4-amd64-sap-applications-2

$ # Infra VPC variables for ABAP HANA
REGION      = "eu-de"
ZONE        = "eu-de-2"
VPC          = "ic4sap" # EXISTING Security group name
SECURITY_GROUP = "ic4sap-securitygroup" # EXISTING Security group name
RESOURCE_GROUP = "wes-automation"
SUBNET       = "ic4sap-subnet" # EXISTING Subnet name
SSH_KEYS     = [ "r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a" , "r010-3fc9fe7-d4a7-41ce-8bb3-d96e936b2c7e" ]
ID_RSA_FILE_PATH = "ansible/id_rsa"

# SAP AAS variables:
HOSTNAME = "sapnwapp"
PROFILE = "bx2-4x16"
IMAGE = "ibm-redhat-8-6-amd64-sap-applications-2"

```

4. Customize your SAP system configuration. In the same file, input.auto.tfvars, edit the SAP system configuration variables that are passed to the Ansible automated deployment. For descriptions of the variables, see the [readme](#) file.

```

$ # SAP system configuration - for ASE SYB
sap_sid = "NWD"
sap_ci_host = "10.243.132.10"
sap_ci_hostname = "sapnwase"
sap_ci_instance_number = "00"
sap_asc_s_instance_number = "01"
sap_aas_instance_number = "00"

# Kits paths
kit_sapcar_file = "/storage/NW75SYB/SAPCAR_1010-70006178.EXE"
kit_swpm_file = "/storage/NW75SYB/SWPM10SP31_7-20009701.SAR"
kit_saphotagent_file = "/storage/NW75SYB/SAPHOSTAGENT51_51-20009394.SAR"

```

```

$ # SAP system configuration - for ABAP HANA
sap_sid = "NWD"
sap_ci_host = "10.243.132.10"
sap_ci_hostname = "sapnwapp01"
sap_ci_instance_number = "00"
sap_asc_s_instance_number = "01"
hdb_instance_number = "00"
sap_aas_instance_number = "00"

# Kits paths
kit_sapcar_file = "/storage/NW75HDB/SAPCAR_1010-70006178.EXE"
kit_swpm_file = "/storage/NW75HDB/SWPM10SP31_7-20009701.SAR"
kit_saphotagent_file = "/storage/NW75HDB/SAPHOSTAGENT51_51-20009394.SAR"
kit_hdbclient_file = "/storage/NW75HDB/IMDB_CLIENT20_009_28-80002082.SAR"

```

Ansible decompresses the rest of the SAP kit files. For more information, see the [readme](#) file.

5. Initialize the Terraform CLI.

```
terraform init
```

6. Create a Terraform execution plan. The Terraform execution plan summarizes all the actions that are done to create the virtual private cloud instance in your account.

```
terraform plan plan1
```

Enter an SAP main password and your API key.

The SAP main password must be 10 - 14 characters long and contain at least one digit (0-9). It can contain only the following characters: a-z, A-Z, 0-9, @, #, \$, . *This password cannot contain exclamation points '!'. The password must not start with a digit or an underscore ().*

7. Verify that the plan shows all of the resources that you want to create and that the names and values are correct. If the plan needs to be adjusted, edit the input.auto.tfvars file to correct resources and run terraform plan again.
8. Apply the saved plan.

```
$ terraform apply "plan1"
```

The virtual private cloud and components are created and you see output similar to the `terraform plan` output.

9. Add the SAP credentials and the virtual server instance IP to the SAP GUI. For more information about the SAP GUI, see [SAP GUI](#).

Next steps

If you need to rename your resources after they are created, modify the input.auto.tfvars file to change the names and run `terraform plan` and `terraform apply` again. Do not use the IBM Cloud Dashboard and user interface to modify your VPC after it is created. The Terraform scripts create a complete solution and selectively modifying resources with the user interface might cause unexpected results.

If you need to remove the SAP Netweaver 7.X on HANA or AnyDB installation, go to your project folder and run `terraform destroy`. The `terraform destroy` command does not remove the VPC in this scenario because the VPC was created before these Terraform scripts were run.

Related information

For more information about Terraform on IBM Cloud, see [Getting started with Terraform on IBM Cloud](#).

For more information about using Terraform for creating only a VPC for SAP, without the SAP architecture, see [Creating single-tier virtual private cloud for SAP by using Terraform](#).

SAP One Support Notes that apply to this document:

- [SAP Note 84555 - Windows Server, Linux®, and UNIX: Certified hardware](#)
- [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#)
- [SAP Note 2923773 - Linux® on IBM Cloud \(IaaS\): Adaption of your SAP license](#)
- [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#)
- [SAP Note 2369910 - SAP Software on Linux®: General information](#)
- [SAP Note 171380 - Released IBM hardware \(Intel processors\) and IBM cloud services offers](#)
- [SAP Note 1380654 - SAP support in IaaS environments](#)

This document is referenced by:

- [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#)
- [SAP Note 2588225 - SAP on IBM Cloud: Protect against speculative execution vulnerabilities](#)
- [SAP Note 1380654 - SAP support in IaaS environments](#)
- [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#)

SAP NetWeaver 7.x on HANA db 3-tier in VPC

Automating SAP workload HA deployment on IBM Cloud VPC with Terraform and Ansible

You can use Terraform to automate IBM Cloud® VPC provisioning. The VPC provisioned includes virtual server instances with high network performance. The VPC infrastructure contains various Infrastructure-as-a-Service (IaaS) offerings, including virtual servers. After the VPC is provisioned, the scripts use the Ansible Playbooks to install the SAP system.

IBM Cloud VPC introduction

VPC is a public cloud offering that an enterprise uses to establish its own private cloud-like computing environment on shared [public cloud](#) infrastructure. VPC gives an enterprise the ability to define and control a virtual network that is logically isolated from all other public cloud tenants, creating a private and secure place on the public cloud.

Imagine that a cloud provider's infrastructure is a residential apartment building and multiple families live inside. A public cloud tenant is a kind of sharing an apartment with a few roommates. In contrast, having a VPC is like having your own private condominium; no one else has the key, and no one can enter the space without your permission.

VPC's logical isolation is implemented by using virtual network functions and security features that give the enterprise customer granular control over which IP addresses or applications can access particular resources. It is analogous to the "friends-only" or "public/private" controls on social media accounts used to restrict who can or can't see your otherwise public posts.

With IBM Cloud VPC, you can use the UI, CLI, and API to manually provision virtual server instances for VPC with high network performance. VPC infrastructure contains various Infrastructure-as-a-Service (IaaS) offerings including virtual servers for VPC.

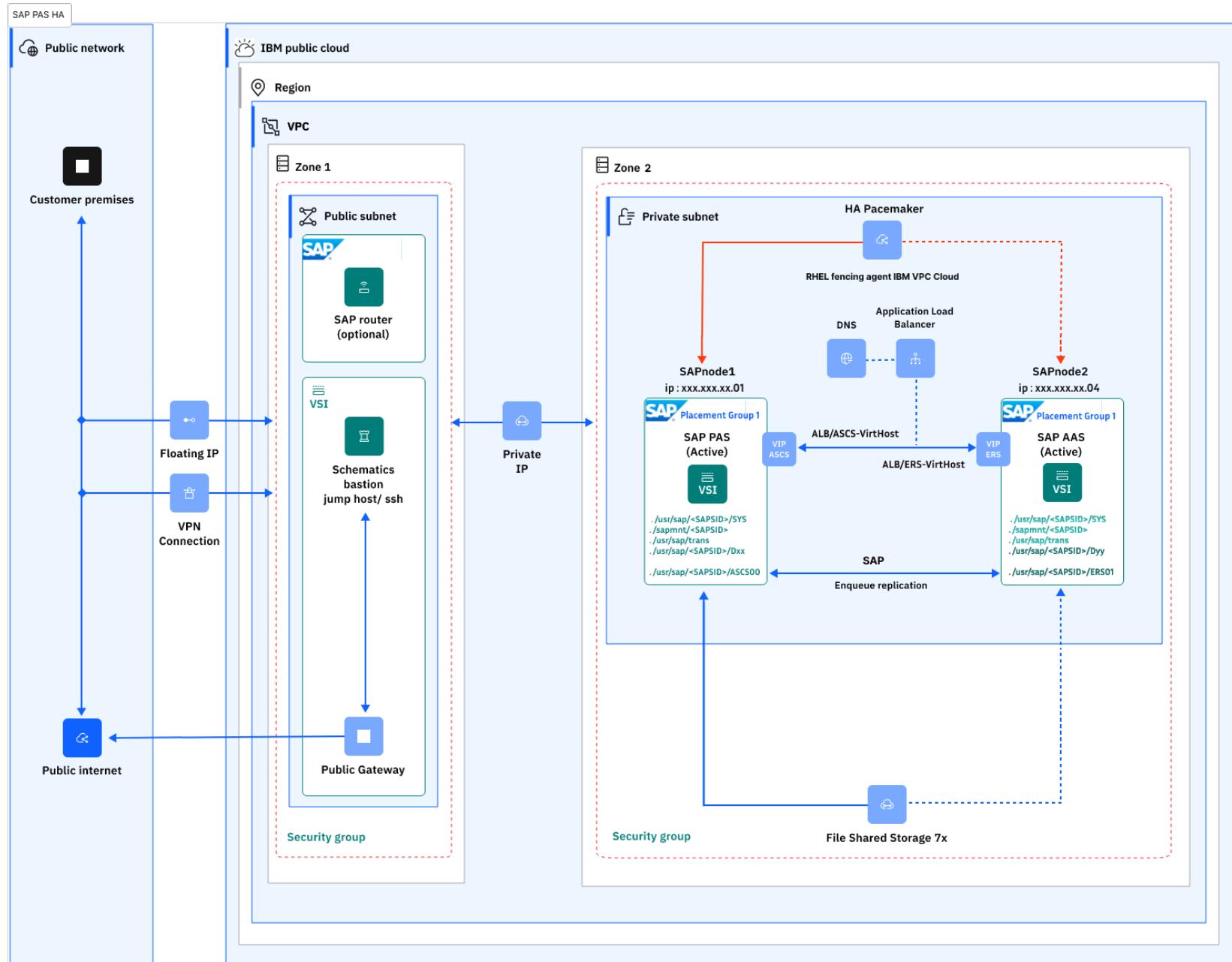
Use the following information to understand a simple use-case for planning, creating, and configuring resources for your VPC, and learn more about VPC overviews and VPC tutorials. For more information about the VPC, see [Getting started with Virtual Private Cloud \(VPC\)](#).

SAP products architecture on IBM Cloud VPC

A [Virtual Private Cloud \(VPC\)](#) contains one of the most secure and reliable cloud environments for SAP applications within your own VPC with virtual server instances. This represents an Infrastructure-as-a-Service (IaaS){: external} within IBM Cloud that offers all the benefits of isolated, secure, and flexible virtual cloud infrastructure from IBM. In comparison, the IBM Cloud classic infrastructure virtual servers offering uses virtual instances with native and VLAN networking to communicate with each other within a data center; however, the instances are restricted in one well-working pod by using subnet and VLAN networking as a gap scale up of virtual resources should rely between the pods. The IBM Cloud VPC network orchestrator layer concept eliminates the pod boundaries and restrictions, so this new concept handles all the networking for every virtual instance running within VPC across regions and zones.

Highly available system for SAP NetWeaver on IBM Cloud VPC

In a Highly Available (HA) system, every instance can run on a separate IBM Cloud virtual server instance. The cluster HA configuration for the SAP application server consists of two virtual server instances, each of them located in the same zone within the region by using placement groups. Placement groups assure that both cluster resources and cloud resources are also located in different compute nodes as specified in the following placement groups section:



SAP HA for SAP applications cluster nodes PAS (Active) and AAS (Active)

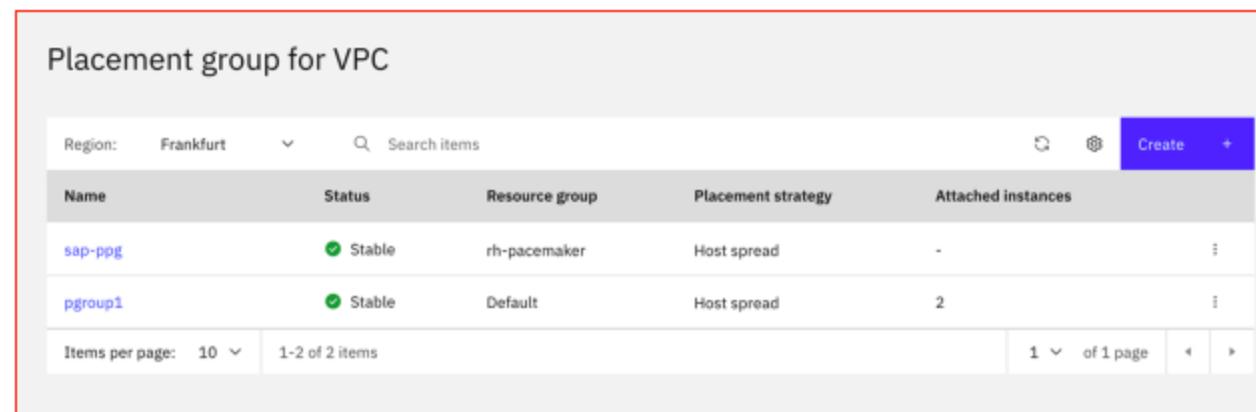
Placement groups on IBM Cloud VPC for SAP HA architecture

Placement Groups (PG) for VPC have two different anti-affinity strategies for high availability. By using the placement strategies, you minimize the chance of service disruption with virtual server instances that are placed on different hosts or into an infrastructure with separate power and network supplies.

The design of placement groups for IBM Cloud virtual servers solves this issue. Placement groups give a measure of control over the host on which a new public virtual server is placed. In this release, a “spread” rule is implemented, which means that the virtual servers within a placement group are spread onto different hosts. You can build a highly available application within a data center and know that your virtual servers are isolated from each other.

Placement groups with the spread rule are available to create in selected IBM Cloud data centers. After a spread rule is created, you can provision a virtual server into that group and ensure that it is not on the same host as any of your other virtual servers. This feature comes with no cost.

You can create your placement group and assign up to four new virtual server instances. With the spread rule, each of your virtual servers are provisioned on different physical hosts. In the following configuration example, the “Power Spread” option is used:



Placement groups host spread

Placement group for VPC					
Name	Status	Resource group	Placement strategy	Attached instances	
sapha-poc	Stable	wes-ic4sap-resourcegroup	Power spread	4	
Items per page: 10 1 item 1 of 1 page					

Placement groups power spread

Following are the SAP instances that are required for HA scenario:

- ABAP SAP Central Services (ASCS) instance - contains the ABAP message server and the ABAP enqueue server.
- Enqueue Replication Server (ERS) instance for the ASCS instance.
- Database instance
- Primary Application Server (PAS) instance on node 1.
- Additional Application Server (AAS) instance on node 2.



Note: It is recommended to run both the ASCS instance and the ERS instance in a switchover cluster infrastructure.

IBM Cloud File Storage for VPC for SAP HA architecture

[IBM Cloud File Storage for VPC](#) technology is used to make the SAP directories available to the SAP system. The technologies of choice are NFS, shared disks, and cluster file system. If you have decided to use the HA solution for your SAP system, make sure that you properly address the HA requirements of the SAP file systems in your SAP environment.

File shares for VPC								
Name	Status	Resource groups	Location	Mount targets	Size	Replication role	Encryption type	
usrsap-as1-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-as2-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-sapsacs-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-sapers-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-sapmnt-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-sapsys-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-trans-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	80 GB	None	Provider managed	

File shares for VPC

- File shares that are mounted as NFS permanent file systems on both cluster nodes for SAP HA application:
 - `/usr/sap/<SAPSID>/SYS`
 - `/sapmnt<SAPSID>`
 - `/usr/sap/trans`
- Cluster-managed file systems for SAP HA application: ASCS
 - `/usr/sap/<SAPSID>/ASCS00`
 - `/usr/sap/<SAPSID>/ERS01`
- Permanent NFS mount on SAP HA application node 1 PAS instance:
 - `/usr/sap/<SAPSID>/Dxx`
- Permanent NFS mount on SAP HA application node 2 dialog instance:
 - `/usr/sap/<SAPSID>/Dyy`

Prerequisites

You need to install the hardware (hosts, disks, and network) and decide how to distribute the database, SAP instances, and if required, the Network File System (NFS) server over the cluster nodes.

Context

Following are the types of SAP directories:

- Physically shared directories: `/<sapmnt>/<SAPSID>` and `/usr/sap/trans`

- Logically shared directories that are bound to a node, such as `/usr/sap`, with the following local directories:
 - `/usr/sap/<SAPSID>`
 - `/usr/sap/<SAPSID>/SYS`
 - `/usr/sap/hostctrl`
- Local directories that contain the SAP instances such as `/usr/sap/<SAPSID>/ASCS<Instance_Number>`
- The global transport directory may reside on a separate SAP transport host as a standard three systems transport layer configuration.

You need at least two nodes and a shared file system for distributed ASCS and ERS instances. The assumption is that the rest of the components are distributed on other nodes.

ASCS and ERS installation

In order for the ASCS and ERS instances to be able to move from one node to the other, they need to be installed on a shared file system and use virtual hostnames based on the virtual IP.

In this VPC-based SAP HA solution, the shared file system that is required by the cluster is replaced by the NFS-mounted file storage, and the virtual IP is replaced by the Application Load Balancer for VPC (ALB).

In this scenario, three ALBs are used, one for each Single Point of Failure (SPOF) component in order to replace the virtual IP requirement: ALB for ASCS, ALB for ERS, and ALB for ASE Sybase. Each ALB is configured as a backend for the corresponding cluster servers and redirects all of the communication that is received on the front-end ports to the active server in the backend pool.

Load balancers for VPC						
Region:	Frankfurt	▼	<input type="text"/> poc	X		
Name	Status	Family	Resource group	Type	Hostname	Location
db-alb-hana-poc	Active	Application	wes-ic4sap-resourcegroup	Private	20bdd130-eu-de.lb.appdomain.cloud	Frankfurt
sap-alb-ers-poc	Active	Application	wes-ic4sap-resourcegroup	Private	3941d983-eu-de.lb.appdomain.cloud	Frankfurt
sap-alb-ascs-poc	Active	Application	wes-ic4sap-resourcegroup	Private	56a9190d-eu-de.lb.appdomain.cloud	Frankfurt

Application load balancer management of HA IPs mechanism

Private application load balancer

A [private application load balancer](#) is accessible through your private subnets that you configured to create the load balancer.

Similar to a public application load balancer, your private application load balancer service instance is assigned an FQDN; however, this domain name is registered with one or more private IP addresses.

IBM Cloud operations change the number and value of your assigned private IP addresses over time, based on maintenance and scaling activities. The backend virtual server instances that host your application must run in the same region and under the same VPC.

Use the assigned ALB FQDN to send traffic to the private application load balancer to avoid connectivity problems to your applications during system maintenance or scaling down activities.

Each ALB sends traffic to the cluster node where the application (ASCS, ERS, ASE Sybase DB) is running. During the cluster failover, the ALB redirects all the traffic to the new node where the resources are up and running.



Note: DNS-as-a-Service (DNSaaS) is the management IBM Cloud VPC DNS service of HA and FQDN (IPs) mechanism.



Note: The ALB has a default of 50 seconds for client and server timeout, so after 50 seconds of inactivity, the connection is closed. To support SAP connections through ALB and not lose connection after 50 seconds, you need to request a change this value to a minimum of 300 seconds (client-side idle connection = minimum 300s and server-side idle connection = minimum 300s). To request this change, open a support ticket. This is an account-wide change that affects all of the ALBs in your account. For more information, see [Connection timeouts](#).

DNS Services with VPC

[IBM Cloud DNS Services](#) provide private DNS to VPC users. Private DNS zones are resolvable only on IBM Cloud and from explicitly [permitted networks](#) in an account. To get started, create a DNS Services instance by using the IBM Cloud console.

DNS Services allows you to:

- Create the private DNS zones that are collections for holding the domain names.
- Create the DNS resource records under these DNS zones.
- Specify the access controls used for the DNS resolution of resource records on a zone-wide level.

DNS Services also maintains its own worldwide set of DNS resolvers. Instances that are provisioned under IBM Cloud on an IBM Cloud network can use resource records that are configured through IBM Cloud DNS Services by querying DNS Services resolvers.

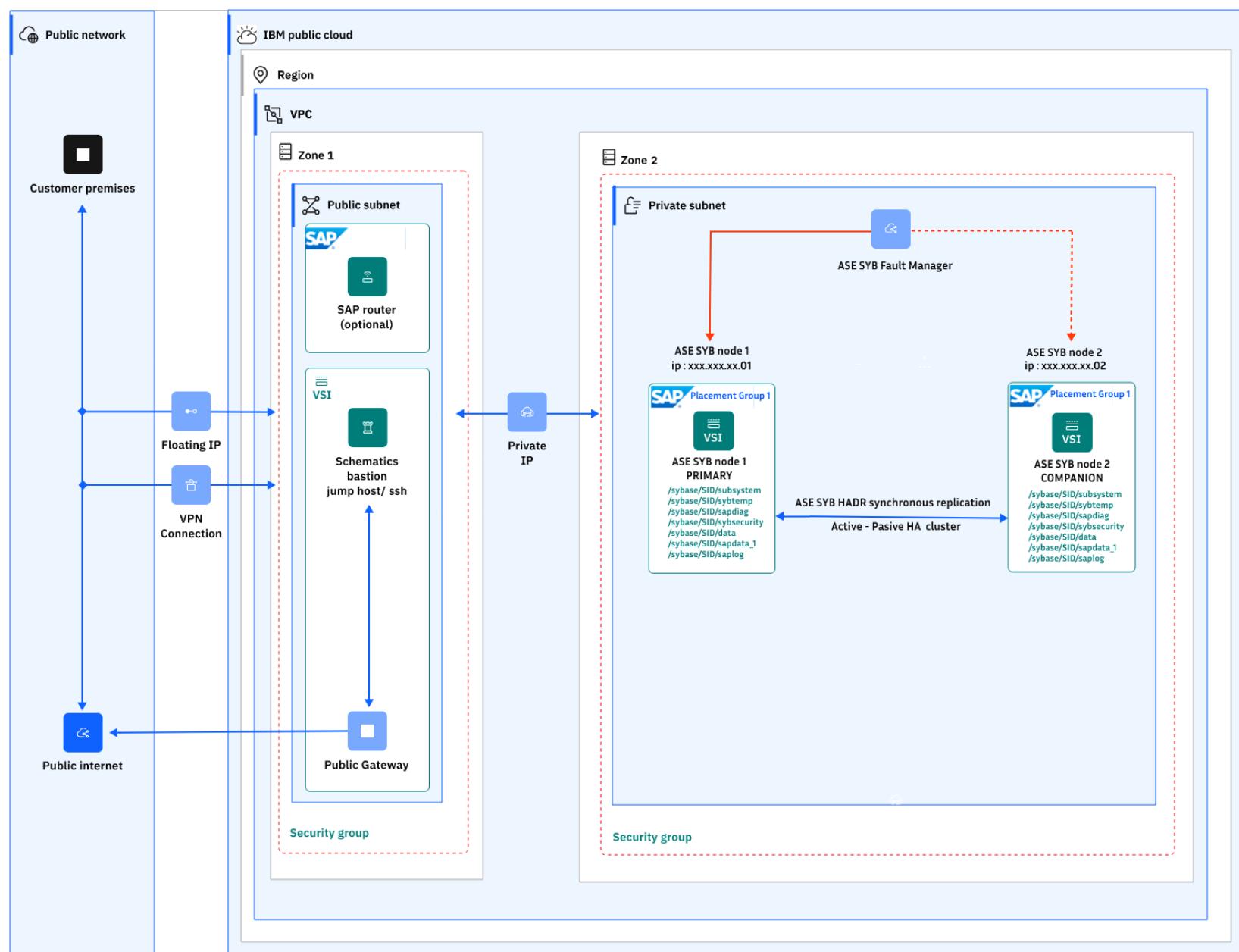
Resource records and zones that are configured through DNS Services are:

- Separated from the wider public DNS, and their publicly accessible records.
- Hidden from the system outside of and not part of the IBM Cloud private network.
- Accessible only from the system that you authorize on the IBM Cloud private network.
- Resolvable only via the resolvers provided by the service.

The DNS service maps the FQDN of each ALB to the virtual hostnames of the ASCS, ERS, and ASE Sybase that are used by SAP applications.

Type	Name	Value	TTL
CNAME	dbpochana	is an alias of 20bdd130-eu-de.lb.appdomain.cloud	12 hr
CNAME	sappocers	is an alias of 3941d983-eu-de.lb.appdomain.cloud	12 hr
CNAME	sappocases	is an alias of 56a9190d-eu-de.lb.appdomain.cloud	12 hr

Highly available system for SAP ASE Sybase database with HADR system



SAP HA for ASE Sybase DB instances cluster nodes primary (Active) and Secondary (Companion)

At the most basic level, a standard HA ASE Sybase cluster in an active(primary)-passive(companion) configuration has two nodes: one is the primary node and the other is the standby node. This means that the primary node is actively serving the active SAP DB instances (Primary and Companion), while the standby node is waiting to jump in if there is any failure.

The cluster is set with a virtual hostname IP (hostname is mapped to the FQDN of the ASE Sybase ALB through DNS, which is the same as

explained previously for SAP ASCS and ERS instances). Application instances (PAS and AAS) are used on the SAP profiles to call that particular component. The cluster assigns the virtual IP to the active node and uses a heartbeat monitor to confirm the availability of the components. If the primary node stops responding, it triggers the automatic failover mechanism that calls the standby node to step up to become the primary node. The ALB detects the change, redirects the traffic to the new active node, and assigns the virtual IP to it, restoring the component availability. Once fixed, the failed node comes online as a standby node.

SAP Sybase HADR system supports synchronous replication

The SAP Sybase HADR system supports synchronous replication between the primary and standby servers for high availability. An active-active setup is a two-node configuration where both nodes in the cluster include SAP ASE managing independent workloads, capable of taking over each others workload in the event of a failure.

The SAP ASE server that takes over the workload is called a secondary companion, and the SAP ASE server that fails is called the primary companion. Together they are companion servers. This movement from one node to another is called failover. After the primary companion is ready to resume its workload, it is moved back to its original node. This movement is called a failback.

When a system fails over, clients that are connected to the primary companion and use the failover property automatically reestablish their network connections to the secondary companion. You must tune your operating system to successfully manage both servers during fail over. See your operating system documentation for information about configuring your system for high availability. An SAP ASE configured for failover in an active-active setup can be shut down using the shutdown command only after you have suspended SAP ASE from the companion configuration, at both the server level and the platform level.

The always-on option in a High Availability and Disaster Recovery (HADR) system consists of two SAP ASE servers:

- Primary on which all transaction processing takes place.
- Warm standby (referred to as a "standby server" in DR mode, and as a "companion" in HA mode) for the primary server, and contains copies of designated databases from the primary server.



Note: The HADR feature that is shipped with SAP ASE version 16.0 SP02 supports only a single-companion server.

Some high-availability solutions (for example, the SAP Adaptive Server Enterprise Cluster Edition) share or use common resources between nodes. However, the HADR system is a "shared nothing" configuration, each node has separate resources including disks.

In an HADR system, servers are separate entities and data is replicated from the primary server to the companion server. If the primary server fails, a companion server is promoted to the role of primary server either manually or automatically. Once the promotion is complete, clients can reconnect to the new primary server, and see all committed data, including data that was committed on the previous primary server.

Servers can be separated geographically, which makes an HADR system capable of withstanding the loss of an entire computing facility.



Note: The HADR system includes an embedded SAP Replication Server, which synchronizes the databases between the primary and companion servers. SAP ASE uses the Replication Management Agent (RMA) to communicate with Replication Server and SAP Replication Server uses Open Client connectivity to communicate with the companion SAP ASE.

The Replication Agent detects any data changes made on the primary server and sends them to the primary SAP Replication Server. In the figure above, the unidirectional arrows indicate that, although both SAP Replication Servers are configured, only one direction is enabled at a time.

The HADR system supports synchronous replication between the primary and standby servers for high availability so the two servers can keep in sync with Zero Data Loss (ZDL). This requires a network link that is fast enough between the primary and standby server so that synchronous replication can keep up with the primary servers workload. Generally, this means that the network latency is approximately the same speed as the local disk IO speed, a few (fewer than 10) milliseconds. Anything longer than a few milliseconds may result in a slower response to write operations at the primary.

The HADR system supports asynchronous replication between the primary and standby servers for disaster recovery. The primary and standby servers by using asynchronous replication can be geographically distant, meaning they can have a slower network link. With asynchronous replication, Replication Agent Thread captures the primary servers workload, which is delivered asynchronously to SAP Replication Server. The SAP Replication Server applies these workload change to the companion server.

The most fundamental service that is offered by the HADR system is the failover; planned or unplanned from the primary to the companion server, which allows maintenance activity to occur on the old primary server, while applications continue on the new primary.

The HADR system provides protection in the event of a disaster. If the primary server is lost, the companion server can be used as a replacement. Client applications can switch to the companion server, and the companion server is quickly available for users. If the SAP Replication Server was in synchronous mode before the failure of the primary server, the Fault Manager automatically initiates failover with

zero data loss.

Fault Manager installation on the SAP ASCS node

The required parameters are asked during the installation process to create a profile for the fault manager and then adds it to the instance start profile. It is also possible to run the installation by using an existing profile: `sybdbfm install pf=<SYBHA.PFL>` In this case, the installation process will only ask for profile parameters missing in the profile.



Note: Fault manger is integrated with ASCS on same SAP PAS/AAS cluster (start/stop/move together).

There may be some data loss if the SAP Replication Server was in asynchronous mode and you must use manual intervention to failover for disaster recovery.

Connection attempts to the companion server without the necessary privileges are silently redirected to the primary companion via the login redirection mechanism, which is supported by Connectivity libraries. If login redirection is not enabled, client connections fail and are disconnected.

The SAP ASE HADR option installs the below components:

- SAP ASE
- SAP Replication Server
- Replication Management Agent (RMA)
- SAP Host Agent
- Fault Manager
- SAP ASE Cockpit



Note: This automation is offered at no cost; however, the provisioned infrastructure comes at cost.

VPC with Additional Application Server (AAS) ABAP on Linux for SAP HANA

You can use Terraform scripts to create a single-tier VPC and create the AAS to HANA and AnyDB infrastructure on the VPC. The Terraform scripts use the VPC information that you provide and then call the Ansible playbook to create the SAP architecture on the specified VPC. Terraform on IBM Cloud® enables predictable and consistent provisioning of IBM Cloud Virtual Private Cloud (VPC) infrastructure resources so that you can rapidly build complex, cloud environments. IBM Cloud VPC infrastructure consists of SAP certified hardware that uses Intel® Xeon CPUs and more Intel® technologies.

You have two deployment methods to choose from:

- Terraform scripts that run from the CLI on your bastion server.
- Schematics user interface accessed from your cloud dashboard menu.

You can create SAP AAS NetWeaver 7.x on the SAP HANA-based ABAP stack.

SAP solution implemented

Many SAP enterprise solutions are built on the SAP platform (SAP NetWeaver) including:

- SAP HANA as Primary Persistence for SAP NetWeaver-based applications
- SAP Business Suite applications (ERP, CRM, and SCM, and other applications),
- SAP Business Warehouse (BW), and
- Other SAP enterprise solutions

SAP NetWeaver has two distinct aspects, ABAP and Java. Many applications that are built on the SAP NetWeaver's ABAP or Java (or both) application servers run on SAP DB owned HANA and ASE Sybase either in AnyDB platforms (MSSQL, Oracle, and Db2).

Technical interfaces are available for applications that are built on the SAP NetWeaver AS ABAP and AS Java to run on SAP HANA and AnyDB. However, specific development enablement is normally required for each application to ensure that it runs optimally on the SAP HANA. SAP Business Suite applications (ERP, CRM, SCM, and other applications), SAP Business Warehouse (BW), and other SAP NetWeaver-based applications were modified to run on SAP HANA and have many advantages. Also, various components and complimentary applications that are built on SAP NetWeaver can also run on SAP HANA or AnyDB by using the provided SAP NetWeaver DB interfaces.

The SAP HANA as primary persistence for SAP NetWeaver-based applications scenario has one restriction: SAP NetWeaver ABAP and Java

application servers must run on separate hardware servers from the SAP HANA hardware.

What is created

The scripts automate the virtual infrastructure resources, provisioning the processes for the SAP architecture in an existing VPC with a distributed environment. SAP AAS NetWeaver 7.x (HANA or ASE SYB) application server on a distinct VSI VPC system and SAP HANA DB on a dedicated server type VSI VPC box are provisioned. The scripts work in two phases.

During the first phase of [Automate SAP bastion server – SAP media storage repository](#), the following virtual infrastructure resources based on the components from the existing VPC created by the bastion server are:

- 1 VPC where the virtual server instance is provisioned.
- 1 security group. The rules for this security group are:
 - Allow inbound DNS traffic (port 53).
 - Allow inbound SSH traffic (TCP port 22).
 - Allow all outbound traffic from the virtual server instance.
 - Allow all traffic in the security group.
- 1 subnet to enable the networking in your VPC.
- 2 virtual server instances with SAP certified storage and network configurations.
- 1 floating IP address used to access your VPC virtual server instance over the public network.

During the second phase, the Ansible Playbooks is called and the SAP architecture is installed for both dedicated virtual server instance (VSI) SAP application; VSI system and dedicated SAP HANA VSI box. The SAP architecture that is deployed on the SAP NetWeaver 7.x release is a stand-alone dedicated SAP HANA 2.0 box release. For more information about this architecture, see [Automating SAP HANA stand-alone virtual server instance on IBM Cloud® VPC by using Terraform and Ansible](#).

You can provision only one instance of the service per IBM Cloud region.

Schematics deployment

When you run the scripts with the Schematics interface, you:

- Enter the workspace information.
- Enter the GitHub path for the chosen solution either on NetWeaver AAS for HANA.
- Modify the parameters in the Schematics interface. They are the same parameters as the `input.auto.tfvars` file that you use with the cli.

Virtual server instance configuration

Following are the supported operating system images for SAP NetWeaver primary application server:

- ibm-redhat-8-4-amd64-sap-applications-2
- ibm-redhat-8-6-amd64-sap-applications-2
- ibm-sles-15-3-amd64-sap-applications-2
- ibm-sles-15-4-amd64-sap-applications-3

Following are the supported operating system images for SAP HANA database:

- ibm-redhat-8-4-amd64-sap-hana-2
- ibm-redhat-8-6-amd64-sap-hana-2
- ibm-sles-15-3-amd64-sap-hana-2
- ibm-sles-15-4-amd64-sap-hana-1

For both server instances there are:

- Two SSH keys are configured to access SSH as `root`.
- Three storage volumes as described in the `input.auto.tfvars` file.

What is created for anydb

The scripts use the information that you provide for an existing VPC and deploy AAS to SAP HANA or AnyDB on a different host than CI (SAP Central Instance) VSI host. For more information about this architecture, see [SAP NetWeaver 7.x on UNIX with HANA or AnyDB on IBM Cloud](#)

[VPC on IBM Cloud VPC](#). You specify the information for the VPC to use in the `input.auto.tfvars` file.

The scripts call the Ansible Playbooks to install the SAP architecture.

Script files

The configuration and script files are provided on GitHub. Each supported interface for the SAP solution installation has its own folder in the GitHub repository:

- [GitHub repository for Terraform – AAS HANA](#)

Terraform interface

To run the Terraform script, you modify:

- The `input.auto.tfvars` file to specify the existing VPC resources for your solution. Specify the variables for the existing VPC:
 - VPC name
 - Security group
 - Subnet
 - Hostname
 - Profile
 - Image
 - Up to two SSH keys

You can change the default SAP system configuration settings to match your solution. You can also specify the location where you downloaded the SAP kits.

The IBM Cloud Provider plug-in for Terraform on IBM Cloud uses these configuration files to install AAS to SAP HANA and AnyDB on the specified VPC in your IBM Cloud account.

Support

There are no warranties of any kind, and there is no service or technical support available for these materials from IBM®. As a recommended practice, review carefully any materials that you download from this site before using them on a live system.

Though the materials provided herein are not supported by the IBM® Service organization, your comments are welcomed by the developers, who reserve the right to revise, readapt or remove the materials at any time. To report a problem, or provide suggestions or comments, open a GitHub issue.

Before you begin

Before you use the scripts in the bastion cli:

- Set up your account to access the VPC. Make sure that your account is [upgraded to a paid account](#).
- If you have not already, create a Bastion server to store the SAP kits. For more information, see [Automate SAP bastion server - SAP media storage repository](#).
- Download the SAP kits from the SAP Portal to your Deployment Server. Make note of the download locations. Ansible decompresses the files. For more information, see the [readme](#) file.
- [Create or retrieve an IBM Cloud API key](#). The API key is used to authenticate with the IBM Cloud platform and to determine your permissions for IBM Cloud services.
- [Create or retrieve your SSH key ID](#). You need the 40-digit UUID for the SSH key, not the SSH key name.
- Terraform should already be installed on the bastion server that you deployed. For more information, see [Bastion server for SAP deployment](#).
- (Optional - Catalog Tile) create secrets for your credentials and passwords by using the [Secrets Manager](#).

Deploying SAP AAS NetWeaver 7.x on HANA by using the Schematics user interface

Use these steps to configure the SAP Additional Application Server (AAS) NetWeaver with HANA or AnyDB on your existing VPC by using the Schematics interface. The script takes 2 - 3 hours to complete.

1. From the IBM Cloud menu, select **Schematics**.
2. Click **Create** workspace.

3. On the **Specify template** page:
 - Enter the URL for the Schematics interface.
 - Select the **Terraform version** that is listed in the readme file.
 - Click **Next**.
4. On the **workspace details** page:
 - Enter a name for the workspace.
 - Select a **Resource group**.
 - Select a **Location** for your workspace. The workspace location does not have to match the resource location.
 - Select **Next**.
5. Select **Create** to create your workspace.
6. On the workspace settings page, in the input variables section, review the default input variables and provide values that match your solution.
 For a more detailed description of each parameter, check the GitHub repo [AAS HANA readme](#) file, chapter "Input parameter file". Also, make sure to mark the parameters that contain sensitive information like passwords, API, and ssh private keys as "sensitive". These parameters are marked as "sensitive" in the readme file, under "Input parameter file".
7. On the workspace settings page, click **Generate plan**. Wait for the plan to complete.
8. Click **View log** to review the log files of your terraform execution plan.
9. Apply your Terraform template by clicking **Apply plan**.
10. Review the log file to ensure that no errors occur during the provisioning, modification, or deletion process.

Deploying SAP AAS NetWeaver (ABAP) on HANA with the Deployable Architecture tile interface

Use these steps to configure the SAP AAS NetWeaver (ABAP) on HANA on your existing VPC by using the catalog tile interface. The script takes 2 - 3 hours to complete.

1. From the IBM Cloud catalog, select **VPC with Additional Application Server ABAP on Linux for SAP HANA** on HANA tile. The **Create** tab opens for VPC with Additional Application Server ABAP on Linux for SAP HANA. For more information about this deployment, see the About tab or the readme file link.
2. Select the latest version.
3. Select **VPC with Additional Application Server ABAP on Linux for SAP HANA on Deployable Architecture tile** variation.
4. Click **Review deployment** options:
 - **Add to project** to add this deployment to an IBM Cloud project and combine it with other deployments. IBM Cloud projects include several more pipeline steps before deployment, including deployment validation, cost calculation, compliance verification, and approval process.
 - **Create from the CLI** to get the CLI command. With this command you can trigger the deployment from the CLI.
 - **Work with code** to embed the code into other terraform deployments.
 - **Deploy with IBM Cloud Schematics** to trigger the deployment process directly.
5. Select **Deploy with IBM Cloud Schematics**.
6. Add the input parameters for this installation. There are 3 categories of parameters:
 - **Workspace** - These parameters define the workspace that is automatically created in Schematics:
 - Enter a name for the workspace or use the default name.
 - The Resource Group used to create resources. Use default or create a Resource Group.
 - Select a location to create your Schematics workspace. The workspace location need not match the resource location.
 - **Required input variables** - Review the default input variables and provide values that match your solution. These parameters are specific to your deployment. For more detailed information, see the [Readme file](#).

Parameter	Description
BASTION_FLOATING_IP	Required only for Schematics Deployments. The Floating IP from the Bastion Server.

HOSTNAME	The hostname for the VSI. The hostname should be up to 13 characters as required by SAP. For more information on the rules regarding hostnames for SAP systems, check SAP Note 611361: Hostnames of SAP ABAP Platform servers
REGION	The cloud region to deploy the solution. The regions and zones for VPC are listed here . Review supported locations in IBM Cloud Schematics here . Sample value: eu-de.
RESOURCE_GROUP	The name of an existing Resource Group for VSIs and Volumes resources. Default value: "Default". The list of Resource Groups is available here .
SECURITY_GROUP	The name of an existing Security group. The list of security groups is available here .
SSH_KEYS	The list of SSH Keys UUIDs that are allowed to SSH as root to the VSI can contain one or more IDs. The list of SSH Keys is available here . Sample input (use your own SSH UUIDs from IBM Cloud){: external}: ["r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a", "r010-3fcfd9fe7-d4a7-41ce-8bb3-d96e936b2c7e"]
SUBNET	The name of an existing subnet. The list of subnets is available here .
VPC	The name of an existing VPC. The list of VPCs is available here .
ZONE	The cloud zone where to deploy the solution. Sample value: eu-de-2.
ibmcloud_api_key	IBM Cloud API key (Sensitive* value).
private_ssh_key	Required only for Schematics Deployments - Input your id_rsa private key pair content in OpenSSH format (Sensitive* value). This private key should be used only during the terraform provisioning and it is recommended to be changed after the SAP deployment.
hdb_instance_number	The instance number of the SAP HANA database server.
sap_aas_instance_number	Technical identifier for the internal processes of the additional application server.
sap_ascs_instance_number	Technical identifier for the internal processes of ASCS.
sap_ci_host	IP address of the existing SAP Central Instance.
sap_ci_hostname	The hostname of the existing SAP Central Instance.
sap_ci_instance_number	Technical identifier for the internal processes of the Central Instance.
sap_sid	The SAP system ID identifies the entire SAP system.
sap_main_password	Common password for all users that are created during the installation (See Obs*).

Required Variables

- **Optional variables** - Review and update the optional input variables. The Ansible scripts expect the SAP kits to be in the default locations listed. For more information, see the [Readme file - Input Parameters](#).

Parameter	Description
ID_RSA_FILE_PATH	The file path for private_ssh_key is automatically generated by default. If it is changed, it must contain the relative path from Git repo folders. Default value: "ansible/id_rsa".
IMAGE	The OS image used for the VSI. A list of images is available here .
PROFILE	The profile used for the VSI. A list of profiles is available here . For more information about supported DB/OS and IBM Gen 2 Virtual Server Instances (VSI), check SAP Note 2927211: SAP Applications on IBM Virtual Private Cloud .

VOL1	Volume 1 Size - The size for the disks in GB that are to be attached to the VSI and used by SAP.
VOL2	Volume 2 Size - The size for the disks in GB that are to be attached to the VSI and used by SAP.
kit_sapcar_file	Path to the sapcar binary, as downloaded from SAP Support Portal.
kit_swpm_file	Path to the SWPM archive (SAR), as downloaded from SAP Support Portal.
kit_saphostagent_file	Path to the SAP Host Agent archive (SAR), as downloaded from SAP Support Portal.
kit_hdbclient_file	Path to the HANA DB client archive (SAR), as downloaded from SAP Support Portal.

Optional Variables

7. Accept the license agreement.
8. Select **Deploy**. The deployment starts and you are directed to the Schematics page that displays the script log files for you to monitor the deployment progress.

Creating the infrastructure using Terraform with the bastion server CLI

Use these steps to configure the IBM Cloud Provider plug-in and use Terraform to install SAP AAS to SAP HANA and AnyDB on your existing VPC on an already deployed SAP NetWeaver 7.X with SAP HANA 2.0 or ASE SYB as a Central Instance.

The script takes 1 - 2 hours to complete.

1. Access the bastion server cli.
2. Clone the solution repository and change to the folder.

ASE SYB 16 Clone the solution repository from <https://github.com/IBM-Cloud/sap-aas-abap-ase-syb> and cd to the sap-aas-abap-ase-syb/cli folder.

```
$ git clone https://github.com/IBM-Cloud/sap-aas-abap-ase-syb
cd sap-aas-abap-ase-syb/cli/
```

SAP HANA 2.0: Clone the solution repository from <https://github.com/IBM-Cloud/sap-abap-hana-aas> and cd to the sap-abap-hana-aas folder.

```
$ git clone https://github.com/IBM-Cloud/sap-abap-hana-aas.git
cd sap-abap-hana-aas/
```

3. Modify the `input.auto.tfvars` file to specify the information for the existing VPC, your region, zone, networking component names, hostname for the AAS VSI,profile, and image. You need your 40-digit SSH key ID for this file. The second SSH key is optional. For more options for profile, see [Instance Profiles](#). For more options, see [Images](#). For descriptions of the variables, see the [readme](#) file.

The VSI OS images that are supported for this solution for Netweaver Additional Application Server are:

- ibm-redhat-8-4-amd64-sap-applications-2
- ibm-redhat-8-6-amd64-sap-applications-2
- ibm-sles-15-3-amd64-sap-applications-2
- ibm-sles-15-4-amd64-sap-applications-4

```
$ # Infra VPC variables for ASE SYB
REGION    = "eu-de"
ZONE      = "eu-de-2"
VPC       = "ic4sap"                      # EXISTING Security group name
SECURITY_GROUP = "ic4sap-securitygroup"    # EXISTING Security group name
RESOURCE_GROUP = "wes-automation"
SUBNET    = "ic4sap-subnet"                 # EXISTING Subnet name
SSH_KEYS   = [ "r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a" , "r010-3fcfd9fe7-d4a7-41ce-8bb3-
d96e936b2c7e" ]

# SAP AAS VSI variables:
```

```

HOSTNAME = "sapnwase-as01"
PROFILE = "bx2-4x16"
IMAGE = "ibm-redhat-8-4-amd64-sap-applications-2

$ # Infra VPC variables for ABAP HANA
REGION      = "eu-de"
ZONE        = "eu-de-2"
VPC          = "ic4sap" # EXISTING Security group name
SECURITY_GROUP = "ic4sap-securitygroup" # EXISTING Security group name
RESOURCE_GROUP = "wes-automation"
SUBNET       = "ic4sap-subnet" # EXISTING Subnet name
SSH_KEYS     = [ "r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a" , "r010-3fc9fe7-d4a7-41ce-8bb3-d96e936b2c7e" ]
ID_RSA_FILE_PATH = "ansible/id_rsa"

# SAP AAS variables:
HOSTNAME = "sapnwapp"
PROFILE = "bx2-4x16"
IMAGE = "ibm-redhat-8-6-amd64-sap-applications-2"

```

4. Customize your SAP system configuration. In the same file, input.auto.tfvars, edit the SAP system configuration variables that are passed to the Ansible automated deployment. For descriptions of the variables, see the [readme](#) file.

```

$ # SAP system configuration - for ASE SYB
sap_sid = "NWD"
sap_ci_host = "10.243.132.10"
sap_ci_hostname = "sapnwase"
sap_ci_instance_number = "00"
sap_asc_s_instance_number = "01"
sap_aas_instance_number = "00"

# Kits paths
kit_sapcar_file = "/storage/NW75SYB/SAPCAR_1010-70006178.EXE"
kit_swpm_file = "/storage/NW75SYB/SWPM10SP31_7-20009701.SAR"
kit_saphotagent_file = "/storage/NW75SYB/SAPHOSTAGENT51_51-20009394.SAR"

```

```

$ # SAP system configuration - for ABAP HANA
sap_sid = "NWD"
sap_ci_host = "10.243.132.10"
sap_ci_hostname = "sapnwapp01"
sap_ci_instance_number = "00"
sap_asc_s_instance_number = "01"
hdb_instance_number = "00"
sap_aas_instance_number = "00"

# Kits paths
kit_sapcar_file = "/storage/NW75HDB/SAPCAR_1010-70006178.EXE"
kit_swpm_file = "/storage/NW75HDB/SWPM10SP31_7-20009701.SAR"
kit_saphotagent_file = "/storage/NW75HDB/SAPHOSTAGENT51_51-20009394.SAR"
kit_hdbclient_file = "/storage/NW75HDB/IMDB_CLIENT20_009_28-80002082.SAR"

```

Ansible decompresses the rest of the SAP kit files. For more information, see the [readme](#) file.

5. Initialize the Terraform CLI.

```
terraform init
```

6. Create a Terraform execution plan. The Terraform execution plan summarizes all the actions that are done to create the virtual private cloud instance in your account.

```
terraform plan plan1
```

Enter an SAP main password and your API key.

The SAP main password must be 10 - 14 characters long and contain at least one digit (0-9). It can contain only the following characters: a-z, A-Z, 0-9, @, #, \$, . *This password cannot contain exclamation points '!'. The password must not start with a digit or an underscore ().*

7. Verify that the plan shows all of the resources that you want to create and that the names and values are correct. If the plan needs to be adjusted, edit the input.auto.tfvars file to correct resources and run terraform plan again.
8. Apply the saved plan.

```
$ terraform apply "plan1"
```

The virtual private cloud and components are created and you see output similar to the `terraform plan` output.

9. Add the SAP credentials and the virtual server instance IP to the SAP GUI. For more information about the SAP GUI, see [SAP GUI](#).

Next steps

If you need to rename your resources after they are created, modify the `input.auto.tfvars` file to change the names and run `terraform plan` and `terraform apply` again. Do not use the IBM Cloud Dashboard and user interface to modify your VPC after it is created. The Terraform scripts create a complete solution and selectively modifying resources with the user interface might cause unexpected results.

If you need to remove the SAP Netweaver 7.X on HANA or AnyDB installation, go to your project folder and run `terraform destroy`. The `terraform destroy` command does not remove the VPC in this scenario because the VPC was created before these Terraform scripts were run.

Related information

For more information about Terraform on IBM Cloud, see [Getting started with Terraform on IBM Cloud](#).

For more information about using Terraform for creating only a VPC for SAP, without the SAP architecture, see [Creating single-tier virtual private cloud for SAP by using Terraform](#).

SAP One Support Notes that apply to this document:

- [SAP Note 84555 - Windows Server, Linux®, and UNIX: Certified hardware](#)
- [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#)
- [SAP Note 2923773 - Linux® on IBM Cloud \(IaaS\): Adaption of your SAP license](#)
- [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#)
- [SAP Note 2369910 - SAP Software on Linux®: General information](#)
- [SAP Note 171380 - Released IBM hardware \(Intel processors\) and IBM cloud services offers](#)
- [SAP Note 1380654 - SAP support in IaaS environments](#)

This document is referenced by:

- [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#)
- [SAP Note 2588225 - SAP on IBM Cloud: Protect against speculative execution vulnerabilities](#)
- [SAP Note 1380654 - SAP support in IaaS environments](#)
- [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#)

SAP ASE standalone database instance in VPC

Automating SAP workload HA deployment on IBM Cloud VPC with Terraform and Ansible

You can use Terraform to automate IBM Cloud® VPC provisioning. The VPC provisioned includes virtual server instances with high network performance. The VPC infrastructure contains various Infrastructure-as-a-Service (IaaS) offerings, including virtual servers. After the VPC is provisioned, the scripts use the Ansible Playbooks to install the SAP system.

IBM Cloud VPC introduction

VPC is a public cloud offering that an enterprise uses to establish its own private cloud-like computing environment on shared [public cloud](#) infrastructure. VPC gives an enterprise the ability to define and control a virtual network that is logically isolated from all other public cloud tenants, creating a private and secure place on the public cloud.

Imagine that a cloud provider's infrastructure is a residential apartment building and multiple families live inside. A public cloud tenant is a kind of sharing an apartment with a few roommates. In contrast, having a VPC is like having your own private condominium; no one else has the key, and no one can enter the space without your permission.

VPC's logical isolation is implemented by using virtual network functions and security features that give the enterprise customer granular control over which IP addresses or applications can access particular resources. It is analogous to the "friends-only" or "public/private" controls on social media accounts used to restrict who can or can't see your otherwise public posts.

With IBM Cloud VPC, you can use the UI, CLI, and API to manually provision virtual server instances for VPC with high network performance. VPC infrastructure contains various Infrastructure-as-a-Service (IaaS) offerings including virtual servers for VPC.

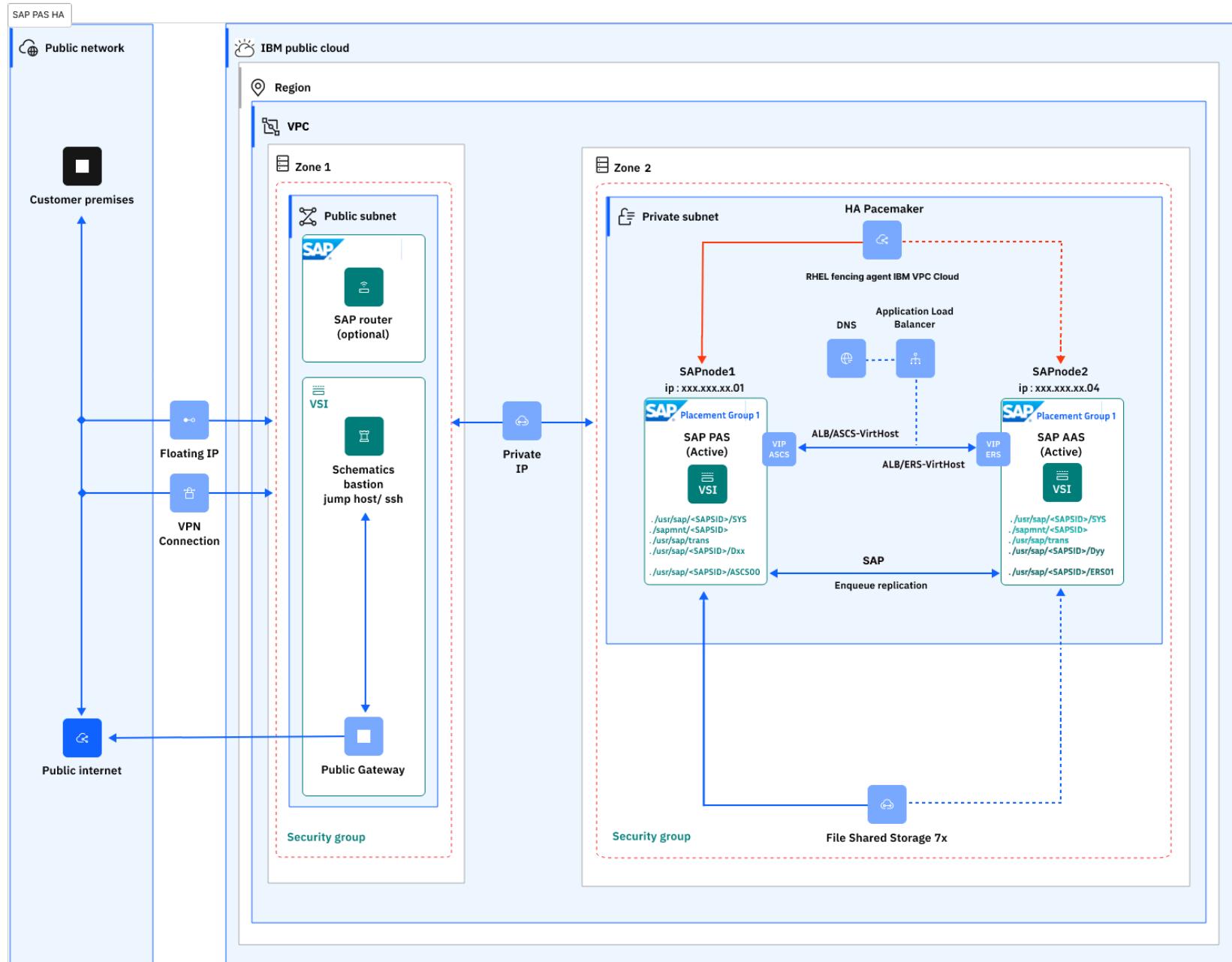
Use the following information to understand a simple use-case for planning, creating, and configuring resources for your VPC, and learn more about VPC overviews and VPC tutorials. For more information about the VPC, see [Getting started with Virtual Private Cloud \(VPC\)](#).

SAP products architecture on IBM Cloud VPC

A [Virtual Private Cloud \(VPC\)](#) contains one of the most secure and reliable cloud environments for SAP applications within your own VPC with virtual server instances. This represents an Infrastructure-as-a-Service (IaaS){: external} within IBM Cloud that offers all the benefits of isolated, secure, and flexible virtual cloud infrastructure from IBM. In comparison, the IBM Cloud classic infrastructure virtual servers offering uses virtual instances with native and VLAN networking to communicate with each other within a data center; however, the instances are restricted in one well-working pod by using subnet and VLAN networking as a gap scale up of virtual resources should rely between the pods. The IBM Cloud VPC network orchestrator layer concept eliminates the pod boundaries and restrictions, so this new concept handles all the networking for every virtual instance running within VPC across regions and zones.

Highly available system for SAP NetWeaver on IBM Cloud VPC

In a Highly Available (HA) system, every instance can run on a separate IBM Cloud virtual server instance. The cluster HA configuration for the SAP application server consists of two virtual server instances, each of them located in the same zone within the region by using placement groups. Placement groups assure that both cluster resources and cloud resources are also located in different compute nodes as specified in the following placement groups section:



SAP HA for SAP applications cluster nodes PAS (Active) and AAS (Active)

Placement groups on IBM Cloud VPC for SAP HA architecture

Placement Groups (PG) for VPC have two different anti-affinity strategies for high availability. By using the placement strategies, you minimize the chance of service disruption with virtual server instances that are placed on different hosts or into an infrastructure with separate power and network supplies.

The design of placement groups for IBM Cloud virtual servers solves this issue. Placement groups give a measure of control over the host on which a new public virtual server is placed. In this release, a “spread” rule is implemented, which means that the virtual servers within a placement group are spread onto different hosts. You can build a highly available application within a data center and know that your virtual servers are isolated from each other.

Placement groups with the spread rule are available to create in selected IBM Cloud data centers. After a spread rule is created, you can provision a virtual server into that group and ensure that it is not on the same host as any of your other virtual servers. This feature comes with no cost.

You can create your placement group and assign up to four new virtual server instances. With the spread rule, each of your virtual servers are provisioned on different physical hosts. In the following configuration example, the “Power Spread” option is used:

Name	Status	Resource group	Placement strategy	Attached instances
sap-ppg	Stable	rh-pacemaker	Host spread	-
pgroup1	Stable	Default	Host spread	2

Placement groups host spread

Placement group for VPC					
Name	Status	Resource group	Placement strategy	Attached instances	
sapha-poc	Stable	wes-ic4sap-resourcegroup	Power spread	4	
Items per page: 10 1 item 1 of 1 page					

Placement groups power spread

Following are the SAP instances that are required for HA scenario:

- ABAP SAP Central Services (ASCS) instance - contains the ABAP message server and the ABAP enqueue server.
- Enqueue Replication Server (ERS) instance for the ASCS instance.
- Database instance
- Primary Application Server (PAS) instance on node 1.
- Additional Application Server (AAS) instance on node 2.



Note: It is recommended to run both the ASCS instance and the ERS instance in a switchover cluster infrastructure.

IBM Cloud File Storage for VPC for SAP HA architecture

[IBM Cloud File Storage for VPC](#) technology is used to make the SAP directories available to the SAP system. The technologies of choice are NFS, shared disks, and cluster file system. If you have decided to use the HA solution for your SAP system, make sure that you properly address the HA requirements of the SAP file systems in your SAP environment.

File shares for VPC								
Name	Status	Resource groups	Location	Mount targets	Size	Replication role	Encryption type	
usrsap-as1-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-as2-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-sapsacs-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-sapers-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-sapmnt-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-sapsys-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-trans-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	80 GB	None	Provider managed	

File shares for VPC

- File shares that are mounted as NFS permanent file systems on both cluster nodes for SAP HA application:
 - `/usr/sap/<SAPSID>/SYS`
 - `/sapmnt<SAPSID>`
 - `/usr/sap/trans`
- Cluster-managed file systems for SAP HA application: ASCS
 - `/usr/sap/<SAPSID>/ASCS00`
 - `/usr/sap/<SAPSID>/ERS01`
- Permanent NFS mount on SAP HA application node 1 PAS instance:
 - `/usr/sap/<SAPSID>/Dxx`
- Permanent NFS mount on SAP HA application node 2 dialog instance:
 - `/usr/sap/<SAPSID>/Dyy`

Prerequisites

You need to install the hardware (hosts, disks, and network) and decide how to distribute the database, SAP instances, and if required, the Network File System (NFS) server over the cluster nodes.

Context

Following are the types of SAP directories:

- Physically shared directories: `/<sapmnt>/<SAPSID>` and `/usr/sap/trans`

- Logically shared directories that are bound to a node, such as `/usr/sap`, with the following local directories:
 - `/usr/sap/<SAPSID>`
 - `/usr/sap/<SAPSID>/SYS`
 - `/usr/sap/hostctrl`
- Local directories that contain the SAP instances such as `/usr/sap/<SAPSID>/ASCS<Instance_Number>`
- The global transport directory may reside on a separate SAP transport host as a standard three systems transport layer configuration.

You need at least two nodes and a shared file system for distributed ASCS and ERS instances. The assumption is that the rest of the components are distributed on other nodes.

ASCS and ERS installation

In order for the ASCS and ERS instances to be able to move from one node to the other, they need to be installed on a shared file system and use virtual hostnames based on the virtual IP.

In this VPC-based SAP HA solution, the shared file system that is required by the cluster is replaced by the NFS-mounted file storage, and the virtual IP is replaced by the Application Load Balancer for VPC (ALB).

In this scenario, three ALBs are used, one for each Single Point of Failure (SPOF) component in order to replace the virtual IP requirement: ALB for ASCS, ALB for ERS, and ALB for ASE Sybase. Each ALB is configured as a backend for the corresponding cluster servers and redirects all of the communication that is received on the front-end ports to the active server in the backend pool.

Load balancers for VPC						
Region:	Frankfurt	▼	<input type="text"/> poc	X		
Name	Status	Family	Resource group	Type	Hostname	Location
db-alb-hana-poc	Active	Application	wes-ic4sap-resourcegroup	Private	20bdd130-eu-de.lb.appdomain.cloud	Frankfurt
sap-alb-ers-poc	Active	Application	wes-ic4sap-resourcegroup	Private	3941d983-eu-de.lb.appdomain.cloud	Frankfurt
sap-alb-ascs-poc	Active	Application	wes-ic4sap-resourcegroup	Private	56a9190d-eu-de.lb.appdomain.cloud	Frankfurt

Application load balancer management of HA IPs mechanism

Private application load balancer

A [private application load balancer](#) is accessible through your private subnets that you configured to create the load balancer.

Similar to a public application load balancer, your private application load balancer service instance is assigned an FQDN; however, this domain name is registered with one or more private IP addresses.

IBM Cloud operations change the number and value of your assigned private IP addresses over time, based on maintenance and scaling activities. The backend virtual server instances that host your application must run in the same region and under the same VPC.

Use the assigned ALB FQDN to send traffic to the private application load balancer to avoid connectivity problems to your applications during system maintenance or scaling down activities.

Each ALB sends traffic to the cluster node where the application (ASCS, ERS, ASE Sybase DB) is running. During the cluster failover, the ALB redirects all the traffic to the new node where the resources are up and running.



Note: DNS-as-a-Service (DNSaaS) is the management IBM Cloud VPC DNS service of HA and FQDN (IPs) mechanism.



Note: The ALB has a default of 50 seconds for client and server timeout, so after 50 seconds of inactivity, the connection is closed. To support SAP connections through ALB and not lose connection after 50 seconds, you need to request a change this value to a minimum of 300 seconds (client-side idle connection = minimum 300s and server-side idle connection = minimum 300s). To request this change, open a support ticket. This is an account-wide change that affects all of the ALBs in your account. For more information, see [Connection timeouts](#).

DNS Services with VPC

[IBM Cloud DNS Services](#) provide private DNS to VPC users. Private DNS zones are resolvable only on IBM Cloud and from explicitly [permitted networks](#) in an account. To get started, create a DNS Services instance by using the IBM Cloud console.

DNS Services allows you to:

- Create the private DNS zones that are collections for holding the domain names.
- Create the DNS resource records under these DNS zones.
- Specify the access controls used for the DNS resolution of resource records on a zone-wide level.

DNS Services also maintains its own worldwide set of DNS resolvers. Instances that are provisioned under IBM Cloud on an IBM Cloud network can use resource records that are configured through IBM Cloud DNS Services by querying DNS Services resolvers.

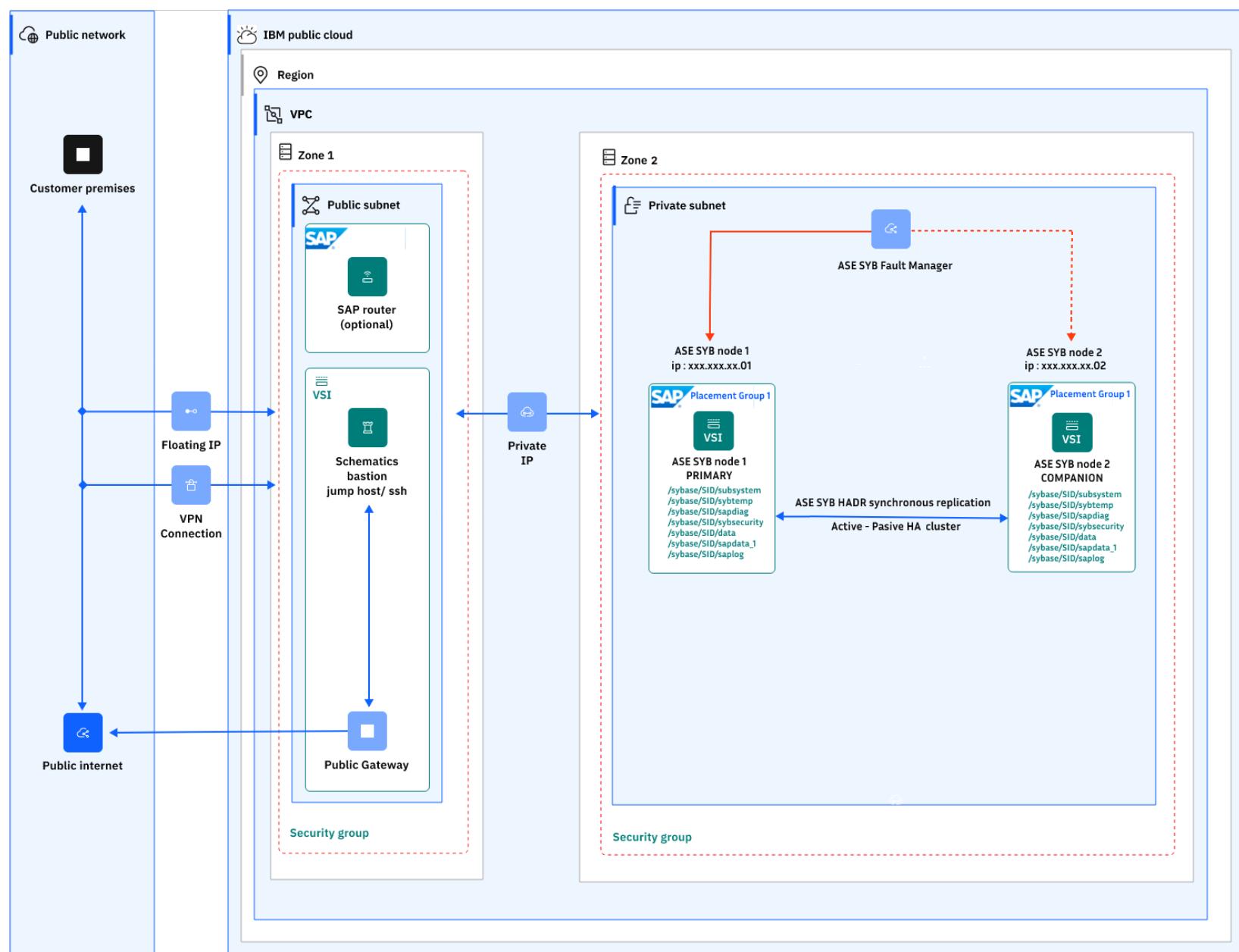
Resource records and zones that are configured through DNS Services are:

- Separated from the wider public DNS, and their publicly accessible records.
- Hidden from the system outside of and not part of the IBM Cloud private network.
- Accessible only from the system that you authorize on the IBM Cloud private network.
- Resolvable only via the resolvers provided by the service.

The DNS service maps the FQDN of each ALB to the virtual hostnames of the ASCS, ERS, and ASE Sybase that are used by SAP applications.

Type	Name	Value	TTL
CNAME	dbpochana	is an alias of 20bdd130-eu-de.lb.appdomain.cloud	12 hr
CNAME	sappocers	is an alias of 3941d983-eu-de.lb.appdomain.cloud	12 hr
CNAME	sappocases	is an alias of 56a9190d-eu-de.lb.appdomain.cloud	12 hr

Highly available system for SAP ASE Sybase database with HADR system



SAP HA for ASE Sybase DB instances cluster nodes primary (Active) and Secondary (Companion)

At the most basic level, a standard HA ASE Sybase cluster in an active(primary)-passive(companion) configuration has two nodes: one is the primary node and the other is the standby node. This means that the primary node is actively serving the active SAP DB instances (Primary and Companion), while the standby node is waiting to jump in if there is any failure.

The cluster is set with a virtual hostname IP (hostname is mapped to the FQDN of the ASE Sybase ALB through DNS, which is the same as

explained previously for SAP ASCS and ERS instances). Application instances (PAS and AAS) are used on the SAP profiles to call that particular component. The cluster assigns the virtual IP to the active node and uses a heartbeat monitor to confirm the availability of the components. If the primary node stops responding, it triggers the automatic failover mechanism that calls the standby node to step up to become the primary node. The ALB detects the change, redirects the traffic to the new active node, and assigns the virtual IP to it, restoring the component availability. Once fixed, the failed node comes online as a standby node.

SAP Sybase HADR system supports synchronous replication

The SAP Sybase HADR system supports synchronous replication between the primary and standby servers for high availability. An active-active setup is a two-node configuration where both nodes in the cluster include SAP ASE managing independent workloads, capable of taking over each others workload in the event of a failure.

The SAP ASE server that takes over the workload is called a secondary companion, and the SAP ASE server that fails is called the primary companion. Together they are companion servers. This movement from one node to another is called failover. After the primary companion is ready to resume its workload, it is moved back to its original node. This movement is called a failback.

When a system fails over, clients that are connected to the primary companion and use the failover property automatically reestablish their network connections to the secondary companion. You must tune your operating system to successfully manage both servers during fail over. See your operating system documentation for information about configuring your system for high availability. An SAP ASE configured for failover in an active-active setup can be shut down using the shutdown command only after you have suspended SAP ASE from the companion configuration, at both the server level and the platform level.

The always-on option in a High Availability and Disaster Recovery (HADR) system consists of two SAP ASE servers:

- Primary on which all transaction processing takes place.
- Warm standby (referred to as a "standby server" in DR mode, and as a "companion" in HA mode) for the primary server, and contains copies of designated databases from the primary server.



Note: The HADR feature that is shipped with SAP ASE version 16.0 SP02 supports only a single-companion server.

Some high-availability solutions (for example, the SAP Adaptive Server Enterprise Cluster Edition) share or use common resources between nodes. However, the HADR system is a "shared nothing" configuration, each node has separate resources including disks.

In an HADR system, servers are separate entities and data is replicated from the primary server to the companion server. If the primary server fails, a companion server is promoted to the role of primary server either manually or automatically. Once the promotion is complete, clients can reconnect to the new primary server, and see all committed data, including data that was committed on the previous primary server.

Servers can be separated geographically, which makes an HADR system capable of withstanding the loss of an entire computing facility.



Note: The HADR system includes an embedded SAP Replication Server, which synchronizes the databases between the primary and companion servers. SAP ASE uses the Replication Management Agent (RMA) to communicate with Replication Server and SAP Replication Server uses Open Client connectivity to communicate with the companion SAP ASE.

The Replication Agent detects any data changes made on the primary server and sends them to the primary SAP Replication Server. In the figure above, the unidirectional arrows indicate that, although both SAP Replication Servers are configured, only one direction is enabled at a time.

The HADR system supports synchronous replication between the primary and standby servers for high availability so the two servers can keep in sync with Zero Data Loss (ZDL). This requires a network link that is fast enough between the primary and standby server so that synchronous replication can keep up with the primary servers workload. Generally, this means that the network latency is approximately the same speed as the local disk IO speed, a few (fewer than 10) milliseconds. Anything longer than a few milliseconds may result in a slower response to write operations at the primary.

The HADR system supports asynchronous replication between the primary and standby servers for disaster recovery. The primary and standby servers by using asynchronous replication can be geographically distant, meaning they can have a slower network link. With asynchronous replication, Replication Agent Thread captures the primary servers workload, which is delivered asynchronously to SAP Replication Server. The SAP Replication Server applies these workload change to the companion server.

The most fundamental service that is offered by the HADR system is the failover; planned or unplanned from the primary to the companion server, which allows maintenance activity to occur on the old primary server, while applications continue on the new primary.

The HADR system provides protection in the event of a disaster. If the primary server is lost, the companion server can be used as a replacement. Client applications can switch to the companion server, and the companion server is quickly available for users. If the SAP Replication Server was in synchronous mode before the failure of the primary server, the Fault Manager automatically initiates failover with

zero data loss.

Fault Manager installation on the SAP ASCS node

The required parameters are asked during the installation process to create a profile for the fault manager and then adds it to the instance start profile. It is also possible to run the installation by using an existing profile: `sybdbfm install pf=<SYBHA.PFL>` In this case, the installation process will only ask for profile parameters missing in the profile.



Note: Fault manger is integrated with ASCS on same SAP PAS/AAS cluster (start/stop/move together).

There may be some data loss if the SAP Replication Server was in asynchronous mode and you must use manual intervention to failover for disaster recovery.

Connection attempts to the companion server without the necessary privileges are silently redirected to the primary companion via the login redirection mechanism, which is supported by Connectivity libraries. If login redirection is not enabled, client connections fail and are disconnected.

The SAP ASE HADR option installs the below components:

- SAP ASE
- SAP Replication Server
- Replication Management Agent (RMA)
- SAP Host Agent
- Fault Manager
- SAP ASE Cockpit



Note: This automation is offered at no cost; however, the provisioned infrastructure comes at cost.

VPC with Additional Application Server (AAS) ABAP on Linux for SAP HANA

You can use Terraform scripts to create a single-tier VPC and create the AAS to HANA and AnyDB infrastructure on the VPC. The Terraform scripts use the VPC information that you provide and then call the Ansible playbook to create the SAP architecture on the specified VPC. Terraform on IBM Cloud® enables predictable and consistent provisioning of IBM Cloud Virtual Private Cloud (VPC) infrastructure resources so that you can rapidly build complex, cloud environments. IBM Cloud VPC infrastructure consists of SAP certified hardware that uses Intel® Xeon CPUs and more Intel® technologies.

You have two deployment methods to choose from:

- Terraform scripts that run from the CLI on your bastion server.
- Schematics user interface accessed from your cloud dashboard menu.

You can create SAP AAS NetWeaver 7.x on the SAP HANA-based ABAP stack.

SAP solution implemented

Many SAP enterprise solutions are built on the SAP platform (SAP NetWeaver) including:

- SAP HANA as Primary Persistence for SAP NetWeaver-based applications
- SAP Business Suite applications (ERP, CRM, and SCM, and other applications),
- SAP Business Warehouse (BW), and
- Other SAP enterprise solutions

SAP NetWeaver has two distinct aspects, ABAP and Java. Many applications that are built on the SAP NetWeaver's ABAP or Java (or both) application servers run on SAP DB owned HANA and ASE Sybase either in AnyDB platforms (MSSQL, Oracle, and Db2).

Technical interfaces are available for applications that are built on the SAP NetWeaver AS ABAP and AS Java to run on SAP HANA and AnyDB. However, specific development enablement is normally required for each application to ensure that it runs optimally on the SAP HANA. SAP Business Suite applications (ERP, CRM, SCM, and other applications), SAP Business Warehouse (BW), and other SAP NetWeaver-based applications were modified to run on SAP HANA and have many advantages. Also, various components and complimentary applications that are built on SAP NetWeaver can also run on SAP HANA or AnyDB by using the provided SAP NetWeaver DB interfaces.

The SAP HANA as primary persistence for SAP NetWeaver-based applications scenario has one restriction: SAP NetWeaver ABAP and Java

application servers must run on separate hardware servers from the SAP HANA hardware.

What is created

The scripts automate the virtual infrastructure resources, provisioning the processes for the SAP architecture in an existing VPC with a distributed environment. SAP AAS NetWeaver 7.x (HANA or ASE SYB) application server on a distinct VSI VPC system and SAP HANA DB on a dedicated server type VSI VPC box are provisioned. The scripts work in two phases.

During the first phase of [Automate SAP bastion server – SAP media storage repository](#), the following virtual infrastructure resources based on the components from the existing VPC created by the bastion server are:

- 1 VPC where the virtual server instance is provisioned.
- 1 security group. The rules for this security group are:
 - Allow inbound DNS traffic (port 53).
 - Allow inbound SSH traffic (TCP port 22).
 - Allow all outbound traffic from the virtual server instance.
 - Allow all traffic in the security group.
- 1 subnet to enable the networking in your VPC.
- 2 virtual server instances with SAP certified storage and network configurations.
- 1 floating IP address used to access your VPC virtual server instance over the public network.

During the second phase, the Ansible Playbooks is called and the SAP architecture is installed for both dedicated virtual server instance (VSI) SAP application; VSI system and dedicated SAP HANA VSI box. The SAP architecture that is deployed on the SAP NetWeaver 7.x release is a stand-alone dedicated SAP HANA 2.0 box release. For more information about this architecture, see [Automating SAP HANA stand-alone virtual server instance on IBM Cloud® VPC by using Terraform and Ansible](#).

You can provision only one instance of the service per IBM Cloud region.

Schematics deployment

When you run the scripts with the Schematics interface, you:

- Enter the workspace information.
- Enter the GitHub path for the chosen solution either on NetWeaver AAS for HANA.
- Modify the parameters in the Schematics interface. They are the same parameters as the `input.auto.tfvars` file that you use with the cli.

Virtual server instance configuration

Following are the supported operating system images for SAP NetWeaver primary application server:

- ibm-redhat-8-4-amd64-sap-applications-2
- ibm-redhat-8-6-amd64-sap-applications-2
- ibm-sles-15-3-amd64-sap-applications-2
- ibm-sles-15-4-amd64-sap-applications-3

Following are the supported operating system images for SAP HANA database:

- ibm-redhat-8-4-amd64-sap-hana-2
- ibm-redhat-8-6-amd64-sap-hana-2
- ibm-sles-15-3-amd64-sap-hana-2
- ibm-sles-15-4-amd64-sap-hana-1

For both server instances there are:

- Two SSH keys are configured to access SSH as `root`.
- Three storage volumes as described in the `input.auto.tfvars` file.

What is created for anydb

The scripts use the information that you provide for an existing VPC and deploy AAS to SAP HANA or AnyDB on a different host than CI (SAP Central Instance) VSI host. For more information about this architecture, see [SAP NetWeaver 7.x on UNIX with HANA or AnyDB on IBM Cloud](#)

[VPC on IBM Cloud VPC](#). You specify the information for the VPC to use in the `input.auto.tfvars` file.

The scripts call the Ansible Playbooks to install the SAP architecture.

Script files

The configuration and script files are provided on GitHub. Each supported interface for the SAP solution installation has its own folder in the GitHub repository:

- [GitHub repository for Terraform – AAS HANA](#)

Terraform interface

To run the Terraform script, you modify:

- The `input.auto.tfvars` file to specify the existing VPC resources for your solution. Specify the variables for the existing VPC:
 - VPC name
 - Security group
 - Subnet
 - Hostname
 - Profile
 - Image
 - Up to two SSH keys

You can change the default SAP system configuration settings to match your solution. You can also specify the location where you downloaded the SAP kits.

The IBM Cloud Provider plug-in for Terraform on IBM Cloud uses these configuration files to install AAS to SAP HANA and AnyDB on the specified VPC in your IBM Cloud account.

Support

There are no warranties of any kind, and there is no service or technical support available for these materials from IBM®. As a recommended practice, review carefully any materials that you download from this site before using them on a live system.

Though the materials provided herein are not supported by the IBM® Service organization, your comments are welcomed by the developers, who reserve the right to revise, readapt or remove the materials at any time. To report a problem, or provide suggestions or comments, open a GitHub issue.

Before you begin

Before you use the scripts in the bastion cli:

- Set up your account to access the VPC. Make sure that your account is [upgraded to a paid account](#).
- If you have not already, create a Bastion server to store the SAP kits. For more information, see [Automate SAP bastion server - SAP media storage repository](#).
- Download the SAP kits from the SAP Portal to your Deployment Server. Make note of the download locations. Ansible decompresses the files. For more information, see the [readme](#) file.
- [Create or retrieve an IBM Cloud API key](#). The API key is used to authenticate with the IBM Cloud platform and to determine your permissions for IBM Cloud services.
- [Create or retrieve your SSH key ID](#). You need the 40-digit UUID for the SSH key, not the SSH key name.
- Terraform should already be installed on the bastion server that you deployed. For more information, see [Bastion server for SAP deployment](#).
- (Optional - Catalog Tile) create secrets for your credentials and passwords by using the [Secrets Manager](#).

Deploying SAP AAS NetWeaver 7.x on HANA by using the Schematics user interface

Use these steps to configure the SAP Additional Application Server (AAS) NetWeaver with HANA or AnyDB on your existing VPC by using the Schematics interface. The script takes 2 - 3 hours to complete.

1. From the IBM Cloud menu, select **Schematics**.
2. Click **Create** workspace.

3. On the **Specify template** page:
 - Enter the URL for the Schematics interface.
 - Select the **Terraform version** that is listed in the readme file.
 - Click **Next**.
4. On the **workspace details** page:
 - Enter a name for the workspace.
 - Select a **Resource group**.
 - Select a **Location** for your workspace. The workspace location does not have to match the resource location.
 - Select **Next**.
5. Select **Create** to create your workspace.
6. On the workspace settings page, in the input variables section, review the default input variables and provide values that match your solution.
 For a more detailed description of each parameter, check the GitHub repo [AAS HANA readme](#) file, chapter "Input parameter file". Also, make sure to mark the parameters that contain sensitive information like passwords, API, and ssh private keys as "sensitive". These parameters are marked as "sensitive" in the readme file, under "Input parameter file".
7. On the workspace settings page, click **Generate plan**. Wait for the plan to complete.
8. Click **View log** to review the log files of your terraform execution plan.
9. Apply your Terraform template by clicking **Apply plan**.
10. Review the log file to ensure that no errors occur during the provisioning, modification, or deletion process.

Deploying SAP AAS NetWeaver (ABAP) on HANA with the Deployable Architecture tile interface

Use these steps to configure the SAP AAS NetWeaver (ABAP) on HANA on your existing VPC by using the catalog tile interface. The script takes 2 - 3 hours to complete.

1. From the IBM Cloud catalog, select **VPC with Additional Application Server ABAP on Linux for SAP HANA** on HANA tile. The **Create** tab opens for VPC with Additional Application Server ABAP on Linux for SAP HANA. For more information about this deployment, see the About tab or the readme file link.
2. Select the latest version.
3. Select **VPC with Additional Application Server ABAP on Linux for SAP HANA on Deployable Architecture tile** variation.
4. Click **Review deployment** options:
 - **Add to project** to add this deployment to an IBM Cloud project and combine it with other deployments. IBM Cloud projects include several more pipeline steps before deployment, including deployment validation, cost calculation, compliance verification, and approval process.
 - **Create from the CLI** to get the CLI command. With this command you can trigger the deployment from the CLI.
 - **Work with code** to embed the code into other terraform deployments.
 - **Deploy with IBM Cloud Schematics** to trigger the deployment process directly.
5. Select **Deploy with IBM Cloud Schematics**.
6. Add the input parameters for this installation. There are 3 categories of parameters:
 - **Workspace** - These parameters define the workspace that is automatically created in Schematics:
 - Enter a name for the workspace or use the default name.
 - The Resource Group used to create resources. Use default or create a Resource Group.
 - Select a location to create your Schematics workspace. The workspace location need not match the resource location.
 - **Required input variables** - Review the default input variables and provide values that match your solution. These parameters are specific to your deployment. For more detailed information, see the [Readme file](#).

Parameter	Description
BASTION_FLOATING_IP	Required only for Schematics Deployments. The Floating IP from the Bastion Server.

HOSTNAME	The hostname for the VSI. The hostname should be up to 13 characters as required by SAP. For more information on the rules regarding hostnames for SAP systems, check SAP Note 611361: Hostnames of SAP ABAP Platform servers
REGION	The cloud region to deploy the solution. The regions and zones for VPC are listed here . Review supported locations in IBM Cloud Schematics here . Sample value: eu-de.
RESOURCE_GROUP	The name of an existing Resource Group for VSIs and Volumes resources. Default value: "Default". The list of Resource Groups is available here .
SECURITY_GROUP	The name of an existing Security group. The list of security groups is available here .
SSH_KEYS	The list of SSH Keys UUIDs that are allowed to SSH as root to the VSI can contain one or more IDs. The list of SSH Keys is available here . Sample input (use your own SSH UUIDs from IBM Cloud){: external}: ["r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a", "r010-3fcfd9fe7-d4a7-41ce-8bb3-d96e936b2c7e"]
SUBNET	The name of an existing subnet. The list of subnets is available here .
VPC	The name of an existing VPC. The list of VPCs is available here .
ZONE	The cloud zone where to deploy the solution. Sample value: eu-de-2.
ibmcloud_api_key	IBM Cloud API key (Sensitive* value).
private_ssh_key	Required only for Schematics Deployments - Input your id_rsa private key pair content in OpenSSH format (Sensitive* value). This private key should be used only during the terraform provisioning and it is recommended to be changed after the SAP deployment.
hdb_instance_number	The instance number of the SAP HANA database server.
sap_aas_instance_number	Technical identifier for the internal processes of the additional application server.
sap_ascs_instance_number	Technical identifier for the internal processes of ASCS.
sap_ci_host	IP address of the existing SAP Central Instance.
sap_ci_hostname	The hostname of the existing SAP Central Instance.
sap_ci_instance_number	Technical identifier for the internal processes of the Central Instance.
sap_sid	The SAP system ID identifies the entire SAP system.
sap_main_password	Common password for all users that are created during the installation (See Obs*).

Required Variables

- **Optional variables** - Review and update the optional input variables. The Ansible scripts expect the SAP kits to be in the default locations listed. For more information, see the [Readme file - Input Parameters](#).

Parameter	Description
ID_RSA_FILE_PATH	The file path for private_ssh_key is automatically generated by default. If it is changed, it must contain the relative path from Git repo folders. Default value: "ansible/id_rsa".
IMAGE	The OS image used for the VSI. A list of images is available here .
PROFILE	The profile used for the VSI. A list of profiles is available here . For more information about supported DB/OS and IBM Gen 2 Virtual Server Instances (VSI), check SAP Note 2927211: SAP Applications on IBM Virtual Private Cloud .

VOL1	Volume 1 Size - The size for the disks in GB that are to be attached to the VSI and used by SAP.
VOL2	Volume 2 Size - The size for the disks in GB that are to be attached to the VSI and used by SAP.
kit_sapcar_file	Path to the sapcar binary, as downloaded from SAP Support Portal.
kit_swpm_file	Path to the SWPM archive (SAR), as downloaded from SAP Support Portal.
kit_saphostagent_file	Path to the SAP Host Agent archive (SAR), as downloaded from SAP Support Portal.
kit_hdbclient_file	Path to the HANA DB client archive (SAR), as downloaded from SAP Support Portal.

Optional Variables

7. Accept the license agreement.
8. Select **Deploy**. The deployment starts and you are directed to the Schematics page that displays the script log files for you to monitor the deployment progress.

Creating the infrastructure using Terraform with the bastion server CLI

Use these steps to configure the IBM Cloud Provider plug-in and use Terraform to install SAP AAS to SAP HANA and AnyDB on your existing VPC on an already deployed SAP NetWeaver 7.X with SAP HANA 2.0 or ASE SYB as a Central Instance.

The script takes 1 - 2 hours to complete.

1. Access the bastion server cli.
2. Clone the solution repository and change to the folder.

ASE SYB 16 Clone the solution repository from <https://github.com/IBM-Cloud/sap-aas-abap-ase-syb> and cd to the sap-aas-abap-ase-syb/cli folder.

```
$ git clone https://github.com/IBM-Cloud/sap-aas-abap-ase-syb
cd sap-aas-abap-ase-syb/cli/
```

SAP HANA 2.0: Clone the solution repository from <https://github.com/IBM-Cloud/sap-abap-hana-aas> and cd to the sap-abap-hana-aas folder.

```
$ git clone https://github.com/IBM-Cloud/sap-abap-hana-aas.git
cd sap-abap-hana-aas/
```

3. Modify the `input.auto.tfvars` file to specify the information for the existing VPC, your region, zone, networking component names, hostname for the AAS VSI,profile, and image. You need your 40-digit SSH key ID for this file. The second SSH key is optional. For more options for profile, see [Instance Profiles](#). For more options, see [Images](#). For descriptions of the variables, see the [readme](#) file.

The VSI OS images that are supported for this solution for Netweaver Additional Application Server are:

- ibm-redhat-8-4-amd64-sap-applications-2
- ibm-redhat-8-6-amd64-sap-applications-2
- ibm-sles-15-3-amd64-sap-applications-2
- ibm-sles-15-4-amd64-sap-applications-4

```
$ # Infra VPC variables for ASE SYB
REGION    = "eu-de"
ZONE      = "eu-de-2"
VPC       = "ic4sap"                      # EXISTING Security group name
SECURITY_GROUP = "ic4sap-securitygroup"     # EXISTING Security group name
RESOURCE_GROUP = "wes-automation"
SUBNET    = "ic4sap-subnet"                 # EXISTING Subnet name
SSH_KEYS   = [ "r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a" , "r010-3fcfd9fe7-d4a7-41ce-8bb3-
d96e936b2c7e" ]

# SAP AAS VSI variables:
```

```

HOSTNAME = "sapnwase-as01"
PROFILE = "bx2-4x16"
IMAGE = "ibm-redhat-8-4-amd64-sap-applications-2

$ # Infra VPC variables for ABAP HANA
REGION      = "eu-de"
ZONE        = "eu-de-2"
VPC          = "ic4sap" # EXISTING Security group name
SECURITY_GROUP = "ic4sap-securitygroup" # EXISTING Security group name
RESOURCE_GROUP = "wes-automation"
SUBNET       = "ic4sap-subnet" # EXISTING Subnet name
SSH_KEYS     = [ "r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a" , "r010-3fc9fe7-d4a7-41ce-8bb3-d96e936b2c7e" ]
ID_RSA_FILE_PATH = "ansible/id_rsa"

# SAP AAS variables:
HOSTNAME = "sapnwapp"
PROFILE = "bx2-4x16"
IMAGE = "ibm-redhat-8-6-amd64-sap-applications-2"

```

4. Customize your SAP system configuration. In the same file, input.auto.tfvars, edit the SAP system configuration variables that are passed to the Ansible automated deployment. For descriptions of the variables, see the [readme](#) file.

```

$ # SAP system configuration - for ASE SYB
sap_sid = "NWD"
sap_ci_host = "10.243.132.10"
sap_ci_hostname = "sapnwase"
sap_ci_instance_number = "00"
sap_asc_s_instance_number = "01"
sap_aas_instance_number = "00"

# Kits paths
kit_sapcar_file = "/storage/NW75SYB/SAPCAR_1010-70006178.EXE"
kit_swpm_file = "/storage/NW75SYB/SWPM10SP31_7-20009701.SAR"
kit_saphotagent_file = "/storage/NW75SYB/SAPHOSTAGENT51_51-20009394.SAR"

```

```

$ # SAP system configuration - for ABAP HANA
sap_sid = "NWD"
sap_ci_host = "10.243.132.10"
sap_ci_hostname = "sapnwapp01"
sap_ci_instance_number = "00"
sap_asc_s_instance_number = "01"
hdb_instance_number = "00"
sap_aas_instance_number = "00"

# Kits paths
kit_sapcar_file = "/storage/NW75HDB/SAPCAR_1010-70006178.EXE"
kit_swpm_file = "/storage/NW75HDB/SWPM10SP31_7-20009701.SAR"
kit_saphotagent_file = "/storage/NW75HDB/SAPHOSTAGENT51_51-20009394.SAR"
kit_hdbclient_file = "/storage/NW75HDB/IMDB_CLIENT20_009_28-80002082.SAR"

```

Ansible decompresses the rest of the SAP kit files. For more information, see the [readme](#) file.

5. Initialize the Terraform CLI.

```
terraform init
```

6. Create a Terraform execution plan. The Terraform execution plan summarizes all the actions that are done to create the virtual private cloud instance in your account.

```
terraform plan plan1
```

Enter an SAP main password and your API key.

The SAP main password must be 10 - 14 characters long and contain at least one digit (0-9). It can contain only the following characters: a-z, A-Z, 0-9, @, #, \$, . *This password cannot contain exclamation points '!'. The password must not start with a digit or an underscore ().*

7. Verify that the plan shows all of the resources that you want to create and that the names and values are correct. If the plan needs to be adjusted, edit the input.auto.tfvars file to correct resources and run terraform plan again.
8. Apply the saved plan.

```
$ terraform apply "plan1"
```

The virtual private cloud and components are created and you see output similar to the `terraform plan` output.

9. Add the SAP credentials and the virtual server instance IP to the SAP GUI. For more information about the SAP GUI, see [SAP GUI](#).

Next steps

If you need to rename your resources after they are created, modify the `input.auto.tfvars` file to change the names and run `terraform plan` and `terraform apply` again. Do not use the IBM Cloud Dashboard and user interface to modify your VPC after it is created. The Terraform scripts create a complete solution and selectively modifying resources with the user interface might cause unexpected results.

If you need to remove the SAP Netweaver 7.X on HANA or AnyDB installation, go to your project folder and run `terraform destroy`. The `terraform destroy` command does not remove the VPC in this scenario because the VPC was created before these Terraform scripts were run.

Related information

For more information about Terraform on IBM Cloud, see [Getting started with Terraform on IBM Cloud](#).

For more information about using Terraform for creating only a VPC for SAP, without the SAP architecture, see [Creating single-tier virtual private cloud for SAP by using Terraform](#).

SAP One Support Notes that apply to this document:

- [SAP Note 84555 - Windows Server, Linux®, and UNIX: Certified hardware](#)
- [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#)
- [SAP Note 2923773 - Linux® on IBM Cloud \(IaaS\): Adaption of your SAP license](#)
- [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#)
- [SAP Note 2369910 - SAP Software on Linux®: General information](#)
- [SAP Note 171380 - Released IBM hardware \(Intel processors\) and IBM cloud services offers](#)
- [SAP Note 1380654 - SAP support in IaaS environments](#)

This document is referenced by:

- [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#)
- [SAP Note 2588225 - SAP on IBM Cloud: Protect against speculative execution vulnerabilities](#)
- [SAP Note 1380654 - SAP support in IaaS environments](#)
- [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#)

SAP workloads in VPC

Introduction to SAP workloads on IBM Cloud® VPC

The objective of this document is to provide solution designs for the deployment of SAP solution types on IBM Cloud® Virtual Private Cloud (VPC). This solution:

- Accelerate and simplify solution design by providing a standard IBM Cloud® VPC deployment architecture. For more information, see [Architecture framework](#).
- Provide end to end enterprise-class solution design that includes diagrams, component architecture decisions, and rationale for cloud component selection for a secure, resilient SAP on IBM Cloud VPC.
- Verify if requirements can be met by performance, system availability, and security perspectives.

 **Important:** SAP configuration and SAP component deployment scenarios are not covered in this solution design. It is limited to IBM Cloud infrastructure options to support SAP workloads.

Enterprise-class, mission-critical workloads need to be secure, resilient, and provide High Availability (HA) and Disaster Recovery (DR). This pattern can be used as a guide to meet typical user requirements and provide a base reference solution for a secure and resilient SAP NetWeaver and HANA or SAP NetWeaver and AnyDB deployment to IBM Cloud VPC. This supports the deployment of SAP Business Applications running on SAP NetWeaver, SAP HANA or SAP AnyDB, and other SAP products by using other technologies. Other technologies include SAP Content Server or newer applications such as SAP Data Intelligence.

IBM Cloud SAP-Certified infrastructure provides the flexibility to run SAP workloads in the IBM Cloud and also addresses issues such as:

- Moving SAP workloads to the cloud
- Rapidly expanding or contracting capacity
- Supplementing an existing private cloud architecture

IBM Cloud® VPC introduction

IBM Cloud Virtual Servers for VPC offers fast provisioning compute capacity, also known as virtual machines with the highest network speeds and most secure, software-defined networking resources available on the IBM Cloud. This is built on IBM Cloud Virtual Private Cloud (VPC) featuring powerful, 4th Gen Intel® Xeon® processors with new Intel® Software Guard Extensions (Intel® SGX®) to help protect data in use through a unique application isolation technology.

A VPC is a public cloud offering that an enterprise uses to establish its own private cloud-like computing environment on shared [public cloud](#) infrastructure. VPC gives an enterprise the ability to define and control a virtual network that is logically isolated from all other public cloud tenants, creating a private, secure place on the public cloud.

A VPC's logical isolation is implemented by using virtual network functions and security features that give an enterprise user granular control over which IP addresses or applications can access particular resources.

SAP workloads on the IBM Cloud® VPC

As part of an ongoing partnership with SAP, IBM is constantly providing new platform configurations for certification by SAP as part of its Infrastructure-as-a-Service (IaaS) offering, designed to best fit any SAP workload scenario from small business to intensive workloads running SAP HANA.

SAP note [2927211](#) offers a complete description of SAP products, database solutions, and OS releases that are available in IBM Cloud VPC. These are supported by SAP which is part of IBM's Infrastructure-as-a-Service (IaaS) virtual machines and bare metal servers.

The Infrastructure-as-a-Service (IaaS) server types within the IBM Cloud VPC Infrastructure environment are the Intel Bare Metal Servers and the Intel Virtual Servers, based on IBM Cloud's managed KVM hypervisor.

Linux operating systems

Windows Server operating

systems

Applications running on the ABAP Platform (inter alia the technology foundation for S/4 HANA 1809 and higher)	<ul style="list-style-type: none"> ■ SAP Kernel 7.53 (min. PL #622 for all JAVA components) ■ SAP Kernel 7.73 (min. PL #258) ■ SAP Kernel 7.77 (min. PL #212) ■ higher SAP Kernel versions 	<ul style="list-style-type: none"> ■ SAP Kernel 7.53 (min. PL #718 for all JAVA components) ■ SAP Kernel 7.73 (min. PL #322) ■ SAP Kernel 7.77 (min. PL #313) ■ SAP Kernel 7.81 (min. PL #25) ■ higher SAP Kernel versions
---	--	---

Applications running on the Application Servers ABAP and/ or Java as part of SAP NetWeaver 7.4 or higher	<ul style="list-style-type: none"> ■ SAP Kernel 7.49 (min. PL #913) ■ SAP Kernel 7.53 (min. PL #622) ■ higher SAP Kernel versions 	<ul style="list-style-type: none"> ■ SAP Kernel 7.49 (min. PL #932) ■ SAP Kernel 7.53 (min. PL #718) ■ higher SAP Kernel versions
--	--	--

Applications running on the Application Server ABAP and/ or Java as part of SAP NetWeaver 7.1 or higher	<ul style="list-style-type: none"> ■ SAP Kernel 7.21 EXT (min. PL #1322) ■ SAP Kernel 7.22 EXT / EX2 (min. PL #1011) ■ higher SAP Kernel versions 	<ul style="list-style-type: none"> ■ SAP Kernel 7.21 EXT (min. PL #1400) ■ SAP Kernel 7.22 EXT (min. PL #1018) ■ higher SAP Kernel versions
---	--	--

Applications running on the Application Server ABAP as part of SAP NetWeaver 7.0x	<ul style="list-style-type: none"> ■ SAP Kernel 7.21 EXT (min. PL #1322) ■ SAP Kernel 7.22 EXT / EX2 (min. PL #1011) ■ higher SAP Kernel versions 	<ul style="list-style-type: none"> ■ SAP Kernel 7.21 EXT (min. PL #1400) ■ SAP Kernel 7.22 EXT (min. PL #1018) ■ higher SAP Kernel versions
---	--	--

SAP Kernel and supported operating system

Versions

SAP Search and Classification (TREX)	<ul style="list-style-type: none"> ■ SAP TREX 7.10 on RHEL 7.4 and higher ■ SAP TREX 7.10 on SLES 12 SP4 and higher ■ SAP TREX 7.10 on Windows Server 2016 and higher
--------------------------------------	--

SAP liveCache	The minimal version for SAP LC/LCAPPs 10.0 SP 46 including liveCache 7.9.10.04 and LCA-Build 46, released for EhP 4 for SAP SCM 7.0 or higher. For details, see SAP Note 2074842 .
---------------	--

SAP Content Server	SAP Content Server 7.53 and higher version on Linux and Windows Server. For more information, see SAP Note 719971 (SAP Content Server release strategy){: external}.
--------------------	--

SAP IQ	The SAP IQ 16.x version is used. For more information, see SAP Note 2133194 .
--------	---

SAP Business Objects	For the support of SAP BusinessObjects Business Intelligence suite on IBM Cloud see SAP Note 2279688 .
----------------------	--

SAP Business One	<ul style="list-style-type: none"> ■ SAP Business One (B1), version for SQL Server according to the Hardware Requirements Guide. ■ SAP Business One (B1), version for HANA according to SAP Note 2058870 (SAP Business One, version for SAP HANA on public IaaS platforms).
------------------	---

SAP products and supported versions

Versions

RDBMS	<ul style="list-style-type: none"> ■ IBM Db2 for LUW version 10.5 or higher. ■ SAP ASE 16.0 SP03 or higher, most recent patch level highly recommended - see also SAP Note 2922454 (SAP Adaptive Server Enterprise (SAP ASE) on Cloud Platforms). ■ SAP MaxDB 7.9, most recent patch level highly recommended - see also SAP Note 2949393 (SAP MaxDB/liveCache in Cloud environments). ■ Microsoft SQL Server 2012 and higher. ■ SAP HANA - See the detailed server specifications in the Certified IaaS Platform section of the Certified and Supported SAP HANA Hardware Directory.
-------	--

RDBMS supported versions

Supported Operating Systems

- Red Hat Enterprise Linux (RHEL) version 7 or higher.
- SUSE Linux Enterprise Server (SLES) version 12 SP4 or higher.
- Microsoft Windows Server 2016, 2019, and 2022.

For more information on valid DB/OS combinations please consult the SAP [Product Availability Matrix \(PAM\)](#).

Prerequisites

- Create an API key for your VPC. The API key is used to authenticate with the IBM Cloud platform and to determine your permissions for IBM Cloud services. For more information, see [Create or retrieve an IBM Cloud API key](#).
- Create a SSH key on the IBM Cloud VPC. For more information, see [Create or retrieve your SSH key ID](#).

Before deploying any SAP workload in the IBM Cloud VPC, there are certain IBM Cloud services which need to be provisioned. The order in which these are provisioned is mentioned here:

- VPC for SAP provisioning
 - New Subnet for the VPC
 - Security Group for the VPC
 - New Intel Virtual Server Instance (VSI)
 - Block storage for Intel Virtual Server Instances (VSIs) – additional storage can be added post VSI creation
 - NFS-based file storage for VPC – additional request for certain deployment scenarios

VPC for SAP provisioning



Important: Before deploying any SAP workload into VSI, a IBM Cloud VPC must be created.

Following are the steps to setup the VPC:

1. Click **Menu** icon > **VPC Infrastructure** > **Network** > **VPCs**.
2. Choose the **Region** and click **Create**.
3. Confirm the **Location** (Geography and Region).
4. Enter a unique name for the VPC.
5. Select a **Resource group**. Use resource groups to organize your account resources for access control and billing purposes.
For more information, see [Best practices for organizing resources in a resource group](#) and [What makes a good resource group strategy?](#).
6. **Optional:** Enter the tags to help you organize and find your resources. You can add more tags later. For more information, see [Working with tags](#).
7. Select whether the default security group allows inbound SSH and ping traffic to virtual server instances in this VPC. You can configure more rules for the default security group later.
8. **Optional:** Default address prefixes. Disable this option if you do not want to assign default subnet address prefixes to each zone in your VPC. After you create the VPC, go to the details page and set your own subnet address prefixes. If you disable this option, the new subnet for VPC section will be hidden and requires manual definition after the VPC is created. The value is set to default.

! **Important:** You can only enable a VPC for classic access when it is created. You cannot update a VPC to add or remove classic access. In addition, you can have only one classic access VPC in your account at any time. For more information, see [Create an IBM Cloud VPC](#).

New subnet for VPC

Following are the steps to create a new subnet for the VPC:

1. To add a new subnet during the creation of new VPC, click **Add subnet**.
2. Enter a **unique name** for the VPC subnet.
3. Select a **Resource group** for the subnet.
4. Select a **Location** for the subnet. The location consists of a region and a zone.



Tip: The region is automatically inherited from the VPC (currently in creation).

5. **Optional:** Make use of tags to better organize and find your resources.
6. Enter an **address prefix**, **number of addresses**, and an **IP range** for the subnet. The IP range is entered in CIDR notation, for example: 10.240.0.0/24. Usually, you can use the default IP range. If you want to specify a custom IP range, you can use the IP range calculator to select a different address prefix or change the number of addresses.
- !** **Important:** A subnet cannot be resized after it has been created.
7. Attach a public gateway to the subnet to allow all the attached resources to communicate with the public internet (not mandatory for certain scenarios).
8. Click **Create** virtual private cloud.

If you have disabled the default address prefixes, which hides the new subnet for VPC section on the VPC ordering page, then you need to manually define your subnets before provisioning your virtual servers for VPC. Following are the steps to set up your subnets:

1. Click **Menu** icon > **Infrastructure** > **Network** > **Subnets**.
2. Choose the desired **Region** and click **Create**.
3. Confirm the **Location** (Geography, Region and Zone).
4. Enter a unique name and select the VPC to be associated.
5. Select a **Resource group**.
6. **Optional:** Use tags to better organize and find your resources.
7. Choose the VPC fro the subnet to be associated.
8. Enter an **Address prefix**, **Total IP addresses** and an **IP range** for the subnet. The IP range is entered in CIDR notation, for example: 10.240.0.0/24. Usually, you can use the default IP range. If you want to specify a custom IP range, you can use the IP range calculator to select a different address prefix or change the number of addresses.
9. Leave the values as default for the **Routing table** and **Subnet access control list**.
10. Choose a **Public gateway** to the subnet to allow all the attached resources to communicate with the public internet (not mandatory for certain scenarios).
11. Review the costs of your subnet resource and click **Create subnet**.

Security Group for VPC

After creating the VPC and subnet, a default Security Group will be automatically provisioned.

1. Navigate to **Menu** icon > **Infrastructure** > **Network** > **VPCs**.
2. Selecting the VPC, displays the **Overview** tab, showing various information on the VPC and the default security group.
3. Click on the default security group, to display the Overview tab.
4. Navigate to the **Rules** tab to bring forward the Inbound rules and Outbound rules settings.

By default, this Security Group is unrestricted, and the user should close the Inbound/Outbound access according to its security requirements and regulations.

New Intel Virtual Server Instance (VSI)

Before provisioning an Intel VSI (compute component of any SAP Workload), you should understand the available profile families in the IBM Cloud VPC.

Virtual server profile names

In IBM Cloud VPC, the profile families that are certified for SAP are:

- Compute Optimized
- Balanced
- Memory Optimized
- Very High Memory Optimized
- Ultra High Memory Optimized

All the memory family profiles provide memory intensive workloads, such as demanding database applications, in-memory analytics workloads, and are designed for SAP HANA workloads. For more information, see [x86-64 instance profiles](#). For more information about SAP profiles, see [Intel Virtual Server certified profiles on VPC infrastructure for SAP HANA](#) and [Intel Virtual Server certified profiles on VPC infrastructure for SAP NetWeaver](#).

The following profile families are available to provision the VSI:

Profile Families	Description
Balanced	Balanced profiles offer a core to RAM ratio that is best for midsize databases and common cloud applications with moderate traffic.
Compute	Compute profiles offer a core to RAM ratio that is best for moderate to high web traffic workloads. Compute profiles are best for workloads with intensive CPU demands, such as high web traffic workloads, production batch processing, and front-end web servers.
Memory	Memory profiles offer a core to RAM ratio that is best for memory caching and real-time analytics workloads. Memory profiles are best for memory intensive workloads, such as large caching workloads, intensive database applications, or in-memory analytics workloads.
Very High Memory	Very High Memory profiles offer a core to RAM ratio of 1 vCPU to 14 GiB of RAM. This family is optimized for running small to medium in-memory databases and OLAP workloads, such as SAP BW/4 HANA.
Ultra High Memory	Ultra High Memory profiles offer the most memory per core with 1 vCPU to 28 GiB of RAM. These profiles are optimized to run large in-memory databases and OLTP workloads, such as SAP S/4 HANA.
GPU	GPU enabled profiles provide on-demand access to NVIDIA V100 and A100 GPUs to accelerate AI, high-performance computing, data science, and graphics workloads.
Storage Optimized	Storage Optimized profiles offer temporary SSD instance storage disks at a ratio of 1 vCPU to 300 GB instance storage with a smaller price point per GB. These profiles are designed for storage-dense workloads and offer virtio interface type for attached disks.
Confidential Compute	Confidential Compute-supported profiles use processor reserved memory called EPC (Enclave Page Cache) to encrypt application data. Processor reserved memory EPC maintains confidentiality and integrity.

Profile Families

The first letter of the profile name indicates the profile family:

First letter	Characteristics of the related profile family
c	Compute Optimized family, vCPU to memory ratio 1:2 or 1:2.5
b	Balanced family, vCPU to memory ratio 1:4 or 1:5
m	Memory Optimized family, higher vCPU to memory ratio 1:8 or 1:10

v	Very High Memory Optimized family, very high vCPU to memory ratio 1:14
u	Ultra High Memory Optimized family, ultra high vCPU to memory ratio 1:28
First letter of profile family	

Instance storage

Instance storage is a set of one or more solid-state drives (full or isolated partial storage spaces) attached to your virtual server instance when the instance is provisioned. Instance storage is close to the compute resources of the virtual server and on a high-speed communication channel that is independent from the network. An instance storage disk provides fast, affordable, temporary storage to improve the performance of cloud native workloads with scratch space, caching buffers, or a place for replicated data. The data that is stored on instance storage is temporary, which means that the data is attached directly to the instance lifecycle. The instance storage disk is automatically created and destroyed with the instance. Instance storage data is not lost when an instance is rebooted.

Instance storage is a complementary storage technology to boot and block storage volumes that are offered with VPC. For more information, see [About instance storage on IBM Cloud VPC](#). Below are the examples for instance storage disks:

- **Distributed File Systems:** Technologies like Hadoop Distributed File System (HDFS) replicate data across multiple servers to improve read bandwidth and ensure reliability. It is recommended to maintain at least three copies of the data, ideally across availability zones, when using Instance Storage for these workloads.
- **Transactional jobs:** Transaction processing usually creates a significant number of temporary files. Instance storage is a great place to temporarily store that data while the transactions are processed, with the results stored persistently on a data volume.

Block storage for virtual servers on VPC infrastructure

When you create secondary data volumes, you select a volume profile to meet your requirements. Volume profiles are available in three predefined [tiers](#) or as a [custom profile](#). These volume profiles relate to virtual server instance profiles:

- A 3 IOPS general-purpose tier profile provides IOPS/GB performance suitable for a virtual server instance Balanced profile.
- A 5-IOPS tier profile provides IOPS/GB performance suitable for a virtual server instance Compute profile.
- A 10-IOPS tier profile provides IOPS/GB performance suitable for a virtual server instance Memory profile.

For network storage, IOPS per GB is limited and performance varies based on the workload. For Relational Database Management Systems (RDBMS), it is beneficial to store both the database log and data on the same volume, depending on the applications behavior. In general, for typical RDBMS-based applications, a 5 IOPS/GB profile is reasonable. If your application relies on specific KPIs for storage performance, test the storage throughput before deploying software.

More information on Block Storage for Virtual Servers Instances on VPC can be found under [About Block Storage for VPC](#).

NFS-based file storage for VSI on VPC infrastructure

IBM Cloud® File Storage for VPC is a zonal file storage offering that provides NFS-based file storage services. You can create file shares in an availability zone within a region. You can share them with multiple virtual server instances within the same zone or other zones in your region, across multiple VPCs. You can also limit access to a file share to a specific virtual server instance within a VPC and encrypt the data in transit.

File Storage for VPC provides file shares within the VPC Infrastructure. You create a file share in a zone and create the mount targets for the share per VPC. Replication between the source file share and a replica file share can be enabled. So if an outage at the primary site was to occur, you can fail over to the replica file share. Data on a file share is encrypted at rest with IBM-managed encryption by default. For added security, you can use your own root keys to protect your file shares with customer-managed keys.

For more information on NFS-based file storage for Virtual Server Instances on VPC Infrastructure, see [About File Storage for VPC](#).

Catalog images on VPC

When provisioning IBM Cloud virtual servers for VPC on x86 architecture, choose from the supported stock images, a virtual server operating system bundle, or a custom image from IBM Cloud Object Storage. The selected image determines the operating system that is provisioned for your instance. If the image selected is a virtual server operating system bundle stock image, then the software that is part of that bundle is also included in your instance.

In the [IBM Cloud console](#), go to the navigation **Menu** icon > **Infrastructure** > **Compute** > **Images**.

There are 3 different types of images for VPC:

1. [Custom images](#) (includes [Image from volume](#))
2. [Stock images](#)
3. Catalog images

To share or publish a custom image within your enterprise, you must create a private catalog, which allows you to manage access to products for multiple accounts within the same enterprise. You can share any existing x86 virtual server custom image with a private catalog, except for an encrypted image. For more information about these limitations, see [VPC considerations when using custom images in a private catalog](#).



Note: When you select a catalog image, ensure that you are informed about any associated billing plans.

Catalog images are billed in one of the following ways:

- Free trial
- Usage-based
- Bring Your Own License (BYOL)

Bring your own OS product license

When you have your own operating system license, you can install on your virtual server based on the instructions. For more information about custom images, see [Importing and managing custom images](#). The OS chosen must be certified for SAP and have access to the necessary OS packages for SAP. For more information, see [Bring your own license](#).

Provisioning the Intel Virtual Server Instance (VSI)

Once you understand the server profile, storage, and image options, then the Intel Virtual Server Instance (VSI) can be provisioned.

1. Click **Menu** icon > **Infrastructure > virtual server instances**.
2. From the virtual server instance main screen, click **Create** after ensuring the right **Region** is selected.
3. Choose the desired **Location**. This is done by choosing the Geography, Region and Zone.
4. Enter a unique name for the virtual server, that becomes the hostname. SAP hostnames must consist of a maximum of 13 alpha-numeric characters. For more information about SAP hostnames, see [SAP Notes 611361](#) and [129997](#).
5. Choose a **Resource group**.
6. **Optional:** Enter tags to help you organize and find your resources. You can add more tags later. For more information, see [Working with tags](#).
7. Select your preferred operating system from either Windows Server, Red Hat Linux or SUSE Linux to run SAP NetWeaver, or from Red Hat or SUSE to run SAP HANA. Ensure **SAP certified** is selected.

Select an image

The image that you select determines the operating system and software that is provisioned for your instance. You have the flexibility to select from a range of images, including stock images provided by IBM, one of your own custom images, or trusted third-party marketplace images and private enterprise images listed in the catalog. You can also boot an image from a snapshot or an existing volume. For more information about image, snapshot, and existing volume options, see [Creating virtual server instances](#).

Architecture ①

Intel x86 architecture	<input checked="" type="radio"/>
---------------------------	----------------------------------

IBM Z, LinuxONE s390x architecture	<input type="radio"/>
---------------------------------------	-----------------------

Stock images

Custom images

Catalog images

Snapshot

Existing volume

1 applied X

Search items

X

Operating system

- Linux based
- Windows based
- Generic

Certifications

- SAP certified

Name	Operating system	Version	Size	Date imported (Local)
ibm-redhat-9-4-amd64-sap-hana-4	Red Hat Enterprise Linux for SAP HANA	9.x for SAP HANA	2 GB	February 10 2025 at 3:27:55 PM
ibm-redhat-9-4-amd64-sap-applications-4	Red Hat Enterprise Linux for SAP Applications	9.x for SAP Applications	2 GB	February 10 2025 at 3:27:19 PM
ibm-redhat-9-2-amd64-sap-hana-5	Red Hat Enterprise Linux for SAP	9.x for SAP HANA	2 GB	February 10 2025 at 3:26:10 PM
ibm-redhat-9-2-amd64-sap-applications-5	Red Hat Enterprise Linux for SAP	9.x for SAP Applications	2 GB	February 10 2025 at 3:25:32 PM

Catalog Images

8. Select **Profile**. For more information, see based on the guidance that is detailed in [Intel Virtual Server certified profiles for SAP HANA](#) or [Intel Virtual Server certified profiles for SAP NetWeaver](#), which lists the profiles that are certified for SAP HANA and SAP NetWeaver.
9. Select the SSH key that you want to add to the virtual server. For this step, you can create a new SSH key.
10. In the **Data Volumes** section, click **Create**. This will allow adding data disks to the provisioned VSI. Afterwards, these disks can be used

for partitioning and storage management (File system distribution).

- For SAP HANA, these volumes must meet special KPI needs that are defined by SAP and are mandatory. For more information, see [Storage specifications - Intel Virtual Server certified profiles for SAP HANA](#) or [Storage design considerations](#) to learn these special needs and how you should configure the data volumes.
 - For SAP NetWeaver, these volumes are based on the requirements of the installed SAP NetWeaver instance. The standard tiered options are 3K, 5K, and 10K IOPS, and custom IOPS. These options can be used to accommodate the specific requirements.
11. During **Data Volume** creation, the option Auto-delete can be enabled, if required. This will mark the data volume to be automatically deleted when the VSI itself will be deleted. Consider this option carefully.
- Data volume sizes must be specified in GB and Profile and IOPS values need to be specified. More information on IOPS can be found under Block Storage for VPC profiles. Choose your preferred encryption method and click **Create**.
12. Under **Networking**, select the Virtual Private Cloud (VPC) to attach the virtual server.
13. By default, the virtual network interface option will be selected. This is the suggested option.
14. Under Network attachments, click **Edit** to change the Security Group, thus the Inbound/Outbound rules. This can also be done later, after the VSI is provisioned.
15. Review the costs for your VSI resource and click **Create virtual server**.

Related information

- [Release notes for IBM Cloud VPC](#)
- [SAP Note 84555 - Windows Server, Linux®, and UNIX: Certified hardware](#)
- [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#)
- [SAP Note 2923773 - Linux® on IBM Cloud \(IaaS\): Adaption of your SAP License](#)
- [SAP Note 171380 - Released IBM hardware \(Intel processors\) and IBM Cloud services offers](#)
- [SAP Note 1380654 - SAP support in IaaS environments](#)
- [SAP Note 2369910 - SAP Software on Linux®: General information](#)
- [SAP Note 3108316 - Red Hat Enterprise Linux 9.x: Installation and Configuration](#)
- [SAP Note 1597355 - Swap-space recommendation for Linux](#)
- [SAP Product Availability Matrix](#)

SAP NetWeaver with Db2

Automating SAP workload HA deployment on IBM Cloud VPC with Terraform and Ansible

You can use Terraform to automate IBM Cloud® VPC provisioning. The VPC provisioned includes virtual server instances with high network performance. The VPC infrastructure contains various Infrastructure-as-a-Service (IaaS) offerings, including virtual servers. After the VPC is provisioned, the scripts use the Ansible Playbooks to install the SAP system.

IBM Cloud VPC introduction

VPC is a public cloud offering that an enterprise uses to establish its own private cloud-like computing environment on shared [public cloud](#) infrastructure. VPC gives an enterprise the ability to define and control a virtual network that is logically isolated from all other public cloud tenants, creating a private and secure place on the public cloud.

Imagine that a cloud provider's infrastructure is a residential apartment building and multiple families live inside. A public cloud tenant is a kind of sharing an apartment with a few roommates. In contrast, having a VPC is like having your own private condominium; no one else has the key, and no one can enter the space without your permission.

VPC's logical isolation is implemented by using virtual network functions and security features that give the enterprise customer granular control over which IP addresses or applications can access particular resources. It is analogous to the "friends-only" or "public/private" controls on social media accounts used to restrict who can or can't see your otherwise public posts.

With IBM Cloud VPC, you can use the UI, CLI, and API to manually provision virtual server instances for VPC with high network performance. VPC infrastructure contains various Infrastructure-as-a-Service (IaaS) offerings including virtual servers for VPC.

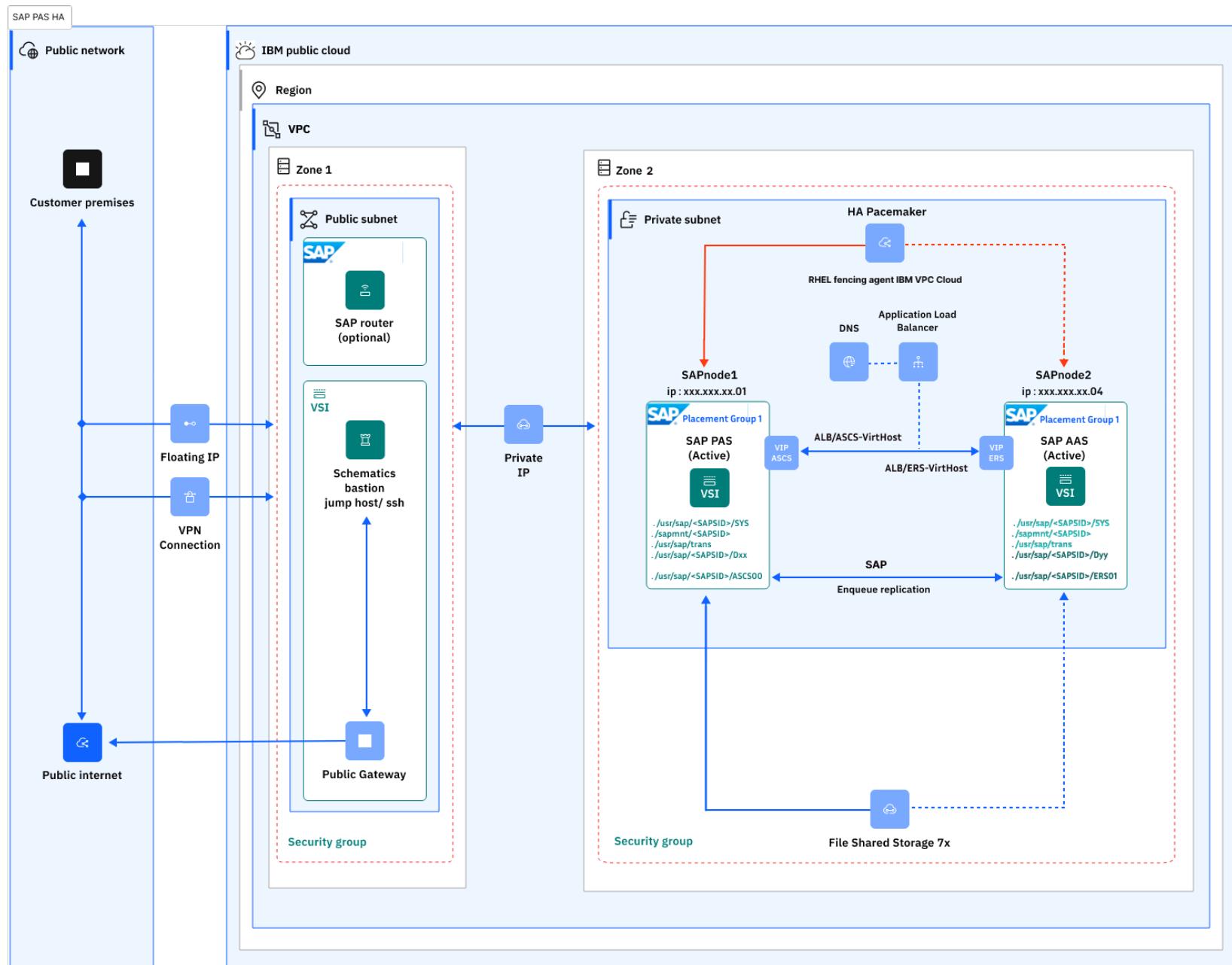
Use the following information to understand a simple use-case for planning, creating, and configuring resources for your VPC, and learn more about VPC overviews and VPC tutorials. For more information about the VPC, see [Getting started with Virtual Private Cloud \(VPC\)](#).

SAP products architecture on IBM Cloud VPC

A [Virtual Private Cloud \(VPC\)](#) contains one of the most secure and reliable cloud environments for SAP applications within your own VPC with virtual server instances. This represents an Infrastructure-as-a-Service (IaaS){: external} within IBM Cloud that offers all the benefits of isolated, secure, and flexible virtual cloud infrastructure from IBM. In comparison, the IBM Cloud classic infrastructure virtual servers offering uses virtual instances with native and VLAN networking to communicate with each other within a data center; however, the instances are restricted in one well-working pod by using subnet and VLAN networking as a gap scale up of virtual resources should rely between the pods. The IBM Cloud VPC network orchestrator layer concept eliminates the pod boundaries and restrictions, so this new concept handles all the networking for every virtual instance running within VPC across regions and zones.

Highly available system for SAP NetWeaver on IBM Cloud VPC

In a Highly Available (HA) system, every instance can run on a separate IBM Cloud virtual server instance. The cluster HA configuration for the SAP application server consists of two virtual server instances, each of them located in the same zone within the region by using placement groups. Placement groups assure that both cluster resources and cloud resources are also located in different compute nodes as specified in the following placement groups section:



SAP HA for SAP applications cluster nodes PAS (Active) and AAS (Active)

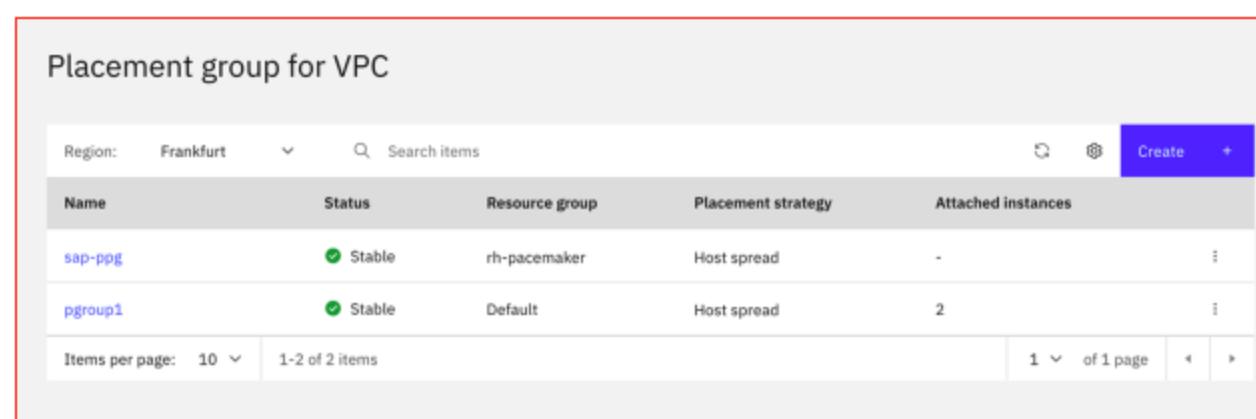
Placement groups on IBM Cloud VPC for SAP HA architecture

Placement Groups (PG) for VPC have two different anti-affinity strategies for high availability. By using the placement strategies, you minimize the chance of service disruption with virtual server instances that are placed on different hosts or into an infrastructure with separate power and network supplies.

The design of placement groups for IBM Cloud virtual servers solves this issue. Placement groups give a measure of control over the host on which a new public virtual server is placed. In this release, a “spread” rule is implemented, which means that the virtual servers within a placement group are spread onto different hosts. You can build a highly available application within a data center and know that your virtual servers are isolated from each other.

Placement groups with the spread rule are available to create in selected IBM Cloud data centers. After a spread rule is created, you can provision a virtual server into that group and ensure that it is not on the same host as any of your other virtual servers. This feature comes with no cost.

You can create your placement group and assign up to four new virtual server instances. With the spread rule, each of your virtual servers are provisioned on different physical hosts. In the following configuration example, the “Power Spread” option is used:



Placement groups host spread

Placement group for VPC					
Name	Status	Resource group	Placement strategy	Attached instances	
sapha-poc	Stable	wes-ic4sap-resourcegroup	Power spread	4	
Items per page: 10 1 item 1 of 1 page					

Placement groups power spread

Following are the SAP instances that are required for HA scenario:

- ABAP SAP Central Services (ASCS) instance - contains the ABAP message server and the ABAP enqueue server.
- Enqueue Replication Server (ERS) instance for the ASCS instance.
- Database instance
- Primary Application Server (PAS) instance on node 1.
- Additional Application Server (AAS) instance on node 2.



Note: It is recommended to run both the ASCS instance and the ERS instance in a switchover cluster infrastructure.

IBM Cloud File Storage for VPC for SAP HA architecture

[IBM Cloud File Storage for VPC](#) technology is used to make the SAP directories available to the SAP system. The technologies of choice are NFS, shared disks, and cluster file system. If you have decided to use the HA solution for your SAP system, make sure that you properly address the HA requirements of the SAP file systems in your SAP environment.

File shares for VPC								
Name	Status	Resource groups	Location	Mount targets	Size	Replication role	Encryption type	
usrsap-as1-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-as2-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-sapscs-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-sapers-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-sapmnt-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-sapsys-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-trans-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	80 GB	None	Provider managed	

File shares for VPC

- File shares that are mounted as NFS permanent file systems on both cluster nodes for SAP HA application:
 - `/usr/sap/<SAPSID>/SYS`
 - `/sapmnt<SAPSID>`
 - `/usr/sap/trans`
- Cluster-managed file systems for SAP HA application: ASCS
 - `/usr/sap/<SAPSID>/ASCS00`
 - `/usr/sap/<SAPSID>/ERS01`
- Permanent NFS mount on SAP HA application node 1 PAS instance:
 - `/usr/sap/<SAPSID>/Dxx`
- Permanent NFS mount on SAP HA application node 2 dialog instance:
 - `/usr/sap/<SAPSID>/Dyy`

Prerequisites

You need to install the hardware (hosts, disks, and network) and decide how to distribute the database, SAP instances, and if required, the Network File System (NFS) server over the cluster nodes.

Context

Following are the types of SAP directories:

- Physically shared directories: `/<sapmnt>/<SAPSID>` and `/usr/sap/trans`

- Logically shared directories that are bound to a node, such as `/usr/sap`, with the following local directories:
 - `/usr/sap/<SAPSID>`
 - `/usr/sap/<SAPSID>/SYS`
 - `/usr/sap/hostctrl`
- Local directories that contain the SAP instances such as `/usr/sap/<SAPSID>/ASCS<Instance_Number>`
- The global transport directory may reside on a separate SAP transport host as a standard three systems transport layer configuration.

You need at least two nodes and a shared file system for distributed ASCS and ERS instances. The assumption is that the rest of the components are distributed on other nodes.

ASCS and ERS installation

In order for the ASCS and ERS instances to be able to move from one node to the other, they need to be installed on a shared file system and use virtual hostnames based on the virtual IP.

In this VPC-based SAP HA solution, the shared file system that is required by the cluster is replaced by the NFS-mounted file storage, and the virtual IP is replaced by the Application Load Balancer for VPC (ALB).

In this scenario, three ALBs are used, one for each Single Point of Failure (SPOF) component in order to replace the virtual IP requirement: ALB for ASCS, ALB for ERS, and ALB for ASE Sybase. Each ALB is configured as a backend for the corresponding cluster servers and redirects all of the communication that is received on the front-end ports to the active server in the backend pool.

Load balancers for VPC						
Region:	Frankfurt	▼	<input type="text"/> poc	X		
Name	Status	Family	Resource group	Type	Hostname	Location
db-alb-hana-poc	Active	Application	wes-ic4sap-resourcegroup	Private	20bdd130-eu-de.lb.appdomain.cloud	Frankfurt
sap-alb-ers-poc	Active	Application	wes-ic4sap-resourcegroup	Private	3941d983-eu-de.lb.appdomain.cloud	Frankfurt
sap-alb-ascs-poc	Active	Application	wes-ic4sap-resourcegroup	Private	56a9190d-eu-de.lb.appdomain.cloud	Frankfurt

Application load balancer management of HA IPs mechanism

Private application load balancer

A [private application load balancer](#) is accessible through your private subnets that you configured to create the load balancer.

Similar to a public application load balancer, your private application load balancer service instance is assigned an FQDN; however, this domain name is registered with one or more private IP addresses.

IBM Cloud operations change the number and value of your assigned private IP addresses over time, based on maintenance and scaling activities. The backend virtual server instances that host your application must run in the same region and under the same VPC.

Use the assigned ALB FQDN to send traffic to the private application load balancer to avoid connectivity problems to your applications during system maintenance or scaling down activities.

Each ALB sends traffic to the cluster node where the application (ASCS, ERS, ASE Sybase DB) is running. During the cluster failover, the ALB redirects all the traffic to the new node where the resources are up and running.



Note: DNS-as-a-Service (DNSaaS) is the management IBM Cloud VPC DNS service of HA and FQDN (IPs) mechanism.



Note: The ALB has a default of 50 seconds for client and server timeout, so after 50 seconds of inactivity, the connection is closed. To support SAP connections through ALB and not lose connection after 50 seconds, you need to request a change this value to a minimum of 300 seconds (client-side idle connection = minimum 300s and server-side idle connection = minimum 300s). To request this change, open a support ticket. This is an account-wide change that affects all of the ALBs in your account. For more information, see [Connection timeouts](#).

DNS Services with VPC

[IBM Cloud DNS Services](#) provide private DNS to VPC users. Private DNS zones are resolvable only on IBM Cloud and from explicitly [permitted networks](#) in an account. To get started, create a DNS Services instance by using the IBM Cloud console.

DNS Services allows you to:

- Create the private DNS zones that are collections for holding the domain names.
- Create the DNS resource records under these DNS zones.
- Specify the access controls used for the DNS resolution of resource records on a zone-wide level.

DNS Services also maintains its own worldwide set of DNS resolvers. Instances that are provisioned under IBM Cloud on an IBM Cloud network can use resource records that are configured through IBM Cloud DNS Services by querying DNS Services resolvers.

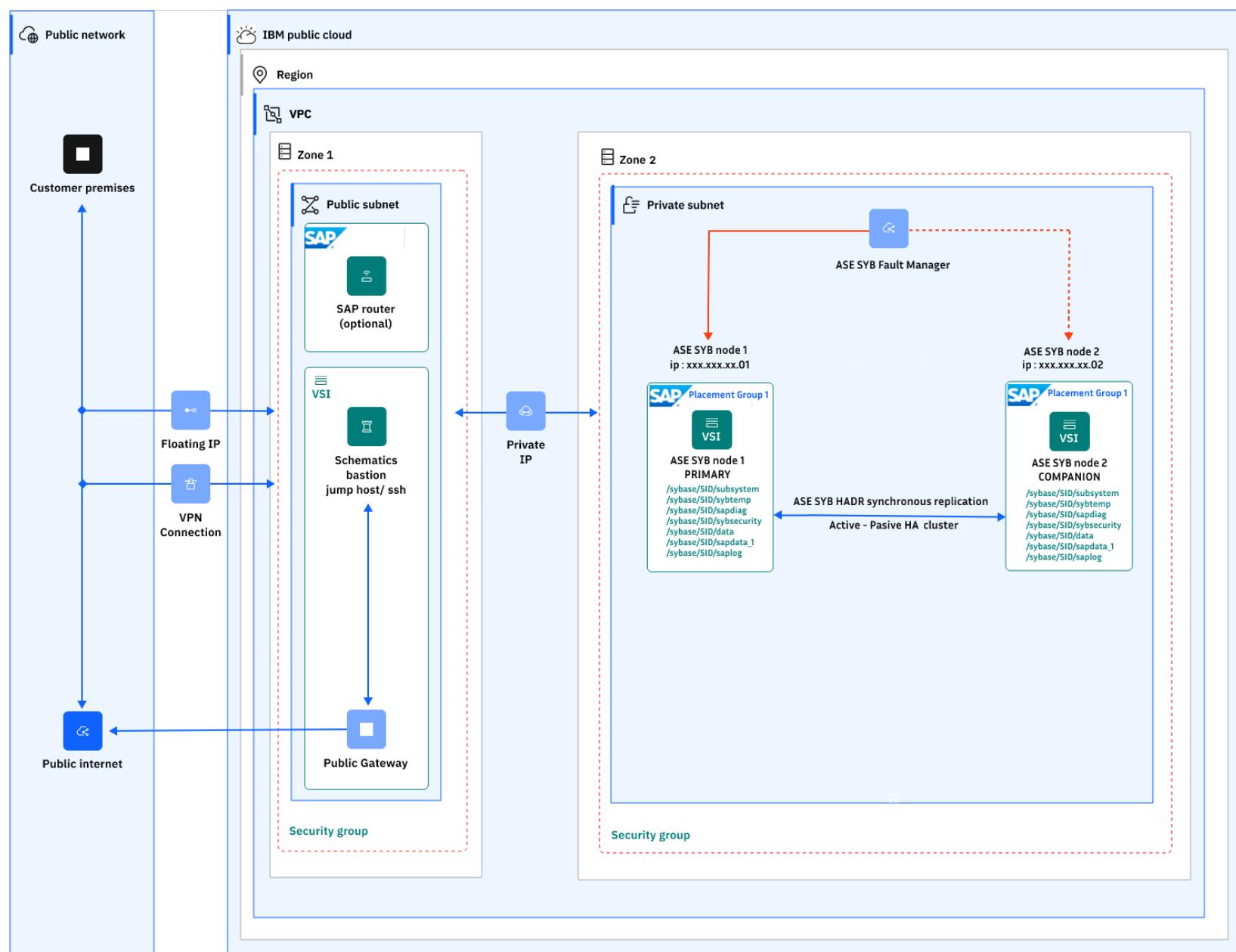
Resource records and zones that are configured through DNS Services are:

- Separated from the wider public DNS, and their publicly accessible records.
- Hidden from the system outside of and not part of the IBM Cloud private network.
- Accessible only from the system that you authorize on the IBM Cloud private network.
- Resolvable only via the resolvers provided by the service.

The DNS service maps the FQDN of each ALB to the virtual hostnames of the ASCS, ERS, and ASE Sybase that are used by SAP applications.

Type	Name	Value	TTL
CNAME	dbpochana	is an alias of 20bdd130-eu-de.lb.appdomain.cloud	12 hr
CNAME	sappocers	is an alias of 3941d983-eu-de.lb.appdomain.cloud	12 hr
CNAME	sappocases	is an alias of 56a9190d-eu-de.lb.appdomain.cloud	12 hr

Highly available system for SAP ASE Sybase database with HADR system



SAP HA for ASE Sybase DB instances cluster nodes primary (Active) and Secondary (Companion)

At the most basic level, a standard HA ASE Sybase cluster in an active(primary)-passive(companion) configuration has two nodes: one is the primary node and the other is the standby node. This means that the primary node is actively serving the active SAP DB instances (Primary and Companion), while the standby node is waiting to jump in if there is any failure.

The cluster is set with a virtual hostname IP (hostname is mapped to the FQDN of the ASE Sybase ALB through DNS, which is the same as

explained previously for SAP ASCS and ERS instances). Application instances (PAS and AAS) are used on the SAP profiles to call that particular component. The cluster assigns the virtual IP to the active node and uses a heartbeat monitor to confirm the availability of the components. If the primary node stops responding, it triggers the automatic failover mechanism that calls the standby node to step up to become the primary node. The ALB detects the change, redirects the traffic to the new active node, and assigns the virtual IP to it, restoring the component availability. Once fixed, the failed node comes online as a standby node.

SAP Sybase HADR system supports synchronous replication

The SAP Sybase HADR system supports synchronous replication between the primary and standby servers for high availability. An active-active setup is a two-node configuration where both nodes in the cluster include SAP ASE managing independent workloads, capable of taking over each others workload in the event of a failure.

The SAP ASE server that takes over the workload is called a secondary companion, and the SAP ASE server that fails is called the primary companion. Together they are companion servers. This movement from one node to another is called failover. After the primary companion is ready to resume its workload, it is moved back to its original node. This movement is called a failback.

When a system fails over, clients that are connected to the primary companion and use the failover property automatically reestablish their network connections to the secondary companion. You must tune your operating system to successfully manage both servers during fail over. See your operating system documentation for information about configuring your system for high availability. An SAP ASE configured for failover in an active-active setup can be shut down using the shutdown command only after you have suspended SAP ASE from the companion configuration, at both the server level and the platform level.

The always-on option in a High Availability and Disaster Recovery (HADR) system consists of two SAP ASE servers:

- Primary on which all transaction processing takes place.
- Warm standby (referred to as a "standby server" in DR mode, and as a "companion" in HA mode) for the primary server, and contains copies of designated databases from the primary server.



Note: The HADR feature that is shipped with SAP ASE version 16.0 SP02 supports only a single-companion server.

Some high-availability solutions (for example, the SAP Adaptive Server Enterprise Cluster Edition) share or use common resources between nodes. However, the HADR system is a "shared nothing" configuration, each node has separate resources including disks.

In an HADR system, servers are separate entities and data is replicated from the primary server to the companion server. If the primary server fails, a companion server is promoted to the role of primary server either manually or automatically. Once the promotion is complete, clients can reconnect to the new primary server, and see all committed data, including data that was committed on the previous primary server.

Servers can be separated geographically, which makes an HADR system capable of withstanding the loss of an entire computing facility.



Note: The HADR system includes an embedded SAP Replication Server, which synchronizes the databases between the primary and companion servers. SAP ASE uses the Replication Management Agent (RMA) to communicate with Replication Server and SAP Replication Server uses Open Client connectivity to communicate with the companion SAP ASE.

The Replication Agent detects any data changes made on the primary server and sends them to the primary SAP Replication Server. In the figure above, the unidirectional arrows indicate that, although both SAP Replication Servers are configured, only one direction is enabled at a time.

The HADR system supports synchronous replication between the primary and standby servers for high availability so the two servers can keep in sync with Zero Data Loss (ZDL). This requires a network link that is fast enough between the primary and standby server so that synchronous replication can keep up with the primary servers workload. Generally, this means that the network latency is approximately the same speed as the local disk IO speed, a few (fewer than 10) milliseconds. Anything longer than a few milliseconds may result in a slower response to write operations at the primary.

The HADR system supports asynchronous replication between the primary and standby servers for disaster recovery. The primary and standby servers by using asynchronous replication can be geographically distant, meaning they can have a slower network link. With asynchronous replication, Replication Agent Thread captures the primary servers workload, which is delivered asynchronously to SAP Replication Server. The SAP Replication Server applies these workload change to the companion server.

The most fundamental service that is offered by the HADR system is the failover; planned or unplanned from the primary to the companion server, which allows maintenance activity to occur on the old primary server, while applications continue on the new primary.

The HADR system provides protection in the event of a disaster. If the primary server is lost, the companion server can be used as a replacement. Client applications can switch to the companion server, and the companion server is quickly available for users. If the SAP Replication Server was in synchronous mode before the failure of the primary server, the Fault Manager automatically initiates failover with

zero data loss.

Fault Manager installation on the SAP ASCS node

The required parameters are asked during the installation process to create a profile for the fault manager and then adds it to the instance start profile. It is also possible to run the installation by using an existing profile: `sybdbfm install pf=<SYBHA.PFL>` In this case, the installation process will only ask for profile parameters missing in the profile.



Note: Fault manger is integrated with ASCS on same SAP PAS/AAS cluster (start/stop/move together).

There may be some data loss if the SAP Replication Server was in asynchronous mode and you must use manual intervention to failover for disaster recovery.

Connection attempts to the companion server without the necessary privileges are silently redirected to the primary companion via the login redirection mechanism, which is supported by Connectivity libraries. If login redirection is not enabled, client connections fail and are disconnected.

The SAP ASE HADR option installs the below components:

- SAP ASE
- SAP Replication Server
- Replication Management Agent (RMA)
- SAP Host Agent
- Fault Manager
- SAP ASE Cockpit



Note: This automation is offered at no cost; however, the provisioned infrastructure comes at cost.

VPC with Additional Application Server (AAS) ABAP on Linux for SAP HANA

You can use Terraform scripts to create a single-tier VPC and create the AAS to HANA and AnyDB infrastructure on the VPC. The Terraform scripts use the VPC information that you provide and then call the Ansible playbook to create the SAP architecture on the specified VPC. Terraform on IBM Cloud® enables predictable and consistent provisioning of IBM Cloud Virtual Private Cloud (VPC) infrastructure resources so that you can rapidly build complex, cloud environments. IBM Cloud VPC infrastructure consists of SAP certified hardware that uses Intel® Xeon CPUs and more Intel® technologies.

You have two deployment methods to choose from:

- Terraform scripts that run from the CLI on your bastion server.
- Schematics user interface accessed from your cloud dashboard menu.

You can create SAP AAS NetWeaver 7.x on the SAP HANA-based ABAP stack.

SAP solution implemented

Many SAP enterprise solutions are built on the SAP platform (SAP NetWeaver) including:

- SAP HANA as Primary Persistence for SAP NetWeaver-based applications
- SAP Business Suite applications (ERP, CRM, and SCM, and other applications),
- SAP Business Warehouse (BW), and
- Other SAP enterprise solutions

SAP NetWeaver has two distinct aspects, ABAP and Java. Many applications that are built on the SAP NetWeaver's ABAP or Java (or both) application servers run on SAP DB owned HANA and ASE Sybase either in AnyDB platforms (MSSQL, Oracle, and Db2).

Technical interfaces are available for applications that are built on the SAP NetWeaver AS ABAP and AS Java to run on SAP HANA and AnyDB. However, specific development enablement is normally required for each application to ensure that it runs optimally on the SAP HANA. SAP Business Suite applications (ERP, CRM, SCM, and other applications), SAP Business Warehouse (BW), and other SAP NetWeaver-based applications were modified to run on SAP HANA and have many advantages. Also, various components and complimentary applications that are built on SAP NetWeaver can also run on SAP HANA or AnyDB by using the provided SAP NetWeaver DB interfaces.

The SAP HANA as primary persistence for SAP NetWeaver-based applications scenario has one restriction: SAP NetWeaver ABAP and Java

application servers must run on separate hardware servers from the SAP HANA hardware.

What is created

The scripts automate the virtual infrastructure resources, provisioning the processes for the SAP architecture in an existing VPC with a distributed environment. SAP AAS NetWeaver 7.x (HANA or ASE SYB) application server on a distinct VSI VPC system and SAP HANA DB on a dedicated server type VSI VPC box are provisioned. The scripts work in two phases.

During the first phase of [Automate SAP bastion server – SAP media storage repository](#), the following virtual infrastructure resources based on the components from the existing VPC created by the bastion server are:

- 1 VPC where the virtual server instance is provisioned.
- 1 security group. The rules for this security group are:
 - Allow inbound DNS traffic (port 53).
 - Allow inbound SSH traffic (TCP port 22).
 - Allow all outbound traffic from the virtual server instance.
 - Allow all traffic in the security group.
- 1 subnet to enable the networking in your VPC.
- 2 virtual server instances with SAP certified storage and network configurations.
- 1 floating IP address used to access your VPC virtual server instance over the public network.

During the second phase, the Ansible Playbooks is called and the SAP architecture is installed for both dedicated virtual server instance (VSI) SAP application; VSI system and dedicated SAP HANA VSI box. The SAP architecture that is deployed on the SAP NetWeaver 7.x release is a stand-alone dedicated SAP HANA 2.0 box release. For more information about this architecture, see [Automating SAP HANA stand-alone virtual server instance on IBM Cloud® VPC by using Terraform and Ansible](#).

You can provision only one instance of the service per IBM Cloud region.

Schematics deployment

When you run the scripts with the Schematics interface, you:

- Enter the workspace information.
- Enter the GitHub path for the chosen solution either on NetWeaver AAS for HANA.
- Modify the parameters in the Schematics interface. They are the same parameters as the `input.auto.tfvars` file that you use with the cli.

Virtual server instance configuration

Following are the supported operating system images for SAP NetWeaver primary application server:

- ibm-redhat-8-4-amd64-sap-applications-2
- ibm-redhat-8-6-amd64-sap-applications-2
- ibm-sles-15-3-amd64-sap-applications-2
- ibm-sles-15-4-amd64-sap-applications-3

Following are the supported operating system images for SAP HANA database:

- ibm-redhat-8-4-amd64-sap-hana-2
- ibm-redhat-8-6-amd64-sap-hana-2
- ibm-sles-15-3-amd64-sap-hana-2
- ibm-sles-15-4-amd64-sap-hana-1

For both server instances there are:

- Two SSH keys are configured to access SSH as `root`.
- Three storage volumes as described in the `input.auto.tfvars` file.

What is created for anydb

The scripts use the information that you provide for an existing VPC and deploy AAS to SAP HANA or AnyDB on a different host than CI (SAP Central Instance) VSI host. For more information about this architecture, see [SAP NetWeaver 7.x on UNIX with HANA or AnyDB on IBM Cloud](#)

[VPC on IBM Cloud VPC](#). You specify the information for the VPC to use in the `input.auto.tfvars` file.

The scripts call the Ansible Playbooks to install the SAP architecture.

Script files

The configuration and script files are provided on GitHub. Each supported interface for the SAP solution installation has its own folder in the GitHub repository:

- [GitHub repository for Terraform – AAS HANA](#)

Terraform interface

To run the Terraform script, you modify:

- The `input.auto.tfvars` file to specify the existing VPC resources for your solution. Specify the variables for the existing VPC:
 - VPC name
 - Security group
 - Subnet
 - Hostname
 - Profile
 - Image
 - Up to two SSH keys

You can change the default SAP system configuration settings to match your solution. You can also specify the location where you downloaded the SAP kits.

The IBM Cloud Provider plug-in for Terraform on IBM Cloud uses these configuration files to install AAS to SAP HANA and AnyDB on the specified VPC in your IBM Cloud account.

Support

There are no warranties of any kind, and there is no service or technical support available for these materials from IBM®. As a recommended practice, review carefully any materials that you download from this site before using them on a live system.

Though the materials provided herein are not supported by the IBM® Service organization, your comments are welcomed by the developers, who reserve the right to revise, readapt or remove the materials at any time. To report a problem, or provide suggestions or comments, open a GitHub issue.

Before you begin

Before you use the scripts in the bastion cli:

- Set up your account to access the VPC. Make sure that your account is [upgraded to a paid account](#).
- If you have not already, create a Bastion server to store the SAP kits. For more information, see [Automate SAP bastion server - SAP media storage repository](#).
- Download the SAP kits from the SAP Portal to your Deployment Server. Make note of the download locations. Ansible decompresses the files. For more information, see the [readme](#) file.
- [Create or retrieve an IBM Cloud API key](#). The API key is used to authenticate with the IBM Cloud platform and to determine your permissions for IBM Cloud services.
- [Create or retrieve your SSH key ID](#). You need the 40-digit UUID for the SSH key, not the SSH key name.
- Terraform should already be installed on the bastion server that you deployed. For more information, see [Bastion server for SAP deployment](#).
- (Optional - Catalog Tile) create secrets for your credentials and passwords by using the [Secrets Manager](#).

Deploying SAP AAS NetWeaver 7.x on HANA by using the Schematics user interface

Use these steps to configure the SAP Additional Application Server (AAS) NetWeaver with HANA or AnyDB on your existing VPC by using the Schematics interface. The script takes 2 - 3 hours to complete.

1. From the IBM Cloud menu, select **Schematics**.
2. Click **Create** workspace.

3. On the **Specify template** page:
 - Enter the URL for the Schematics interface.
 - Select the **Terraform version** that is listed in the readme file.
 - Click **Next**.
4. On the **workspace details** page:
 - Enter a name for the workspace.
 - Select a **Resource group**.
 - Select a **Location** for your workspace. The workspace location does not have to match the resource location.
 - Select **Next**.
5. Select **Create** to create your workspace.
6. On the workspace settings page, in the input variables section, review the default input variables and provide values that match your solution.
 For a more detailed description of each parameter, check the GitHub repo [AAS HANA readme](#) file, chapter "Input parameter file". Also, make sure to mark the parameters that contain sensitive information like passwords, API, and ssh private keys as "sensitive". These parameters are marked as "sensitive" in the readme file, under "Input parameter file".
7. On the workspace settings page, click **Generate plan**. Wait for the plan to complete.
8. Click **View log** to review the log files of your terraform execution plan.
9. Apply your Terraform template by clicking **Apply plan**.
10. Review the log file to ensure that no errors occur during the provisioning, modification, or deletion process.

Deploying SAP AAS NetWeaver (ABAP) on HANA with the Deployable Architecture tile interface

Use these steps to configure the SAP AAS NetWeaver (ABAP) on HANA on your existing VPC by using the catalog tile interface. The script takes 2 - 3 hours to complete.

1. From the IBM Cloud catalog, select **VPC with Additional Application Server ABAP on Linux for SAP HANA** on HANA tile. The **Create** tab opens for VPC with Additional Application Server ABAP on Linux for SAP HANA. For more information about this deployment, see the About tab or the readme file link.
2. Select the latest version.
3. Select **VPC with Additional Application Server ABAP on Linux for SAP HANA on Deployable Architecture tile** variation.
4. Click **Review deployment** options:
 - **Add to project** to add this deployment to an IBM Cloud project and combine it with other deployments. IBM Cloud projects include several more pipeline steps before deployment, including deployment validation, cost calculation, compliance verification, and approval process.
 - **Create from the CLI** to get the CLI command. With this command you can trigger the deployment from the CLI.
 - **Work with code** to embed the code into other terraform deployments.
 - **Deploy with IBM Cloud Schematics** to trigger the deployment process directly.
5. Select **Deploy with IBM Cloud Schematics**.
6. Add the input parameters for this installation. There are 3 categories of parameters:
 - **Workspace** - These parameters define the workspace that is automatically created in Schematics:
 - Enter a name for the workspace or use the default name.
 - The Resource Group used to create resources. Use default or create a Resource Group.
 - Select a location to create your Schematics workspace. The workspace location need not match the resource location.
 - **Required input variables** - Review the default input variables and provide values that match your solution. These parameters are specific to your deployment. For more detailed information, see the [Readme file](#).

Parameter	Description
BASTION_FLOATING_IP	Required only for Schematics Deployments. The Floating IP from the Bastion Server.

HOSTNAME	The hostname for the VSI. The hostname should be up to 13 characters as required by SAP. For more information on the rules regarding hostnames for SAP systems, check SAP Note 611361: Hostnames of SAP ABAP Platform servers
REGION	The cloud region to deploy the solution. The regions and zones for VPC are listed here . Review supported locations in IBM Cloud Schematics here . Sample value: eu-de.
RESOURCE_GROUP	The name of an existing Resource Group for VSIs and Volumes resources. Default value: "Default". The list of Resource Groups is available here .
SECURITY_GROUP	The name of an existing Security group. The list of security groups is available here .
SSH_KEYS	The list of SSH Keys UUIDs that are allowed to SSH as root to the VSI can contain one or more IDs. The list of SSH Keys is available here . Sample input (use your own SSH UUIDs from IBM Cloud){: external}: ["r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a", "r010-3fcfd9fe7-d4a7-41ce-8bb3-d96e936b2c7e"]
SUBNET	The name of an existing subnet. The list of subnets is available here .
VPC	The name of an existing VPC. The list of VPCs is available here .
ZONE	The cloud zone where to deploy the solution. Sample value: eu-de-2.
ibmcloud_api_key	IBM Cloud API key (Sensitive* value).
private_ssh_key	Required only for Schematics Deployments - Input your id_rsa private key pair content in OpenSSH format (Sensitive* value). This private key should be used only during the terraform provisioning and it is recommended to be changed after the SAP deployment.
hdb_instance_number	The instance number of the SAP HANA database server.
sap_aas_instance_number	Technical identifier for the internal processes of the additional application server.
sap_ascs_instance_number	Technical identifier for the internal processes of ASCS.
sap_ci_host	IP address of the existing SAP Central Instance.
sap_ci_hostname	The hostname of the existing SAP Central Instance.
sap_ci_instance_number	Technical identifier for the internal processes of the Central Instance.
sap_sid	The SAP system ID identifies the entire SAP system.
sap_main_password	Common password for all users that are created during the installation (See Obs*).

Required Variables

- **Optional variables** - Review and update the optional input variables. The Ansible scripts expect the SAP kits to be in the default locations listed. For more information, see the [Readme file - Input Parameters](#).

Parameter	Description
ID_RSA_FILE_PATH	The file path for private_ssh_key is automatically generated by default. If it is changed, it must contain the relative path from Git repo folders. Default value: "ansible/id_rsa".
IMAGE	The OS image used for the VSI. A list of images is available here .
PROFILE	The profile used for the VSI. A list of profiles is available here . For more information about supported DB/OS and IBM Gen 2 Virtual Server Instances (VSI), check SAP Note 2927211: SAP Applications on IBM Virtual Private Cloud .

VOL1	Volume 1 Size - The size for the disks in GB that are to be attached to the VSI and used by SAP.
VOL2	Volume 2 Size - The size for the disks in GB that are to be attached to the VSI and used by SAP.
kit_sapcar_file	Path to the sapcar binary, as downloaded from SAP Support Portal.
kit_swpm_file	Path to the SWPM archive (SAR), as downloaded from SAP Support Portal.
kit_saphostagent_file	Path to the SAP Host Agent archive (SAR), as downloaded from SAP Support Portal.
kit_hdbclient_file	Path to the HANA DB client archive (SAR), as downloaded from SAP Support Portal.

Optional Variables

7. Accept the license agreement.
8. Select **Deploy**. The deployment starts and you are directed to the Schematics page that displays the script log files for you to monitor the deployment progress.

Creating the infrastructure using Terraform with the bastion server CLI

Use these steps to configure the IBM Cloud Provider plug-in and use Terraform to install SAP AAS to SAP HANA and AnyDB on your existing VPC on an already deployed SAP NetWeaver 7.X with SAP HANA 2.0 or ASE SYB as a Central Instance.

The script takes 1 - 2 hours to complete.

1. Access the bastion server cli.
2. Clone the solution repository and change to the folder.

ASE SYB 16 Clone the solution repository from <https://github.com/IBM-Cloud/sap-aas-abap-ase-syb> and cd to the sap-aas-abap-ase-syb/cli folder.

```
$ git clone https://github.com/IBM-Cloud/sap-aas-abap-ase-syb
cd sap-aas-abap-ase-syb/cli/
```

SAP HANA 2.0: Clone the solution repository from <https://github.com/IBM-Cloud/sap-abap-hana-aas> and cd to the sap-abap-hana-aas folder.

```
$ git clone https://github.com/IBM-Cloud/sap-abap-hana-aas.git
cd sap-abap-hana-aas/
```

3. Modify the `input.auto.tfvars` file to specify the information for the existing VPC, your region, zone, networking component names, hostname for the AAS VSI,profile, and image. You need your 40-digit SSH key ID for this file. The second SSH key is optional. For more options for profile, see [Instance Profiles](#). For more options, see [Images](#). For descriptions of the variables, see the [readme](#) file.

The VSI OS images that are supported for this solution for Netweaver Additional Application Server are:

- ibm-redhat-8-4-amd64-sap-applications-2
- ibm-redhat-8-6-amd64-sap-applications-2
- ibm-sles-15-3-amd64-sap-applications-2
- ibm-sles-15-4-amd64-sap-applications-4

```
$ # Infra VPC variables for ASE SYB
REGION    = "eu-de"
ZONE      = "eu-de-2"
VPC       = "ic4sap"                      # EXISTING Security group name
SECURITY_GROUP = "ic4sap-securitygroup"    # EXISTING Security group name
RESOURCE_GROUP = "wes-automation"
SUBNET    = "ic4sap-subnet"                 # EXISTING Subnet name
SSH_KEYS   = [ "r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a" , "r010-3fcfd9fe7-d4a7-41ce-8bb3-
d96e936b2c7e" ]

# SAP AAS VSI variables:
```

```

HOSTNAME = "sapnwase-as01"
PROFILE = "bx2-4x16"
IMAGE = "ibm-redhat-8-4-amd64-sap-applications-2

$ # Infra VPC variables for ABAP HANA
REGION      = "eu-de"
ZONE        = "eu-de-2"
VPC          = "ic4sap" # EXISTING Security group name
SECURITY_GROUP = "ic4sap-securitygroup" # EXISTING Security group name
RESOURCE_GROUP = "wes-automation"
SUBNET       = "ic4sap-subnet" # EXISTING Subnet name
SSH_KEYS     = [ "r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a" , "r010-3fc9fe7-d4a7-41ce-8bb3-d96e936b2c7e" ]
ID_RSA_FILE_PATH = "ansible/id_rsa"

# SAP AAS variables:
HOSTNAME = "sapnwapp"
PROFILE = "bx2-4x16"
IMAGE = "ibm-redhat-8-6-amd64-sap-applications-2"

```

4. Customize your SAP system configuration. In the same file, input.auto.tfvars, edit the SAP system configuration variables that are passed to the Ansible automated deployment. For descriptions of the variables, see the [readme](#) file.

```

$ # SAP system configuration - for ASE SYB
sap_sid = "NWD"
sap_ci_host = "10.243.132.10"
sap_ci_hostname = "sapnwase"
sap_ci_instance_number = "00"
sap_asc_s_instance_number = "01"
sap_aas_instance_number = "00"

# Kits paths
kit_sapcar_file = "/storage/NW75SYB/SAPCAR_1010-70006178.EXE"
kit_swpm_file = "/storage/NW75SYB/SWPM10SP31_7-20009701.SAR"
kit_saphotagent_file = "/storage/NW75SYB/SAPHOSTAGENT51_51-20009394.SAR"

```

```

$ # SAP system configuration - for ABAP HANA
sap_sid = "NWD"
sap_ci_host = "10.243.132.10"
sap_ci_hostname = "sapnwapp01"
sap_ci_instance_number = "00"
sap_asc_s_instance_number = "01"
hdb_instance_number = "00"
sap_aas_instance_number = "00"

# Kits paths
kit_sapcar_file = "/storage/NW75HDB/SAPCAR_1010-70006178.EXE"
kit_swpm_file = "/storage/NW75HDB/SWPM10SP31_7-20009701.SAR"
kit_saphotagent_file = "/storage/NW75HDB/SAPHOSTAGENT51_51-20009394.SAR"
kit_hdbclient_file = "/storage/NW75HDB/IMDB_CLIENT20_009_28-80002082.SAR"

```

Ansible decompresses the rest of the SAP kit files. For more information, see the [readme](#) file.

5. Initialize the Terraform CLI.

```
terraform init
```

6. Create a Terraform execution plan. The Terraform execution plan summarizes all the actions that are done to create the virtual private cloud instance in your account.

```
terraform plan plan1
```

Enter an SAP main password and your API key.

The SAP main password must be 10 - 14 characters long and contain at least one digit (0-9). It can contain only the following characters: a-z, A-Z, 0-9, @, #, \$, . *This password cannot contain exclamation points '!'. The password must not start with a digit or an underscore ().*

7. Verify that the plan shows all of the resources that you want to create and that the names and values are correct. If the plan needs to be adjusted, edit the input.auto.tfvars file to correct resources and run terraform plan again.
8. Apply the saved plan.

```
$ terraform apply "plan1"
```

The virtual private cloud and components are created and you see output similar to the `terraform plan` output.

9. Add the SAP credentials and the virtual server instance IP to the SAP GUI. For more information about the SAP GUI, see [SAP GUI](#).

Next steps

If you need to rename your resources after they are created, modify the input.auto.tfvars file to change the names and run `terraform plan` and `terraform apply` again. Do not use the IBM Cloud Dashboard and user interface to modify your VPC after it is created. The Terraform scripts create a complete solution and selectively modifying resources with the user interface might cause unexpected results.

If you need to remove the SAP Netweaver 7.X on HANA or AnyDB installation, go to your project folder and run `terraform destroy`. The `terraform destroy` command does not remove the VPC in this scenario because the VPC was created before these Terraform scripts were run.

Related information

For more information about Terraform on IBM Cloud, see [Getting started with Terraform on IBM Cloud](#).

For more information about using Terraform for creating only a VPC for SAP, without the SAP architecture, see [Creating single-tier virtual private cloud for SAP by using Terraform](#).

SAP One Support Notes that apply to this document:

- [SAP Note 84555 - Windows Server, Linux®, and UNIX: Certified hardware](#)
- [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#)
- [SAP Note 2923773 - Linux® on IBM Cloud \(IaaS\): Adaption of your SAP license](#)
- [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#)
- [SAP Note 2369910 - SAP Software on Linux®: General information](#)
- [SAP Note 171380 - Released IBM hardware \(Intel processors\) and IBM cloud services offers](#)
- [SAP Note 1380654 - SAP support in IaaS environments](#)

This document is referenced by:

- [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#)
- [SAP Note 2588225 - SAP on IBM Cloud: Protect against speculative execution vulnerabilities](#)
- [SAP Note 1380654 - SAP support in IaaS environments](#)
- [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#)

SAP NetWeaver with ASE

Automating SAP workload HA deployment on IBM Cloud VPC with Terraform and Ansible

You can use Terraform to automate IBM Cloud® VPC provisioning. The VPC provisioned includes virtual server instances with high network performance. The VPC infrastructure contains various Infrastructure-as-a-Service (IaaS) offerings, including virtual servers. After the VPC is provisioned, the scripts use the Ansible Playbooks to install the SAP system.

IBM Cloud VPC introduction

VPC is a public cloud offering that an enterprise uses to establish its own private cloud-like computing environment on shared [public cloud](#) infrastructure. VPC gives an enterprise the ability to define and control a virtual network that is logically isolated from all other public cloud tenants, creating a private and secure place on the public cloud.

Imagine that a cloud provider's infrastructure is a residential apartment building and multiple families live inside. A public cloud tenant is a kind of sharing an apartment with a few roommates. In contrast, having a VPC is like having your own private condominium; no one else has the key, and no one can enter the space without your permission.

VPC's logical isolation is implemented by using virtual network functions and security features that give the enterprise customer granular control over which IP addresses or applications can access particular resources. It is analogous to the "friends-only" or "public/private" controls on social media accounts used to restrict who can or can't see your otherwise public posts.

With IBM Cloud VPC, you can use the UI, CLI, and API to manually provision virtual server instances for VPC with high network performance. VPC infrastructure contains various Infrastructure-as-a-Service (IaaS) offerings including virtual servers for VPC.

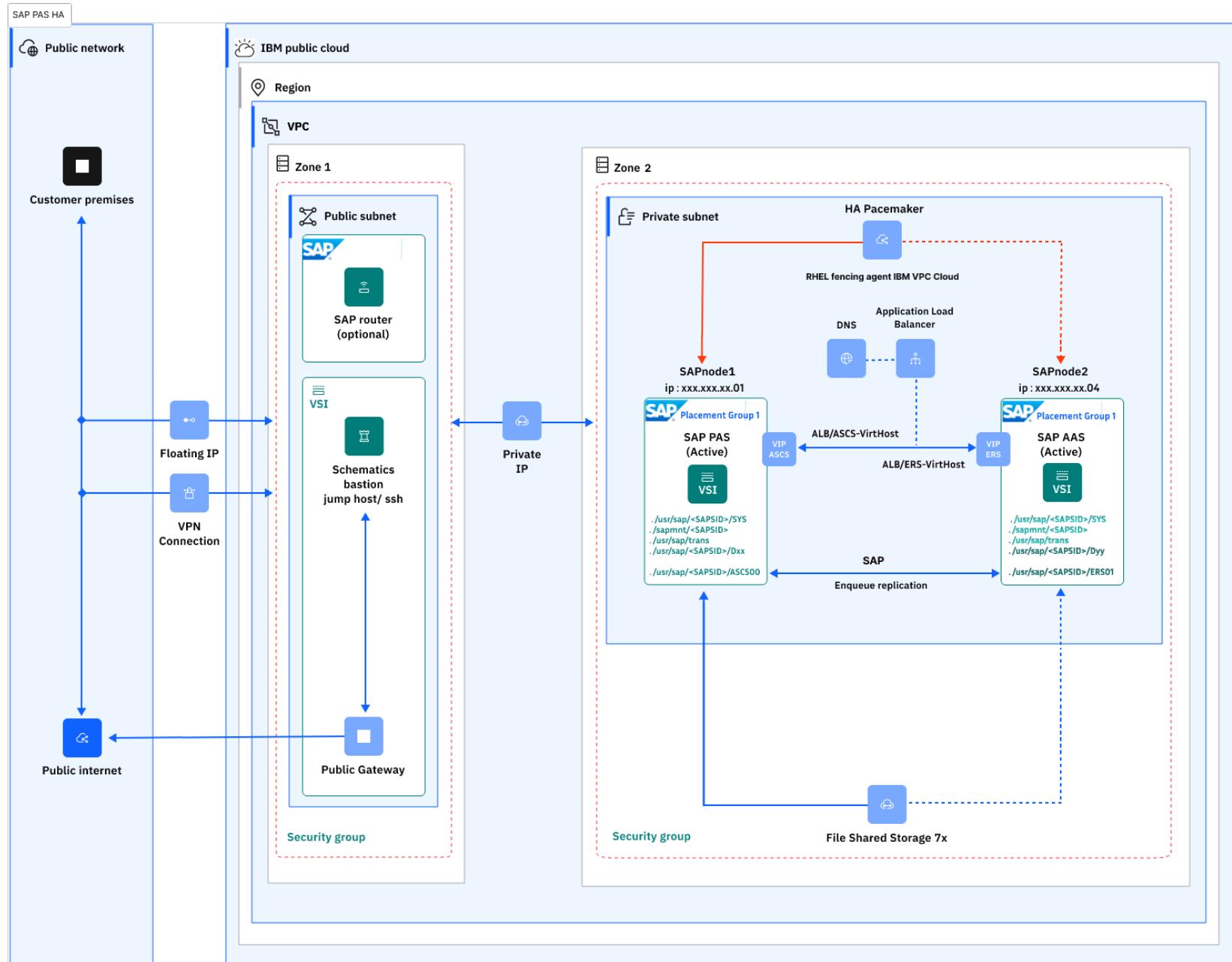
Use the following information to understand a simple use-case for planning, creating, and configuring resources for your VPC, and learn more about VPC overviews and VPC tutorials. For more information about the VPC, see [Getting started with Virtual Private Cloud \(VPC\)](#).

SAP products architecture on IBM Cloud VPC

A [Virtual Private Cloud \(VPC\)](#) contains one of the most secure and reliable cloud environments for SAP applications within your own VPC with virtual server instances. This represents an Infrastructure-as-a-Service (IaaS){: external} within IBM Cloud that offers all the benefits of isolated, secure, and flexible virtual cloud infrastructure from IBM. In comparison, the IBM Cloud classic infrastructure virtual servers offering uses virtual instances with native and VLAN networking to communicate with each other within a data center; however, the instances are restricted in one well-working pod by using subnet and VLAN networking as a gap scale up of virtual resources should rely between the pods. The IBM Cloud VPC network orchestrator layer concept eliminates the pod boundaries and restrictions, so this new concept handles all the networking for every virtual instance running within VPC across regions and zones.

Highly available system for SAP NetWeaver on IBM Cloud VPC

In a Highly Available (HA) system, every instance can run on a separate IBM Cloud virtual server instance. The cluster HA configuration for the SAP application server consists of two virtual server instances, each of them located in the same zone within the region by using placement groups. Placement groups assure that both cluster resources and cloud resources are also located in different compute nodes as specified in the following placement groups section:



SAP HA for SAP applications cluster nodes PAS (Active) and AAS (Active)

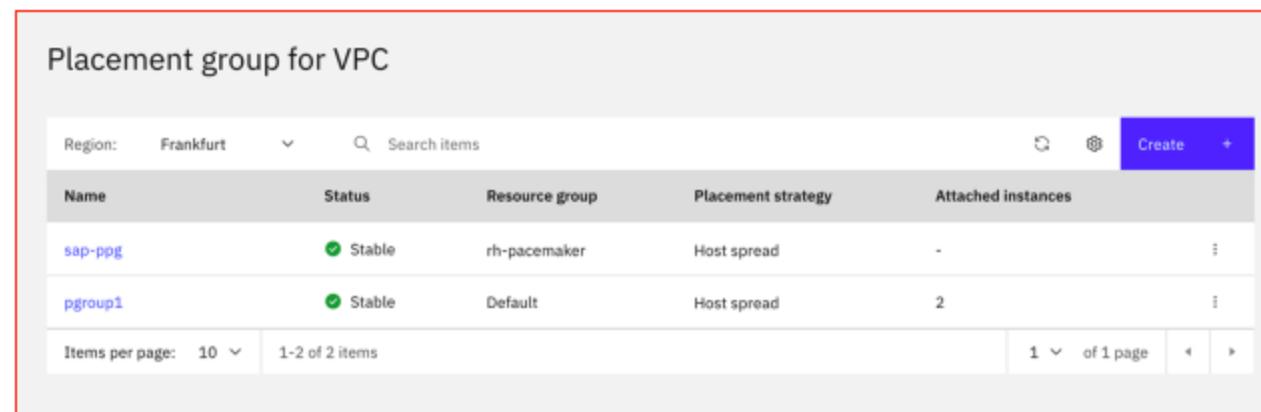
Placement groups on IBM Cloud VPC for SAP HA architecture

Placement Groups (PG) for VPC have two different anti-affinity strategies for high availability. By using the placement strategies, you minimize the chance of service disruption with virtual server instances that are placed on different hosts or into an infrastructure with separate power and network supplies.

The design of placement groups for IBM Cloud virtual servers solves this issue. Placement groups give a measure of control over the host on which a new public virtual server is placed. In this release, a “spread” rule is implemented, which means that the virtual servers within a placement group are spread onto different hosts. You can build a highly available application within a data center and know that your virtual servers are isolated from each other.

Placement groups with the spread rule are available to create in selected IBM Cloud data centers. After a spread rule is created, you can provision a virtual server into that group and ensure that it is not on the same host as any of your other virtual servers. This feature comes with no cost.

You can create your placement group and assign up to four new virtual server instances. With the spread rule, each of your virtual servers are provisioned on different physical hosts. In the following configuration example, the “Power Spread” option is used:



Placement groups host spread

Placement group for VPC					
Name	Status	Resource group	Placement strategy	Attached instances	
sapha-poc	Stable	wes-ic4sap-resourcegroup	Power spread	4	⋮
Items per page: 10 1 item 1 of 1 page ⋮					

Placement groups power spread

Following are the SAP instances that are required for HA scenario:

- ABAP SAP Central Services (ASCS) instance - contains the ABAP message server and the ABAP enqueue server.
- Enqueue Replication Server (ERS) instance for the ASCS instance.
- Database instance
- Primary Application Server (PAS) instance on node 1.
- Additional Application Server (AAS) instance on node 2.



Note: It is recommended to run both the ASCS instance and the ERS instance in a switchover cluster infrastructure.

IBM Cloud File Storage for VPC for SAP HA architecture

[IBM Cloud File Storage for VPC](#) technology is used to make the SAP directories available to the SAP system. The technologies of choice are NFS, shared disks, and cluster file system. If you have decided to use the HA solution for your SAP system, make sure that you properly address the HA requirements of the SAP file systems in your SAP environment.

File shares for VPC								
Name	Status	Resource groups	Location	Mount targets	Size	Replication role	Encryption type	
usrsap-as1-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	⋮
usrsap-as2-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	⋮
usrsap-sapsacs-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	⋮
usrsap-sapers-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	⋮
usrsap-sapmnt-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	⋮
usrsap-sapsys-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	⋮
usrsap-trans-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	80 GB	None	Provider managed	⋮

File shares for VPC

- File shares that are mounted as NFS permanent file systems on both cluster nodes for SAP HA application:
 - `/usr/sap/<SAPSID>/SYS`
 - `/sapmnt<SAPSID>`
 - `/usr/sap/trans`
- Cluster-managed file systems for SAP HA application: ASCS
 - `/usr/sap/<SAPSID>/ASCS00`
 - `/usr/sap/<SAPSID>/ERS01`
- Permanent NFS mount on SAP HA application node 1 PAS instance:
 - `/usr/sap/<SAPSID>/Dxx`
- Permanent NFS mount on SAP HA application node 2 dialog instance:
 - `/usr/sap/<SAPSID>/Dyy`

Prerequisites

You need to install the hardware (hosts, disks, and network) and decide how to distribute the database, SAP instances, and if required, the Network File System (NFS) server over the cluster nodes.

Context

Following are the types of SAP directories:

- Physically shared directories: `/<sapmnt>/<SAPSID>` and `/usr/sap/trans`

- Logically shared directories that are bound to a node, such as `/usr/sap`, with the following local directories:
 - `/usr/sap/<SAPSID>`
 - `/usr/sap/<SAPSID>/SYS`
 - `/usr/sap/hostctrl`
- Local directories that contain the SAP instances such as `/usr/sap/<SAPSID>/ASCS<Instance_Number>`
- The global transport directory may reside on a separate SAP transport host as a standard three systems transport layer configuration.

You need at least two nodes and a shared file system for distributed ASCS and ERS instances. The assumption is that the rest of the components are distributed on other nodes.

ASCS and ERS installation

In order for the ASCS and ERS instances to be able to move from one node to the other, they need to be installed on a shared file system and use virtual hostnames based on the virtual IP.

In this VPC-based SAP HA solution, the shared file system that is required by the cluster is replaced by the NFS-mounted file storage, and the virtual IP is replaced by the Application Load Balancer for VPC (ALB).

In this scenario, three ALBs are used, one for each Single Point of Failure (SPOF) component in order to replace the virtual IP requirement: ALB for ASCS, ALB for ERS, and ALB for ASE Sybase. Each ALB is configured as a backend for the corresponding cluster servers and redirects all of the communication that is received on the front-end ports to the active server in the backend pool.

Load balancers for VPC						
Region:	Frankfurt	▼	Search: poc	X		
Name	Status	Family	Resource group	Type	Hostname	Location
db-alb-hana-poc	Active	Application	wes-ic4sap-resourcegroup	Private	20bdd130-eu-de.lb.appdomain.cloud	Frankfurt
sap-alb-ers-poc	Active	Application	wes-ic4sap-resourcegroup	Private	3941d983-eu-de.lb.appdomain.cloud	Frankfurt
sap-alb-ascs-poc	Active	Application	wes-ic4sap-resourcegroup	Private	56a9190d-eu-de.lb.appdomain.cloud	Frankfurt

Application load balancer management of HA IPs mechanism

Private application load balancer

A [private application load balancer](#) is accessible through your private subnets that you configured to create the load balancer.

Similar to a public application load balancer, your private application load balancer service instance is assigned an FQDN; however, this domain name is registered with one or more private IP addresses.

IBM Cloud operations change the number and value of your assigned private IP addresses over time, based on maintenance and scaling activities. The backend virtual server instances that host your application must run in the same region and under the same VPC.

Use the assigned ALB FQDN to send traffic to the private application load balancer to avoid connectivity problems to your applications during system maintenance or scaling down activities.

Each ALB sends traffic to the cluster node where the application (ASCS, ERS, ASE Sybase DB) is running. During the cluster failover, the ALB redirects all the traffic to the new node where the resources are up and running.



Note: DNS-as-a-Service (DNSaaS) is the management IBM Cloud VPC DNS service of HA and FQDN (IPs) mechanism.



Note: The ALB has a default of 50 seconds for client and server timeout, so after 50 seconds of inactivity, the connection is closed. To support SAP connections through ALB and not lose connection after 50 seconds, you need to request a change this value to a minimum of 300 seconds (client-side idle connection = minimum 300s and server-side idle connection = minimum 300s). To request this change, open a support ticket. This is an account-wide change that affects all of the ALBs in your account. For more information, see [Connection timeouts](#).

DNS Services with VPC

[IBM Cloud DNS Services](#) provide private DNS to VPC users. Private DNS zones are resolvable only on IBM Cloud and from explicitly [permitted networks](#) in an account. To get started, create a DNS Services instance by using the IBM Cloud console.

DNS Services allows you to:

- Create the private DNS zones that are collections for holding the domain names.
- Create the DNS resource records under these DNS zones.
- Specify the access controls used for the DNS resolution of resource records on a zone-wide level.

DNS Services also maintains its own worldwide set of DNS resolvers. Instances that are provisioned under IBM Cloud on an IBM Cloud network can use resource records that are configured through IBM Cloud DNS Services by querying DNS Services resolvers.

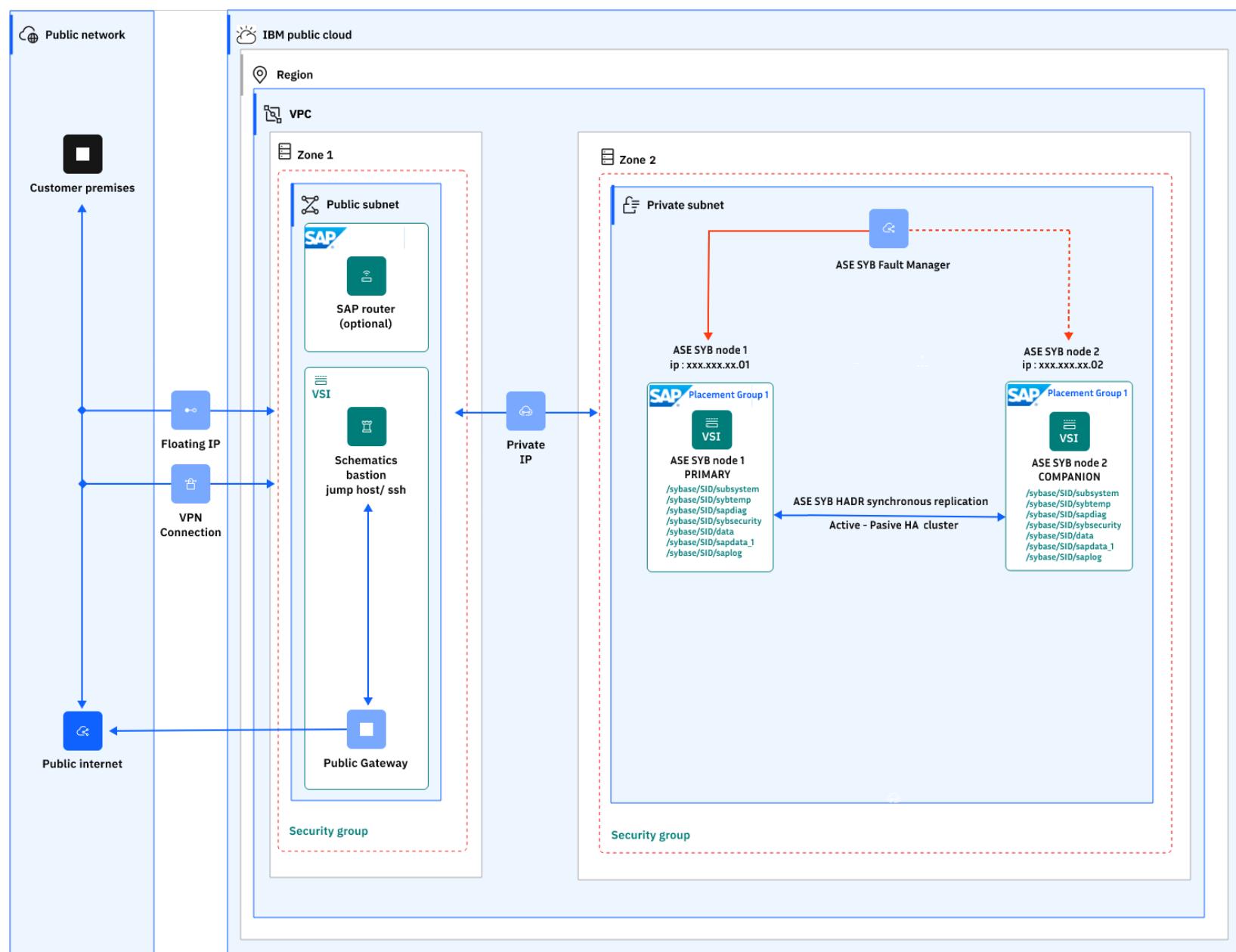
Resource records and zones that are configured through DNS Services are:

- Separated from the wider public DNS, and their publicly accessible records.
- Hidden from the system outside of and not part of the IBM Cloud private network.
- Accessible only from the system that you authorize on the IBM Cloud private network.
- Resolvable only via the resolvers provided by the service.

The DNS service maps the FQDN of each ALB to the virtual hostnames of the ASCS, ERS, and ASE Sybase that are used by SAP applications.

Type	Name	Value	TTL
CNAME	dbpochana	is an alias of 20bdd130-eu-de.lb.appdomain.cloud	12 hr
CNAME	sappocers	is an alias of 3941d983-eu-de.lb.appdomain.cloud	12 hr
CNAME	sappocases	is an alias of 56a9190d-eu-de.lb.appdomain.cloud	12 hr

Highly available system for SAP ASE Sybase database with HADR system



SAP HA for ASE Sybase DB instances cluster nodes primary (Active) and Secondary (Companion)

At the most basic level, a standard HA ASE Sybase cluster in an active(primary)-passive(companion) configuration has two nodes: one is the primary node and the other is the standby node. This means that the primary node is actively serving the active SAP DB instances (Primary and Companion), while the standby node is waiting to jump in if there is any failure.

The cluster is set with a virtual hostname IP (hostname is mapped to the FQDN of the ASE Sybase ALB through DNS, which is the same as

explained previously for SAP ASCS and ERS instances). Application instances (PAS and AAS) are used on the SAP profiles to call that particular component. The cluster assigns the virtual IP to the active node and uses a heartbeat monitor to confirm the availability of the components. If the primary node stops responding, it triggers the automatic failover mechanism that calls the standby node to step up to become the primary node. The ALB detects the change, redirects the traffic to the new active node, and assigns the virtual IP to it, restoring the component availability. Once fixed, the failed node comes online as a standby node.

SAP Sybase HADR system supports synchronous replication

The SAP Sybase HADR system supports synchronous replication between the primary and standby servers for high availability. An active-active setup is a two-node configuration where both nodes in the cluster include SAP ASE managing independent workloads, capable of taking over each others workload in the event of a failure.

The SAP ASE server that takes over the workload is called a secondary companion, and the SAP ASE server that fails is called the primary companion. Together they are companion servers. This movement from one node to another is called failover. After the primary companion is ready to resume its workload, it is moved back to its original node. This movement is called a failback.

When a system fails over, clients that are connected to the primary companion and use the failover property automatically reestablish their network connections to the secondary companion. You must tune your operating system to successfully manage both servers during fail over. See your operating system documentation for information about configuring your system for high availability. An SAP ASE configured for failover in an active-active setup can be shut down using the shutdown command only after you have suspended SAP ASE from the companion configuration, at both the server level and the platform level.

The always-on option in a High Availability and Disaster Recovery (HADR) system consists of two SAP ASE servers:

- Primary on which all transaction processing takes place.
- Warm standby (referred to as a "standby server" in DR mode, and as a "companion" in HA mode) for the primary server, and contains copies of designated databases from the primary server.



Note: The HADR feature that is shipped with SAP ASE version 16.0 SP02 supports only a single-companion server.

Some high-availability solutions (for example, the SAP Adaptive Server Enterprise Cluster Edition) share or use common resources between nodes. However, the HADR system is a "shared nothing" configuration, each node has separate resources including disks.

In an HADR system, servers are separate entities and data is replicated from the primary server to the companion server. If the primary server fails, a companion server is promoted to the role of primary server either manually or automatically. Once the promotion is complete, clients can reconnect to the new primary server, and see all committed data, including data that was committed on the previous primary server.

Servers can be separated geographically, which makes an HADR system capable of withstanding the loss of an entire computing facility.



Note: The HADR system includes an embedded SAP Replication Server, which synchronizes the databases between the primary and companion servers. SAP ASE uses the Replication Management Agent (RMA) to communicate with Replication Server and SAP Replication Server uses Open Client connectivity to communicate with the companion SAP ASE.

The Replication Agent detects any data changes made on the primary server and sends them to the primary SAP Replication Server. In the figure above, the unidirectional arrows indicate that, although both SAP Replication Servers are configured, only one direction is enabled at a time.

The HADR system supports synchronous replication between the primary and standby servers for high availability so the two servers can keep in sync with Zero Data Loss (ZDL). This requires a network link that is fast enough between the primary and standby server so that synchronous replication can keep up with the primary servers workload. Generally, this means that the network latency is approximately the same speed as the local disk IO speed, a few (fewer than 10) milliseconds. Anything longer than a few milliseconds may result in a slower response to write operations at the primary.

The HADR system supports asynchronous replication between the primary and standby servers for disaster recovery. The primary and standby servers by using asynchronous replication can be geographically distant, meaning they can have a slower network link. With asynchronous replication, Replication Agent Thread captures the primary servers workload, which is delivered asynchronously to SAP Replication Server. The SAP Replication Server applies these workload change to the companion server.

The most fundamental service that is offered by the HADR system is the failover; planned or unplanned from the primary to the companion server, which allows maintenance activity to occur on the old primary server, while applications continue on the new primary.

The HADR system provides protection in the event of a disaster. If the primary server is lost, the companion server can be used as a replacement. Client applications can switch to the companion server, and the companion server is quickly available for users. If the SAP Replication Server was in synchronous mode before the failure of the primary server, the Fault Manager automatically initiates failover with

zero data loss.

Fault Manager installation on the SAP ASCS node

The required parameters are asked during the installation process to create a profile for the fault manager and then adds it to the instance start profile. It is also possible to run the installation by using an existing profile: `sybdbfm install pf=<SYBHA.PFL>` In this case, the installation process will only ask for profile parameters missing in the profile.



Note: Fault manger is integrated with ASCS on same SAP PAS/AAS cluster (start/stop/move together).

There may be some data loss if the SAP Replication Server was in asynchronous mode and you must use manual intervention to failover for disaster recovery.

Connection attempts to the companion server without the necessary privileges are silently redirected to the primary companion via the login redirection mechanism, which is supported by Connectivity libraries. If login redirection is not enabled, client connections fail and are disconnected.

The SAP ASE HADR option installs the below components:

- SAP ASE
- SAP Replication Server
- Replication Management Agent (RMA)
- SAP Host Agent
- Fault Manager
- SAP ASE Cockpit



Note: This automation is offered at no cost; however, the provisioned infrastructure comes at cost.

VPC with Additional Application Server (AAS) ABAP on Linux for SAP HANA

You can use Terraform scripts to create a single-tier VPC and create the AAS to HANA and AnyDB infrastructure on the VPC. The Terraform scripts use the VPC information that you provide and then call the Ansible playbook to create the SAP architecture on the specified VPC. Terraform on IBM Cloud® enables predictable and consistent provisioning of IBM Cloud Virtual Private Cloud (VPC) infrastructure resources so that you can rapidly build complex, cloud environments. IBM Cloud VPC infrastructure consists of SAP certified hardware that uses Intel® Xeon CPUs and more Intel® technologies.

You have two deployment methods to choose from:

- Terraform scripts that run from the CLI on your bastion server.
- Schematics user interface accessed from your cloud dashboard menu.

You can create SAP AAS NetWeaver 7.x on the SAP HANA-based ABAP stack.

SAP solution implemented

Many SAP enterprise solutions are built on the SAP platform (SAP NetWeaver) including:

- SAP HANA as Primary Persistence for SAP NetWeaver-based applications
- SAP Business Suite applications (ERP, CRM, and SCM, and other applications),
- SAP Business Warehouse (BW), and
- Other SAP enterprise solutions

SAP NetWeaver has two distinct aspects, ABAP and Java. Many applications that are built on the SAP NetWeaver's ABAP or Java (or both) application servers run on SAP DB owned HANA and ASE Sybase either in AnyDB platforms (MSSQL, Oracle, and Db2).

Technical interfaces are available for applications that are built on the SAP NetWeaver AS ABAP and AS Java to run on SAP HANA and AnyDB. However, specific development enablement is normally required for each application to ensure that it runs optimally on the SAP HANA. SAP Business Suite applications (ERP, CRM, SCM, and other applications), SAP Business Warehouse (BW), and other SAP NetWeaver-based applications were modified to run on SAP HANA and have many advantages. Also, various components and complimentary applications that are built on SAP NetWeaver can also run on SAP HANA or AnyDB by using the provided SAP NetWeaver DB interfaces.

The SAP HANA as primary persistence for SAP NetWeaver-based applications scenario has one restriction: SAP NetWeaver ABAP and Java

application servers must run on separate hardware servers from the SAP HANA hardware.

What is created

The scripts automate the virtual infrastructure resources, provisioning the processes for the SAP architecture in an existing VPC with a distributed environment. SAP AAS NetWeaver 7.x (HANA or ASE SYB) application server on a distinct VSI VPC system and SAP HANA DB on a dedicated server type VSI VPC box are provisioned. The scripts work in two phases.

During the first phase of [Automate SAP bastion server – SAP media storage repository](#), the following virtual infrastructure resources based on the components from the existing VPC created by the bastion server are:

- 1 VPC where the virtual server instance is provisioned.
- 1 security group. The rules for this security group are:
 - Allow inbound DNS traffic (port 53).
 - Allow inbound SSH traffic (TCP port 22).
 - Allow all outbound traffic from the virtual server instance.
 - Allow all traffic in the security group.
- 1 subnet to enable the networking in your VPC.
- 2 virtual server instances with SAP certified storage and network configurations.
- 1 floating IP address used to access your VPC virtual server instance over the public network.

During the second phase, the Ansible Playbooks is called and the SAP architecture is installed for both dedicated virtual server instance (VSI) SAP application; VSI system and dedicated SAP HANA VSI box. The SAP architecture that is deployed on the SAP NetWeaver 7.x release is a stand-alone dedicated SAP HANA 2.0 box release. For more information about this architecture, see [Automating SAP HANA stand-alone virtual server instance on IBM Cloud® VPC by using Terraform and Ansible](#).

You can provision only one instance of the service per IBM Cloud region.

Schematics deployment

When you run the scripts with the Schematics interface, you:

- Enter the workspace information.
- Enter the GitHub path for the chosen solution either on NetWeaver AAS for HANA.
- Modify the parameters in the Schematics interface. They are the same parameters as the `input.auto.tfvars` file that you use with the cli.

Virtual server instance configuration

Following are the supported operating system images for SAP NetWeaver primary application server:

- ibm-redhat-8-4-amd64-sap-applications-2
- ibm-redhat-8-6-amd64-sap-applications-2
- ibm-sles-15-3-amd64-sap-applications-2
- ibm-sles-15-4-amd64-sap-applications-3

Following are the supported operating system images for SAP HANA database:

- ibm-redhat-8-4-amd64-sap-hana-2
- ibm-redhat-8-6-amd64-sap-hana-2
- ibm-sles-15-3-amd64-sap-hana-2
- ibm-sles-15-4-amd64-sap-hana-1

For both server instances there are:

- Two SSH keys are configured to access SSH as `root`.
- Three storage volumes as described in the `input.auto.tfvars` file.

What is created for anydb

The scripts use the information that you provide for an existing VPC and deploy AAS to SAP HANA or AnyDB on a different host than CI (SAP Central Instance) VSI host. For more information about this architecture, see [SAP NetWeaver 7.x on UNIX with HANA or AnyDB on IBM Cloud](#)

[VPC on IBM Cloud VPC](#). You specify the information for the VPC to use in the `input.auto.tfvars` file.

The scripts call the Ansible Playbooks to install the SAP architecture.

Script files

The configuration and script files are provided on GitHub. Each supported interface for the SAP solution installation has its own folder in the GitHub repository:

- [GitHub repository for Terraform – AAS HANA](#)

Terraform interface

To run the Terraform script, you modify:

- The `input.auto.tfvars` file to specify the existing VPC resources for your solution. Specify the variables for the existing VPC:
 - VPC name
 - Security group
 - Subnet
 - Hostname
 - Profile
 - Image
 - Up to two SSH keys

You can change the default SAP system configuration settings to match your solution. You can also specify the location where you downloaded the SAP kits.

The IBM Cloud Provider plug-in for Terraform on IBM Cloud uses these configuration files to install AAS to SAP HANA and AnyDB on the specified VPC in your IBM Cloud account.

Support

There are no warranties of any kind, and there is no service or technical support available for these materials from IBM®. As a recommended practice, review carefully any materials that you download from this site before using them on a live system.

Though the materials provided herein are not supported by the IBM® Service organization, your comments are welcomed by the developers, who reserve the right to revise, readapt or remove the materials at any time. To report a problem, or provide suggestions or comments, open a GitHub issue.

Before you begin

Before you use the scripts in the bastion cli:

- Set up your account to access the VPC. Make sure that your account is [upgraded to a paid account](#).
- If you have not already, create a Bastion server to store the SAP kits. For more information, see [Automate SAP bastion server - SAP media storage repository](#).
- Download the SAP kits from the SAP Portal to your Deployment Server. Make note of the download locations. Ansible decompresses the files. For more information, see the [readme](#) file.
- [Create or retrieve an IBM Cloud API key](#). The API key is used to authenticate with the IBM Cloud platform and to determine your permissions for IBM Cloud services.
- [Create or retrieve your SSH key ID](#). You need the 40-digit UUID for the SSH key, not the SSH key name.
- Terraform should already be installed on the bastion server that you deployed. For more information, see [Bastion server for SAP deployment](#).
- (Optional - Catalog Tile) create secrets for your credentials and passwords by using the [Secrets Manager](#).

Deploying SAP AAS NetWeaver 7.x on HANA by using the Schematics user interface

Use these steps to configure the SAP Additional Application Server (AAS) NetWeaver with HANA or AnyDB on your existing VPC by using the Schematics interface. The script takes 2 - 3 hours to complete.

1. From the IBM Cloud menu, select **Schematics**.
2. Click **Create** workspace.

3. On the **Specify template** page:
 - Enter the URL for the Schematics interface.
 - Select the **Terraform version** that is listed in the readme file.
 - Click **Next**.
4. On the **workspace details** page:
 - Enter a name for the workspace.
 - Select a **Resource group**.
 - Select a **Location** for your workspace. The workspace location does not have to match the resource location.
 - Select **Next**.
5. Select **Create** to create your workspace.
6. On the workspace settings page, in the input variables section, review the default input variables and provide values that match your solution.
 For a more detailed description of each parameter, check the GitHub repo [AAS HANA readme](#) file, chapter “Input parameter file”. Also, make sure to mark the parameters that contain sensitive information like passwords, API, and ssh private keys as “sensitive”. These parameters are marked as “sensitive” in the readme file, under “Input parameter file”.
7. On the workspace settings page, click **Generate plan**. Wait for the plan to complete.
8. Click **View log** to review the log files of your terraform execution plan.
9. Apply your Terraform template by clicking **Apply plan**.
10. Review the log file to ensure that no errors occur during the provisioning, modification, or deletion process.

Deploying SAP AAS NetWeaver (ABAP) on HANA with the Deployable Architecture tile interface

Use these steps to configure the SAP AAS NetWeaver (ABAP) on HANA on your existing VPC by using the catalog tile interface. The script takes 2 - 3 hours to complete.

1. From the IBM Cloud catalog, select **VPC with Additional Application Server ABAP on Linux for SAP HANA** on HANA tile. The **Create** tab opens for VPC with Additional Application Server ABAP on Linux for SAP HANA. For more information about this deployment, see the About tab or the readme file link.
2. Select the latest version.
3. Select **VPC with Additional Application Server ABAP on Linux for SAP HANA on Deployable Architecture tile** variation.
4. Click **Review deployment** options:
 - **Add to project** to add this deployment to an IBM Cloud project and combine it with other deployments. IBM Cloud projects include several more pipeline steps before deployment, including deployment validation, cost calculation, compliance verification, and approval process.
 - **Create from the CLI** to get the CLI command. With this command you can trigger the deployment from the CLI.
 - **Work with code** to embed the code into other terraform deployments.
 - **Deploy with IBM Cloud Schematics** to trigger the deployment process directly.
5. Select **Deploy with IBM Cloud Schematics**.
6. Add the input parameters for this installation. There are 3 categories of parameters:
 - **Workspace** - These parameters define the workspace that is automatically created in Schematics:
 - Enter a name for the workspace or use the default name.
 - The Resource Group used to create resources. Use default or create a Resource Group.
 - Select a location to create your Schematics workspace. The workspace location need not match the resource location.
 - **Required input variables** - Review the default input variables and provide values that match your solution. These parameters are specific to your deployment. For more detailed information, see the [Readme file](#).

Parameter	Description
BASTION_FLOATING_IP	Required only for Schematics Deployments. The Floating IP from the Bastion Server.

HOSTNAME	The hostname for the VSI. The hostname should be up to 13 characters as required by SAP. For more information on the rules regarding hostnames for SAP systems, check SAP Note 611361: Hostnames of SAP ABAP Platform servers
REGION	The cloud region to deploy the solution. The regions and zones for VPC are listed here . Review supported locations in IBM Cloud Schematics here . Sample value: eu-de.
RESOURCE_GROUP	The name of an existing Resource Group for VSIs and Volumes resources. Default value: "Default". The list of Resource Groups is available here .
SECURITY_GROUP	The name of an existing Security group. The list of security groups is available here .
SSH_KEYS	The list of SSH Keys UUIDs that are allowed to SSH as root to the VSI can contain one or more IDs. The list of SSH Keys is available here . Sample input (use your own SSH UUIDs from IBM Cloud){: external}: ["r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a", "r010-3fcfd9fe7-d4a7-41ce-8bb3-d96e936b2c7e"]
SUBNET	The name of an existing subnet. The list of subnets is available here .
VPC	The name of an existing VPC. The list of VPCs is available here .
ZONE	The cloud zone where to deploy the solution. Sample value: eu-de-2.
ibmcloud_api_key	IBM Cloud API key (Sensitive* value).
private_ssh_key	Required only for Schematics Deployments - Input your id_rsa private key pair content in OpenSSH format (Sensitive* value). This private key should be used only during the terraform provisioning and it is recommended to be changed after the SAP deployment.
hdb_instance_number	The instance number of the SAP HANA database server.
sap_aas_instance_number	Technical identifier for the internal processes of the additional application server.
sap_asci_instance_number	Technical identifier for the internal processes of ASCS.
sap_ci_host	IP address of the existing SAP Central Instance.
sap_ci_hostname	The hostname of the existing SAP Central Instance.
sap_ci_instance_number	Technical identifier for the internal processes of the Central Instance.
sap_sid	The SAP system ID identifies the entire SAP system.
sap_main_password	Common password for all users that are created during the installation (See Obs*).

Required Variables

- **Optional variables** - Review and update the optional input variables. The Ansible scripts expect the SAP kits to be in the default locations listed. For more information, see the [Readme file - Input Parameters](#).

Parameter	Description
ID_RSA_FILE_PATH	The file path for private_ssh_key is automatically generated by default. If it is changed, it must contain the relative path from Git repo folders. Default value: "ansible/id_rsa".
IMAGE	The OS image used for the VSI. A list of images is available here .
PROFILE	The profile used for the VSI. A list of profiles is available here . For more information about supported DB/OS and IBM Gen 2 Virtual Server Instances (VSI), check SAP Note 2927211: SAP Applications on IBM Virtual Private Cloud .

VOL1	Volume 1 Size - The size for the disks in GB that are to be attached to the VSI and used by SAP.
VOL2	Volume 2 Size - The size for the disks in GB that are to be attached to the VSI and used by SAP.
kit_sapcar_file	Path to the sapcar binary, as downloaded from SAP Support Portal.
kit_swpm_file	Path to the SWPM archive (SAR), as downloaded from SAP Support Portal.
kit_saphostagent_file	Path to the SAP Host Agent archive (SAR), as downloaded from SAP Support Portal.
kit_hdbclient_file	Path to the HANA DB client archive (SAR), as downloaded from SAP Support Portal.

Optional Variables

7. Accept the license agreement.
8. Select **Deploy**. The deployment starts and you are directed to the Schematics page that displays the script log files for you to monitor the deployment progress.

Creating the infrastructure using Terraform with the bastion server CLI

Use these steps to configure the IBM Cloud Provider plug-in and use Terraform to install SAP AAS to SAP HANA and AnyDB on your existing VPC on an already deployed SAP NetWeaver 7.X with SAP HANA 2.0 or ASE SYB as a Central Instance.

The script takes 1 - 2 hours to complete.

1. Access the bastion server cli.
2. Clone the solution repository and change to the folder.

ASE SYB 16 Clone the solution repository from <https://github.com/IBM-Cloud/sap-aas-abap-ase-syb> and cd to the sap-aas-abap-ase-syb/cli folder.

```
$ git clone https://github.com/IBM-Cloud/sap-aas-abap-ase-syb
cd sap-aas-abap-ase-syb/cli/
```

SAP HANA 2.0: Clone the solution repository from <https://github.com/IBM-Cloud/sap-abap-hana-aas> and cd to the sap-abap-hana-aas folder.

```
$ git clone https://github.com/IBM-Cloud/sap-abap-hana-aas.git
cd sap-abap-hana-aas/
```

3. Modify the `input.auto.tfvars` file to specify the information for the existing VPC, your region, zone, networking component names, hostname for the AAS VSI,profile, and image. You need your 40-digit SSH key ID for this file. The second SSH key is optional. For more options for profile, see [Instance Profiles](#). For more options, see [Images](#). For descriptions of the variables, see the [readme](#) file.

The VSI OS images that are supported for this solution for Netweaver Additional Application Server are:

- ibm-redhat-8-4-amd64-sap-applications-2
- ibm-redhat-8-6-amd64-sap-applications-2
- ibm-sles-15-3-amd64-sap-applications-2
- ibm-sles-15-4-amd64-sap-applications-4

```
$ # Infra VPC variables for ASE SYB
REGION    = "eu-de"
ZONE      = "eu-de-2"
VPC       = "ic4sap"                      # EXISTING Security group name
SECURITY_GROUP = "ic4sap-securitygroup"     # EXISTING Security group name
RESOURCE_GROUP = "wes-automation"
SUBNET    = "ic4sap-subnet"                 # EXISTING Subnet name
SSH_KEYS   = [ "r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a" , "r010-3fcfd9fe7-d4a7-41ce-8bb3-
d96e936b2c7e" ]

# SAP AAS VSI variables:
```

```

HOSTNAME = "sapnwase-as01"
PROFILE = "bx2-4x16"
IMAGE = "ibm-redhat-8-4-amd64-sap-applications-2

$ # Infra VPC variables for ABAP HANA
REGION      = "eu-de"
ZONE        = "eu-de-2"
VPC          = "ic4sap" # EXISTING Security group name
SECURITY_GROUP = "ic4sap-securitygroup" # EXISTING Security group name
RESOURCE_GROUP = "wes-automation"
SUBNET       = "ic4sap-subnet" # EXISTING Subnet name
SSH_KEYS     = [ "r010-57bfc315-f9e5-46bf-bf61-d87a24a9ce7a" , "r010-3fc9fe7-d4a7-41ce-8bb3-d96e936b2c7e" ]
ID_RSA_FILE_PATH = "ansible/id_rsa"

# SAP AAS variables:
HOSTNAME = "sapnwapp"
PROFILE = "bx2-4x16"
IMAGE = "ibm-redhat-8-6-amd64-sap-applications-2"

```

4. Customize your SAP system configuration. In the same file, input.auto.tfvars, edit the SAP system configuration variables that are passed to the Ansible automated deployment. For descriptions of the variables, see the [readme](#) file.

```

$ # SAP system configuration - for ASE SYB
sap_sid = "NWD"
sap_ci_host = "10.243.132.10"
sap_ci_hostname = "sapnwase"
sap_ci_instance_number = "00"
sap_asc_s_instance_number = "01"
sap_aas_instance_number = "00"

# Kits paths
kit_sapcar_file = "/storage/NW75SYB/SAPCAR_1010-70006178.EXE"
kit_swpm_file = "/storage/NW75SYB/SWPM10SP31_7-20009701.SAR"
kit_saphotagent_file = "/storage/NW75SYB/SAPHOSTAGENT51_51-20009394.SAR"

```

```

$ # SAP system configuration - for ABAP HANA
sap_sid = "NWD"
sap_ci_host = "10.243.132.10"
sap_ci_hostname = "sapnwapp01"
sap_ci_instance_number = "00"
sap_asc_s_instance_number = "01"
hdb_instance_number = "00"
sap_aas_instance_number = "00"

# Kits paths
kit_sapcar_file = "/storage/NW75HDB/SAPCAR_1010-70006178.EXE"
kit_swpm_file = "/storage/NW75HDB/SWPM10SP31_7-20009701.SAR"
kit_saphotagent_file = "/storage/NW75HDB/SAPHOSTAGENT51_51-20009394.SAR"
kit_hdbclient_file = "/storage/NW75HDB/IMDB_CLIENT20_009_28-80002082.SAR"

```

Ansible decompresses the rest of the SAP kit files. For more information, see the [readme](#) file.

5. Initialize the Terraform CLI.

```
terraform init
```

6. Create a Terraform execution plan. The Terraform execution plan summarizes all the actions that are done to create the virtual private cloud instance in your account.

```
terraform plan plan1
```

Enter an SAP main password and your API key.

The SAP main password must be 10 - 14 characters long and contain at least one digit (0-9). It can contain only the following characters: a-z, A-Z, 0-9, @, #, \$, . *This password cannot contain exclamation points '!'. The password must not start with a digit or an underscore ().*

7. Verify that the plan shows all of the resources that you want to create and that the names and values are correct. If the plan needs to be adjusted, edit the input.auto.tfvars file to correct resources and run terraform plan again.
8. Apply the saved plan.

```
$ terraform apply "plan1"
```

The virtual private cloud and components are created and you see output similar to the `terraform plan` output.

9. Add the SAP credentials and the virtual server instance IP to the SAP GUI. For more information about the SAP GUI, see [SAP GUI](#).

Next steps

If you need to rename your resources after they are created, modify the `input.auto.tfvars` file to change the names and run `terraform plan` and `terraform apply` again. Do not use the IBM Cloud Dashboard and user interface to modify your VPC after it is created. The Terraform scripts create a complete solution and selectively modifying resources with the user interface might cause unexpected results.

If you need to remove the SAP Netweaver 7.X on HANA or AnyDB installation, go to your project folder and run `terraform destroy`. The `terraform destroy` command does not remove the VPC in this scenario because the VPC was created before these Terraform scripts were run.

Related information

For more information about Terraform on IBM Cloud, see [Getting started with Terraform on IBM Cloud](#).

For more information about using Terraform for creating only a VPC for SAP, without the SAP architecture, see [Creating single-tier virtual private cloud for SAP by using Terraform](#).

SAP One Support Notes that apply to this document:

- [SAP Note 84555 - Windows Server, Linux®, and UNIX: Certified hardware](#)
- [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#)
- [SAP Note 2923773 - Linux® on IBM Cloud \(IaaS\): Adaption of your SAP license](#)
- [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#)
- [SAP Note 2369910 - SAP Software on Linux®: General information](#)
- [SAP Note 171380 - Released IBM hardware \(Intel processors\) and IBM cloud services offers](#)
- [SAP Note 1380654 - SAP support in IaaS environments](#)

This document is referenced by:

- [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#)
- [SAP Note 2588225 - SAP on IBM Cloud: Protect against speculative execution vulnerabilities](#)
- [SAP Note 1380654 - SAP support in IaaS environments](#)
- [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#)

High availability scenarios on Power Virtual Server

Automating SAP workload HA deployment on IBM Cloud VPC with Terraform and Ansible

You can use Terraform to automate IBM Cloud® VPC provisioning. The VPC provisioned includes virtual server instances with high network performance. The VPC infrastructure contains various Infrastructure-as-a-Service (IaaS) offerings, including virtual servers. After the VPC is provisioned, the scripts use the Ansible Playbooks to install the SAP system.

IBM Cloud VPC introduction

VPC is a public cloud offering that an enterprise uses to establish its own private cloud-like computing environment on shared [public cloud](#) infrastructure. VPC gives an enterprise the ability to define and control a virtual network that is logically isolated from all other public cloud tenants, creating a private and secure place on the public cloud.

Imagine that a cloud provider's infrastructure is a residential apartment building and multiple families live inside. A public cloud tenant is a kind of sharing an apartment with a few roommates. In contrast, having a VPC is like having your own private condominium; no one else has the key, and no one can enter the space without your permission.

VPC's logical isolation is implemented by using virtual network functions and security features that give the enterprise customer granular control over which IP addresses or applications can access particular resources. It is analogous to the "friends-only" or "public/private" controls on social media accounts used to restrict who can or can't see your otherwise public posts.

With IBM Cloud VPC, you can use the UI, CLI, and API to manually provision virtual server instances for VPC with high network performance. VPC infrastructure contains various Infrastructure-as-a-Service (IaaS) offerings including virtual servers for VPC.

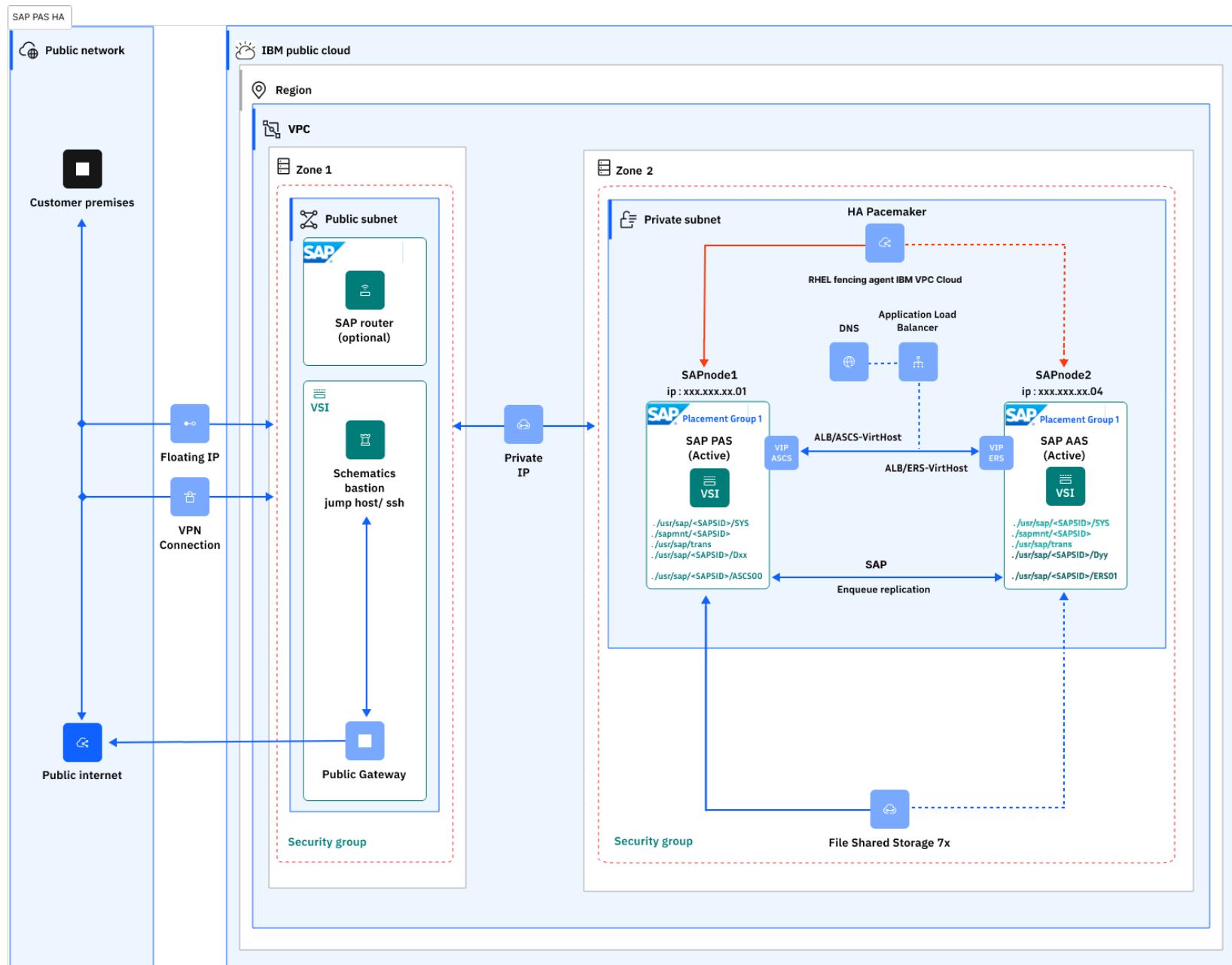
Use the following information to understand a simple use-case for planning, creating, and configuring resources for your VPC, and learn more about VPC overviews and VPC tutorials. For more information about the VPC, see [Getting started with Virtual Private Cloud \(VPC\)](#).

SAP products architecture on IBM Cloud VPC

A [Virtual Private Cloud \(VPC\)](#) contains one of the most secure and reliable cloud environments for SAP applications within your own VPC with virtual server instances. This represents an Infrastructure-as-a-Service (IaaS){: external} within IBM Cloud that offers all the benefits of isolated, secure, and flexible virtual cloud infrastructure from IBM. In comparison, the IBM Cloud classic infrastructure virtual servers offering uses virtual instances with native and VLAN networking to communicate with each other within a data center; however, the instances are restricted in one well-working pod by using subnet and VLAN networking as a gap scale up of virtual resources should rely between the pods. The IBM Cloud VPC network orchestrator layer concept eliminates the pod boundaries and restrictions, so this new concept handles all the networking for every virtual instance running within VPC across regions and zones.

Highly available system for SAP NetWeaver on IBM Cloud VPC

In a Highly Available (HA) system, every instance can run on a separate IBM Cloud virtual server instance. The cluster HA configuration for the SAP application server consists of two virtual server instances, each of them located in the same zone within the region by using placement groups. Placement groups assure that both cluster resources and cloud resources are also located in different compute nodes as specified in the following placement groups section:



SAP HA for SAP applications cluster nodes PAS (Active) and AAS (Active)

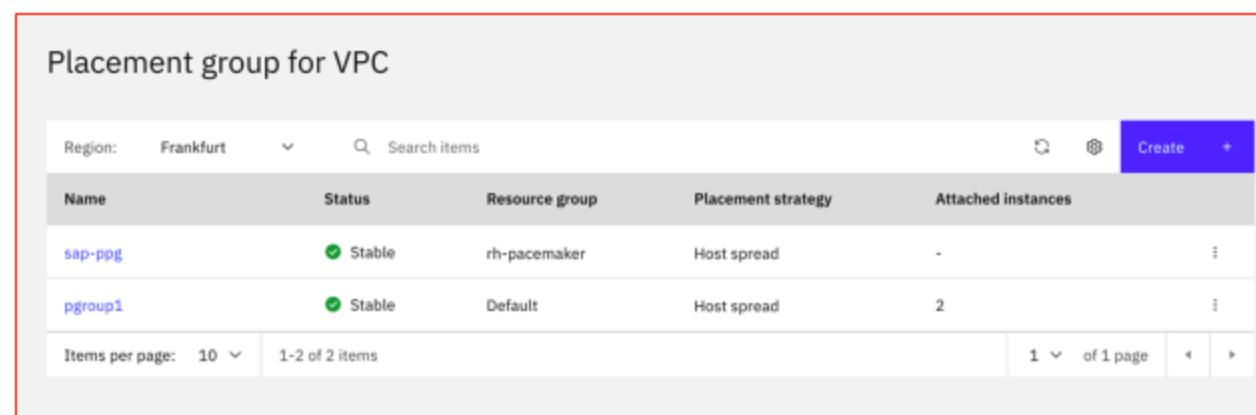
Placement groups on IBM Cloud VPC for SAP HA architecture

Placement Groups (PG) for VPC have two different anti-affinity strategies for high availability. By using the placement strategies, you minimize the chance of service disruption with virtual server instances that are placed on different hosts or into an infrastructure with separate power and network supplies.

The design of placement groups for IBM Cloud virtual servers solves this issue. Placement groups give a measure of control over the host on which a new public virtual server is placed. In this release, a “spread” rule is implemented, which means that the virtual servers within a placement group are spread onto different hosts. You can build a highly available application within a data center and know that your virtual servers are isolated from each other.

Placement groups with the spread rule are available to create in selected IBM Cloud data centers. After a spread rule is created, you can provision a virtual server into that group and ensure that it is not on the same host as any of your other virtual servers. This feature comes with no cost.

You can create your placement group and assign up to four new virtual server instances. With the spread rule, each of your virtual servers are provisioned on different physical hosts. In the following configuration example, the “Power Spread” option is used:



Placement groups host spread

Placement group for VPC					
Name	Status	Resource group	Placement strategy	Attached instances	
sapha-poc	Stable	wes-ic4sap-resourcegroup	Power spread	4	⋮
Items per page: 10 1 item 1 of 1 page ⋮					

Placement groups power spread

Following are the SAP instances that are required for HA scenario:

- ABAP SAP Central Services (ASCS) instance - contains the ABAP message server and the ABAP enqueue server.
- Enqueue Replication Server (ERS) instance for the ASCS instance.
- Database instance
- Primary Application Server (PAS) instance on node 1.
- Additional Application Server (AAS) instance on node 2.



Note: It is recommended to run both the ASCS instance and the ERS instance in a switchover cluster infrastructure.

IBM Cloud File Storage for VPC for SAP HA architecture

[IBM Cloud File Storage for VPC](#) technology is used to make the SAP directories available to the SAP system. The technologies of choice are NFS, shared disks, and cluster file system. If you have decided to use the HA solution for your SAP system, make sure that you properly address the HA requirements of the SAP file systems in your SAP environment.

File shares for VPC								
Name	Status	Resource groups	Location	Mount targets	Size	Replication role	Encryption type	
usrsap-as1-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	⋮
usrsap-as2-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	⋮
usrsap-sapsacs-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	⋮
usrsap-sapers-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	⋮
usrsap-sapmnt-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	⋮
usrsap-sapsys-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	⋮
usrsap-trans-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	80 GB	None	Provider managed	⋮

File shares for VPC

- File shares that are mounted as NFS permanent file systems on both cluster nodes for SAP HA application:
 - `/usr/sap/<SAPSID>/SYS`
 - `/sapmnt<SAPSID>`
 - `/usr/sap/trans`
- Cluster-managed file systems for SAP HA application: ASCS
 - `/usr/sap/<SAPSID>/ASCS00`
 - `/usr/sap/<SAPSID>/ERS01`
- Permanent NFS mount on SAP HA application node 1 PAS instance:
 - `/usr/sap/<SAPSID>/Dxx`
- Permanent NFS mount on SAP HA application node 2 dialog instance:
 - `/usr/sap/<SAPSID>/Dyy`

Prerequisites

You need to install the hardware (hosts, disks, and network) and decide how to distribute the database, SAP instances, and if required, the Network File System (NFS) server over the cluster nodes.

Context

Following are the types of SAP directories:

- Physically shared directories: `/<sapmnt>/<SAPSID>` and `/usr/sap/trans`

- Logically shared directories that are bound to a node, such as `/usr/sap`, with the following local directories:
 - `/usr/sap/<SAPSID>`
 - `/usr/sap/<SAPSID>/SYS`
 - `/usr/sap/hostctrl`
- Local directories that contain the SAP instances such as `/usr/sap/<SAPSID>/ASCS<Instance_Number>`
- The global transport directory may reside on a separate SAP transport host as a standard three systems transport layer configuration.

You need at least two nodes and a shared file system for distributed ASCS and ERS instances. The assumption is that the rest of the components are distributed on other nodes.

ASCS and ERS installation

In order for the ASCS and ERS instances to be able to move from one node to the other, they need to be installed on a shared file system and use virtual hostnames based on the virtual IP.

In this VPC-based SAP HA solution, the shared file system that is required by the cluster is replaced by the NFS-mounted file storage, and the virtual IP is replaced by the Application Load Balancer for VPC (ALB).

In this scenario, three ALBs are used, one for each Single Point of Failure (SPOF) component in order to replace the virtual IP requirement: ALB for ASCS, ALB for ERS, and ALB for ASE Sybase. Each ALB is configured as a backend for the corresponding cluster servers and redirects all of the communication that is received on the front-end ports to the active server in the backend pool.

Load balancers for VPC						
Region:	Frankfurt	▼	<input type="text"/> poc	X		
Name	Status	Family	Resource group	Type	Hostname	Location
db-alb-hana-poc	Active	Application	wes-ic4sap-resourcegroup	Private	20bdd130-eu-de.lb.appdomain.cloud	Frankfurt
sap-alb-ers-poc	Active	Application	wes-ic4sap-resourcegroup	Private	3941d983-eu-de.lb.appdomain.cloud	Frankfurt
sap-alb-ascs-poc	Active	Application	wes-ic4sap-resourcegroup	Private	56a9190d-eu-de.lb.appdomain.cloud	Frankfurt

Application load balancer management of HA IPs mechanism

Private application load balancer

A [private application load balancer](#) is accessible through your private subnets that you configured to create the load balancer.

Similar to a public application load balancer, your private application load balancer service instance is assigned an FQDN; however, this domain name is registered with one or more private IP addresses.

IBM Cloud operations change the number and value of your assigned private IP addresses over time, based on maintenance and scaling activities. The backend virtual server instances that host your application must run in the same region and under the same VPC.

Use the assigned ALB FQDN to send traffic to the private application load balancer to avoid connectivity problems to your applications during system maintenance or scaling down activities.

Each ALB sends traffic to the cluster node where the application (ASCS, ERS, ASE Sybase DB) is running. During the cluster failover, the ALB redirects all the traffic to the new node where the resources are up and running.



Note: DNS-as-a-Service (DNSaaS) is the management IBM Cloud VPC DNS service of HA and FQDN (IPs) mechanism.



Note: The ALB has a default of 50 seconds for client and server timeout, so after 50 seconds of inactivity, the connection is closed. To support SAP connections through ALB and not lose connection after 50 seconds, you need to request a change this value to a minimum of 300 seconds (client-side idle connection = minimum 300s and server-side idle connection = minimum 300s). To request this change, open a support ticket. This is an account-wide change that affects all of the ALBs in your account. For more information, see [Connection timeouts](#).

DNS Services with VPC

[IBM Cloud DNS Services](#) provide private DNS to VPC users. Private DNS zones are resolvable only on IBM Cloud and from explicitly [permitted networks](#) in an account. To get started, create a DNS Services instance by using the IBM Cloud console.

DNS Services allows you to:

- Create the private DNS zones that are collections for holding the domain names.
- Create the DNS resource records under these DNS zones.
- Specify the access controls used for the DNS resolution of resource records on a zone-wide level.

DNS Services also maintains its own worldwide set of DNS resolvers. Instances that are provisioned under IBM Cloud on an IBM Cloud network can use resource records that are configured through IBM Cloud DNS Services by querying DNS Services resolvers.

Resource records and zones that are configured through DNS Services are:

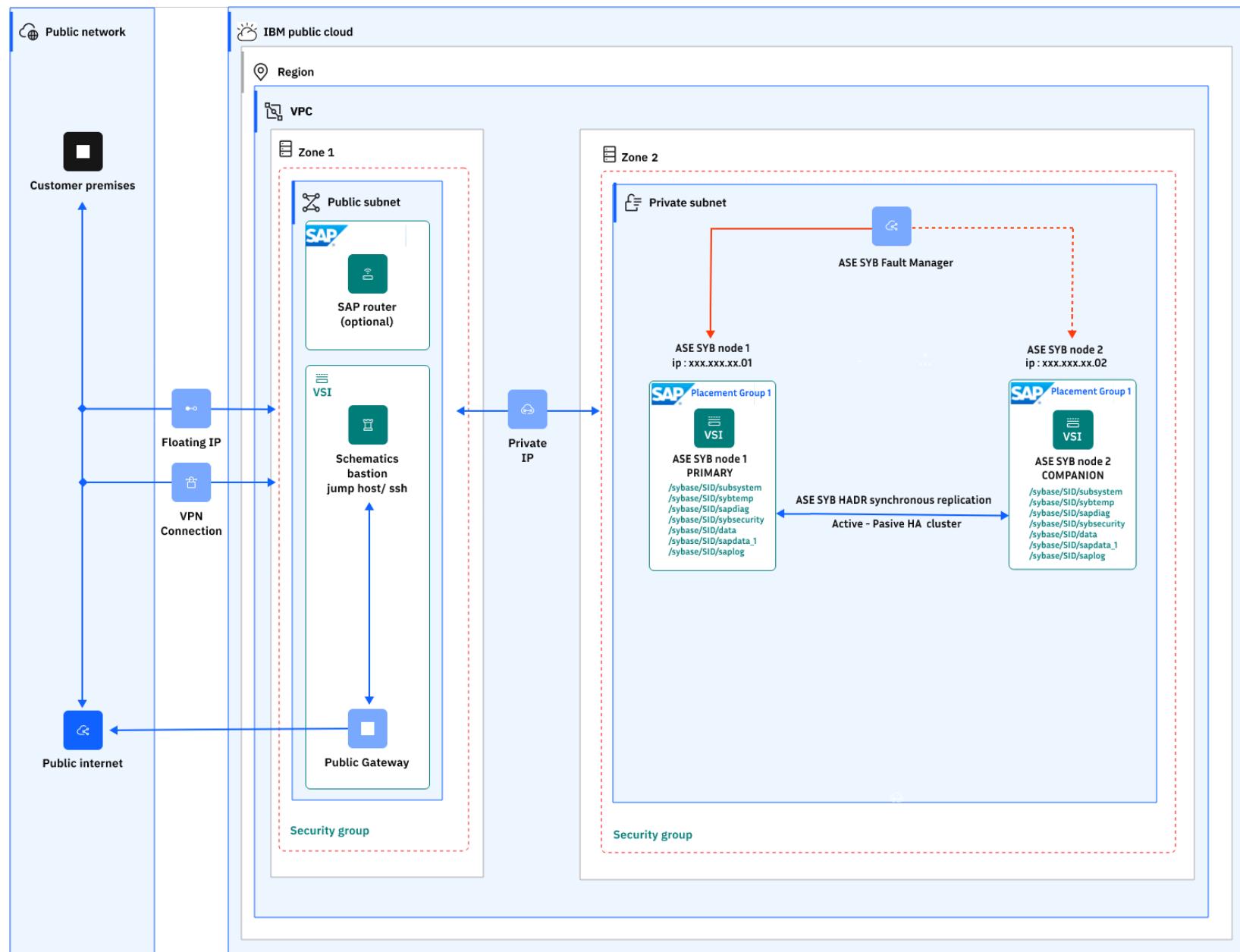
- Separated from the wider public DNS, and their publicly accessible records.
- Hidden from the system outside of and not part of the IBM Cloud private network.
- Accessible only from the system that you authorize on the IBM Cloud private network.
- Resolvable only via the resolvers provided by the service.

The DNS service maps the FQDN of each ALB to the virtual hostnames of the ASCS, ERS, and ASE Sybase that are used by SAP applications.

Type	Name	Value	TTL
CNAME	dbpochana	is an alias of 20bdd130-eu-de.lb.appdomain.cloud	12 hr
CNAME	sappocers	is an alias of 3941d983-eu-de.lb.appdomain.cloud	12 hr
CNAME	sappocases	is an alias of 56a9190d-eu-de.lb.appdomain.cloud	12 hr

DNS records

Highly available system for SAP ASE Sybase database with HADR system



SAP HA for ASE Sybase DB instances cluster nodes primary (Active) and Secondary (Companion)

At the most basic level, a standard HA ASE Sybase cluster in an active(primary)-passive(companion) configuration has two nodes: one is the primary node and the other is the standby node. This means that the primary node is actively serving the active SAP DB instances (Primary and Companion), while the standby node is waiting to jump in if there is any failure.

The cluster is set with a virtual hostname IP (hostname is mapped to the FQDN of the ASE Sybase ALB through DNS, which is the same as

explained previously for SAP ASCS and ERS instances). Application instances (PAS and AAS) are used on the SAP profiles to call that particular component. The cluster assigns the virtual IP to the active node and uses a heartbeat monitor to confirm the availability of the components. If the primary node stops responding, it triggers the automatic failover mechanism that calls the standby node to step up to become the primary node. The ALB detects the change, redirects the traffic to the new active node, and assigns the virtual IP to it, restoring the component availability. Once fixed, the failed node comes online as a standby node.

SAP Sybase HADR system supports synchronous replication

The SAP Sybase HADR system supports synchronous replication between the primary and standby servers for high availability. An active-active setup is a two-node configuration where both nodes in the cluster include SAP ASE managing independent workloads, capable of taking over each others workload in the event of a failure.

The SAP ASE server that takes over the workload is called a secondary companion, and the SAP ASE server that fails is called the primary companion. Together they are companion servers. This movement from one node to another is called failover. After the primary companion is ready to resume its workload, it is moved back to its original node. This movement is called a failback.

When a system fails over, clients that are connected to the primary companion and use the failover property automatically reestablish their network connections to the secondary companion. You must tune your operating system to successfully manage both servers during fail over. See your operating system documentation for information about configuring your system for high availability. An SAP ASE configured for failover in an active-active setup can be shut down using the shutdown command only after you have suspended SAP ASE from the companion configuration, at both the server level and the platform level.

The always-on option in a High Availability and Disaster Recovery (HADR) system consists of two SAP ASE servers:

- Primary on which all transaction processing takes place.
- Warm standby (referred to as a "standby server" in DR mode, and as a "companion" in HA mode) for the primary server, and contains copies of designated databases from the primary server.



Note: The HADR feature that is shipped with SAP ASE version 16.0 SP02 supports only a single-companion server.

Some high-availability solutions (for example, the SAP Adaptive Server Enterprise Cluster Edition) share or use common resources between nodes. However, the HADR system is a "shared nothing" configuration, each node has separate resources including disks.

In an HADR system, servers are separate entities and data is replicated from the primary server to the companion server. If the primary server fails, a companion server is promoted to the role of primary server either manually or automatically. Once the promotion is complete, clients can reconnect to the new primary server, and see all committed data, including data that was committed on the previous primary server.

Servers can be separated geographically, which makes an HADR system capable of withstanding the loss of an entire computing facility.



Note: The HADR system includes an embedded SAP Replication Server, which synchronizes the databases between the primary and companion servers. SAP ASE uses the Replication Management Agent (RMA) to communicate with Replication Server and SAP Replication Server uses Open Client connectivity to communicate with the companion SAP ASE.

The Replication Agent detects any data changes made on the primary server and sends them to the primary SAP Replication Server. In the figure above, the unidirectional arrows indicate that, although both SAP Replication Servers are configured, only one direction is enabled at a time.

The HADR system supports synchronous replication between the primary and standby servers for high availability so the two servers can keep in sync with Zero Data Loss (ZDL). This requires a network link that is fast enough between the primary and standby server so that synchronous replication can keep up with the primary servers workload. Generally, this means that the network latency is approximately the same speed as the local disk IO speed, a few (fewer than 10) milliseconds. Anything longer than a few milliseconds may result in a slower response to write operations at the primary.

The HADR system supports asynchronous replication between the primary and standby servers for disaster recovery. The primary and standby servers by using asynchronous replication can be geographically distant, meaning they can have a slower network link. With asynchronous replication, Replication Agent Thread captures the primary servers workload, which is delivered asynchronously to SAP Replication Server. The SAP Replication Server applies these workload change to the companion server.

The most fundamental service that is offered by the HADR system is the failover; planned or unplanned from the primary to the companion server, which allows maintenance activity to occur on the old primary server, while applications continue on the new primary.

The HADR system provides protection in the event of a disaster. If the primary server is lost, the companion server can be used as a replacement. Client applications can switch to the companion server, and the companion server is quickly available for users. If the SAP Replication Server was in synchronous mode before the failure of the primary server, the Fault Manager automatically initiates failover with

zero data loss.

Fault Manager installation on the SAP ASCS node

The required parameters are asked during the installation process to create a profile for the fault manager and then adds it to the instance start profile. It is also possible to run the installation by using an existing profile: `sybdbfm install pf=<SYBHA.PFL>` In this case, the installation process will only ask for profile parameters missing in the profile.



Note: Fault manger is integrated with ASCS on same SAP PAS/AAS cluster (start/stop/move together).

There may be some data loss if the SAP Replication Server was in asynchronous mode and you must use manual intervention to failover for disaster recovery.

Connection attempts to the companion server without the necessary privileges are silently redirected to the primary companion via the login redirection mechanism, which is supported by Connectivity libraries. If login redirection is not enabled, client connections fail and are disconnected.

The SAP ASE HADR option installs the below components:

- SAP ASE
- SAP Replication Server
- Replication Management Agent (RMA)
- SAP Host Agent
- Fault Manager
- SAP ASE Cockpit



Note: This automation is offered at no cost; however, the provisioned infrastructure comes at cost.

Implementing high availability for SAP applications on IBM Power Virtual Server References

The following is a comprehensive list of product documentation, Red Hat Knowledge Base articles, and SAP notes that you need to review before you implement high availability for SAP solutions. A Red Hat Customer Portal ID is required to access Knowledge Base articles and an SAP User ID is required to access SAP Notes.

General requirements

- An [IBM Cloud](#) account
- An [SAP for Me](#) account
- A [Red Hat Customer Portal](#) account

A valid *RHEL for SAP Applications* or *RHEL for SAP Solutions* subscription is required to enable the repositories that you need to install SAP HANA and the resource agents for HA configurations.

Red Hat Enterprise Linux Cluster product documentation

Product Documentation

[Configuring and managing high availability clusters](#)

RHEL 8 cluster documentation

Product Documentation

[Configuring and managing high availability clusters](#)

RHEL 9 cluster documentation

Red Hat Enterprise Linux for SAP Solutions product documentation

Product Documentation

[Configuring RHEL 8 for SAP HANA2 installation](#)

[Red Hat HA Solutions for SAP HANA, S/4HANA, and NetWeaver based SAP Applications](#)

[Automating SAP HANA Scale-Up System Replication by using the RHEL HA Add-On](#)

[Configuring a Cost-Optimized SAP S/4HANA HA cluster \(HANA System Replication + ENSA2\) by using the RHEL HA Add-On](#)

[Configuring SAP HANA Scale-Up Multitarget System Replication for disaster recovery](#)

[Configuring an Active-Passive NFS server in a Red Hat High Availability cluster](#)

RHEL 8 for SAP documentation

Product Documentation

[Installing RHEL 9 for SAP Solutions](#)

[Red Hat HA Solutions for SAP HANA, S/4HANA, and NetWeaver based SAP Applications](#)

[Automating SAP HANA Scale-Up System Replication by using the RHEL HA Add-On](#)

[Configuring SAP HANA Scale-Up Multitarget System Replication for disaster recovery](#)

[Configuring HA clusters to manage SAP NetWeaver or SAP S/4HANA Application server instances by using the RHEL HA Add-On](#)

RHEL 9 for SAP documentation

Red Hat Enterprise Linux general cluster knowledge base articles

- [Support Policies for RHEL High Availability Clusters](#)
- [Support Policies for RHEL High Availability Clusters - General Requirements for Fencing/STONITH](#)
- [Support Policies for RHEL High Availability Clusters - IBM Power Systems Virtual Server \(PowerVS\) Virtual Machines as Cluster Members](#)
- [Available Fencing Types and Fencing Agents for a Red Hat High-Availability Cluster](#)
- [Configuring a RHEL HA Cluster Fence Agent for an IBM Power Virtual Server](#)
- [How to configure HA-LVM Cluster by using system_id in RHEL 8 and above](#)

Red Hat Enterprise Linux for SAP cluster knowledge base articles

- [Support Policies for RHEL High Availability Clusters - Management of SAP HANA in a Cluster](#)
- [Automating SAP HANA Scale-Up System Replication by using the RHEL HA Add-On](#)
- [Support Policies for RHEL High Availability Clusters - Management of SAP S/4HANA in a cluster](#)
- [Configuring SAP S/4HANA ASCS/ERS with Standalone Enqueue Server 2 \(ENSA2\) in Pacemaker](#)
- [The Systemd-Based SAP Startup Framework](#)
- [Pacemaker cluster does not trigger a takeover of HANA System Replication when the `hdbindexserver` process of the primary HANA instance hangs/crashes](#)

SAP HANA product documentation

- [SAP HANA Server Installation and Update Guide](#)
- [SAP HANA Administration Guide](#)
- [SAP HANA System Replication](#)
- [SAP HANA System Replication - Active/Active \(Read Enabled\)](#)
- [SAP HANA SQL and System Views Reference Guide](#)
- [Implementing a HA/DR Provider](#)

SAP Notes

SAP Notes

[SAP Note 2772999 - Red Hat Enterprise Linux 8.x: Installation and Configuration](#)

[SAP Note 2235581 - SAP HANA: Supported Operating Systems](#)

[SAP Note 2777782 - SAP HANA DB: Recommended OS Settings for RHEL 8](#)

[SAP Note 2369981 - Required configuration steps for authentication with HANA System Replication](#)

[SAP note 3115048 - sapstartsrv with native Linux systemd support](#)

[SAP note 3139184 - Linux: systemd integration for sapstartsrv and SAP Host Agent](#)

SAP Notes for RHEL 8

SAP Notes

[SAP Note 3108316 - Red Hat Enterprise Linux 9.x: Installation and Configuration](#)

[SAP Note 2235581 - SAP HANA: Supported Operating Systems](#)

[SAP Note 3108302 - SAP HANA DB: Recommended OS Settings for RHEL 9](#)

[SAP Note 2369981 - Required configuration steps for authentication with HANA System Replication](#)

[SAP note 3115048 - sapstartsrv with native Linux systemd support](#)

[SAP note 3139184 - Linux: systemd integration for sapstartsrv and SAP Host Agent](#)

SAP Notes for RHEL 9

Creating instances for a high availability cluster

Use the following information and procedures to create the Power Virtual Server instances that are required for a high availability cluster implementation.

Before you begin

Review the general requirements, product documentation, support articles, and SAP notes listed in [Implementing high availability for SAP applications on IBM Power Virtual Server References](#).

Creating a workspace

A workspace is an environment that acts as a folder for all Power Virtual Server resources in a geographical region. These resources include compute, network, and storage volumes. Resources cannot be moved or shared between different workspaces. Each workspace is bound to a single data center.

To create a workspace, follow the steps that are described in [Creating a Power Virtual Server workspace](#).

The created workspaces are listed under **Workspaces** on the left navigation pane of the Power Virtual Server user interface.

Creating private network subnets

A virtual server instance is connected to the network and is assigned an IP address from the defined range of IP addresses. It is recommended that you connect the cluster nodes to a private network rather than a public network.

Follow the steps in [Configuring a private network subnet](#) to create a subnet.



Note: You need at least one private subnet in the workspace.

Reserving virtual IP addresses

A high availability cluster typically requires *virtual IP addresses* that must move with the application in a failover scenario.

Reserve the required IP addresses in the subnet to prevent Power Virtual Server from assigning a specific IP address to another virtual server instance. See [Reserving IP addresses](#).



Note: Make sure that the IP address you want to reserve is within the CIDR range of the subnet and within the *IP range* that you previously restricted.

Exploring more network architecture options

If your Power Virtual Server *workspace* is enabled for *Power Edge Router* (PER), you already have network communication with parts of the IBM Cloud network. The PER solution creates a direct connection to the IBM Cloud Multi Protocol Label Switching (MPLS) backbone, making it easier for different parts of the IBM network to communicate with each other. For more information, see [Getting started with the Power Edge Router](#).

Otherwise, create IBM Cloud® connections to connect your Power Virtual Server instances to other IBM Cloud resources within your account. IBM Cloud connections are not required to configure a high availability cluster in Power Virtual Server. They might be required for integration scenarios with the IBM Cloud Classic network and Virtual Private Cloud (VPC) infrastructures. For more information, see [IBM Power Virtual Server Cloud Connections](#).

Use IBM Transit Gateway to connect your Power Virtual Server to IBM Cloud classic and Virtual Private Cloud (VPC) infrastructures outside your account or region. For more information about integrating the on-premises network and Power Virtual Server, see [Network architecture diagrams](#).

Creating an SSH key

Use the following steps to create one or more SSH keys for root login.

Create a keypair and load the public key to the SSH keys store in Power Virtual Server. During deployment of the virtual server instance, specify one or more keys from the keystore. These keys are added to the `authorized_keys` file of the root user, and allow you to securely log in to the virtual server instance by using your private key.

For more information, see [Generating an SSH key](#).



Tip: The preferred choice is the *ed25519* key type. It offers both security and performance advantages.

1. Log in to [Workspaces](#).
2. Click the **workspace** name and **View virtual servers**.
3. Click [SSH keys](#).
4. Click **Create SSH key**.
5. Enter a **Key name**. Then, copy and paste the **public key** that you generated earlier into the field.
6. Click **Add SSH key**.

Selecting a boot image

You have several options to obtain operating system images for the cluster nodes. Use the following steps to select a boot image.

You can choose from several types of stock images that are already prepared for Power Virtual Server. Images are available in the *IBM Provided Subscription* and *Client Provided Subscription* sections of the Power Virtual Server provisioning page. For more information, see [Full Linux® subscription for IBM Power Virtual Server \(Off-premises\)](#).

If you want to import a custom Linux image, you must first upload the image to the IBM Cloud Object Storage in OVA format.

- [Importing a boot image](#)
- [Deploying a custom image within IBM Power Virtual Server](#)

Before you begin, make sure that the OVA image is loaded in the storage bucket.

Creating virtual server instances for the cluster

Complete the following steps to create the virtual server instances that you want to use as high availability cluster nodes.

1. Log in to [Workspaces](#).
2. Click the **workspace** name and **View virtual servers**.
3. Click **Virtual server instances > Create Instance**. You need to step through the subsections **General, Boot Image, Profile, Storage Volume, Network Interfaces**.
4. In subsection **General**, enter the **Instance name**.
5. For a singlezone implementation, click **+** to increase the **Number of instances** to 2. Select **Numerical postfix** as *Instance naming convention*, and select **Different server** as *Placement group colocation policy*. A placement group with colocation policy *Different server* is automatically created as part of the virtual server instances deployment.
6. Select an **SSH key** and click **Continue**.
7. In the **Boot image** section, select the **Operating system** according to your subscription model. Use one of the Linux selections either from the *IBM-provided subscription* or through your *Client-provided subscription*. In the **Tier* section, select the desired storage tier. Keep **Auto-select pool** for selecting the *Storage Pool*. Click **Continue**.
8. In **Profile**, select **Machine type, Core type**, and the virtual server instance **profile** to match your workload requirements. Click **Continue**.
9. In **Storage volumes**, click **Continue**.

! **Important:** When you deploy multiple instances, the storage volumes that are created are shared by all instances. Certain high availability cluster scenarios require shared volumes. In these cases, create the shared volumes later. For SAP HANA, see [Storage configuration for SAP HANA](#). These volumes must be created later for the individual server instances after their deployment is complete.

10. In the **Network Interfaces** subsection, it is preferable that the cluster nodes are not directly accessible from a public network, so leave the *Public networks* configuration as **Off**.
11. Click **Attach** to attach the virtual server instances to an existing subnet.
12. In the *Attach an existing network* screen, select one of the *Existing networks*. You can either select **Automatically assign IP address from IP range**, or **Manually specify an IP address from IP range** to specify an available IP address.
13. Click **Attach**.
14. Click **Finish**, check the *I agree to the Terms and Conditions* flag, and click **Create**.

The deployment of the virtual server instances starts.

For a multizone region deployment, repeat the same steps to create the second virtual server instance in a different workspace.

Preparing the operating system for installing an SAP solution

If you deployed a virtual server instance from a stock image, you need to perform extra configuration tasks before you can install SAP software. For more information, see [Configuring a Power Virtual Server instance](#).

Creating a Custom Role, Service ID, and API key in IBM Cloud

A *Service ID* in IBM Cloud identifies a service or an application in a similar way as a user ID identifies a user. Create a *service ID* for the fencing agent to allow access to IBM Power Cloud actions such as monitoring or controlling the virtual server instances. Create a custom role in advance to limit the allowed IBM Power Cloud API actions to only those actions that are required for fencing.

Managing *Custom Roles, Service IDs, and API keys* are part of IBM Cloud Identity and Access Management (IAM). Navigate to the IAM for the following steps.

Log in to IBM Cloud Identity and Access Management

Go to the IBM Cloud Identity and Access Management (IAM) console.

1. Log on to [IBM Cloud](#).
2. On the menu bar, click **Manage** and select **Access (IAM)**.

Creating a custom role for the fencing agent

Create a *custom role* in IAM and assign the set of actions that are required for a fencing operation to the role. You must grant access for the following actions.

- reading objects in the *cloud_instance* or *workspace*
- listing virtual server instances
- getting information about a virtual server instance
- performing an action on a virtual server instance



Note: The action set of a custom role must be unique within the account. You cannot create multiple custom roles with the same action set.

Create a **custom role** in IAM.

1. Click **Roles > Create**.
2. Enter the **Name**, **ID**, and **Description** for the custom role.
3. Select *Workspace for Power Virtual Server* from the **Service** drop-down list.
4. Select *Manager* from the **View the actions for** drop-down list.
5. In the **Actions** list, locate the following actions. Click **Add** for each of them.
 - power-iaas.pvm-instance.list
 - power-iaas.pvm-instance.read
 - power-iaas.pvm-instance.action
6. Click **Create** to save the role.

Creating a custom role for the `powervs-subnet` resource agent



Note: This step is only required if you are implementing a cluster in a multizone region environment with the `powervs-subnet` resource agent.

Create a *custom role* in IAM and assign the set of actions that are required for a `subnet move` operation in the role. You must grant access for the following actions.

- reading objects in the *cloud_instance* or *workspace*
- listing and getting information for subnets in the *workspace*
- creating and deleting subnets in the *workspace*
- attaching and detaching subnets to or from a virtual server instance
- deleting network ports

Create a **custom role** in IAM.

1. Click **Roles > Create**.
2. Enter the **Name**, **ID**, and **Description** for the custom role.
3. Select *Workspace for Power Virtual Server* in the **Service** drop-down list.
4. Select *Manager* from the **View the actions for** drop-down list.
5. In the **Actions** list, locate the following actions. Click **Add** for each of them.
 - power-iaas.cloud-instance.read
 - power-iaas.pvm-instance-network.list
 - power-iaas.pvm-instance-network.read
 - power-iaas.network.list
 - power-iaas.network.create
 - power-iaas.network.delete
 - power-iaas.network-port.delete
 - power-iaas.pvm-instance-network.create
 - power-iaas.pvm-instance-network.delete
6. Click **Create** to save the role.

Creating a Service ID

Create a *Service ID* for the fencing agent and assign one or more custom roles to it. In a multizone region implementation, you can create a second *Service ID* for the `powervs-subnet` resource agent. It is also possible to use a common Service ID for both agents (see the note in the previous section). If you are using a common Service ID, assign both the custom role for fencing and the custom role for the `powervs-subnet` resource agent.

Create a **Service ID** in IAM.

1. Click **Service IDs > Create**.
2. Enter a **Name** and **Description** for the service ID.
3. Click **Create**.
4. In the *Access policies* section, click **Assign access**.
5. In the *Service* section, select **Workspace for Power Virtual Server** and click **Next**.
6. In the *Resource* section, select **Specific Resources > Service Instance > string equals > name of the workspace that you created earlier**. Click **Next**.
7. In the *Roles and actions* section, select one or more of the custom roles that you created earlier in **Custom access** and click **next**.
8. You can skip the *Conditions (Optional)* section.
9. Click **Add** and then **Assign** to create the *Service ID*.



Important: If you create a *Service ID* for the `powervs-subnet` resource agent in a multizone region implementation, you must grant access to both workspace resources. In the *Access policies* section, click **Assign access** again and follow the steps to assign access for the second workspace.

Creating an API key for the Service ID

When you configure the *fencing agent* in a high availability cluster or the *powervs-subnet* resource agent in a multizone region implementation, you must specify an *API key*. The *API key* authorizes the fencing agent or resource agent to use the IBM Power Cloud API to perform the actions that are defined in the *Service ID*.

Create the **API Key** for the **Service ID** in the IAM.

1. Click **Service IDs** and select the *Service ID* that you created earlier.
2. Click **API Keys** to switch to the *Create and manage API keys for this service ID* tab.
3. Click **Create**.
4. Enter a **Name** and a **Description** for the key.
5. Click **Create**.

Click download to save the API key to a JSON file. Keep the downloaded file in a safe place.



Important: The key is available for 300 seconds. After 300 seconds, you won't be able to view or retrieve the key.

Collecting parameters for configuring a high availability cluster

Several parameters are required to set up a specific high availability scenario. These include the following parameters, which can be collected now.

- *Cloud Resource Name (CRN)* of the Power Virtual Server workspace
- Virtual server *instance IDs*
- Extra parameters that must be derived from the *CRN*
- API key for the *fencing agent*
- API key for the *powervs-subnet* resource agent if you are implementing a multizone region environment

The uppercase variables in the following section indicate that these parameters are used as environment variables to simplify the cluster setup. Make a note of their contents now, as they will be needed in the setup instructions for a specific high availability scenario.

1. `CLOUD_REGION` contains the geographical area of your virtual server instance and is used to target the correct [Power Cloud API endpoint](#).

`CLOUD_REGION` if you are using public endpoints

Public endpoint URLs match the pattern `https://<CLOUD_REGION>.power-iaas.cloud.ibm.com`. For `CLOUD_REGION`, note the first word in the hostname in the public endpoint URL of the specific location. For example, sites `syd04` and `syd05` map to `syd`.

`CLOUD_REGION` if you are using private endpoints

Private endpoint URLs match the pattern `https://private.<CLOUD_REGION>.power-iaas.cloud.ibm.com`. For `CLOUD_REGION`, note the second word in the hostname in the private endpoint URL of the specific location. For example, sites `syd04` and `syd05` map to `au-syd`.

2. Log in to [Workspaces - Power Virtual Server](#). The list contains the name and CRN of the workspaces.

Locate your **Workspace**, or both workspaces for a multizone region deployment. Click **Copy** next to the CRN and paste it into a temporary document.

A CRN has multiple sections that are divided by a colon. The base format of a CRN is:

`crn:version:cname:ctype:service-name:location:scope:service-instance:resource-type:resource`

service-name

The fifth field of the CRN of the workspace is always `power-iaas`, the **service-name**.

location

The sixth field is the **location** that needs to be mapped to a region.

scope

The seventh field is the **Tenant ID**.

service-instance

The eighth field is the **Cloud Instance ID** or **GUID**.

3. `IBMCLOUD_CRN_1` contains the full *CRN*.

4. `GUID_1` refers to the contents of the *service-instance* field in the *CRN*.

5. In a multizone region deployment, use the *CRN* of the second workspace and note the contents for `IBM_CLOUD_CRN_2` and `GUID_2`.

6. Click the workspace name and then **View virtual servers**. Click the virtual server instance names and find their **ID**.

7. Note these IDs for `POWERVSI_1` and `POWERVSI_2`. In a multizone deployment, use the second workspace to find the ID of the second instance.

8. `APIKEY` contains the API key for the fencing agent. Use the value of the `apikey` entry in the JSON file that was downloaded in the [Creating an API key for the Service ID](#) section.

In a multizone region deployment, an API key is also required for the `powervs-subnet` cluster resource agent. As before, you can use the value of the `apikey` entry for the `APIKEY` variable. However, the preferred option is to place a copy of the downloaded JSON file on both nodes and set `APIKEY` to a string that starts with a `@` sign followed by the full path to the key file.

Implementing a RHEL HA Add-On cluster for SAP solutions

Implementing a Red Hat Enterprise Linux High Availability Add-On cluster

Use the following information and procedures to implement a Red Hat Enterprise Linux (RHEL) High Availability Add-On cluster. The cluster uses instances in [IBM® Power® Virtual Server](#) as cluster nodes.

The information describes how to transform the individual virtual server instances into a cluster.

These procedures include installing the high availability packages and agents on each cluster node and configuring the fencing devices.



Note: This information is intended for architects and specialists who are planning a high availability deployment of SAP applications on

Before you begin

Review the general requirements, product documentation, support articles, and SAP notes listed in [Implementing high availability for SAP applications on IBM Power Virtual Server References](#).

Creating virtual server instances for the cluster

Use the instructions in [Creating instances for a high availability cluster](#) to create the virtual server instances that you want to use as cluster nodes.

Preparing the nodes for RHEL HA Add-On installation

The following section describes basic preparation steps on the cluster nodes. Make sure that you follow the steps on both nodes.

Log in as the root user to each of the cluster nodes.

Adding cluster node entries to the hosts file

On both nodes, add the IP addresses and hostnames of both nodes to the `/etc/hosts` file.

For more information, see [Setting up /etc/hosts files on RHEL cluster nodes](#).

Preparing environment variables

To simplify the setup process, prepare some environment variables for the root user. These environment variables are used with later operating system commands in this information.

On both nodes, create a file with the following environment variables and update to your environment.

```
# General settings
export CLUSTERNAME="SAP_CLUSTER"          # Cluster name

export APIKEY=<APIKEY>                   # API Key of the IBM Cloud IAM ServiceID for the fencing agent
export CLOUD_REGION=<CLOUD_REGION>        # Workspace region
export PROXY_IP=<IP_ADDRESS>              # Proxy server IP address

# Workspace 1
export IBMCLOUD_CRN_1=<IBMCLOUD_CRN_1>    # Workspace CRN
export GUID_1=<GUID_1>                      # Workspace GUID

# Virtual server instance 1
export NODE1=<HOSTNAME_1>                  # Virtual server instance hostname
export POWERVSI_1=<POWERVSI_1>              # Virtual server instance id

# Virtual server instance 2
export NODE2=<HOSTNAME_2>                  # Virtual server instance hostname
export POWERVSI_2=<POWERVSI_2>              # Virtual server instance id
```

To find the settings for the `APIKEY`, `IBMCLOUD_CRN_1`, `GUID_1`, and `POWERVSI_?` variables, follow the steps in [Collecting parameters for configuring a high availability cluster](#).

Installing and configuring a RHEL HA Add-On cluster

Use the following steps to set up a two-node cluster for an IBM Power Virtual Server.

The instructions are based on the Red Hat product documentation and articles that are listed in [Implementing high availability for SAP applications on IBM Power Virtual Server References](#).



Tip: You need to perform some steps on both nodes and some steps on either NODE1 or on NODE2.

Installing RHEL HA Add-On software

Install the required software packages.

Checking the RHEL HA repository

Check that the RHEL High Availability repository is enabled.

On both nodes, use the following command.

```
$ dnf repolist
```

Use the following command to enable the HA repository if it is missing.

```
$ subscription-manager repos \
--enable="rhel-8-for-ppc64le-highavailability-e4s-rpms"
```

For RHEL 9, use this command.

```
$ subscription-manager repos \
--enable="rhel-9-for-ppc64le-highavailability-e4s-rpms"
```

```
$ dnf clean all
```

```
$ dnf repolist
```

Installing the RHEL HA Add-On software packages

Install the required software packages.

On both nodes, run the following command.

```
$ dnf install -y pcs pacemaker fence-agents-ibm-powervs
```

Make sure that you install the minimal version of the *fence-agents-ibm-powervs* package dependent on your Red Hat Enterprise Linux release:

RHEL 8

fence-agents-ibm-powervs-4.2.1-121.el8

RHEL 9

fence-agents-ibm-powervs-4.10.0-43.el9

Configuring a RHEL HA Add-On cluster

Configuring firewall services

Add the high availability service to the RHEL firewall if *firewalld.service* is installed and enabled.

On both nodes, run the following commands.

```
$ firewall-cmd --permanent --add-service=high-availability
```

```
$ firewall-cmd --reload
```

Starting the PCS daemon

Start the PCS daemon that is used for controlling and configuring RHEL HA Add-On clusters through PCS.

On both nodes, run the following commands.

```
$ systemctl enable --now pcsd.service
```

Make sure that the PCS service is running:

```
$ systemctl status pcsd.service
```

Setting a password for hacluster user ID

Set the password for the hacluster user ID.

On both nodes, run the following command.

```
$ passwd hacluster
```

Authenticating the cluster nodes

Use the following command to authenticate user hacluster to the PCS daemon on the nodes in the cluster. The command prompts you for the password that you set in the previous step.

On NODE1, run the following command.

```
$ pcs host auth ${NODE1} ${NODE2} -u hacluster
```

 **Tip:** If you get an error message similar to `Error: Unable to communicate with {NODE2}`, check whether you have any proxy variables set in your environment (`env | grep -i proxy`). You need to unset these variables or define a `no_proxy` variable to exclude the cluster nodes: `export no_proxy=${NODE1},${NODE2},$no_proxy`

Configuring and starting the cluster nodes

Configure the cluster configuration file and synchronize the configuration to the specified nodes.

The `--start` option also starts the cluster service on the nodes.

On NODE1, run the following command.

```
$ pcs cluster setup ${CLUSTERNAME} --start ${NODE1} ${NODE2}
```

```
$ pcs status
```

Creating the fencing device

STONITH is an acronym for "Shoot The Other Node In The Head" and protects your data from corruption in a split-brain situation.

 **Important:** You must enable STONITH (fencing) for a RHEL HA Add-On production cluster.

Fence agent `fence_ibm_powervs` is the only supported agent for a STONITH device on Power Virtual Server clusters.

The fence agent connects to the [Power Cloud API](#) by using parameters `APIKEY`, `IBMCLOUD_CRN_1`, `CLOUD_REGION`, `GUID`, and the instance IDs `POWERVSI_1` and `POWERVSI_2`.

You can test the agent invocation by using the parameters that you gathered in the [Collecting parameters for configuring a high availability cluster](#) section.

Identifying the virtual server instances for fencing

Use the `list` option of `fence_ibm_powervs` to identify and or verify the instance IDs of the two cluster nodes:

On any node, run the following command.

```
$ fence_ibm_powervs \
  --token=${APIKEY} \
  --crn=${IBMCLOUD_CRN_1} \
  --instance=${GUID_1} \
  --region=${CLOUD_REGION} \
  --api-type=public \
-o list
```

If the virtual server instances have access to only a private network, you must use the `--api-type=private` option, which also requires an extra `--proxy` option.

Example:

```
$ fence_ibm_powervs \
--token=${APIKEY} \
--crn=${IBMCLOUD_CRN_1} \
--instance=${GUID_1} \
--region=${CLOUD_REGION} \
--api-type=private \
--proxy=http://.${PROXY_IP}:3128 \
-o list
```

Continue by using `--api-type=private` in the following examples.

Checking the status of both virtual server instances

On both nodes, run the following commands.

```
$ time fence_ibm_powervs \
--token=${APIKEY} \
--crn=${IBMCLOUD_CRN_1} \
--instance=${GUID_1} \
--region=${CLOUD_REGION} \
--plug=${POWERVSI_1} \
--api-type=private \
--proxy=http://.${PROXY_IP}:3128 \
-o status
```

```
$ time fence_ibm_powervs \
--token=${APIKEY} \
--crn=${IBMCLOUD_CRN_1} \
--instance=${GUID_1} \
--region=${CLOUD_REGION} \
--plug=${POWERVSI_2} \
--api-type=private \
--proxy=http://.${PROXY_IP}:3128 \
-o status
```

The `status` action of the fence agent against a virtual server instance {pvm_instance_id} displays its power status.

On both nodes, the two commands must report `Status: ON`.

The output of the `time` command might be useful later when you choose timeouts for the STONITH device.

You can add the `-v` flag for verbose output, which shows more information about connecting to the Power Cloud API and querying virtual server power status.

Creating a stonith device

The following command shows the device-specific options for the `fence_ibm_powervs` fencing agent.

```
$ pcs stonith describe fence_ibm_powervs
```

Create the stonith device for both virtual server instances.

On NODE1, run the following command.

```
$ pcs stonith create res_fence_ibm_powervs fence_ibm_powervs \
token=${APIKEY} \
crn=${IBMCLOUD_CRN_1} \
instance=${GUID_1} \
region=${CLOUD_REGION} \
api_type=private \
proxy=http://.${PROXY_IP}:3128 \
pcmk_host_map="${NODE1}:${POWERVSI_1};${NODE2}:${POWERVSI_2}" \
```

```
pcmk_reboot_timeout=600 \
pcmk_monitor_timeout=600 \
pcmk_status_timeout=60
```

 **Important:** Although the `fence_ibm_powervs` agent uses `api-type` as an option when started from the command line, the stonith resource needs to be created by using `api_type`.

Verify the configuration with the following commands.

```
$ pcs config
```

```
$ pcs status
```

```
$ pcs stonith config
```

```
$ pcs stonith status
```

Setting the stonith-action cluster property

To speed up failover times in an IBM Power Virtual Server cluster, you can change the cluster property `stonith-action` to `off`. When the cluster performs a fencing action, it triggers a *power off* operation instead of a *reboot* for the fenced instance.

After this change, you always need to log in to the IBM Cloud Console, and manually start an instance that was fenced by the cluster.

```
$ pcs property set stonith-action=off
```

Verify the change.

```
$ pcs config
```

Testing fencing operations

To test the STONITH configuration, you need to manually fence the nodes.

On NODE1, run the following commands.

```
$ pcs stonith fence ${NODE2}
```

```
$ pcs status
```

As a result, NODE2 stops.

Activate NODE2, then start the cluster on the node and try to fence NODE1.

On NODE2, run the following commands.

```
$ pcs cluster start
```

```
$ pcs status
```

```
$ pcs stonith status
```

```
$ pcs stonith fence ${NODE1}
```

NODE1 stops.

Activate NODE1, then start the cluster on the node.

On NODE1, run the following command.

```
$ pcs cluster start
```

```
$ pcs status
```

```
$ pcs stonith status
```

Implementing a Red Hat Enterprise Linux High Availability Add-On cluster in a multizone region environment

Use the following information and procedures to implement a Red Hat Enterprise Linux (RHEL) High Availability Add-On cluster in a multizone region environment. The cluster uses instances in [IBM® Power® Virtual Server](#) as cluster nodes. The virtual server instances run in different zones in a multizone region. The setup uses the `powervs-subnet` cluster resource agent to manage the service IP address of an application in a multizone region implementation. The resource agent supports only the use of different zones in the same multizone region. Deployment across multiple regions is not supported. See [Multizone regions \(MZR\)](#) and [IBM Cloud regions](#) for more information about multizone regions and available locations.

The information describes how to transform the individual virtual server instances into a cluster.

These procedures include installing the high availability packages and agents on each cluster node and configuring the fencing devices.



Note: This information is intended for architects and specialists who are planning a high availability deployment of SAP applications on Power Virtual Server. It is not intended to replace existing SAP or Red Hat documentation.

Before you begin

Review the general requirements, product documentation, support articles, and SAP notes listed in [Implementing high availability for SAP applications on IBM Power Virtual Server References](#).

Creating virtual server instances for the cluster

Use the instructions in [Creating instances for a high availability cluster](#) to create the virtual server instances that you want to use as cluster nodes.

Create two workspaces in two zones of a multizone region. Create a [Transit Gateway](#) and add both workspaces to the connections. Create two virtual server instances, one in each workspace.

Preparing the nodes for RHEL HA Add-On installation

The following section describes basic preparation steps on the cluster nodes. Make sure that you follow the steps on both nodes.

Log in as the root user to each of the cluster nodes.

Adding cluster node entries to the hosts file

On both nodes, add the IP addresses and hostnames of both nodes to the `/etc/hosts` file.

For more information, see [Setting up /etc/hosts files on RHEL cluster nodes](#).

Preparing environment variables

To simplify the setup process, prepare some environment variables for the root user. These environment variables are used with later operating system commands in this information.

On both nodes, set the following environment variables.

```
# General settings
export CLUSTERNAME="SAP_CLUSTER"          # Cluster name

export APIKEY=<APIKEY>                   # API Key of the IBM Cloud IAM ServiceID for the fencing agent
export CLOUD_REGION=<CLOUD_REGION>        # Multizone region name
export PROXY_IP=<IP_ADDRESS>              # IP address of proxy server

# Workspace 1
export IBMCLOUD_CRN_1=<IBMCLOUD_CRN_1>    # Workspace CRN
export GUID_1=<GUID_1>                      # Workspace GUID

# Workspace 2
```

```

export IBMCLOUD_CRN_2=<IBMCLOUD_CRN_2>      # Workspace CRN
export GUID_2=<GUID_2>                          # Workspace GUID

# Virtual server instance 1
export NODE1=<HOSTNAME_1>                      # Virtual server instance hostname
export POWERVSI_1=<POWERVSI_1>                  # Virtual server instance id

# Virtual server instance 2
export NODE2=<HOSTNAME_2>                      # Virtual server instance
export POWERVSI_2=<POWERVSI_2>                  # Virtual server instance id

```

To find the settings for the `APIKEY`, `IBMCLOUD_CRN_?`, `GUID_?`, and `POWERVSI_?` variables, follow the steps in [Collecting parameters for configuring a high availability cluster](#).

Installing and configuring a RHEL HA Add-On cluster

Use the following steps to set up a two-node cluster for an IBM Power Virtual Server.

The instructions are based on the Red Hat product documentation and articles that are listed in [Implementing high availability for SAP applications on IBM Power Virtual Server References](#).

 **Tip:** You need to complete some steps on both nodes and some steps on either NODE1 or on NODE2.

Installing RHEL HA Add-On software

Install the required software packages. The minimum operating system version required to use the `powervs-subnet` resource agent is RHEL 9.2.

The `@server` group must be installed on the operating system. This installation is a standard requirement for SAP applications.

Checking the RHEL HA repository

Check that the appropriate repository is enabled on both nodes by using the following command.

```
$ dnf repolist
```

Use the following commands to enable the HA repository if it is missing.

```
$ subscription-manager repos \
--enable="rhel-9-for-ppc64le-highavailability-e4s-rpms"
```

```
$ dnf clean all
```

```
$ dnf repolist
```

Installing the RHEL HA Add-On software packages

Install the required software packages on both nodes by running the following command.

```
$ dnf install -y pcs pacemaker fence-agents-ibm-powervs
```

Make sure that you install the minimal version of the `fence-agents-ibm-powervs` package dependent on your Red Hat Enterprise Linux release:

RHEL 9

`fence-agents-ibm-powervs-4.10.0-43.el9`

Configuring a RHEL HA Add-On cluster

Use the following steps to configure a RHEL HA Add-On cluster.

Configuring firewall services

Add the high availability service to the RHEL firewall if `firewalld.service` is installed and enabled.

On both nodes, run the following commands.

```
$ firewall-cmd --permanent --add-service=high-availability  
$ firewall-cmd --reload
```

Starting the PCS daemon

Start the PCS daemon that is used for controlling and configuring RHEL HA Add-On clusters through PCS.

On both nodes, run the following commands.

```
$ systemctl enable --now pcsd.service
```

Make sure that the PCS service is running.

```
$ systemctl status pcsd.service
```

Setting a password for the hacluster user ID

Set the password for the hacluster user ID.

On both nodes, run the following command.

```
$ passwd hacluster
```

Authenticating the cluster nodes

Use the following command to authenticate the user hacluster to the PCS daemon on the nodes in the cluster. The command prompts you for the password that you set in the previous step.

On NODE1, run the following command.

```
$ pcs host auth ${NODE1} ${NODE2} -u hacluster
```

Configuring and starting the cluster nodes

Configure the cluster configuration file and synchronize the configuration to the specified nodes.

The `--start` option also starts the cluster service on the nodes.

On NODE1, run the following command.

```
$ pcs cluster setup ${CLUSTERNAME} --start ${NODE1} ${NODE2}  
  
$ pcs status
```

Creating the fencing device

STONITH is an acronym for "Shoot The Other Node In The Head" and protects your data from corruption in a split-brain situation.

 **Important:** You must enable STONITH (fencing) for a RHEL HA Add-On production cluster.

Fence agent `fence_ibm_powervs` is the only supported agent for a STONITH device on Power Virtual Server clusters.

You must configure a fencing device for each of the two workspaces in the multizone region. The fence agent connects to the [Power Cloud API](#) by using the common `APIKEY` and `CLOUD_REGION` parameters. The parameters `IBMCLOUD_CRN_<n>`, `GUID_<n>`, and the instance ID `POWERVSI_<n>` are specific to the workspace. You can test the agent invocation by using the parameters that you gathered in the [Collecting](#)

[parameters for configuring a high availability cluster](#) section.

Identifying the virtual server instances for fencing

Use the *list* option of *fence_ibm_powervs* to identify and or verify the instance IDs of the two cluster nodes.

On any node, run the following commands.

```
$ fence_ibm_powervs \
--token=${APIKEY} \
--crn=${IBMCLOUD_CRN_1} \
--instance=${GUID_1} \
--region=${CLOUD_REGION} \
--api-type=public \
-o list
```

```
$ fence_ibm_powervs \
--token=${APIKEY} \
--crn=${IBMCLOUD_CRN_2} \
--instance=${GUID_2} \
--region=${CLOUD_REGION} \
--api-type=public \
-o list
```

If the virtual server instances have access to only a private network, you must use the `--api-type=private` option, which also requires an extra `--proxy` option.

Example:

```
$ fence_ibm_powervs \
--token=${APIKEY} \
--crn=${IBMCLOUD_CRN_1} \
--instance=${GUID_1} \
--region=${CLOUD_REGION} \
--api-type=private \
--proxy=http:// ${PROXY_IP}:3128 \
-o list
```

The following examples use the `--api-type=private` option.

Checking the status of both virtual server instances

On both nodes, run the following commands.

```
$ time fence_ibm_powervs \
--token=${APIKEY} \
--crn=${IBMCLOUD_CRN_1} \
--instance=${GUID_1} \
--region=${CLOUD_REGION} \
--plug=${POWERVSI_1} \
--api-type=private \
--proxy=http:// ${PROXY_IP}:3128 \
-o status
```

```
$ time fence_ibm_powervs \
--token=${APIKEY} \
--crn=${IBMCLOUD_CRN_2} \
--instance=${GUID_2} \
--region=${CLOUD_REGION} \
--plug=${POWERVSI_2} \
--api-type=private \
--proxy=http:// ${PROXY_IP}:3128 \
-o status
```

The `status` action of the fence agent against a virtual server instance `--plug=<POWERVSI_n>` displays its power status.

On both nodes, the two commands must report `Status: ON`.

The output of the `time` command might be useful later when you choose timeouts for the STONITH device.

You can add the `-v` flag for verbose output, which shows more information about connecting to the Power Cloud API and querying virtual server power status.

Creating the stonith devices

The following command shows the device-specific options for the `fence_ibm_powervs` fencing agent.

```
$ pcs stonith describe fence_ibm_powervs
```

Create the stonith device for both virtual server instances.

On NODE1, run the following commands.

```
$ pcs stonith create fence_node1 fence_ibm_powervs \
  token=${APIKEY} \
  crn=${IBMCLOUD_CRN_1} \
  instance=${GUID_1} \
  region=${CLOUD_REGION} \
  api_type=private \
  proxy=http://.${PROXY_IP}:3128 \
  pcmk_host_map="${NODE1}:${POWERVSI_1}" \
  pcmk_reboot_timeout=600 \
  pcmk_monitor_timeout=600 \
  pcmk_status_timeout=60
```

```
$ pcs stonith create fence_node2 fence_ibm_powervs \
  token=${APIKEY} \
  crn=${IBMCLOUD_CRN_2} \
  instance=${GUID_2} \
  region=${CLOUD_REGION} \
  api_type=private \
  proxy=http://.${PROXY_IP}:3128 \
  pcmk_host_map="${NODE2}:${POWERVSI_2}" \
  pcmk_reboot_timeout=600 \
  pcmk_monitor_timeout=600 \
  pcmk_status_timeout=60
```

 **Important:** Although the `fence_ibm_powervs` agent uses `api-type` as an option when started from the command line, the stonith resource needs to be created by using `api_type`.

Verify the configuration with the following commands.

```
$ pcs config
```

```
$ pcs status
```

```
$ pcs stonith config
```

```
$ pcs stonith status
```

Setting the stonith-action cluster property

For the `powervs-subnet` resource agent to work, you must set the `stonith-action` cluster property to `off`. When the cluster performs a fencing action, it triggers an `off` operation instead of a `reboot` for the fenced instance.

After this change, you always need to log in to the IBM Cloud Console, and manually start an instance that was fenced by the cluster.

```
$ pcs property set stonith-action=off
```

Verify the change.

```
$ pcs config
```

Testing fencing operations

To test the STONITH configuration, manually fence the nodes.

On NODE1, run the following commands.

```
$ pcs stonith fence ${NODE2}
```

```
$ pcs status
```

As a result, NODE2 stops.

Activate NODE2, then start the cluster on the node and try to fence NODE1.

On NODE2, run the following commands.

```
$ pcs cluster start
```

```
$ pcs status
```

```
$ pcs stonith status
```

```
$ pcs stonith fence ${NODE1}
```

NODE1 stops.

Activate NODE2, then start the cluster on the node.

On NODE1, run the following command.

```
$ pcs cluster start
```

```
$ pcs status
```

```
$ pcs stonith status
```

Disabling the automatic startup of cluster services when the server boots

After a virtual server instance restarts, it takes some time for its *STATUS* to become *ACTIVE* and its *Health Status* to become *OK*. The *powervs-subnet* resource agent requires these states to function properly. Therefore, you must disable automatic cluster startup and start the cluster manually after the instance reaches the required states.

On any node, disable the automatic startup of cluster services at boot time.

```
$ pcs cluster disable --all
```

When you restart an instance, check the instance status in the IBM Cloud Console and wait until the *Status* field shows *Active* with a green checkmark. Then, use the following command to manually start the cluster.

```
$ pcs cluster start
```

Preparing a multizone RHEL HA Add-On cluster for a virtual IP address resource

Use the following steps to prepare a multizone RHEL HA Add-on cluster for a virtual IP address resource.

Verifying operating system requirements

Verify that the `NetworkManager-config-server` package is installed.

On both nodes, run the following command.

```
$ dnf list NetworkManager-config-server
```

Sample output:

```
# dnf list NetworkManager-config-server
Installed Packages
NetworkManager-config-server.noarch                               1:1.42.2-16.el9_2
@rhel-9-for-ppc64le-baseos-e4s-rpms
```

Make sure that the NetworkManager `no-auto-default` configuration variable is set to `*`.

```
$ NetworkManager --print-config | grep "no-auto-default=*
```

Sample output:

```
# NetworkManager --print-config | grep "no-auto-default="
no-auto-default=*
```

If the `no-auto-default` shows a value other than `*`, edit the `/etc/NetworkManager/conf.d/00-server.conf` file and change the variable as needed.

Installing the `powervs-subnet` resource agent

Currently, the `powervs-subnet` resource agent is available in the ClusterLabs GitHub resource agent repository.

Download the resource agent from <https://github.com/ClusterLabs/resource-agents/blob/main/heartbeat/powervs-subnet.in> and place a copy in the `/tmp` directory on both nodes.

On both nodes, install the script in the `OCF Resource Agents` heartbeat directory and set its permissions.

```
$ sed -e 's|#!@PYTHON@|#!/usr/bin/python3|' /tmp/powervs-subnet.in \
> /usr/lib/ocf/resource.d/heartbeat/powervs-subnet
```

```
$ chmod 755 /usr/lib/ocf/resource.d/heartbeat/powervs-subnet
```

Use the following command to verify the installation and display a brief description of the resource agent.

```
$ pcs resource describe powervs-subnet
```

Creating a service ID for the `powervs-subnet` resource agent

Follow the steps in [Creating a Custom Role, Service ID, and API key in IBM Cloud](#) to create a `Service ID` and an `API key` for the `powervs-subnet` resource agent.

Conclusion

This completes the basic cluster implementation and the necessary preparations for creating a `powervs-subnet` cluster resource. The `powervs-subnet` cluster resource itself is created during the configuration of the specific high availability scenario.

You can now proceed with the specific instructions for your planned high availability scenario.

Configuring SAP HANA scale-up system replication in a Red Hat Enterprise Linux High Availability Add-On cluster

The following information describes the configuration of a Red Hat Enterprise Linux (RHEL) High Availability Add-On cluster for managing `SAP HANA Scale-Up System Replication`. The cluster uses virtual server instances in [IBM® Power® Virtual Server](#) as cluster nodes.

The instructions describe how to automate SAP HANA Scale-Up System Replication for a single database deployment in a performance-optimized scenario on a RHEL HA Add-on cluster.



Note: This information is intended for architects and specialists that are planning a high-availability deployment of SAP HANA on Power Virtual Server.

Before you begin

Review the general requirements, product documentation, support articles, and SAP notes listed in [Implementing high availability for SAP applications on IBM Power Virtual Server References](#).

Prerequisites

- A Red Hat High Availability cluster is deployed on two virtual server instances in Power Virtual Server.
 - Install and set up the RHEL HA Add-On cluster according to [Implementing a Red Hat Enterprise Linux High Availability Add-On cluster](#).
 - Configure and verify fencing as described in the preceding document.
- The virtual server instances need to fulfill hardware and resource requirements for the SAP HANA systems in scope. Follow the guidelines in the [Planning your deployment](#) document.
- The hostnames of the virtual server instances must meet the SAP HANA requirement.
- SAP HANA is installed on both virtual server instances and SAP HANA System Replication is configured. The installation of SAP HANA and setup of HANA System Replication is not specific to the Power Virtual Server environment, and you need to follow the standard procedures.
- A valid *RHEL for SAP Applications* or *RHEL for SAP Solutions* subscription is required to enable the repositories that you need to install SAP HANA and the resource agents for HA configurations.

Configuring SAP HANA System Replication in a RHEL HA Add-On cluster on IBM Power Virtual Server

The instructions are based on the Red Hat product documentation and articles that are listed in [Implementing high availability for SAP applications on IBM Power Virtual Server References](#).

Preparing environment variables

To simplify the setup, prepare the following environment variables for root on both nodes. These environment variables are used with later operating system commands in this information.

On both nodes, set the following environment variables.

```
# General settings
export SID=<SID>          # SAP HANA System ID (uppercase)
export sid=<sid>            # SAP HANA System ID (lowercase)
export INSTNO=<INSTNO>      # SAP HANA instance number

# Cluster node 1
export NODE1=<HOSTNAME_1>  # Virtual server instance hostname
export DC1="Site1"          # HANA System Replication site name

# Cluster node 2
export NODE2=<HOSTNAME_2>  # Virtual server instance hostname
export DC2="Site2"          # HANA System Replication site name

# Single zone
export VIP=<IP address>    # SAP HANA System Replication cluster virtual IP address

# Multizone region
export CLOUD_REGION=<CLOUD_REGION>      # Multizone region name
export APIKEY="APIKEY or path to file"     # API Key of the IBM Cloud IAM ServiceID for the resource agent
export API_TYPE="private or public"         # Use private or public API endpoints
export IBMCLoud_CRN_1=<IBMCLoud_CRN_1>   # Workspace 1 CRN
export IBMCLoud_CRN_2=<IBMCLoud_CRN_2>   # Workspace 2 CRN
export POWERVSI_1=<POWERVSI_1>           # Virtual server instance 1 id
export POWERVSI_2=<POWERVSI_2>           # Virtual server instance 2 id
export SUBNET_NAME="vip-${sid}-net"        # Name which is used to define the subnet in IBM Cloud
export CIDR="CIDR of subnet"              # CIDR of the subnet containing the service IP address
export VIP="Service IP address"          # IP address in the subnet
export JUMBO="true or false"              # Enable Jumbo frames
```

Setting extra environment variables for a single zone implementation

Review the information in [Reserving virtual IP addresses](#) and reserve a virtual IP address for the SAP HANA System Replication cluster. Set the

VIP environment variable to the reserved IP address.

Setting extra environment variables for a multizone region implementation

Set the `CLOUD_REGION`, `APIKEY`, `IBMCLOUD_CRN_?`, `POWERVSI_?` variables as described in [Collecting parameters for configuring a high availability cluster](#) section. Set the `API_TYPE` variable to `private` to communicate with the IBM Cloud IAM and IBM Power Cloud API via private endpoints. The `SUBNET_NAME` variable contains the name of the subnet. The `CIDR` variable represents the *Classless Inter-Domain Routing (CIDR)* notation for the subnet in the format `<IPv4_address>/number`. The `VIP` variable is the IP address of the virtual IP address resource and must belong to the `CIDR` of the subnet. Set the `JUMBO` variable to `true` if you want to enable the subnet for a large MTU size.

The following is an example of how to set the extra environment variables that are required for a multizone region implementation.

```
export CLOUD_REGION="eu-de"
export IBMCLOUD_CRN_1="crn:v1:bluemix:public:power-iaas:eu-de-2:a/a1b2c3d4e5f60123456789a1b2c3d4e5:a1b2c3d4-0123-4567-89ab-a1b2c3d4e5f6::"
export IBMCLOUD_CRN_2="crn:v1:bluemix:public:power-iaas:eu-de-1:a/a1b2c3d4e5f60123456789a1b2c3d4e5:e5f6a1b2-cdef-0123-4567-a1b2c3d4e5f6::"
export POWERVSI_1="a1b2c3d4-0123-890a-f012-0123456789ab"
export POWERVSI_2="e5f6a1b2-4567-bcde-3456-cdef01234567"
export APIKEY="@/root/.apikey.json"
export API_TYPE="private"
export SUBNET_NAME="vip-mha-net"
export CIDR="10.40.11.100/30"
export VIP="10.40.11.102"
export JUMBO="true"
```

Installing SAP HANA resource agents

Run the following command to install the RHEL HA Add-On resource agents for SAP HANA System Replication.

```
$ dnf install -y resource-agents-sap-hana
```

Starting the SAP HANA system

Start SAP HANA and verify that HANA System Replication is active. For more information, see [2.4. Checking SAP HANA System Replication state](#).

On both nodes, run the following commands.

```
$ sudo -i -u ${sid}adm -- HDB start

$ sudo -i -u ${sid}adm -- <<EOT
    hdbnsutil -sr_state
    HDBSettings.sh systemReplicationStatus.py
EOT
```

Enabling the SAP HANA srConnectionChanged() hook

Recent versions of SAP HANA provide *hooks* so SAP HANA can send out notifications for certain events. For more information, see [Implementing a HA/DR Provider](#).

The `srConnectionChanged()` hook improves the ability of the cluster to detect a status change of HANA System Replication that requires an action from the cluster. The goal is to prevent data loss and corruption by preventing accidental takeovers.

Activating the srConnectionChanged() hook on all SAP HANA instances

1. Stop the cluster.

On NODE1, run the following command.

```
$ pcs cluster stop --all
```

2. Install the hook script that is provided by the `resource-agents-sap-hana` package in the `/hana/shared/myHooks` directory for each HANA instance, and set the required ownership.

On both nodes, run the following commands.

```
$ mkdir -p /hana/shared/myHooks  
  
$ cp /usr/share/SAPHanaSR/srHook/SAPHanaSR.py /hana/shared/myHooks  
  
$ chown -R ${sid}adm:sapsys /hana/shared/myHooks
```

3. Update the `global.ini` file on each HANA node to enable the hook script.

On both nodes, run the following command.

```
$ sudo -i -u ${sid}adm -- <<EOT  
    python \${DIR_INSTANCE}/exe/python_support/setParameter.py \  
        -set SYSTEM/global.ini/ha_dr_provider_SAPHanaSR/provider=SAPHanaSR \  
        -set SYSTEM/global.ini/ha_dr_provider_SAPHanaSR/path=/hana/shared/myHooks \  
        -set SYSTEM/global.ini/ha_dr_provider_SAPHanaSR/execution_order=1 \  
        -set SYSTEM/global.ini/trace/ha_dr_saphanasr=info  
EOT
```

4. Verify the changed file.

On both nodes, run the following command.

```
$ cat /hana/shared/\${SID}/global/hdb/custom/config/global.ini
```

5. Create sudo settings for SAP HANA OS user.

You need the following sudo settings to allow the `\${sid}adm` user script can update the node attributes when the `srConnectionChanged()` hook runs.

On both nodes, run the following commands.

Create a file with the required sudo aliases and user specifications.

```
$ cat >> /etc/sudoers.d/20-saphana << EOT  
Cmnd_Alias DC1_SOK = /usr/sbin/crm_attribute -n hana_\${sid}_site_srHook_\${DC1} -v SOK -t crm_config -s SAPHanaSR  
Cmnd_Alias DC1_SFAIL = /usr/sbin/crm_attribute -n hana_\${sid}_site_srHook_\${DC1} -v SFAIL -t crm_config -s SAPHanaSR  
Cmnd_Alias DC2_SOK = /usr/sbin/crm_attribute -n hana_\${sid}_site_srHook_\${DC2} -v SOK -t crm_config -s SAPHanaSR  
Cmnd_Alias DC2_SFAIL = /usr/sbin/crm_attribute -n hana_\${sid}_site_srHook_\${DC2} -v SFAIL -t crm_config -s SAPHanaSR  
\${sid}adm ALL=(ALL) NOPASSWD: DC1_SOK, DC1_SFAIL, DC2_SOK, DC2_SFAIL  
Defaults!DC1_SOK, DC1_SFAIL, DC2_SOK, DC2_SFAIL !requiretty  
EOT
```

Adjust the permissions and check for syntax errors.

```
$ chown root:root /etc/sudoers.d/20-saphana  
  
$ chmod 0440 /etc/sudoers.d/20-saphana  
  
$ cat /etc/sudoers.d/20-saphana  
  
$ visudo -c
```



Note: Any problems that are reported by the `visudo -c` command must be corrected.

1. Verify that the hook functions.

- Restart both HANA instances and verify that the hook script works as expected.
- Perform an action to trigger the hook, such as stopping a HANA instance.
- Check whether the hook logged anything in the trace files.

On both nodes, run the following commands.

Stop the HANA instance.

```
$ sudo -i -u ${sid}adm -- HDB stop
```

Start the HANA instance.

```
$ sudo -i -u ${sid}adm -- HDB start
```

Check that the hook logged some messages to the trace files.

```
$ sudo -i -u ${sid}adm -- sh -c 'grep "ha_dr_SAPHanaSR.*crm_attribute" $DIR_INSTANCE/$VTHOSTNAME/trace/nameserver_* | cut -d" " -f2,3,5,17'
```

After you verify that the hooks function, you can restart the HA cluster.

2. Start the cluster.

On NODE1, run the following commands.

Start the cluster.

```
$ pcs cluster start --all
```

Check the status of the cluster.

```
$ pcs status --full
```

Configuring general cluster properties

To avoid resource failover during initial testing and post-production, set the following default values for the resource-stickiness and migration-threshold parameters.

Keep in mind that defaults don't apply to resources that override them with their own defined values.

On NODE1, run the following commands.

```
$ pcs resource defaults update resource-stickiness=1000
```

```
$ pcs resource defaults update migration-threshold=5000
```

Creating a cloned SAPHanaTopology resource

The *SAPHanaTopology* resource gathers the status and configuration of SAP HANA System Replication on each node. It also starts and monitors the local *SAP HostAgent*, which is required for starting, stopping, and monitoring SAP HANA instances.

On NODE1, run the following commands.

Create the *SAPHanaTopology* resource.

```
$ pcs resource create SAPHanaTopology_${SID}_${INSTNO} SAPHanaTopology \
  SID=${SID} InstanceNumber=${INSTNO} \
  op start timeout=600 \
  op stop timeout=300 \
  op monitor interval=10 timeout=600 \
  clone clone-max=2 clone-node-max=1 interleave=true
```

Check the configuration and the cluster status by running the following commands.

```
$ pcs resource config SAPHanaTopology_${SID}_${INSTNO}
```

```
$ pcs resource config SAPHanaTopology_${SID}_${INSTNO}-clone
```

```
$ pcs status --full
```

Creating a promotable SAPHana resource

The *SAPHana* resource manages two SAP HANA instances that are configured as HANA System Replication nodes.

On NODE1, create the *SAPHana* resource by running the following command.

```
$ pcs resource create SAPHana_${SID}_${INSTNO} SAPHana \
  SID=${SID} InstanceNumber=${INSTNO} \
  PREFER_SITE_TAKEOVER=true \
  DUPLICATE_PRIMARY_TIMEOUT=7200 \
  AUTOMATED_REGISTER=false \
  op start timeout=3600 \
  op stop timeout=3600 \
  op monitor interval=61 role="Unpromoted" timeout=700 \
  op monitor interval=59 role="Promoted" timeout=700 \
  op promote timeout=3600 \
  op demote timeout=3600 \
  promotable notify=true clone-max=2 clone-node-max=1 interleave=true
```

Check the configuration and the cluster status.

```
$ pcs resource config SAPHana_${SID}_${INSTNO}
$ pcs status --full
```

Creating a virtual IP address cluster resource

Depending on the scenario, proceed to one of the following sections:

- [Creating a virtual IP address cluster resource in a single zone environment](#) if the cluster nodes are running in a single Power Virtual Server workspace
- [Creating a virtual IP address cluster resource in a multizone region environment](#) if the cluster nodes are running in separate Power Virtual Server workspaces

Creating a virtual IP address cluster resource in a single zone environment

Use the reserved IP address to create a virtual IP address cluster resource. This virtual IP address is used to reach the SAP HANA System Replication primary instance.

Create the virtual IP address cluster resource with the following command.

```
$ pcs resource create vip_${SID}_${INSTNO} IPAddr2 ip=$VIP
```

Check the configured virtual IP address cluster resource and the cluster status.

```
$ pcs resource config vip_${SID}_${INSTNO}
$ pcs status --full
```

Proceed to the [Creating cluster resource constraints](#) section.

Creating a virtual IP address cluster resource in a multizone region environment

Verify that you have completed all the steps in the [Preparing a multi-zone RHEL HA Add-On cluster for a virtual IP address resource](#) section.

 **Note:** Run the `pcs resource describe powervs-subnet` command to get information about the resource agent parameters.

On NODE1, create a `powervs-subnet` cluster resource by running the following command.

```
$ pcs resource create vip_${SID}_${INSTNO} powervs-subnet \
  api_key=${APIKEY} \
  api_type=${API_TYPE} \
  cidr=${CIDR} \
  ip=${VIP} \
  crn_host_map="${NODE1}: ${IBMCLOUD_CRN_1}; ${NODE2}: ${IBMCLOUD_CRN_2}" \
  vsi_host_map="${NODE1}: ${POWERVSI_1}; ${NODE2}: ${POWERVSI_2}" \
```

```
jumbo=${JUMBO} \
region=${CLOUD_REGION} \
subnet_name=${SUBNET_NAME} \
op start timeout=720 \
op stop timeout=300 \
op monitor interval=60 timeout=30
```



Note: If you set `API_TYPE` to `public`, you must also specify a `proxy` parameter.



Important: Ensure that both virtual server instances in the cluster have the status `Active` and the health status `OK` before running the `pcs resource config` command.

Check the configured virtual IP address resource and the cluster status.

```
$ pcs resource config vip_${SID}_${INSTNO}
```

Sample output:

```
$ pcs status --full
```

The following example is a sample output of an SAP HANA System Replication cluster in a multizone region setup.

```
# pcs status --full
Cluster name: SAP_MHA
Status of pacemakerd: 'Pacemaker is running' (last updated 2024-07-31 11:37:49 +02:00)
Cluster Summary:
  * Stack: corosync
  * Current DC: cl-mha-2 (2) (version 2.1.5-9.el9_2.4-a3f44794f94) - partition with quorum
  * Last updated: Wed Jul 31 11:37:50 2024
  * Last change: Wed Jul 31 11:37:31 2024 by root via crm_attribute on cl-mha-1
  * 2 nodes configured
  * 7 resource instances configured

Node List:
  * Node cl-mha-1 (1): online, feature set 3.16.2
  * Node cl-mha-2 (2): online, feature set 3.16.2

Full List of Resources:
  * fence_node1 (stonith:fence_ibm_powerys): Started cl-mha-1
```

```

* fence_node2 (stonith:fence_ibm_powervs): Started cl-mha-2
* Clone Set: SAPHanaTopology_MHA_00-clone [SAPHanaTopology_MHA_00]:
  * SAPHanaTopology_MHA_00 (ocf:heartbeat:SAPHanaTopology): Started cl-mha-2
  * SAPHanaTopology_MHA_00 (ocf:heartbeat:SAPHanaTopology): Started cl-mha-1
* Clone Set: SAPHana_MHA_00-clone [SAPHana_MHA_00] (promotable):
  * SAPHana_MHA_00 (ocf:heartbeat:SAPHana): Unpromoted cl-mha-2
  * SAPHana_MHA_00 (ocf:heartbeat:SAPHana): Promoted cl-mha-1
* vip_MHA_00 (ocf:heartbeat:powervs-subnet): Started cl-mha-1

Node Attributes:
* Node: cl-mha-1 (1):
  * hana_mha_clone_state : PROMOTED
  * hana_mha_op_mode : logreplay
  * hana_mha_remoteHost : cl-mha-2
  * hana_mha_roles : 4:P:master1:master:worker:master
  * hana_mha_site : SiteA
  * hana_mha_sra : -
  * hana_mha_srah : -
  * hana_mha_srmode : syncmem
  * hana_mha_sync_state : PRIM
  * hana_mha_version : 2.00.075.00
  * hana_mha_vhost : cl-mha-1
  * lpa_mha_lpt : 1722418651
  * master-SAPHana_MHA_00 : 150
* Node: cl-mha-2 (2):
  * hana_mha_clone_state : DEMOTED
  * hana_mha_op_mode : logreplay
  * hana_mha_remoteHost : cl-mha-1
  * hana_mha_roles : 4:S:master1:master:worker:master
  * hana_mha_site : SiteB
  * hana_mha_sra : -
  * hana_mha_srah : -
  * hana_mha_srmode : syncmem
  * hana_mha_sync_state : SOK
  * hana_mha_version : 2.00.075.00
  * hana_mha_vhost : cl-mha-2
  * lpa_mha_lpt : 30
  * master-SAPHana_MHA_00 : 100

```

Migration Summary:

Tickets:

PCSD Status:

cl-mha-1: Online
cl-mha-2: Online

Daemon Status:

corosync: active/disabled
pacemaker: active/disabled
pcsd: active/enabled

Proceed to the [Creating cluster resource constraints](#) section.

Creating cluster resource constraints

Make sure that *SAPHanaTopology* resources are started before you start the *SAPHana* resources.

The virtual IP address must be present on the node where the primary resource of "SAPHana" is running.

1. Create a resource constraint to start "SAPHanaTopology" before "SAPHana". This constraint mandates the start order of these resources.

On NODE1, use the following command to create the *SAPHanaTopology* order constraint:

```
$ pcs constraint order SAPHanaTopology_${SID}_${INSTNO}-clone \
  then SAPHana_${SID}_${INSTNO}-clone symmetrical=false
```

Check the configuration.

```
$ pcs constraint
```

2. Create a resource constraint to colocate the virtual IP address with primary. This constraint collocates the virtual IP address resource with the SAPHana resource that was promoted as primary.

On NODE1, run the following command to create the virtual IP address colocation constraint.

```
$ pcs constraint colocation add vip_${SID}_${INSTNO} \
    with Promoted SAPHana_${SID}_${INSTNO}-clone 2000
```

Check the configuration and the cluster status.

```
$ pcs constraint
```

Sample output:

```
# pcs constraint
Location Constraints:
Ordering Constraints:
    start SAPHanaTopology_HDB_00-clone then start SAPHana_HDB_00-clone (kind:Mandatory) (non-symmetrical)
Colocation Constraints:
    vip_HDB_00 with SAPHana_HDB_00-clone (score:2000) (rsc-role:Started) (with-rsc-role:Promoted)
Ticket Constraints:
```

Verify the cluster status.

```
$ pcs status --full
```

On the promoted cluster node, verify that the cluster service IP address is active.

```
$ ip addr show
```

Enabling the SAP HANA srServiceStateChanged() hook (optional)

SAP HANA has built-in functions to monitor its `indexserver`. In case of a problem, SAP HANA tries to recover automatically by stopping and restarting the process. To stop the process or clean up after a crash, the Linux kernel must release all memory that is allocated by the process. For large databases, this cleanup can take a long time. During this time, SAP HANA continues to operate and accept new client requests. As a result, SAP HANA system replication can become out of sync. If another error occurs in the SAP HANA instance before the restart and recovery of the `indexserver` is complete, data consistency is at risk.

The `ChkSrv.py` script for the `srServiceStateChanged()` hook reacts to such a situation and can stop the entire SAP HANA instance for faster recovery. If `automated failover` is enabled in the cluster, and the secondary node is in a healthy state, a takeover operation is started. Otherwise, recovery must continue locally, but is accelerated by the forced restart of the SAP HANA instance.



Note: The SAP HANA `srServiceStateChanged()` hook is available with `resource-agents-sap-hana` version 0.162.3 and later.

The hook script analyzes the events in the instance, applies filters to the event details, and triggers actions based on the results. It distinguishes between an SAP HANA `indexserver` process that is stopped and restarted by SAP HANA and the process that is stopped during an instance shutdown.

Depending on the configuration of the `action_on_lost` parameter, the hook takes different actions:

Ignore

This action simply logs the events and decision information to a log file.

Stop

This action triggers a graceful stop of the SAP HANA instance by using the sapcontrol command.

Kill

This action triggers the HDB kill- `<signal>` command with a default signal 9. The signal can be configured.

Both the `stop` and the `kill` actions result in a stopped SAP HANA instance, the `kill` action is slightly faster.

Activating the srServiceStateChanged() hook on all SAP HANA instances

The `srServiceStateChanged()` hook can be added while SAP HANA is running on both nodes.

- For each HANA instance, install the hook script that is provided by the `resource-agents-sap-hana` package in the `/hana/shared/myHooks` directory and set the required ownership.

On both nodes, run the following commands.

```
$ cp /usr/share/SAPHanaSR/srHook/ChkSrv.py /hana/shared/myHooks
```

```
$ chown ${sid}adm:sapsys /hana/shared/myHooks/ChkSrv.py
```

- Update the `global.ini` file on each SAP HANA node to enable the hook script.

On both nodes, run the following command.

```
$ sudo -i -u ${sid}adm -- <<EOT
python \${DIR_INSTANCE}/exe/python_support/setParameter.py \
-set SYSTEM/global.ini/ha_dr_provider_ChkSrv/provider=ChkSrv \
-set SYSTEM/global.ini/ha_dr_provider_ChkSrv/path=/hana/shared/myHooks \
-set SYSTEM/global.ini/ha_dr_provider_ChkSrv/execution_order=2 \
-set SYSTEM/global.ini/ha_dr_provider_ChkSrv/action_on_lost=stop \
-set SYSTEM/global.ini/trace/ha_dr_chksrv=info
EOT
```

The `action_on_lost` parameter in this example is set to `stop`, the default setting is `ignore`. You can optionally set the parameters `stop_timeout` (default: `20` seconds) and `kill_signal` (default: `9`).

- Activate the `ChkSrv.py` hook

On both nodes, run the following command to reload the HA-DR providers.

```
$ sudo -i -u ${sid}adm -- hdbnsutil -reloadHADRProviders
```

- Check that the hook logged some messages to the trace files.

On both nodes, run the following command.

```
$ sudo -i -u ${sid}adm -- sh -c 'grep "ha_dr_ChkSrv" ${DIR_INSTANCE}/$VTHOSTNAME/trace/nameserver_* | cut -d" " -f2,3,6-'
```

Enabling automated registration of secondary instance

You need to set the parameter `AUTOMATED_REGISTER` according to your operational requirements. If you want to keep the ability to revert to the state of the previous primary SAP HANA instance, then `AUTOMATED_REGISTER=false` avoids an automatic registration of the previous primary as a new secondary.

If you experience an issue with the data after a takeover that was triggered by the cluster, you can manually revert if `AUTOMATED_REGISTER` is set to `false`.

If `AUTOMATED_REGISTER` is set to `true`, the previous primary SAP HANA instance automatically registers as secondary, and cannot be activated on its previous history. The advantage of `AUTOMATED_REGISTER=true` is that high-availability capability is automatically reestablished after the failed node reappears in the cluster.

For now, it is recommended to keep `AUTOMATED_REGISTER` on default value `false` until the cluster is fully tested and that you verify that the failover scenarios work as expected.

 **Tip:** The `pcs resource update` command is used to modify resource attributes and `pcs resource update SAPHana_${SID}_${INSTNO} AUTOMATED_REGISTER=true` sets the attribute to `true`.

Testing SAP HANA System Replication cluster

It is vital to thoroughly test the cluster configuration to make sure that the cluster is working correctly. The following information provides a few sample failover test scenarios, but is not a complete list of test scenarios.

For example, the description of each test case includes the following information.

- Component that is being tested
- Description of the test
- Prerequisites and the cluster state before you start the failover test
- Test procedure
- Expected behavior and results
- Recovery procedure

Test 1 - Testing a failure of the primary database instance

Use the following information to test the failure of the primary database instance.

Test 1 - Description

Simulate a crash of the primary HANA database instance that is running on NODE1.

Test 1 - Prerequisites

- A functional two-node RHEL HA Add-On cluster for HANA system replication.
- Both cluster nodes are active.
- Cluster that is started on NODE1 and NODE2.
- Cluster Resource `SAPHana_${SID}_${INSTNO}` that is configured with `AUTOMATED_REGISTER=false`.
- Check SAP HANA System Replication status:
 - Primary SAP HANA database is running on NODE1
 - Secondary SAP HANA database is running on NODE2
 - HANA System Replication is activated and in sync

Test 1 - Test procedure

Crash SAP HANA primary by sending a SIGKILL signal as the user `${sid}adm`.

On NODE1, run the following command.

```
$ sudo -i -u ${sid}adm -- HDB kill-9
```

Test 1 - Expected behavior

- SAP HANA primary instance on NODE1 crashes.
- The cluster detects the stopped primary HANA database and marks the resource as `failed`.
- The cluster promotes the secondary HANA database on NODE2 to take over as the new primary.
- The cluster releases the virtual IP address on NODE1, and acquires it on the new primary on NODE2.
- If an application, such as SAP NetWeaver, is connected to a tenant database of SAP HANA, the application automatically reconnects to the new primary.

Test 1 - Recovery procedure

As the cluster resource `SAPHana_${SID}_${INSTNO}` is configured with `AUTOMATED_REGISTER=false`, the cluster doesn't restart the failed HANA database, and doesn't register it against the new primary. Which means that the status on the new primary (NODE2) also shows the secondary in status 'CONNECTION TIMEOUT'.

To reregister the previous primary as a new secondary use the following commands.

On NODE1, run the following command.

```
$ sudo -i -u ${sid}adm -- <<EOT
hdbnsutil -sr_register \
--name=${DC1} \
--remoteHost=${NODE2} \
--remoteInstance=00 \
--replicationMode=sync \
```

```
--operationMode=logreplay \
--online
EOT
```

Verify the system replication status:

```
$ sudo -i -u ${sid}adm -- <<EOT
    hdbsutil -sr_state
    HDBSettings.sh systemReplicationStatus.py
EOT
```

After the manual register and resource refreshes, the new secondary instance restarts and shows up in status synced (**SOK**).

On NODE1, run the following command.

```
$ pcs resource refresh SAPHana_${SID}_${INSTNO}
$ pcs status --full
```

Test 2 - Testing a failure of the node that is running the primary database

Use the following information to test the failure of the node that is running the primary database.

Test 2 - Description

Simulate a crash of the node that is running the primary HANA database.

Test 2 - Preparation

Make sure that the cluster resource **SAPHana_\${SID}_\${INSTNO}** is configured with **AUTOMATED_REGISTER=true**.

On NODE1, run the following command.

```
$ pcs resource update SAPHana_${SID}_${INSTNO} AUTOMATED_REGISTER=true
$ pcs resource config SAPHana_${SID}_${INSTNO}
```

Test 2 - Prerequisites

- A functional two-node RHEL HA Add-On cluster for HANA system replication.
- Both nodes are active.
- Cluster is started on NODE1 and NODE2.
- Check SAP HANA System Replication status.
 - Primary SAP HANA database is running on NODE2
 - Secondary SAP HANA database is running on NODE1
 - HANA System Replication is activated and in sync

Test 2 - Test procedure

Crash primary on NODE2 by sending a *crash* system request.

On NODE2, run the following command.

```
$ sync; echo c > /proc/sysrq-trigger
```

Test 2 - Expected behavior

- NODE2 shuts down.
- The cluster detects the failed node and sets its state to **OFFLINE**.
- The cluster promotes the secondary HANA database on NODE1 to take over as the new primary.
- The cluster acquires the virtual IP address on NODE1 on the new primary.

- If an application, such as SAP NetWeaver, is connected to a tenant database of SAP HANA, the application automatically reconnects to the new primary.

Test 2 - Recovery procedure

Log in to the IBM Cloud® Console and start the NODE2 instance. Wait until NODE2 is available again, then restart the cluster framework.

On NODE2, run the following command.

```
$ pcs cluster start
```

```
$ pcs status --full
```

As the cluster resource `SAPHana_${SID}_${INSTNO}` is configured with `AUTOMATED_REGISTER=true`, SAP HANA restarts when NODE2 rejoins the cluster and the former primary reregisters as a secondary.

Test 3 - Testing a failure of the secondary database instance

Use the following information to test the failure of the secondary database instance.

Test 3 - Description

Simulate a crash of the secondary HANA database.

Test 3 - Prerequisites

- A functional two-node RHEL HA Add-On cluster for HANA system replication.
- Both nodes are active.
- Cluster is started on NODE1 and NODE2.
- Cluster Resource `SAPHana_${SID}_${INSTNO}` is configured with `AUTOMATED_REGISTER=true`.
- Check SAP HANA System Replication status:
 - Primary SAP HANA database is running on NODE1
 - Secondary SAP HANA database is running on NODE2
 - HANA System Replication is activated and in sync

Test 3 - Test Procedure

Crash SAP HANA secondary by sending a SIGKILL signal as the user `${sid}adm`.

On NODE2, run the following command.

```
$ sudo -i -u ${sid}adm -- HDB kill-9
```

Test 3 - Expected behavior

- SAP HANA secondary on NODE2 crashes.
- The cluster detects the stopped secondary HANA database and marks the resource as `failed`.
- The cluster restarts the secondary HANA database.
- The cluster detects that the system replication is in sync again.

Test 3 - Recovery procedure

Wait until the secondary HANA instance starts and syncs again (`SO`), then cleanup the failed resource actions as shown in `pcs status`.

On NODE2, run the following command.

```
$ pcs resource refresh SAPHana_${SID}_${INSTNO}
```

```
$ pcs status --full
```

Test 4 - Testing a manual move of a SAPHana resource to another node

Use the following information to test the manual move of a SAPHana resource to another node.

Test 4 - Description

Use cluster commands to move the primary instance to the other node for maintenance purposes.

Test 4 - Prerequisites

- A functional two-node RHEL HA Add-On cluster for HANA system replication.
- Both nodes are active.
- Cluster is started on NODE1 and NODE2.
- Cluster Resource `SAPHana_${SID}_${INSTNO}` is configured with `AUTOMATED_REGISTER=true`.
- Check SAP HANA System Replication status:
 - Primary SAP HANA database is running on NODE1
 - Secondary SAP HANA database is running on NODE2
 - HANA System Replication is activated and in sync

Test 4 - Test procedure

Move SAP HANA primary to other node by using the `pcs resource move` command.

On NODE1, run the following command.

```
$ pcs resource move SAPHana_${SID}_${INSTNO}-clone
```

Test 4 - Expected behavior

- The cluster creates location constraints to move the resource.
- The cluster triggers a takeover to the secondary HANA database.
- If an application, such as SAP NetWeaver, is connected to a tenant database of SAP HANA, the application automatically reconnects to the new primary.

Test 4 - Recovery procedure

The automatically created location constraints must be removed to allow automatic failover in the future.

Wait until the primary HANA instance is active and remove the constraints.

The cluster registers and starts the HANA database as a new secondary instance.

On NODE1, run the following command.

```
$ pcs constraint
```

```
$ pcs resource clear SAPHana_${SID}_${INSTNO}-clone
```

```
$ pcs constraint
```

```
$ pcs status --full
```

Configuring SAP HANA cost-optimized scale-up system replication in a Red Hat Enterprise Linux High Availability Add-On cluster

The following information describes the configuration of a Red Hat Enterprise Linux (RHEL) High Availability Add-On cluster for managing *SAP HANA Cost-Optimized Scale-Up System Replication*. The cluster uses virtual server instances in [IBM® Power® Virtual Server](#) as cluster nodes.

In a *cost-optimized* configuration, a nonproduction SAP HANA system runs on the secondary node during normal operation. The hardware resources on the secondary node are shared between the nonproduction system and the SAP HANA System Replication secondary. The

memory usage of the production System Replication secondary is reduced by disabling the preload of column table data.

If a failover occurs, the nonproduction instance is stopped automatically before the node takes over the production workload. The takeover time is longer compared to a performance optimized configuration.



Note: This information is intended for architects and specialists that are planning a high-availability deployment of SAP HANA on Power Virtual Server.

Before you begin

Review the general requirements, product documentation, support articles, and SAP notes listed in [Implementing high availability for SAP applications on IBM Power Virtual Server References](#).

Prerequisites

- A Red Hat High Availability cluster is deployed on two virtual server instances in Power Virtual Server.
 - Install and set up the RHEL HA Add-On cluster according to [Implementing a Red Hat Enterprise Linux High Availability Add-On cluster](#).
 - Configure and verify fencing as described in the preceding document.
- The virtual server instances need to fulfill hardware and resource requirements for the SAP HANA systems in scope. Follow the guidelines in the [Planning your deployment](#) document.
- The hostnames of the virtual server instances must meet the SAP HANA requirement.
- SAP HANA is installed on both virtual server instances and SAP HANA System Replication is configured. The installation of SAP HANA and setup of HANA System Replication is not specific to the Power Virtual Server environment, and you need to follow the standard procedures.
- A nonproduction SAP HANA System is installed on NODE2 with a different `SID` and `Instance Number` than the production system. The nonproduction system needs its own dedicated storage volumes and file systems. Restrict the *Global Memory Allocation Limit* for the nonproduction system to ensure sufficient memory for the HANA system replication workload on the secondary. The limit is set with the `global_allocation_limit` parameter in the `[memorymanager]` section of the `global.ini` configuration file.
- Optional, a virtual IP address is reserved for the nonproduction system as described in [Reserving virtual IP addresses](#).

Setting up the cost optimized scenario

The cost optimized scenario is an extension of the setup that is described in [Configuring SAP HANA scale-up system replication in a Red Hat Enterprise Linux High Availability Add-On cluster](#). Complete the setup for the production system System Replication cluster before you continue with the following steps.

Preparing environment variables

To simplify the setup, prepare the following environment variables for user ID `root` on NODE2. These environment variables are used with later operating system commands in this information.

On NODE2, set the following environment variables.

```
# General settings
export SID_NP=<SID>                      # SAP HANA System ID of non-production system (uppercase)
export sid_np=<sid>                          # SAP HANA System ID of non-production system (lowercase)
export INSTNO_NP=<INSTNO>                     # SAP HANA Instance Number of non-production system

# Cluster nodes
export NODE1=<Hostname 1>                   # Hostname of virtual server instance 1 (production primary)
export NODE2=<Hostname 2>                   # Hostname of virtual server instance 2 (non-production, production secondary)

# Optional virtual IP address
export VIP_NP=<IP address>                 # Virtual IP address for the non-production system
```

Configuring the SAP HANA HA/DR provider hook

The SAP HANA nameserver provides a Python-based API that is called at important points during the HANA System Replication takeover process. These API calls are used to run customer-specific operations ([Implementing a HA/DR Provider](#)).

In the cost-optimized scenario, the SAP HANA HA/DR provider hook is used to automatically reconfigure the SAP HANA instance during the takeover event.

The following section shows a sample set up of a hook script for a *cost-optimized* SAP HANA System Replication environment. When you implement automation of the cost-optimized SAP HANA System Replication HA environment in the cluster, the takeover hook script must be thoroughly tested. Run the tests manually. Shut down the nonproduction SAP HANA instance on the secondary node, perform a takeover, and verify that the hook script correctly reconfigures the primary HANA DB.

Creating a database user in the SAP HANA production database

Use the following steps to create a database user in the SAP HANA production database.

1. Create a database user in the *SystemDB* of the SAP HANA production system, or provide credentials of an existing user. The hook script uses this database user to connect to the production database and alter the configuration parameters.

Log in to the *SystemDB* of the primary instance by using the SAP HANA database interactive terminal *hdbsql* or *SAP HANA Cockpit*, and create a new user.

For example, connect to the database by using *hdbsql* in a terminal session.

```
$ sudo -i -u ${sid}adm -- hdbsql -i ${INSTNO} -d SYSTEMDB -u SYSTEM
```

Create a user.

```
CREATE USER HA_HOOK PASSWORD <Password> NO FORCE FIRST_PASSWORD_CHANGE;
```

Grant the required privileges to the user.

Grant privilege *INFILE ADMIN* to allow for changes of profile parameters.

```
GRANT INFILE ADMIN TO HA_HOOK;
```

Verify the *HA_HOOK* user.

```
$ sudo -i -u ${sid}adm -- hdbsql -d SYSTEMDB -u SYSTEM select \* from users where user_name = '\'HA_HOOK\';
```

2. Add the user credentials to the secure user store *hdbuserstore*.

On both nodes, run the following command. Use the password that you set in the previous step.

```
$ sudo -i -u ${sid}adm -- hdbuserstore SET HA_HOOK_KEY localhost:3${INSTNO}13 HA_HOOK <Password>
```

Check the update to the *hdbuserstore*.

```
$ sudo -i -u ${sid}adm -- hdbuserstore list
```

On the primary instance, test the connection with the stored user key.

```
$ sudo -i -u ${sid}adm -- hdbsql -U HA_HOOK_KEY select \* from m_inifiles;
```

Creating the hook script

Python sample files for creating hook scripts are delivered as part of the SAP HANA installation. The samples are located in directory `$DIR_INSTANCE/exe/python_support/hdb_ha_dr`.

The target directory `/hana/shared/myHooks` was already created for hook `SAPHanaSR.py`. Create a HA/DR provider hook in `/hana/shared/myHooks`. The following hook script is based on the `HADRdummy.py` sample.

On NODE2, edit the file `/hana/shared/myHooks/SAPHanaCostOptSR.py` and add the following content.

```
"""
```

```
Sample for a HA/DR hook provider.
```

```
When using your own code in here, please copy this file to location on /hana/shared outside the HANA installation.  
This file will be overwritten with each hdbupd call! To configure your own changed version of this file, please add  
to your global.ini lines similar to this:
```

```
[ha_dr_provider_<className>]
```

```

provider = <className>
path = /hana/shared/haHook
execution_order = 1

For all hooks, 0 must be returned in case of success.
"""

from __future__ import absolute_import
from hdb_ha_dr.client import HADRBase, Helper
from hdbcli import dbapi
import os, time

class SAPHanaCostOptSR(HADRBase):

    def __init__(self, *args, **kwargs):
        # delegate construction to base class
        super(SAPHanaCostOptSR, self).__init__(*args, **kwargs)

    def about(self):
        return {"provider_company" : "SAP",
                "provider_name" : "SAPHanaCostOptSR", # provider name = class name
                "provider_description" : "Handle reconfiguration event for cost-optimized system replication",
                "provider_version" : "1.0"}

    def postTakeover(self, rc, **kwargs):
        """Post takeover hook."""

        # prepared SQL statements to remove memory allocation limit and pre-load of column tables
        stmnt1 = "ALTER SYSTEM ALTER CONFIGURATION ('global.ini','SYSTEM') UNSET
('memorymanager','global_allocation_limit') WITH RECONFIGURE"
        stmnt2 = "ALTER SYSTEM ALTER CONFIGURATION ('global.ini','SYSTEM') UNSET
('system_replication','preload_column_tables') WITH RECONFIGURE

        myPort = int('3' + os.environ.get('DIR_INSTANCE')[-2:] + '15')
        myKey = self.config.get("userkey") if self.config.hasKey("userkey") else "HA_HOOK_KEY"

        self.tracer.info("%s.postTakeover method called with rc=%s" % (self.__class__.__name__, rc))
        self.tracer.info("%s.postTakeover method: userkey: %s, port: %s" % (self.__class__.__name__, myKey, myPort))

        if rc in (0, 1):
            # rc == 0: normal takeover succeeded
            # rc == 1: waiting for force takeover
            conn = dbapi.connect(userkey=myKey, address='localhost', port=myPort)
            self.tracer.info("%s: Connect using userkey %s - %s" % (self.__class__.__name__, myKey,
conn.isconnected()))
            cursor = conn.cursor()
            rc1 = cursor.execute(stmnt1)
            self.tracer.info("%s: (%s) - %s" % (self.__class__.__name__, stmnt1, rc1))
            rc2 = cursor.execute(stmnt2)
            self.tracer.info("%s: (%s) - %s" % (self.__class__.__name__, stmnt2, rc2))
            return 0
        elif rc == 2:
            # rc == 2: error, something went wrong
            return 0

```

Activating the cost optimized hook

Use the following steps to activate the cost optimized hook.

1. Stop the cluster.

On any cluster node, run the following command.

```
$ pcs cluster stop --all
```

2. Set the file ownership of the hook script.

On NODE2, run the following command.

```
$ chown -R ${sid}adm:sapsys /hana/shared/myHooks
```

3. Update the `global.ini` configuration file on NODE2 to enable the hook script.

On NODE2, run the following command to add the required parameters to the `global.ini` file.

```
$ sudo -i -u ${sid}adm -- <<EOT
    python \${DIR_INSTANCE}/exe/python_support/setParameter.py \
        -set SYSTEM/global.ini/ha_dr_provider_SAPHanaCostOptSR/provider=SAPHanaCostOptSR \
        -set SYSTEM/global.ini/ha_dr_provider_SAPHanaCostOptSR/path=/hana/shared/myHooks \
        -set SYSTEM/global.ini/ha_dr_provider_SAPHanaCostOptSR/userkey=HA_HOOK_KEY \
        -set SYSTEM/global.ini/ha_dr_provider_SAPHanaCostOptSR/execution_order=2 \
        -set SYSTEM/global.ini/trace/ha_dr_saphanacostoptsr=info
EOT
```

4. Check the content of the `global.ini` file.

```
$ cat /hana/shared/\${SID}/global/hdb/custom/config/global.ini
```

5. Verify that the hook functions.

- Restart the HANA instance on NODE2 and verify that the hook script works as expected.
- Trigger the hook with an SAP HANA takeover operation.
- Check whether the hook logged anything in the trace files.

```
$ sudo -i -u ${sid}adm -- \
    sh -c 'grep SAPHanaCostOptSR \$DIR_INSTANCE/\$VTHOSTNAME/trace/nameserver_*.trc'
```

After you verify that the hook functions, you can restart the HA cluster.

6. Start the HA cluster.

On any cluster node, run the following command.

```
$ pcs cluster start --all
```

Check the status of the cluster.

```
$ pcs status --full
```

Defining limits for SAP HANA resource usage on the secondary node

All SAP HANA systems that are running on NODE2 share the available memory of the node. Memory configuration of the secondary system SAP HANA `\${SID}` must be limited to the amount required for system replication so that the nonproduction systems can use the remaining memory.

SAP documentation [Secondary System Usage](#) describes the different scenarios and provides parameter recommendations.

The preload of column tables on the secondary system is disabled to restrict its memory consumption by setting the database configuration parameter `preload_column_tables = false`. This parameter is found in the `[system_replication]` section of the instance configuration file for SAP HANA production system on NODE2.

The `global_allocation_limit` is set in the `[memorymanager]` section to limit memory allocation for the SAP HANA production system and the nonproduction system that is running on NODE2.

On NODE2, define an environment variable with the wanted memory limit for the secondary HANA production instance.

```
$ export GLOBAL_ALLOCATION_LIMIT=<memory_size_in_mb_for_hana_secondary>
```

Then, run the following command to update the `global.ini` configuration file.

```
$ sudo -i -u ${sid}adm -- <<EOT
    python \${DIR_INSTANCE}/exe/python_support/setParameter.py \
        -set SYSTEM/global.ini/system_replication/preload_column_tables=false \
        -set SYSTEM/global.ini/memorymanager/global_allocation_limit=\$GLOBAL_ALLOCATION_LIMIT
EOT
```

Verify the configuration file.

```
$ cat /hana/shared/${SID}/global/hdb/custom/config/global.ini
```

You cannot use `hdbsql` and `ALTER SYSTEM ALTER CONFIGURATION ...` statements on the secondary, no SQL connect is possible in this state. Activate the change by using the `hdbnsutil -reconfig` command.

```
$ sudo -i -u ${sid}adm -- hdbnsutil -reconfig
```

Update the `global.ini` configuration file of the nonproduction instance to allow for the memory resource usage of the secondary.

On NODE2, define an environment variable with the wanted memory limit for the nonproduction HANA instance.

```
$ export NON_PROD_GLOBAL_ALLOCATION_LIMIT=<memory_size_in_mb_for_non_prod_hana>
```

Then, run the following command to update the `global.ini` configuration file.

```
$ sudo -i -u ${sid_np}adm -- <<EOT
  python \${DIR_INSTANCE}/exe/python_support/setParameter.py \
    -set SYSTEM/global.ini/memorymanager/global_allocation_limit=\$NON_PROD_GLOBAL_ALLOCATION_LIMIT \
    -reconfigure
EOT
```

Verify the configuration file.

```
$ cat /hana/shared/${SID_NP}/global/hdb/custom/config/global.ini
```

Run the following command to check the current database memory limit.

```
$ sudo -i -u ${sid_np}adm -- hdbccons "mm globallimit" | grep limit
```

Configuring cluster resources for the nonproduction instance

Use the following information to configure cluster resources for the nonproduction instance.

Installing the SAPInstance resource agent

The `resource-agents-sap` package includes the `SAPInstance` cluster resource agent, which is used to manage the additional nonproduction SAP HANA instance.

On NODE2, run the following command to install the resource agent.

```
$ dnf install -y resource-agents-sap
```

If needed, use `subscription-manager` to enable the `SAP NetWeaver` repository.

```
$ subscription-manager repos --enable="rhel-8-for-ppc64le-sap-netweaver-e4s-rpms"
```

Creating the cluster resource for managing the nonproduction instance

On NODE2, run the following command.

```
$ pcs resource create SAPHana_np_${SID_NP}_HDB${INSTNO_NP} SAPInstance \
  InstanceName="\${SID_NP}_HDB\${INSTNO_NP}\_\$\{NODE2\}" \
  MONITOR_SERVICES="hdbindexserver|hdbnameserver" \
  START_PROFILE="/usr/sap/\${SID_NP}/SYS/profile/\${SID_NP}_HDB\${INSTNO_NP}\_\$\{NODE2\}" \
  op start timeout=600 op stop timeout=600 op monitor interval=60 timeout=600 \
  --group group_\$\{sid_np\}_non_prod
```

If you want to assign a virtual IP address to the nonproduction instance, add a `IPaddr2` cluster resource.

```
$ pcs resource create vip_np IPaddr2 \
  ip="\${VIP_NP}" \
  --group group_\$\{sid_np\}_non_prod
```

Create a cluster constraint to prevent that the nonproduction system starts on NODE1.

```
$ pcs constraint location add loc-${sid_np}-avoid-${NODE1} \
    group_${sid_np}_non_prod ${NODE1} -INFINITY resource-discovery=never
```

When the production system assumes the *PRIMARY* role on NODE2 if a takeover occurs, the nonproduction system stops and its memory resources are released. The following cluster constraints make sure that the primary production instance and the nonproduction instance never run together on one node, and that the nonproduction instance stops before the production instance is promoted.

```
$ pcs constraint colocation add group_${sid_np}_non_prod with master SAPHana_${SID}_${INSTNO}-clone score=-INFINITY
```

```
$ pcs constraint order stop group_${sid_np}_non_prod then promote SAPHana_${SID}_${INSTNO}-clone
```

The cluster configuration is complete.

Run the following command to check the status of the defined cluster resources.

```
$ pcs status --full
```

Sample output:

```
# pcs status --full
Cluster name: SAP_PRD
Cluster Summary:
  * Stack: corosync
  * Current DC: cl-prd-2 (2) (version 2.0.5-9.el8_4.5-ba59be7122) - partition with quorum
  * Last updated: Fri Apr 28 16:38:00 2023
  * Last change: Fri Apr 28 16:37:49 2023 by hacluster via crmd on cl-prd-1
  * 2 nodes configured
  * 8 resource instances configured

Node List:
  * Online: [ cl-prd-1 (1) cl-prd-2 (2) ]

Full List of Resources:
  * res_fence_ibm_powervs (stonith:fence_ibm_powervs): Started cl-prd-2
  * Clone Set: SAPHanaTopology_PRD_00-clone [SAPHanaTopology_PRD_00]:
    * SAPHanaTopology_PRD_00 (ocf::heartbeat:SAPHanaTopology): Started cl-prd-2
    * SAPHanaTopology_PRD_00 (ocf::heartbeat:SAPHanaTopology): Started cl-prd-1
  * Clone Set: SAPHana_PRD_00-clone [SAPHana_PRD_00] (promotable):
    * SAPHana_PRD_00 (ocf::heartbeat:SAPHana): Slave cl-prd-2
    * SAPHana_PRD_00 (ocf::heartbeat:SAPHana): Master cl-prd-1
  * vip_PRD_00 (ocf::heartbeat:IPaddr2): Started cl-prd-1
  * Resource Group: group_dev_non_prod:
    * vip_np (ocf::heartbeat:IPaddr2): Started cl-prd-2
    * SAPHana_np_DEV_HDB10 (ocf::heartbeat:SAPInstance): Started cl-prd-2

Node Attributes:
  * Node: cl-prd-1 (1):
    * hana_prd_clone_state : PROMOTED
    * hana_prd_op_mode : logreplay
    * hana_prd_remoteHost : cl-prd-2
    * hana_prd_roles : 4:P:master1:master:worker:master
    * hana_prd_site : SiteA
    * hana_prd_srmode : syncmem
    * hana_prd_sync_state : PRIM
    * hana_prd_version : 2.00.070.00.1679989823
    * hana_prd_vhost : cl-prd-1
    * lpa_prd_lpt : 1682692638
    * master-SAPHana_PRD_00 : 150
  * Node: cl-prd-2 (2):
    * hana_prd_clone_state : DEMOTED
    * hana_prd_op_mode : logreplay
    * hana_prd_remoteHost : cl-prd-1
    * hana_prd_roles : 4:S:master1:master:worker:master
    * hana_prd_site : SiteB
    * hana_prd_srmode : syncmem
    * hana_prd_sync_state : SOK
```

```

* hana_prd_version      : 2.00.070.00.1679989823
* hana_prd_vhost        : cl-prd-2
* lpa_prd_lpt           : 30
* master-SAPHana_PRD_00 : 100

```

Migration Summary:

Tickets:

PCSD Status:

```

cl-prd-1: Online
cl-prd-2: Online

```

Daemon Status:

```

corosync: active/disabled
pacemaker: active/disabled
pcsd: active/enabled

```

Run the following command to check the defined constraints.

Sample output:

```

# pcs constraint --full
Location Constraints:
  Resource: group_dev_non_prod
    Disabled on:
      Node: cl-prd-1 (score:-INFINITY) (resource-discovery=never) (id:loc-dev-avoid-cl-prd-1)
Ordering Constraints:
  start SAPHanaTopology_PRD_00-clone then start SAPHana_PRD_00-clone (kind:Mandatory) (non-symmetrical) (id:order-SAPHanaTopology_PRD_00-clone-SAPHana_PRD_00-clone-mandatory)
  stop group_dev_non_prod then promote SAPHana_PRD_00-clone (kind:Mandatory) (id:order-group_dev_non_prod-SAPHana_PRD_00-clone-mandatory)
Colocation Constraints:
  vip_PRD_00 with SAPHana_PRD_00-clone (score:2000) (rsc-role:Started) (with-rsc-role:Master) (id:colocation-vip_PRD_00-SAPHana_PRD_00-clone-2000)
  group_dev_non_prod with SAPHana_PRD_00-clone (score:-INFINITY) (rsc-role:Started) (with-rsc-role:Master) (id:colocation-group_dev_non_prod-SAPHana_PRD_00-clone-INFINITY)
Ticket Constraints:

```

Enabling the automated registration of the secondary instance

You need to set the parameter `AUTOMATED_REGISTER` according to your operational requirements. If you want to keep the ability to revert to the state of the previous primary SAP HANA instance, then `AUTOMATED_REGISTER=false` avoids an automatic registration of the previous primary as a new secondary.

If you experience an issue with the data after a takeover that was triggered by the cluster, you can manually revert if `AUTOMATED_REGISTER` is set to `false`.

If `AUTOMATED_REGISTER` is set to `true`, the previous primary SAP HANA instance automatically registers as secondary, and cannot be activated on its previous history. The advantage of `AUTOMATED_REGISTER=true` is that high-availability is automatically reestablished after the failed node reappears in the cluster.

For now, it is recommended to keep `AUTOMATED_REGISTER` on default value `false` until the cluster is fully tested and that you verify that the failover scenarios work as expected.

 **Tip:** The `pcs resource update` command is used to modify resource attributes and `pcs resource update SAPHana_${SID}_${INSTNO} AUTOMATED_REGISTER=true` sets the attribute to `true`.

Testing the SAP HANA System Replication cluster

It is vital to thoroughly test the cluster configuration to make sure that the cluster is working correctly. The following information provides a few sample failover test scenarios, but is not a complete list of test scenarios.

For example, the description of each test case includes the following information.

- Which component is being tested
- Description of the test

- Prerequisites and the initial state before you start the failover test
- Test procedure
- Expected behavior and results
- Recovery procedure

Test1 - Testing the failure of the primary database instance

Use the following information to test the failure of the primary database instance.

Test1 - Description

Simulate a crash of the primary HANA database instance that is running on NODE1.

Test1 - Prerequisites

- A functional two-node RHEL HA Add-On cluster for HANA system replication.
- Both cluster nodes are active.
- Cluster is started on NODE1 and NODE2.
- Cluster Resource `SAPHana_${SID}_${INSTNO}` is configured with `AUTOMATED_REGISTER=false`.
- Check SAP HANA System Replication status:
 - The primary SAP HANA database is running on NODE1.
 - The secondary SAP HANA database is running on NODE2.
 - HANA System Replication is activated and in sync.
- The secondary SAP HANA database on NODE2 is running with reduced memory configuration.
 - The `global_allocation_limit` is reduced.
 - Preload of column tables is disabled (`preload_column_tables = false`).
- A nonproduction SAP HANA system `_${SID}_NP` is running on NODE2.

Test1 - Test procedure

Crash SAP HANA primary by sending a SIGKILL signal as user `_${sid}adm`.

On NODE1, run the following command.

```
$ sudo -i -u ${sid}adm -- HDB kill-9
```

Test1 - Expected behavior

- SAP HANA primary instance on NODE1 crashes.
- The cluster detects the stopped primary HANA database and marks the resource as `failed`.
- The cluster promotes the secondary HANA database on NODE2 to take over as new primary.
 - The cluster stops the nonproduction database `_${SID}_NP` on NODE2.
 - During activation, the `global_allocation_limit` and `preload_column_tables` parameters are reset to default.
- The cluster releases the virtual IP address on NODE1, and acquires it on the new primary on NODE2.
- If an application, such as SAP NetWeaver, is connected to a tenant database of SAP HANA, the application automatically reconnects to the new primary.

On NODE2, run the following commands to check that the `global_allocation_limit` and `preload_column_tables` are unset.

```
$ sudo -i -u ${sid}adm -- hdbcons "mm globallimit" | grep limit
```

```
$ grep -E "global_allocation_limit|preload_column_tables" \
/hana/shared/${SID}/global/hdb/custom/config/global.ini
```

Test1 - Recovery procedure

As the cluster resource `SAPHana_${SID}_${INSTNO}` is configured with `AUTOMATED_REGISTER=false`, the cluster doesn't restart the failed HANA database, and doesn't register it against the new primary. The status on the new primary (NODE2) shows the secondary in status

'CONNECTION TIMEOUT'.

On NODE1, run the following commands to register the previous primary as new secondary.

```
$ sudo -i -u ${sid}adm -- <<EOT
    hdbnsutil -sr_register \
        --name=${DC1} \
        --remoteHost=${NODE2} \
        --remoteInstance=${INSTNO} \
        --replicationMode=sync \
        --operationMode=logreplay \
        --online
EOT
```

Verify the system replication status.

```
$ sudo -i -u ${sid}adm -- <<EOT
    hdbnsutil -sr_state
    HDBSettings.sh systemReplicationStatus.py
EOT
```

On NODE1, run the following command to start the cluster node.

```
$ pcs cluster start
```

The new secondary instance restarts and shows up in status synced (`SOK`).

```
$ pcs status --full
```

Configure cluster resource `SAPHana_${SID}_${INSTNO}` with `AUTOMATED_REGISTER=true`.

On NODE1, run the following command.

```
$ pcs resource update SAPHana_${SID}_${INSTNO} AUTOMATED_REGISTER=true
```

```
$ pcs resource config SAPHana_${SID}_${INSTNO}
```

Test2 - Testing the manual move of SAPHana resource to another node

Use the following information to test the manual move of SAPHana resource to another node.

Test2 - Description

Use cluster commands to move the primary instance back to the other node.

Test2 - Prerequisites

- A functional two-node RHEL HA Add-On cluster for HANA system replication.
- Both cluster nodes are active.
- Cluster is started on NODE1 and NODE2.
- Cluster Resource `SAPHana_${SID}_${INSTNO}` is configured with `AUTOMATED_REGISTER=true`.
- Check SAP HANA System Replication status:
 - The primary SAP HANA database is running on NODE2.
 - The secondary SAP HANA database is running on NODE1.
 - HANA System Replication is activated and in sync.
- The nonproduction SAP HANA system `_${SID}_NP` is stopped on NODE2.

Test2 - Test Preparation

Unmanage the cluster resource for the nonproduction SAP HANA system to prevent that it starts when the memory resources of the secondary are not restricted.

On NODE1, run the following command.

```
$ pcs resource unmanage group_${sid_np}_non_prod
```

Test2 - Test Procedure

On NODE1, run the following command to move the SAP HANA primary back to NODE1.

```
$ pcs resource move SAPHana_${SID}_${INSTNO}-clone
```

Test2 - Expected behavior

- The cluster creates a location constraint to move the resource.
- The cluster triggers a takeover to the secondary HANA database on NODE1.
- If an application, such as SAP NetWeaver, is connected to a tenant database of SAP HANA, the application automatically reconnects to the new primary.
- The resource of the nonproduction SAP HANA system `_${SID}_NP` is in the *unmanaged* state and isn't started automatically.

Test2 - Recovery procedure

Several steps need to be followed to reestablish the complete HA scenario.

1. Wait until the primary HANA instance is active. Then, reduce the memory footprint of the secondary.

On NODE2, run the following commands to reduce the memory.

```
$ export GLOBAL_ALLOCATION_LIMIT=<size_in_mb_for_hana_secondary>

$ sudo -i -u ${sid}adm -- <<EOT
    python \${DIR_INSTANCE}/exe/python_support/setParameter.py \
        -set SYSTEM/global.ini/system_replication/preload_column_tables=false \
        -set SYSTEM/global.ini/memorymanager/global_allocation_limit=\$GLOBAL_ALLOCATION_LIMIT
EOT
```

2. Remove the location constraint, which triggers the start of the secondary instance.

```
$ pcs resource clear SAPHana_${SID}_${INSTNO}-clone
```

Verify that the constraint is cleared.

```
$ pcs constraint
```

Check the cluster status.

```
$ pcs status --full
```

3. On NODE2, run the following commands to check that the `global_allocation_limit` and `preload_column_tables` are set.

```
$ sudo -i -u ${sid}adm -- hdbcons "mm globallimit" | grep limit

$ grep -E "global_allocation_limit|preload_column_tables" \
    /hana/shared/${SID}/global/hdb/custom/config/global.ini
```

4. Reactivate the resource for the nonproduction SAP HANA system.

On NODE2, run the following command.

```
$ pcs resource manage group_${sid_np}_non_prod
```

The resource of the nonproduction SAP HANA system `_${SID}_NP` is *managed* and the nonproduction system starts on NODE2.

```
$ pcs status --full
```

Test3 - Testing failure of node that is running the primary database

Use the following information to test the failure of node that is running the primary database.

Test3 - Description

Simulate a crash of the node that is running the primary HANA database.

Test3 - Prerequisites

- A functional two-node RHEL HA Add-On cluster for HANA system replication.
- Both cluster nodes are active.
- Cluster is started on NODE1 and NODE2.
- Cluster Resource `SAPHana_${SID}_${INSTNO}` is configured with `AUTOMATED_REGISTER=true`.
- Check SAP HANA System Replication status:
 - The primary SAP HANA database is running on NODE1.
 - The secondary SAP HANA database is running on NODE2.
 - HANA System Replication is activated and in sync.
- The secondary SAP HANA database on NODE2 is running with reduced memory configuration.
 - The `global_allocation_limit` is reduced.
 - Preload of column tables is disabled (`preload_column_tables = false`).
- A nonproduction SAP HANA system `_${SID}_NP` is running on NODE2.

Test3 - Test procedure

Crash primary on NODE1 by sending a `crash` system request.

On NODE1, run the following command.

```
$ sync; echo c > /proc/sysrq-trigger
```

Test3 - Expected behavior

- NODE1 shuts down.
- The cluster detects the failed node and sets its state to `OFFLINE`.
- The cluster promotes the secondary HANA database on NODE2 to take over as new primary.
 - The cluster stops the nonproduction database `_${SID}_NP` on NODE2.
 - During activation, the `global_allocation_limit` and `preload_column_tables` parameters of SAP HANA `_${SID}` are reset.
- The cluster acquires the virtual IP address on NODE2 on the new primary.
- If an application, such as SAP NetWeaver, is connected to a tenant database of SAP HANA, the application automatically reconnects to the new primary.

Test3 - Recovery procedure

Log in to the IBM Cloud® console and start NODE1. Wait until NODE1 is available again, then restart the cluster framework.

On NODE1, run the following command.

```
$ pcs cluster start
```

```
$ pcs status --full
```

As cluster resource `SAPHana_${SID}_${INSTNO}` is configured with `AUTOMATED_REGISTER=true`, SAP HANA restarts when NODE1 joins the cluster and the former primary is registered as secondary.

Then, rerun the steps in [Test2 - Test the manual move of SAPHana resource to another node](#) to revert to the initial situation.

Test4 - Testing failure of the secondary database instance

Use the following information to test the failure of the secondary database instance.

Test4 - Description

Simulate a crash of the secondary HANA database.

Test4 - Prerequisites

- A functional two-node RHEL HA Add-On cluster for HANA system replication.
- Both nodes active.
- Cluster is started on NODE1 and NODE2.
- Cluster Resource `SAPHana_${SID}_${INSTNO}` is configured with `AUTOMATED_REGISTER=true`.
- Check SAP HANA System Replication status:
 - The primary SAP HANA database is running on NODE1.
 - The secondary SAP HANA database is running on NODE2.
 - HANA System Replication is activated and sync.

Test4 - Test Procedure

Crash SAP HANA secondary by sending a SIGKILL signal as user `${sid}adm`.

On NODE2, run the following command.

```
$ sudo -i -u ${sid}adm -- HDB kill-9
```

Test4 - Expected behavior

- SAP HANA secondary on NODE2 crashes.
- The cluster detects the stopped secondary HANA database and marks the resource as `failed`.
- The cluster restarts the secondary HANA database.
- The cluster detects that the system replication is in sync again.

Test4 - Recovery Procedure

Wait until the secondary HANA instance starts and synchronized again (`SOK`), then cleanup the failed resource actions as shown in `pcs status`.

On NODE2, run the following command.

```
$ pcs resource refresh SAPHana_${SID}_${INSTNO}
```

```
$ pcs status --full
```

Configuring SAP HANA active/active (read enabled) system replication in a Red Hat Enterprise Linux High Availability Add-On cluster

The following information describes the configuration of a Red Hat Enterprise Linux (RHEL) High Availability Add-On cluster for managing *SAP HANA Active-Active (Read Enabled) System Replication*. The cluster uses virtual server instances in [IBM® Power® Virtual Server](#) as cluster nodes.

In an *Active/Active (read enabled)* configuration, SAP HANA system replication allows read access to the database content on the secondary system.



Note: This information is intended for architects and specialists that are planning a high-availability deployment of SAP HANA on Power Virtual Server.

Before you begin

Review the general requirements, product documentation, support articles, and SAP notes listed in [Implementing high availability for SAP](#)

[applications on IBM Power Virtual Server References](#).

Prerequisites

- A Red Hat High Availability cluster is deployed on two virtual server instances in Power Virtual Server.
 - Install and set up the RHEL HA Add-On cluster according to [Implementing a Red Hat Enterprise Linux High Availability Add-On cluster](#).
 - Configure and verify fencing as described in the preceding document.
- The virtual server instances need to fulfill hardware and resource requirements for the SAP HANA systems in scope. Follow the guidelines in the [Planning your deployment](#) document.
- The hostnames of the virtual server instances must meet the SAP HANA requirement.
- SAP HANA is installed on both virtual server instances and SAP HANA System Replication is configured. The installation of SAP HANA and setup of SAP HANA System Replication is not specific to the Power Virtual Server environment, and you need to follow the standard procedures.

Setting up the Active/Active (read enabled) scenario

The Active/Active (read enabled) system replication scenario is an extension of the setup that is described in [Configuring SAP HANA scale-up system replication in a Red Hat Enterprise Linux High Availability Add-On cluster](#).

Complete the setup for the production system System Replication cluster before you continue with the following steps.

Changing the system replication operation mode to Active/Active (read enabled)

On the node that is running the secondary instance, run the following command to change the operation mode.

1. Put the cluster in maintenance mode.

```
$ pcs property set maintenance-mode=true
```

2. Stop the secondary SAP HANA instance.

```
$ sudo -i -u ${sid}adm -- \
  HDB stop
```

3. Change the system replication operation mode.

```
$ sudo -i -u ${sid}adm -- \
  hdbnsutil -sr_changeOperationMode --mode=logreplay_readaccess
```

4. Start the secondary SAP HANA instance.

```
$ sudo -i -u ${sid}adm -- \
  HDB start
```

5. Remove the cluster from maintenance mode.

```
$ pcs property set maintenance-mode=false
```

Configuring cluster resources for an Active/Active (read enabled) scenario

Use the following information to configure the additional cluster resources that are required for an Active/Active (read enabled) scenario.

Creating a secondary virtual IP address resource

Review the information in [Reserving virtual IP addresses](#) and reserve a virtual IP address for the secondary.

Use the reserved IP address to create a virtual IP address resource. This virtual IP address allows clients to connect to the secondary HANA instance for read-only queries.

On a cluster node, assign the reserved IP address to a `VIP_SECONDARY` environment variable and create the virtual IP address cluster resource by running the following commands.

```
$ export VIP_SECONDARY=<reserved IP address for SAP HANA secondary>
```

```
$ echo $VIP_SECONDARY  
  
$ pcs resource create vip_s_${SID}_${INSTNO} IPaddr2 ip=$VIP_SECONDARY
```

Check the configured virtual IP address and the cluster status.

```
$ pcs resource config vip_s_${SID}_${INSTNO}  
  
$ pcs status --full
```

Creating location constraints for the secondary virtual IP address

Create a cluster constraint to make sure that the secondary virtual IP address is placed on the cluster node that is running the secondary instance.

On a cluster node, run the following commands.

```
$ pcs constraint location vip_s_${SID}_${INSTNO} rule \  
  score=INFINITY hana_${sid}_sync_state eq SOK \  
  and hana_${sid}_roles eq 4:S:master1:master:worker:master  
  
$ pcs constraint location vip_s_${SID}_${INSTNO} rule \  
  score=2000 hana_${sid}_sync_state eq PRIM \  
  and hana_${sid}_roles eq 4:P:master1:master:worker:master
```

These location constraints establish the following behavior for the second virtual IP resource:

- If both SAP HANA primary and SAP HANA secondary are available, and SAP HANA system replication state is **SOK**, then the secondary virtual IP address is assigned to the node where SAP HANA secondary is active.
- If the SAP HANA secondary node is not available or SAP HANA system replication state is not **SOK**, then the secondary virtual IP is assigned to the node where SAP HANA primary is active. When the SAP HANA secondary becomes available and the SAP HANA system replication state is **SOK** again, the second virtual IP address moves back to the node where the SAP HANA secondary is active.
- If SAP HANA primary or the node where it is running becomes unavailable then the SAP HANA secondary takes over the primary role. The second virtual IP remains on the node until the other node turns into SAP HANA secondary role and SAP HANA system replication state is **SOK** again.

This behavior maximizes the time that the secondary virtual IP resource is assigned to a node where a healthy SAP HANA instance is running.

The cluster configuration for the Active/Active (read enabled) scenario is complete.

Checking the cluster configuration

On a cluster node, run the following command to check the status of the cluster resources.

```
$ pcs status --full
```

Sample output:

```
# pcs status --full  
Cluster name: H4S_cluster  
Cluster Summary:  
  * Stack: corosync  
  * Current DC: cl-h4s-1 (1) (version 2.0.5-9.el8_4.5-ba59be7122) - partition with quorum  
  * Last updated: Mon Jul 31 11:46:11 2023  
  * Last change: Mon Jul 31 11:44:34 2023 by root via crm_attribute on cl-h4s-1  
  * 2 nodes configured  
  * 7 resource instances configured  
  
Node List:  
  * Online: [ cl-h4s-1 (1) cl-h4s-2 (2) ]  
  
Full List of Resources:  
  * res_fence_ibm_powervs (stonith:fence_ibm_powervs): Started cl-h4s-1  
  * vip_H4S_00_primary (ocf::heartbeat:IPaddr2): Started cl-h4s-1  
  * Clone Set: SAPHanaTopology_H4S_00-clone [SAPHanaTopology_H4S_00]:
```

```

* SAPHanaTopology_H4S_00 (ocf::heartbeat:SAPHanaTopology): Started cl-h4s-2
* SAPHanaTopology_H4S_00 (ocf::heartbeat:SAPHanaTopology): Started cl-h4s-1
* Clone Set: SAPHana_H4S_00-clone [SAPHana_H4S_00] (promotable):
  * SAPHana_H4S_00 (ocf::heartbeat:SAPHana): Slave cl-h4s-2
  * SAPHana_H4S_00 (ocf::heartbeat:SAPHana): Master cl-h4s-1
* vip_s_H4S_00 (ocf::heartbeat:IPAddr2): Started cl-h4s-2

Node Attributes:
* Node: cl-h4s-1 (1):
  * hana_h4s_clone_state : PROMOTED
  * hana_h4s_op_mode : logreplay_readaccess
  * hana_h4s_remoteHost : cl-h4s-2
  * hana_h4s_roles : 4:P:master1:master:worker:master
  * hana_h4s_site : SiteA
  * hana_h4s_srmode : syncmem
  * hana_h4s_sync_state : PRIM
  * hana_h4s_version : 2.00.070.00.1679989823
  * hana_h4s_vhost : cl-h4s-1
  * lpa_h4s_lpt : 1690796675
  * master-SAPHana_H4S_00 : 150
* Node: cl-h4s-2 (2):
  * hana_h4s_clone_state : DEMOTED
  * hana_h4s_op_mode : logreplay_readaccess
  * hana_h4s_remoteHost : cl-h4s-1
  * hana_h4s_roles : 4:S:master1:master:worker:master
  * hana_h4s_site : SiteB
  * hana_h4s_srmode : syncmem
  * hana_h4s_sync_state : SOK
  * hana_h4s_version : 2.00.070.00.1679989823
  * hana_h4s_vhost : cl-h4s-2
  * lpa_h4s_lpt : 30
  * master-SAPHana_H4S_00 : 100

```

Migration Summary:

Tickets:

PCSD Status:

```

cl-h4s-1: Online
cl-h4s-2: Online

```

Daemon Status:

```

corosync: active/disabled
pacemaker: active/disabled
pcsd: active/enabled

```

On a cluster node, run the following command to check the defined constraints.

```
$ pcs constraint --full
```

Sample output:

```

# pcs constraint --full
Location Constraints:
Resource: vip_s_H4S_00
  Constraint: location-vip_s_H4S_00
    Rule: boolean-op=and score=INFINITY (id:location-vip_s_H4S_00-rule)
      Expression: hana_h4s_sync_state eq SOK (id:location-vip_s_H4S_00-rule-expr)
      Expression: hana_h4s_roles eq 4:S:master1:master:worker:master (id:location-vip_s_H4S_00-rule-expr-1)
  Constraint: location-vip_s_H4S_00-1
    Rule: boolean-op=and score=2000 (id:location-vip_s_H4S_00-1-rule)
      Expression: hana_h4s_sync_state eq PRIM (id:location-vip_s_H4S_00-1-rule-expr)
      Expression: hana_h4s_roles eq 4:P:master1:master:worker:master (id:location-vip_s_H4S_00-1-rule-expr-1)
Ordering Constraints:
  promote SAPHana_H4S_00-clone then start vip_H4S_00_primary (kind:Mandatory) (id:order-SAPHana_H4S_00-clone-vip_H4S_00_primary-mandatory)
  start SAPHanaTopology_H4S_00-clone then start SAPHana_H4S_00-clone (kind:Mandatory) (non-symmetrical) (id:order-SAPHanaTopology_H4S_00-clone-SAPHana_H4S_00-clone-mandatory)
Colocation Constraints:
  vip_H4S_00_primary with SAPHana_H4S_00-clone (score:2000) (rsc-role:Started) (with-rsc-role:Master) (id:colocation-

```

vip_H4S_00_primary-SAPHana_H4S_00-clone-2000)

Ticket Constraints:

Checking access to the read enabled secondary SAP HANA instance

You can use SAP HANA system replication *Active/Active (read enabled)* to connect to the secondary system for improved overall performance. Two connection methods are available to access the read enabled secondary HANA instance:

- Explicit read-only connection The application opens an explicit connection to the secondary HANA instance.
- Hint-based statement routing An application, for example SAP S/4HANA, opens a connection to the primary HANA instance. On this connection, SQL statements with system replication-specific hints are first prepared, and then executed. During their execution, the SQL statements are automatically routed to the secondary system and processed there. For more information about hints, see the [SAP HANA SQL and System Views Reference Guide](#).

Set the following two environment variables to the virtual IP addresses for the SAP HANA primary and secondary.

```
export VIP_PRIMARY=<virtual IP address of SAP HANA primary>
export VIP_SECONDARY=<virtual IP address of SAP HANA secondary>
```

The commands in the following two sections prompt for the password of the SAP HANA **SYSTEM** user. The command output shows the hostname and the IP addresses of the SAP HANA system that ran the SQL statement.

Checking access by using an explicit read-only connection

Verify the connection to the secondary instance by using an explicit read-only connection.

On a cluster node, run the following command.

```
$ sudo -i -u ${sid}adm -- \
    hdbsql -n $VIP_SECONDARY -i $INSTNO -d SYSTEMDB -u SYSTEM \
    "select * from m_host_information \
     where key = 'net_hostnames' or key = 'net_ip_addresses'"
```

The sample output shows that the statement ran on the SAP HANA secondary.

```
HOST,KEY,VALUE
"cl-h4s-2","net_hostnames","cl-h4s-2"
"cl-h4s-2","net_ip_addresses","10.40.10.132,10.40.10.211"
2 rows selected (overall time 7518 usec; server time 291 usec)
```

Checking access by using hint-based statement routing

Verify the connection to the secondary instance by using the hint-based statement routing.

1. Run a connection test by using an explicit connection to the SAP HANA primary without an SQL hint.

On a cluster node, run the following command.

```
$ sudo -i -u ${sid}adm -- \
    hdbsql -n $VIP_PRIMARY -i $INSTNO -d SYSTEMDB -u SYSTEM \
    "select * from m_host_information \
     where key = 'net_hostnames' or key = 'net_ip_addresses'"
```

The sample output shows that the statement ran on the SAP HANA primary.

```
HOST,KEY,VALUE
"cl-h4s-1","net_hostnames","cl-h4s-1"
"cl-h4s-1","net_ip_addresses","10.40.10.162,10.40.10.201"
2 rows selected (overall time 5239 usec; server time 361 usec)
```

2. Run a connection test by using an explicit connection to the SAP HANA primary and the **result_lag** SQL hint.

```
$ sudo -i -u ${sid}adm -- \
    hdbsql -n $VIP_PRIMARY -i $INSTNO -d SYSTEMDB -u SYSTEM \
    "select * from m_host_information \\"
```

```
where key = 'net_hostnames' or key = 'net_ip_addresses' \
with hint(result_lag('hana_sr'))"
```

The sample output shows that the statement ran on the SAP HANA secondary.

```
HOST,KEY,VALUE
"cl-h4s-2","net_hostnames","cl-h4s-2"
"cl-h4s-2","net_ip_addresses","10.40.10.132,10.40.10.211"
2 rows selected (overall time 40.722 msec; server time 16.428 msec)
```

Enabling the automated registration of the secondary instance

You need to set the parameter `AUTOMATED_REGISTER` according to your operational requirements. If you want to keep the ability to revert to the state of the previous primary SAP HANA instance, then `AUTOMATED_REGISTER=false` avoids an automatic registration of the previous primary as a new secondary.

If you experience an issue with the data after a takeover that was triggered by the cluster, you can manually revert if `AUTOMATED_REGISTER` is set to `false`.

If `AUTOMATED_REGISTER` is set to `true`, the previous primary SAP HANA instance automatically registers as secondary, and cannot be activated on its previous history. The advantage of the setting `AUTOMATED_REGISTER=true` is that high-availability automatically reestablishes after the failed node reappears in the cluster.

For now, it is recommended to keep `AUTOMATED_REGISTER` on default value `false` until the cluster is fully tested and that you verify that the failover scenarios work as expected.

 **Tip:** The `pcs resource update` command is used to modify resource attributes and `pcs resource update SAPHana_${SID}_${INSTNO} AUTOMATED_REGISTER=true` sets the attribute to `true`.

Testing SAP HANA System Replication cluster

It is important to thoroughly test the cluster configuration to make sure that the cluster is working correctly. The following information provides a few sample failover test scenarios, but is not a complete list of test scenarios.

For example, the description of each test case includes the following information.

- Component that is being tested
- Description of the test
- Prerequisites and the cluster state before you start the failover test
- Test procedure
- Expected behavior and results
- Recovery procedure

Test1 - Testing failure of the primary database instance

Use the following information to test the failure of the primary database instance.

Test1 - Description

Simulate a crash of the primary SAP HANA database instance that is running on NODE1.

Test1 - Prerequisites

- A functional two-node RHEL HA Add-On cluster for SAP HANA system replication.
- Both cluster nodes are active.
- Cluster that is started on NODE1 and NODE2.
- Cluster Resource `SAPHana_${SID}_${INSTNO}` that is configured with `AUTOMATED_REGISTER=false`.
- Check SAP HANA System Replication status:
 - Primary SAP HANA database is running on NODE1
 - Secondary SAP HANA database is running on NODE2
 - SAP HANA System Replication is activated and in sync

Test1 - Test procedure

Crash SAP HANA primary by sending a SIGKILL signal as the user `${sid}adm`.

On NODE1, run the following command.

```
$ sudo -i -u ${sid}adm -- HDB kill-9
```

Test1 - Expected behavior

- SAP HANA primary instance on NODE1 crashes.
- The cluster detects the stopped primary SAP HANA database and marks the resource as `failed`.
- The cluster promotes the secondary SAP HANA database on NODE2 to take over as the new primary.
- The cluster releases the virtual IP address on NODE1, and acquires it on the new primary on NODE2.
- After the takeover, the secondary SAP HANA instance is unavailable and the secondary virtual IP address stays on NODE2.
- If an application, such as SAP NetWeaver, is connected to a tenant database of SAP HANA, the application automatically reconnects to the new primary.

Test1 - Recovery procedure

As the cluster resource `SAPHana_${SID}_${INSTNO}` is configured with `AUTOMATED_REGISTER=false`, the cluster doesn't restart the failed SAP HANA database, and doesn't register it against the new primary. Which means that the status on the new primary (NODE2) also shows the secondary in status 'CONNECTION TIMEOUT'.

To reregister the previous primary as a new secondary use the following commands.

On NODE1, run the following command.

```
$ sudo -i -u ${sid}adm -- \
  hdbnsutil -sr_register \
  --name=${DC1} \
  --remoteHost=${NODE2} \
  --remoteInstance=00 \
  --replicationMode=sync \
  --operationMode=logreplay_readaccess \
  --online
```

Verify the system replication status:

```
$ sudo -i -u ${sid}adm -- \
  hdbnsutil -sr_state
```

On a cluster node, run the following command to refresh the cluster resource. This command starts the secondary instance.

```
$ pcs resource refresh SAPHana_${SID}_${INSTNO}
```

When the secondary reaches the synced state (`OK`), the secondary virtual IP address moves to NODE1.

On a cluster node, run the following command to check the cluster status.

```
$ pcs status --full
```

Test2 - Testing failure of the node that is running the primary database

Use the following information to test the failure of the node that is running the primary database.

Test2 - Description

Simulate a crash of the node that is running the primary SAP HANA database.

Test2 - Preparation

Make sure that the Cluster Resource `SAPHana_${SID}_${INSTNO}` is configured with `AUTOMATED_REGISTER=true`.

On NODE1, run the following command.

```
$ pcs resource update SAPHana_${SID}_${INSTNO} AUTOMATED_REGISTER=true
```

Verify the `AUTOMATED_REGISTER` setting in the resource configuration.

```
$ pcs resource config SAPHana_${SID}_${INSTNO} | grep Attributes
```

Test2 - Prerequisites

- A functional two-node RHEL HA Add-On cluster for SAP HANA system replication.
- Both nodes are active.
- Cluster is started on NODE1 and NODE2.
- Check SAP HANA System Replication status.
 - Primary SAP HANA database is running on NODE2
 - Secondary SAP HANA database is running on NODE1
 - SAP HANA System Replication is activated and in sync
 - Secondary virtual IP address is active on NODE1

Test2 - Test procedure

Crash primary on NODE2 by sending a `crash` system request.

On NODE2, run the following command.

```
$ sync; echo c > /proc/sysrq-trigger
```

Test2 - Expected behavior

- NODE2 shuts down.
- The cluster detects the failed node and sets its state to `OFFLINE`.
- The cluster promotes the secondary SAP HANA database on NODE1 to take over as the new primary.
- The cluster acquires the virtual IP address on NODE1 on the new primary.
- After the takeover, the secondary SAP HANA instance is unavailable and the secondary virtual IP address stays on NODE1.
- If an application, such as SAP NetWeaver, is connected to a tenant database of SAP HANA, the application automatically reconnects to the new primary.

Test2 - Recovery procedure

Log in to the IBM Cloud® Console and start the NODE2 instance. Wait until NODE2 is available again, then restart the cluster framework.

On NODE2, run the following command.

```
$ pcs cluster start
```

```
$ pcs status --full
```

As a cluster resource `SAPHana_${SID}_${INSTNO}` is configured with `AUTOMATED_REGISTER=true`, SAP HANA restarts when NODE2 rejoins the cluster and the former primary reregisters as a secondary. When the secondary reaches the synced state (`SOK`), the secondary virtual IP address moves to NODE2.

Test3 - Testing the failure of the secondary database instance

Use the following information to test the failure of the secondary database instance.

Test3 - Description

Simulate a crash of the secondary SAP HANA database.

Test3 - Prerequisites

- A functional two-node RHEL HA Add-On cluster for SAP HANA system replication.
- Both nodes are active.
- Cluster is started on NODE1 and NODE2.
- Cluster Resource `SAPHana_${SID}_${INSTNO}` is configured with `AUTOMATED_REGISTER=true`.
- Check SAP HANA System Replication status:
 - Primary SAP HANA database is running on NODE1
 - Secondary SAP HANA database is running on NODE2
 - SAP HANA System Replication is activated and in sync
 - Secondary virtual IP address is active on NODE2

Test3 - Test procedure

Crash SAP HANA secondary by sending a SIGKILL signal as the user `${sid}adm`.

On NODE2, run the following command.

```
$ sudo -i -u ${sid}adm -- HDB kill-9
```

Test3 - Expected behavior

- SAP HANA secondary on NODE2 crashes.
- The cluster detects the stopped secondary SAP HANA database and marks the resource as `failed`.
- The cluster moves the secondary virtual IP address to NODE1.
- The cluster restarts the secondary SAP HANA database.
- The cluster detects that the system replication is in sync again.
- The cluster moves the secondary virtual IP address back to NODE2.

Test3 - Recovery procedure

Wait until the secondary SAP HANA instance starts and syncs again (`SOK`), then cleanup the failed resource actions as shown in `pcs status`.

On a cluster node, run the following commands.

```
$ pcs resource refresh SAPHana_${SID}_${INSTNO}
```

```
$ pcs status --full
```

Test4 - Testing the manual move of a SAPHana resource to another node

Use the following information to test the manual move of a SAPHana resource to another node.

Test4 - Description

Use cluster commands to move the primary instance to the other node for maintenance purposes.

Test4 - Prerequisites

- A functional two-node RHEL HA Add-On cluster for SAP HANA system replication.
- Both nodes are active.
- Cluster is started on NODE1 and NODE2.
- Cluster Resource `SAPHana_${SID}_${INSTNO}` is configured with `AUTOMATED_REGISTER=true`.
- Check SAP HANA System Replication status:
 - Primary SAP HANA database is running on NODE1
 - Secondary SAP HANA database is running on NODE2
 - SAP HANA System Replication is activated and in sync
 - Secondary virtual IP address is active on NODE2

Test4 - Test procedure

Move SAP HANA primary to other node by using the `pcs resource move` command.

On a cluster node, run the following command.

```
$ pcs resource move SAPHana_${SID}_${INSTNO}-clone
```

Sample output:

```
# pcs resource move SAPHana_H4S_00-clone
Warning: Creating location constraint 'cli-ban-SAPHana_H4S_00-clone-on-cl-hdb-1' with a score of -INFINITY for resource
SAPHana_H4S_00-clone on cl-hdb-1.
    This will prevent SAPHana_H4S_00-clone from running on cl-hdb-1 until the constraint is removed
    This will be the case even if cl-hdb-1 is the last node in the cluster
```

Test4 - Expected behavior

- The cluster creates location constraints to move the resource.
- The cluster triggers a takeover to the secondary SAP HANA database.
- The secondary virtual IP address stays on NODE2.
- If an application, such as SAP NetWeaver, is connected to a tenant database of SAP HANA, the application automatically reconnects to the new primary.

Test4 - Recovery procedure

The automatically created location constraints must be removed to allow automatic failover in the future.

Wait until the primary SAP HANA instance is active and remove the constraints.

On a cluster node, run the following command.

```
$ pcs constraint
```

```
$ pcs resource clear SAPHana_${SID}_${INSTNO}-clone
```

```
$ pcs constraint
```

The cluster registers and starts the SAP HANA database as a new secondary instance. After system replication status is in sync again (`SOK`), the cluster moves the secondary virtual IP address to NODE1.

```
$ pcs status --full
```

Configuring SAP HANA multitier system replication in a Red Hat Enterprise Linux High Availability Add-On cluster

The following information describes the configuration of a Red Hat Enterprise Linux (RHEL) High Availability Add-On cluster for managing *SAP HANA system replication* in a multitier replication scenario. The cluster uses virtual server instances in [IBM® Power® Virtual Server](#) as cluster nodes.

You can connect multiple systems in an SAP HANA multitier system replication topology to achieve a higher level of availability. The tertiary SAP HANA instance runs on a third virtual server instance in IBM Power Virtual Server in another workspace. The resource agents for SAP HANA in the Red Hat Enterprise Linux 8 (RHEL) HA add-on require that the tertiary SAP HANA instance is managed manually. The tertiary SAP HANA system is installed on a virtual server instance outside the cluster. After a takeover in the cluster, the tertiary SAP HANA instance must be reregistered manually.

In a *multitier system replication* scenario, a tertiary SAP HANA system runs on a third virtual server instance. The third virtual server instance is deployed in a different IBM Power Virtual Server workspace in another geographical location or zone. The SAP HANA system replication operation mode must be identical for all multitier replication levels. The only exception is *logreplay_readaccess* between the primary and secondary combined with *logreplay* between the secondary and tertiary.

A takeover to the tertiary system on the *Disaster Recovery (DR)* site must be triggered manually.



Note: This information is intended for architects and specialists that are planning a high-availability deployment of SAP HANA on Power Virtual Server.

Before you begin

Review the general requirements, product documentation, support articles, and SAP notes listed in [Implementing high availability for SAP applications on IBM Power Virtual Server References](#).

Prerequisites

- A Red Hat High Availability cluster is deployed on two virtual server instances in one workspace in Power Virtual Server. Use the instructions in the following documents.
 - [Implementing a Red Hat Enterprise Linux High Availability Add-On cluster](#).
 - [Configuring SAP HANA scale-up system replication in a Red Hat Enterprise Linux High Availability Add-On cluster](#).
- A third virtual server instance is deployed in another workspace in Power Virtual Server.
- SAP HANA is installed on the third virtual server instance with the same **SID** and **Instance Number**.
- Optional - you can reserve a virtual IP address for the system on NODE3 as described in [Reserving virtual IP addresses](#). Assigning and unassigning this virtual IP address on NODE3 is a manual task and not part of a cluster operation.

Setting up the multitier scenario

The multitier scenario is an extension of the setup that is described in [Configuring SAP HANA scale-up system replication in a Red Hat Enterprise Linux High Availability Add-On cluster](#). Complete the setup for the system replication cluster before you continue with the following steps.

If the **AUTOMATED_REGISTER** cluster attribute is set to **true**, the reintegration of a failed node in the cluster can lead to a setup with a wrong SAP HANA system replication mode or an undesired SAP HANA system replication topology. To avoid these problems, disable the automatic registration and use the **hdbnsutil** command to register the SAP HANA system manually before you start the cluster on a failed node.

On a cluster node, run the following command to disable the automatic registration.

```
$ pcs resource update SAPHana_${SID}_${INSTNO} AUTOMATED_REGISTER=false
```

Providing network connectivity between the workspaces

1. Use the information in [Creating the workspace](#) to create another workspace in a different geographic location or region.
2. Create subnets and make sure that the IP ranges don't overlap with any subnet of the workspace that hosts the virtual server instances for the cluster. For more information, see [Creating private network subnets](#).
3. Set up IBM Cloud® connections up in both workspaces and activate [Enable IBM Transit Gateway](#). For more information, see [Creating Power Virtual Server Cloud Connections](#).
4. Deploy an IBM Cloud Transit Gateway to interconnect the two IBM Power Virtual Server workspaces.



Note: IBM Cloud Transit Gateway enables the interconnection of IBM Power Virtual Server, IBM Cloud classic, and Virtual Private Cloud (VPC) infrastructures and keeps data within the IBM Cloud networks. For more information about planning and deploying IBM Cloud Transit Gateway, see [Planning for IBM Cloud Transit Gateway](#) and [Ordering IBM Cloud Transit Gateway](#).

5. To add the connections to your transit gateway to establish network connectivity between your IBM Power Virtual Server, open the [Transit Gateway](#) page.
6. Select the name of your transit gateway.
7. Click **Add connection**.
8. Choose **Power Systems Virtual Server** as network connection, and select the **Location** of your workspace.
9. Click **Add** to create a connection.

Preparing environment variables on NODE3

To simplify the setup, prepare the following environment variables for user ID `root` on NODE3. These environment variables are used in subsequent commands in the remainder of the instructions.

On NODE3, create a file with the following environment variables. Then, adapt them according to the configuration of your SAP HANA system.

```
export SID=<SID>          # SAP HANA System ID (uppercase)
export sid=<sid>            # SAP HANA System ID (lowercase)
export INSTNO=<INSTNO>      # SAP HANA Instance Number

export DC3=<Site3>          # HANA System Replication Site Name 3

export NODE1=<Hostname 1>    # Hostname of virtual server instance 1 (production primary)
export NODE2=<Hostname 2>    # Hostname of virtual server instance 2 (production secondary)
export NODE3=<Hostname 3>    # Hostname of virtual server instance 3 (production tertiary)
```

You must source this file before you use the sample commands in the remainder of this document.

For example, if you created a file that is called `sap_tier3.sh`, run the following command on NODE3 to set the environment variables.

```
$ source sap_tier3.sh
```

! Important: Every time that you start a new terminal session, you must run the previous `source` command. As an alternative, you can move add the environment variables file to the `/etc/profile.d` directory during the cluster configuration. In this example, the file is sourced automatically each time you log in to the server.

Verifying network connectivity between the virtual server instances

Verify the network connectivity between the two cluster nodes (NODE1 and NODE2) and NODE3.

1. Log in to both NODE1 and NODE2, and `ping` NODE3.

```
$ ping -c 3 ${NODE3}
```

Sample output:

```
$ # ping -c 3 cl-hdb-3
PING cl-hdb-3 (10.40.20.70) 56(84) bytes of data.
64 bytes from 10.40.20.70 (10.40.20.70): icmp_seq=1 ttl=46 time=78.2 ms
64 bytes from 10.40.20.70 (10.40.20.70): icmp_seq=2 ttl=46 time=78.3 ms
64 bytes from 10.40.20.70 (10.40.20.70): icmp_seq=3 ttl=46 time=78.2 ms

--- cl-hdb-3 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 78.197/78.233/78.264/0.027 ms
```

2. Log in to NODE3 and `ping` NODE1.

```
$ ping -c 3 ${NODE1}
```

Sample output:

```
$ # ping -c 3 cl-hdb-1
PING cl-hdb-1 (10.40.10.60) 56(84) bytes of data.
64 bytes from cl-hdb-1 (10.40.10.60): icmp_seq=1 ttl=46 time=78.3 ms
64 bytes from cl-hdb-1 (10.40.10.60): icmp_seq=2 ttl=46 time=78.2 ms
64 bytes from cl-hdb-1 (10.40.10.60): icmp_seq=3 ttl=46 time=78.3 ms

--- cl-hdb-1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 78.245/78.268/78.287/0.229 ms
```

3. Log in to NODE3 and `ping` NODE2.

```
$ ping -c 3 ${NODE2}
```

Sample output:

```
$ # ping -c 3 cl-hdb-2
PING cl-hdb-2 (10.40.10.194) 56(84) bytes of data.
64 bytes from cl-hdb-2 (10.40.10.194): icmp_seq=1 ttl=46 time=77.6 ms
64 bytes from cl-hdb-2 (10.40.10.194): icmp_seq=2 ttl=46 time=79.1 ms
64 bytes from cl-hdb-2 (10.40.10.194): icmp_seq=3 ttl=46 time=77.7 ms

--- cl-hdb-2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 77.649/78.129/79.071/0.703 ms
```

Copying PKI SSFS storage certificate files to NODE3

The SAP HANA 2.0 data and log transmission channels for the replication process require authentication by using the system *PKI SSFS* storage certificate files.

- [2369981 - Required configuration steps for authentication with HANA System Replication](#))

The system *PKI SSFS* storage certificate files are stored in `/usr/sap/${SID}/SYS/global/security/rsecssfs/` in subdirectories `data` and `key`.

On NODE3, run the following commands to copy files `SSFS_${SID}.DAT` and `SSFS_${SID}.KEY` from NODE2.

```
$ scp ${NODE2}:/usr/sap/${SID}/SYS/global/security/rsecssfs/data/SSFS_${SID}.DAT
/usr/sap/${SID}/SYS/global/security/rsecssfs/data/SSFS_${SID}.DAT
```

```
$ scp ${NODE2}:/usr/sap/${SID}/SYS/global/security/rsecssfs/key/SSFS_${SID}.KEY
/usr/sap/${SID}/SYS/global/security/rsecssfs/key/SSFS_${SID}.KEY
```

The copied *PKI SSFS* storage certificates on NODE3 become active during start of the SAP HANA system. Therefore, it is recommended to copy the files when the SAP HANA system on NODE3 is stopped.

Registering NODE3 as tertiary SAP HANA system replication system

Register the SAP HANA system as a tertiary system replication instance.

1. On NODE2, run the following command to enable this site as a system replication source system.

```
$ sudo -i -u ${sid}adm -- hdbnsutil -sr_enable
```

Sample output:

```
$ $ hdbnsutil -sr_enable
nameserver is active, proceeding ...
successfully enabled system as system replication source site
done.
```

2. On NODE3, stop the SAP HANA system.

```
$ sudo -i -u ${sid}adm -- HDB stop
```

3. On NODE3, register the tertiary system with NODE2.

```
$ sudo -i -u ${sid}adm -- \
hdbnsutil -sr_register \
--name=${DC3} \
--remoteHost=${NODE2} \
--remoteInstance=${INSTNO} \
--replicationMode=async \
--operationMode=logreplay \
--online
```

4. On NODE3, start the tertiary SAP HANA system.

```
$ sudo -i -u ${sid}adm -- HDB start
```

Checking the SAP HANA system replication status

You can monitor the system replication status by using the following tools.

- SAP HANA cockpit
- SAP HANA studio
- `hdbnsutil` command-line tool
- `systemReplicationStatus.py` Python script
- SQL queries

The full output of the `systemReplicationStatus.py` script is available on only the primary system, as a database connection is required to obtain some of the status information.

On NODE1, check the system replication status by using the `systemReplicationStatus.py` Python script.

```
$ sudo -i -u ${sid}adm -- HDBSettings.sh systemReplicationStatus.py
```

Sample output:

```
$ # sudo -i -u hdbadm -- HDBSettings.sh systemReplicationStatus.py
|Database |Host      |Port    |Service Name |Volume ID |Site ID |Site Name |Secondary |Secondary |Secondary |Secondary | | |
|Secondary |          |         |             |          |        |          |          |          |          |          |          |          |
|          |          |          |             |          |        |          |          |          |          |          |          |          |
|Active Status |Mode      |Status    |Status Details |Fully Synced | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
|----- |----- |----- |----- |----- |----- |----- |----- |----- |----- |----- |----- |
|SYSTEMDB |cl-hdb-1 |30001 |nameserver |          |1 |          |SiteA     |cl-hdb-2 |30001 |          |2 |SiteB   |
|YES      |SYNCMEM   |ACTIVE    |          |          |   |          |          |          |          |          |          |
|HDB      |cl-hdb-1 |30007 |xsengine   |          |2 |          |SiteA     |cl-hdb-2 |30007 |          |2 |SiteB   |
|YES      |SYNCMEM   |ACTIVE    |          |          |   |          |          |          |          |          |
|HDB      |cl-hdb-1 |30003 |indexserver|          |3 |          |SiteA     |cl-hdb-2 |30003 |          |2 |SiteB   |
|YES      |SYNCMEM   |ACTIVE    |          |          |   |          |          |          |          |          |
|SYSTEMDB |cl-hdb-2 |30001 |nameserver|          |1 |          |2 |SiteB     |cl-hdb-3 |30001 |          |3 |SiteC   |
|YES      |ASYNC     |ACTIVE    |          |          |   |          |          |          |          |          |
|HDB      |cl-hdb-2 |30007 |xsengine   |          |2 |          |2 |SiteB     |cl-hdb-3 |30007 |          |3 |SiteC   |
|YES      |ASYNC     |ACTIVE    |          |          |   |          |          |          |          |          |
|HDB      |cl-hdb-2 |30003 |indexserver|          |3 |          |2 |SiteB     |cl-hdb-3 |30003 |          |3 |SiteC   |
|YES      |ASYNC     |ACTIVE    |          |          |   |          |          |          |          |          |

status system replication site "2": ACTIVE
status system replication site "3": ACTIVE
overall system replication status: ACTIVE

Local System Replication State
~~~~~
mode: PRIMARY
site id: 1
site name: SiteA
```

An alternative view of the system replication status is available with the `hdbnsutil` command.

On all nodes, run the following command to check the system replication status.

```
$ sudo -i -u ${sid}adm -- hdbnsutil -sr_state
```

Sample output on NODE1:

```
$ # sudo -i -u hdbadm -- hdbnsutil -sr_state
System Replication State
~~~~~
online: true

mode: primary
operation mode: primary
site id: 1
```

```

site name: SiteA

is source system: true
is secondary/consumer system: false
has secondaries/consumers attached: true
is a takeover active: false
is primary suspended: false

Host Mappings:
~~~~~

cl-hdb-1 -> [SiteC] cl-hdb-3
cl-hdb-1 -> [SiteB] cl-hdb-2
cl-hdb-1 -> [SiteA] cl-hdb-1

Site Mappings:
~~~~~

SiteA (primary/primary)
|---SiteB (syncmem/logreplay)
|   |---SiteC (async/logreplay)

Tier of SiteA: 1
Tier of SiteB: 2
Tier of SiteC: 3

Replication mode of SiteA: primary
Replication mode of SiteB: syncmem
Replication mode of SiteC: async

Operation mode of SiteA: primary
Operation mode of SiteB: logreplay
Operation mode of SiteC: logreplay

Mapping: SiteA -> SiteB
Mapping: SiteB -> SiteC

Hint based routing site:
done.

```

Sample output on NODE2:

```

$ # sudo -i -u hdbadm -- hdbnsutil -sr_state

System Replication State
~~~~~

online: true

mode: syncmem
operation mode: logreplay
site id: 2
site name: SiteB

is source system: true
is secondary/consumer system: true
has secondaries/consumers attached: true
is a takeover active: false
is primary suspended: false
is timetravel enabled: false
replay mode: auto
active primary site: 1

primary masters: cl-hdb-1

Host Mappings:
~~~~~

cl-hdb-2 -> [SiteC] cl-hdb-3
cl-hdb-2 -> [SiteB] cl-hdb-2

```

```

cl-hdb-2 -> [SiteA] cl-hdb-1

Site Mappings:
~~~~~
SiteA (primary/primary)
|---SiteB (syncmem/logreplay)
|   |---SiteC (async/logreplay)

Tier of SiteA: 1
Tier of SiteB: 2
Tier of SiteC: 3

Replication mode of SiteA: primary
Replication mode of SiteB: syncmem
Replication mode of SiteC: async

Operation mode of SiteA: primary
Operation mode of SiteB: logreplay
Operation mode of SiteC: logreplay

Mapping: SiteA -> SiteB
Mapping: SiteB -> SiteC

Hint based routing site:
done.

```

Sample output on NODE3:

```

$ # sudo -i -u hdbadm -- hdbnsutil -sr_state

System Replication State
~~~~~

online: true

mode: async
operation mode: logreplay
site id: 3
site name: SiteC

is source system: false
is secondary/consumer system: true
has secondaries/consumers attached: false
is a takeover active: false
is primary suspended: false
is timetravel enabled: false
replay mode: auto
active primary site: 2

primary masters: cl-hdb-2

Host Mappings:
~~~~~

cl-hdb-3 -> [SiteC] cl-hdb-3
cl-hdb-3 -> [SiteB] cl-hdb-2
cl-hdb-3 -> [SiteA] cl-hdb-1

Site Mappings:
~~~~~
SiteA (primary/primary)
|---SiteB (syncmem/logreplay)
|   |---SiteC (async/logreplay)

Tier of SiteA: 1
Tier of SiteB: 2
Tier of SiteC: 3

```

```
Replication mode of SiteA: primary  
Replication mode of SiteB: syncmem  
Replication mode of SiteC: async
```

```
Operation mode of SiteA: primary  
Operation mode of SiteB: logreplay  
Operation mode of SiteC: logreplay
```

```
Mapping: SiteA -> SiteB  
Mapping: SiteB -> SiteC
```

```
Hint based routing site:  
done.
```

Testing the SAP HANA system replication cluster

It is vital to thoroughly test the cluster configuration to make sure that the cluster is working correctly. The following information provides a few sample failover test scenarios, but is not a complete list of test scenarios.

For example, the description of each test case includes the following information.

- Component that is tested
- Description of the test
- Prerequisites and the initial state before the failover test
- Test procedure
- Expected behavior and results
- Recovery procedure

Test1 - Testing the failure of the primary database instance

Use the following information to test the failure of the primary database instance.

Test1 - Description

Simulate a crash of the primary SAP HANA database instance that runs on NODE1.

Test1 - Prerequisites

- A functional two-node RHEL HA Add-On cluster for HANA system replication.
- Both cluster nodes are active.
- Cluster is started on NODE1 and NODE2.
- Cluster resource `SAPHana_${SID}_${INSTNO}` is configured with `AUTOMATED_REGISTER=false`.
- Check SAP HANA system replication status:
 - SAP HANA multitier system replication is activated and in sync.
 - The primary SAP HANA system runs on NODE1.
 - The secondary SAP HANA system runs on NODE2.
 - The tertiary SAP HANA system runs on NODE3 and is registered with NODE2.

Check the current system replication status on NODE1.

```
$ sudo -i -u ${sid}adm -- HDBSettings.sh systemReplicationStatus.py
```

Sample output:

```
$ # sudo -i -u hdbadm -- HDBSettings.sh systemReplicationStatus.py  
|Database|Host|Port|Service Name|Volume ID|Site ID|Site Name|Secondary|Secondary|Secondary|Secondary|  
|Secondary|Replication|Replication|Replication|Replication|Secondary|  
|Active Status|Mode|Status|Status Details|Fully Synced| | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
|SYSTEMDB|cl-hdb-1|30001|nameserver|1|1|SiteA|cl-hdb-2|30001|2|SiteB|  
|YES|SYNCEM|ACTIVE|||True|
```

```

|HDB      |cl-hdb-1 |30007 |xsengine   | 2 | 1 |SiteA    |cl-hdb-2 | 30007 | 2 |SiteB
|YES      |SYNCMEM   |ACTIVE     |           |   | 1 |SiteA    |cl-hdb-2 | 30003 | 2 |SiteB
|HDB      |cl-hdb-1 |30003 |indexserver| 3 | 1 |SiteA    |cl-hdb-2 | 30003 | 2 |SiteB
|YES      |SYNCMEM   |ACTIVE     |           |   | 1 |SiteA    |cl-hdb-2 | 30001 | 3 |SiteC
|SYSTEMDB |cl-hdb-2 |30001 |nameserver| 1 | 2 |SiteB    |cl-hdb-3 | 30001 | 3 |SiteC
|YES      |ASYNC     |ACTIVE     |           |   | 2 |SiteB    |cl-hdb-3 | 30007 | 3 |SiteC
|HDB      |cl-hdb-2 |30007 |xsengine   | 2 | 2 |SiteB    |cl-hdb-3 | 30007 | 3 |SiteC
|YES      |ASYNC     |ACTIVE     |           |   | 2 |SiteB    |cl-hdb-3 | 30003 | 3 |SiteC
|HDB      |cl-hdb-2 |30003 |indexserver| 3 | 2 |SiteB    |cl-hdb-3 | 30003 | 3 |SiteC
|YES      |ASYNC     |ACTIVE     |           |   | 2 |SiteB    |cl-hdb-3 | 30003 | 3 |SiteC

status system replication site "2": ACTIVE
status system replication site "3": ACTIVE
overall system replication status: ACTIVE

Local System Replication State
~~~~~
mode: PRIMARY
site id: 1
site name: SiteA

```

Test1 - Test procedure

Crash SAP HANA primary by sending a SIGKILL signal as user `${sid}adm`.

On NODE1, run the following command.

```
$ sudo -i -u ${sid}adm -- HDB kill-9
```

Test1 - Expected behavior

- SAP HANA primary instance on NODE1 crashes.
- The cluster detects the stopped primary and marks the resource as `undefined`.
- The cluster promotes the secondary SAP HANA system on NODE2, which takes over as primary.
- The cluster releases the virtual IP address on NODE1, and acquires it on the primary on NODE2.
- If an application, such as SAP NetWeaver, is connected to a tenant database of SAP HANA, the application automatically reconnects to the new primary.

On NODE1, run the following command to check the cluster status.

```
$ pcs status --full
```

Sample output:

```

$ pcs status --full

Cluster name: HDB_cluster
Cluster Summary:
  * Stack: corosync
  * Current DC: cl-hdb-1 (1) (version 2.0.5-9.el8_4.5-ba59be7122) - partition with quorum
  * Last updated: Mon Jul 10 16:00:38 2023
  * Last change: Mon Jul 10 15:58:50 2023 by root via crm_attribute on cl-hdb-2
  * 2 nodes configured
  * 6 resource instances configured

Node List:
  * Online: [ cl-hdb-1 (1) cl-hdb-2 (2) ]

Full List of Resources:
  * res_fence_ibm_powervs      (stonith:fence_ibm_powervs):      Started cl-hdb-1
  * vip_HDB_00_primary    (ocf::heartbeat:IPaddr2):      Started cl-hdb-2
  * Clone Set: SAPHanaTopology_HDB_00-clone [SAPHanaTopology_HDB_00]:
    * SAPHanaTopology_HDB_00    (ocf::heartbeat:SAPHanaTopology):      Started cl-hdb-1
    * SAPHanaTopology_HDB_00    (ocf::heartbeat:SAPHanaTopology):      Started cl-hdb-2
  * Clone Set: SAPHana_HDB_00-clone [SAPHana_HDB_00] (promotable):
    * SAPHana_HDB_00    (ocf::heartbeat:SAPHana):      Master cl-hdb-2

```

```

* SAPHana_HDB_00    (ocf::heartbeat:SAPHana):      Stopped

Node Attributes:
 * Node: cl-hdb-1 (1):
   * hana_hdb_clone_state      : UNDEFINED
   * hana_hdb_op_mode         : logreplay
   * hana_hdb_remoteHost       : cl-hdb-2
   * hana_hdb_roles            : 1:P:master1::worker:
   * hana_hdb_site              : SiteA
   * hana_hdb_srah              : -
   * hana_hdb_srmode            : sync
   * hana_hdb_sync_state        : SFAIL
   * hana_hdb_version           : 2.00.070.00.1679989823
   * hana_hdb_vhost             : cl-hdb-1
   * lpa_hdb_lpt                : 10
   * master-SAPHana_HDB_00       : -9000
 * Node: cl-hdb-2 (2):
   * hana_hdb_clone_state      : PROMOTED
   * hana_hdb_op_mode          : logreplay
   * hana_hdb_remoteHost        : cl-hdb-1
   * hana_hdb_roles             : 4:P:master1:master:worker:master
   * hana_hdb_site              : SiteB
   * hana_hdb_sra                : -
   * hana_hdb_srah              : -
   * hana_hdb_srmode            : sync
   * hana_hdb_sync_state        : PRIM
   * hana_hdb_version           : 2.00.070.00.1679989823
   * hana_hdb_vhost             : cl-hdb-2
   * lpa_hdb_lpt                : 1688997529
   * master-SAPHana_HDB_00       : 150

```

Migration Summary:

```

* Node: cl-hdb-1 (1):
  * SAPHana_HDB_00: migration-threshold=5000 fail-count=1000000 last-failure='Mon Jul 10 15:56:06 2023'

```

Failed Resource Actions:

```

* SAPHana_HDB_00_start_0 on cl-hdb-1 'not running' (7): call=51, status='complete', exitreason='', last-rc-change='2023-07-10 15:56:04 +02:00', queued=0ms, exec=1527ms

```

Tickets:

PCSD Status:

```

cl-hdb-1: Online
cl-hdb-2: Online

```

Daemon Status:

```

corosync: active/disabled
pacemaker: active/disabled
pcsd: active/enabled

```

On NODE2, run the following command to check the system replication status.

```
$ sudo -i -u ${sid}adm -- HDBSettings.sh systemReplicationStatus.py
```

Sample output:

```

$ # sudo -i -u hdbadm -- HDBSettings.sh systemReplicationStatus.py
|Database|Host|Port|Service Name|Volume ID|Site ID|Site Name|Secondary|Secondary|Secondary|Secondary|
|Secondary|Replication|Replication|Replication|Replication|Secondary| |
|Active Status|Mode|Status|Status Details|Fully Synced| |
|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
|SYSTEMDB|cl-hdb-2|30001|nameserver|1|2|SiteB|cl-hdb-3|30001|3|SiteC
|YES|ASYNC|ACTIVE|||True|
|HDB|cl-hdb-2|30007|xsengine|2|2|SiteB|cl-hdb-3|30007|3|SiteC
|YES|ASYNC|ACTIVE|||True|
|HDB|cl-hdb-2|30003|indexserver|3|2|SiteB|cl-hdb-3|30003|3|SiteC
|YES|ASYNC|ACTIVE|||True|

```

```
status system replication site "3": ACTIVE
overall system replication status: ACTIVE

Local System Replication State
~~~~~
mode: PRIMARY
site id: 2
site name: SiteB
```

Test1 - Recovery procedure

As the cluster resource `SAPHana_${SID}_${INSTNO}` is configured with `AUTOMATED_REGISTER=false`, you need to register the SAP HANA system on NODE1 manually with the primary on NODE2.

! Important: When you register SAP HANA on NODE1 as a secondary, the SAP HANA system replication topology changes. Both SAP HANA systems on NODE3 at `SiteC` and NODE1 at `SiteA` are then registered as secondaries to the primary SAP HANA database that runs on NODE2 at `SiteB`.

! Important: If you want to stay with a multtier topology, you need to unregister the SAP HANA system on NODE3 at `SiteC` first. Then, you register the SAP HANA system on NODE1 at `SiteA` with the primary on NODE2 at `SiteB`. Finally, you register the SAP HANA system on NODE3 at `SiteC` with secondary on NODE1 at `SiteA`.

On NODE1, run the following command to register the system with the primary on NODE2.

```
$ sudo -i -u ${sid}adm -- \
  hdbnsutil -sr_register \
  --name=${DC1} \
  --remoteHost=${NODE2} \
  --remoteInstance=${INSTNO} \
  --replicationMode=syncmem \
  --operationMode=logreplay \
  --online
```

On NODE1, run the following command to verify the resource status.

```
$ pcs resource status
```

The cluster resource `SAPHana_${SID}_${INSTNO}-clone` remains in status `Stopped` on NODE1.

Sample output:

```
$ # pcs resource status
* vip_HDB_00_primary (ocf::heartbeat:IPaddr2):           Started cl-hdb-2
* Clone Set: SAPHanaTopology_HDB_00-clone [SAPHanaTopology_HDB_00]:
  * Started: [ cl-hdb-1 cl-hdb-2 ]
* Clone Set: SAPHana_HDB_00-clone [SAPHana_HDB_00] (promotable):
  * Masters: [ cl-hdb-2 ]
  * Stopped: [ cl-hdb-1 ]
```

On a cluster node, run the following command to clear the failure status of the resource.

```
$ pcs resource cleanup SAPHana_${SID}_${INSTNO}-clone
```

Sample output:

```
$ # pcs resource cleanup SAPHana_HDB_00-clone
Cleaned up SAPHana_HDB_00:0 on cl-hdb-2
Cleaned up SAPHana_HDB_00:0 on cl-hdb-1
Cleaned up SAPHana_HDB_00:1 on cl-hdb-2
Cleaned up SAPHana_HDB_00:1 on cl-hdb-1
Waiting for 1 reply from the controller
... got reply (done)
```

After a while, verify the system replication status on NODE2.

```
$ sudo -i -u ${sid}adm -- HDBSettings.sh systemReplicationStatus.py
```

Sample output:

```
$ # sudo -i -u hdbadm -- HDBSettings.sh systemReplicationStatus.py
|Database |Host      |Port     |Service Name |Volume ID |Site ID |Site Name |Secondary|Secondary |Secondary |Secondary
|Secondary |          |          |           |          |          |          |          |          |          |          |
|          |          |          |           |          |          |          |          |          |          |          |
|Active Status |Mode      |Status     |Status Details |Fully Synced | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
|----- |----- |----- |----- |----- |----- |----- |----- |----- |----- |----- |
|SYSTEMDB |cl-hdb-2 |30001 |nameserver |          1 |          2 |SiteB    |cl-hdb-3 | 30001 |          3 |SiteC
|YES      |ASYNC     |ACTIVE    |          |          |          |True     |          |          |          |
|HDB      |cl-hdb-2 |30007 |xsengine   |          2 |          2 |SiteB    |cl-hdb-3 | 30007 |          3 |SiteC
|YES      |ASYNC     |ACTIVE    |          |          |          |True     |          |          |          |
|HDB      |cl-hdb-2 |30003 |indexserver|          3 |          2 |SiteB    |cl-hdb-3 | 30003 |          3 |SiteC
|YES      |ASYNC     |ACTIVE    |          |          |          |True     |          |          |          |
|SYSTEMDB |cl-hdb-2 |30001 |nameserver|          1 |          2 |SiteB    |cl-hdb-1 | 30001 |          1 |SiteA
|YES      |SYNCMEM   |ACTIVE    |          |          |          |True     |          |          |          |
|HDB      |cl-hdb-2 |30007 |xsengine   |          2 |          2 |SiteB    |cl-hdb-1 | 30007 |          1 |SiteA
|YES      |SYNCMEM   |ACTIVE    |          |          |          |True     |          |          |          |
|HDB      |cl-hdb-2 |30003 |indexserver|          3 |          2 |SiteB    |cl-hdb-1 | 30003 |          1 |SiteA
|YES      |SYNCMEM   |ACTIVE    |          |          |          |True     |          |          |          |

status system replication site "3": ACTIVE
status system replication site "1": ACTIVE
overall system replication status: ACTIVE

Local System Replication State
~~~~~
mode: PRIMARY
site id: 2
site name: SiteB
```

⚠️ Important: The SAP HANA system replication topology that is changed to a multitarget environment. The primary runs on NODE2 at **SiteB**. Both NODE3 at **SiteC** and NODE1 at **SiteA** are registered as secondaries. If another takeover occurs and NODE1 at **SiteA** is promoted to primary again, NODE3 at **SiteC** is decoupled.

To create a multtier landscape with NODE3 at **SiteC** as a tertiary system, repeat the steps similar to [Registering NODE3 as tertiary SAP HANA system replication system](#) and register NODE3 to the secondary on NODE1.

1. On NODE1, run the following command to enable this site as a system replication source system.

```
$ sudo -i -u ${sid}adm -- hdbnsutil -sr_enable
```

Sample output:

```
$ # sudo -i -u hdbadm -- hdbnsutil -sr_enable
nameserver is active, proceeding ...
successfully enabled system as system replication source site
done.
```

2. On NODE3, register the system with NODE1 at **SiteA**.

```
$ sudo -i -u ${sid}adm -- \
  hdbnsutil -sr_register \
  --name=${DC3} \
  --remoteHost=${NODE1} \
  --remoteInstance=${INSTNO} \
  --replicationMode=async \
  --operationMode=logreplay \
  --online
```

```
$ # sudo -i -u hdbadm -- hdbnsutil -sr_register --name=SiteC --remoteHost=cl-hdb-1 --remoteInstance=00 --  
replicationMode=async --operationMode=logreplay --online  
adding site ...  
collecting information ...  
updating local ini files ...  
done.
```

- Verify the system replication status on all three nodes as described in [Checking the SAP HANA system replication status](#).

Test2 - Testing the manual move of a SAPHana resource to another node

Use the following information to test the manual move of the SAPHana resource to another node.

Test2 - Description

Use cluster commands to move the primary instance to the other cluster node.

Test2 - Prerequisites

- A functional two-node RHEL HA Add-On cluster for HANA system replication.
- Both cluster nodes are active.
- Cluster is started on NODE1 and NODE2.
- Cluster Resource `SAPHana_{SID}_{INSTNO}` is configured with `AUTOMATED_REGISTER=false`.
- Check SAP HANA system replication status:
 - HANA system replication is activated and in sync.
 - The primary SAP HANA system runs on NODE2.
 - The secondary SAP HANA system runs on NODE1.
 - The tertiary SAP HANA system runs on NODE3 and is registered with NODE1.

Test2 - Test procedure

- On NODE3, stop the tertiary HANA system before you perform the controlled move of the primary to NODE1.

```
$ sudo -i -u ${sid}adm -- HDB stop
```

- On a cluster node, run the following command to move the primary back to NODE1.

```
$ pcs resource move SAPHana_{SID}_{INSTNO}-clone
```

- Wait until the primary is up on NODE1. Then, register NODE2 with the primary on NODE1.

On NODE2, run the following command.

```
$ sudo -i -u ${sid}adm -- \  
hdbnsutil -sr_register \  
--name=${DC2} \  
--remoteHost=${NODE1} \  
--remoteInstance=${INSTNO} \  
--replicationMode=syncmem \  
--operationMode=logreplay \  
--online
```

- On a cluster node, run the following command to clear the resource.

```
$ pcs resource clear SAPHana_{SID}_{INSTNO}-clone
```

This command clears the location constraint, which was created by the move command. The cluster starts the SAP HANA system on NODE2.

- On NODE2, run the following command to enable this site as a system replication source system.

```
$ sudo -i -u ${sid}adm -- hdbnsutil -sr_enable
```

6. On NODE3, run the following command to register the system with NODE2.

```
$ sudo -i -u ${sid}adm -- \
    hdbnsutil -sr_register \
        --name=${DC3} \
        --remoteHost=${NODE2} \
        --remoteInstance=${INSTNO} \
        --replicationMode=async \
        --operationMode=logreplay \
        --online
```

7. On NODE3, start the tertiary HANA system.

```
$ sudo -i -u ${sid}adm -- HDB start
```

8. Verify the system replication status on all three nodes as described in [Checking the SAP HANA system replication status](#).

Test2 - Expected behavior

- The cluster creates a location constraint to move the resource.
- The cluster triggers a takeover to the secondary HANA system on NODE1.
- If an application, such as SAP NetWeaver, is connected to a tenant database of SAP HANA, the application automatically reconnects to the new primary.
- Register NODE2 with the primary on NODE1.
- Run `pcs resource clear` command to remove the location constraint. This command triggers the start of the secondary instance on NODE2.
- After you register and start the HANA system on NODE3 at `SiteC`, the tertiary HANA system is registered with NODE2.

Test2 - Recovery procedure

No recovery procedure is required. The test sequence reestablished the initial SAP HANA multitier system replication topology.

Test3 - Testing failure of node that runs the primary database

Use the following information to test the failure of node that runs the primary database.

Test3 - Description

Simulate a crash of the node that runs the primary HANA database.

Test3 - Prerequisites

- A functional two-node RHEL HA Add-On cluster for HANA system replication.
- Both cluster nodes are active.
- Cluster is started on NODE1 and NODE2.
- Cluster Resource `SAPHana_${SID}_${INSTNO}` is configured with `AUTOMATED_REGISTER=false`.
- Check SAP HANA system replication status:
 - HANA system replication is activated and in sync.
 - The primary SAP HANA system runs on NODE1.
 - The secondary SAP HANA system runs on NODE2.
 - The secondary SAP HANA system runs on NODE3 and is registered with NODE2.

Test3 - Test procedure

Crash the primary on NODE1 by sending a `crash` system request.

On NODE1, run the following command.

```
$ sync; echo c > /proc/sysrq-trigger
```

Test3 - Expected behavior

- NODE1 shuts down.
- The cluster detects the failed node and sets its state to **OFFLINE**.
- The cluster promotes the secondary HANA database on NODE2 to take over as new primary.
- The cluster acquires the virtual IP address on NODE2.
- If an application, such as SAP NetWeaver, is connected to a tenant database of SAP HANA, the application automatically reconnects to the new primary.
- The tertiary SAP HANA system that runs on NODE3 is still registered with NODE2.

Verify the SAP HANA system replication status on NODE2.

```
$ sudo -i -u ${sid}adm -- HDBSettings.sh systemReplicationStatus.py
```

Sample output:

```
$ # sudo -i -u hdbadm -- HDBSettings.sh systemReplicationStatus.py
|Database |Host      |Port    |Service Name |Volume ID |Site ID |Site Name |Secondary|Secondary |Secondary |Secondary | | |
|Secondary |          |         |             |          |        |         |          |          |          |          |          |          |
|          |          |          |             |          |        |         |          |          |          |          |          |          |
|Active Status |Mode      |Status     |Status Details |Fully Synced | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
|SYSTEMDB |cl-hdb-2 |30001  |nameserver   |       1 |       2 |SiteB     |cl-hdb-3 | 30001  |       3 |SiteC
|YES      |ASYNC     |ACTIVE     |             |       |       |True      |          |          |       |
|HDB      |cl-hdb-2 |30007  |xsengine     |       2 |       2 |SiteB     |cl-hdb-3 | 30007  |       3 |SiteC
|YES      |ASYNC     |ACTIVE     |             |       |       |True      |          |          |       |
|HDB      |cl-hdb-2 |30003  |indexserver  |       3 |       2 |SiteB     |cl-hdb-3 | 30003  |       3 |SiteC
|YES      |ASYNC     |ACTIVE     |             |       |       |True      |          |          |       |

status system replication site "3": ACTIVE
overall system replication status: ACTIVE

Local System Replication State
~~~~~
mode: PRIMARY
site id: 2
site name: SiteB
```

Test3 - Recovery procedure

Log in to the IBM Cloud console and start NODE1.

1. On NODE1, run the following command to register the system with the primary on NODE2.

```
$ sudo -i -u ${sid}adm -- \
  hdbnsutil -sr_register \
  --name=${DC1} \
  --remoteHost=${NODE2} \
  --remoteInstance=${INSTNO} \
  --replicationMode=syncmem \
  --operationMode=logreplay \
  --online
```

2. On NODE1, run the following command to start the cluster services.

```
$ pcs cluster start
```

3. On a cluster node, run the following command to check the cluster status.

```
$ pcs status --full
```

4. On NODE2, verify the SAP HANA system replication status.

```
$ sudo -i -u ${sid}adm -- HDBSettings.sh systemReplicationStatus.py
```

Sample output:

```
$ # sudo -i -u hdbadm -- HDBSettings.sh systemReplicationStatus.py
|Database |Host      |Port    |Service Name |Volume ID |Site ID |Site Name |Secondary|Secondary |Secondary |Secondary
|Secondary   |Replication |Replication |Replication   |Secondary   |
|           |           |           |           |           |           |           |           |           |           |
|Name |Active Status |Mode      |Status     |Status Details |Fully Synced | | | | |
|---|---|---|---|---|---|---|---|---|---|
|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
|SYSTEMDB |cl-hdb-2 |30001 |nameserver |           |1 |2 |SiteB |cl-hdb-3 |30001 |3 |SiteC
|YES     |ASYNC     |ACTIVE    |           |           | |True |           |           |           |
|HDB     |cl-hdb-2 |30007 |xsengine  |           |2 |2 |SiteB |cl-hdb-3 |30007 |3 |SiteC
|YES     |ASYNC     |ACTIVE    |           |           | |True |           |           |           |
|HDB     |cl-hdb-2 |30003 |indexserver |           |3 |2 |SiteB |cl-hdb-3 |30003 |3 |SiteC
|YES     |ASYNC     |ACTIVE    |           |           | |True |           |           |           |
|SYSTEMDB |cl-hdb-2 |30001 |nameserver |           |1 |2 |SiteB |cl-hdb-1 |30001 |1 |SiteA
|YES     |SYNCMEM   |ACTIVE    |           |           | |True |           |           |           |
|HDB     |cl-hdb-2 |30007 |xsengine  |           |2 |2 |SiteB |cl-hdb-1 |30007 |1 |SiteA
|YES     |SYNCMEM   |ACTIVE    |           |           | |True |           |           |           |
|HDB     |cl-hdb-2 |30003 |indexserver |           |3 |2 |SiteB |cl-hdb-1 |30003 |1 |SiteA
|YES     |SYNCMEM   |ACTIVE    |           |           | |True |           |           |           |

status system replication site "3": ACTIVE
status system replication site "1": ACTIVE
overall system replication status: ACTIVE

Local System Replication State
~~~~~
mode: PRIMARY
site id: 2
site name: SiteB
```

5. Run the steps in [Test1 - Recovery procedure](#) to rebuild the SAP HANA system replication multilayer topology for NODE3 at **SiteC**.
6. Run the steps in [Test2 - Test the manual move of SAPHana resource to another node](#) to revert to the initial topology.

Test4 - Testing failure of the secondary database instance

Use the following information to test the failure of the secondary database instance.

Test4 - Description

Simulate a crash of the secondary HANA database.

Test4 - Prerequisites

- A functional two-node RHEL HA Add-On cluster for HANA system replication.
- Both nodes are active.
- Cluster is started on NODE1 and NODE2.
- Cluster Resource **SAPHana_\${SID}_\${INSTNO}** is configured with **AUTOMATED_REGISTER=false**.
- Check SAP HANA system replication status:
 - HANA system replication is active and in sync.
 - The primary SAP HANA system runs on NODE1.
 - The secondary SAP HANA system runs on NODE2.
 - The tertiary SAP HANA system runs on NODE3 and is registered with NODE2.

Test4 - Test procedure

Crash SAP HANA secondary by sending a SIGKILL signal as user **\${sid}adm**.

On NODE2, run the following command.

```
$ sudo -i -u ${sid}adm -- HDB kill-9
```

Test4 - Expected behavior

- SAP HANA secondary on NODE2 crashes.
- The cluster detects the stopped secondary HANA system and marks the resource as **failed**.
- The cluster restarts the secondary HANA system.
- The cluster detects that the system replication is in sync again.
- The tertiary SAP HANA system that runs on NODE3 gets in sync again.

On NODE1, check the SAP HANA system replication status periodically to observe the recovery steps.

```
$ watch -n 5 sudo -i -u ${sid}adm -- HDBSettings.sh systemReplicationStatus.py
```

Sample output:

```
$ # sudo -i -u hdbadm -- HDBSettings.sh systemReplicationStatus.py
|Database |Host      |Port    |Service Name |Volume ID |Site ID |Site Name |Secondary|Secondary |Secondary |Secondary | |
|Secondary   |           |         |           |           |         |         |           |           |           |           |           |
|           |           |           |           |           |           |           |           |           |           |           |
|Active Status |Mode       |Status     |Status Details |           |           |           |           |           |           | |
|---|---|---|---|---|---|---|---|---|---|---|
|----- |----- |----- |----- |----- |----- |----- |----- |----- |----- |----- |
|SYSTEMDB |cl-hdb-1 |30001 |nameserver |1 |1 |SiteA |cl-hdb-2 |30001 |2 |SiteB
|CONNECTION TIMEOUT |SYNCMEM |ERROR |Communication channel closed |False |
|HDB |cl-hdb-1 |30007 |xsengine |2 |1 |SiteA |cl-hdb-2 |30007 |2 |SiteB
|CONNECTION TIMEOUT |SYNCMEM |ERROR |Communication channel closed |False |
|HDB |cl-hdb-1 |30003 |indexserver |3 |1 |SiteA |cl-hdb-2 |30003 |2 |SiteB
|CONNECTION TIMEOUT |SYNCMEM |ERROR |Communication channel closed |False |
|SYSTEMDB |cl-hdb-2 |30001 |nameserver |1 |2 |SiteB |cl-hdb-3 |30001 |3 |SiteC
|UNKNOWN |UNKNOWN |Site with id '2' is not reachable |False |
|HDB |cl-hdb-2 |30007 |xsengine |2 |2 |SiteB |cl-hdb-3 |30007 |3 |SiteC
|UNKNOWN |UNKNOWN |Site with id '2' is not reachable |False |
|HDB |cl-hdb-2 |30003 |indexserver |3 |2 |SiteB |cl-hdb-3 |30003 |3 |SiteC
|UNKNOWN |UNKNOWN |Site with id '2' is not reachable |False |

status system replication site "2": ERROR
status system replication site "3": UNKNOWN
overall system replication status: ERROR

Local System Replication State
~~~~~
mode: PRIMARY
site id: 1
site name: SiteA
```

Test4 - Recovery procedure

Wait until the secondary HANA instance starts and synchronized again (**SOK**), then cleanup the failed resource actions that are shown in the **pcs status** output.

1. On a cluster node, run the following command.

```
$ pcs resource refresh SAPHana_${SID}_${INSTNO}
```

2. Check the cluster status.

```
$ pcs status --full
```

Test5 - Testing DR activation on the node that runs the tertiary database

Use the following information to test the failure of both nodes in the primary workspace.

Test5 - Description

Simulate a crash of the nodes that run the primary and secondary SAP HANA database.

Test5 - Prerequisites

- A functional two-node RHEL HA Add-On cluster for HANA system replication.
- Both cluster nodes are active.
- Cluster is started on NODE1 and NODE2.
- Cluster Resource `SAPHana_${SID}_${INSTNO}` is configured with `AUTOMATED_REGISTER=false`.
- Check SAP HANA system replication status:
 - HANA system replication is active and in sync.
 - The primary SAP HANA system runs on NODE1.
 - The secondary SAP HANA system runs on NODE2.
 - The tertiary SAP HANA system runs on NODE3 and is registered with NODE2.

Test5 - Test procedure

Crash primary on NODE1 and secondary on NODE2 by sending a `crash` system request on both nodes.

1. On NODE1, run the following command.

```
$ sync; echo c > /proc/sysrq-trigger
```

2. On NODE2, run the following command.

```
$ sync; echo c > /proc/sysrq-trigger
```

3. On NODE3, run the following command to activate the HANA system as the new primary.

```
$ sudo -i -u ${sid}adm -- hdbnsutil -sr_takeover
```

Sample output:

```
$ # sudo -i -u hdbadm -- hdbnsutil -sr_takeover
done.
```

Test5 - Expected behavior

- NODE1 and NODE2 halt immediately.
- After the manual takeover, NODE3 runs the primary SAP HANA system.
- An application, such as SAP NetWeaver, can connect to the SAP HANA system on NODE3.

On NODE3, run the following command to verify that the SAP HANA system runs as primary.

```
$ sudo -i -u ${sid}adm -- hdbnsutil -sr_state
```

Sample output:

```
$ # sudo -i -u hdbadm -- hdbnsutil -sr_state

System Replication State
~~~~~

online: true

mode: primary
operation mode: primary
site id: 3
site name: SiteC

is source system: true
is secondary/consumer system: false
has secondaries/consumers attached: false
```

```
is a takeover active: false
is primary suspended: false

Host Mappings:
~~~~~
cl-hdb-3 -> [SiteC] cl-hdb-3

Site Mappings:
~~~~~
SiteC (primary/primary)

Tier of SiteC: 1

Replication mode of SiteC: primary

Operation mode of SiteC: primary

Hint based routing site:
done.
```

Test5 - Recovery procedure

The recovery procedure after a takeover to the tertiary SAP HANA system is complex and is documented as a separate test in the *Test6* section.

Test6 - Restoring the original SAP HANA multitier system replication topology

Use the following information to revert to the original system replication topology after a takeover to the tertiary SAP HANA system.

Check the following SAP documentation.

- [Restore the Original SAP HANA Multitier System Replication Configuration](#)

Test6 - Description

Reactivate the cluster in the primary workspace and restore the original system replication topology.

Test6 - Prerequisites

- A two-node RHEL HA Add-On cluster for HANA system replication in the primary workspace.
- Both virtual server instances of the cluster are stopped.
- The primary SAP HANA system runs on NODE3.

Test6 - Test procedure

1. Log in to the IBM Cloud console and start both NODE1 and NODE2.
2. Wait until both nodes are available again.
3. Ensure that the Red Hat HA Add-On cluster services are stopped on both cluster nodes NODE1 and NODE2.
4. On NODE3, verify that SAP HANA system replication is enabled.

```
$ sudo -i -u ${sid}adm -- hdbnsutil -sr_state
```

5. On NODE1, run the following command to set an environment variable with the hostname of NODE3.

```
$ export NODE3=<Hostname 3> # Hostname of virtual server instance 3 (production tertiary)
```

6. On NODE1, run the following command to register the SAP HANA system with the primary on NODE3.

```
$ sudo -i -u ${sid}adm -- \
    hdbnsutil -sr_register \
    --name=${DC1} \
```

```
--remoteHost=${NODE3} \
--remoteInstance=${INSTNO} \
--replicationMode=async \
--operationMode=logreplay \
--online
```

7. On NODE1, check the system replication configuration.

```
$ sudo -i -u ${sid}adm -- hdbnsutil -sr_state
```

Sample output:

```
$
System Replication State
~~~~~
online: false

mode: async
operation mode: unknown
site id: 1
site name: SiteA

is source system: unknown
is secondary/consumer system: true
has secondaries/consumers attached: unknown
is a takeover active: false
is primary suspended: false
is timetravel enabled: false
replay mode: auto
active primary site: 3

primary masters: cl-hdb-3
done.
```

8. On NODE1, start the SAP HANA system to start the system replication.

```
$ sudo -i -u ${sid}adm -- HDB start
```

9. On NODE3, check the system replication status and wait until the secondary on NODE1 is fully synchronized.

```
$ sudo -i -u ${sid}adm -- HDBSettings.sh systemReplicationStatus.py
```

Sample output:

```
$ # sudo -i -u hdbadm -- HDBSettings.sh systemReplicationStatus.py
|Database |Host      |Port    |Service Name |Volume ID |Site ID |Site Name |Secondary |Secondary |Secondary |
|Secondary |Secondary   |Replication |Replication |Replication |Secondary   |Host       |Port       |Site ID   |Site      |
|Name     |Active Status |Mode      |Status      |Status Details |Fully Synced | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
|SYSTEMDB |cl-hdb-3 |30001  |nameserver  |1          |3          |SiteC     |cl-hdb-1  |30001  |1         |SiteA    |
|YES      |ASYNC      |ACTIVE    |           |           |True      |           |           |           |           |
|HDB      |cl-hdb-3  |30007  |xsengine   |2          |3          |SiteC     |cl-hdb-1  |30007  |1         |SiteA    |
|YES      |ASYNC      |ACTIVE    |           |           |True      |           |           |           |           |
|HDB      |cl-hdb-3  |30003  |indexserver|3          |3          |SiteC     |cl-hdb-1  |30003  |1         |SiteA    |
|YES      |ASYNC      |ACTIVE    |           |           |True      |           |           |           |           |

status system replication site "1": ACTIVE
overall system replication status: ACTIVE
```

```
Local System Replication State
~~~~~
```

```
mode: PRIMARY
site id: 3
site name: SiteC
```



Important: You need a downtime window to perform the move of the primary role back to NODE1. All application servers that are connected to NODE3 must be stopped.

A *takeover with handshake* suspends all transactions on the primary system on NODE3 and the takeover is only executed when all remaining redo log is available on NODE1.

1. On NODE1, run the following command to takeover the primary role.

```
$ sudo -i -u ${sid}adm -- hdbnsutil -sr_takeover --suspendPrimary
```

2. On NODE1, check that the HANA system runs as primary.

```
$ sudo -i -u ${sid}adm -- hdbnsutil -sr state
```

3. On NODE3, run the following command to verify the system replication status.

```
$ sudo -i -u ${sid}adm -- HDBSettings.sh systemReplicationStatus.py
```

```
$ # sudo -i -u hdbadm -- HDBSettings.sh systemReplicationStatus.py
|Database |Host      |Port    |Service Name |Volume ID |Site ID |Site Name |Secondary|Secondary |Secondary |Secondary |
|Secondary   |Replication |Replication |Replication           |Secondary   |
|           |           |           |           |           |           |           |           |           |           |
|           |           |           |           |           |           |           |           |           |           |
|Name |Active Status |Mode       |Status     |Status Details           |Fully Synced | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
|SYSTEMDB |cl-hdb-3 |30001 |nameserver |           1 |           3 |SiteC     |cl-hdb-1 |30001 |           1 |
|PRIMARY   |           |           |           |IS PRIMARY (e.g. after takeover) |           False |
|HDB       |cl-hdb-3 |30007 |xsengine  |           2 |           3 |SiteC     |cl-hdb-1 |30007 |           1 |
|PRIMARY   |           |           |           |IS PRIMARY (e.g. after takeover) |           False |
|HDB       |cl-hdb-3 |30003 |indexserver |           3 |           3 |SiteC     |cl-hdb-1 |30003 |           1 |
|PRIMARY   |           |           |           |IS PRIMARY (e.g. after takeover) |           False |

status system replication site "1": ERROR
overall system replication status: ERROR

Local System Replication State
~~~~~
mode: PRIMARY
site id: 3
site name: SiteC
```

The following summary shows the status after these steps.

- NODE1 runs as primary, but no application is connected.
 - NODE2 is up, but SAP HANA is not started.
 - NODE3 is up and SAP HANA is blocked in `suspendPrimary` mode.
 - Red Hat HA Add-On cluster services are stopped on NODE1 and NODE2.

1. On NODE2, run the following command to register with the primary on NODE1.

```
$ sudo -i -u ${sid}adm -- \
    hdbnsutil -sr_register \
    --name=${DC2} \
    --remoteHost=${NODE1} \
    --remoteInstance=${INSTNO} \
    --replicationMode=syncmem \
    --operationMode=logreplay \
    --online
```

2. On NODE2, start SAP HANA to start the replication.

```
$ sudo -i -u ${sid}adm -- HDB start
```

- On NODE1, check the system replication status and wait until the secondary on NODE2 is fully synchronized.

```
$ sudo -i -u ${sid}adm -- HDBSettings.sh systemReplicationStatus.py
```

Sample output:

```
$ # sudo -i -u hdbadm -- HDBSettings.sh systemReplicationStatus.py
|Database |Host      |Port     |Service Name |Volume ID |Site ID |Site Name |Secondary |Secondary |Secondary |
|Secondary |Secondary      |Replication |Replication |Replication |Secondary      |
|          |           |           |           |           |           |           |           |           |
|Name    |Active Status |Mode       |Status      |Status Details |Fully Synced | | | | |
|---|---|---|---|---|---|---|---|---|---|
|----- |----- |----- |----- |----- |----- |----- |----- |----- |----- |
|SYSTEMDB |cl-hdb-1 |30001  |nameserver  |1          |1          |SiteA     |cl-hdb-2 |30001  |2 |SiteB
|YES      |SYNC        |ACTIVE     |           |           |True      |           |           |           |
|HDB      |cl-hdb-1 |30007  |xsengine   |2          |1          |SiteA     |cl-hdb-2 |30007  |2 |SiteB
|YES      |SYNC        |ACTIVE     |           |           |True      |           |           |           |
|HDB      |cl-hdb-1 |30003  |indexserver|3          |1          |SiteA     |cl-hdb-2 |30003  |2 |SiteB
|YES      |SYNC        |ACTIVE     |           |           |True      |           |           |           |

status system replication site "2": ACTIVE
overall system replication status: ACTIVE

Local System Replication State
~~~~~
mode: PRIMARY
site id: 1
site name: SiteA
```

The following summary shows the status after these steps.

- NODE1 runs as primary, but no application is connected.
- NODE2 runs as secondary.
- NODE3 is up and SAP HANA is blocked in `suspendPrimary` mode.
- Red Hat HA Add-On cluster services are stopped on NODE1 and NODE2.

- On a cluster node, run the following command to start the cluster.

```
$ pcs cluster start --all
```

- Check the cluster status and verify that it is fully operational again.

```
$ pcs status --full
```

The following summary shows the status after these steps.

- NODE1 runs as primary.
- NODE2 runs as secondary.
- Red Hat HA Add-On cluster services are started and the cluster manages SAP HANA system replication on NODE1 and NODE2.
- NODE3 is up and SAP HANA is blocked in `suspendPrimary` mode.

- On NODE2, run the following command to enable it as system replication source site.

```
$ sudo -i -u ${sid}adm -- hdbnsutil -sr_enable
```

Sample output:

```
$ # sudo -i -u hdbadm -- hdbnsutil -sr_enable
nameserver is active, proceeding ...
successfully enabled system as system replication source site
done.
```

- On NODE2, check the system replication configuration.

```
$ sudo -i -u ${sid}adm -- hdbnsutil -sr_state
```

Sample output:

```
$ # sudo -i -u hdbadm -- hdbnsutil -sr_state
```

System Replication State

online: true

mode: sync

operation mode: logreplay

site id: 2

site name: SiteB

is source system: true

is secondary/consumer system: true

has secondaries/consumers attached: false

is a takeover active: false

is primary suspended: false

is timetravel enabled: false

replay mode: auto

active primary site: 1

primary masters: cl-hdb-1

Host Mappings:

```
cl-hdb-2 -> [SiteB] cl-hdb-2
cl-hdb-2 -> [SiteA] cl-hdb-1
```

Site Mappings:

```
SiteA (primary/primary)
|---SiteB (sync/logreplay)
```

Tier of SiteA: 1

Tier of SiteB: 2

Replication mode of SiteA: primary

Replication mode of SiteB: sync

Operation mode of SiteA: primary

Operation mode of SiteB: logreplay

Mapping: SiteA -> SiteB

Hint based routing site:

done.

3. On NODE3, run the following command to register the system with NODE2.

```
$ sudo -i -u ${sid}adm -- \
  hdbnsutil -sr_register \
  --name=${DC3} \
  --remoteHost=${NODE2} \
  --remoteInstance=${INSTNO} \
  --replicationMode=async \
  --operationMode=logreplay \
  --online
```

4. On NODE1, run the following command to verify the new SAP HANA system replication topology.

```
$ sudo -i -u ${sid}adm -- HDBSettings.sh systemReplicationStatus.py
```

The SAP HANA system on NODE3 at SiteC reappears in the SAP HANA system replication topology. When you run the `hdbnsutil -sr_register` command, the system stops and `CONNECTION TIMEOUT` is shown in the output.

Sample output:

```
$ # sudo -i -u hdbadm -- HDBSettings.sh systemReplicationStatus.py
|Database |Host      |Port    |Service Name |Volume ID |Site ID |Site Name |Secondary|Secondary |Secondary |Secondary |
|Secondary           |Replication |Replication |Replication   |Secondary   |
|                   |           |           |           |           |           |           |Host      |Port      |Site ID  |Site
|Name  |Active Status |Mode     |Status     |Status Details |Fully Synced | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
|SYSTEMDB |cl-hdb-1 |30001 |nameserver |           |1 |       1 |SiteA    |cl-hdb-2 |30001 |       2 |SiteB
|YES          |SYNCFMEM |ACTIVE   |           |           | |           |True     |
|HDB          |cl-hdb-1 |30007 |xsengine  |           |2 |       1 |SiteA    |cl-hdb-2 |30007 |       2 |SiteB
|YES          |SYNCFMEM |ACTIVE   |           |           | |           |True     |
|HDB          |cl-hdb-1 |30003 |indexserver |           |3 |       1 |SiteA    |cl-hdb-2 |30003 |       2 |SiteB
|YES          |SYNCFMEM |ACTIVE   |           |           | |           |True     |
|SYSTEMDB |cl-hdb-2 |30001 |nameserver |           |1 |       2 |SiteB    |cl-hdb-3 |30001 |       3 |SiteC
|CONNECTION TIMEOUT |ASYNC    |UNKNOWN  |           |           | |           |False    |
|HDB          |cl-hdb-2 |30007 |xsengine  |           |2 |       2 |SiteB    |cl-hdb-3 |30007 |       3 |SiteC
|CONNECTION TIMEOUT |ASYNC    |UNKNOWN  |           |           | |           |False    |
|HDB          |cl-hdb-2 |30003 |indexserver |           |3 |       2 |SiteB    |cl-hdb-3 |30003 |       3 |SiteC
|CONNECTION TIMEOUT |ASYNC    |UNKNOWN  |           |           | |           |False    |

status system replication site "2": ACTIVE
status system replication site "3": UNKNOWN
overall system replication status: UNKNOWN

Local System Replication State
~~~~~
```

5. On NODE3, run the following command to start the tertiary HANA system.

```
$ sudo -i -u ${sid}adm -- HDB start
```

The following summary shows the final status after these steps.

- NODE1 runs as primary.
 - NODE2 runs as secondary.
 - Red Hat HA Add-On cluster services are started and the cluster manages SAP HANA system replication on NODE1 and NODE2.
 - NODE3 runs as tertiary.

On NODE1, run the following command to verify the SAP HANA system replication topology

```
$ sudo -i -u ${sid}adm -- HDBSettings.sh systemReplicationStatus.py
```

Sample output:

# sudo -i -u hdbadm -- HDBSettings.sh systemReplicationStatus.py												
Database	Host	Port	Service Name	Volume ID	Site ID	Site Name	Secondary	Secondary	Secondary	Secondary	Secondary	Secondary
Secondary	Replication	Replication	Replication	Replication	Secondary		Host	Port	Site ID	Site Name		
Active Status	Mode	Status		Status Details	Fully Synced							
-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----
-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----
SYSTEMDB	cl-hdb-1	30001	nameserver		1	1	SiteA	cl-hdb-2	30001		2	SiteB
YES	SYNC	ACTIVE				True						
HDB	cl-hdb-1	30007	xsgengine		2	1	SiteA	cl-hdb-2	30007		2	SiteB
YES	SYNC	ACTIVE				True						
HDB	cl-hdb-1	30003	indexserver		3	1	SiteA	cl-hdb-2	30003		2	SiteB
YES	SYNC	ACTIVE				True						
SYSTEMDB	cl-hdb-2	30001	nameserver		1	2	SiteB	cl-hdb-3	30001		3	SiteC
YES	ASYNC	ACTIVE				True						

```

|HDB      |cl-hdb-2 |30007 |xsengine   |    2 |    2 |SiteB     |cl-hdb-3 | 30007 |    3 |SiteC
|YES          |ASYNC      |ACTIVE      |           |           |True |           |
|HDB      |cl-hdb-2 |30003 |indexserver |    3 |    2 |SiteB     |cl-hdb-3 | 30003 |    3 |SiteC
|YES          |ASYNC      |ACTIVE      |           |           |True |           |

status system replication site "2": ACTIVE
status system replication site "3": ACTIVE
overall system replication status: ACTIVE

Local System Replication State
~~~~~
mode: PRIMARY
site id: 1
site name: SiteA

```

Configuring SAP HANA multitarget system replication in a Red Hat Enterprise Linux High Availability Add-On cluster

The following information describes the configuration of a Red Hat Enterprise Linux (RHEL) High Availability Add-On cluster for managing SAP HANA system replication in a multitarget replication scenario. The cluster uses virtual server instances in [IBM® Power® Virtual Server](#) as cluster nodes.

You can connect multiple systems in an SAP HANA multitarget system replication topology to achieve a higher level of availability. A third SAP HANA instance runs on a virtual server instance in IBM Power Virtual Server in another workspace. The resource agents for SAP HANA in the Red Hat Enterprise Linux 8 (RHEL) HA add-on require that the third SAP HANA instance is managed manually and is installed on a virtual server instance outside the cluster.

In a *multitarget system replication* scenario, one secondary SAP HANA system runs on a virtual server instance in the cluster and another secondary HANA system runs on a virtual server instance that is deployed in a *Disaster Recovery (DR) site*. The *DR site* is implemented in a different IBM Power Virtual Server workspace in another geographical location or zone. The SAP HANA system replication operation mode must be identical for all multitarget replication levels.

A takeover of the secondary system in the *DR site* must be triggered manually.



Note: This information is intended for architects and specialists that are planning a high-availability deployment of SAP HANA on Power Virtual Server.

Before you begin

Review the general requirements, product documentation, support articles, and SAP notes listed in [Implementing high availability for SAP applications on IBM Power Virtual Server References](#).

Prerequisites

- A Red Hat High Availability cluster is deployed on two virtual server instances in one workspace in Power Virtual Server. Follow the instructions in the following documents.
 - [Implementing a Red Hat Enterprise Linux High Availability Add-On cluster](#).
 - [Configuring SAP HANA scale-up system replication in a Red Hat Enterprise Linux High Availability Add-On cluster](#).
- A third virtual server instance is deployed in another workspace in Power Virtual Server.
- SAP HANA is installed on the third virtual server instance with the same **SID** and **Instance Number**.
- Optional - you can reserve a virtual IP address for the system on NODE3 as described in [Reserving virtual IP addresses](#). Assigning and unassigning this virtual IP address on NODE3 is a manual task and not part of a cluster operation.

Setting up a multitarget scenario

A multitarget scenario is an extension of the setup that is described in [Configuring SAP HANA scale-up system replication in a Red Hat Enterprise Linux High Availability Add-On cluster](#). Make sure that you complete the setup for the system replication cluster before you continue with the following steps.

To simplify the cluster operations, you can set the **AUTOMATED_REGISTER** cluster attribute of the **SAPHana** resource to **true**. With **AUTOMATED_REGISTER=true**, the cluster performs an automatic registration of the previous primary as a new secondary after the failed node reappears in the cluster.

On a cluster node, run the following command to verify the `AUTOMATED_REGISTER` cluster attribute of the resource.

```
$ pcs resource config SAPHana_${SID}_${INSTNO}
```

Sample output:

```
# pcs resource config SAPHana_${SID}_${INSTNO}
Resource: SAPHana_HDB_00 (class=ocf provider=heartbeat type=SAPHana)
  Attributes: AUTOMATED_REGISTER=true DUPLICATE_PRIMARY_TIMEOUT=900 InstanceNumber=00 PREFER_SITE_TAKEOVER=True SID=HDB
  Operations: demote interval=0s timeout=3600 (SAPHana_HDB_00-demote-interval-0s)
    methods interval=0s timeout=5 (SAPHana_HDB_00-methods-interval-0s)
    monitor interval=121 role=Slave timeout=700 (SAPHana_HDB_00-monitor-interval-121)
    monitor interval=119 role=Master timeout=700 (SAPHana_HDB_00-monitor-interval-119)
    promote interval=0s timeout=3600 (SAPHana_HDB_00-promote-interval-0s)
    reload interval=0s timeout=5 (SAPHana_HDB_00-reload-interval-0s)
    start interval=0s timeout=3600 (SAPHana_HDB_00-start-interval-0s)
    stop interval=0s timeout=3600 (SAPHana_HDB_00-stop-interval-0s)
```

If the `AUTOMATED_REGISTER` cluster attribute is currently set to `false`, use the following command to enable the automatic registration.

```
$ pcs resource update SAPHana_${SID}_${INSTNO} AUTOMATED_REGISTER=true
```

Providing network connectivity between the workspaces

1. Use the information in [Creating the workspace](#) to create another workspace in a different geographic location or region.
2. Create subnets and make sure that the IP ranges don't overlap with any subnet of the workspace that hosts the virtual server instances for the cluster. For more information, see [Creating private network subnets](#).
3. Set up IBM Cloud® connections up in both workspaces and activate *Enable IBM Transit Gateway*. For more information, see [Creating Power Virtual Server Cloud Connections](#).
4. Deploy an IBM Cloud Transit Gateway to interconnect the two IBM Power Virtual Server workspaces.



Note: IBM Cloud Transit Gateway enables the interconnection of IBM Power Virtual Server, IBM Cloud classic, and Virtual Private Cloud (VPC) infrastructures and keeps data within the IBM Cloud networks. For more information about planning and deploying IBM Cloud Transit Gateway, see [Planning for IBM Cloud Transit Gateway](#) and [Ordering IBM Cloud Transit Gateway](#).

5. To add the connections to your transit gateway to establish network connectivity between your IBM Power Virtual Server, open the [Transit Gateway](#) page.
6. Select the name of your transit gateway.
7. Click **Add connection**.
8. Choose **Power Systems Virtual Server** as network connection, and select the **Location** of your workspace.
9. Click **Add** to create a connection.

Preparing environment variables on NODE3

To simplify the setup, prepare the following environment variables for user ID `root` on NODE3. These environment variables are used in subsequent commands in the remainder of the instructions.

On NODE3, create a file with the following environment variables. Then, adapt the variables according to the configuration of your SAP HANA system.

```
export SID=<SID>          # SAP HANA System ID (uppercase)
export sid=<sid>            # SAP HANA System ID (lowercase)
export INSTNO=<INSTNO>      # SAP HANA Instance Number

export DC3=<Site3>          # HANA System Replication Site Name 3

export NODE1=<Hostname 1>   # Hostname of virtual server instance 1 (production primary)
export NODE2=<Hostname 2>   # Hostname of virtual server instance 2 (production secondary)
export NODE3=<Hostname 3>   # Hostname of virtual server instance 3 (production tertiary)
```

You must source this file before you can use the sample commands in the remainder of this document.

For example, if you created a file that is named `sap_dr_site.sh`, run the following command on NODE3 to set the environment variables.

```
$ source sap_dr_site.sh
```

⚠ Important: Every time that you start a new terminal session, you must run the previous `source` command. Alternatively, you can move the environment variables file to the `/etc/profile.d` directory for the duration of the cluster configuration. In this example, the file is sourced automatically each time you log in to the server.

Verifying network connectivity between the virtual server instances

Verify the network connectivity between the two cluster nodes (NODE1 and NODE2) and NODE3.

1. Log in to both NODE1 and NODE2, and `ping` NODE3.

```
$ ping -c 3 ${NODE3}
```

Sample output:

```
# ping -c 3 cl-hdb-3
PING cl-hdb-3 (10.40.20.70) 56(84) bytes of data.
64 bytes from 10.40.20.70 (10.40.20.70): icmp_seq=1 ttl=46 time=78.2 ms
64 bytes from 10.40.20.70 (10.40.20.70): icmp_seq=2 ttl=46 time=78.3 ms
64 bytes from 10.40.20.70 (10.40.20.70): icmp_seq=3 ttl=46 time=78.2 ms

--- cl-hdb-3 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 78.197/78.233/78.264/0.027 ms
```

2. Log in to NODE3 and `ping` NODE1.

```
$ ping -c 3 ${NODE1}
```

Sample output:

```
# ping -c 3 cl-hdb-1
PING cl-hdb-1 (10.40.10.60) 56(84) bytes of data.
64 bytes from cl-hdb-1 (10.40.10.60): icmp_seq=1 ttl=46 time=78.3 ms
64 bytes from cl-hdb-1 (10.40.10.60): icmp_seq=2 ttl=46 time=78.2 ms
64 bytes from cl-hdb-1 (10.40.10.60): icmp_seq=3 ttl=46 time=78.3 ms

--- cl-hdb-1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 78.245/78.268/78.287/0.229 ms
```

3. Log in to NODE3 and `ping` NODE2.

```
$ ping -c 3 ${NODE2}
```

Sample output:

```
# ping -c 3 cl-hdb-2
PING cl-hdb-2 (10.40.10.194) 56(84) bytes of data.
64 bytes from cl-hdb-2 (10.40.10.194): icmp_seq=1 ttl=46 time=77.6 ms
64 bytes from cl-hdb-2 (10.40.10.194): icmp_seq=2 ttl=46 time=79.1 ms
64 bytes from cl-hdb-2 (10.40.10.194): icmp_seq=3 ttl=46 time=77.7 ms

--- cl-hdb-2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 77.649/78.129/79.071/0.703 ms
```

Copying PKI SSFS storage certificate files to NODE3

The SAP HANA 2.0 data and log transmission channels for the replication process require authentication by using the system `PKI SSFS` storage

certificate files.

- [2369981 - Required configuration steps for authentication with HANA System Replication](#))

The system PKI SSFS storage certificate files are stored in `/usr/sap/${SID}/SYS/global/security/rsecssfs/` in subdirectories `data` and `key`.

On NODE3, run the following commands to copy files `SSFS_${SID}.DAT` and `SSFS_${SID}.KEY` from NODE1.

```
$ scp ${NODE1}:/usr/sap/${SID}/SYS/global/security/rsecssfs/data/SSFS_${SID}.DAT  
/usr/sap/${SID}/SYS/global/security/rsecssfs/data/SSFS_${SID}.DAT
```

```
$ scp ${NODE1}:/usr/sap/${SID}/SYS/global/security/rsecssfs/key/SSFS_${SID}.KEY  
/usr/sap/${SID}/SYS/global/security/rsecssfs/key/SSFS_${SID}.KEY
```

The copied *PKI SSFS* storage certificates on NODE3 become active during the start of the SAP HANA system. Therefore, it is recommended to copy the files when the SAP HANA system on NODE3 is stopped.

Registering NODE3 as a secondary SAP HANA DR system replication system

Register the SAP HANA system as a secondary DR system replication instance.

1. On NODE3, stop the SAP HANA system.

```
$ sudo -i -u ${sid}adm -- HDB stop
```

2. On NODE3, register the secondary SAP HANA instance with NODE1.

```
$ sudo -i -u ${sid}adm -- \
    hdbnsutil -sr_register \
        --name=${DC3} \
        --remoteHost=${NODE1} \
        --remoteInstance=${INSTNO} \
        --replicationMode=async \
        --operationMode=logreplay \
        --online
```

3. On NODE3, start the secondary SAP HANA instance.

```
$ sudo -i -u ${sid}adm -- HDB start
```

Checking the SAP HANA system replication status

You can monitor the system replication status by using the following tools.

- SAP HANA cockpit
 - SAP HANA studio
 - `hdbnsutil` command-line tool
 - `systemReplicationStatus.py` Python script
 - SQL queries

The full output of the `systemReplicationStatus.py` script is available on only the primary system, as a database connection is required to obtain some of the status information.

On NODE1, check the system replication status by using the `systemReplicationStatus.py` Python script.

```
$ sudo -i -u ${sid}adm -- HDBSettings.sh systemReplicationStatus.py
```

Sample output:

```

|-----|-----|-----|-----|-----|
|SYSTEMDB |cl-hdb-1 |30001 |nameserver | 1 | 1 |SiteA |cl-hdb-3 | 30001 | 3 |SiteC
|YES |ASYNC |ACTIVE | 2 | 1 |SiteA |cl-hdb-3 | 30007 | 3 |SiteC
|HDB |cl-hdb-1 |30007 |xsengine | 3 | 1 |SiteA |cl-hdb-3 | 30003 | 3 |SiteC
|YES |ASYNC |ACTIVE | 1 | 1 |SiteA |cl-hdb-2 | 30001 | 2 |SiteB
|HDB |cl-hdb-1 |30007 |xsengine | 2 | 1 |SiteA |cl-hdb-2 | 30007 | 2 |SiteB
|YES |SYNCMEM |ACTIVE | 3 | 1 |SiteA |cl-hdb-2 | 30003 | 2 |SiteB
|YES |SYNCMEM |ACTIVE | 4 | 1 |SiteA |cl-hdb-1 | 30001 | 1 |SiteB

status system replication site "3": ACTIVE
status system replication site "2": ACTIVE
overall system replication status: ACTIVE

Local System Replication State
~~~~~
mode: PRIMARY
site id: 1
site name: SiteA

```

An alternative view of the system replication status is available with the `hdbnsutil` command.

On all nodes, run the following command to check the system replication status.

```
$ sudo -i -u ${sid}adm -- hdbnsutil -sr_state
```

Sample output on NODE1:

```

# sudo -i -u hdbadm -- hdbnsutil -sr_state

System Replication State
~~~~~

online: true

mode: primary
operation mode: primary
site id: 1
site name: SiteA

is source system: true
is secondary/consumer system: false
has secondaries/consumers attached: true
is a takeover active: false
is primary suspended: false

Host Mappings:
~~~~~

cl-hdb-1 -> [SiteC] cl-hdb-3
cl-hdb-1 -> [SiteB] cl-hdb-2
cl-hdb-1 -> [SiteA] cl-hdb-1

Site Mappings:
~~~~~

SiteA (primary/primary)
|---SiteC (async/logreplay)
|---SiteB (syncmem/logreplay)

Tier of SiteA: 1
Tier of SiteC: 2
Tier of SiteB: 2

Replication mode of SiteA: primary

```

```

Replication mode of SiteC: async
Replication mode of SiteB: syncmem

Operation mode of SiteA: primary
Operation mode of SiteC: logreplay
Operation mode of SiteB: logreplay

Mapping: SiteA -> SiteC
Mapping: SiteA -> SiteB

Hint based routing site:
done.

```

Sample output on NODE2:

```

# sudo -i -u hdbadm -- hdbnsutil -sr_state

System Replication State
~~~~~

online: true

mode: syncmem
operation mode: logreplay
site id: 2
site name: SiteB

is source system: true
is secondary/consumer system: true
has secondaries/consumers attached: false
is a takeover active: false
is primary suspended: false
is timetravel enabled: false
replay mode: auto
active primary site: 1

primary masters: cl-hdb-1

Host Mappings:
~~~~~

cl-hdb-2 -> [SiteC] cl-hdb-3
cl-hdb-2 -> [SiteB] cl-hdb-2
cl-hdb-2 -> [SiteA] cl-hdb-1

Site Mappings:
~~~~~

SiteA (primary/primary)
|---SiteC (async/logreplay)
|---SiteB (syncmem/logreplay)

Tier of SiteA: 1
Tier of SiteC: 2
Tier of SiteB: 2

Replication mode of SiteA: primary
Replication mode of SiteC: async
Replication mode of SiteB: syncmem

Operation mode of SiteA: primary
Operation mode of SiteC: logreplay
Operation mode of SiteB: logreplay

Mapping: SiteA -> SiteC
Mapping: SiteA -> SiteB

Hint based routing site:
done.

```

Sample output on NODE3:

```
# sudo -i -u hdbadm -- hdbnsutil -sr_state

System Replication State
~~~~~

online: true

mode: async
operation mode: logreplay
site id: 3
site name: SiteC

is source system: false
is secondary/consumer system: true
has secondaries/consumers attached: false
is a takeover active: false
is primary suspended: false
is timetravel enabled: false
replay mode: auto
active primary site: 1

primary masters: cl-hdb-1

Host Mappings:
~~~~~

cl-hdb-3 -> [SiteC] cl-hdb-3
cl-hdb-3 -> [SiteB] cl-hdb-2
cl-hdb-3 -> [SiteA] cl-hdb-1

Site Mappings:
~~~~~

SiteA (primary/primary)
|---SiteC (async/logreplay)
|---SiteB (syncmem/logreplay)

Tier of SiteA: 1
Tier of SiteC: 2
Tier of SiteB: 2

Replication mode of SiteA: primary
Replication mode of SiteC: async
Replication mode of SiteB: syncmem

Operation mode of SiteA: primary
Operation mode of SiteC: logreplay
Operation mode of SiteB: logreplay

Mapping: SiteA -> SiteC
Mapping: SiteA -> SiteB

Hint based routing site:
done.
done.
```

On all nodes, run the following command to check the replication mode and the operation mode.

```
$ sudo -i -u ${sid}adm -- \
    hdbnsutil -sr_state \
    --sapcontrol=1 2>/dev/null | grep -E "site(Operation|Replication)Mode"
```

Sample output:

```
# sudo -i -u ${sid}adm -- hdbnsutil -sr_state --sapcontrol=1 2>/dev/null | grep -E "site(Operation|Replication)Mode"
siteReplicationMode/SiteA=primary
siteReplicationMode/SiteB=syncmem
```

```
siteOperationMode/SiteA=primary  
siteOperationMode/SiteB=logreplay
```

Enabling automatic registration of secondaries after a takeover

In multitarget replication scenarios, SAP HANA can automatically reregister the secondaries that were previously registered before a takeover. To enable this feature, set the parameter `register_secondaries_on_takeover` in the `[system_replication]` section in the `global.ini` file to `true`. After a failover of an SAP HANA primary system to a secondary, the other secondary system reregisters automatically to the new primary system.

This option must be added to the `global.ini` file on all potential primary sites.

On all three nodes, run the following command to change the parameter.

```
$ sudo -i -u ${sid}adm -- <<EOT  
    python \${DIR_INSTANCE}/exe/python_support/setParameter.py \  
        -set SYSTEM/global.ini/system_replication/register_secondaries_on_takeover=true  
EOT
```

Verify the `[system_replication]` section in the `global.ini` configuration file.

```
$ cat /hana/shared/\${SID}/global/hdb/custom/config/global.ini
```

Testing the SAP HANA system replication cluster

It is vital to thoroughly test the cluster configuration to make sure that the cluster is working correctly. The following information provides a few sample failover test scenarios, but is not a complete list of test scenarios.

For example, the description of each test case includes the following information.

- Component that is tested
- Description of the test
- Prerequisites and the initial state before the failover test
- Test procedure
- Expected behavior and results
- Recovery procedure

Test1 - Testing the failure of the primary database instance

Use the following information to test the failure of the primary database instance.

Test1 - Description

Simulate a crash of the primary SAP HANA database instance that runs on NODE1.

Test1 - Prerequisites

- A functional two-node RHEL HA Add-On cluster for HANA system replication.
- Both cluster nodes are active.
- The cluster is started on NODE1 and NODE2.
- The cluster resource `SAPHana_\${SID}_\${INSTNO}` is configured with `AUTOMATED_REGISTER=true`.
- Check SAP HANA system replication status:
 - SAP HANA multitarget system replication is activated and in sync.
 - The primary SAP HANA system runs on NODE1.
 - The secondary SAP HANA system runs on NODE2.
 - Another secondary SAP HANA system runs on NODE3 at the `DR site` and is registered with NODE1.

Check the current system replication status on NODE1.

```
$ sudo -i -u ${sid}adm -- HDBSettings.sh systemReplicationStatus.py
```

Sample output:

```
# sudo -i -u hdbadm -- HDBSettings.sh systemReplicationStatus.py
|Database |Host      |Port    |Service Name |Volume ID |Site ID |Site Name |Secondary |Secondary |Secondary |Secondary |
|Secondary   |Replication |Replication |Replication   |Secondary   |
|           |           |           |           |           |           |           |           |           |           |
|Active Status |Mode      |Status     |Status Details |Fully Synced | | | | | |
|---|---|---|---|---|---|---|---|---|---|
|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
|SYSTEMDB |cl-hdb-1 |30001  |nameserver  |1 |1 |SiteA    |cl-hdb-3 |30001  |3 |SiteC
|YES      |ASYNC    |ACTIVE    |           |           |True |           |           |           |
|HDB      |cl-hdb-1 |30007  |xsengine   |2 |1 |SiteA    |cl-hdb-3 |30007  |3 |SiteC
|YES      |ASYNC    |ACTIVE    |           |           |True |           |           |
|HDB      |cl-hdb-1 |30003  |indexserver|3 |1 |SiteA    |cl-hdb-3 |30003  |3 |SiteC
|YES      |ASYNC    |ACTIVE    |           |           |True |           |           |
|SYSTEMDB |cl-hdb-2 |30001  |nameserver  |1 |2 |SiteA    |cl-hdb-2 |30001  |2 |SiteB
|YES      |SYNCMEM  |ACTIVE    |           |           |True |           |           |
|HDB      |cl-hdb-2 |30007  |xsengine   |2 |2 |SiteA    |cl-hdb-2 |30007  |2 |SiteB
|YES      |SYNCMEM  |ACTIVE    |           |           |True |           |           |
|HDB      |cl-hdb-2 |30003  |indexserver|3 |2 |SiteA    |cl-hdb-2 |30003  |2 |SiteB
|YES      |SYNCMEM  |ACTIVE    |           |           |True |           |           |

status system replication site "3": ACTIVE
status system replication site "2": ACTIVE
overall system replication status: ACTIVE

Local System Replication State
~~~~~
mode: PRIMARY
site id: 1
site name: SiteA
```

Test1 - Test procedure

Crash SAP HANA primary by sending a SIGKILL signal as user `${sid}adm`.

On NODE1, run the following command.

```
$ sudo -i -u ${sid}adm -- HDB kill-9
```

Test1 - Expected behavior

- The SAP HANA primary instance on NODE1 crashes.
- The cluster detects the stopped primary and marks the resource as `undefined`.
- The cluster promotes the secondary SAP HANA system on NODE2, which takes over as primary.
- The cluster releases the virtual IP address on NODE1, and acquires it on the primary on NODE2.
- If an application, such as SAP NetWeaver, is connected to a tenant database of SAP HANA, the application automatically reconnects to the new primary.
- The secondary HANA system that runs on NODE3 at the *DR site* is automatically reregistered to the new primary that runs on NODE2.
- The cluster waits until the primary on NODE2 is fully active and registers the failed instance on NODE1 as a secondary.
- The cluster starts the secondary HANA instance on NODE1.

On NODE1, run the following command to check the cluster status.

```
$ pcs status --full
```

Sample output:

```
pcs status --full
Cluster name: HDB_cluster
Cluster Summary:
  * Stack: corosync
  * Current DC: cl-hdb-1 (1) (version 2.0.5-9.el8_4.5-ba59be7122) - partition with quorum
  * Last updated: Mon Oct  9 10:46:59 2023
  * Last change: Mon Oct  9 10:46:54 2023 by root via crm_attribute on cl-hdb-2
  * 2 nodes configured
```

```

* 6 resource instances configured

Node List:
* Online: [ cl-hdb-1 (1) cl-hdb-2 (2) ]

Full List of Resources:
* res_fence_ibm_powervs      (stonith:fence_ibm_powervs):      Started cl-hdb-1
* vip_HDB_00_primary   (ocf::heartbeat:IPaddr2):      Started cl-hdb-2
* Clone Set: SAPHanaTopology_HDB_00-clone [SAPHanaTopology_HDB_00]:
  * SAPHanaTopology_HDB_00    (ocf::heartbeat:SAPHanaTopology):      Started cl-hdb-1
  * SAPHanaTopology_HDB_00    (ocf::heartbeat:SAPHanaTopology):      Started cl-hdb-2
* Clone Set: SAPHana_HDB_00-clone [SAPHana_HDB_00] (promotable):
  * SAPHana_HDB_00    (ocf::heartbeat:SAPHana):      Slave cl-hdb-1
  * SAPHana_HDB_00    (ocf::heartbeat:SAPHana):      Master cl-hdb-2

Node Attributes:
* Node: cl-hdb-1 (1):
  * hana_hdb_clone_state      : DEMOTED
  * hana_hdb_op_mode          : logreplay
  * hana_hdb_remoteHost       : cl-hdb-2
  * hana_hdb_roles            : 4:S:master1:master:worker:master
  * hana_hdb_site              : SiteA
  * hana_hdb_sra                :
  * hana_hdb_srah              :
  * hana_hdb_srmode            : syncmem
  * hana_hdb_sync_state        : SOK
  * hana_hdb_version           : 2.00.070.00
  * hana_hdb_vhost             : cl-hdb-1
  * lpa_hdb_lpt                :
  * master-SAPHana_HDB_00      : 100

* Node: cl-hdb-2 (2):
  * hana_hdb_clone_state      : PROMOTED
  * hana_hdb_op_mode          : logreplay
  * hana_hdb_remoteHost       : cl-hdb-1
  * hana_hdb_roles            : 4:P:master1:master:worker:master
  * hana_hdb_site              : SiteB
  * hana_hdb_sra                :
  * hana_hdb_srah              :
  * hana_hdb_srmode            : syncmem
  * hana_hdb_sync_state        : PRIM
  * hana_hdb_version           : 2.00.070.00
  * hana_hdb_vhost             : cl-hdb-2
  * lpa_hdb_lpt                :
  * master-SAPHana_HDB_00      : 150

Migration Summary:
* Node: cl-hdb-1 (1):
  * SAPHana_HDB_00: migration-threshold=5000 fail-count=1 last-failure='Mon Oct 9 10:39:58 2023'

Failed Resource Actions:
* SAPHana_HDB_00_monitor_119000 on cl-hdb-1 'master (failed)' (9): call=31, status='complete', exitreason='', last-rc-change='2023-10-09 10:39:58 +02:00', queued=0ms, exec=0ms

Tickets:

PCSD Status:
  cl-hdb-1: Online
  cl-hdb-2: Online

Daemon Status:
  corosync: active/disabled
  pacemaker: active/disabled
  pcsd: active/enabled

```

On NODE2, run the following command to check the system replication status.

```
$ sudo -i -u ${sid}adm -- HDBSettings.sh systemReplicationStatus.py
```

Sample output:

```
# sudo -i -u hdbadm -- HDBSettings.sh systemReplicationStatus.py
|Database |Host      |Port    |Service Name |Volume ID |Site ID |Site Name |Secondary |Secondary |Secondary |Secondary |
|Secondary   |Replication |Replication |Replication   |Replication |Secondary   |
|           |           |           |           |           |           |           |           |           |           |           |
|Active Status |Mode      |Status     |Status Details |Fully Synced | | | | | |
|---|---|---|---|---|---|---|---|---|---|
|----- |----- |----- |----- |----- |----- |----- |----- |----- |----- |
|SYSTEMDB |cl-hdb-2 |30001 |nameserver |           |1 |           |2 |SiteB |cl-hdb-3 |           |3 |SiteC
|YES       |ASYNC    |ACTIVE    |           |           |   |           |   |True  |           |   |
|HDB       |cl-hdb-2 |30007 |xsengine  |           |2 |           |2 |SiteB |cl-hdb-3 |           |3 |SiteC
|YES       |ASYNC    |ACTIVE    |           |           |   |           |   |True  |           |   |
|HDB       |cl-hdb-2 |30003 |indexserver |           |3 |           |2 |SiteB |cl-hdb-3 |           |3 |SiteC
|YES       |ASYNC    |ACTIVE    |           |           |   |           |   |True  |           |   |
|SYSTEMDB |cl-hdb-2 |30001 |nameserver |           |1 |           |2 |SiteB |cl-hdb-1 |           |1 |SiteA
|YES       |SYNCMEM  |ACTIVE    |           |           |   |           |   |True  |           |   |
|HDB       |cl-hdb-2 |30007 |xsengine  |           |2 |           |2 |SiteB |cl-hdb-1 |           |1 |SiteA
|YES       |SYNCMEM  |ACTIVE    |           |           |   |           |   |True  |           |   |
|HDB       |cl-hdb-2 |30003 |indexserver |           |3 |           |2 |SiteB |cl-hdb-1 |           |1 |SiteA
|YES       |SYNCMEM  |ACTIVE    |           |           |   |           |   |True  |           |   |

status system replication site "3": ACTIVE
status system replication site "1": ACTIVE
overall system replication status: ACTIVE

Local System Replication State
~~~~~
mode: PRIMARY
site id: 2
site name: SiteB
```

The SAP HANA primary runs on NODE2 at `SiteB`. The secondary on NODE3 is automatically reregistered to the new primary that runs on NODE2. As the cluster resource `SAPHana_${SID}_${INSTNO}` is configured with `AUTOMATED_REGISTER=true`, the cluster registers the SAP HANA system on NODE1 automatically as a secondary to the primary on NODE2.

Test2 - Testing the manual move of a SAPHana resource to another node

Use the following information to test the manual move of the SAPHana resource to another node.

Test2 - Description

Use cluster commands to move the primary instance to the other cluster node.

Test2 - Prerequisites

- A functional two-node RHEL HA Add-On cluster for HANA system replication.
- Both cluster nodes are active.
- The cluster is started on NODE1 and NODE2.
- The cluster resource `SAPHana_${SID}_${INSTNO}` is configured with `AUTOMATED_REGISTER=true`.
- Check SAP HANA system replication status:
 - HANA system replication is activated and in sync.
 - The primary SAP HANA system runs on NODE2.
 - The secondary SAP HANA system runs on NODE1.
 - Another secondary SAP HANA system runs on NODE3 at the `DR site` and is registered with NODE2.

Test2 - Test procedure

1. On a cluster node, run the following command to move the primary back to NODE1.

```
$ pcs resource move SAPHana_${SID}_${INSTNO}-clone
```

Sample output:

```
# pcs resource move SAPHana_${SID}_${INSTNO}-clone
```

```
Warning: Creating location constraint 'cli-ban-SAPHana_HDB_00-clone-on-cl-hdb-2' with a score of -INFINITY for
resource SAPHana_HDB_00-clone on cl-hdb-2.
This will prevent SAPHana_HDB_00-clone from running on cl-hdb-2 until the constraint is removed
This will be the case even if cl-hdb-2 is the last node in the cluster
```

After the primary is active on NODE1, SAP HANA automatically reregisters the instance on NODE3 as a secondary to NODE1.

2. Wait until the primary is up on NODE1. Then, remove the location constraint.

```
$ pcs resource clear SAPHana_${SID}_${INSTNO}-clone
```

Sample output:

```
# pcs resource clear SAPHana_${SID}_${INSTNO}-clone
Removing constraint: cli-ban-SAPHana_HDB_00-clone-on-cl-hdb-2
```

This command clears the location constraint that was created by the move command. The cluster starts the SAP HANA system on NODE2.

3. Verify the system replication status on all three nodes as described in [Checking the SAP HANA system replication status](#).

Test2 - Expected behavior

- The cluster creates a location constraint to move the resource.
- The cluster triggers a takeover to the secondary HANA system on NODE1.
- If an application, such as SAP NetWeaver, is connected to a tenant database of SAP HANA, the application automatically reconnects to the new primary.
- Register NODE2 with the primary on NODE1.
- Run `pcs resource clear` command to remove the location constraint. This command triggers the start of the secondary instance on NODE2.
- The secondary HANA system that runs on NODE3 at the *DR site* is automatically reregistered to the new primary that runs on NODE1.

Test2 - Recovery procedure

No recovery procedure is required. The test sequence reestablished the initial SAP HANA multitarget system replication topology.

Test3 - Testing failure of node that runs the primary database

Use the following information to test the failure of the node that runs the primary database.

Test3 - Description

Simulate a crash of the node that runs the primary HANA database.

Test3 - Prerequisites

- A functional two-node RHEL HA Add-On cluster for HANA system replication.
- Both cluster nodes are active.
- The cluster is started on NODE1 and NODE2.
- The cluster resource `SAPHana_${SID}_${INSTNO}` is configured with `AUTOMATED_REGISTER=true`.
- Check SAP HANA system replication status:
 - HANA system replication is activated and in sync.
 - The primary SAP HANA system runs on NODE1.
 - The secondary SAP HANA system runs on NODE2.
 - Another secondary SAP HANA system runs on NODE3 at the *DR site* and is registered with NODE1.

Test3 - Test procedure

Crash the primary on NODE1 by sending a *crash* system request.

On NODE1, run the following command.

```
$ sync; echo c > /proc/sysrq-trigger
```

Test3 - Expected behavior

- NODE1 crashes.
 - The cluster detects the failed node and sets its state to **OFFLINE**.
 - The cluster promotes the secondary HANA database on NODE2 to take over as the new primary.
 - The cluster acquires the virtual IP address on NODE2.
 - If an application, such as SAP NetWeaver, is connected to a tenant database of SAP HANA, the application automatically reconnects to the new primary.
 - The secondary SAP HANA system that runs on NODE3 at the *DR site* is automatically reregistered to NODE2.

Verify the SAP HANA system replication status on NODE2.

```
$ sudo -i -u ${sid}adm -- HDBSettings.sh systemReplicationStatus.py
```

Sample output:

```
# sudo -i -u hdbadm -- HDBSettings.sh systemReplicationStatus.py
Database | Host | Port | Service Name | Volume ID | Site ID | Site Name | Secondary | Secondary | Secondary | Secondary
| Secondary | Replication | Replication | Replication | Secondary | |
| | | | | | | Host | Port | Site ID | Site Name
| Active Status | Mode | Status | Status Details | Fully Synced |
| ----- | ----- | ----- | ----- | ----- | ----- | ----- | ----- | ----- | ----- | -----
|----- | ----- | ----- | ----- | ----- | ----- | ----- | ----- | ----- | ----- | -----
| SYSTEMDB | cl-hdb-2 | 30001 | nameserver | 1 | 2 | SiteB | cl-hdb-3 | 30001 | 3 | SiteC
| YES | ASYNC | ACTIVE | | | True | |
| HDB | cl-hdb-2 | 30007 | xsengine | 2 | 2 | SiteB | cl-hdb-3 | 30007 | 3 | SiteC
| YES | ASYNC | ACTIVE | | | True | |
| HDB | cl-hdb-2 | 30003 | indexserver | 3 | 2 | SiteB | cl-hdb-3 | 30003 | 3 | SiteC
| YES | ASYNC | ACTIVE | | | True | |

status system replication site "3": ACTIVE
overall system replication status: ACTIVE

Local System Replication State
~~~~~
```

Test3 - Recovery procedure

1. Log in to the IBM Cloud console and start NODE1.
 2. On NODE1, run the following command to start the cluster services

```
$ pcs cluster start
```

- 3 On a cluster node, run the following command to check the cluster status

```
$ pcs status --full
```

- #### 4 On NODE2 verify the SAP HANA system replication status

```
$ sudo -i -u ${sid}adm -- HDBSettings.sh systemReplicationStatus.py
```

```
# sudo -i -u hdbadm -- HDBSettings.sh systemReplicationStatus.py  
|Database|Host|Port|Service Name|Volume ID|Site ID|Site Name|Secondary|Secondary|Secondary
```

Name	Active	Status	Mode	Status	Status Details	Fully Synced	Host	Port	Site ID	Site
SYSTEMDB	YES	cl-hdb-2	HDB	30001	nameserver	1	2	SiteB	cl-hdb-3	30001 3 SiteC
ASYNC		ACTIVE					True			
xsengine	YES	cl-hdb-2	HDB	30007	xsengine	2	2	SiteB	cl-hdb-3	30007 3 SiteC
ACTIVE							True			
indexserver	HDB	cl-hdb-2	30003		indexserver	3	2	SiteB	cl-hdb-3	30003 3 SiteC
ASYNC							True			
nameserver	YES	cl-hdb-2	HDB	30001	nameserver	1	2	SiteB	cl-hdb-1	30001 1 SiteA
ACTIVE							True			
SYNCMEM	HDB	cl-hdb-2	30007		xsengine	2	2	SiteB	cl-hdb-1	30007 1 SiteA
ACTIVE							True			
indexserver	HDB	cl-hdb-2	30003		indexserver	3	2	SiteB	cl-hdb-1	30003 1 SiteA
ASYNC							True			
SYNCMEM	YES	cl-hdb-2								
ACTIVE										

```
status system replication site "3": ACTIVE
status system replication site "1": ACTIVE
overall system replication status: ACTIVE
```

Local System Replication State

```
mode: PRIMARY
site id: 2
site name: SiteB
```

- Run the steps in [Test2 - Test the manual move of SAP Hana resource to another node](#) to revert to the initial topology.

Test4 - Testing DR activation on the node that runs at the DR site

Use the following information to test the failure of both nodes in the primary workspace.

Test4 - Description

Simulate a crash of the nodes that run the primary and secondary SAP HANA databases.

Test4 - Prerequisites

- A functional two-node RHEL HA Add-On cluster for HANA system replication.
- Both cluster nodes are active.
- The cluster is started on NODE1 and NODE2.
- The cluster resource `SAPHana_${SID}_${INSTNO}` is configured with `AUTOMATED_REGISTER=true`.
- Check SAP HANA system replication status:
 - SAP HANA multitarget system replication is activated and in sync.
 - The primary SAP HANA system runs on NODE1.
 - The secondary SAP HANA system runs on NODE2.
 - Another secondary SAP HANA system runs on NODE3 at the *DR site* and is registered with NODE1.

Test4 - Test procedure

Crash primary on NODE1 and secondary on NODE2 by sending a `crash` system request on both nodes.

- On NODE1, run the following command.

```
$ sync; echo c > /proc/sysrq-trigger
```

- On NODE2, run the following command.

```
$ sync; echo c > /proc/sysrq-trigger
```

- On NODE3, run the following command to activate the HANA system as primary.

```
$ sudo -i -u ${sid}adm -- hdbnsutil -sr_takeover
```

Sample output:

```
# sudo -i -u hdbadm -- hdbnsutil -sr_takeover
done.
```

Test4 - Expected behavior

- NODE1 and NODE2 halt immediately.
- After the manual takeover, NODE3 runs the primary SAP HANA system.
- An application, such as SAP NetWeaver, can connect to the SAP HANA system on NODE3.

 **Important:** NODE3 is not part of the cluster and does not takeover the virtual IP address after a HANA system replication takeover. The start up of application servers that connect to NODE3 at the *DR site* requires extra effort, which is not described in this document.

On NODE3, run the following command to verify that the SAP HANA system runs as primary.

```
$ sudo -i -u ${sid}adm -- hdbnsutil -sr_state
```

Sample output:

```
# sudo -i -u hdbadm -- hdbnsutil -sr_state

System Replication State
~~~~~

online: true

mode: primary
operation mode: primary
site id: 3
site name: SiteC

is source system: true
is secondary/consumer system: false
has secondaries/consumers attached: false
is a takeover active: false
is primary suspended: false

Host Mappings:
~~~~~

cl-hdb-3 -> [SiteC] cl-hdb-3
cl-hdb-3 -> [SiteB] cl-hdb-2

Site Mappings:
~~~~~

SiteC (primary/primary)

Tier of SiteC: 1

Replication mode of SiteC: primary

Operation mode of SiteC: primary

Hint based routing site:
done.
```

Test4 - Recovery procedure

The recovery procedure after a takeover to the *DR site* is complex and is documented as a separate test in the *Test5* section.

Test5 - Restoring the original SAP HANA multitarget system replication topology

Use the following information to revert to the original system replication topology after a takeover to the SAP HANA system that runs at the *DR site*.

Check the following SAP documentation.

- [Restore the Original SAP HANA multitarget System Replication Configuration](#)

Test5 - Description

Restore the original system replication topology and reactivate the cluster in the primary workspace.

Test5 - Prerequisites

- A two-node RHEL HA Add-On cluster for HANA system replication in the primary workspace.
- Both virtual server instances of the cluster are stopped.
- The primary SAP HANA system runs on NODE3 at the *DR site*.

Test5 - Test procedure

1. Restart virtual server instances in the primary workspace.
 - a. Log in to the IBM Cloud console and start both NODE1 and NODE2.
 - b. Wait until both nodes are available.
 - c. Make sure that the Red Hat HA Add-On cluster services are stopped on both cluster nodes.
2. Register the SAP HANA system on NODE1 as a secondary.
 - a. On NODE3, verify that SAP HANA system replication is enabled.

```
$ sudo -i -u ${sid}adm -- hdbnsutil -sr_state
```

- b. On NODE1, run the following command to set an environment variable with the hostname of NODE3.

```
$ export NODE3=<Hostname 3> # Hostname of virtual server instance 3 (production tertiary)
```

- c. On NODE1, run the following command to register the SAP HANA system with the primary on NODE3.

```
$ sudo -i -u ${sid}adm -- \
  hdbnsutil -sr_register \
  --name=${DC1} \
  --remoteHost=${NODE3} \
  --remoteInstance=${INSTNO} \
  --replicationMode=async \
  --operationMode=logreplay \
  --online
```

- d. On NODE1, check the system replication configuration.

```
$ sudo -i -u ${sid}adm -- hdbnsutil -sr_state
```

Sample output:

```
System Replication State
~~~~~
online: false

mode: async
operation mode: unknown
site id: 1
site name: SiteA
```

```

is source system: unknown
is secondary/consumer system: true
has secondaries/consumers attached: unknown
is a takeover active: false
is primary suspended: false
is timetravel enabled: false
replay mode: auto
active primary site: 3

primary masters: cl-hdb-3
done.

```

- e. On NODE1, start the SAP HANA system to start the system replication.

```
$ sudo -i -u ${sid}adm -- HDB start
```

- f. On NODE3, check the system replication status and wait until the secondary on NODE1 is fully synchronized.

```
$ sudo -i -u ${sid}adm -- HDBSettings.sh systemReplicationStatus.py
```

Sample output:

```

# sudo -i -u hdbadm -- HDBSettings.sh systemReplicationStatus.py
|Database |Host      |Port    |Service Name |Volume ID |Site ID |Site Name |Secondary |Secondary |Secondary |
|Secondary |Secondary      |Replication |Replication |Replication |Secondary      |Secondary |Secondary |Secondary |
|          |           |           |           |           |           |           |           |           |           |
|Site Name |Active Status |Mode       |Status       |Status Details |Fully Synced | | | | |
|---|---|---|---|---|---|---|---|---|---|
|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
|SYSTEMDB |cl-hdb-3   |30001    |nameserver  |1          |3        |SiteC     |cl-hdb-1  |30001   |1
|SiteA    |YES         |ASYNC     |ACTIVE      |           |           |True      |           |
|HDB      |cl-hdb-3   |30007    |xsengine   |2          |3        |SiteC     |cl-hdb-1  |30007   |1
|SiteA    |YES         |ASYNC     |ACTIVE      |           |           |True      |           |
|HDB      |cl-hdb-3   |30003    |indexserver|3          |3        |SiteC     |cl-hdb-1  |30003   |1
|SiteA    |YES         |ASYNC     |ACTIVE      |           |           |True      |           |

status system replication site "1": ACTIVE
overall system replication status: ACTIVE

Local System Replication State
~~~~~
mode: PRIMARY
site id: 3
site name: SiteC

```

3. Initiate a fallback to the primary workspace.



Important: You need a downtime window to perform the move of the primary role back to NODE1.

To optimize the downtime window, the SAP HANA system on NODE2 can be registered as secondary to NODE3 now before the downtime window. The drawback is that a higher amount of data is transferred between the two Power Virtual Server workspaces.

In the following, the SAP HANA system on NODE2 is registered as secondary to NODE1 after NODE1 becomes primary again.

- Stop all applications and SAP application servers that are connected to NODE3.
- On NODE1, run the following command to takeover the primary role.

A *takeover with handshake* suspends all transactions on the primary system on NODE3 and the takeover is only executed when all remaining redo log is available on NODE1.

```
$ sudo -i -u ${sid}adm -- hdbnsutil -sr_takeover --suspendPrimary
```

- On NODE1, check that the HANA system runs as primary.

```
$ sudo -i -u ${sid}adm -- hdbnsutil -sr_state
```

- d. On NODE3, run the following command to verify the system replication status.

```
$ sudo -i -u ${sid}adm -- hdbnsutil -sr_state
```

Sample output:

```
# sudo -i -u ${sid}adm -- hdbnsutil -sr_state

System Replication State
~~~~~

online: true

SUSPEND PRIMARY ACTIVE
mode: primary
operation mode: primary
site id: 3
site name: SiteC

is source system: true
is secondary/consumer system: false
has secondaries/consumers attached: true
is a takeover active: false
is primary suspended: true

Host Mappings:
~~~~~

cl-hdb-3 -> [SiteC] cl-hdb-3
cl-hdb-3 -> [SiteB] cl-hdb-2
cl-hdb-3 -> [SiteA] cl-hdb-1

Site Mappings:
~~~~~

SiteC (primary/primary)
|---SiteA (async/logreplay)

Tier of SiteC: 1
Tier of SiteA: 2

Replication mode of SiteC: primary
Replication mode of SiteA: async

Operation mode of SiteC: primary
Operation mode of SiteA: logreplay

Mapping: SiteC -> SiteA

Hint based routing site:
done.
```

The following summary shows the status after these steps.

- NODE1 runs as primary, but no application is connected.
- NODE2 is up, but SAP HANA is not started.
- NODE3 is up and SAP HANA is blocked in *suspendPrimary* mode.
- Red Hat HA Add-On cluster services are stopped on NODE1 and NODE2.

4. Register the SAP HANA system on NODE2 as a secondary.

- a. On NODE2, run the following command to register the SAP HANA instance with the primary on NODE1.

```
$ sudo -i -u ${sid}adm -- \
  hdbnsutil -sr_register \
  --name=${DC2} \
  --remoteHost=${NODE1} \
  --remoteInstance=${INSTNO} \
  --replicationMode=syncmem \
```

```
--operationMode=logreplay \
--online
```

- b. On NODE2, start SAP HANA to start the replication.

```
$ sudo -i -u ${sid}adm -- HDB start
```

- c. On NODE1, check the system replication status and wait until the secondary on NODE2 is fully synchronized.

```
$ sudo -i -u ${sid}adm -- HDBSettings.sh systemReplicationStatus.py
```

Sample output:

```
# sudo -i -u hdbadm -- HDBSettings.sh systemReplicationStatus.py
|Database |Host      |Port    |Service Name |Volume ID |Site ID |Site Name |Secondary |Secondary |Secondary
|Secondary |Secondary   |Replication |Replication |Replication |Secondary   |Secondary   |
|          |           |           |           |           |           |           |           |           |
|Site Name |Active Status |Mode      |Status      |Status Details |Fully Synced |
|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
|SYSTEMDB  |cl-hdb-1  |30001   |nameserver  |1          |1        |SiteA     |cl-hdb-2  |30001   |2
|SiteB     |YES        |SYNCMEM   |ACTIVE      |           |           |True      |           |
|HDB       |cl-hdb-1  |30007   |xsengine   |2          |1        |SiteA     |cl-hdb-2  |30007   |2
|SiteB     |YES        |SYNCMEM   |ACTIVE      |           |           |True      |           |
|HDB       |cl-hdb-1  |30003   |indexserver|3          |1        |SiteA     |cl-hdb-2  |30003   |2
|SiteB     |YES        |SYNCMEM   |ACTIVE      |           |           |True      |           |

status system replication site "2": ACTIVE
overall system replication status: ACTIVE

Local System Replication State
~~~~~
mode: PRIMARY
site id: 1
site name: SiteA
```

The following summary shows the status after these steps.

- NODE1 runs as primary, but no application is connected.
- NODE2 runs as secondary.
- NODE3 is up and SAP HANA is blocked in `suspendPrimary` mode.
- Red Hat HA Add-On cluster services are stopped on NODE1 and NODE2.

5. Restart the cluster on NODE1 and NODE2.

- a. Stop the SAP HANA systems on NODE1 and NODE2.

On NODE1, run

```
$ sudo -i -u ${sid}adm -- HDB stop
```

On NODE2, run

```
$ sudo -i -u ${sid}adm -- HDB stop
```

- b. On a cluster node, run the following command to start the cluster.

```
$ pcs cluster start --all
```

- c. Check the cluster status and verify that it is fully operational again.

```
$ pcs status --full
```

- d. On NODE1, check the system replication status.

```
$ sudo -i -u ${sid}adm -- HDBSettings.sh systemReplicationStatus.py
```

Sample output:

```
# sudo -i -u ${sid}adm -- HDBSettings.sh systemReplicationStatus.py
Database |Host      |Port    |Service Name |Volume ID |Site ID |Site Name |Secondary |Secondary |Secondary
|Secondary |Secondary      |Replication |Replication |Replication     |Secondary      |
|          |          |           |           |           |           |           |Host       |Port      |Site ID
|Site Name |Active Status |Mode      |Status      |Status Details |Fully Synced | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
|SYSTEMDB |cl-hdb-1 |30001  |nameserver  |          1 |          1 |SiteA     |cl-hdb-2  | 30001  |      2
|SiteB   |YES        |SYNCFMEM |ACTIVE      |          |          |          |True      |          |
|HDB     |cl-hdb-1 |30007  |xsengine    |          2 |          1 |SiteA     |cl-hdb-2  | 30007  |      2
|SiteB   |YES        |SYNCFMEM |ACTIVE      |          |          |          |True      |          |
|HDB     |cl-hdb-1 |30003  |indexserver |          3 |          1 |SiteA     |cl-hdb-2  | 30003  |      2
|SiteB   |YES        |SYNCFMEM |ACTIVE      |          |          |          |True      |

status system replication site "2": ACTIVE
overall system replication status: ACTIVE

Local System Replication State
~~~~~
```

The following summary shows the status after these steps.

- NODE1 runs as primary.
 - NODE2 runs as secondary.
 - Red Hat HA Add-On cluster services are started and the cluster manages SAP HANA system replication on NODE1 and NODE2.
 - NODE3 is up and SAP HANA is blocked in *suspendPrimary* mode.

6. Register the SAP HANA system on NODE3 as a secondary.

- a. On NODE3, run the following command to register the system with NODE1.

```
$ sudo -i -u ${sid}adm -- \
  hdbnsutil -sr_register \
    --name=${DC3} \
    --remoteHost=${NODE1} \
    --remoteInstance=${INSTNO} \
    --replicationMode=async \
    --operationMode=logreplay \
    --online
```

- b. On NODE1, run the following command to verify the new SAP HANA system replication topology.

```
$ sudo -i -u ${sid}adm -- HDBSettings.sh systemReplicationStatus.py
```

The previous `hdbnsutil -sr_register` command triggers a restart of the SAP HANA system. During this restart, you might observe a `CONNECTION TIMEOUT` status in the output.

Sample output:

```

|SiteB |YES           |SYNCFMEM   |ACTIVE      |          |          |True    |
|HDB   |cl-hdb-1 |30003 |indexserver |       3 |       1 |SiteA    |cl-hdb-2 |30003 |     2
|SiteB |YES           |SYNCFMEM   |ACTIVE      |          |          |True    |
|SYSTEMDB|cl-hdb-2 |30001 |nameserver |       1 |       2 |SiteB    |cl-hdb-3 |30001 |     3
|SiteC |CONNECTION TIMEOUT |ASYNC     |UNKNOWN    |          |          |False   |
|HDB   |cl-hdb-2 |30007 |xsengine   |       2 |       2 |SiteB    |cl-hdb-3 |30007 |     3
|SiteC |CONNECTION TIMEOUT |ASYNC     |UNKNOWN    |          |          |False   |
|HDB   |cl-hdb-2 |30003 |indexserver |       3 |       2 |SiteB    |cl-hdb-3 |30003 |     3
|SiteC |CONNECTION TIMEOUT |ASYNC     |UNKNOWN    |          |          |False   |

```

```

status system replication site "2": ACTIVE
status system replication site "3": UNKNOWN
overall system replication status: UNKNOWN

```

Local System Replication State

```

mode: PRIMARY
site id: 1
site name: SiteA

```

In case the system does not automatically restart after the `hdbnsutil -sr_register` command, you need to stop and start it manually.

The following is a sample output of such a situation. The replication status of NODE3 shows `IS PRIMARY (e.g. after takeover)` and it does not change when you check the status multiple times.

```

# sudo -i -u ${sid}adm -- HDBSettings.sh systemReplicationStatus.py
|Database |Host      |Port      |Service Name |Volume ID |Site ID |Site Name |Secondary|Secondary |Secondary
|Secondary |Secondary |Replication |Replication |Replication |          |          |          |          |          |          |          |          |
|          |          |          |          |          |          |          |          |          |          |          |          |          |          |
|Site Name |Active Status |Mode      |Status      |Status Details |          |          |          |          |          |          |          |          |
|----- |----- |----- |----- |----- |----- |----- |----- |----- |----- |----- |----- |----- |
|SYSTEMDB |cl-hdb-1 |30001 |nameserver |       1 |       1 |SiteA    |cl-hdb-3 |30001 |     3 |
|PRIMARY  |          |          |          |          |          |          |          |          |          |          |          |          |
|HDB     |cl-hdb-1 |30007 |xsengine   |       2 |       1 |SiteA    |cl-hdb-3 |30007 |     3 |
|PRIMARY  |          |          |          |          |          |          |          |          |          |          |          |
|HDB     |cl-hdb-1 |30003 |indexserver |       3 |       1 |SiteA    |cl-hdb-3 |30003 |     3 |
|PRIMARY  |          |          |          |          |          |          |          |          |          |          |          |
|SYSTEMDB|cl-hdb-1 |30001 |nameserver |       1 |       1 |SiteA    |cl-hdb-2 |30001 |     2 |
|SiteB   |YES        |SYNCFMEM |ACTIVE     |          |          |          |          |          |          |          |          |
|HDB     |cl-hdb-1 |30007 |xsengine   |       2 |       1 |SiteA    |cl-hdb-2 |30007 |     2 |
|SiteB   |YES        |SYNCFMEM |ACTIVE     |          |          |          |          |          |          |          |
|HDB     |cl-hdb-1 |30003 |indexserver |       3 |       1 |SiteA    |cl-hdb-2 |30003 |     2 |
|SiteB   |YES        |SYNCFMEM |ACTIVE     |          |          |          |          |          |          |          |

```

```

status system replication site "3": ERROR
status system replication site "2": ACTIVE
overall system replication status: ERROR

```

Local System Replication State

```

mode: PRIMARY
site id: 1
site name: SiteA

```

On NODE3, run the following command to restart the secondary HANA system.

```
$ sudo -i -u ${sid}adm -- HDB restart
```

The following summary shows the final status after these steps.

- NODE1 runs as primary.
- NODE2 runs as secondary.
- NODE3 runs as another secondary at the *DR site*.
- NODE2 and NODE3 are both registered to NODE1.

- Red Hat HA Add-On cluster services are started and the cluster manages SAP HANA system replication on NODE1 and NODE2.

On NODE1, run the following command to verify the SAP HANA system replication topology.

```
$ sudo -i -u ${sid}adm -- HDBSettings.sh systemReplicationStatus.py
```

Sample output:

```
$ # sudo -i -u hdbadm -- HDBSettings.sh systemReplicationStatus.py
|Database |Host      |Port     |Service Name |Volume ID |Site ID |Site Name |Secondary |Secondary |Secondary |
|Secondary |Secondary      |Replication |Replication |Replication   |Secondary   |
|          |           |           |           |           |           |Host       |Port       |Site ID    |Site      |
|Name     |Active Status |Mode      |Status      |Status Details |Fully Synced | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
|SYSTEMDB |cl-hdb-1  |30001   |nameserver  |1          |1        |SiteA     |cl-hdb-2  |30001    |2        |SiteB    |
|YES      |SYNCFMEM   |ACTIVE    |           |           |True      |           |           |           |           |
|HDB      |cl-hdb-1  |30007   |xsengine   |2          |1        |SiteA     |cl-hdb-2  |30007    |2        |SiteB    |
|YES      |SYNCFMEM   |ACTIVE    |           |           |True      |           |           |           |
|HDB      |cl-hdb-1  |30003   |indexserver|3          |1        |SiteA     |cl-hdb-2  |30003    |2        |SiteB    |
|YES      |SYNCFMEM   |ACTIVE    |           |           |True      |           |           |           |
|SYSTEMDB |cl-hdb-2  |30001   |nameserver|1          |2        |SiteB     |cl-hdb-3  |30001    |3        |SiteC    |
|YES      |ASYNC      |ACTIVE    |           |           |True      |           |           |           |
|HDB      |cl-hdb-2  |30007   |xsengine   |2          |2        |SiteB     |cl-hdb-3  |30007    |3        |SiteC    |
|YES      |ASYNC      |ACTIVE    |           |           |True      |           |           |           |
|HDB      |cl-hdb-2  |30003   |indexserver|3          |2        |SiteB     |cl-hdb-3  |30003    |3        |SiteC    |
|YES      |ASYNC      |ACTIVE    |           |           |True      |           |           |           |

status system replication site "2": ACTIVE
status system replication site "3": ACTIVE
overall system replication status: ACTIVE

Local System Replication State
-----
mode: PRIMARY
site id: 1
site name: SiteA
```

Configuring high availability for SAP S/4HANA (ASCS and ERS) in a Red Hat Enterprise Linux High Availability Add-On cluster

The following information describes the configuration of *ABAP SAP Central Services (ASCS)* and *Enqueue Replication Server (ERS)* in a Red Hat Enterprise Linux (RHEL) High Availability Add-On cluster. The cluster uses virtual server instances in [IBM® Power® Virtual Server](#) as cluster nodes.

This example configuration applies to the second generation of the [Standalone Enqueue Server](#), also called *ENSA2*.

Starting with the release of SAP S/4HANA 1809, ENSA2 is installed by default, and can be configured in a two-node or multi-node cluster. This example uses the *ENSA2* setup for a two-node RHEL HA Add-On cluster. If the *ASCS* service fails in a two-node cluster, it restarts on the node where the *ERS* instance is running. The lock entries for the SAP application are then restored from the copy of the lock table in the *ERS* instance. When an administrator activates the failed cluster node, the *ERS* instance moves to the other node (anti-collocation) to protect its copy of the lock table.

It is recommended that you install the SAP database instance and other SAP application server instances on virtual server instances outside the two-node cluster for *ASCS* and *ERS*.

Before you begin

Review the general requirements, product documentation, support articles, and SAP notes listed in [Implementing high availability for SAP applications on IBM Power Virtual Server References](#).

Prerequisites

- This information describes a setup that uses shareable storage volumes accessible on both cluster nodes. Certain file systems are created on shareable storage volumes so that they can be mounted on both cluster nodes. This setup applies to both instance

directories.

- `/usr/sap/<SID>/ASCS<INSTNO>` of the ASCS instance.
- `/usr/sap/<SID>/ERS<INSTNO>` of the ERS instance.

Make sure that the storage volumes that were created for these file systems are attached to both virtual server instances. During SAP instance installation and RHEL HA Add-On cluster configuration, each instance directory must be mounted on its appropriate node. HA-LVM ensures that each of the two instance directories is mounted on only one node at a time.



Important: Different storage setups for the instance directories, such as NFS mounts, are possible. Storage setup steps for file storage or creation of cluster file system resources are not described in this document.

- The virtual hostnames for the ASCS and ERS instances must meet the requirements as documented in [Hostnames of SAP ABAP Platform servers](#). Make sure that the virtual IP addresses for the SAP instances are assigned to a network adapter and that they can communicate in the network.
- SAP application server instances require a common shared file system `sapmnt /sapmnt/<SID>` with *read and write* access, and other shared file systems such as `saptrans /usr/sap/trans`. These file systems are typically provided by an external NFS server. The NFS server must be high-available and must not be installed on virtual servers that are part of the ENSA2 cluster.

[Configuring an Active-Passive NFS Server in a Red Hat High Availability Cluster](#) describes the implementation of an active-passive NFS server in a RHEL HA Add-On cluster with Red Hat Enterprise Linux 8 by using virtual server instances in Power Virtual Server. The RHEL HA Add-On cluster for the active-passive NFS server must be deployed in a single Power Virtual Server workspace.

Preparing nodes to install ASCS and ERS instances

The following information describes how to prepare the nodes for installing the SAP ASCS and ERS instances.

Preparing environment variables

To simplify the setup, prepare the following environment variables for user `root` on both cluster nodes. These environment variables are used with later operating system commands in this information.

On both nodes, set the following environment variables.

```
# General settings
export SID=<SID>                      # SAP System ID (uppercase)
export sid=<sid>                        # SAP System ID (lowercase)

# ASCS instance
export ASCS_INSTNO=<INSTNO>          # ASCS instance number
export ASCS_VH=<virtual hostname>    # ASCS virtual hostname
export ASCS_IP=<IP address>          # ASCS virtual IP address
export ASCS_VG=<vg name>            # ASCS volume group name
export ASCS_LV=<lv name>            # ASCS logical volume name

# ERS instance
export ERS_INSTNO=<INSTNO>          # ERS instance number
export ERS_VH=<virtual hostname>    # ERS virtual hostname
export ERS_IP=<IP address>          # ERS virtual IP address
export ERS_VG=<vg name>            # ERS volume group name
export ERS_LV=<lv name>            # ERS logical volume name

# NFS settings
export NFS_SERVER="NFS server"        # Hostname or IP address of the highly available NFS server
export NFS_SHARE="NFS server directory" # Exported file system directory on the NFS server
export NFS_OPTIONS="rw,sec=sys"        # Sample NFS client mount options
```

It is recommended to use meaningful names for the volume groups and logical volumes that designate their content. For example, include the *SID* and *ascsv* or *ers* in the name. Don't use hyphens in the volume group or logical volume names.

- s01ascsv and s01ascslv
- s01ersvg and s01erslv

Assigning virtual IP addresses

Review the information in [Reserving virtual IP addresses](#).

Check whether the virtual IP address for the SAP instance is present. Otherwise, you need to identify the correct network adapter to assign the IP address.

On both nodes, check the list of currently active IP addresses.

```
$ ip -o -f inet address show | '/scope global/ {print $2, $4}'
```

Sample output of the previous command.

```
# ip -o -f inet address show | awk '/scope global/ {print $2, $4}'  
env2 10.51.0.66/24  
env3 10.52.0.41/24  
env4 10.111.1.28/24
```

The device name of the network adapter appears in the first column. The second column lists the active IP addresses and the number of bits that are reserved for the netmask - which are separated by a slash.

If the virtual IP address for the SAP instance is not present, make sure that it isn't erroneously set on another virtual server instance.

On NODE1, run the following command.

```
$ ping -c 3 ${ASCS_VH}
```

Sample output:

```
# ping -c 2 cl-sap-scs  
PING cl-sap-scs (10.111.1.248) 56(84) bytes of data.  
From cl-sap-1.tst.ibm.com (10.111.1.28) icmp_seq=1 Destination Host Unreachable  
From cl-sap-1.tst.ibm.com (10.111.1.28) icmp_seq=2 Destination Host Unreachable  
  
--- cl-sap-ers ping statistics ---  
2 packets transmitted, 0 received, +2 errors, 100% packet loss, time 2112ms  
pipe 3
```

If the `ping` output shows `Destination Host Unreachable`, the IP address is available, and you can assign the IP alias to the virtual server instance. Use the correct device name `env` of the network adapter that matches the subnet of the IP address.

Example command on NODE1:

```
$ ip addr add ${ASCS_IP} dev env4
```

Example command on NODE2:

```
$ ip addr add ${ERS_IP} dev env4
```



Note: According to your specific network configuration, the device name for the network adapter might be different.

The IP address is required for the SAP installation, and is set manually. Later, the virtual IP addresses are controlled by the Red Hat HA Cluster Add-on.

Preparing volume groups, logical volumes, and shared file systems

Shared storage is an important resource in an *ENSA2* cluster. *ASCS* and *ERS* must be able to run on both nodes, and their runtime environment is stored in the shared storage volumes. All cluster nodes need to access the shared storage volumes, but only one node has exclusive read and write access to a volume.

Preparing Logical Volume Manager high availability settings

Edit the file `/etc/lvm/lvm.conf` to include the *system ID* in the volume group.

On both nodes, edit the `lvm.conf` file.

```
$ vi /etc/lvm/lvm.conf
```

Search for the `system_id_source` parameter and change its value to `uname`.

Sample setting for the `system_id_source` parameter in `/etc/lvm/lvm.conf`.

```
system_id_source = "uname"
```

Identifying World Wide Names of shared storage volumes

Determine the World Wide Name (WWN) for each storage volume that is part of one of the shared volume groups.

1. Log in to IBM Cloud® to the [Storage volumes](#) view of Power Virtual Server.
2. Select your **workspace**.
3. Filter on the *volume prefix* in the *Storage volumes* list, and identify all the **World Wide Names** of the volumes that are in scope for ASCS and ERS instances. The *World Wide Name* is a 32-digit hexadecimal number.



Tip: Make sure that the attribute **Shareable** is *On* for those volumes.

In the [Virtual server instances](#) view, go to both virtual server instances of the cluster. Verify that all volumes that are in scope for ASCS and ERS are attached to both virtual server instances.

When you attach a new storage volume to a virtual server instance, make sure that you *rescan the SCSI bus* to detect the new volume. Afterward, update the *multipath configuration* of the virtual server instance.

On the nodes with new storage volume attachments, run the following command.

```
$ rescan-scsi-bus.sh && sleep 10 && multipathd reconfigure
```

Log in to both cluster nodes, and add the **WWN** to the environment variables of user `root`.



Tip: Use the `pvs --all` command to determine the appropriate **WWN** values.

On NODE1, export the `ASCS_PVID` environment variable.

```
export ASCS_PVID=3<WWN> # WWN of shared storage volume for ASCS
```

On NODE2, export the `ERS_PVID` environment variable.

```
export ERS_PVID=3<WWN> # WWN of shared storage volume for ERS
```



Tip: Make sure that you set the environment variable by using the hexadecimal number with lowercase letters.

Creating physical volumes

On NODE1, run the following command.

```
$ pvcreate /dev/mapper/${ASCS_PVID}
```

Sample output:

```
# pvcreate /dev/mapper/${ASCS_PVID}
Physical volume "/dev/mapper/36005076810810335700000000002ddc" successfully created.
```

On NODE2, run the following command.

```
$ pvcreate /dev/mapper/${ERS_PVID}
```

Sample output:

```
# pvcreate /dev/mapper/${ERS_PVID}
Physical volume "/dev/mapper/36005076810810335700000000002e31" successfully created.
```

Creating volume groups

Create the volume group for the *ASCS*.

On NODE1, run the following command.

```
$ vgcreate ${ASCS_VG} /dev/mapper/${ASCS_PVID}
```

Verify that the *System ID* is set.

```
$ vgs -o+systemid
```

Sample output:

```
# vgs -o+systemid
VG          #PV #LV #SN Attr   VSize   VFree   System ID
s01ascsvg    1   0   0 wz--n- <50.00g <50.00g cl-sap-1
```

Create the volume group for the *ERS*.

On NODE2, run the following command.

```
$ vgcreate ${ERS_VG} /dev/mapper/${ERS_PVID}
```

Verify that the System ID is set.

Sample output:

```
# vgs -o+systemid
VG          #PV #LV #SN Attr   VSize   VFree   System ID
s01ersvg     1   0   0 wz--n- <50.00g <50.00g cl-sap-2
```

Creating logical volumes and file systems

Create the logical volume for the *ASCS* and format it as an *XFS* file system.

On NODE1, run the following commands.

```
$ lvcreate -l 100%FREE -n ${ASCS_LV} ${ASCS_VG}
```

```
$ mkfs.xfs /dev/${ASCS_VG}/${ASCS_LV}
```

Create the logical volume for the *ERS* and format it as an *XFS* file system.

On NODE2, run the following commands.

```
$ lvcreate -l 100%FREE -n ${ERS_LV} ${ERS_VG}
```

```
$ mkfs.xfs /dev/${ERS_VG}/${ERS_LV}
```

Making sure that a volume group is not activated on multiple cluster nodes

Volume groups that are managed by the cluster must not activate automatically on startup.

Tip: For RHEL 8.5 and later, disable autoactivation when creating the volume group by specifying the `--setautoactivation n` flag on the `vgcreate` command.

On both nodes, edit the `/etc/lvm/lvm.conf` file and modify the `auto_activation_volume_list` entry to limit autoactivation to specific volume groups.

```
$ vi /etc/lvm/lvm.conf
```

Locate the `auto_activation_volume_list` parameter and add all volume groups except the one you defined for the NFS cluster to this list.

See an example of how to set the `auto_activation_volume_list` entry in `/etc/lvm/lvm.conf`:

```
auto_activation_volume_list = [ "rhel_root" ]
```

Rebuild the `initramfs` boot image to make sure that the boot image does not activate a volume group that is controlled by the cluster.

On both nodes, run the following command.

```
$ dracut -H -f /boot/initramfs-$(uname -r).img $(uname -r)
```

Reboot both nodes.

Mounting the file systems for SAP installation

Activate the volume groups and mount the SAP instance file systems.

On *NODE1 (ASCS)*, run the following commands.

```
$ vgchange -a y ${ASCS_VG}
```

```
$ mkdir -p /usr/sap/${SID}/ASCS${ASCS_INSTNO}
```

```
$ mount /dev/${ASCS_VG}/${ASCS_LV} /usr/sap/${SID}/ASCS${ASCS_INSTNO}
```

On *NODE2 (ERS)*, run the following commands.

```
$ vgchange -a y ${ERS_VG}
```

```
$ mkdir -p /usr/sap/${SID}/ERS${ERS_INSTNO}
```

```
$ mount /dev/${ERS_VG}/${ERS_LV} /usr/sap/${SID}/ERS${ERS_INSTNO}
```

Mounting the required NFS file systems

On both nodes, make sure that the NFS file systems `/sapmnt` and `/usr/sap/trans` are mounted.

```
$ mount | grep nfs
```

Creating ASCS and ERS mount points on the other node

Create the mount points for the instance file systems and adjust their ownership.

On *NODE1*, run the following commands.

```
$ mkdir /usr/sap/${SID}/ERS${ERS_INSTNO}
```

```
$ chown ${sid}adm:sapsys /usr/sap/${SID}/ERS${ERS_INSTNO}
```

On *NODE2*, run the following commands.

```
$ mkdir /usr/sap/${SID}/ASCS${ASCS_INSTNO}
```

```
$ chown ${sid}adm:sapsys /usr/sap/${SID}/ASCS${ASCS_INSTNO}
```

Installing the ASCS and ERS instances

Use the SAP Software Provisioning Manager (SWPM) to install both instances.

- Install SAP instances on the cluster nodes.
 - Install an ASCS instance on *NODE1* by using the virtual hostname `${ASCS_VH}` that is associated with the virtual IP address for

ASCS:

```
<swpm>/sapinst SAPINST_USE_HOSTNAME=${ASCS_VH}
```

- Install an *EBS* instance on NODE2 by using the virtual hostname `${ERS_VH}` that is associated with the virtual IP address for *EBS*:

```
<swpm>/sapinst SAPINST_USE_HOSTNAME=${ERS_VH}
```

- Install all other SAP application instances outside the cluster.

Installing and setting up the RHEL HA Add-On cluster

Install and set up the RHEL HA Add-On cluster according to [Implementing a Red Hat Enterprise Linux High Availability Add-On cluster](#).

Configure and test fencing as described in [Creating the fencing device](#).

Preparing the ASCS and ERS instances for cluster integration

Use the following steps to prepare the SAP instances for the cluster integration.

Disabling the automatic start of the SAP instance agents for ASCS and ERS

You must disable the automatic start of the `sapstartsrv` instance agents for both ASCS and ERS instances after a reboot.

Verifying the SAP instance agent integration type

Recent versions of the SAP instance agent `sapstartsrv` provide native `systemd` support on Linux. For more information, refer to the SAP notes that are listed at [SAP Notes](#).

On both nodes, check the content of the `/usr/sap/sapservices` file.

```
$ cat /usr/sap/sapservices
```

In the `systemd` format, the lines start with `systemctl` entries.

Example:

```
systemctl --no-ask-password start SAPS01_01 # sapstartsrv pf=/usr/sap/S01/SYS/profile/S01_ASCS01_cl-sap-scs
```

If the entries for ASCS and ERS are in `systemd` format, continue with the steps in [Disabling systemd services of the ASCS and the ERS SAP instance](#).

In the `classic` format, the lines start with `LD_LIBRARY_PATH` entries.

Example:

```
LD_LIBRARY_PATH=/usr/sap/S01/ASC01/exe:$LD_LIBRARY_PATH;export LD_LIBRARY_PATH;/usr/sap/S01/ASC01/exe/sapstartsrv  
pf=/usr/sap/S01/SYS/profile/S01_ASCS01_cl-sap-scs -D -u s01adm
```

If the entries for ASCS and ERS are in `classic` format, then modify the `/usr/sap/sapservices` file to prevent the automatic start of the `sapstartsrv` instance agent for both ASCS and ERS instances after a reboot.

On both nodes, remove or comment out the `sapstartsrv` entries for both ASCS and ERS in the SAP services file.

```
$ sed -i -e 's/^LD_LIBRARY_PATH=/#LD_LIBRARY_PATH=/' /usr/sap/sapservices
```

Example:

```
#LD_LIBRARY_PATH=/usr/sap/S01/ASC01/exe:$LD_LIBRARY_PATH;export LD_LIBRARY_PATH;/usr/sap/S01/ASC01/exe/sapstartsrv  
pf=/usr/sap/S01/SYS/profile/S01_ASCS01_cl-sap-scs -D -u s01adm
```

Proceed to [Installing permanent SAP license keys](#).

Disabling systemd services of the ASCS and the ERS instances

On both nodes, disable the instance agent for the ASCS.

```
$ systemctl disable --now SAP${SID}_${ASCS_INSTNO}.service
```

On both nodes, disable the instance agent for the ERS.

```
$ systemctl disable --now SAP${SID}_${ERS_INSTNO}.service
```

Disabling systemd restart of a crashed ASCS or ERS instance

Systemd has its own mechanisms for restarting a crashed service. In a high availability setup, only the HA cluster is responsible for managing the SAP ASCS and ERS instances. Create **systemd drop-in files** on both cluster nodes to prevent **systemd** from restarting a crashed SAP instance.

On both nodes, create the directories for the drop-in files.

```
$ mkdir /etc/systemd/system/SAP${SID}_${ASCS_INSTNO}.service.d
```

```
$ mkdir /etc/systemd/system/SAP${SID}_${ERS_INSTNO}.service.d
```

On both nodes, create the drop-in files for ASCS and ERS.

```
$ cat >> /etc/systemd/system/SAP${SID}_${ASCS_INSTNO}.service.d/HA.conf << EOT
[Service]
Restart=no
EOT
```

```
$ cat >> /etc/systemd/system/SAP${SID}_${ERS_INSTNO}.service.d/HA.conf << EOT
[Service]
Restart=no
EOT
```



Note: `Restart=no` must be in the **[Service]** section, and the drop-in files must be available on all cluster nodes.

On both nodes, reload the **systemd** unit files.

```
$ systemctl daemon-reload
```

Installing permanent SAP license keys

When the SAP ASCS instance is installed on a Power Virtual Server instance, the SAP license mechanism relies on the partition UUID. For more information, see [SAP note 2879336 - Hardware key based on unique ID](#).

On both nodes, run the following command as user `<sid>adm` to identify the **HARDWARE KEY** of the node.

```
$ sudo -i -u ${sid}adm -- sh -c 'saplikey -get'
```

Sample output:

```
$ sudo -i -u ${sid}adm -- sh -c 'saplikey -get'
saplikey: HARDWARE KEY = H1428224519
```

Note the **HARDWARE KEY** of each node.

You need both hardware keys to request two different SAP license keys. Check the following SAP notes for more information about requesting SAP license keys:

- [2879336 - Hardware key based on unique ID](#)
- [2662880 - How to request SAP license keys for failover systems](#)

Installing SAP resource agents

Install the required software packages. The `resource-agents-sap` includes the *SAPInstance cluster resource agent* for managing the SAP instances.

Unless `sap_cluster_connector` is configured for the SAP instance, the RHEL HA Add-On cluster considers any state change of the instance as an issue. If other SAP tools such as `sapcontrol` are used to manage the instance, then `sap_cluster_connector` grants permission to control SAP instances that are running inside the cluster. If the SAP instances are managed by only cluster tools, the implementation of `sap_cluster_connector` is not necessary.

Install the packages for the resource agent and the *SAP Cluster Connector* library. For more information, see [How to enable the SAP HA Interface for SAP ABAP application server instances managed by the RHEL HA Add-On](#)

On both nodes, run the following commands.

If needed, use `subscription-manager` to enable the SAP NetWeaver repository. The [RHEL for SAP Subscriptions and Repositories](#) documentation describes how to enable the required repositories.

```
$ subscription-manager repos --enable="rhel-8-for-ppc64le-sap-netweaver-e4s-rpms"
```

Install the required packages.

```
$ dnf install -y resource-agents-sap sap-cluster-connector
```

Configuring SAP Cluster Connector

Add user `${sid}adm` to the `haclient` group.

On both nodes, run the following command.

```
$ usermod -a -G haclient ${sid}adm
```

Adapting the SAP instance profiles

Modify the start profiles of all SAP instances that are managed by *SAP tools* outside the cluster. Both *ASCS* and *EBS* instances can be controlled by the RHEL HA Add-On cluster and its resource agents. Adjust the SAP instance profiles to prevent an automatic restart of instance processes.

On NODE1, navigate to the SAP profile directory.

```
$ cd /sapmnt/${SID}/profile
```

Change all occurrences of `Restart_Program` to `Start_Program` in the instance profile of both *ASCS* and *EBS*.

```
$ sed -i -e 's/Restart_Program_\([0-9][0-9]\)/Start_Program_\1/' ${SID}_ASCS${ASCS_INSTNO}_${ASCS_VH}
```

```
$ sed -i -e 's/Restart_Program_\([0-9][0-9]\)/Start_Program_\1/' ${SID}_EBS${ERS_INSTNO}_${ERS_VH}
```

Add the following two lines at the end of the SAP instance profile to configure `sap_cluster_connector` for the *ASCS* and *EBS* instances.

```
service/halib = $(DIR_EXECUTABLE)/saphascriptco.so  
service/halib_cluster_connector = /usr/bin/sap_cluster_connector
```

Configuring ASCS and ERS cluster resources

Up to this point, the following are assumed:

- A RHEL HA Add-On cluster is running on both virtual server instances and fencing of the nodes was tested.
- The SAP System is running.
 - SAP *ASCS* is installed and active on node 1 of the cluster.
 - SAP *EBS* is installed and active on node 2 of the cluster.
- All steps in [Prepare ASCS and ERS instances for the cluster integration](#) are complete.

Configuring sapmnt cluster resource

Create a cloned *Filesystem* cluster resource to mount the *SAPMNT* share from an external NFS server to all cluster nodes.

Make sure that the environment variable `${NFS_VH}` is set to the virtual hostname of the NFS server, and `${NFS_OPTIONS}` is set to your

desired mount options.

On NODE1, run the following command.

```
$ pcs resource create fs_sapmnt Filesystem \
  device="${NFS_VH}:/${SID}/sapmnt" \
  directory="/sapmnt/${SID}" \
  fstype='nfs' \
  options="${NFS_OPTIONS}" \
  clone interleave=true
```

Configuring ASCS resource group

Create a resource for the virtual IP address of the ASCS.

On NODE1, run the following command.

```
$ pcs resource create ${sid}_vip_ascss${ASCS_INSTNO} IPAddr2 \
  ip=${ASCS_IP} \
  --group ${sid}_ascss${ASCS_INSTNO}_group
```

In this example of creating resources for an HA-LVM file system on a shared storage volume, you create resources for LVM-activate and for the instance file system of the ASCS.

```
$ pcs resource create ${sid}_fs_ascss${ASCS_INSTNO}_lvm LVM-activate \
  vgname="${ASCS_VG}" \
  vg_access_mode=system_id \
  --group ${sid}_ascss${ASCS_INSTNO}_group

$ pcs resource create ${sid}_fs_ascss${ASCS_INSTNO} Filesystem \
  device="/dev/mapper/${ASCS_VG}-${ASCS_LV}" \
  directory=/usr/sap/${SID}/ASCSS${ASCS_INSTNO} \
  fstype=xfs \
  --group ${sid}_ascss${ASCS_INSTNO}_group
```

In the alternative example that the instance file system of the ASCS is provided by an HA NFS server, only the file system resource is required. Make sure that you have defined the environment variable `${NFS_VH}` according to your *NFS server*, and that you have created a directory `${SID}/ASCSS` under the NFS root directory during the SAP installation of the ASCS instance.

```
$ pcs resource create ${sid}_fs_ascss${ASCS_INSTNO} Filesystem \
  device="${NFS_VH}:/${SID}/ASCSS" \
  directory=/usr/sap/${SID}/ASCSS${ASCS_INSTNO} \
  fstype=nfs \
  options="${NFS_OPTIONS}" \
  force_unmount=safe \
  op start interval=0 timeout=60 \
  op stop interval=0 timeout=120 \
  --group ${sid}_ascss${ASCS_INSTNO}_group
```

Create a resource for managing the ASCS instance.

```
$ pcs resource create ${sid}_ascss${ASCS_INSTNO} SAPInstance \
  InstanceName="${SID}_ASCSS${ASCS_INSTNO}_${ASCS_VH}" \
  START_PROFILE=/sapmnt/${SID}/profile/${SID}_ASCSS${ASCS_INSTNO}_${ASCS_VH} \
  AUTOMATIC_RECOVER=false \
  meta resource-stickiness=5000 \
  migration-threshold=1 failure-timeout=60 \
  op monitor interval=20 on-fail=restart timeout=60 \
  op start interval=0 timeout=600 \
  op stop interval=0 timeout=600 \
  --group ${sid}_ascss${ASCS_INSTNO}_group
```



Note: The `meta resource-stickiness=5000` option is used to balance the failover constraint with ERS so that the resource stays on the node where it started and doesn't migrate uncontrollably in the cluster.

Add a resource stickiness to the group to make sure that the ASCS remains on the node.

```
$ pcs resource meta ${sid}_ascss${ASCS_INSTNO}_group \
    resource-stickiness=3000
```

Configuring the ERS resource group

Create a resource for the virtual IP address of the *ERS*.

On NODE1, run the following command.

```
$ pcs resource create ${sid}_vip_ers${ERS_INSTNO} IPAddr2 \
    ip=${ERS_IP} \
    --group ${sid}_ers${ERS_INSTNO}_group
```

In the example of creating resources for an HA-LVM file system on a shared storage volume, you create resources for LVM-activate and for the instance file system of the *ERS*.

```
$ pcs resource create ${sid}_fs_ers${ERS_INSTNO}_lvm LVM-activate \
    vgname="${ERS_VG}" \
    vg_access_mode=system_id \
    --group ${sid}_ers${ERS_INSTNO}_group
```

```
$ pcs resource create ${sid}_fs_ers${ERS_INSTNO} Filesystem \
    device="/dev/mapper/${ERS_VG}-${ERS_LV}" \
    directory=/usr/sap/${SID}/ERS${ERS_INSTNO} \
    fstype=xfs \
    --group ${sid}_ers${ERS_INSTNO}_group
```

In the alternative example that the instance file system of the *ERS* is provided by an HA NFS server, only the file system resource is required. Make sure that you have defined the environment variable `${NFS_VH}` according to your *NFS* server, and that you have created a directory `${SID}/ERS` under the NFS root directory during the SAP installation of the *ERS* instance.

```
$ pcs resource create ${sid}_fs_ers${ERS_INSTNO} Filesystem \
    device="${NFS_VH}:${SID}/ERS" \
    directory=/usr/sap/${SID}/ERS${ERS_INSTNO} \
    fstype=nfs \
    options="${NFS_OPTIONS}" \
    force_unmount=safe \
    op start interval=0 timeout=60 \
    op stop interval=0 timeout=120 \
    --group ${sid}_ers${ERS_INSTNO}_group
```

Create a resource for managing the *ERS* instance.

```
$ pcs resource create ${sid}_ers${ERS_INSTNO} SAPInstance \
    InstanceName="${SID}_ERS${ERS_INSTNO}_${ERS_VH}" \
    START_PROFILE=/sapmnt/${SID}/profile/${SID}_ERS${ERS_INSTNO}_${ERS_VH} \
    AUTOMATIC_RECOVER=false \
    IS_ERS=true \
    op monitor interval=20 on-fail=restart timeout=60 \
    op start interval=0 timeout=600 \
    op stop interval=0 timeout=600 \
    --group ${sid}_ers${ERS_INSTNO}_group
```

Configuring cluster resource constraints

A colocation constraint prevents resource groups `${sid}_ascss${ASCS_INSTNO}_group` and `${sid}_ers${ERS_INSTNO}_group` from being active on the same node whenever possible. The stickiness score of `-5000` makes sure that they run on the same node if only a single node is available.

```
$ pcs constraint colocation add \
    ${sid}_ers${ERS_INSTNO}_group with ${sid}_ascss${ASCS_INSTNO}_group -- -5000
```

An order constraint controls that resource group `${sid}_ascss${ASCS_INSTNO}_group` starts before `${sid}_ers${ERS_INSTNO}_group`.

```
$ pcs constraint order start \
    ${sid}_ascss${ASCS_INSTNO}_group then stop ${sid}_ers${ERS_INSTNO}_group \
```

```
symmetrical=\nkind=Optional
```

The following two order constraints make sure that the file system `SAPMNT` mounts before resource groups `${sid}_ascs${ASCS_INSTNO}_group` and `${sid}_ers${ERS_INSTNO}_group` start.

```
$ pcs constraint order fs_sapmnt-clone then ${sid}_ascs${ASCS_INSTNO}_group
```

```
$ pcs constraint order fs_sapmnt-clone then ${sid}_ers${ERS_INSTNO}_group
```

The cluster setup is complete.

Testing an SAP ENSA2 cluster

It is vital to thoroughly test the cluster configuration to make sure that the cluster is working correctly. The following information provides a few sample failover test scenarios, but is not a complete list of test scenarios.

For example, the description of each test case includes the following information.

- Component under test
- Description of the test
- Prerequisites and the initial state before failover test
- Test procedure
- Expected behavior and results
- Recovery procedure

Test 1 - Testing a failure of the ASCS instance

Test 1 - Description

Simulate a crash of the SAP ASCS instance that is running on NODE1.

Test 1 - Prerequisites

- A functional two-node RHEL HA Add-On cluster for SAP ENSA2.
- Both cluster nodes are active.
- Cluster is started on NODE1 and NODE2.
 - Resource group `${sid}_ascs${ASCS_INSTNO}_group` is active on NODE1.
 - Resources `${sid}_vip_ascs${ASCS_INSTNO}`, `${sid}_fs_ascs${ASCS_INSTNO}_lvm`, `${sid}_fs_ascs${ASCS_INSTNO}` and `${sid}_ascs${ASCS_INSTNO}` are `Started` on NODE1.
 - Resource group `${sid}_ers${ERS_INSTNO}_group` is active on NODE2.
 - Resources `${sid}_vip_ers${ERS_INSTNO}`, `${sid}_fs_ers${ERS_INSTNO}_lvm`, `${sid}_fs_ers${ERS_INSTNO}` and `${sid}_ers${ERS_INSTNO}` are `Started` on NODE2.
- Check SAP instance processes:
 - ASCS instance is running on NODE1.
 - ERS instance is running on NODE2.

```
$ pcs status
```

Sample output:

```
# pcs status\nCluster name: SAP_ASCS\nCluster Summary:\n  * Stack: corosync\n  * Current DC: cl-sap-1 (version 2.0.5-9.el8_4.5-ba59be7122) - partition with quorum\n  * Last updated: Tue Feb 14 07:59:16 2023\n  * Last change: Tue Feb 14 05:02:22 2023 by hacluster via crmd on cl-sap-1\n  * 2 nodes configured\n  * 11 resource instances configured
```

```

Node List:
* Online: [ cl-sap-1 cl-sap-2 ]

Full List of Resources:
* res_fence_ibm_powervs (stonith:fence_ibm_powervs): Started cl-sap-2
* Resource Group: s01_ascos01_group:
  * s01_vip_ascos01 (ocf::heartbeat:IPaddr2): Started cl-sap-1
  * s01_fs_ascos01_lvm (ocf::heartbeat:LVM-activate): Started cl-sap-1
  * s01_fs_ascos01 (ocf::heartbeat:Filesystem): Started cl-sap-1
  * s01_ascos01 (ocf::heartbeat:SAPIstance): Started cl-sap-1
* Resource Group: s01_ers02_group:
  * s01_vip_ers02 (ocf::heartbeat:IPaddr2): Started cl-sap-2
  * s01_fs_ers02_lvm (ocf::heartbeat:LVM-activate): Started cl-sap-2
  * s01_fs_ers02 (ocf::heartbeat:Filesystem): Started cl-sap-2
  * s01_ers02 (ocf::heartbeat:SAPIstance): Started cl-sap-2
* Clone Set: fs_sapmnt-clone [fs_sapmnt]:
  * Started: [ cl-sap-1 cl-sap-2 ]

Daemon Status:
corosync: active/disabled
pacemaker: active/disabled
pcsd: active/enabled

```

Test 1 - Test Procedure

To crash the SAP ASCS instance, send a SIGKILL signal to the enqueue server as user `${sid}adm`.

On NODE1, identify the PID of the enqueue server.

```
$ pgrep -af "(en|enq).sap"
```

Send a SIGKILL signal to the identified process.

Sample output:

```
# pgrep -af "(en|enq).sap"
30186 en.sapS01_ASCS01_pf=/usr/sap/S01/SYS/profile/S01_ASCS01_cl-sap-scs
# kill -9 30186
```

Test 1 - Expected behavior

- SAP ASCS instance on NODE1 crashes.
- The cluster detects the crashed ASCS instance.
- The cluster stops the dependent resources on NODE1 (virtual IP address, file system `/usr/sap/${SID}/ASCSS{ASC斯_INSTNO}`, and the LVM resources), and acquires them on NODE2.
- The cluster starts the ASCS on NODE2.
- The cluster stops the ERS instance on NODE2.
- The cluster stops the dependent resources on NODE1 (virtual IP address, file system `/usr/sap/${SID}/ERS${ERS_INSTNO}`, and the LVM resources), and acquires them on NODE1.
- The cluster starts the ERS on NODE1.

After a few seconds, check the status with the following command.

```
$ pcs status
```

Sample output:

```
# pcs status
Cluster name: SAP_ASCS
Cluster Summary:
* Stack: corosync
* Current DC: cl-sap-1 (version 2.0.5-9.el8_4.5-ba59be7122) - partition with quorum
* Last updated: Tue Feb 14 08:10:18 2023
* Last change: Tue Feb 14 05:02:22 2023 by hacluster via crmd on cl-sap-1
* 2 nodes configured
```

```

* 11 resource instances configured

Node List:
* Online: [ cl-sap-1 cl-sap-2 ]

Full List of Resources:
* res_fence_ibm_powervs (stonith:fence_ibm_powervs): Started cl-sap-2
* Resource Group: s01_asc01_group:
  * s01_vip_asc01 (ocf::heartbeat:IPaddr2): Started cl-sap-2
  * s01_fs_asc01_lvm (ocf::heartbeat:LVM-activate): Started cl-sap-2
  * s01_fs_asc01 (ocf::heartbeat:Filesystem): Started cl-sap-2
  * s01_asc01 (ocf::heartbeat:SAPIstance): Started cl-sap-2
* Resource Group: s01_ers02_group:
  * s01_vip_ers02 (ocf::heartbeat:IPaddr2): Started cl-sap-1
  * s01_fs_ers02_lvm (ocf::heartbeat:LVM-activate): Started cl-sap-1
  * s01_fs_ers02 (ocf::heartbeat:Filesystem): Started cl-sap-1
  * s01_ers02 (ocf::heartbeat:SAPIstance): Started cl-sap-1
* Clone Set: fs_sapmnt-clone [fs_sapmnt]:
  * Started: [ cl-sap-1 cl-sap-2 ]

Daemon Status:
corosync: active/disabled
pacemaker: active/disabled
pcsd: active/enabled

```

Test 2 - Testing a failure of the node that is running the ASCS instance

Use the following information to test a failure of the node that is running the ASCS instance.

Test 2 - Description

Simulate a crash of the node where the ASCS instance is running.

Test 2 - Prerequisites

- A functional two-node RHEL HA Add-On cluster for SAP ENSA2.
- Both cluster nodes are active.
- Cluster is started on NODE1 and NODE2.
 - Resource group \${sid}_asc01_\${ASCS_INSTNO}_group is active on NODE2.
 - Resources \${sid}_vip_asc01_\${ASCS_INSTNO}, \${sid}_fs_asc01_\${ASCS_INSTNO}_lvm, \${sid}_fs_asc01_\${ASCS_INSTNO} and \${sid}_asc01_\${ASCS_INSTNO} are **Started** on NODE2.
 - Resource group \${sid}_ers02_\${ERS_INSTNO}_group is active on NODE1.
 - Resources \${sid}_vip_ers02_\${ERS_INSTNO}, \${sid}_fs_ers02_\${ERS_INSTNO}_lvm, \${sid}_fs_ers02_\${ERS_INSTNO} and \${sid}_ers02_\${ERS_INSTNO} are **Started** on NODE1.
- Check SAP instance processes:
 - ASCS instance is running on NODE2.
 - ERS instance is running on NODE1.

Test 2 - Test procedure

Crash NODE2 by sending a *crash* system request.

On NODE2, run the following command.

```
$ sync; echo c > /proc/sysrq-trigger
```

Test 2 - Expected behavior

- NODE2 restarts.
- The cluster detects the failed node and sets its state to offline (UNCLEAN).
- The cluster acquires the ASCS resources (virtual IP address, file system `/usr/sap/${SID}/ASCS${ASCS_INSTNO}`, and the LVM items) on NODE1.
- The cluster starts the ASCS on NODE1.

- The cluster stops the *ECS* instance on NODE1.
- The cluster stops the dependent resources on NODE1 (virtual IP address, file system `/usr/sap/${SID}/ERS${ECS_INSTNO}`, and the LVM resources), and releases them.

After a while, check the status with the following command.

 **Note:** The second node is offline and both resource groups are running on the first node.

```
$ pcs status
```

Sample output:

```
# pcs status
Cluster name: SAP_ASCS
Cluster Summary:
  * Stack: corosync
  * Current DC: cl-sap-1 (version 2.0.5-9.el8_4.5-ba59be7122) - partition with quorum
  * Last updated: Tue Feb 14 08:34:16 2023
  * Last change: Tue Feb 14 08:34:04 2023 by hacluster via crmd on cl-sap-1
  * 2 nodes configured
  * 11 resource instances configured

Node List:
  * Online: [ cl-sap-1 ]
  * OFFLINE: [ cl-sap-2 ]

Full List of Resources:
  * res_fence_ibm_powervs (stonith:fence_ibm_powervs): Started cl-sap-1
  * Resource Group: s01_ascos01_group:
    * s01_vip_ascos01 (ocf::heartbeat:IPaddr2): Started cl-sap-1
    * s01_fs_ascos01_lvm (ocf::heartbeat:LVM-activate): Started cl-sap-1
    * s01_fs_ascos01 (ocf::heartbeat:Filesystem): Started cl-sap-1
    * s01_ascos01 (ocf::heartbeat:SAPIstance): Started cl-sap-1
  * Resource Group: s01_ers02_group:
    * s01_vip_ers02 (ocf::heartbeat:IPaddr2): Started cl-sap-1
    * s01_fs_ers02_lvm (ocf::heartbeat:LVM-activate): Started cl-sap-1
    * s01_fs_ers02 (ocf::heartbeat:Filesystem): Started cl-sap-1
    * s01_ers02 (ocf::heartbeat:SAPIstance): Started cl-sap-1
  * Clone Set: fs_sapmnt-clone [fs_sapmnt]:
    * Started: [ cl-sap-1 ]
    * Stopped: [ cl-sap-2 ]

Daemon Status:
  corosync: active/disabled
  pacemaker: active/disabled
  pcsd: active/enabled
```

Test 2 - Recovery procedure

Wait until NODE2 restarts, then restart the cluster framework.

On NODE1, run the following command.

```
$ pcs cluster start
```

- The cluster starts on NODE2 and acquires the *ECS* resources (virtual IP address, file system `/usr/sap/${SID}/ERS${ECS_INSTNO}`, and the LVM resources) on NODE2.
- The cluster starts the *ECS* instance on NODE2.

Wait a moment and check the status with the following command. The *ECS* resource group moved to the second node.

```
$ pcs status
```

Sample output:

```

# pcs status
Cluster name: SAP_ASCS
Cluster Summary:
  * Stack: corosync
  * Current DC: cl-sap-1 (version 2.0.5-9.el8_4.5-ba59be7122) - partition with quorum
  * Last updated: Tue Feb 14 08:41:23 2023
  * Last change: Tue Feb 14 08:34:04 2023 by hacluster via crmd on cl-sap-1
  * 2 nodes configured
  * 11 resource instances configured

Node List:
  * Online: [ cl-sap-1 cl-sap-2 ]

Full List of Resources:
  * res_fence_ibm_powervs (stonith:fence_ibm_powervs): Started cl-sap-1
  * Resource Group: s01_asc01_group:
    * s01_vip_asc01 (ocf::heartbeat:IPaddr2): Started cl-sap-1
    * s01_fs_asc01_lvm (ocf::heartbeat:LVM-activate): Started cl-sap-1
    * s01_fs_asc01 (ocf::heartbeat:Filesystem): Started cl-sap-1
    * s01_asc01 (ocf::heartbeat:SAPIstance): Started cl-sap-1
  * Resource Group: s01_ers02_group:
    * s01_vip_ers02 (ocf::heartbeat:IPaddr2): Started cl-sap-2
    * s01_fs_ers02_lvm (ocf::heartbeat:LVM-activate): Started cl-sap-2
    * s01_fs_ers02 (ocf::heartbeat:Filesystem): Started cl-sap-2
    * s01_ers02 (ocf::heartbeat:SAPIstance): Started cl-sap-2
  * Clone Set: fs_sapmnt-clone [fs_sapmnt]:
    * Started: [ cl-sap-1 cl-sap-2 ]

Daemon Status:
  corosync: active/disabled
  pacemaker: active/disabled
  pcsd: active/enabled

```

Test 3 - Testing a failure of the *EBS* instance

Use the following information to test the failure of an ERS instance.

Test 3 - Description

Simulate a crash of the *EBS* instance.

Test 3 - Prerequisites

- A functional two-node RHEL HA Add-On cluster for SAP ENSA2.
- Both cluster nodes are active.
- Cluster starts on NODE1 and NODE2.
 - Resource group \${sid}_asc01_group is active on NODE1.
 - Resources \${sid}_vip_asc01, \${sid}_fs_asc01_lvm, \${sid}_fs_asc01 and \${sid}_asc01 are **Started** on NODE1.
 - Resource group \${sid}_ers02_group is active on NODE2.
 - Resources \${sid}_vip_ers02, \${sid}_fs_ers02_lvm, \${sid}_fs_ers02 and \${sid}_ers02 are **Started** on NODE2.
- Check SAP instance processes:
 - ASCS instance is running on NODE1.
 - ERS instance is running on NODE2.

Test 3 - Test Procedure

Crash the SAP *EBS* instance by sending a SIGKILL signal.

On NODE2, identify the PID of the enqueue replication server.

```
$ pgrep -af "(er|enqr).sap"
```

Send a SIGKILL signal to the identified process.

Sample output:

```
# pgrep -af "(er|enqr).sap"
2527198 er.sapS01_ERS02 pf=/usr/sap/S01/ERS02/profile/S01_ERS02_cl-sap-ers NR=01
# kill -9 2527198
```

Test 3 - Expected behavior

- SAP Enqueue Replication Server on NODE2 crashes immediately.
- The cluster detects the stopped *ERS* and marks the resource as failed.
- The cluster restarts the *ERS* on NODE2.

Check the status with the following command.

```
$ pcs status
```

The `${sid}_ers${ERS_INSTNO}` *ERS* resource restarted on the second node. If you run the `pcs status` command too soon, you might see the *ERS* resource briefly in status `FAILED`.

Sample output:

```
# pcs status
Cluster name: SAP_ASCS
Cluster Summary:
  * Stack: corosync
  * Current DC: cl-sap-1 (version 2.0.5-9.el8_4.5-ba59be7122) - partition with quorum
  * Last updated: Tue Feb 14 08:50:53 2023
  * Last change: Tue Feb 14 08:50:50 2023 by hacluster via crmd on cl-sap-2
  * 2 nodes configured
  * 11 resource instances configured

Node List:
  * Online: [ cl-sap-1 cl-sap-2 ]

Full List of Resources:
  * res_fence_ibm_powervs (stonith:fence_ibm_powervs): Started cl-sap-1
  * Resource Group: s01_asc01_group:
    * s01_vip_asc01 (ocf::heartbeat:IPaddr2): Started cl-sap-1
    * s01_fs_asc01_lvm (ocf::heartbeat:LVM-activate): Started cl-sap-1
    * s01_fs_asc01 (ocf::heartbeat:Filesystem): Started cl-sap-1
    * s01_asc01 (ocf::heartbeat:SAPIstance): Started cl-sap-1
  * Resource Group: s01_ers02_group:
    * s01_vip_ers02 (ocf::heartbeat:IPaddr2): Started cl-sap-2
    * s01_fs_ers02_lvm (ocf::heartbeat:LVM-activate): Started cl-sap-2
    * s01_fs_ers02 (ocf::heartbeat:Filesystem): Started cl-sap-2
    * s01_ers02 (ocf::heartbeat:SAPIstance): Started cl-sap-2
  * Clone Set: fs_sapmnt-clone [fs_sapmnt]:
    * Started: [ cl-sap-1 cl-sap-2 ]

Daemon Status:
  corosync: active/disabled
  pacemaker: active/disabled
  pcsd: active/enabled
```

Test 3 - Recovery Procedure

On NODE2, run the following commands.

```
$ pcs resource refresh
```

```
$ pcs status --full
```

Test 4 - Testing a manual move of the ASCS instance

Use the following information to test a manual move of an ASCS instance.

Test 4 - Description

Use SAP Control commands to move the ASCS instance to the other node for maintenance purposes.

Test 4 - Prerequisites

- A functional two-node RHEL HA Add-On cluster for SAP ENSA2.
- The `sap_cluster_connector` is installed and configured.
- Both cluster nodes are active.
- Cluster is started on NODE1 and NODE2.
 - Resource group \${sid}_ascss\${ASCS_INSTNO}_group is active on NODE1.
 - Resources \${sid}_vip_ascss\${ASCS_INSTNO}, \${sid}_fs_ascss\${ASCS_INSTNO}_lvm, \${sid}_fs_ascss\${ASCS_INSTNO} and \${sid}_ascss\${ASCS_INSTNO} are `Started` on NODE1.
 - Resource group \${sid}_ers\${ERS_INSTNO}_group is active on NODE2.
 - Resources \${sid}_vip_ers\${ERS_INSTNO}, \${sid}_fs_ers\${ERS_INSTNO}_lvm, \${sid}_fs_ers\${ERS_INSTNO} and \${sid}_ers\${ERS_INSTNO} are `Started` on NODE2.
- Check SAP instance processes:
 - ASCS instance is running on NODE1.
 - ERS instance is running on NODE2.

Test 4 - Test Procedure

Log in to NODE1 and run `sapcontrol` to move the ASCS instance to the other node.

```
$ sudo -i -u ${sid}adm -- sh -c "sapcontrol -nr ${ASCS_INSTNO} -function HAFailoverToNode"
```

Test 4 - Expected behavior

- `sapcontrol` interacts with the cluster through the `sap-cluster-connector`.
- The cluster creates location constraints to move the resource.

Check the status with the following command. Keep in mind that the ASCS resource group moved to the second node. If you run the `pcs status` command too soon, you might see some resources `stopping` and `starting`.

```
$ pcs status
```

Sample output:

```
# pcs status
Cluster name: SAP_ASCS
Cluster Summary:
  * Stack: corosync
  * Current DC: cl-sap-1 (version 2.0.5-9.el8_4.5-ba59be7122) - partition with quorum
  * Last updated: Tue Feb 14 09:03:19 2023
  * Last change: Tue Feb 14 09:01:40 2023 by s01adm via crm_resource on cl-sap-1
  * 2 nodes configured
  * 11 resource instances configured

Node List:
  * Online: [ cl-sap-1 cl-sap-2 ]

Full List of Resources:
  * res_fence_ibm_powervs (stonith:fence_ibm_powervs): Started cl-sap-1
  * Resource Group: s01_ascss01_group:
    * s01_vip_ascss01 (ocf::heartbeat:IPAddr2): Started cl-sap-2
    * s01_fs_ascss01_lvm (ocf::heartbeat:LVM-activate): Started cl-sap-2
    * s01_fs_ascss01 (ocf::heartbeat:Filesystem): Started cl-sap-2
    * s01_ascss01 (ocf::heartbeat:SAPIstance): Started cl-sap-2
  * Resource Group: s01_ers02_group:
    * s01_vip_ers02 (ocf::heartbeat:IPAddr2): Started cl-sap-1
```

```

* s01_fs_ers02_lvm (ocf::heartbeat:LVM-activate): Started cl-sap-1
* s01_fs_ers02 (ocf::heartbeat:Filesystem): Started cl-sap-1
* s01_ers02 (ocf::heartbeat:SAPInstance): Started cl-sap-1
* Clone Set: fs_sapmnt-clone [fs_sapmnt]:
  * Started: [ cl-sap-1 cl-sap-2 ]

Daemon Status:
corosync: active/disabled
pacemaker: active/disabled
pcsd: active/enabled

```

Test 4 - Recovery Procedure

Wait until the ASCS instance is active on NODE2. After five minutes, the cluster removes the created location constraints automatically.

The following instructions show how to remove the constraints manually.

On NODE2, run the following command.

```
$ pcs constraint
```

Sample output:

```

# pcs constraint
Location Constraints:
Resource: s01_asc01_group
  Constraint: cli-ban-s01_asc01_group-on-cl-sap-1
    Rule: boolean-op=and score=-INFINITY
      Expression: #uname eq string cl-sap-1
      Expression: date lt 2023-02-08 09:33:50 -05:00
Ordering Constraints:
  start s01_asc01_group then stop s01_ers02_group (kind:Optional) (non-symmetrical)
  start fs_sapmnt-clone then start s01_asc01_group (kind:Mandatory)
  start fs_sapmnt-clone then start s01_ers02_group (kind:Mandatory)
Colocation Constraints:
  s01_ers02_group with s01_asc01_group (score:-5000)
Ticket Constraints:

```

```
$ pcs resource clear ${sid}_asc01_group
```

The *Location constraints* are removed:

```
$ pcs constraint
```

Sample output:

```

# pcs constraint
Location Constraints:
Ordering Constraints:
  start s01_asc01_group then stop s01_ers02_group (kind:Optional) (non-symmetrical)
  start fs_sapmnt-clone then start s01_asc01_group (kind:Mandatory)
  start fs_sapmnt-clone then start s01_ers02_group (kind:Mandatory)
Colocation Constraints:
  s01_ers02_group with s01_asc01_group (score:-5000)
Ticket Constraints:

```

Configuring high availability for SAP S/4HANA (ASCS and ERS) in a Red Hat Enterprise Linux High Availability Add-On cluster in a multizone region environment

The following information describes the configuration of *ABAP SAP Central Services (ASCS)* and *Enqueue Replication Server (ERS)* in a Red Hat Enterprise Linux (RHEL) High Availability Add-On cluster. The cluster uses virtual server instances in [IBM® Power® Virtual Server](#) as cluster nodes.

This example configuration applies to the second generation of the [Standalone Enqueue Server](#), also called *ENSA2*.

Starting with the release of SAP S/4HANA 1809, ENSA2 is installed by default, and can be configured in a two-node or multi-node cluster. This

example uses the *ENSA2* setup for a two-node RHEL HA Add-On cluster. If the *ASCS* service fails in a two-node cluster, it restarts on the node where the *ERS* instance is running. The lock entries for the SAP application are then restored from the copy of the lock table in the *ERS* instance. When an administrator activates the failed cluster node, the *ERS* instance moves to the other node (anti-collocation) to protect its copy of the lock table.

It is recommended that you install the SAP database instance and other SAP application server instances on virtual server instances outside the two-node cluster for *ASCS* and *ERS*.

Before you begin

Review the general requirements, product documentation, support articles, and SAP notes listed in [Implementing high availability for SAP applications on IBM Power Virtual Server References](#).

Prerequisites

- This information describes a setup that uses NFS mounted storage for the instance directories.
 - The *ASCS* instance uses the mount point `/usr/sap/<SID>/ASCS<INSTNO>`.
 - The *ERS* instance uses the mount point `/usr/sap/<SID>/ERS<INSTNO>`.
 - Both instances use the `/sapmnt/<SID>` mount point with shared *read and write* access.
 - Other shared file systems such as *saptrans* `/usr/sap/trans` might be needed.

! Important: Make sure that a highly available NFS server is configured to serve these shares. The NFS server must not be installed on a virtual server that is part of the *ENSA2* cluster. This document does not describe the steps for setting up file storage or creating cluster file system resources.

- The virtual hostnames for the *ASCS* and *ERS* instances must meet the requirements as documented in [Hostnames of SAP ABAP Platform servers](#).
- The subnets and the virtual IP addresses for the *ASCS* and *ERS* instances must not exist in the Power Virtual Server workspaces. They are configured as cluster resources. However, you must add the virtual IP addresses and virtual hostnames for the *ASCS* and *ERS* instances to the Domain Name Service (DNS) and to the `/etc/hosts` file on all cluster nodes.

Preparing nodes to install ASCS and ERS instances

The following information describes how to prepare the nodes for installing the SAP *ASCS* and *ERS* instances.

Preparing environment variables

To simplify the setup, prepare the following environment variables for user `root` on both cluster nodes. These environment variables are used with later operating system commands in this information.

On both nodes, set the following environment variables.

```
# General settings
export CLUSTERNAME="SAP_S01"          # Cluster name
export NODE1=<HOSTNAME_1>              # Virtual server instance 1 hostname
export NODE2=<HOSTNAME_2>              # Virtual server instance 2 hostname

export SID=<SID>                      # SAP System ID (uppercase)
export sid=<sid>                      # SAP System ID (lowercase)

# ASCS instance
export ASCS_INSTNO=<INSTNO>          # ASCS instance number
export ASCS_NET=<Subnet name>         # Name for the ASCS subnet in IBM Cloud
export ASCS_CIDR=<CIDR of subnet>     # CIDR of the ASCS subnet containing the service IP address
export ASCS_VH=<virtual hostname>      # ASCS virtual hostname
export ASCS_IP=<IP address>           # ASCS virtual IP address

# ERS instance
export ERS_INSTNO=<INSTNO>          # ERS instance number
export ERS_NET=<Subnet name>         # Name for the ERS subnet in IBM Cloud
export ERS_CIDR=<CIDR of subnet>     # CIDR of the ERS subnet containing the service IP address
export ERS_VH=<virtual hostname>      # ERS virtual hostname
export ERS_IP=<IP address>           # ERS virtual IP address
```

```

# Other multizone region settings
export CLOUD_REGION=<CLOUD_REGION>          # Multizone region name
export APIKEY="APIKEY or path to file"         # API key of the ServiceID for the resource agent
export API_TYPE="private or public"             # Use private or public API endpoints
export IBMCLOUD_CRN_1=<IBMCLOUD_CRN_1>        # Workspace 1 CRN
export IBMCLOUD_CRN_2=<IBMCLOUD_CRN_2>        # Workspace 2 CRN
export POWERVSI_1=<POWERVSI_1>                 # Virtual server 1 instance id
export POWERVSI_2=<POWERVSI_2>                 # Virtual server 2 instance id
export JUMBO="true or false"                   # Enable Jumbo frames

# NFS settings
export NFS_SERVER="NFS server"                # Hostname or IP address of the highly available NFS server
export NFS_SHARE="NFS server directory"         # Exported file system directory on the NFS server
export NFS_OPTIONS="rw,sec=sys"                 # Sample NFS client mount options

```

The following is an example of how to set the extra environment variables that are required for a multizone region implementation.

```

# General settings
export CLUSTERNAME="SAP_S01"                  # Cluster name
export NODE1="cl-s01-1"                        # Virtual service instance 1 hostname
export NODE2="cl-s01-2"                        # Virtual server instance 2 hostname

export SID="S01"                                # SAP System ID (uppercase)
export sid="s01"                                 # SAP System ID (lowercase)

# ASCS instance
export ASCS_INSTNO="21"                         # ASCS instance number
export ASCS_NET="s01-ascs-net"                   # Name for the ASCS subnet in IBM Cloud
export ASCS_CIDR="10.40.21.100/30"               # CIDR of the ASCS subnet containing the service IP address
export ASCS_VH="s01ascs"                         # ASCS virtual hostname
export ASCS_IP="10.40.21.102"                    # ASCS virtual IP address

# ERS instance
export ERS_INSTNO="22"                          # ERS instance number
export ERS_NET="s01-ers-net"                     # Name for the ERS subnet in IBM Cloud
export ERS_CIDR="10.40.22.100/30"               # CIDR of the ERS subnet containing the service IP address
export ERS_VH="s01ers"                           # ERS virtual hostname
export ERS_IP="10.40.22.102"                     # ERS virtual IP address

# Other multizone region settings
export CLOUD_REGION="eu-de"
export IBMCLOUD_CRN_1="crn:v1:bluemix:public:power-iaas:eu-de-2:a/a1b2c3d4e5f60123456789a1b2c3d4e5:a1b2c3d4-0123-4567-89ab-a1b2c3d4e5f6::"
export IBMCLOUD_CRN_2="crn:v1:bluemix:public:power-iaas:eu-de-1:a/a1b2c3d4e5f60123456789a1b2c3d4e5:e5f6a1b2-cdef-0123-4567-a1b2c3d4e5f6::"
export POWERVSI_1="a1b2c3d4-0123-890a-f012-0123456789ab"
export POWERVSI_2="e5f6a1b2-4567-bcde-3456-cdef01234567"
export APIKEY="@/root/.apikey.json"
export API_TYPE="private"
export JUMBO="true"

# NFS settings
export NFS_SERVER="cl-nfs"                      # Hostname or IP address of the highly available NFS server
export NFS_SHARE="/sapS01"                       # Exported file system directory on the NFS server
export NFS_OPTIONS="rw,sec=sys"                  # Sample NFS client mount options

```

Creating mount points for the instance file systems

On both nodes, run the following command to create the mount points for the instance file systems.

```
$ mkdir -p /usr/sap/${SID}/{ASCS${ASCS_INSTNO},ERS${ERS_INSTNO}} /sapmnt/${SID}
```

Installing and setting up the RHEL HA Add-On cluster

Install and set up the RHEL HA Add-On cluster according to [Implementing a RHEL HA Add-On cluster on IBM Power Virtual Server in a Multizone Region Environment](#).

Configure and test the cluster fencing as described in [Creating the fencing device](#).

Preparing cluster resources before the SAP installation

Make sure that the RHEL HA Add-On cluster is running on both virtual server instances and that node fencing has been tested.

Configuring the cluster resource for sapmnt

On NODE1, run the following command to create a cloned *Filesystem* cluster resource that mounts *SAPMNT* from an NFS server on all cluster nodes.

```
$ pcs resource create fs_sapmnt Filesystem \
  device="${NFS_SERVER}:${NFS_SHARE}/sapmnt" \
  directory="/sapmnt/${SID}" \
  fstype='nfs' \
  options="${NFS_OPTIONS}" \
  clone interleave=true
```

Preparing to install the ASCS instance on NODE1

On NODE1, run the following command to create a *Filesystem* cluster resource that mounts the ASCS instance directory.

```
$ pcs resource create ${sid}_fs_asc${ASCS_INSTNO} Filesystem \
  device="${NFS_SERVER}:${NFS_SHARE}/ASCS" \
  directory=/usr/sap/${SID}/ASCS${ASCS_INSTNO} \
  fstype=nfs \
  options="${NFS_OPTIONS}" \
  force_unmount=safe \
  op start interval=0 timeout=60 \
  op stop interval=0 timeout=120 \
  --group ${sid}_asc${ASCS_INSTNO}_group
```

On NODE1, run the following command to create a `powervs-subnet` cluster resource for the ASCS virtual IP address.

```
$ pcs resource create ${sid}_vip_asc${ASCS_INSTNO} powervs-subnet \
  api_key=${APIKEY} \
  api_type=${API_TYPE} \
  cidr=${ASCS_CIDR} \
  ip=${ASCS_IP} \
  crn_host_map="${NODE1}: ${IBMCLOUD_CRN_1}; ${NODE2}: ${IBMCLOUD_CRN_2}" \
  vsi_host_map="${NODE1}: ${POWERVSI_1}; ${NODE2}: ${POWERVSI_2}" \
  jumbo=${JUMBO} \
  region=${CLOUD_REGION} \
  subnet_name=${ASCS_NET} \
  route_table=5${ASCS_INSTNO} \
  op start timeout=720 \
  op stop timeout=300 \
  op monitor interval=60 timeout=30 \
  --group ${sid}_asc${ASCS_INSTNO}_group
```

Preparing to install the ERS instance on NODE2

On NODE1, run the following command to create a *Filesystem* cluster resource to mount the *ERS* instance directory.

```
$ pcs resource create ${sid}_fs_ers${ERS_INSTNO} Filesystem \
  device="${NFS_SERVER}:${NFS_SHARE}/ERS" \
  directory=/usr/sap/${SID}/ERS${ERS_INSTNO} \
  fstype=nfs \
  options="${NFS_OPTIONS}" \
  force_unmount=safe \
  op start interval=0 timeout=60 \
  op stop interval=0 timeout=120 \
  --group ${sid}_ers${ERS_INSTNO}_group
```

On NODE1, run the following command to create a `powervs-subnet` cluster resource for the ERS virtual IP address.

```
$ pcs resource create ${sid}_vip_ers${ERS_INSTNO} powervs-subnet \
  api_key=${APIKEY} \
  api_type=${API_TYPE} \
  cidr=${ERS_CIDR} \
```

```

ip=${ERS_IP} \
crn_host_map="${NODE1}:${IBMCLOUD_CRN_1};${NODE2}:${IBMCLOUD_CRN_2}" \
vsi_host_map="${NODE1}:${POWERVSI_1};${NODE2}:${POWERVSI_2}" \
jumbo=${JUMBO} \
region=${CLOUD_REGION} \
subnet_name=${ERS_NET} \
route_table=5${ERS_INSTNO} \
op start timeout=720 \
op stop timeout=300 \
op monitor interval=60 timeout=30 \
--group ${sid}_ers${ERS_INSTNO}_group

```

Verifying the cluster configuration

On NODE1, run the following command to verify the cluster configuration at this stage.

```
$ pcs status --full
```

Sample output:

```

# pcs status --full
Cluster name: SAP_S01
Status of pacemakerd: 'Pacemaker is running' (last updated 2024-11-20 14:04:05 +01:00)
Cluster Summary:
  * Stack: corosync
  * Current DC: cl-s01-2 (2) (version 2.1.5-9.el9_2.4-a3f44794f94) - partition with quorum
  * Last updated: Wed Nov 20 14:04:06 2024
  * Last change: Wed Nov 20 13:51:19 2024 by hacluster via crmd on cl-s01-2
  * 2 nodes configured
  * 8 resource instances configured

Node List:
  * Node cl-s01-1 (1): online, feature set 3.16.2
  * Node cl-s01-2 (2): online, feature set 3.16.2

Full List of Resources:
  * fence_node1 (stonith:fence_ibm_powervs): Started cl-s01-2
  * fence_node2 (stonith:fence_ibm_powervs): Started cl-s01-2
  * Clone Set: fs_sapmnt-clone [fs_sapmnt]:
    * fs_sapmnt (ocf:heartbeat:Filesystem): Started cl-s01-1
    * fs_sapmnt (ocf:heartbeat:Filesystem): Started cl-s01-2
  * Resource Group: s01_asc21_group:
    * s01_fs_asc21 (ocf:heartbeat:Filesystem): Started cl-s01-1
    * s01_vip_asc21 (ocf:heartbeat:powervs-subnet): Started cl-s01-1
  * Resource Group: s01_ers22_group:
    * s01_fs_ers22 (ocf:heartbeat:Filesystem): Started cl-s01-1
    * s01_vip_ers22 (ocf:heartbeat:powervs-subnet): Started cl-s01-1

Migration Summary:

Tickets:

PCSD Status:
  cl-s01-1: Online
  cl-s01-2: Online

Daemon Status:
  corosync: active/disabled
  pacemaker: active/disabled
  pcsd: active/enabled

```

Make sure that the `${sid}_asc${ASCS_INSTNO}_group` cluster resource group runs on NODE1 and the `${sid}_ers${ERS_INSTNO}_group` cluster resource group runs on NODE2. If necessary, use the `pcs resource move <resource_group_name>` command to move the resource group to the correct node.

Changing the ownership of the ASCS and ERS mount points

The ASCS and ERS mount points must be owned by the `sidadm` user. You must define the required users and groups and set the mount point ownership before you can start the instance installation.

On both nodes, use the following steps to set the required owner.

1. Start the *SAP Software Provisioning Manager (SWPM)* to create the operating system users and groups.

```
<swpm>/sapinst
```

In the SWPM web interface, use the path *System Rename > Preparations > Operating System Users and Group*. Note the user and group IDs and make sure that they are the same on both nodes.

2. Change the ownership of the mount points.

```
$ chown -R ${sid}adm:sapsys /sapmnt/${SID} /usr/sap/${SID}
```

Installing the ASCS and ERS instances

Use SWPM to install both instances.

- Install ASCS and *E*RS instances on the cluster nodes.

- On NODE1, use the virtual hostname `${ASCS_VH}` that is associated with the ASCS virtual IP address and install an ASCS instance.

```
<swpm>/sapinst SAPINST_USE_HOSTNAME=${ASCS_VH}
```

- On NODE2, use the virtual hostname `${ERS_VH}` that is associated with the *E*RS virtual IP address and install an *E*RS instance.

```
<swpm>/sapinst SAPINST_USE_HOSTNAME=${ERS_VH}
```

- Install all other SAP application instances outside the cluster.

Preparing the ASCS and ERS instances for cluster integration

Use the following steps to prepare the SAP instances for the cluster integration.

Disabling the automatic start of the SAP instance agents for ASCS and ERS

You must disable the automatic start of the `sapstartsrv` instance agents for both ASCS and *E*RS instances after a reboot.

Verifying the SAP instance agent integration type

Recent versions of the SAP instance agent `sapstartsrv` provide native `systemd` support on Linux. For more information, refer to the the SAP notes that are listed at [SAP Notes](#).

On both nodes, check the content of the `/usr/sap/sapservices` file.

```
$ cat /usr/sap/sapservices
```

In the `systemd` format, the lines start with `systemctl` entries.

Example:

```
systemctl --no-ask-password start SAPS01_01 # sapstartsrv pf=/usr/sap/S01/SYS/profile/S01_ASCS01_cl-sap-scs
```

If the entries for ASCS and ERS are in `systemd` format, continue with the steps in [Disabling systemd services of the ASCS and the ERS SAP instance](#).

In the `classic` format, the lines start with `LD_LIBRARY_PATH` entries.

Example:

```
LD_LIBRARY_PATH=/usr/sap/S01/ASC01/exe:$LD_LIBRARY_PATH;export LD_LIBRARY_PATH;/usr/sap/S01/ASC01/exe/sapstartsrv  
pf=/usr/sap/S01/SYS/profile/S01_ASC01_cl-sap-scs -D -u s01adm
```

If the entries for ASCS and ERS are in `classic` format, then modify the `/usr/sap/sapservices` file to prevent the automatic start of the `sapstartsrv` instance agent for both ASCS and *E*RS instances after a reboot.

On both nodes, remove or comment out the `sapstartsrv` entries for both ASCS and ERS in the SAP services file.

```
$ sed -i -e 's/^LD_LIBRARY_PATH=/#LD_LIBRARY_PATH=/' /usr/sap/sapservices
```

Example:

```
#LD_LIBRARY_PATH=/usr/sap/S01/ASCS01/exe:$LD_LIBRARY_PATH;export LD_LIBRARY_PATH;/usr/sap/S01/ASCS01/exe/sapstartsrv  
pf=/usr/sap/S01/SYS/profile/S01_ASCS01_cl-sap-scs -D -u s01adm
```

Proceed to [Installing permanent SAP license keys](#).

Disabling systemd services of the ASCS and the ERS instances

On both nodes, disable the instance agent for the ASCS.

```
$ systemctl disable --now SAP${SID}_${ASC斯_INSTNO}.service
```

On both nodes, disable the instance agent for the ERS.

```
$ systemctl disable --now SAP${SID}_${ERS_INSTNO}.service
```

Disabling systemd restart of a crashed ASCS or ERS instance

`Systemd` has its own mechanisms for restarting a crashed service. In a high availability setup, only the HA cluster is responsible for managing the SAP ASCS and ERS instances. Create `systemd drop-in files` on both cluster nodes to prevent `systemd` from restarting a crashed SAP instance.

On both nodes, create the directories for the drop-in files.

```
$ mkdir /etc/systemd/system/SAP${SID}_${ASC斯_INSTNO}.service.d
```

```
$ mkdir /etc/systemd/system/SAP${SID}_${ERS_INSTNO}.service.d
```

On both nodes, create the drop-in files for ASCS and ERS.

```
$ cat >> /etc/systemd/system/SAP${SID}_${ASC斯_INSTNO}.service.d/HA.conf << EOT  
[Service]  
Restart=no  
EOT
```

```
$ cat >> /etc/systemd/system/SAP${SID}_${ERS_INSTNO}.service.d/HA.conf << EOT  
[Service]  
Restart=no  
EOT
```



Note: `Restart=no` must be in the `[Service]` section, and the drop-in files must be available on all cluster nodes.

On both nodes, reload the `systemd` unit files.

```
$ systemctl daemon-reload
```

Installing permanent SAP license keys

When the SAP ASCS instance is installed on a Power Virtual Server instance, the SAP license mechanism relies on the partition UUID. For more information, see [SAP note 2879336 - Hardware key based on unique ID](#).

On both nodes, run the following command as user `<sid>adm` to identify the `HARDWARE KEY` of the node.

```
$ sudo -i -u ${sid}adm -- sh -c 'saplikey -get'
```

Sample output:

```
$ sudo -i -u ${sid}adm -- sh -c 'saplikey -get'  
saplikey: HARDWARE KEY = H1428224519
```

Note the **HARDWARE KEY** of each node.

You need both hardware keys to request two different SAP license keys. Check the following SAP notes for more information about requesting SAP license keys:

- [2879336 - Hardware key based on unique ID](#)
- [2662880 - How to request SAP license keys for failover systems](#)

Installing SAP resource agents

Install the required software packages. The **resource-agents-sap** includes the *SAPInstance cluster resource agent* for managing the SAP instances.

Unless **sap_cluster_connector** is configured for the SAP instance, the RHEL HA Add-On cluster considers any state change of the instance as an issue. If other SAP tools such as **sapcontrol** are used to manage the instance, then **sap_cluster_connector** grants permission to control SAP instances that are running inside the cluster. If the SAP instances are managed by only cluster tools, the implementation of **sap_cluster_connector** is not necessary.

Install the packages for the resource agent and the *SAP Cluster Connector* library. For more information, see [How to enable the SAP HA Interface for SAP ABAP application server instances managed by the RHEL HA Add-On](#)

On both nodes, run the following commands.

If needed, use **subscription-manager** to enable the SAP NetWeaver repository. The [RHEL for SAP Subscriptions and Repositories](#) documentation describes how to enable the required repositories.

```
$ subscription-manager repos --enable="rhel-8-for-ppc64le-sap-netweaver-e4s-rpms"
```

Install the required packages.

```
$ dnf install -y resource-agents-sap sap-cluster-connector
```

Configuring SAP Cluster Connector

Add user **\${sid}adm** to the **haclient** group.

On both nodes, run the following command.

```
$ usermod -a -G haclient ${sid}adm
```

Adapting the SAP instance profiles

Modify the start profiles of all SAP instances that are managed by *SAP tools* outside the cluster. Both *ASCS* and *ERS* instances can be controlled by the RHEL HA Add-On cluster and its resource agents. Adjust the SAP instance profiles to prevent an automatic restart of instance processes.

On NODE1, navigate to the SAP profile directory.

```
$ cd /sapmnt/${SID}/profile
```

Change all occurrences of **Restart_Program** to **Start_Program** in the instance profile of both *ASCS* and *ERS*.

```
$ sed -i -e 's/Restart_Program_\([0-9][0-9]\)/Start_Program_\1/' ${SID}_ASCS${ASCS_INSTNO}_${ASCS_VH}
```

```
$ sed -i -e 's/Restart_Program_\([0-9][0-9]\)/Start_Program_\1/' ${SID}_ERS${ERS_INSTNO}_${ERS_VH}
```

Add the following two lines at the end of the SAP instance profile to configure **sap_cluster_connector** for the *ASCS* and *ERS* instances.

```
service/halib = $(DIR_EXECUTABLE)/saphascriptco.so  
service/halib_cluster_connector = /usr/bin/sap_cluster_connector
```

Configuring the ASCS and ERS cluster resources

Up to this point, the following are assumed:

- A RHEL HA Add-On cluster is running on both virtual server instances and node fencing has been tested.
- A cloned *Filesystem* cluster resource is configured to mount the *sapmnt* share.
- Two *Filesystem* cluster resources are configured to mount the *ASCS* and *ERS* instance file systems.
- Two *powervs-subnet* cluster resources are configured for the virtual IP addresses of the *ASCS* and *ERS* instances.
- The *ASCS* instance is installed and active on NODE1.
- THE *ERS* instance is installed and active on NODE2.
- All steps according to [Prepare ASCS and ERS instances for the cluster integration](#) are complete.

Configuring the ASCS cluster resource group

On NODE1, run the following commands to create a cluster resource for managing the *ASCS* instance.

```
$ pcs resource create ${sid}_ascss${ASCS_INSTNO} SAPInstance \
  InstanceName="${SID}_ASCS${ASCS_INSTNO}_${ASCS_VH}" \
  START_PROFILE=/sapmnt/${SID}/profile/${SID}_ASCS${ASCS_INSTNO}_${ASCS_VH} \
  AUTOMATIC_RECOVER=false \
  meta resource-stickiness=5000 \
  migration-threshold=1 failure-timeout=60 \
  op monitor interval=20 on-fail=restart timeout=60 \
  op start interval=0 timeout=600 \
  op stop interval=0 timeout=600 \
  --group ${sid}_ascss${ASCS_INSTNO}_group
```

 **Note:** The `meta resource-stickiness=5000` option is used to balance the failover constraint with ERS so that the resource stays on the node where it started and doesn't migrate uncontrollably in the cluster.

Add a resource stickiness to the group to ensure that the *ASCS* instance stays on the node.

```
$ pcs resource meta ${sid}_ascss${ASCS_INSTNO}_group \
  resource-stickiness=3000
```

Configuring the ERS cluster resource group

On NODE2, run the following command to create a resource for managing the *ERS* instance.

```
$ pcs resource create ${sid}_ers${ERS_INSTNO} SAPInstance \
  InstanceName="${SID}_ERS${ERS_INSTNO}_${ERS_VH}" \
  START_PROFILE=/sapmnt/${SID}/profile/${SID}_ERS${ERS_INSTNO}_${ERS_VH} \
  AUTOMATIC_RECOVER=false \
  IS_ERS=true \
  op monitor interval=20 on-fail=restart timeout=60 \
  op start interval=0 timeout=600 \
  op stop interval=0 timeout=600 \
  --group ${sid}_ers${ERS_INSTNO}_group
```

Configuring the cluster constraints

On NODE1, run the following command to create the cluster constraints.

A colocation constraint prevents resource groups `${sid}_ascss${ASCS_INSTNO}_group` and `${sid}_ers${ERS_INSTNO}_group` from being active on the same node whenever possible. If only a single node is available, the stickiness value of `-5000` ensures that they run on the same node.

```
$ pcs constraint colocation add \
  ${sid}_ers${ERS_INSTNO}_group with ${sid}_ascss${ASCS_INSTNO}_group -- -5000
```

An order constraint controls that `${sid}_ascss${ASCS_INSTNO}_group` starts before `${sid}_ers${ERS_INSTNO}_group`.

```
$ pcs constraint order start \
  ${sid}_ascss${ASCS_INSTNO}_group then stop ${sid}_ers${ERS_INSTNO}_group \
  symmetrical=false \
  kind=Optional
```

The following two order constraints ensure that the `SAPMNT` file system mounts before `${sid}_ascs${ASCS_INSTNO}_group` and `${sid}_ers${ERS_INSTNO}_group` start.

```
$ pcs constraint order fs_sapmnt-clone then ${sid}_ascs${ASCS_INSTNO}_group
```

```
$ pcs constraint order fs_sapmnt-clone then ${sid}_ers${ERS_INSTNO}_group
```

Conclusion

This completes the *ENSA2* cluster implementation in a multizone region environment.

You should now proceed with testing the cluster, similar to the tests described in [Testing an SAP ENSA2 cluster](#).

The following is a sample output of the `pcs status` command for a completed *ENSA2* cluster in a multi-zone region implementation.

```
Cluster name: SAP_S01
Status of pacemakerd: 'Pacemaker is running' (last updated 2024-11-22 09:42:15 +01:00)
Cluster Summary:
  * Stack: corosync
  * Current DC: cl-s01-1 (version 2.1.5-9.el9_2.4-a3f44794f94) - partition with quorum
  * Last updated: Fri Nov 22 09:42:15 2024
  * Last change: Fri Nov 22 09:06:18 2024 by root via cibadmin on cl-s01-1
  * 2 nodes configured
  * 10 resource instances configured

Node List:
  * Online: [ cl-s01-1 cl-s01-2 ]

Full List of Resources:
  * fence_node1 (stonith:fence_ibm_powervs): Started cl-s01-1
  * fence_node2 (stonith:fence_ibm_powervs): Started cl-s01-2
  * Clone Set: fs_sapmnt-clone [fs_sapmnt]:
    * Started: [ cl-s01-1 cl-s01-2 ]
  * Resource Group: s01_ascs21_group:
    * s01_fs_ascs21 (ocf:heartbeat:Filesystem): Started cl-s01-1
    * s01_vip_ascs21 (ocf:heartbeat:powervs-subnet): Started cl-s01-1
    * s01_ascs21 (ocf:heartbeat:SAPIstance): Started cl-s01-1
  * Resource Group: s01_ers22_group:
    * s01_fs_ers22 (ocf:heartbeat:Filesystem): Started cl-s01-2
    * s01_vip_ers22 (ocf:heartbeat:powervs-subnet): Started cl-s01-2
    * s01_ers22 (ocf:heartbeat:SAPIstance): Started cl-s01-2

Daemon Status:
  corosync: active/disabled
  pacemaker: active/disabled
  pcsd: active/enabled
```

Configuring an active-passive NFS Server in a Red Hat Enterprise Linux High Availability Add-On cluster

The following information describes the configuration of an active-passive NFS server in a Red Hat Enterprise Linux (RHEL) High Availability Add-On cluster. The cluster uses virtual server instances in [IBM® Power® Virtual Server](#) as cluster nodes.

The described setup uses shareable storage volumes that are accessible on both cluster nodes. The file systems for the NFS exports are created on those shareable storage volumes. HA-LVM makes sure that the volume group is active on one node at a time.

In the example setup, one shared volume group `nfssharevg` contains three logical volumes `nfssharelv`, `sap${SID}lv`, and `saptranslv`. XFS file systems are created on those logical volumes and are mounted on `/nfsshare`, `/nfshare/export/sap${SID}`, `/nfsshare/export/saptrans`.

The instructions are based on the Red Hat product documentation and articles that are listed in [Implementing high availability for SAP applications on IBM Power Virtual Server References](#).

Before you begin

Review the general requirements, product documentation, support articles, and SAP notes listed in [Implementing high availability for SAP applications on IBM Power Virtual Server References](#).

Prerequisites

A virtual hostname and IP address is required for the NFS server. Make sure that the virtual IP address is defined on the network interface, and reachable in the network.

Name resolution and reverse lookup for physical and virtual IP names and addresses must be unique and consistent on all NFS server and client nodes. Details of the NFS clients (subnet, required NFS export options) must be available. You need to enter them during the cluster setup.

Preparing for a highly available NFS server

Use the following information to prepare the environment for a highly available NFS server.

Installing NFS software packages

On both nodes, run the following commands.

```
$ dnf install -y nfs-utils
```

Preparing LVM objects

All cluster nodes need access to the shared storage volumes, but only one node has exclusive read and write access to a volume.

Preparing active-passive HA LVM

On both nodes, edit file `/etc/lvm/lvm.conf` to include the system ID in the volume group. Search for the configuration setting `system_id_source` and change its value to "uname".

Sample setting of `system_id_source` in `/etc/lvm/lvm.conf`:

```
# grep "system_id_source =" /etc/lvm/lvm.conf
system_id_source = "uname"
```

Verify that the `LVM system ID` for the node matches the `uname -n` output.

```
$ lvm systemid
```

```
$ uname -n
```

Sample output:

```
# lvm systemid
  system ID: cl-nfs-1
# uname -n
  cl-nfs-1
```

Identifying the World Wide Names of shared storage volumes

Identify the World Wide Names (WWN) for all volumes that are used in the shared volume group.

1. Log in to IBM Cloud® and go to the [Storage volumes](#) view of Power Virtual Server.
2. Select your **workspace**.
3. Filter for the *volume prefix* in the *Storage volumes* list, and identify all the **World Wide Names** of the volumes in scope (the *World Wide Name* is a 32-digit hexadecimal number).



Note: Make sure that the attribute **Shareable** is *On* for those volumes.

4. In the [Virtual server instances](#) view, go to both virtual server instances of the cluster and verify that in scope volumes are attached to both virtual server instances.

Discovering new SAN volumes on cluster nodes

When you attach a new storage volume to a virtual server instance, you need to rescan the SCSI bus to detect the new volume. Then, update the *multipath configuration* of the virtual server instance.

On the nodes with new storage volume attachments, run the following command.

```
$ rescan-scsi-bus.sh && sleep 10 && multipathd reconfigure
```

 **Tip:** The WWN value of a volume can also be found with the `pvs --all` command.

Preparing environment variables

To simplify the setup, prepare the following environment variables for user ID `root` on both nodes. These environment variables are used in subsequent commands in the remainder of this document.

On both nodes, create a file with the environment variables. Then, adapt them to your configuration.

Adapt `NFS_VH`, `NFS_IP`, `NFS_CLIENTSPEC`, and `NFS_OPTIONS` to your environment. For `NFS_PVID`, use the *WWN* that you identified previously. In addition to the file system that is used for the NFS share, the example shows two more file systems that are used for an SAP system landscape with system ID `${SID}` and the SAP transport directory. The sample sizes `${NFS_SZ1}`, `${NFS_SZ2}`, and `${NFS_SZ3}` are percentages of the `${NFS_VG}` volume group size and need to be modified according to your requirements. The volume group names and mount point names are suggestions and need to be changed to match your own naming conventions.

 **Tip:** Make sure that you set the `NFS_PVID` environment variable by using lowercase letters in the hexadecimal number.

```
# virtual hostnames
export NFS_VH=<virtual hostname>          # virtual hostname for NFS server
export NFS_IP=<IP address>                  # virtual IP address for NFS server

# LVM storage for NFS file systems
export NFS_PVID=3<WWN>                      # WWN of shareable storage volume used for NFS
export NFS_VG="nfssharevg"                     # volume group name for NFS exported file systems

# NFS share file system
export NFS_LV1="nfssharelv"                    # logical volume name export #1
export NFS_SZ1="5%VG"                          # logical volume size
export NFS_FS1="/nfsshare"                     # file system mount point
export NFS_ROOT="${NFS_FS1}/export"            # base export directory

# NFS share file system for SAP system ID <SID>
export SID=<SID>                            # SAP system ID
export NFS_LV2="sap${SID}lv"                   # logical volume name export #2
export NFS_SZ2="40%VG"                         # logical volume size
export NFS_FS2="${NFS_ROOT}/sap${SID}"         # file system mount point

# NFS share file system for SAP transport directory
export NFS_LV3="saptranslv"                   # logical volume name export #3
export NFS_SZ3="40%VG"                         # logical volume size
export NFS_FS3="${NFS_ROOT}/saptrans"          # file system mount point

# NFS client options
export NFS_CLIENTSPEC="10.111.1.0/24"        # client specs (subnet and netmask) for allowed NFS clients
export NFS_OPTIONS="rw,sync,no_root_squash,no_subtree_check,crossmnt" # options for NFS export
```

You must source this file before you use the sample commands in the remainder of this document.

For example, if you created a file that is named `nfs_envs.sh`, run the following command on both nodes to set the environment variables.

```
$ source nfs_envs.sh
```

 **Note:** Every time that you start a new terminal session, you must run the `source` command. Alternatively, you can add the environment variables file to the `/etc/profile.d` directory during the cluster configuration. In this example, the file is sourced automatically each time you log in to the server.

Creating LVM objects

Use the following information to create LVM objects.

Creating physical volumes

On NODE1, run the following command.

```
$ pvcreate /dev/mapper/${NFS_PVID}
```

Sample output:

```
pvcreate /dev/mapper/${NFS_PVID}
Physical volume "/dev/mapper/36005076810810335700000000002ddc" successfully created.
```

Creating a volume group

On NODE1, create the volume group for the NFS export.

```
$ vgcreate ${NFS_VG} /dev/mapper/${NFS_PVID}
```

Verify that the *System ID* is set.

```
$ vgs -o+systemid
```

Sample output:

```
# vgs -o+systemid
VG          #PV #LV #SN Attr   VSize   VFree   System ID
nfssharevg    1   0   0 wz--n- <50.00g <50.00g cl-sap-1
```

Creating logical volumes

On NODE1, create three logical volumes for the NFS export.

```
$ lvcreate -l ${NFS_SZ1} -n ${NFS_LV1} ${NFS_VG}
```

```
$ lvcreate -l ${NFS_SZ2} -n ${NFS_LV2} ${NFS_VG}
```

```
$ lvcreate -l ${NFS_SZ3} -n ${NFS_LV3} ${NFS_VG}
```

Creating the file systems

On NODE1, create the file systems for NFS exports.

The example uses file system type `xfs`. Other file system types are possible. Then, the resource definitions need to be changed.

```
$ mkfs.xfs /dev/${NFS_VG}/${NFS_LV1}
```

```
$ mkfs.xfs /dev/${NFS_VG}/${NFS_LV2}
```

```
$ mkfs.xfs /dev/${NFS_VG}/${NFS_LV3}
```

Creating the mount point for the NFS export

On both nodes, run the following command.

```
$ mkdir -p ${NFS_FS1}
```

Making sure that a volume group is not activated on multiple cluster nodes

Volume groups that are managed by Pacemaker must not activate automatically on startup.

Tip: For RHEL 8.5 and later, you can disable autoactivation for a volume group when you create the volume group by specifying the `--setautoactivation n` flag for the `vgcreate` command.

On both nodes, edit file `/etc/lvm/lvm.conf` and modify the `auto_activation_volume_list` entry to limit autoactivation to specific volume groups. Search for parameter `auto_activation_volume_list` and add the volume groups, other than the volume group that you defined for the NFS cluster, as entries in that list.

Sample setting of the `auto_activation_volume_list` entry in `/etc/lvm/lvm.conf`:

```
auto_activation_volume_list = [ "rhel_root" ]
```

Rebuild the `initramfs` boot image to make sure that the boot image does not activate a volume group that is controlled by the cluster.

On both nodes, run the following command.

```
$ dracut -H -f /boot/initramfs-$(uname -r).img $(uname -r)
```

Reboot both nodes.

Installing and setting up the RHEL HA Add-On cluster

Use the following instructions to perform the initial cluster configuration.

- Install and set up the RHEL HA Add-On cluster according to [Implementing a Red Hat Enterprise Linux High Availability Add-On cluster](#).
- Configure and test fencing as described in [Creating the fencing device](#).

Sample output of the cluster status at this stage.

```
# pcs status
Cluster name: SAP_NFS
Cluster Summary:
  * Stack: corosync
  * Current DC: cl-nfs-1 (version 2.0.5-9.el8_4.5-ba59be7122) - partition with quorum
  * Last updated: Fri Mar 10 10:35:42 2023
  * Last change: Fri Mar 10 09:52:08 2023 by root via cibadmin on cl-nfs-1
  * 2 nodes configured
  * 1 resource instance configured

Node List:
  * Online: [ cl-nfs-1 cl-nfs-2 ]

Full List of Resources:
  * res_fence_ibm_powervs (stonith:fence_ibm_powervs): Started cl-nfs-1

Daemon Status:
  corosync: active/disabled
  pacemaker: active/disabled
  pcsd: active/enabled
```

Configuring general cluster properties

To prevent the cluster from moving healthy resources to another node (for example when you restart the cluster on a previously failed node), you can set the default value for the `resource-stickiness` meta attribute to 1.

On NODE1, run the following command.

```
$ pcs resource defaults update resource-stickiness=1
```

Configuring NFS resource group and resources

Use the following steps to configure the NFS resources in the cluster.

Creating the LVM-activate resource

To make sure that all NFS resources run on the same node, configure them as part of the resource group `nfsgroup`.

This resource group is created with the first resource. Resources start in the order in which they are added to the group. The resources stop in reverse order.

On NODE1, run the following command.

```
$ pcs resource create nfs_vg ocf:heartbeat:LVM-activate \
    vgname=${NFS_VG} \
    vg_access_mode=system_id \
    --group nfsgroup
```

To avoid data corruption, don't configure more than one *LVM-activate* resource that uses the same LVM volume group in an active-passive HA configuration. Don't configure an LVM-activate resource as a clone resource in an active-passive HA configuration.

Check the status of the cluster and verify that resource `nfs_vg` is active.

On NODE1, run the following command.

```
$ pcs resource status
```

Sample output:

```
# pcs resource status
* Resource Group: nfsgroup:
  * nfs_vg      (ocf::heartbeat:LVM-activate):   Started cl-nfs-1
```

The following command configures the `xfs` file system resources for the `nfsgroup` resource group. The file systems use LVM volume group `${NFS_VG}` and the logical volumes (`${NFS_LV1}`, `${NFS_LV2}`, `${NFS_LV3}`) that were created before.

On NODE1, run the following command.

```
$ pcs resource create nfs_fs1 Filesystem \
    device=/dev/${NFS_VG}/${NFS_LV1} \
    directory=${NFS_FS1} \
    fstype=xfs \
    --group nfsgroup
```

You can specify mount options as part of the resource configuration for a file system resource by using the `options=<options>` parameter. Run `pcs resource describe filesystem` for a complete list of configuration options.

Check the status of the cluster and verify that the resource `nfs_fs1` is active.

```
$ pcs resource status
```

Sample output:

```
# pcs resource status
* Resource Group: nfsgroup:
  * nfs_vg      (ocf::heartbeat:LVM-activate):   Started cl-nfs-1
  * nfs_fs1     (ocf::heartbeat:Filesystem):       Started cl-nfs-1
```

On the node with the active resource group `nfsgroup`, create two subdirectories in `${NFS_FS1}`. `${NFS_FS1}/stat` is used as `nfs_shared_infodir` for NFS lock information and `${NFS_FS1}/export` is used as NFS root.

```
$ mkdir ${NFS_FS1}/stat ${NFS_FS1}/export
```

Create the mount points for the other exported file systems.

On both nodes, run the following command.

```
$ mkdir ${NFS_FS2} ${NFS_FS3}
```

Create the resources for the other two NFS file systems.

On NODE1, run the following commands.

```
$ pcs resource create nfs_fs2 Filesystem \
```

```
device=/dev/${NFS_VG}/${NFS_LV2} \
directory=${NFS_FS2} \
fstype=xfs \
--group nfsgroup
```

```
$ pcs resource create nfs_fs3 Filesystem \
device=/dev/${NFS_VG}/${NFS_LV3} \
directory=${NFS_FS3} \
fstype=xfs \
--group nfsgroup
```

Check the status of the cluster and verify that all three file system resources (`nfs_fs1`, `nfs_fs2`, `nfs_fs3`) are active.

```
$ pcs resource status
```

Sample output:

```
# pcs resource status
* Resource Group: nfsgroup:
  * nfs_vg    (ocf::heartbeat:LVM-activate): Started cl-nfs-1
  * nfs_fs1   (ocf::heartbeat:Filesystem):   Started cl-nfs-1
  * nfs_fs2   (ocf::heartbeat:Filesystem):   Started cl-nfs-1
  * nfs_fs3   (ocf::heartbeat:Filesystem):   Started cl-nfs-1
```

Creating the nfsserver resource

On NODE1, create a resource for managing the NFS server.

```
$ pcs resource create nfs_daemon nfsserver \
nfs_shared_infodir=${NFS_FS1}/stat \
nfs_no_notify=true \
--group nfsgroup
```

The `nfs_shared_infodir` parameter of the `nfsserver` resource specifies a directory where the NFS server stores stateful information.

Check the status of the cluster and verify that the NFS server is started.

```
$ pcs resource status
```

Sample output:

```
# pcs resource status
* Resource Group: nfsgroup:
  * nfs_vg    (ocf::heartbeat:LVM-activate): Started cl-nfs-1
  * nfs_fs1   (ocf::heartbeat:Filesystem):   Started cl-nfs-1
  * nfs_fs2   (ocf::heartbeat:Filesystem):   Started cl-nfs-1
  * nfs_fs3   (ocf::heartbeat:Filesystem):   Started cl-nfs-1
  * nfs_daemon    (ocf::heartbeat:nfsserver): Started cl-nfs-1
```

Creating the exportfs resource

To export the `${NFS_ROOT}` directory, add the `exportfs` resources to the `nfsgroup` group, which builds a virtual directory for NFSv4 clients. NFSv3 clients can access these exports too.

On NODE1, run the following command.

```
$ pcs resource create nfs_export exportfs \
clientspec=${NFS_CLIENTSPEC} \
options=${NFS_OPTIONS} \
directory=${NFS_ROOT} \
fsid=0 \
--group nfsgroup
```

Configuring a floating IP address resource

Review the information in [Reserving virtual IP addresses](#) and reserve a virtual IP address for the NFS cluster.

Create a resource for the virtual IP address of the NFS Server. NFS clients access the NFS share by using the floating IP address.

On NODE1, run the following command.

```
$ pcs resource create nfs_ip IPAddr2 \
    ip=${NFS_IP} \
    --group nfsgroup
```

Configuring a notify resource

The *nfsnotify* resource sends FSv3 reboot notifications after the entire NFS deployment initializes.

On NODE1, run the following command.

```
$ pcs resource create nfs_notify nfsnotify \
    source_host=${NFS_IP} \
    --group nfsgroup
```

The NFS cluster setup is now complete.

On NODE1, run the following command to check the status.

```
$ pcs resource status
```

Sample output:

```
# pcs resource status
* Resource Group: nfsgroup:
  * nfs_vg    (ocf::heartbeat:LVM-activate):    Started cl-nfs-1
  * nfs_fs1   (ocf::heartbeat:Filesystem):        Started cl-nfs-1
  * nfs_fs2   (ocf::heartbeat:Filesystem):        Started cl-nfs-1
  * nfs_fs3   (ocf::heartbeat:Filesystem):        Started cl-nfs-1
  * nfs_daemon      (ocf::heartbeat:nfsserver):    Started cl-nfs-1
  * nfs_export     (ocf::heartbeat:exportfs):       Started cl-nfs-1
  * nfs_ip       (ocf::heartbeat:IPAddr2):        Started cl-nfs-1
  * nfs_notify     (ocf::heartbeat:nfsnotify):      Started cl-nfs-1
```

Testing the NFS server cluster

You can validate the NFS resource configuration in a high availability cluster by using the following procedures. You can mount the exported file system with either NFSv3 or NFSv4. Run the following tests to verify that the NFS cluster functions.

Test1 - Testing the NFS export

Use the following information to test the NFS export.

Run all the commands on an *NFS client node* outside the HA NFS cluster.

Verify the NFS exports.

```
$ showmount -e ${NFS_IP}
```

The `showmount` command displays information about file systems that are exported by an NFS Server (NFS v3). Verify that the output lists all the exported directories.

Create a temporary directory on the *NFS client node*. Then, mount the NFS file system and create the directory structure that is required for the SAP installation.

In the first example, only `/usr/sap/trans` and `/sapmnt/${SID}` are NFS mounted on the SAP application server instance.

Prepare the mount points that are used for the SAP installation.

```
$ mkdir -p /sapmnt/${SID} \
    /usr/sap/trans
```

Change the attributes of the mount points.

```
$ chattr +i /sapmnt/${SID} \
    /usr/sap/trans
```

Mount the NFS shares.

```
$ mount -t nfs4 -o sec=sys ${NFS_VH}:/saptrans /usr/sap/trans
```

```
$ mount -t nfs4 -o sec=sys ${NFS_VH}:/sap${SID}/sapmnt /sapmnt/${SID}
```

Change the ownership and the permissions.

```
$ chown ${sid}adm:sapsys /usr/sap/trans
```

```
$ chmod g+w /usr/sap/trans
```

```
$ chown -R ${sid}adm:sapsys /sapmnt/${SID}
```

Unmount the file systems.

```
$ umount /usr/sap/trans
```

```
$ umount /sapmnt/${SID}
```

Add the new file systems to `/etc/fstab`.

```
$ cat >> /etc/fstab << EOT
${NFS_VH}:/saptrans /usr/sap/trans nfs4 sec=sys 0 0
${NFS_VH}:/sap${SID}/sapmnt /sapmnt/${SID} nfs4 sec=sys 0 0
EOT
```

Check the updated file.

```
$ cat /etc/fstab
```

In the second example, `/usr/sap/trans`, `/sapmnt/${SID}`, and all instance directories are NFS mounted on the SAP application server instances.

Export environment variables for the ASCS and ERS system numbers. Change the following numbers to the system numbers that you used during ASCS and ERS installation.

```
$ export ASCS_NR=01
```

```
$ export ERS_NR=02
```

Prepare the final mount points that are used for the SAP installation.

```
$ mkdir -p /sapmnt/${SID} \
    /usr/sap/trans \
    /usr/sap/${SID}/SYS \
    /usr/sap/${SID}/ASCS${ASCS_INSTNO} \
    /usr/sap/${SID}/ERS${ERS_INSTNO}
```

Change the attributes of the mount points.

```
$ chattr +i /sapmnt/${SID} \
    /usr/sap/trans \
    /usr/sap/${SID}/SYS \
    /usr/sap/${SID}/ASCS${ASCS_INSTNO} \
    /usr/sap/${SID}/ERS${ERS_INSTNO}
```

Mount the NFS shares to create the required subdirectories, change the ownership, and change the permissions.

```
$ mount -t nfs4 -o sec=sys ${NFS_VH}:/saptrans /mnt
```

```
$ chown ${sid}adm:sapsys /mnt
```

```
$ chmod g+w /mnt
```

```
$ umount /mnt
```

```
$ mount -t nfs4 -o sec=sys ${NFS_VH}:/sap${SID} /mnt
```

```
$ mkdir -p /mnt/sapmnt \
    /mnt/ASCS \
    /mnt/ERS \
    /mnt/SYS \
    /mnt/PAS \
    /mnt/AS1
```

```
$ chown -R ${sid}adm:sapsys /mnt
```

```
$ umount /mnt
```

Add the new file systems to `/etc/fstab`.

```
$ cat >> /etc/fstab < EOT
${NFS_VH}:/saptrans /usr/sap/trans nfs4 sec=sys 0 0
${NFS_VH}:/sap${SID}/sapmnt /sapmnt/${SID} nfs4 sec=sys 0 0
${NFS_VH}:/sap${SID}/ASCS /usr/sap/${SID}/ASCS${ASCS_INSTNO} nfs4 sec=sys 0 0
${NFS_VH}:/sap${SID}/ERS /usr/sap/${SID}/ERS${ERS_INSTNO} nfs4 sec=sys 0 0
${NFS_VH}:/sap${SID}/SYS /usr/sap/${SID}/SYS nfs4 sec=sys 0 0
EOT
```

Check the updated file.

```
$ cat /etc/fstab
```

Test2 - Testing the failover of the NFS server

Use the following information to test the failover of the NFS server.

Test2 - Description

Simulate a crash of the cluster node that has the NFS resources.

Test2 - Prerequisites

- A functional two-node RHEL HA Add-On cluster for an NFS HA server.
- Cluster is started on both nodes.
- The file systems are mounted on an *NFS client node* outside the cluster and the applications can access the content.

Test2 - Test procedure

Crash the cluster node by sending a `shutoff` system request.

First, check the cluster status and identify the node where the `nfsgroup` resource group is running.

On NODE1, run the following command.

```
$ pcs status
```

Then, log in to the identified cluster node and send a `crash` system request.

```
$ sync; echo c > /proc/sysrq-trigger
```

Test2 - Expected behavior

- The node with the active *nfsgroup* resource group shuts down.
- The cluster detects the failed node and starts a fencing action.
- The fencing operation sets the state of the fenced node to offline.
- The cluster acquires the *NFS Server* resources on the failover node.

Check that all the resources started on the failover node.

```
$ pcs resource status
```

Sample output:

```
# pcs resource status
* Resource Group: nfsgroup:
  * nfs_vg    (ocf::heartbeat:LVM-activate): Started cl-nfs-2
  * nfs_fs1   (ocf::heartbeat:Filesystem):    Started cl-nfs-2
  * nfs_fs2   (ocf::heartbeat:Filesystem):    Started cl-nfs-2
  * nfs_fs3   (ocf::heartbeat:Filesystem):    Started cl-nfs-2
  * nfs_daemon      (ocf::heartbeat:nfsserver):     Started cl-nfs-2
  * nfs_export      (ocf::heartbeat:exportfs):      Started cl-nfs-2
  * nfs_ip       (ocf::heartbeat:IPAddr2):        Started cl-nfs-2
  * nfs_notify      (ocf::heartbeat:nfsnotify):     Started cl-nfs-2
```

Verify that the file system is still mounted on the *NFS client node*, and that the applications can still access the content.

Test2 - Recovery procedure

Log in to the IBM Cloud Console and start the stopped instance. Wait until the cluster node is available again, then restart the cluster framework.

On the cluster node, run the following command.

```
$ pcs cluster start
```

Check the cluster status.

```
$ pcs status
```

Sample output:

```
# pcs status
Cluster name: SAP_NFS
Cluster Summary:
  * Stack: corosync
  * Current DC: cl-nfs-1 (version 2.0.5-9.el8_4.5-ba59be7122) - partition with quorum
  * Last updated: Mon Mar 20 08:11:28 2023
  * Last change: Mon Mar 20 07:56:25 2023 by hacluster via crmd on cl-nfs-1
  * 2 nodes configured
  * 9 resource instances configured

Node List:
  * Online: [ cl-nfs-1 cl-nfs-2 ]

Full List of Resources:
  * res_fence_ibm_powervs (stonith:fence_ibm_powervs): Started cl-nfs-1
  * Resource Group: nfsgroup:
    * nfs_vg (ocf::heartbeat:LVM-activate): Started cl-nfs-2
    * nfs_fs1 (ocf::heartbeat:Filesystem):    Started cl-nfs-2
    * nfs_fs2 (ocf::heartbeat:Filesystem):    Started cl-nfs-2
    * nfs_fs3 (ocf::heartbeat:Filesystem):    Started cl-nfs-2
    * nfs_daemon (ocf::heartbeat:nfsserver):     Started cl-nfs-2
    * nfs_export (ocf::heartbeat:exportfs):      Started cl-nfs-2
```

```
* nfs_ip (ocf::heartbeat:IPaddr2): Started cl-nfs-2
* nfs_notify (ocf::heartbeat:nfsnotify): Started cl-nfs-2
```

Daemon Status:

```
corosync: active/disabled
pacemaker: active/disabled
pcsd: active/enabled
```

Migration

From on-premises to Power Virtual server

Automating SAP workload HA deployment on IBM Cloud VPC with Terraform and Ansible

You can use Terraform to automate IBM Cloud® VPC provisioning. The VPC provisioned includes virtual server instances with high network performance. The VPC infrastructure contains various Infrastructure-as-a-Service (IaaS) offerings, including virtual servers. After the VPC is provisioned, the scripts use the Ansible Playbooks to install the SAP system.

IBM Cloud VPC introduction

VPC is a public cloud offering that an enterprise uses to establish its own private cloud-like computing environment on shared [public cloud](#) infrastructure. VPC gives an enterprise the ability to define and control a virtual network that is logically isolated from all other public cloud tenants, creating a private and secure place on the public cloud.

Imagine that a cloud provider's infrastructure is a residential apartment building and multiple families live inside. A public cloud tenant is a kind of sharing an apartment with a few roommates. In contrast, having a VPC is like having your own private condominium; no one else has the key, and no one can enter the space without your permission.

VPC's logical isolation is implemented by using virtual network functions and security features that give the enterprise customer granular control over which IP addresses or applications can access particular resources. It is analogous to the "friends-only" or "public/private" controls on social media accounts used to restrict who can or can't see your otherwise public posts.

With IBM Cloud VPC, you can use the UI, CLI, and API to manually provision virtual server instances for VPC with high network performance. VPC infrastructure contains various Infrastructure-as-a-Service (IaaS) offerings including virtual servers for VPC.

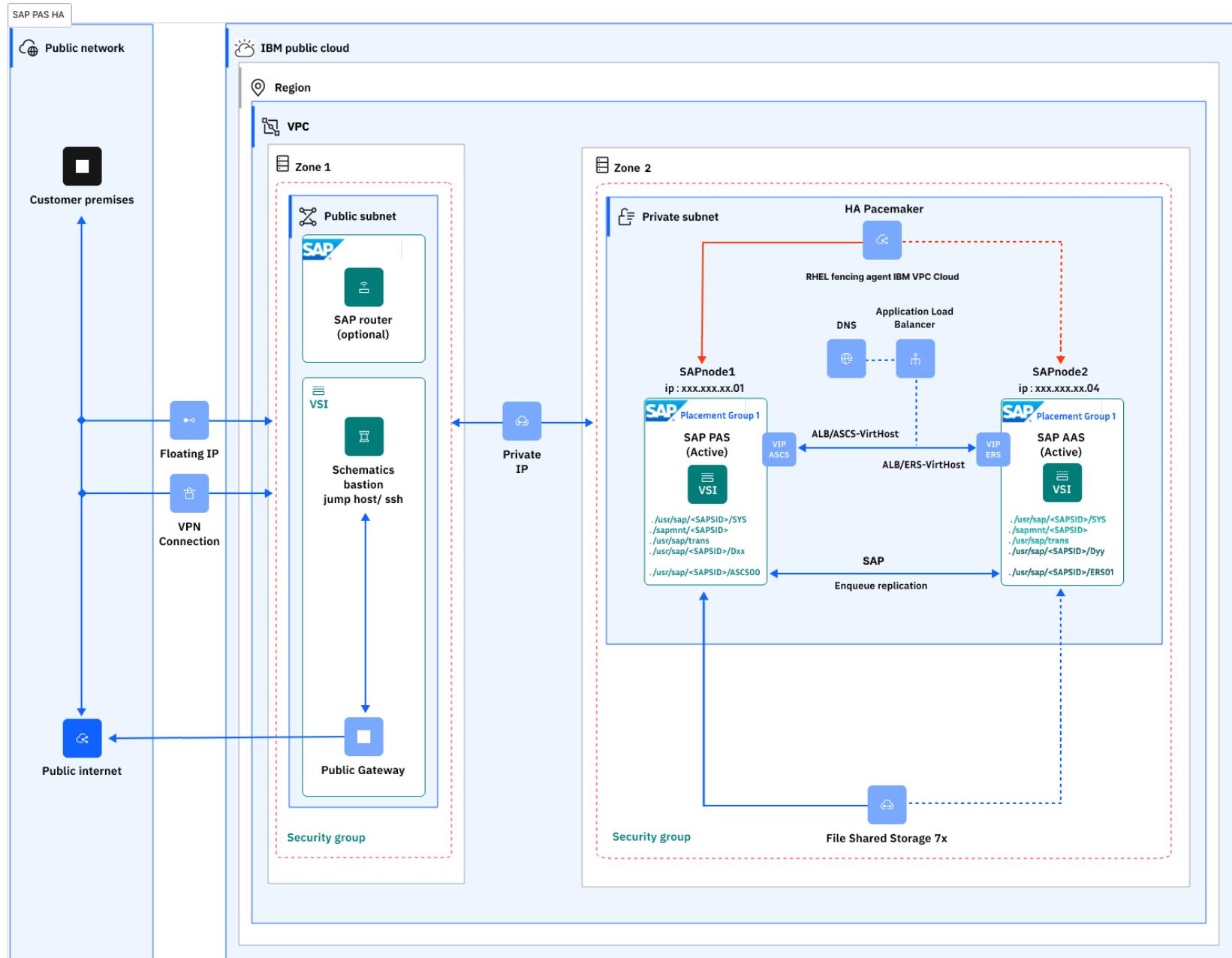
Use the following information to understand a simple use-case for planning, creating, and configuring resources for your VPC, and learn more about VPC overviews and VPC tutorials. For more information about the VPC, see [Getting started with Virtual Private Cloud \(VPC\)](#).

SAP products architecture on IBM Cloud VPC

A [Virtual Private Cloud \(VPC\)](#) contains one of the most secure and reliable cloud environments for SAP applications within your own VPC with virtual server instances. This represents an Infrastructure-as-a-Service (IaaS){: external} within IBM Cloud that offers all the benefits of isolated, secure, and flexible virtual cloud infrastructure from IBM. In comparison, the IBM Cloud classic infrastructure virtual servers offering uses virtual instances with native and VLAN networking to communicate with each other within a data center; however, the instances are restricted in one well-working pod by using subnet and VLAN networking as a gap scale up of virtual resources should rely between the pods. The IBM Cloud VPC network orchestrator layer concept eliminates the pod boundaries and restrictions, so this new concept handles all the networking for every virtual instance running within VPC across regions and zones.

Highly available system for SAP NetWeaver on IBM Cloud VPC

In a Highly Available (HA) system, every instance can run on a separate IBM Cloud virtual server instance. The cluster HA configuration for the SAP application server consists of two virtual server instances, each of them located in the same zone within the region by using placement groups. Placement groups assure that both cluster resources and cloud resources are also located in different compute nodes as specified in the following placement groups section:



SAP HA for SAP applications cluster nodes PAS (Active) and AAS (Active)

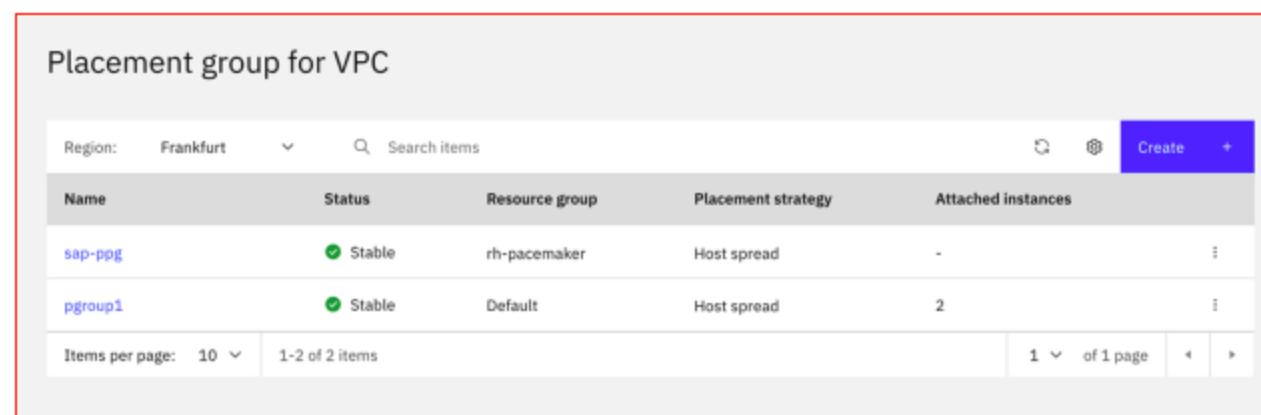
Placement groups on IBM Cloud VPC for SAP HA architecture

Placement Groups (PG) for VPC have two different anti-affinity strategies for high availability. By using the placement strategies, you minimize the chance of service disruption with virtual server instances that are placed on different hosts or into an infrastructure with separate power and network supplies.

The design of placement groups for IBM Cloud virtual servers solves this issue. Placement groups give a measure of control over the host on which a new public virtual server is placed. In this release, a “spread” rule is implemented, which means that the virtual servers within a placement group are spread onto different hosts. You can build a highly available application within a data center and know that your virtual servers are isolated from each other.

Placement groups with the spread rule are available to create in selected IBM Cloud data centers. After a spread rule is created, you can provision a virtual server into that group and ensure that it is not on the same host as any of your other virtual servers. This feature comes with no cost.

You can create your placement group and assign up to four new virtual server instances. With the spread rule, each of your virtual servers are provisioned on different physical hosts. In the following configuration example, the “Power Spread” option is used:



Placement groups host spread

Placement group for VPC					
Name	Status	Resource group	Placement strategy	Attached instances	
sapha-poc	Stable	wes-ic4sap-resourcegroup	Power spread	4	
Items per page: 10 1 item 1 of 1 page					

Placement groups power spread

Following are the SAP instances that are required for HA scenario:

- ABAP SAP Central Services (ASCS) instance - contains the ABAP message server and the ABAP enqueue server.
- Enqueue Replication Server (ERS) instance for the ASCS instance.
- Database instance
- Primary Application Server (PAS) instance on node 1.
- Additional Application Server (AAS) instance on node 2.



Note: It is recommended to run both the ASCS instance and the ERS instance in a switchover cluster infrastructure.

IBM Cloud File Storage for VPC for SAP HA architecture

[IBM Cloud File Storage for VPC](#) technology is used to make the SAP directories available to the SAP system. The technologies of choice are NFS, shared disks, and cluster file system. If you have decided to use the HA solution for your SAP system, make sure that you properly address the HA requirements of the SAP file systems in your SAP environment.

File shares for VPC								
Name	Status	Resource groups	Location	Mount targets	Size	Replication role	Encryption type	
usrsap-as1-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-as2-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-sapsacs-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-sapers-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-sapmnt-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-sapsys-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-trans-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	80 GB	None	Provider managed	

File shares for VPC

- File shares that are mounted as NFS permanent file systems on both cluster nodes for SAP HA application:
 - `/usr/sap/<SAPSID>/SYS`
 - `/sapmnt<SAPSID>`
 - `/usr/sap/trans`
- Cluster-managed file systems for SAP HA application: ASCS
 - `/usr/sap/<SAPSID>/ASCS00`
 - `/usr/sap/<SAPSID>/ERS01`
- Permanent NFS mount on SAP HA application node 1 PAS instance:
 - `/usr/sap/<SAPSID>/Dxx`
- Permanent NFS mount on SAP HA application node 2 dialog instance:
 - `/usr/sap/<SAPSID>/Dyy`

Prerequisites

You need to install the hardware (hosts, disks, and network) and decide how to distribute the database, SAP instances, and if required, the Network File System (NFS) server over the cluster nodes.

Context

Following are the types of SAP directories:

- Physically shared directories: `/<sapmnt>/<SAPSID>` and `/usr/sap/trans`

- Logically shared directories that are bound to a node, such as `/usr/sap`, with the following local directories:
 - `/usr/sap/<SAPSID>`
 - `/usr/sap/<SAPSID>/SYS`
 - `/usr/sap/hostctrl`
- Local directories that contain the SAP instances such as `/usr/sap/<SAPSID>/ASCS<Instance_Number>`
- The global transport directory may reside on a separate SAP transport host as a standard three systems transport layer configuration.

You need at least two nodes and a shared file system for distributed ASCS and ERS instances. The assumption is that the rest of the components are distributed on other nodes.

ASCS and ERS installation

In order for the ASCS and ERS instances to be able to move from one node to the other, they need to be installed on a shared file system and use virtual hostnames based on the virtual IP.

In this VPC-based SAP HA solution, the shared file system that is required by the cluster is replaced by the NFS-mounted file storage, and the virtual IP is replaced by the Application Load Balancer for VPC (ALB).

In this scenario, three ALBs are used, one for each Single Point of Failure (SPOF) component in order to replace the virtual IP requirement: ALB for ASCS, ALB for ERS, and ALB for ASE Sybase. Each ALB is configured as a backend for the corresponding cluster servers and redirects all of the communication that is received on the front-end ports to the active server in the backend pool.

Load balancers for VPC						
Region:	Frankfurt	▼	Search: poc	X		
Name	Status	Family	Resource group	Type	Hostname	Location
db-alb-hana-poc	Active	Application	wes-ic4sap-resourcegroup	Private	20bdd130-eu-de.lb.appdomain.cloud	Frankfurt
sap-alb-ers-poc	Active	Application	wes-ic4sap-resourcegroup	Private	3941d983-eu-de.lb.appdomain.cloud	Frankfurt
sap-alb-ascs-poc	Active	Application	wes-ic4sap-resourcegroup	Private	56a9190d-eu-de.lb.appdomain.cloud	Frankfurt

Application load balancer management of HA IPs mechanism

Private application load balancer

A [private application load balancer](#) is accessible through your private subnets that you configured to create the load balancer.

Similar to a public application load balancer, your private application load balancer service instance is assigned an FQDN; however, this domain name is registered with one or more private IP addresses.

IBM Cloud operations change the number and value of your assigned private IP addresses over time, based on maintenance and scaling activities. The backend virtual server instances that host your application must run in the same region and under the same VPC.

Use the assigned ALB FQDN to send traffic to the private application load balancer to avoid connectivity problems to your applications during system maintenance or scaling down activities.

Each ALB sends traffic to the cluster node where the application (ASCS, ERS, ASE Sybase DB) is running. During the cluster failover, the ALB redirects all the traffic to the new node where the resources are up and running.



Note: DNS-as-a-Service (DNSaaS) is the management IBM Cloud VPC DNS service of HA and FQDN (IPs) mechanism.



Note: The ALB has a default of 50 seconds for client and server timeout, so after 50 seconds of inactivity, the connection is closed. To support SAP connections through ALB and not lose connection after 50 seconds, you need to request a change this value to a minimum of 300 seconds (client-side idle connection = minimum 300s and server-side idle connection = minimum 300s). To request this change, open a support ticket. This is an account-wide change that affects all of the ALBs in your account. For more information, see [Connection timeouts](#).

DNS Services with VPC

[IBM Cloud DNS Services](#) provide private DNS to VPC users. Private DNS zones are resolvable only on IBM Cloud and from explicitly [permitted networks](#) in an account. To get started, create a DNS Services instance by using the IBM Cloud console.

DNS Services allows you to:

- Create the private DNS zones that are collections for holding the domain names.
- Create the DNS resource records under these DNS zones.
- Specify the access controls used for the DNS resolution of resource records on a zone-wide level.

DNS Services also maintains its own worldwide set of DNS resolvers. Instances that are provisioned under IBM Cloud on an IBM Cloud network can use resource records that are configured through IBM Cloud DNS Services by querying DNS Services resolvers.

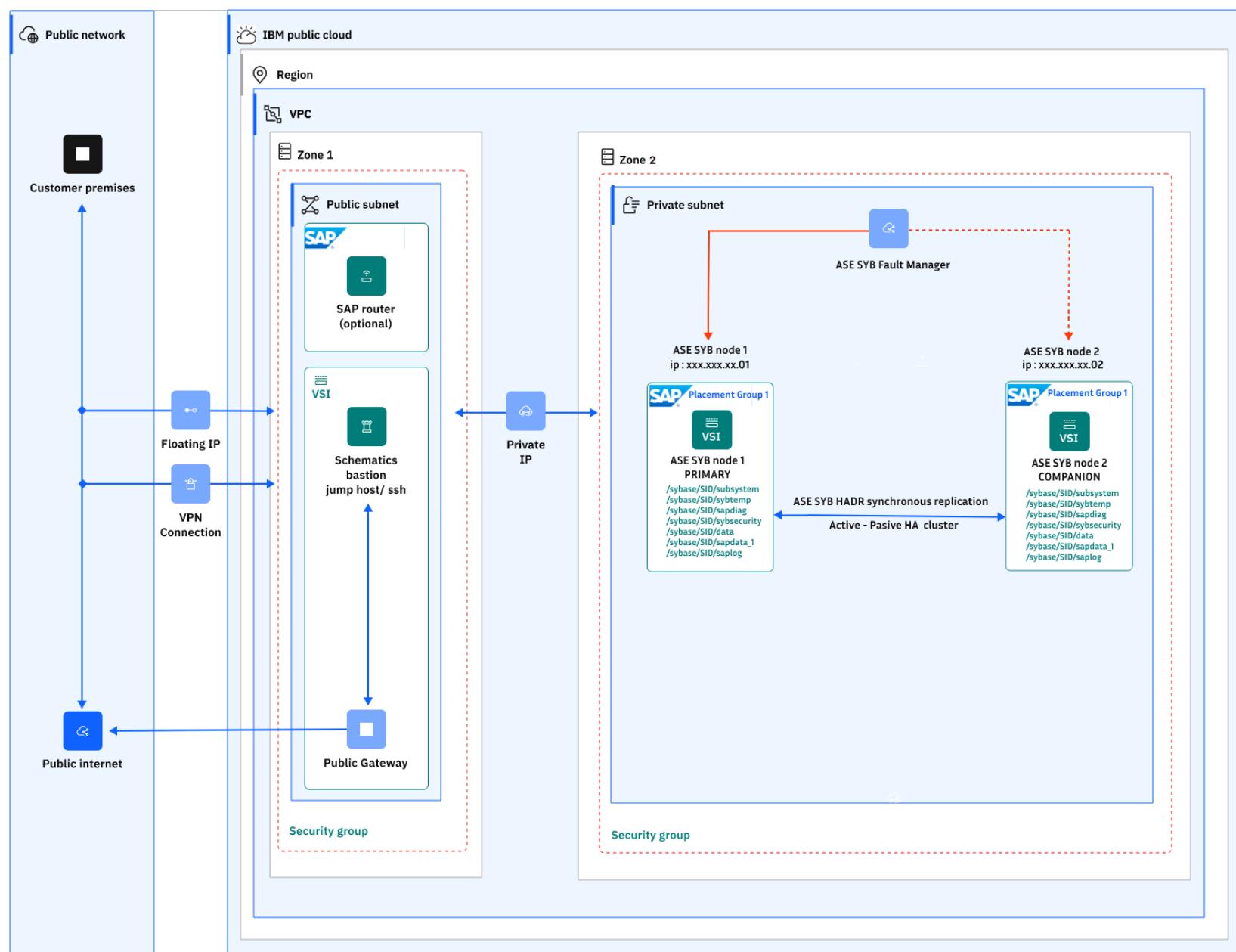
Resource records and zones that are configured through DNS Services are:

- Separated from the wider public DNS, and their publicly accessible records.
- Hidden from the system outside of and not part of the IBM Cloud private network.
- Accessible only from the system that you authorize on the IBM Cloud private network.
- Resolvable only via the resolvers provided by the service.

The DNS service maps the FQDN of each ALB to the virtual hostnames of the ASCS, ERS, and ASE Sybase that are used by SAP applications.

Type	Name	Value	TTL
CNAME	dbpochana	is an alias of 20bdd130-eu-de.lb.appdomain.cloud	12 hr
CNAME	sappocers	is an alias of 3941d983-eu-de.lb.appdomain.cloud	12 hr
CNAME	sappocases	is an alias of 56a9190d-eu-de.lb.appdomain.cloud	12 hr

Highly available system for SAP ASE Sybase database with HADR system



SAP HA for ASE Sybase DB instances cluster nodes primary (Active) and Secondary (Companion)

At the most basic level, a standard HA ASE Sybase cluster in an active(primary)-passive(companion) configuration has two nodes: one is the primary node and the other is the standby node. This means that the primary node is actively serving the active SAP DB instances (Primary and Companion), while the standby node is waiting to jump in if there is any failure.

The cluster is set with a virtual hostname IP (hostname is mapped to the FQDN of the ASE Sybase ALB through DNS, which is the same as

explained previously for SAP ASCS and ERS instances). Application instances (PAS and AAS) are used on the SAP profiles to call that particular component. The cluster assigns the virtual IP to the active node and uses a heartbeat monitor to confirm the availability of the components. If the primary node stops responding, it triggers the automatic failover mechanism that calls the standby node to step up to become the primary node. The ALB detects the change, redirects the traffic to the new active node, and assigns the virtual IP to it, restoring the component availability. Once fixed, the failed node comes online as a standby node.

SAP Sybase HADR system supports synchronous replication

The SAP Sybase HADR system supports synchronous replication between the primary and standby servers for high availability. An active-active setup is a two-node configuration where both nodes in the cluster include SAP ASE managing independent workloads, capable of taking over each others workload in the event of a failure.

The SAP ASE server that takes over the workload is called a secondary companion, and the SAP ASE server that fails is called the primary companion. Together they are companion servers. This movement from one node to another is called failover. After the primary companion is ready to resume its workload, it is moved back to its original node. This movement is called a failback.

When a system fails over, clients that are connected to the primary companion and use the failover property automatically reestablish their network connections to the secondary companion. You must tune your operating system to successfully manage both servers during fail over. See your operating system documentation for information about configuring your system for high availability. An SAP ASE configured for failover in an active-active setup can be shut down using the shutdown command only after you have suspended SAP ASE from the companion configuration, at both the server level and the platform level.

The always-on option in a High Availability and Disaster Recovery (HADR) system consists of two SAP ASE servers:

- Primary on which all transaction processing takes place.
- Warm standby (referred to as a "standby server" in DR mode, and as a "companion" in HA mode) for the primary server, and contains copies of designated databases from the primary server.



Note: The HADR feature that is shipped with SAP ASE version 16.0 SP02 supports only a single-companion server.

Some high-availability solutions (for example, the SAP Adaptive Server Enterprise Cluster Edition) share or use common resources between nodes. However, the HADR system is a "shared nothing" configuration, each node has separate resources including disks.

In an HADR system, servers are separate entities and data is replicated from the primary server to the companion server. If the primary server fails, a companion server is promoted to the role of primary server either manually or automatically. Once the promotion is complete, clients can reconnect to the new primary server, and see all committed data, including data that was committed on the previous primary server.

Servers can be separated geographically, which makes an HADR system capable of withstanding the loss of an entire computing facility.



Note: The HADR system includes an embedded SAP Replication Server, which synchronizes the databases between the primary and companion servers. SAP ASE uses the Replication Management Agent (RMA) to communicate with Replication Server and SAP Replication Server uses Open Client connectivity to communicate with the companion SAP ASE.

The Replication Agent detects any data changes made on the primary server and sends them to the primary SAP Replication Server. In the figure above, the unidirectional arrows indicate that, although both SAP Replication Servers are configured, only one direction is enabled at a time.

The HADR system supports synchronous replication between the primary and standby servers for high availability so the two servers can keep in sync with Zero Data Loss (ZDL). This requires a network link that is fast enough between the primary and standby server so that synchronous replication can keep up with the primary servers workload. Generally, this means that the network latency is approximately the same speed as the local disk IO speed, a few (fewer than 10) milliseconds. Anything longer than a few milliseconds may result in a slower response to write operations at the primary.

The HADR system supports asynchronous replication between the primary and standby servers for disaster recovery. The primary and standby servers by using asynchronous replication can be geographically distant, meaning they can have a slower network link. With asynchronous replication, Replication Agent Thread captures the primary servers workload, which is delivered asynchronously to SAP Replication Server. The SAP Replication Server applies these workload change to the companion server.

The most fundamental service that is offered by the HADR system is the failover; planned or unplanned from the primary to the companion server, which allows maintenance activity to occur on the old primary server, while applications continue on the new primary.

The HADR system provides protection in the event of a disaster. If the primary server is lost, the companion server can be used as a replacement. Client applications can switch to the companion server, and the companion server is quickly available for users. If the SAP Replication Server was in synchronous mode before the failure of the primary server, the Fault Manager automatically initiates failover with

zero data loss.

Fault Manager installation on the SAP ASCS node

The required parameters are asked during the installation process to create a profile for the fault manager and then adds it to the instance start profile. It is also possible to run the installation by using an existing profile: `sybdbfm install pf=<SYBHA.PFL>` In this case, the installation process will only ask for profile parameters missing in the profile.



Note: Fault manger is integrated with ASCS on same SAP PAS/AAS cluster (start/stop/move together).

There may be some data loss if the SAP Replication Server was in asynchronous mode and you must use manual intervention to failover for disaster recovery.

Connection attempts to the companion server without the necessary privileges are silently redirected to the primary companion via the login redirection mechanism, which is supported by Connectivity libraries. If login redirection is not enabled, client connections fail and are disconnected.

The SAP ASE HADR option installs the below components:

- SAP ASE
- SAP Replication Server
- Replication Management Agent (RMA)
- SAP Host Agent
- Fault Manager
- SAP ASE Cockpit



Note: This automation is offered at no cost; however, the provisioned infrastructure comes at cost.

Hybrid Cloud Network Consideration for SAP applications on IBM Power Virtual Server

A hybrid cloud environment combines the on-premises site with IBM® Power® Virtual Server. To join SAP S/4HANA systems between both sites, multiple network connection options are available.

Due to typically huge SAP S/4HANA database sizes, a minimum network bandwidth is mandatory for productive systems.

The following topics are covered in the following sections:

- A rough network migration minimum bandwidth considerations for SAP workloads
- A brief overview of hybrid cloud connection options that are available that includes links to the setup descriptions
- Extra required network services to migrate an SAP system
- Test of network connections for SAP workload



Note: This information doesn't replace existing SAP or other vendor documentation.

Network bandwidth considerations

Bandwidth is determined by the required connection speed between on-premises and IBM Cloud® depends on project scenario, network protocols, migration path, and project target.

A hybrid scenario with collaborating systems in IBM Cloud® and on-premises needs different requirements when compared with a one-time move of a system to IBM Cloud® for isolated testing.

Network bandwidth is the main limiting factor for

- Full synchronization time of the database servers
- Delta replication time
- Outage time during takeover



Important: The full synchronization is necessary as well for the initial upload as to fix synchronization issues when they occur.

Discuss bandwidth with your network provider and network specialist, as every connection type is different.

Example - Synchronization time estimation for an IPsec connection

As a rough estimation, consider an example that uses an IPsec VPN connection over a dedicated internet connection. A full synchronization time can be estimated by using the following formula:

$$\text{Time} = 200\% * (\text{data transfer size}) / \text{Bandwidth}$$

Estimation example.

- Data base size: 922 GB
- Expected changes while data transfers: 10%
- Data transfer size: $110\% * 922 \text{ GB} = 1024 \text{ GB}$
- Bandwidth: 500 MBit/s = 0.061 GB/s
- Estimated transfer time is $200\% * 1024/0.061 = 33554 \text{ sec} = 9:19 \text{ hours}$

The calculated +100% overhead is a broad approach for necessary TCP/IP headers, IPsec headers, and extra data transfers. It does not consider data retransmission or shared network usage. This estimation is intended to help determine the required minimum bandwidth.

The following table lists the calculated transfer times for a 1-Terabyte database:

Data base transfer size	Bandwidth	Overhead	Time for full sync
1024 GB	10 GBps	+100%	00:27 hours
1024 GB	5 GBps	+100%	00:54 hours
1024 GB	2 GBps	+100%	02:16 hours
1024 GB	1 GBps	+100%	04:33 hours
1024 GB	500 MBps	+100%	09:19 hours
1024 GB	250 MBps	+100%	18:38 hours
1024 GB	150 MBps	+100%	31:38 hours

Calculated estimated time for IPsec VPN full synchronization

As an example, if an SAP system needs to be productive again within 8 hours after a synchronization error occurred, for a 922 GB database size, the calculated network bandwidth must be greater than 500 MB/s.



Important: This estimation is based on assumptions. It is not qualified or intended to determine the accurate replication time. Consult your network provider, or measure the time of a test replication to determine reliable values specific for your network setup.

Network connection option overview

A hybrid cloud setup in general combines the customer network with a customer network segment in IBM Cloud®. It is an extension of the existing customer network, as if you would connect a remote data center.

Connecting an on-premises network with IBM Power Servers in Power Virtual Server in IBM Cloud® is described in [Network architecture diagrams](#).

If you are new to Power Virtual Server, architectures from the [Power Edge Router \(PER\) use cases](#) are the recommended ones and are the easiest to implement. If you have an existing Power Virtual Server workspace, you might either consider migrating to the newer PER setup or inspect the [Power Virtual Server networking environment](#) description.

Both PER and non-PER architectures offer these types of network connection options:

IBM Cloud® Direct Link 2.0

IBM Cloud® Direct Link is a suite of offerings that enables the creation of direct, private connections between your on-premises network and IBM Cloud®, without traversing the public internet. For more information, see [Getting started with IBM Cloud® Direct Link \(2.0\)](#) and [Connecting an on-premises data center](#).

Internet VPN

Internet VPN uses the public internet to connect on-premises networks and IBM Cloud® networks through a VPN. At IBM Cloud® the VPN is either terminated by a gateway device, gateway appliance, or a VPN as a service (VPNaas). Read the IBM Power Virtual Server specific [Creating VPN connections](#) article.

The easiest way to establish a site-to-site VPN is to start with the VPN-as-a-service (VPNaas). Read the article [FAQs for site-to-site VPN gateways](#) for more details.

Required network services

A hybrid cloud setup extends your company network to your instances in IBM Cloud®. Servers and clients in this hybrid network need to communicate with each other.

A hybrid cloud setup helps with the following points:

- Routing between both networks works
- Firewall rules permit traffic through required ports
- DNS name resolution for both networks works

Testing network connections for an SAP workload

SAP provides a tool `niping` that checks the network interface up to OSI layer 4, which means it verifies that transport layer TCP/UDP packages can be exchanged. This SAP tool demonstrates a working connection, even if ICMP packages are dropped and a simple ping would fail.

Refer to [SAP Note 500235 - Network Diagnosis with NIPING](#) for further NIPING details.

For migrating SAP systems by using SAP HANA database replication between SAP HANA databases on-premises and Power Virtual Server, the source and target servers are the two database servers. The following two commands verify the connection between a source- and a target-system.

1. *NIPING server*: Use the following command to run the `niping` server on one system, for example named `host1`.

```
$ niping -s
```

2. *NIPING client*: Then, run the niping client application on the second system to verify the connection to the first system `host1`.

```
$ niping -c -H host1
```



Note: An SAP Router is typically not involved in server-to-server communication. Consult the niping documentation to determine the proper connection string if you are using an SAP Router.

Migrating SAP S/4HANA to IBM Power Virtual Server

Steps before you migrate an SAP S/4HANA database

The following sections cover several important advisories to prepare for the SAP HANA database migration. Read and implement the relevant SAP notes.

Before you attempt any data migration or replication action, check the source database for any existing issues.

If issues exist, it might be one of the following issues.

- Interrupted or failed garbage collection.
- Source databases still contain entries, tables, or data from actions such as client deletion, which leads to a false positive on the true size of the database.
- Reported inconsistencies during the database check.
- Extreme load or unload actions that lead to orphaned entries.
- Hardware issues that occurred during a delta merge from memory to disk.
- Excessive page memory dumps were detected, which can indicate page corruptions.
- Alerts that are displayed during an SAP HANA Mini Check.



Important: Incorrectly performing any data migration or replication action can result in data loss and application inconsistencies. Make sure that you read and understand the associated SAP Notes and correction notes before you perform any related task. IBM Cloud® is not liable for any data loss or application integrity.

The following sections contain SAP-advised pre-steps to help make sure that the source database is in a consistent state. Before any migration or backup or recovery operation begins that the consistency (such as Row store, Column Store, Pages) and trace files that are on the source database are closely examined for any existing issues. These recommended steps must be completed before you start the migration.

Checking and confirming database health

Check the health of your database to reduce the risk of transferring existing issues to your target system. Health checks prevent pre-existing issues (such as consistency or block corruption) from migrating onto the target SAP HANA system. SAP HANA System Replication can't help you in this scenario, so it is important to perform these necessary checks. Use the following SAP Notes to assist you.

- [SAP Note 2116157 - FAQ: SAP HANA Consistency Checks and Corruptions](#)
- [SAP Note 2272121 - How To: Analyzing Physical Corruptions with the SAP HANA Persistence Diagnosis Tool](#)
- [SAP Note 2380176 - FAQ: SAP HANA Database Trace](#)

Checking the database trace files

The database trace is written to service specific files on operating system level. The trace directory is located here:

```
/usr/sap/<SID>/HDB<inst>/<host>/trace/DB_<SID>/
```

The following alias in the environment of the `<sid>adm` user helps you to quickly switch to the trace directory on the OS level:

```
cdtrace
```

The database trace files use the following naming convention:

```
<service>_<host>.<port>.<counter>.trc
```

In the context of dynamic tiering, a file with the following convention can exist (SAP Note 2871785):

```
eserver_console_<host>.<port>.<counter>.trc
```

 Example:

```
indexserver_saphana01.30003.024.trc
```

 You can access these files either directly, at the operating system level, or in one of the following ways:

- [SAP HANA Studio -> Administration -> Diagnosis Files](#)
- [DBACOCKPIT -> Diagnostics -> Diagnosis Files](#)

More checking information

- [SAP HANA Administration Guide - Persistence Consistency Check](#)

The SQL statements that are in the following SAP notes indicate whether a database reorganization is required and the amount of space that is saved after the reorg action takes place.

This check serves two purposes.

1. Highlights whether the reorg action is required on the SAP HANA database.
2. If a reorg action is required, it provides an estimated size after space saving actions are completed.

Reorganizing database row store

If your database is heavily fragmented, a row store reorganization is required.

Starting from SAP HANA 2.0 SPS04, online row store reorganization automatically triggers for large row store (allocated size \geq 3.2 GB) if the utilization ratio is less than the defined threshold.

By default, the threshold is 60% and the utilization ratio is checked in the background once an hour.

- [SAP Note 2789255 - Automatic Online Row Store Reorganization](#)

If your database version is less than `SAP HANA 2.0 SPS04`, then follow the instructions that are in

- [SAP Note 1813245 - SAP HANA Row Store Reorganization](#)

- [SAP Note 1977584 - Technical Consistency Checks for SAP HANA Databases](#) This SAP Note contains useful SQL statements to check the CATALOG, DEPENDENCY, and TABLE CONSISTENCY.

! **Important:** Make sure that you pay attention to the instructions that are in these SAP Notes and follow each step that relates to your existing SAP HANA version.

SQL mini checks

Use this SQL statement to show the current size of the SAP HANA database.

```
SELECT HOST, PORT, TO_DECIMAL( SUM(FREE_SIZE)*100 / SUM(ALLOCATED_SIZE), 10,2) "Free Space Ratio in %",TO_DECIMAL(
SUM(ALLOCATED_SIZE)/1048576, 10, 2) "Allocated Size in MB",TO_DECIMAL( SUM(FREE_SIZE)/1048576, 10, 2) "Free Size in MB"
FROM
M_RS_MEMORY WHERE ( CATEGORY = 'TABLE' ) and ( ALLOCATED_SIZE > 0 ) GROUP BY HOST, PORT
```

For more useful SQL statements, you can use the following SAP Note. This SAP Note includes some useful SQL statements that you can run from the command line by using the `hdbsql` executable file. Or, you can use the SQL Console that is built into SAP HANA Studio.

- [1969700 - SQL Statement Collection for SAP HANA](#)

! **Important:** Commands from SQLStatements_Internal.zip impose an increased risk of instabilities such as crashes or terminations. If you run these commands, run them with care. Perhaps running them first on a DEV or POC system first.

The following SQL statement helps you identify critical technical issues. When you download the SQL Collection compressed files, search for `SQL: "HANA_Configuration_MiniChecks"`.

`SQL: "HANA_Configuration_MiniChecks"` performs several mini checks and returns `C = 'X'` if it finds a potentially critical situation. You can use the following SAP Note to interpret the results.

- [SAP Note 1999993 - How-To: Interpreting SAP HANA Mini Check Results](#)

Scheduling an SAP HANA sizing report on the source system

If you plan to migrate an existing SAP system from an on-premise site to your IBM Cloud® environment, you need to first run an SAP Sizing report. The current version for the SAP HANA memory sizing report is `Advanced correction version 17`.

- [SAP Note 3338309 HANA memory Sizing report - Advanced correction 17](#)

If you want to run the SAP HANA Sizing report, see the following SAP Note.

- [SAP Note 1872170 - ABAP on HANA sizing report \(S/4HANA, Suite on HANA...\)](#)

It is advised that you use the most recent Advanced Correction of the SAP Sizing report. When you run the report, make sure that you include the forecast for SAP HANA database growth. The generated report states the anticipated required CPU, memory, and storage recommendations for your Power Virtual Server instance target. Go to IBM Cloud® and select the most recent certified profile that is available for IBM Power Virtual Servers.

- [SAP 2947579 - SAP HANA on IBM Power Virtual Servers](#)
- [SAP 2188482 - SAP HANA on IBM Power Systems: Supported hardware and features](#)

Extra sizing SAP Notes

- [SAP Note 2363248 - SAP BW/4HANA Hardware Sizing](#)
- [SAP SD benchmark results](#)
- [Measuring in SAPS \(SAP Application Performance Standard\)](#)

Using the EarlyWatch Alert reports as an early indicator

If your on-premises landscape has an SAP Solution Manager set up, you can generate the EarlyWatch Alert report for your source system.

The report outlines specific issues that your on-premises source system might have. You must address SQL performance indicators, Urgent performance KPI indicators immediately. Issues that are classified as `Red` or `Severe problems detected` must be handled as soon as possible.

Check the EarlyWatch Alert report for existing issues with the source SAP HANA database and act upon each finding in the `Service Summary`

or [Alert Overview](#) sections, based on its severity.

More related SAP Notes for EarlyWatch Alert reports

- [SAP Note 1257308 - FAQ: Using EarlyWatch Alert](#)
- [SAP Note 1958910 - EarlyWatch Alert For HANA Database](#)
- [SAP Note 1911180 - HANA EarlyWatch Alerts \(EWA\) Issues](#)
- [SAP Solution Manager - Help Portal Documentation](#)

Source database credentials

When you add an SAP HANA system to the SAP HANA System Replication setup, remember that the replication process from source primary to the target secondary server overwrites the MDC User Tables `SAP${sid}.USR02`. So, it is important to know (by checking the SAP HANA Studio) what the current user with SYS privileges that was used to register the MDC in SAP HANA Studio on the source. As a [Best Practice](#), make sure that you know the login credentials for the database user and the password for the source system. If, for example, you forget the passwords and proceed with the SAP HANA System Replication from the source to the target you can test the secondary target by swapping the primary and secondary servers. If you do not know the login credentials for the database user and the password on the source system then you can't register the system in either SAP HANA Studio or an SAP HANA Cockpit setup.

Creating the target SAP HANA system on IBM Power Virtual Server

Planning the IBM Power Virtual Server deployment

A Power Server workspace in your IBM Cloud account is a prerequisite for the following steps. Read details in [Hybrid Cloud Network Considerations for SAP on IBM Power Virtual Server](#).

A hybrid cloud network connection needs to be in place, as described in [Hybrid Cloud Network Considerations for SAP on IBM Power Virtual Server](#).

The Planning for a deployable SAP HANA infrastructure is described in [Planning your deployment](#).

The sizing aspect of the target system is vital to your planning. Follow the recommendations mentioned in the SAP HANA Sizing report on the source system. Also, consider the findings of the EarlyWatch Alert report (EWA report). Both factors provide a realistic approach on the recommended size of your target system, see [Sizing process for SAP Systems](#).

Comparing the required CPU, cores and storage for your target system

- [IBM Cloud Doclink SAP Planning/Sizing](#)

Check that the certified profiles in IBM Cloud® are close to or match the recommendations that are mentioned in the source system sizing report and also consider the EWA report summary.

Select the correct IBM Power Systems Virtual Server Certified Profile from the following two links:

- [IBM Power Virtual Server Certified Profiles SAP HANA](#)
- [SAP Note 2947579 - SAP HANA on IBM Power Virtual Servers](#)

Target server must have equal or greater storage capacity than the source system and be sized correctly

Remember to take SAP HANA database growth into consideration and the need to follow the IBM System Storage Architecture and Configuration Guidelines for SAP HANA TDI.

The following document outlines the required storage configuration for the target server in IBM Cloud:

- [IBM System Storage Architecture and Configuration Guide for SAP HANA TDI](#)

Consider the extra space that you need to create a file system mount point to store software executable files and the initial SAP HANA system backup. Depending on your planned IBM Power Virtual Server infrastructure, you can create the file system as an NFS mount to export to other systems in the architecture.

Creating the software repository file system and transfer the installation packages

As used in previous demo systems, the mount point `swrepo` is created with at least 200 GB of free space. Download the SAP HANA Software from SAP Marketplace - the version that matches your SAP HANA version from the source system.

- [Software Downloads main page](#)

- Access Software Downloads in SAP for Me
- Enter your SAP "S" user ID and password to proceed.
- [Software Center Catalog view](#)
 - Support Packages & Upgrades
 - By Alphabetical Index (A-Z)
 - "H"
 - SAP HANA PLATFORM EDITION
 - SAP HANA PLATFORM EDITION 2.0
 - SAP HANA DATABASE 2.0
 - Make sure that the Selection box shows **LINUX ON POWER LE 64BIT**
 - Select the IMDB_SERVER20 that is installed on the Source System, and download to your laptop or PC
 - Go back to the SAP HANA PLATFORM EDITION 2.0 page
 - SAP HANA CLIENT 2.0
 - Make sure that the Selection box shows **LINUX ON POWER LE 64BIT**
 - Select the release that you installed on the source system (or one version higher if your version is not on the list)
 - Navigate back to * [Software Center Catalog view](#)
 - Support Packages & Upgrades
 - On the right side, is a search box, search for **SAPCAR**
 - On the Displayed results list, select **SAPCAR 7.53** Maintenance Software Component
 - Select the file **SAPCAR_1200-70007726.EXE** and make sure that the Selection box shows **LINUX ON POWER LE 64BIT**
 - Download to your laptop or PC or Jump Host

Create a directory **/swrepo** on the target system.

```
$ sudo mkdir /swrepo
```

Make sure that your user owns this directory, so the user can work and extract files.

```
$ sudo chown $USER: /swrepo
```

Transfer the installation files and sapcar utility downloads to the target SAP HANA server **/swrepo** mount point. The SAPCAR utility needs executable permissions to unpack the .SAR archive files.

```
$ chmod -R 755 /swrepo/SAPCAR_1200-70007726.EXE
```

Tip: You can set an alias SAPCAR for this utility in the **.bash_profile**. This setting enables the SAPCAR command from any directory.

To add a line to your bash profile, use the following command.

```
$ echo "alias SAPCAR='/swrepo/SAPCAR_1200-70007726.EXE'" >>$HOME/.bash_profile
```

Use the source command to enable the new defined alias.

```
$ source $HOME/.bash_profile
```

Check whether it works by running **SAPCAR -v** to get the version list:

```
$ SAPCAR -v
```

Unpacking the files

Use the following examples to unpack the files.

```
$ SAPCAR -xvf IMDB_CLIENT20_XXX_XX-XXXXXXXX.SAR -manifest /SAP_HANA_CLIENT/SIGNATURE.SMF
```

The sapcar file extraction output looks like the following example.

```

x SAP_HANA_CLIENT/SIGNATURE.SMF
SAPCAR: 98 file(s) extracted

SAPCAR -xvf IMDB_SERVER20_XXX_XX-XXXXXXX.SAR -manifest /SAP_HANA_DATABASE/SIGNATURE.SMF

x /SAP_HANA_DATABASE/SIGNATURE.SMF
SAPCAR: 355 file(s) extracted

```

During extraction directories `/swrepo/SAP_HANA_DATABASE` and `/swrepo/SAP_HANA_CLIENT` are created and contain the files that are required for the installation.

Making sure that the target server OS and patch level match the source server

Check the operating system version and patch level on the target system. For productive systems, the same level makes sure that the installation performs similar and migrating runs with ease. For nonproductive systems, for example, a proof of concept system (POC) in IBM Power Virtual Server, a higher operating system version is a valid option.

Target server - Both RHEL and SLES

To determine the operating system version and patch level, run the following command.

```
$ cat /etc/os-release
```

Alternatively on Red Hat Linux systems you can use a second file.

```
$ cat /etc/redhat-release
```

On SUSE Linux Enterprise Server (for SAP Applications) the release and patch level can be listed with the following command.

```
$ lsb_release -a
```

Making sure that the file system and mount points match the source system

The source and target systems must have the identical mapping for storage, LVM, and file systems. Only on target is the larger storage capacity that is needed or the Migration. File system structure requirements are also highlighted in the beginning of this section with the TDI requirements. Also, consider that the mount point and file ownership UID and GID match the source system. Also, mount points need the same `<SID>` defined on both systems. When you install SAP HANA on the target system, the same `<SID>` and `<instance number>` from the source system are used.

```

$ export SID=<SID>                      # SAP HANA System ID (uppercase)
export sid=<sid>                         # SAP HANA System ID (lowercase)
export INSTNO=<INSTNO>                     # SAP HANA Instance Number

export SiteOnPrem=<PrimarySiteName>       # HANA System Replication Site Name 1 - Migration from On-Prem - Source
export SiteOnCloud=<secondarySiteName>      # HANA System Replication Site Name 2 - Migration to On-Cloud - Target

export NODE1=<Hostname 1>                  # Hostname of On-Prem Server
export NODE2=<Hostname 2>                  # Hostname of IBM Power Virtual Server Instance

```

Entries in `/etc/hosts` for all systems involved in the migration project

The `/etc/hosts` file needs to contain entries for the Source System and any dependent SAP Netweaver or S/4 FES Application Server. You can use a DNS server for your network resource resolution, but it helps if you include the IP addresses, short name, FQDN, and description to help identify servers in the landscape in the `/etc/hosts` file, especially if issues occur with network resolution or the DNS services.

Preparing and tuning the OS for SAP HANA

Use the following SAP Notes to begin the preparation phase of the target system for the installation of SAP HANA.

- [SAP Note 2777782 - SAP HANA DB: Recommended OS Settings for RHEL 8](#)
- [SAP Note 2772999 - Red Hat Enterprise Linux 8.x: Installation and Configuration](#)
- [SAP Note 3018133 - Linux: Running SAP applications compiled with GCC 10.x](#)

Make sure that you completed the tasks that are mentioned in the `Recommended OS Settings for RHEL 8` as these tasks are important

tuning and performance settings that need to be applied. If ignored, it can impact the installation of SAP products and the performance thereafter.

Pre-SAP HANA checks by using the hcmt tool

The SAP HANA hardware and cloud measurement tools `hcmt` help measure and analyze your hardware or cloud systems before you deploy SAP HANA or apply for SAP HANA certification. The tools consist of the following components:

- SAP HANA hardware and cloud measurement tool
- SAP HANA hardware and cloud measurement analysis

Use the following SAP Note to check and verify the OS and configuration before you install SAP HANA.

- [SAP Note 2493172 - SAP HANA Hardware and Cloud Measurement Tools](#)

Tip: If you have a port issue when you run `hcmt`, open a second Terminal session. Navigate to the setup directory of `hcmt`, now start a session that keeps the required port open.

To run `hcmt` in server-client mode, you need to start two sessions:

1. `hcmt` server mode on - a jump host to collect test result from remote servers
2. `hcmt` client on the target systems that are intended to run SAP HANA, run `hcmt` performance test by using the full execution plan.

Hcmt server session

The hcmt server collects data that is measured on hcmt client systems. A typical system to run the hcmt server is a jump host or similar system. Navigate to the directory where hcmt is installed, and run the following command

```
$ sudo ./hcmt -v -S
```

The following example is the expected output.

```
hcmt-2.00.062.00.1650891137 (2022-04-25 15:12:20)

Server started, listening on port 50000 ...
```

Hcmt client session

On the target system that you want to be the SAP HANA server, run the `hcmt` command as a client by using the full execution plan.

```
$ sudo ./hcmt -v -p /swrepo/HCMT/setup/config/full_executionplan.json
```

System output:

```
hcmt-2.00.062.00.1650891137 (2022-04-25 15:12:20)
Loading executionplan
LogVolume (/hana/log):
DataVolume (/hana/data):
Hosts: <`Leave Blank!!!!`> Leave this field blank, otherwise it will affect the test.
Start execution of plan
Executing Test C9C9F832-854F-492D-8E7EFB4609AC435C
Note: CPU Micro Benchmark
```

Tip: If you receive an error 'Port 50000 is already used', SAP HANA is probably installed already. Stop the SAP HANA system and then run the `hcmt` command again.

Plan Variant: CPU Performance

This command generates a hcmresult-YYYYMMDDHHMMSS.zip file in the setup directory. Upload this file to the HCMT SAP website and review the results to make sure that the HANA is set up and configured correctly.

- [SAP HCMT Cloud Server URL](#)

If you experience issues, you can still use the old check tool.

- [SAP Note 1943937 – Hardware Configuration Check Tool](#)

Installing SAP HANA on the target system

Remember the following variables:

```
export SID=<SID>                      # SAP HANA System ID (uppercase)
export sid=<sid>                        # SAP HANA System ID (lowercase)
export INSTNO=<INSTNO>                   # SAP HANA Instance Number
```

For this example, the installation is up to the point where you need to enter "Y" to continue. Navigate back to the HANA_DATABASE directory.

Run the SAP HANA database lifecycle manager command.

```
$ sudo ./hdblcm
```

The following example is the expected output.

```
SAP HANA Lifecycle Management - SAP HANA Database 2.00.061.00.1644229038
*****
```

This will scan the directories for the required software.

```
Scanning software locations...
Detected components:
  SAP HANA Database (2.00.061.00.1644229038) in /swrepo/HANA/SAP_HANA_DATABASE/server
  SAP HANA Database Client (2.11.20.1644165757) in /swrepo/HANA/SAP_HANA_CLIENT/client

Do you want to specify additional components location? (y/n) [n]: `n`
```

Choose **n** for no additional components location and continue.

```
Choose an action

Index | Action           | Description
-----|-----|-----
1    | install          | Install new system
2    | extract_components | Extract components
3    | print_detected_components | Print detected components
4    | Exit (do nothing) | 

Enter selected action index [4]: `1`
```

Enter **1** and press **<enter>** key to install a new system.

Output continues with the following example.

```
SAP HANA Database version '2.00.061.00.1644229038' will be installed.

Select additional components for installation:

Index | Components | Description
-----|-----|-----
1    | all         | All components
2    | server      | No additional components
3    | client      | Install SAP HANA Database Client version 2.11.20.1644165757

Enter comma-separated list of the selected indices [3]: `1`
```

Enter **1** and press **<enter>** to install all components. Accept a series of defaults on the next line in the output.

```
Enter Installation Path [`/hana/shared`]:
Enter Local Host Name [`Yourhostname`]:
Do you want to add hosts to the system? (y/n) [`n`]:
```

Enter **n** for no additional systems. Check the source SAP HANA database system parameters:

- source SAP HANA **SID**
- source SAP HANA **Instance Number**

Continue with the same values for the target system:

```
Enter SAP HANA System ID: `<Needs to match the source system>`  
Enter Instance Number [00]: `<Needs to match the source system>`  
Enter Local Host Worker Group [default]:  
  
Index | System Usage | Description  
-----  
1 | production | System is used in a production environment  
2 | test | System is used for testing, not production  
3 | development | System is used for development, not production  
4 | custom | System usage is neither production, test nor development  
  
Select System Usage / Enter Index [4]: 2
```

Enter a number that represents the planned function. In the example, **2** indicates a system for testing.

Accept more default values:

```
Do you want to enable data and log volume encryption? [n]:  
Enter Location of Data Volumes [/hana/data/<SID>]:  
Enter Location of Log Volumes [/hana/log/<SID>]:  
Restrict maximum memory allocation? [n]:  
Apply System Size Dependent Resource Limits? (SAP Note 3014176) [y]:
```

Determine these passwords as set on the source system:

- **sapadm** password
- **<sid>adm** password
- System Database User **SYSTEM** password

Set the same passwords on the target system:

```
Enter SAP Host Agent User (sapadm) Password: <Use the same password used on the source system>  
Confirm SAP Host Agent User (sapadm) Password: <Use the same password used on the source system>  
Enter System Administrator (<sid>adm) Password: <Use the same password used on the source system>  
Confirm System Administrator (<sid>adm) Password: <Use the same password used on the source system>  
Enter System Administrator Home Directory [/usr/sap/<SID>/home]:  
Enter System Administrator Login Shell [/bin/sh]:  
Enter System Administrator User ID [1001]: <check that the user ID number matches the source system>  
Enter ID of User Group (sapsys) [79]: <Check that the GUID number matches the source system>  
Enter System Database User (SYSTEM) Password: <Use the same password used on the source system>  
Confirm System Database User (SYSTEM) Password: <Use the same password used on the source system>  
  
Restart system after machine reboot? [n]:  
Summary before execution
```

At the summary, you can check to make sure that the selections that you made for the installation are correct. Then, select "Y" to begin. After about 20 minutes, you see the following message.

```
Registering SAP HANA Database Components on Local Host...  
- Deploying SAP Host Agent configurations...  
Creating Component List...  
SAP HANA Database System installed  
Log file written to xxxxxxx
```

Checking that SAP HANA is running and determining the version

Run the following **HDB proc** command to verify that all services started on the primary and secondary SAP HANA system.

```
$ sudo -i -u ${sid}adm -- HDB proc
```

SAP HANA version needs to be equal or greater than the primary server

To verify the SAP HANA database version, use the following command on both nodes.

```
$ sudo -i -u ${sid}adm -- HDB version
```

Initial backup of the MDC/SYSTEMDB SAP HANA database

Backup SYSTEMDB

Add both the SYSTEMDB entry and the MDC to the HANA Studio Application. Or, If you have an SAP HANA Cockpit in your landscape, you can add the target system to your HANA Cockpit instead. After both systems are added, complete an initial system backup. On the SYSTEMDB entry, -> right click and select.

- Backup & Recovery
- Backup Up System Database
- Backup Type **Complete Data Backup**
- Destination **File**
- Backup Destination **/swrepo/backup/data/SYSTEMDB** make sure that this directory structure exists and is writable with user **\${sid}adm**.
- Backup Prefix **COMPLETE_DATA_BACKUP_INITIAL_DDMMYYYY** Next
- **Review Backup Setup** and then select **Finish**

Make sure that the **SYSTEMDB@\${SID}** backup completes successfully.

Backup MDC

Backup & Recovery

- Backup Up Tenant Database
- Specify the Tenant Database **\${sid}**. Next
- Backup Type **Complete Data Backup**.
- Destination **File**.
- Backup Destination **/swrepo/backup/data/DB_\${sid}** make sure that this directory structure exists and is writable with user **\${sid}adm**.
- Backup Prefix **COMPLETE_DATA_BACKUP_INITIAL_DDMMYYYY**. Next
- **Review Backup Setup** and then select **Finish**.

Make sure that the backup of **DB_\${sid}** completes without errors.

Check backup status

On the SYSTEMDB entry, -> right click and select the following actions.

- Backup & Recovery
- Select Open **Backup Console**
- Select the tab **Backup Catalog**
- In the Database Field select **\${sid}** for the MDC
- In the Database Field select **<SYSTEMDB>** for the SYSTEMDB

Optional check of the trace log files

The database trace is written to service specific files on operating system level. The trace directory is in the following location:

```
/usr/sap/${sid}/HDB<inst>/<host>/trace/DB_${sid}/
```

The following alias in the environment of the **\${sid}adm** user allows to you quickly switch to the trace directory on the OS level:

```
cdtrace
```

The database trace files use the following naming convention:

```
<service>_<host>.<port>.<counter>.trc
```

In the context of dynamic tiering, a file with the following convention can exist (SAP Note 2871785):

```
eserver_console_<host>.<port>.<counter>.trc
```

- Example:

`indexserver_saphana01.30003.024.trc` You can access these files either directly on the operating system level or in one of the following ways:

- SAP HANA Studio -> Administration -> Diagnosis Files
- DBACOCKPIT -> Diagnostics -> Diagnosis Files

Migrating SAP S/4HANA by using SAP HANA System Replication

Pre-checks before you configure SAP HANA System Replication

Before you configure SAP HANA System Replication, a few prerequisites must be checked. The described Steps are valid for Red Hat Enterprise Linux 8 (RHEL) and SUSE Enterprise Linux (SLES).

Check the SAP HANA database user on the source system

Check with your SAP basis administration team or SAP HANA administrators, which SAP HANA database user is used to access the system. Typically this user the `SYSTEM` user, or the SAP schema owner user if your SAP basis administration team implemented the SAP security advisories.

SAP HANA landscape pre-steps for activating SAP HANA System Replication

Set the environment variables on the primary and secondary SAP HANA systems

To simplify the setup, prepare the following environment variables for `${sid}adm` on both nodes. These environment variables are used in subsequent commands in the remainder of the examples.

On both nodes, run the following commands. Remember that the variables must be the same on both systems, source and target.

```
export SID=<SID>                                # SAP HANA System ID (uppercase)
export sid=<sid>                                 # SAP HANA System ID (lowercase)
export INSTNO=<INSTNO>                            # SAP HANA Instance Number
export DIR_INSTANCE=/usr/sap/${SID}/HDB${INSTNO} # "${sid}adm" home directory

export SiteOnPrem=<PrimarySiteName>      # HANA System Replication Site Name 1 - Migration from On-Prem - Source
export SiteOnCloud=<secondarySiteName>     # HANA System Replication Site Name 2 - Migration to On-Cloud - Target

export NODE1=<Hostname 1>                      # Hostname of On-Prem Server
export NODE2=<Hostname 2>                      # Hostname of IBM Power Virtual Server Instance
```

Make sure that SAP HANA is running on both systems

As the operating system user `${sid}adm`, the command `HDB proc` can be used to verify that all services are started.

Run the following command on both systems, primary and secondary SAP HANA server.

```
$ sudo -i -u ${sid}adm -- HDB proc
```

SAP HANA version must be equal or greater than the primary server

Run the following command on each node to determine the SAP HANA server version.

```
$ sudo -i -u ${sid}adm -- HDB version
```

The target system version must be equal or larger compared with the source system version. The only exception for the version is for an `Active/Active` read enabled configuration, here the HDB version must be identical on source and target system.

- Therefore, make sure that the system configuration is identical on both the source and target servers. Then, compare the settings in the ini-files on both systems.

- For a scale-out configuration, make sure that the number of worker nodes (scale-out) and roles are identical on both the source and target servers.
- The same `${sid}` and `instance numbers` must be used on both systems.
- Back up `PKI SSFS .key and the .dat files` from the primary and secondary systems.
- Copy existing PKI keys from the primary to the secondary system.

To make sure that you can recover to the original installed state, if needed, back up the existing keys on both primary and secondary systems.

```
$ sudo -i -u ${sid}adm -- cp -p /usr/sap/${SID}/SYS/global/security/rsecssfs/data/SSFS_${SID}.DAT
/usr/sap/${SID}/SYS/global/security/rsecssfs/data/SSFS_${SID}.DAT_<hostname>
```

After the backup of the existing PKI SSFS `.key` and `.dat` files is done, you now need to copy the PKI SSFS `.key` and `.dat` files from primary system to the target system.

The SAP HANA 2.0 data and log transmission channels for the replication process require authentication by using the system `PKI SSFS` storage certificate files.

- [SAP Note 2369981 - Required configuration steps for authentication with HANA System Replication](#)

The system `PKI SSFS` storage certificate files are stored in `/usr/sap/${SID}/SYS/global/security/rsecssfs/` in subdirectories `data` and `key` .

On NODE2, run the following commands to copy files `SSFS_${SID}.DAT` and `SSFS_${SID}.KEY` from NODE1.

As `${sid}adm` user, run the following two commands on NODE2.

```
$ scp ${NODE1}::/usr/sap/${SID}/SYS/global/security/rsecssfs/data/SSFS_${SID}.DAT
/usr/sap/${SID}/SYS/global/security/rsecssfs/data/SSFS_${SID}.DAT
```

```
$ scp ${NODE1}::/usr/sap/${SID}/SYS/global/security/rsecssfs/key/SSFS_${SID}.KEY
/usr/sap/${SID}/SYS/global/security/rsecssfs/key/SSFS_${SID}.KEY
```

The copied `PKI SSFS` storage certificates on NODE2 become active during the start of the SAP HANA system.

Check that the configuration parameter `log_mode` is set to normal

Make sure that the configuration parameter `log_mode` is set to *normal* in the `persistence` section of the `global.ini` on both the primary and secondary SAP HANA Servers.

Run the following command on both systems to verify the `log_mode` setting.

```
$ sudo -i -u ${sid}adm -- grep -i 'log_mode' /usr/sap/${SID}/HDB${INSTNO}/exe/config/global.ini
```

The following output is expected.

```
log_mode=normal
```

Register the primary server first

On the primary SAP HANA system, run the following command to register this node as the `primary` for SAP HANA System Replication.

```
$ sudo -i -u ${sid}adm -- hdbnsutil -sr_enable --name=${SiteOnPrem}
```

The following output is expected.

```
nameserver is active, proceeding ...
successfully enabled system as system replication source site
done.
```

Check whether the primary system is registered

Verify that the primary system is successfully registered by using the following command.

```
$ sudo -i -u ${sid}adm -- hdbnsutil -sr_state
```

The following output is expected.

```
System Replication State
~~~~~
online: true

mode: primary
operation mode: primary
site id: 1
site name: SiteOnPrem

is source system: true
is secondary/consumer system: false
has secondaries/consumers attached: false
is a takeover active: false
is primary suspended: false

Host Mappings:
~~~~~

Site Mappings:
~~~~~
SiteCloud (primary/)

Tier of SiteCloud: 1

Replication mode of SiteCloud: primary

Operation mode of SiteOnPrem :

Hint based routing site:
done.
```

Make sure that SAP HANA is not active on the secondary site

The secondary site must not be an active SAP HANA server. Stop SAP HANA database services by using the following command.

```
$ sudo -i -u ${sid}adm -- HDB stop
```

The following output is expected.

```
hdbdaemon will wait maximal 300 seconds for NewDB services finishing.
Stopping instance using: /usr/sap/${SID}/SYS/exe/hdb/sapcontrol -prot NI_HTTP -nr 10 -function Stop 400

10.08.2023 10:32:07
Stop
OK
Waiting for stopped instance using: /usr/sap/${SID}/SYS/exe/hdb/sapcontrol -prot NI_HTTP -nr 10 -function
WaitforStopped 600 2

10.08.2023 10:32:51
WaitforStopped
OK
hdbdaemon is stopped.
```

Register the secondary system

Now register the secondary system.

```
sudo -i -u ${sid}adm -- hdbnsutil -sr_register \
--name=<secondarySiteName> \
```

```
--remoteHost=<primary_host> \
--remoteInstance=<primary_systemnr> \
--replicationMode=[sync|syncmem|async] \
--operationMode=[delta_datashipping|logreplay|logreplay_readaccess]
```

For example, if you use

- `SiteOnCloud` as the secondary site name
- `syncmem` as replication mode and
- `logreplay` as operation mode

The last command looks like the following example.

```
$ sudo -i -u ${sid}adm -- hdbnsutil -sr_register \
--name=${SiteOnCloud} \
--remoteHost=${NODE1} \
--remoteInstance=${INSTNO} \
--replicationMode=syncmem \
--operationMode=logreplay
```

The following output is expected.

```
Thu 10 Aug 10:36:13 CEST 2023
adding site ...
collecting information ...
updating local ini files ...
done.
```

Troubleshoot hdbnsutil errors with SELinux enabled

If security-enhanced Linux (SELinux) is enabled, the output of `hdbnsutil` is not as expected. You can see one of the following two symptoms.

- `Command is not recognized` error message
- Usage information displayed

SELinux, when set to `enforcing`, prevents the command `hdbnsutil` from restarting the saphostagent in the `${sid}adm` user context. You can either add proper SELinux security policies or as SAP recommends. Then, disable SELinux.

Check the current SELinux status with the following command.

```
$ sestatus
```

The following output is an example.

```
SELinux status:           enforcing
```

If `sestatus` command returns with `enforcing`, then commands even when run with root privileges can be blocked, depending on security policy.

To disable SELinux temporarily, run the following command.

```
$ sudo setenforce 0
```

SELinux is now temporarily disabled until the next restart.

Now check with `sestatus` again, the status shows `disabled`.

Check whether the saphostagent process is running with the following command.

```
$ sudo ps -ef | grep -i host
```

If output is empty and no process is displayed, manually restart the saphostagent.

```
$ sudo -i -u ${sid}adm -- /usr/sap/hostctrl/exe/saphostexec -restart /usr/sap/hostctrl/exe/host_profile
```

Check the state on both sides of the SAP HANA System Replication

Check the primary system state

Verify the system replication state on the primary node. Run the following command on the primary server:

```
$ sudo -i -u ${sid}adm -- hdbnsutil -sr_state
```

The following output is expected.

```
System Replication State
~~~~~
online: true

mode: primary
operation mode: primary
site id: 1
site name: SiteOnPrem_hostname

is source system: true
is secondary/consumer system: false
has secondaries/consumers attached: true
is a takeover active: false
is primary suspended: false

Host Mappings:
~~~~~

<SiteOnCloud_hostname> -> [SiteOnPrem_hostname] <SiteOnPrem_hostname_hostname>
<SiteOnCloud_hostname> -> [SiteOnCloud] <SiteOnPrem_hostname_hostname>

Site Mappings:
~~~~~
SiteOnPrem_hostname (primary/primary)
|---SiteOnCloud (syncmem/logreplay)

Tier of SiteCloud: 1
Tier of SiteOnPrem_hostname: 2

Replication mode of SiteOnPrem_hostname: primary
Replication mode of SiteOnCloud: syncmem

Operation mode of SiteOnPrem_hostname: primary
Operation mode of SiteOnCloud logreplay

Mapping: SiteOnPrem_hostname -> SiteOnCloud

Hint based routing site:
done.
```

Check the secondary system state

Now check the system replication state on the second node. Run the same command on the second server.

```
$ sudo -i -u ${sid}adm -- hdbnsutil -sr_state
```

The following output is expected.

```
System Replication State
~~~~~
online: false

mode: syncmem
operation mode: unknown
```

```
site id: 2
site name: SiteOnCloud

is source system: unknown
is secondary/consumer system: true
has secondaries/consumers attached: unknown
is a takeover active: false
is primary suspended: false
is timetravel enabled: false
replay mode: auto
active primary site: 1

primary masters: <SiteOnPrem_hostname_hostname>
done.
```

Restart the secondary server

So far both SAP HANA servers are configured as replication partners. Now restart the secondary SAP HANA server to complete the replication setup.

Run the following command on the secondary server.

```
$ sudo -i -u ${sid}adm -- HDB start
```

The following output is expected.

```
StartService
OK

Starting instance using: /usr/sap/${SID}/SYS/exe/hdb/sapcontrol -prot NI_HTTP -nr 10 -function StartWait 2700 2
OK

10.08.2023 10:38:47
Start
OK

10.08.2023 10:40:17
StartWait
OK
```

Check `HDB info` or `HDB proc` on the secondary side to confirm that SAP HANA is running again. When successful, run the `sr_state` command on the primary system.

```
$ sudo -i -u ${sid}adm -- hdbnsutil -sr_state
```

The following output is expected.

```
System Replication State
~~~~~

online: true

mode: primary
operation mode: primary
site id: 1
site name: SitePrem

is source system: true
is secondary/consumer system: false
has secondaries/consumers attached: true
is a takeover active: false
is primary suspended: false

Host Mappings:
~~~~~

<SiteOnCloud_hostname> -> [SiteOnPrem] <SiteOnPrem>
```

```
<SiteOnCloud_hostname> -> [SiteOnCloud] <SiteOnPrem>
```

```
Site Mappings:  
~~~~~  
SiteOnPrem (primary/primary)  
|---SiteOnCloud (syncmem/logreplay)  
  
Tier of SiteOnPrem : 1  
Tier of SiteOnCloud: 2  
  
Replication mode of SiteOnPrem: primary  
Replication mode of SiteOnCloud: syncmem  
  
Operation mode of SiteOnPrem: primary  
Operation mode of SiteOnCloud: logreplay  
  
Mapping: SiteOnPrem_hostname -> SiteOnCloud  
  
Hint based routing site:  
done.
```

Check replication status

After the secondary system is configured and SAP HANA is started on the secondary server, the replication process automatically starts synchronizing data with a **full replica**. You can verify the initial replication on the primary server and watch the current completion status of the full replication action.

Run the Python script with the following command.

```
$ sudo -i -u ${sid}adm -- python ${DIR_INSTANCE}/exe/python_support/systemReplicationStatus.py
```

The following output is expected.

```
|Database |Host      |Port    |Service Name |Volume ID |Site ID |Site Name |Secondary |Secondary |Secondary |Secondary | |
|Secondary |          |Replication |           |          |          |          |          |          |          |          |          |  
|          |          |          |          |          |          |          |          |          |          |          |  
|Active Status |Mode      |Status     |Status Details |Fully Synced | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|  
|SYSTEMDB |<NODE1> |31001 |nameserver |          |1 |          |1 |SiteOnPrem| <NODE2> |          |31001 |2  
|SiteOnCloud|YES |SYNCMEM |ACTIVE    |          |   |          |   |          |          |          |          |  
|S4H     |<NODE1> |31007 |xsengine  |          |2 |          |1 |SiteOnPrem| <NODE2> |          |31007 |2  
|SiteOnCloud|YES |SYNCMEM |ACTIVE    |          |   |          |   |          |          |          |          |  
|S4H     |<NODE1> |31040 |docstore  |          |5 |          |1 |SiteOnPrem| <NODE2> |          |31040 |2  
|SiteOnCloud|YES |SYNCMEM |ACTIVE    |          |   |          |   |          |          |          |          |  
|S4H     |<NODE1> |31003 |indexserver |          |3 |          |1 |SiteOnPrem| <NODE2> |          |31003 |2  
|SiteOnCloud|YES |SYNCMEM |ACTIVE    |          |   |          |   |          |          |          |          |  
|S4H     |<NODE1> |31011 |dpserver  |          |4 |          |1 |SiteOnPrem| <NODE2> |          |31011 |2  
|SiteOnCloud|YES |SYNCMEM |ACTIVE    |          |   |          |   |          |          |          |          |  
  
status system replication site "1": ACTIVE  
overall system replication status: ACTIVE  
  
Local System Replication State  
~~~~~  
mode: PRIMARY  
site id: 1  
site name: SiteOnPrem_hostname
```

Four methods to check the system replication status

Option 1. `landscapeHostConfiguration.py`

The first option uses the Python script `landscapeHostConfiguration.py` for a server point of view. This script displays a status line per SAP HANA server system.

Run the following command.

```
$ sudo -i -u ${sid}adm -- python ${DIR_INSTANCE}/exe/python_support/landscapeHostConfiguration.py
```

Make sure that each server that is listed in the output shows **OK** in the host status column.

Option 2. systemReplicationStatus.py

The second alternative option uses the Python script **systemReplicationStatus.py** for a database view of the SAP HANA system replication. This script displays one status line for each database and an overall status after the database table.

Run the Python script with the following command.

```
$ sudo -i -u ${sid}adm -- python ${DIR_INSTANCE}/exe/python_support/systemReplicationStatus.py
```

Make sure that each database listed shows an **ACTIVE** in replication status column. The expected script output contains the following line:

```
overall system replication status: ACTIVE
```

Option 3. hdbcons

Check the detailed status of the system replication with the **hdbcons** command and run as **\${sid}adm** user. This third option is a technical per server and per service view.

Run the SAP HANA DB Management Client Console **hdbcons** with the following command.

```
$ sudo -i -u ${sid}adm -- hdbcons -e hdbindexserver "replication info"
```

Option 4. SQL script

The fourth alternative uses an SQL statement that can be run, for example, in SAP HANA studio or cockpit. This option is a hosts-per-site-view of SAP HANA system replication.

Check by running the following SQL statement.

```
$ select host, SECONDARY_HOST, PORT, SITE_NAME, SECONDARY_SITE_NAME, REPLICATION_MODE, REPLICATION_STATUS, REPLICATION_STATUS_DETAILS, SECONDARY_ACTIVE_STATUS from M_SERVICE_REPLICATION;
```

Check especially columns **REPLICATION_STATUS** and **REPLICATION_STATUS_DETAILS** in the SQL output.

Post replication completion

Before you disable the replication setup, check the trace logs for any inconsistencies or anomalies after the replication action is performed. After the replication completes, the database contains all active services on the primary system only. But you can still examine the trace logs for any inconsistencies or issues.

Checking the database trace files

The database trace is written to service specific files on operating system level. The trace directory is located here:

```
/usr/sap/<SID>/HDB<inst>/<host>/trace/DB_<SID>/
```

The following alias in the **`\${sid}adm** user environment allows the **`\${sid}adm** user to quickly change to the trace directory on the operating system level:

```
$ cdtrace
```

The database trace files have the following naming convention: **<service>_<host>. <port>. <counter>. trc**

In the context of dynamic tiering also a file with the following convention can exist (SAP Note 2871785): **esserver_console_<host>. <port>. <counter>. trc**

Example: **indexserver_saphana01.30003.024.trc**

You can access database trace files in three ways:

- Directly on the operating system level
- SAP HANA Studio -> Administration -> Diagnosis Files

SAP HANA System Replication resources

For more information, see the following links:

- [SAP Note 1999880 - HANA System Replication FAQ](#)
- [SAP Note 11969700 - SQL Statement Collection for SAP HANA](#)
- [SAP Note 3357978 - Configuring SAP HANA Multi Target System Replication](#)
- [SAP HANA Replication Setups](#)
- [SAP HANA System Replication](#)
- [SAP HANA multitarget System Replication](#)
- [SAP HANA System Replication](#)
- [SAP Help Portal Documentation HSR HANA 2.0 SP07](#)

Migrating SAP ERP 6.0 with Oracle to IBM Power Virtual Server

Preparation steps on the source system

Target audience and intent

This documentation presents Oracle Database Administrators (DBA's) with two options, both based on Oracle RMAN to migrate AIX-based Oracle databases from IBM Power to IBM Power Virtual Server (IBM Power Virtual Server).

The target audience consists of solution and infrastructure architects and Oracle database administrators.

The intent is to present representative steps to execute plans and procedures to perform Oracle database migrations, recognizing that each migration scenario presents unique challenges in terms of deployment, configuration, and available resources.

In this documentation, the generic term *Discovery* indicates that the customers own Oracle DBA's responsibility to *Discover* and *document* their current Oracle/SAP infrastructure. This is useful should the customer have the need to raise incidents to report issues.

Scope and coverage

All following procedures require network connectivity between the source and the target system, and a sufficient network bandwidth for the data transfer and/or data replication.

A discussion of alternative procedures by using the optional mobile or container solutions such as *Seagate Lyve Mobile Solution* in combination with IBM Cloud Object Storage or *IBM Aspera Connect* to transfer on-premises backups/database files to IBM Power Virtual Server infrastructure is interspersed. Links to detailed information about this service may be found in the IBM Cloud online documentation or in the following links.

- [Seagate Lyve Mobile Solution](#)
- [Getting started with IBM Cloud Object Storage](#)
- [IBM Aspera Connect](#)

Task steps that are required vary per implementation. Refer to cited Oracle documentation for details regarding the execution of specific commands.

For this migration procedure we use User Concept - Oracle Standard as outlined in the following documented SAP Link.

Note that an SAP S-user access is required to access SAP Notes:

- [SAP Note 1915323 - OS User Concept for SAP NetWeaver for 12c and higher](#)

Disclaimer

Any attempt to execute these procedures will be performed in context with Customer's established procedures for operating and maintaining nonproduction and/or production systems. Customer takes customary actions to ensure system availability for maintenance and/or reconfiguration as required, and schedule downtime as required.

The Customer is responsible for reviewing these representative procedures in the context of their particular environment and adjusting as required.

The Oracle Database migration options that are described are not necessarily specific to IBM Power Virtual Server migrations. Oracle technical experts should recognize the procedures that are used, and understand that not every technical detail or consideration have been explicitly

identified. The Oracle Database Admins executing the procedures are expected to understand the full scope of Oracle database backup and recovery methods - including those details that are not explicitly stated.

System discovery and selection of the migration option

System discovery process

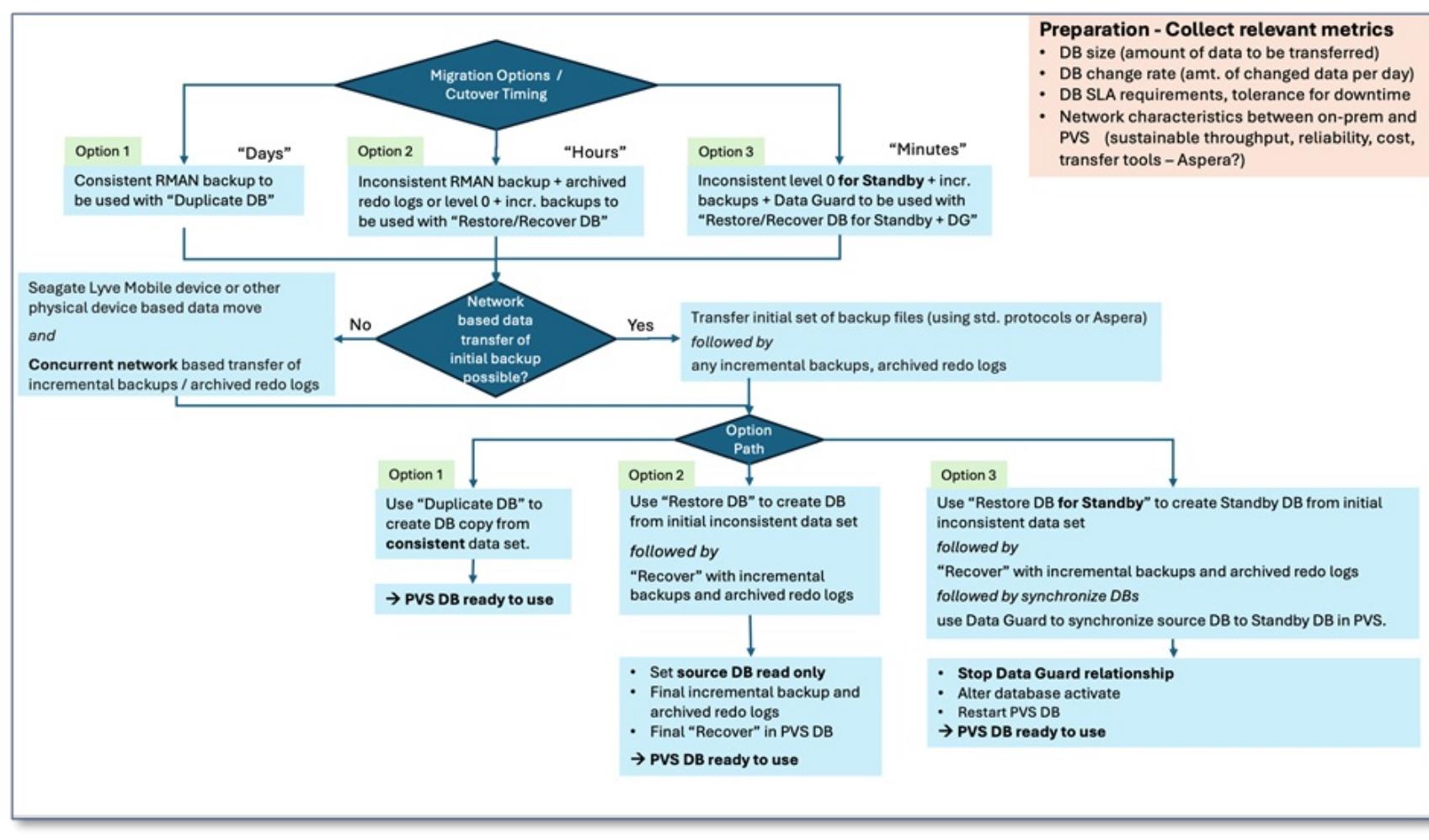
This document assumes that a detailed discovery has been previously collected:

- Business, technical, functional, nonfunctional requirements of the Oracle database being migrated (including access and availability requirements)
- Installation configuration, HW/SW inventory, and sizing information related to the source database and the underlying platform.
 - Collect relevant metrics related to sizing, change rate, service level requirements, tolerance for migration downtime, capacity of networks to support data transfer from source to target, and so on.
 - The target environment has been evaluated and deployed consistent with source system capacity/performance/availability as found in the discovery process.

Migration options covered by this document

The following flowchart illustrates the three options that are covered in this document:

- *Option 1*: Consistent RMAN backup from source, with generated files to be used by the RMAN Duplicate Database procedure to restore to IBM Power Virtual Server.
- *Option 2*: Inconsistent RMAN backup + archived redo logs (or level 0 + incremental backups) from source, with backup files to be used by the RMAN Restore/Recover Database procedure to restore to IBM Power Virtual Server.
- *Option 3*: Leveraging Oracle Data Guard, currently being researched and will be the recommended method if it is the same platform – create a mirror and as soon as it is in sync you can switchover with just minutes of database downtime. The online documentation will be updated as soon as the testing and assessment phases have been completed.



Selecting the migration option

Customer requirements and technical conditions affect the decision to select from the presented options.

1. Service Level Requirements, particularly the Restore Point Objectives (RPO) and Restore Time Objectives (RTO).
 - *Option 1*: As presented assumes that the Customer is comfortable with a considerable service delay (RTO = "Days") before the source database is migrated to the target database. This expectation is often the case for nonproduction workloads but rarely for production databases.
 - *Option 2*: As presented assumes that the Customer is comfortable with a service interruption in terms of "Hours". This expectation is often the case for nonproduction workloads and some production databases.

- *Option 3:* (Not yet presented in this document), incorporating Oracle Data Guard database synchronization, features a potential cutover of service from source to target in minutes.
2. Database Size, Network Throughput and Reliability.
 - Transporting backups of a large database across a network takes time. Consider the following transfer example of 600 GB of backups across an end-to-end network connection where available protocols and bandwidth support 80 megabytes/second throughput. At this rate, it takes roughly 125 minutes to transfer the data. If the database backups are much bigger or if the network connection throughput is less, more transfer time is required. Unreliable networks can disrupt the transfer, requiring you to restart the transfer process, incurring delay.
 - Customers can benefit from specialized transfer tools that compress data before/during transfer, use high-throughput protocols and decompress data after transfer.
 - Access to IBM's Aspera, which can greatly accelerate data transfers from on-premises to IBM Power Virtual Server locations is advantageous.
 3. Availability of Skills to Execute.
 - Options that are provided in this document require experienced Database Administrator skills and the ability to work with infrastructure teams to migrate database content to a new target database on Power Virtual Server within an IBM Power Virtual Server workspace.

Any migration procedures a Customer elects to use need be executed in the context of a detailed, well-rehearsed transfer and cutover plan.

Considerations and technical details for the backup

The RMAN BACKUP command supports backing up the following types of files:

1. Data files and control files.
2. Server parameter file.
3. Archived redo logs
4. RMAN backups

 **Important:** RMAN does not back up these files that are associated with the Oracle database.

Although the database depends on other types of files, such as network configuration files, password files, and the contents of the Oracle home, you cannot back up these files with RMAN. Likewise, some features of Oracle Database, such as external tables, might depend upon files other than the data files, control files, and redo log. Also needed for this procedure is a parameter file from the source database, as well as the files listed that follow:

1. Oracle database parameter file: `init<SID>.ora`
2. TNS network configuration files: (e.g. `listener.ora`, `tnsnames.ora`)
3. Oracle database password file, if this file exists

RMAN does not back up these files. So you need to make sure that these are included on your backup/recovery action, best practice would be to copy those to a directory on the same mount as the RMAN database backups.

When you execute the BACKUP command in RMAN, the output is always either one or more backup sets or one or more image copies. A backup set is an RMAN-specific proprietary format, whereas an image copy is a bit-for-bit copy of a file. By default, RMAN creates backup sets. This document only deals with backup sets.

- [Backup set explanation](#)
- [Image Copy explanation](#)

Assumptions

This document assumes that:

1. If the source database is a production system it likely won't be shut down for a full backup, in which case RMAN incremental backups will be used.
2. No changes to the source database (schema and configuration) are expected by executing this procedure.
3. Database is migrated from source to target by using Oracle RMAN options: Duplicate database, or backup/restore/recover database.
4. The target environment has Oracle homes pre-installed with a version matching the source instance being migrated.
5. RMAN duplicate, restore/recovery provide the option to modify the database data file location, but this option is not covered in this document. The assumption is made that the location of database files, either AIX JFS2 file systems or Oracle ASM disk groups, is

identical between the source and the target environment.

6. The target OS is either:

- An exact copy (an OVA or “Open Virtual Appliance” archive file) of the source operating system generated by using an mksysb procedure, or
- A freshly deployed version of AIX that is supported by IBM and certified by Oracle to support the version of Oracle to be instantiated.

Documentation of an mksysb procedure might be found at:

- [Restoring AIX](#)

Preparation

Discovery has confirmed or identified the following preparation steps.

Document the source database size and configuration

Document current sizing and performance metrics related to compute, IOPS, and storage, of one or more source Oracle instances.

- The target IBM Power Virtual Server Oracle instance should be constructed to at least match the sizing of the existing system.
- Very important on the target system to select disk tier and disk capacity to meet IOPS requirements.
- This discovery process should include execution of a performance test tool against the source database to capture metrics for future reference and comparison to target system deployment.

Provide a recent and successful backup of the source database

Confirm, by using your standard backup tools, that a recent, successful, full backup of the source Oracle system exists. You must be able to completely restore the source system.

- If you cannot confirm it, the migration/discovery team should review RMAN backup procedures.
- In addition, the discovery team should work with customer DBA's or SMEs to validate database integrity and/or identify any existing corrupt blocks or schema problems.

Document the source database

Document the location of source database instances and known credentials for DBA administration access.

Document the RMAN configuration

Document the current Oracle Recovery Manager (RMAN) configuration that is used to perform backups, per instance.

A simple way to obtain this information is by performing the following steps:

Use ssh to connect to the Oracle server.

```
$ ssh oracle@<hostname>
```

Check the variable `$ORACLE_SID` is set.

```
$ echo $ORACLE_SID
```

Usually the SID value is shown. If the last command does not show a value, set the environment variable manually with this command:

```
$ setenv ORACLE_SID <SID value>
```



Note: Replace `<SID value>` with your SID value.

Connect to the source database by using the `rman` command:

```
$ rman target /
```

A typical output looks like this:

```
Recovery Manager: Release 19.0.0.0.0 - Production on Thu May 2 13:24:05 2024
Version 19.22.0.0.0
```

```
Copyright (c) 1982, 2019, Oracle and/or its affiliates. All rights reserved.
connected to target database: Exx (DBID=xxxxxxxx)
```

Display the RMAN configuration settings by using:

```
RMAN> SHOW ALL;
```

Store and/or document output.

Exit the RMAN session by typing:

```
RMAN > exit;
```

Just for your reference, a typical `SHOW ALL` output looks like this:

```
using target database control file instead of recovery catalog
RMAN configuration parameters for database with db_unique_name EXX are:
CONFIGURE RETENTION POLICY TO REDUNDANCY 1; # default
CONFIGURE BACKUP OPTIMIZATION OFF; # default
CONFIGURE DEFAULT DEVICE TYPE TO DISK; # default
CONFIGURE CONTROLFILE AUTOBACKUP ON; # default
CONFIGURE CONTROLFILE AUTOBACKUP FORMAT FOR DEVICE TYPE DISK TO '%F'; # default
CONFIGURE DEVICE TYPE DISK PARALLELISM 8 BACKUP TYPE TO BACKUPSET; # default
CONFIGURE DATAFILE BACKUP COPIES FOR DEVICE TYPE DISK TO 1; # default
CONFIGURE ARCHIVELOG BACKUP COPIES FOR DEVICE TYPE DISK TO 1; # default
CONFIGURE MAXSETSIZE TO UNLIMITED; # default
CONFIGURE ENCRYPTION FOR DATABASE OFF; # default
CONFIGURE ENCRYPTION ALGORITHM 'AES128'; # default
CONFIGURE COMPRESSION ALGORITHM 'BASIC' AS OF RELEASE 'DEFAULT' OPTIMIZE FOR LOAD TRUE ; # default
CONFIGURE RMAN OUTPUT TO KEEP FOR 7 DAYS; # default
CONFIGURE ARCHIVELOG DELETION POLICY TO NONE; # default
CONFIGURE SNAPSHOT CONTROLFILE NAME TO '/oracle/EXX/19/dbs/snapcf_EXX.f'; # default
```

Verify disk space

Confirm that enough disk space is available, formatted, and mounted to accept the compressed *migration* database backup sets.

- Best performance is obtained if the disk space is local to the instance being backed up.
- Backing up database directly to Cloud Object Storage can introduce delays in backup execution due to comparative slowness of the network.
- This procedure will perform a backup, applying medium compression with the following considerations:
 - Compression results in backup file storage that takes approximately 25% of the space that is consumed by the Oracle database.
 - Local file system capacity should be sufficient to store the entire backup set (or sets) required to bring the target database to the restore point desired.
 - Target system requires access to the backup sets, via one of the following options:
 - A local filesystem to which the backup sets will be copied.
 - Installation of Aspera Agent on the on-premises landscape,
 - An NFS direct mount to the Cloud Object Storage device or if using a Seagate Lyve Mobile transfer device. This does not yield the best performance and there have been other observations in the past.



Note: Depending on network/access speed, it can be desirable to copy files from NFS mount to local storage.

File system for backup sets on source

A dedicated local file system e. g. `/backup/rman` for the migration backup sets is referenced. As an alternative option, a direct restore/recovery from the NFS-mounted Seagate Lyve Mobile device was also successfully tested using 10GbE and 100 GbE.

Perform the following commands to confirm available space for backups:

```
$ df -g /backup/rman
```

File system for backup sets on target

The database duplication or restore/recover procedures require access to the set of backup files, via one of the following options:

- A local filesystem to which the backup sets will be copied.
- An NFS mounted to a Seagate Lyve Mobile transfer device, or
- An NFS mounted to IBM Cloud Object Storage to which the backup files have already been copied from the Seagate device.

Back up the source Oracle database by using RMAN

In this section, we cover the generation of the RMAN backup set presenting two options.

Reference

For more details, consult this document: [Oracle Database Backup and Recovery - February 2024](#).

Assumptions

- *Option 1* procedure assumes that a consistent *offline backup* will be taken of the source database.
- *Option 2* procedure requires that the source database is in *ARCHIVELOG* mode before the backup procedure is performed.

Considerations

Customer should balance how parallelism and/or compression is applied (and associated resources that are allocated to support) with requirements for database availability and performance while backups are being performed.

Consider applying *section size* to the backup configuration. Without specifying `section size`, only a small number of huge backup files are created. Large files can be difficult to handle and will be a challenge during data transfer, when a restart is required due to transfer failures. Additionally a few number of backup files limits the number of concurrent processes when restoring data to the target database with parallelism.

Specifying a `good section size` enables control of backup file sizes and at the same time also influence how many files are generated which can then be processed in parallel during restore in IBM Power Virtual Server.

Note that Medium compression requires the Oracle Advanced Compression License. Basic compression is *good*, but significantly slower and achieves lower compression rates. High compression is VERY CPU intensive on the compression side and provides limited compression benefit as compared to Medium only. High compression also requires the Advanced Compression License.

Incremental backup, without database block change tracking activated, performs a full scan of all data files, which translates into a high reading workload. Although enabling block change tracking is not expected to impact the performance of a running DB, testing should be performed in the Customer environment to validate this.

Network transfer comparison between standard protocols and IBM Aspera

A slower version of data transfer is using standard protocols such as scp/sftp. Backup files can be transferred either directly to an IBM AIX LPAR in Power Virtual Server, or to IBM Cloud Object Storage (COS). Using scp/sftp with IBM COS assumes that you are using an IBM FileManager Gateway service or have installed and configured a sftp server within or next to the target IBM Power Virtual Server environment to receive the transfer.

The faster option is using IBM's high-performance Aspera product for data transfer. In many situations, IBM Aspera has been shown to transfer data several times faster than traditional TCP-based protocols.

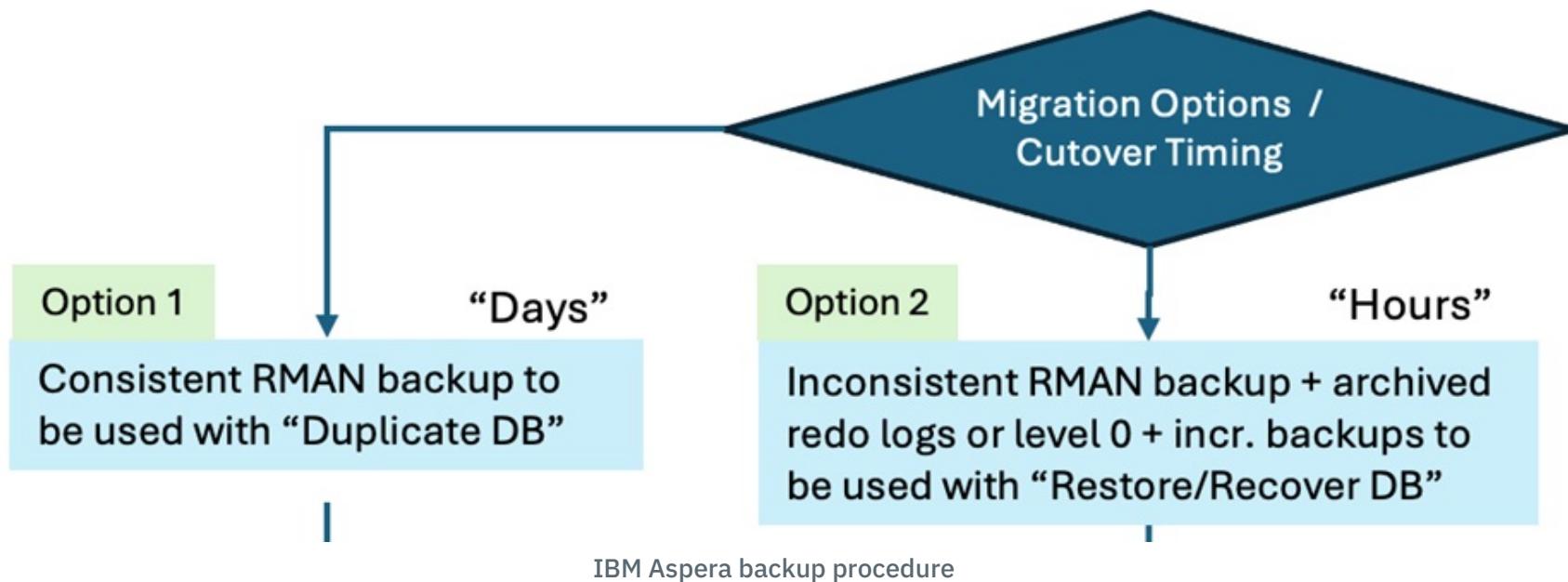
Documentation for IBM Aspera can be found here:

[IBM Aspera Technologies - IBM Cloud](#)



Tip: This reference also contains the [Accelerated network transfer migration guide](#).

Backup procedure options



Procedures specific to both options are presented now.

RMAN option 1 - Offline backup / duplicate database

The following procedure is executed with the database offline and will produce a full consistent backup.

Application and database shutdown

Use standard operational procedures to shut down the SAP system and the Oracle database before performing the backup procedure.

When using the multitenant architecture, you must connect to the root container database (CDB) and the backups include the pluggable databases (PDBs).

More information can be found in:

- [About Performing Operations on CDBs and PDBs.](#)

Ensure that RMAN configuration is documented

As described in the preparation section [Document RMAN Configuration](#), be sure to save or document the current RMAN configuration and associated parameters, before modifying them.

The original RMAN configuration and parameters will be required again to continue with normal scheduled backup operations, after the special backup for migration was completed.

Backup option 1 - Create target directory

Login as the `oracle` user and execute the following commands to create the target backup directory to match the backup script that is described in the next section.

If the directory does not exist the RMAN script fails. Also if using an NFS mount, you need to make sure that the `oracle` user has the correct permissions in the definition file `exports` on the NFS server. The `oracle` user requires read and write (`rw`) permissions. Preferably using NFS is not advisable for the RMAN backup process. Using JFS2 or a locally mounted filesystem achieves better results.

The following two commands create the backup target location and set the environment variable `ORACLE_SID` to the `<SID>`. Replace the term `<SID>` with the correct value for your system:

```
$ mkdir -p /backup/rman/<sid>_option1
```

```
$ setenv ORACLE_SID <SID>
```

You can of course use any target location as long as the oracle user can write to it and you modify the backup script from the next step to use your target directory.

Backup option 1 - Backup script

The RMAN script is used to perform the backup option 1. The commands used in this script are discussed after the script. Copy and paste the script and make the necessary adjustments for your environment.

All RMAN settings and commands are contained in the `option1_backup.rman` script file:

```

connect target /
SHUTDOWN IMMEDIATE
STARTUP MOUNT
CONFIGURE CHANNEL DEVICE TYPE DISK FORMAT '/backup/rman/<sid>_option1/option1_cmp_%d_%U';
CONFIGURE DEVICE TYPE DISK PARALLELISM 60;
CONFIGURE CONTROLFILE AUTOBACKUP ON;
CONFIGURE CONTROLFILE AUTOBACKUP FORMAT FOR DEVICE TYPE DISK TO '/backup/rman/<sid>_option1/option1_cf_%F';
CONFIGURE COMPRESSION ALGORITHM 'HIGH';
CONFIGURE ENCRYPTION FOR DATABASE ON ;
CONFIGURE ENCRYPTION ALGORITHM 'AES256' ;
SET ENCRYPTION ON IDENTIFIED BY passw0rd ONLY ;
BACKUP AS compressed BACKUPSET section size 6000M DEVICE TYPE DISK DATABASE TAG <YOUR TAG ID HERE> include current
controlfile ;
alter database open;
quit;

```

Execute this script from the command line by using the `oracle` user.

```
$ rman @option1_backup.rman
```

RMAN backs up data to the configured default device for the type of backup requested. By default, RMAN creates backups on disk. If a fast recovery area is enabled, and if you do not specify the FORMAT parameter, then RMAN creates backups in the recovery area and automatically gives them unique names. This is the reason for modifying FORMAT in the parameters before this and is repeated here for emphasis.

The following are the main components of the RMAN script used:

Database shutdown and start in mount mode

The database must be cleanly shut down and then started in “mount mode” for the offline backup option 1. To ensure that the backup is consistent, the database must not be open. Database shutdown + mount mode is accomplished by these two lines:

```

SHUTDOWN IMMEDIATE
STARTUP MOUNT

```

Backup control file

The database control file contains the RMAN catalog that is required to restore the backup pieces into a functioning database.

This command includes the control file into the backup:

```

$ CONFIGURE CONTROLFILE AUTOBACKUP ON
BACKUP AS compressed BACKUPSET section size 6000M DEVICE TYPE DISK DATABASE TAG EXX_100K_INITV3 include current
controlfile ;

```

Note that the `CONFIGURE CHANNEL DEVICE TYPE DISK` and `CONFIGURE CONTROLFILE AUTOBACKUP FORMAT` for `DEVICE TYPE DISK` commands in the previous mentioned script include the backup file system location!

Backup parallelism

Set disk device parallelism - likely to speed up the backup and to reduce the backup time window. The optimal parallelism depends on several factors:

- Availability of CPU resources to run that many concurrent backup processes. With the selected compression and encryption each RMAN process typically uses all CPU cycles of a logical processor, assuming the storage subsystem can provide the data fast enough.
- Capability of storage subsystem to support the RMAN data file read and the write to backup location I/O throughput.
- Amount of free physical memory to support the backup processes to read, compress, encrypt the data.
- Parallelism 60 was used in our testing as shown in the RMAN script mentioned previously, but a parallelism of 8, as shown now, maybe a good starting point to find an optimal level during discovery:

```
CONFIGURE DEVICE TYPE DISK PARALLELISM 8 BACKUP TYPE TO BACKUPSET;
```

Backup compression

Set backup file compression. MEDIUM compression is advised for most customers. However HIGH compression has been tested also, as HIGH could be an option under certain circumstances. The use of 'MEDIUM' and 'HIGH' requires the Oracle Advanced Compression license!

- **Tested** `CONFIGURE COMPRESSION ALGORITHM 'HIGH' ;`

- Advised preventing license cost increase `CONFIGURE COMPRESSION ALGORITHM 'MEDIUM' ;`

Backup encryption

Set backup encryption on and modify the algorithm if desired (the default is AES128) and specify the encryption password to be used. Unless you are working with a TDE-encrypted database, every RMAN session requires the setting of the encryption and decryption password; otherwise, the session fails with a "wallet not open" error:

```
CONFIGURE ENCRYPTION FOR DATABASE ON ;
CONFIGURE ENCRYPTION ALGORITHM 'AES256' ;
SET ENCRYPTION ON IDENTIFIED BY passw0rd ONLY ;
```

Backup

The final command then triggers the actual backup of the database to disk. The backup uses the RMAN-specific backup sets. Each RMAN process reads up to 6000M of consecutive data from a data file as a backup piece, compress and encrypt that data and then write it to the destination file system.

The last action is to alter the database to open. Create a specific tag, including the `ORACLE_SID <SID>`, for identification purposes. Set the `section size` to limit the size of a backup part to improve potentially required retransmits if a file transfer to the destination environment fails. Using a TAG is recommended as it simplifies the management of multiple backups in an RMAN catalog:

```
BACKUP AS compressed BACKUPSET section size 6000M DEVICE TYPE DISK DATABASE TAG <SID>_100K_INITV3 include current
controlfile ;
alter database open;
```

Backup validation and cross check

When the backup is complete, use some of the following RMAN commands to validate and cross-check the results.

On the RMAN prompt, use these commands:

```
RMAN> REPORT SCHEMA;
RMAN> LIST BACKUP SUMMARY;
RMAN> BACKUP VALIDATE CHECK LOGICAL DATABASE ARCHIVELOG ALL;
RMAN> VALIDATE DATAFILE 10;
RMAN> VALIDATE BACKUPSET 3;
RMAN> CROSSCHECK BACKUP;
```

Explanation of commands:

- `REPORT SCHEMA` ; - Lists and displays information about the database files, tablespaces and so on.
- `LIST BACKUP SUMMARY` ; - Lists all existing backups. A SUMMARY option can be used.
- `LIST BACKUP <TAG ID>` ; - List a specific backup by TAG ID.
- `BACKUP VALIDATE CHECK LOGICAL DATABASE ARCHIVELOG ALL`; - Validate the contents of backup files.
- `VALIDATE DATAFILE 10`; - Validate a specific datafile.
- `VALIDATE BACKUPSET 3`; - Validate a specific backupset.
- `CROSSCHECK BACKUP`; - Synchronize the physical reality of backups and copies with their logical records in the RMAN repository.

Create PFILE

Create a plain text database parameter file (PFILE) from the binary server parameter file (SPFILE) as follows. The database remains in mounted mode. Remember to use your `<SID>` in the command.

Execute this command as user `oracle` :

```
$ export ORACLE_SID=<SID>
sqlplus "/ as sysdba";
```

Inside SQL*Plus create the parameter file:

```
SQL> create pfile='/backup/rman/init<SID>.ora' from spfile;
```

Be sure to restore all RMAN parameters back to original discovery settings when done.

For this *Option 1* we have created ONE backup to be transferred to and restored on the target system. At this point, to be consistent with a migration scenario, the source database should be shut down and not used any longer.

RMAN option 2 - Online backups

The following backup procedure is executed with the database online, and will produce a single RMAN Level 0 and one or more Level 1 (incremental) backups. It is required that the databases be in *archive log mode* and that it is ensured that all required archived *redo logs* are included in the backups.

An RMAN Incremental *Level 0* backup is a full backup. It includes the complete database.

An RMAN Incremental *Level 1* backup is an incremental backup, capturing the changes since the previous Level 0 or Level 1 backup. The **cumulative** option changes this behavior, consult Oracle RMAN backup concepts documentation for more details.



Note: The full backup (level 0) and all incremental backups (level 1) since the last full backup including the archived redo logs are required to restore and recover the database successfully. When moving the database to a new server - which includes ending services on the source system, the last incremental backup is an offline backup.

When using the *multitenant architecture*, you must connect to the root container database (CDB) and the backups include the pluggable databases (PDBs).

More information can be found in: [Performing Operations on CDBs/PDBs](#)

Check database size

Remember to make sure that you have enough space that is allocated on the filesystem to be able to back up the database. Use the following SQL statement to determine the current database size:

```
$ SELECT SUM (bytes)/1024/1024/1024 AS GB FROM dba_segments;
```

Ensure that RMAN configuration is documented

As described in the preparation section [Document RMAN Configuration](#), be sure to record current RMAN configuration and associated parameters. After completing special backups for migration, you want to ensure RMAN configuration is left as before so normally scheduled backup operations continue.

Backup option 2 - Create target directories

Execute the following commands as the **oracle** user.

The first two commands create the target backup directories for full and incremental backups. If you use a different directory, adapt the two backup scripts in the next section. The third command sets the environment variable **ORACLE_SID**, replace the term **<SID>** with the appropriate SID value of your system:

```
$ mkdir -p /backup/rman/<sid>_option2
mkdir -p /backup/rman/<sid>_option2_inc1

setenv ORACLE_SID <SID>
```

Backup option 2 - Backup scripts

Full online backup - level 0

The first RMAN script **option2_backup_full.rman** configures the RMAN environment and creates the initial level 0 (full) online backup. The key command to start the full (level 0) backup in this script is: **BACKUP ... incremental level 0 ...**

Commands that are used in this script are discussed further into this procedure after the script. Remember to replace the **<sid/SID>** entries to match your directory structure and system value:

All RMAN settings and commands for a full backup are contained in the **option2_backup_full.rman** script file:

```
connect target /
CONFIGURE CHANNEL DEVICE TYPE DISK FORMAT '/backup/rman/<sid>_option2/lev0_%d_%U';
CONFIGURE BACKUP OPTIMIZATION ON;
CONFIGURE DEVICE TYPE DISK PARALLELISM 60;
CONFIGURE CONTROLFILE AUTOBACKUP ON;
CONFIGURE CONTROLFILE AUTOBACKUP FORMAT FOR DEVICE TYPE DISK TO '/backup/rman/<sid>_option2/lev0_cf_%F';
CONFIGURE COMPRESSION ALGORITHM 'MEDIUM';
```

```
CONFIGURE ENCRYPTION FOR DATABASE ON ;
CONFIGURE ENCRYPTION ALGORITHM 'AES256' ;
SET ENCRYPTION ON IDENTIFIED BY passw0rd ONLY ;
BACKUP tag '<Your TAG Here>' incremental level 0 AS compressed BACKUPSET section size 6000M DEVICE TYPE DISK DATABASE
INCLUDE CURRENT CONTROLFILE PLUS ARCHIVELOG;
quit;
```

You can call the script directly from the command line that uses user `oracle` and:

```
$ rman @option2_backup_level0.rman
```

After running the full (level 0) backup, the expected result should be:

```
Recovery Manager complete.
```

RMAN backs up data to the configured default device for the type of backup requested. By default, RMAN creates backups on disk. If a fast recovery area is enabled, and if you do not specify the FORMAT parameter, then RMAN creates backups in the recovery area and automatically gives them unique names. This is the reason for modifying FORMAT in the parameters before this and is repeated here for emphasis.

`RMAN` by default includes ALL archived redo logs in a level 0 or level 1 backup if the `PLUS ARCHIVELOG` flag is specified. This can result in many duplicates of the same file within a consecutive set of incremental backups.

The following directive instructs RMAN to check whether a specific archived redo log was already included in a previous backup and, if yes, do not include the file in a new incremental backup.

If yes, do not include the file in a new incremental backup. Note that this option should NOT be used if other backups are taken of the database that are not to be transferred to the destination, then this option should be set to `OFF`.

```
CONFIGURE BACKUP OPTIMIZATION ON;
```

Restoring the database requires a copy of the database control file as it contains the RMAN catalog that is required to restore the backup pieces into a functioning database.

```
CONFIGURE CONTROLFILE AUTOBACKUP ON;
```

```
BACKUP AS compressed BACKUPSET section size 6000M DEVICE TYPE DISK DATABASE PLUS ARCHIVELOG TAG ECOM_option1 include
current controlfile;
```

Note that the script also contains `CONFIGURE CHANNEL DEVICE TYPE DISK` and `CONFIGURE CONTROLFILE AUTOBACKUP FORMAT for DEVICE TYPE DISK TO <directory>` commands, which define the backup type and file system location.

Set disk device parallelism - likely to speed up the backup and to reduce the backup window.

The optimal parallelism depends on several factors:

- Availability of CPU resources to run many concurrent backup processes. With the selected compression and encryption each RMAN process typically uses all CPU cycles of a logical processor, assuming the storage subsystem can provide the data fast enough.
- Capability of storage subsystem to support the RMAN data file read and write to backup location I/O throughput.
- Amount of free physical memory to support the backup processes to read, compress, encrypt the data.
- Size of the database.

Parallelism 60 was used in our testing as shown in the RMAN script previously mentioned, but a parallelism of 8, as shown here, maybe a good starting point to find an optimal level during discovery.

```
CONFIGURE DEVICE TYPE DISK PARALLELISM 8 BACKUP TYPE TO BACKUPSET;
```

Set backup file compression. MEDIUM is shown, HIGH could be an option under certain circumstances. The use of 'MEDIUM' and 'HIGH' requires the `Oracle Advanced Compression license` !

```
CONFIGURE COMPRESSION ALGORITHM 'MEDIUM' ;
```

Set backup encryption on and modify the algorithm if desired (the default is AES128) and specify the encryption password to be used. Unless you are working with a TDE-encrypted database, every RMAN session requires the setting of the encryption and decryption password; otherwise, the session fails with a "wallet not open" error.

```
CONFIGURE ENCRYPTION FOR DATABASE ON;
CONFIGURE ENCRYPTION ALGORITHM 'AES256';
SET ENCRYPTION ON IDENTIFIED BY passw0rd ONLY ;
```

The final command then triggers the actual backup of the database to disk. The backup uses the RMAN-specific backup sets. Each RMAN process reads 6000M of consecutive data from a data file as a backup piece, compress and encrypt it and then write it to the destination file system. The goal of the section size is to limit the size of a backup piece so that a potentially required retransmit of a failed file transfer to the destination environment is manageable.

As pointed out before, it is essential that archived redo log files are included in the backup and the PLUS ARCHIVELOG flag ensures that RMAN picks up the existing archivelogs. The use of a TAG is strongly recommended as it simplifies the management of multiple backups in an RMAN catalog. “Incremental level 0” specifies this backup as an incremental backup at level 0, which means all data will be included in the backup.

RMAN picks up the existing archivelogs. The use of a TAG is recommended as it simplifies the management of multiple backups in an RMAN catalog. “Incremental level 0” specifies this backup as an incremental backup at level 0, means that all data will be included in the backup.

```
BACKUP tag '<Your TAG here>' incremental level 0 AS compressed BACKUPSET section size 6000M DEVICE TYPE DISK DATABASE
INCLUDE CURRENT CONTROLFILE PLUS ARCHIVELOG TAG <SID>_LEV0;
```

For additional incremental backups we suggest replacing occurrences of “inc1 / INC1” with corresponding “incN / INCN” in the following backup script. Note that it is suggested to store each incremental set of backup files into its own directory for easier management.

Incremental online backup - level 1

The second RMAN script `option2_backup_inc1.rman` configures the RMAN environment and creates the initial level 0 (full) online backup. The key command to start the incremental (level 1) backup in this script is: `BACKUP ... incremental level 1 ...`

Replace the terms `<sid>` with the SID value from your system and ensure the target backup directory defined in the script matches the directory that you have created in. [Backup Option 2 - Create Target Directories](#).

`option2_backup_inc1.rman` script

```
connect target /
CONFIGURE CHANNEL DEVICE TYPE DISK FORMAT '/backup/rman/<sid>_option2_inc1/inc1_%d_%U';
CONFIGURE BACKUP OPTIMIZATION ON;
CONFIGURE DEVICE TYPE DISK PARALLELISM 60;
CONFIGURE CONTROLFILE AUTOBACKUP ON;
CONFIGURE CONTROLFILE AUTOBACKUP FORMAT FOR DEVICE TYPE DISK TO '/backup/rman/<sid>_option2_inc1/inc1_cf_%F';
CONFIGURE COMPRESSION ALGORITHM 'MEDIUM';
CONFIGURE ENCRYPTION FOR DATABASE ON ;
CONFIGURE ENCRYPTION ALGORITHM 'AES256' ;
SET ENCRYPTION ON IDENTIFIED BY passw0rd ONLY ;
BACKUP TAG `<SID>`_INC1 incremental level 1 AS compressed BACKUPSET section size 6000M DEVICE TYPE DISK DATABASE
INCLUDE CURRENT CONTROLFILE PLUS ARCHIVELOG;
quit;
```

As user `oracle` set the environment variable `ORACLE_SID` with the SID value of your system:

```
$ setenv ORACLE_SID <SID>
```

And execute the incremental backup script:

```
$ rman @option2_backup_inc1.rman
```

The incremental level 1 scripts differ from the previously discussed level 0 RMAN script only in 3 areas:

- The directory where the backup files are written to.
- The TAG is used to identify the backup set.
- The specification of level 1 instead of level 0, indicating that this is an incremental backup, which by default, contains all changes since the last level 1 or level 0 backup.

The final incremental backup requires extra preparation steps to determine the date/time stamp to use in the final database recovery step for the destination environment. The time stamp *highlighted* in the *blue* box in the next step is the date/time the database will be recovered to. Any changes after that date/time will be discarded!

Inspect server time and date

Connect to the database as sysdba and execute the commands, as shown instructed. Note that the database is only put into `mount` mode and not `opened`.

Setting the NLS Date format is used as the format model to implicitly cast from `date-to-string` or `string-to-dates`, this is important if you choose to perform a Point in Time recovery.

The second SQL command seen in the following image is forcing Oracle to write to a new redolog, the command ran after shows the date stamp of when the file was created and provides you with a timestamp to roll the database forward to by applying the applicable redlogs.

```
ibmecc01:oracle 31> sqlplus "/ as sysdba"

SQL*Plus: Release 19.0.0.0.0 - Production on Fri May 10 12:39:19 2024
Version 19.22.0.0.0

Copyright (c) 1982, 2023, Oracle. All rights reserved.

Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.22.0.0.0

SQL> alter session set nls_date_format='MM-DD-YYYY HH24:mi:SS' ;

Session altered.

SQL> SELECT SYSDATE FROM DUAL ;

SYSDATE
-----
05-10-2024 12:39:36

SQL> ALTER SYSTEM SWITCH LOGFILE ;

System altered.

SQL> SELECT SYSDATE FROM DUAL ;

SYSDATE
-----
05-10-2024 12:39:48
```

Incremental time stamp

Execute the final incremental backup via RMAN.

Validate and cross-check backups

When backup is complete, within RMAN, you can utilize some of the commands listed after this to validate and cross-check results.

```
RMAN> REPORT SCHEMA;
RMAN> LIST BACKUP SUMMARY;
RMAN> LIST BACKUPSET <TAG ID> ;
RMAN> BACKUP VALIDATE CHECK LOGICAL DATABASE ARCHIVELOG ALL;
RMAN> VALIDATE DATAFILE 10;
RMAN> VALIDATE BACKUPSET 3;
RMAN> CROSSCHECK BACKUP;
```

Lists and displays information about the database files, tablespaces and so on.

Explanation of commands:

- `REPORT SCHEMA` ; - Lists and displays information about the database files, tablespaces and so on.
- `LIST BACKUP SUMMARY` ; - Lists all existing backups. A SUMMARY option can be used.

- `LIST BACKUP <TAG ID> ;` - List a specific backup by TAG ID.
- `BACKUP VALIDATE CHECK LOGICAL DATABASE ARCHIVELOG ALL;` - Validate the contents of backup files.
- `VALIDATE DATAFILE 10;` - Validate a specific datafile.
- `VALIDATE BACKUPSET 3;` - Validate a specific backupset.
- `CROSCHECK BACKUP;` - Synchronize the physical reality of backups and copies with their logical records in the RMAN repository.

Create PFILE

Create a plain text database parameter file (PFILE) from the binary server parameter file (SPFILE) as follows. The database remains in mounted mode. Remember to replace the term `<SID>` with your systems SID in the command.

Execute as user `oracle` these commands:

```
$ setenv ORACLE_SID <SID>
sqlplus "/ as sysdba";
```

In SQL*Plus create the parameter file:

```
SQL> create pfile='/backup/rman/init<SID>.ora' from spfile;
```

Be sure to restore all RMAN parameters back to original discovery settings when done.

For this *Option 2* we have created TWO backup sets, a full and an incremental backup. Both are transferred to and restored on the target system. At this point, to be consistent with a migration scenario, the source database should be shut down and not used any longer.

Restore the Oracle database on the target system

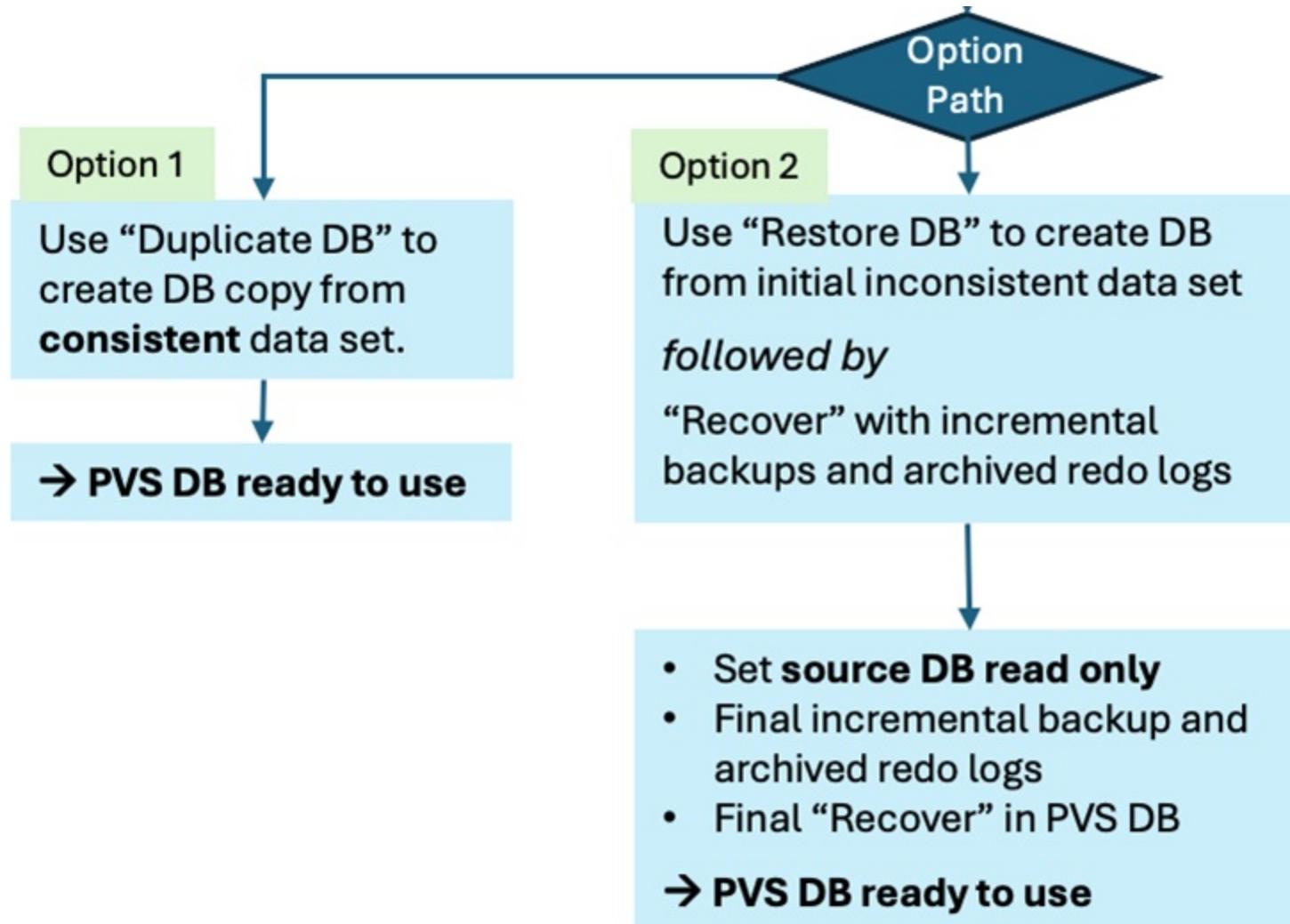
Different options and steps to restore the database on the target system are covered in this section.

Two RMAN restore options

Two methods to restore an Oracle Database to the target system are provided:

1. RMAN Duplicate Database and
2. RMAN Restore/Recover Database.

Both methods will use the backups created in the previous RMAN backup section.



Restore options

Option 1 - RMAN Duplicate Database

This option will use the `auxiliary instance` function of RMAN and can/should be used only when the full set of the consistent RMAN backup files are available on the target server. :

The RMAN “duplicate” command will automatically open the target database with `resetlogs`.

The `resetlogs` operation increments the database incarnation number and, as a result, makes the target database completely independent of the source. Importantly, no incremental level 1 backups or archived REDO logs can be applied to the target database at that point.

Option 2 - RMAN Restore/Recovery

This option should be used to initially establish the target database with an RMAN incremental level 0 and, optionally, one or more incremental level 1 backups as described in the previous section. However, it allows for later incremental level 1 backups and archived REDO logs to be applied to the target database over some amount of time. :

The expectation is that there will be a final cutover time, and the final incremental level 1 backup will be taken, copied/shipped to the target server and applied while the target database is still in a MOUNT state. Once the final backup/archived logs are applied, the database will be manually opened and made available at the cutover time.

Assumptions

1. An IBM cloud account has been established, along with an IBM Power Virtual Server workspace.
2. Within the workspace, manual or automated procedures have been executed to install on the IBM Power Virtual Server instance the necessary Oracle Grid Infrastructure (if using ASM) and Oracle RDBMS homes on AIX. The AIX LPAR should be sized comparable to the source system in terms of compute, memory, storage capacity and performance, with compatible HW/SW versionings applied.
3. All required backup files are accessible to the RMAN duplicate/restore/recover process.

Connectivity and preparation – Oracle on IBM Power Virtual Server

From the target instance command line, you can use the following RMAN procedure to perform a restore.

1. Login as the user `oracle` to the AIX Power Virtual Server where you want to restore the database.
2. Confirm that:
 - Target IBM Power Virtual Server system has a valid installation of the Oracle database software with the same version and patch level of software as in the source environment.
 - The device names for storage of Oracle datafiles and tablespace names are the same as with the source database. If not, `set newname` directives are required (steps are out of scope for this procedure)
 - ASM disk groups (if used) have been established with names and capacities that match the source environment.
 - Backup files are available to RMAN, whether resident on local file storage, Cloud Object Storage, NFS, and so on.

The following procedure options do not describe how to install the Oracle software, but rather how to restore the source database. As with the backup procedure, the presented steps are representative, and details differ from one database environment to another.

Reference the version-specific Oracle Database Installation Guide for AIX on Power Systems and the corresponding GRID Infrastructure documentation for ASM (and RAC, if relevant).

[Database Installation Guide \(Version 19c\)](#)

[Grid Infrastructure Documentation \(Version 19c\)](#)

Check backup file sets on target server

Here is a sample view of backup files that have been staged in the `/backup/rman` folder: Note that files were copied to a local `JFS/2` file system (partial list of files).

```

:oracle 24> pwd
/backups/rman/ibmec01/ec6_option1
:oracle 25> ls -ltr
total 66953720
-rw-r---- 1 oracle oinstall 1114112 May 16 11:41 option1_EC6_6n2qun7o_1239_1_1
-rw-r---- 1 oracle oinstall 1089536 May 16 11:42 option1_EC6_7t2qun8u_1277_1_1
-rw-r---- 1 oracle oinstall 73728 May 16 11:42 option1_EC6_6n2qun7o_1239_2_1
-rw-r---- 1 oracle oinstall 1163264 May 16 11:42 option1_EC6_7u2qun91_1278_1_1
-rw-r---- 1 oracle oinstall 143802368 May 16 11:43 option1_EC6_7s2qun8s_1276_1_1
-rw-r---- 1 oracle oinstall 370745344 May 16 11:44 option1_EC6_7a2qun7v_1258_1_1
-rw-r---- 1 oracle oinstall 396845056 May 16 11:44 option1_EC6_7f2qun89_1263_1_1
-rw-r---- 1 oracle oinstall 422944768 May 16 11:44 option1_EC6_7d2qun85_1261_1_1
-rw-r---- 1 oracle oinstall 405438464 May 16 11:44 option1_EC6_7c2qun81_1260_1_1
-rw-r---- 1 oracle oinstall 293330944 May 16 11:44 option1_EC6_7r2qun8r_1275_1_1
-rw-r---- 1 oracle oinstall 400580608 May 16 11:44 option1_EC6_7b2qun80_1259_1_1
-rw-r---- 1 oracle oinstall 403300352 May 16 11:44 option1_EC6_7h2qun8d_1265_1_1
-rw-r---- 1 oracle oinstall 380665856 May 16 11:44 option1_EC6_7e2qun88_1262_1_1
-rw-r---- 1 oracle oinstall 375504896 May 16 11:44 option1_EC6_7k2qun8i_1268_1_1
-rw-r---- 1 oracle oinstall 435519488 May 16 11:44 option1_EC6_7i2qun8e_1266_1_1
-rw-r---- 1 oracle oinstall 373809152 May 16 11:44 option1_EC6_7j2qun8g_1267_1_1
-rw-r---- 1 oracle oinstall 383893504 May 16 11:44 option1_EC6_7p2qun8p_1273_1_1
-rw-r---- 1 oracle oinstall 396402688 May 16 11:44 option1_EC6_7l2qun8k_1269_1_1
-rw-r---- 1 oracle oinstall 414564352 May 16 11:44 option1_EC6_7g2qun8b_1264_1_1
-rw-r---- 1 oracle oinstall 519069696 May 16 11:44 option1_EC6_7q2qun8q_1274_1_1
-rw-r---- 1 oracle oinstall 378011648 May 16 11:44 option1_EC6_7o2qun8o_1272_1_1
-rw-r---- 1 oracle oinstall 398745600 May 16 11:45 option1_EC6_7n2qun8n_1271_1_1
-rw-r---- 1 oracle oinstall 395542528 May 16 11:45 option1_EC6_7m2qun8m_1270_1_1
-rw-r---- 1 oracle oinstall 1328152576 May 16 11:46 option1_EC6_792qun7v_1257_1_1
-rw-r---- 1 oracle oinstall 1486774272 May 16 11:46 option1_EC6_742qun7r_1252_1_1
-rw-r---- 1 oracle oinstall 1535180800 May 16 11:46 option1_EC6_6r2qun7o_1243_1_1
-rw-r---- 1 oracle oinstall 1524285440 May 16 11:46 option1_EC6_752qun7r_1253_1_1
-rw-r---- 1 oracle oinstall 1486831616 May 16 11:46 option1_EC6_732qun7q_1251_1_1

```

Restore options

Displayed in a separate folder are miscellaneous files directly copied from the on-premises Oracle database, as recommended in the backup procedure before this.

```

[root@rman]# ls -lsa
total 0
0 drwxr-xr-x  2 oracle  dba          256 May 22 15:19 checksum      # Optionally save cksum for backup files
0 drwxr-xr-x  5 oracle  dba          256 May 16 11:14 ibmec01      # Contains the backup files
0 drwxr-xr-x  2 oracle  dba          256 May 22 15:21 ora          # saved parameter file (PFILE) and TNS Configuration

```

Backup folder tree

Check configuration

The Oracle PFILE configuration is now viewed and settings from this file are verified.

Check PFILE

We will now review the Oracle parameter file, or **PFILE**, stored within as **init<SID>.ora**.

Review database parameters that are contained within the saved PFILE and examine those with file name specifications. The parameter **audit_file_dest** references a directory location that does not yet exist on the target server. The other file destinations reference ASM disk groups that should have already been created.

If the file locations in the target server do not match the source environment additional configuration changes are required in the RMAN scripts, so it is important that when **cloning** your Oracle server in IBM Cloud that you compare the configurations that are mentioned in the **init<SID>.ora** file and ensure that the locations exist on your target system.

```

*.audit_file_dest='/oracle/EC6/saptrace/audit'
*.compatible='19.0.0.0'
*.control_file_record_keep_time=30
*.control_files='/oracle/EC6/origlogA/cntrl/cntrlEC6.dbf','/oracle/EC6/origlogB/cntrl/cntrlEC6.dbf','/oracle/EC6/sapdata1/cntrl/cntrlEC6.dbf'
*.db_block_size=8192
*.db_cache_size=7247757312
*.db_name='EC6'
*.db_recovery_file_dest='/oracle/EC6/oraflash'
*.db_recovery_file_dest_size=30000M
*.diagnostic_dest='/oracle/EC6/saptrace'
*.ENCRYPT_NEW_TABLESPACES='DDL'
*.event='10027','10028','10142','10183','10191','10995 level 2','38068 level 100','38085','38087','44951 level 1024','60025','34011029 level 7'#SAP_192000230718_2
02308 RECOMMENDED SETTINGS
*.FILESYSTEMIO_OPTIONS='setall'
*.log_archive_dest_1='LOCATION=/oracle/EC6/oraarch/EC6arch'
*.log_archive_format='%t_%s_%r.dbf'
*.log_checkpoints_to_alert=true

```

Audit file destination

Check audit directory

Check and confirm that the audit file directory is present on the target server and as listed in the PFILE and give the proper ownership and mode.

```

:oracle 37> grep audit_file $ORACLE_HOME/dbs/initEC6.ora
*.audit_file_dest='/oracle/EC6/saptrace/audit'
ibmecc02:oracle 38> ls -lsa /oracle/EC6/saptrace/
total 100
  0 drwxrwxr-x  6 oracle  oinstall      256 May 14  02:11 .
  4 drwxrwxr-x 27 oracle  oinstall    4096 May 16 10:26 ..
96 drwxrwxr-x  2 oracle  oinstall  94208 May 16 13:56 audit
  0 drwxrwxr-x  2 oracle  oinstall      256 May 14  02:10 background
  0 drwxrwxr-x  4 oracle  oinstall      256 May 14 14:10 diag
  0 drwxrwxr-x  2 oracle  oinstall      256 May 14  02:10 usertrace
:oracle 39>

```

Backup folder tree

Check ASM disk groups and other directory definitions

Confirm that ASM disk groups that are referenced in the PFILE exist on target and have sufficient free space. As an oracle grid user, run:

```
$ asmcmd lsdg
```

If ASM groups are not used, review the PFILE and verify that referenced directories exist. At this point, you are ready to proceed with one of the following restore options.

Option 1 - RMAN duplicate database

This procedure takes as input a consistent, Level 0 backup of the source database and restores the contents to a new Oracle instance on Power Virtual Server to create a duplicate database.

The following steps should be executed as the oracle user:

Starting the target database in NOMOUNT mode

Ensure the `ORACLE_SID` environment is set. As user `oracle` set the correct ORACLE_SID for your system:

```
$ setenv ORACLE_SID <SID>
```

Start the Oracle instance in NOMOUNT mode, directly specifying the pfile to be used. Note that in our environment we are using Oracle in an SAP Environment so our ORACLE_HOME was `/oracle/EC9/19.0.0` your environment can be different, change the paths in the example and remember to substitute your own Oracle `<SID>` in the commands mentioned after this.

As user `oracle` execute SQL*Plus and connect to the database as system database administrator:

```
$ sqlplus "/ as sysdba"
```

Inside SQL*Plus execute these SQL statements:

```

SQL> startup nomount pfile='/backup/rman/ora/initEC6.ora';
SQL> create spfile='/oracle/EC6/19.0.0/dbs/spfileEC6.ora' from pfile='/backup/rman/ora/initEC6.ora';
SQL> shutdown immediate;
SQL> startup nomount;

```

```
SQL> show parameter spfile;
```

The spfile parameters typically look like this:

NAME	TYPE	VALUE
spfile	string	/oracle/EC6/19/dbs/spfileEC6.ora

Script to restore database with RMAN - Option 1

Create an RMAN Duplicate Database script referencing the appropriate backup location. The file in this case is stored in the home directory of the ‘oracle’ user.

Optimally, you would create the number of restore channels using the reference to match the number of channels used for backup. If you recall during the backup process we observed that 60 channels were in use, so we match this number in the script.

 **Note:** The following script is appended to show the first 15 rows only, obviously because we need 60 channels, these need to be added to the script, you are required to add the additional rows after `allocate auxiliary channel ch[15-60] device type disk;`

As user `oracle` create this script.

```
rman_duplicate.cmd
```

```
set encryption on identified by passw0rd;
set decryption identified by passw0rd;
run {
    allocate auxiliary channel ch1 device type disk;
    allocate auxiliary channel ch2 device type disk;
    allocate auxiliary channel ch3 device type disk;
    allocate auxiliary channel ch4 device type disk;
    allocate auxiliary channel ch5 device type disk;
    allocate auxiliary channel ch6 device type disk;
    allocate auxiliary channel ch7 device type disk;
    allocate auxiliary channel ch8 device type disk;
    allocate auxiliary channel ch9 device type disk;
    allocate auxiliary channel ch10 device type disk;
    allocate auxiliary channel ch11 device type disk;
    allocate auxiliary channel ch12 device type disk;
    allocate auxiliary channel ch13 device type disk;
    allocate auxiliary channel ch14 device type disk;
    allocate auxiliary channel ch15 device type disk;
    allocate auxiliary channel ch16 device type disk;
    allocate auxiliary channel ch17 device type disk;
    allocate auxiliary channel ch18 device type disk;
    allocate auxiliary channel ch19 device type disk;
    allocate auxiliary channel ch20 device type disk;
    allocate auxiliary channel ch21 device type disk;
    allocate auxiliary channel ch22 device type disk;
    allocate auxiliary channel ch23 device type disk;
    allocate auxiliary channel ch24 device type disk;
    allocate auxiliary channel ch25 device type disk;
    allocate auxiliary channel ch26 device type disk;
    allocate auxiliary channel ch27 device type disk;
    allocate auxiliary channel ch28 device type disk;
    allocate auxiliary channel ch29 device type disk;
    allocate auxiliary channel ch30 device type disk;
    allocate auxiliary channel ch31 device type disk;
    allocate auxiliary channel ch32 device type disk;
    allocate auxiliary channel ch33 device type disk;
    allocate auxiliary channel ch34 device type disk;
    allocate auxiliary channel ch35 device type disk;
    allocate auxiliary channel ch36 device type disk;
    allocate auxiliary channel ch37 device type disk;
    allocate auxiliary channel ch38 device type disk;
    allocate auxiliary channel ch39 device type disk;
    allocate auxiliary channel ch40 device type disk;
    allocate auxiliary channel ch41 device type disk;
    allocate auxiliary channel ch42 device type disk;
    allocate auxiliary channel ch43 device type disk;
```

```

allocate auxiliary channel ch44 device type disk;
allocate auxiliary channel ch45 device type disk;
allocate auxiliary channel ch46 device type disk;
allocate auxiliary channel ch47 device type disk;
allocate auxiliary channel ch48 device type disk;
allocate auxiliary channel ch49 device type disk;
allocate auxiliary channel ch50 device type disk;
allocate auxiliary channel ch51 device type disk;
allocate auxiliary channel ch52 device type disk;
allocate auxiliary channel ch53 device type disk;
allocate auxiliary channel ch54 device type disk;
allocate auxiliary channel ch55 device type disk;
allocate auxiliary channel ch56 device type disk;
allocate auxiliary channel ch57 device type disk;
allocate auxiliary channel ch58 device type disk;
allocate auxiliary channel ch59 device type disk;
allocate auxiliary channel ch60 device type disk;
duplicate database to <DBSID> backup location '/backup/rman/ec6_option1' nofilenamecheck noredo;
}

```

As user `oracle` execute this script:

```
$ rman auxiliary / cmdfile=rman_duplicate.cmd
```

A typical output looks like this:

```

sql clone "alter system set db_name =
''EC6'' comment=
''Modified by RMAN duplicate'' scope=spfile";
sql clone "alter system set db_unique_name =
''EC6'' comment=
''Modified by RMAN duplicate'' scope=spfile";
shutdown clone immediate;
startup clone force nomount
restore clone primary controlfile from '/backup/rman/ec6_option1/option1_cf_c-2254911489-20240516-00';
alter clone database mount;

```

Here, the database is successfully cloned and the resetlogs are also opened leading to the database open status and the message that the Recovery manager action has been successfully completed.

Check the archive log status on the target system

After the target database has been successfully restored, Use the following commands to check Archive log status.

Run the `SQL*Plus` command as user `oracle`:

```
$ sqlplus "/ as sysdba"
```

Inside `SQL*Plus` execute this sql command:

```
SQL> archive log list;
```

The typical output looks like:

Database log mode	No Archive Mode
Automatic archival	Disabled
Archive destination	/oracle/EC6/oraarch/EC6arch
Oldest online log sequence	1
Current log sequence	1

Restarting the database in archive mode

Still in SQL*Plus as sysdba, shut down the database instance by using the NORMAL, IMMEDIATE, or TRANSACTIONAL option:

```
$ SHUTDOWN IMMEDIATE
```

Start the instance and mount the database:

```
$ STARTUP MOUNT
```

And place the database into Archive Mode:

```
$ ALTER DATABASE ARCHIVELOG;
```

Now open the database on the server:

```
$ ALTER DATABASE OPEN;
```

And verify your changes:

```
$ ARCHIVE LOG LIST;
```

Finally create a new database backup on this target system that will also include the Archive files. As described previously in the section [Back up the Source Oracle Database by using RMAN](#)

Reasons for choosing using the options `nofilenamecheck` and `noredo` with `duplicate database`

`nofilenamecheck`

The option `nofilenamecheck` will stop RMAN pre-checking the directory and file location of the target system by comparing the information that is contained with the control files of the duplicate backup. This is necessary if you want to restore a 1-2-1 copy of your source database to target using identical filesystem locations, SID and so on. If the option is not present then, you could receive a warning and the restore stops stating that there are discovered conflicts where target file locations where the datafiles will be restored to match source file locations. If this occurs add the `nofilenamecheck` to the restore command and retry, then the restore works.

`noredo`

The `noredo` option has to be added to the duplicate database command in the `rman_duplicate.cmd` script as shown earlier.

This is informing RMAN that you want to restore the full `offline` backup that is taken and do not check for any redo logs. Oracle DBA's already know the issues when trying to create duplicate backups with the `PLUS ARCHIVELOG` mentioned in the backup command.

Option 2 - RMAN restore/recover database

This procedure establishes an Oracle database on Power Virtual Server from an initial inconsistent data set. It then applies incremental backups and archived redo logs to recover a version of the database at a specific point in time.

Starting the target database in NOMOUNT mode

The following steps should be executed as the user `oracle`. As always replace the term `<SID>` with the SID value of your system:

```
$ setenv ORACLE_SID <SID>
```

Start the Oracle instance in `NOMOUNT` mode, directly specifying the pfile to be used. Note that in our environment we are using Oracle in an SAP Environment so our `ORACLE_HOME` was `/oracle/EC9/19.0.0` your environment can be different, so modify paths in the example and remember to substitute your own Oracle `<SID>` in the commands mentioned after this.

```
$ sqlplus "/ as sysdba"
```

```
SQL> startup nomount pfile='/backup/rman/ora/initEC6.ora';
SQL> create spfile='oracle/EC6/19.0.0/dbs/spfileEC6.ora' from pfile='/backup/rman/ora/initEC6.ora';
SQL> shutdown immediate;
SQL> startup nomount;
SQL> show parameter spfile;
```

The output showing the parameter typically looks like:

NAME	TYPE	VALUE
spfile	string	/oracle/EC6/19/dbs/spfileEC6.ora

Getting the configuration file path in the backup file set

The control file (cf) had been included in the full backup (level 0). Determine the full path of the control file in the backup option2 level0 file set.

Example:

```
$ find /backup/rman/ec6_option2 -name "lev0_cf_*
```

The find command prints all filenames including path that match the name pattern:

```
/backup/rman/ec6_option2/lev0_cf_c-2252531432-20240529-01
```

If no output is given, refer to the backup you created with the option 2 level 0 procedure for the control file location and check if and where the backup file set is on the target server.

Script to restore database level 0 backup with RMAN - Option 2

Modify the recovery script after this to reflect the correct control file and then execute the RMAN script to restore the DB from level 0 backup and also apply any archived redo logs included in that backup via `recover database` as the `restore database` does not apply archived redo logs.

Note the use of the backup TAG to specify from which backup we want to restore. The RMAN catalog in the control file may list multiple backups. For our test I use the same backup tag that was used in the backup section that was previously created, hence why it is a good tip to use backup tags for specific backups.

Remember before script execution the Database should be started in `nomount` and the control file location must be adjusted to your file/backup location as shown in the following example.

`option2_restore_level0.rman` script

```
connect target /
connect target /
set ENCRYPTION ALGORITHM 'AES256' ;
SET DECRYPTION IDENTIFIED BY passw0rd;
run {
    restore controlfile from '/backup/rman/ec6_option2/lev0_cf_c-2252531432-20240529-01';
    alter database mount;
    restore database from tag IBMECC02_EC6_LEV0;
    recover database;
}
```

Description of the restore script

Substitute the correct locations for `archive`, `redologs`, and `controlfiles` that are relevant to your Oracle Environment/Installation.

The backup files are encrypted and RMAN requires the encryption password to be able to restore the database files.

```
SET DECRYPTION IDENTIFIED BY passw0rd;
```

We restore the database control file from the level 0 backup that contains the RMAN catalog we need to map backup pieces to data files as well as the list of data files and their expected locations.

```
restore controlfile from '/backup/rman/ec6_option2/lev0_cf_c-2252531432-20240529-01';
```

We then alter the database to `mount mode` which is required for the next step.

```
alter database mount;
```

Using the TAG we assigned to the level 0 backup that we instruct RMAN to restore the database from that specific backup.

```
restore database from tag IBMECC02_EC6_LEV0;
```

As a final step we apply any in level 0 backup included archive logs to the restored database. Note that this does not open the database so that we can apply future incremental backups and/or archive logs to the database.

```
recover database;
```

Running the restore database level0 script

Ensure that the database instance was started with `startup nomount`

As user `oracle` execute the restore script:

```
$ rman @restore_option2_lev0.rman
```

Sample output is extensive and not listed here.

Restoring the incremental backups (level 1)

The RMAN full backup level 0 was restored successfully. The next step is restoring all incremental level 1 backup set.

Restoring the incremental backups (level 1) - except the final one

Catalog the remainder of the incremental level 1 backupsets and archived logs in the target directory. If multiple incremental backups are provided, this is an iterative process.

For all incremental backups, EXCEPT the last, you can simply execute a

```
$ recover database ;
```

With this step(s) the incremental backup set(s) are cataloged.

Catalog the final incremental backup (level 1)

The final incremental backup requires that the recovery is only until a specific time to be able to open the database!

 **Important:** The target database can remain in `MOUNT` state and have incremental level 1 and archived REDO logs applied continuously, as needed. Catalog new backup pieces and archived logs and recover until ready for final cutover.

The following command assumes that all incremental backups are stored in directories under `/backup/rman`.

Still in SQL*Plus, execute these SQL commands:

```
RMAN> catalog start with '/backup/rman';
```

Sample output, just showing backup files from the first incremental level 1 backup:

```
searching for all files that match the pattern /backup/rman

List of Files Unknown to the Database
=====
File Name: /backup/rman/ec6_option2_incl/inc1_EC6_dk2s0rg6_1460_1_1
File Name: /backup/rman/ec6_option2_incl/inc1_EC6_dl2s0rgc_1461_1_1
File Name: /backup/rman/ec6_option2_incl/inc1_EC6_dl2s0rgc_1461_2_1
File Name: /backup/rman/ec6_option2_incl/inc1_EC6_dm2s0rgc_1462_1_1
File Name: /backup/rman/ec6_option2_incl/inc1_EC6_dn2s0rgc_1463_1_1
File Name: /backup/rman/ec6_option2_incl/inc1_EC6_do2s0rgc_1464_1_1
File Name: /backup/rman/ec6_option2_incl/inc1_EC6_dp2s0rgc_1465_1_1
File Name: /backup/rman/ec6_option2_incl/inc1_EC6_dq2s0rge_1466_1_1
File Name: /backup/rman/ec6_option2_incl/inc1_EC6_dr2s0rgh_1467_1_1
File Name: /backup/rman/ec6_option2_incl/inc1_EC6_ds2s0rgn_1468_1_1
    ...Lines Omitted ...
File Name: /backup/rman/ibmecc02/ec6_option2_incl/inc1_EC6_eo2s0rlq_1496_1_1
File Name: /backup/rman/ibmecc02/ec6_option2_incl/inc1_EC6_ep2s0rlu_1497_1_1
File Name: /backup/rman/ibmecc02/ec6_option2_incl/inc1_EC6_eq2s0rm3_1498_1_1
File Name: /backup/rman/ibmecc02/ec6_option2_incl/inc1_EC6_er2s0rm6_1499_1_1
File Name: /backup/rman/ibmecc02/ec6_option2_incl/inc1_EC6_es2s0rma_1500_1_1
File Name: /backup/rman/ibmecc02/ec6_option2_incl/inc1_EC6_eu2s0rmi_1502_1_1
File Name: /backup/rman/ibmecc02/ec6_option2_incl/inc1_cf_c-2252531432-20240529-02
```

```
Do you really want to catalog the above files (enter YES or NO)? YES
cataloging files...
cataloging done
```

Restoring the final incremental backup (level 1) to a given point in time

For all incremental backups, EXCEPT the final, you can then execute in RMAN:

Remember because the backup was created with encryption you need to update the configuration in RMAN to decrypt the backup that uses the password, otherwise you encounter errors such as `ORA-19913: unable to decrypt backup` and `ORA-28365: wallet is not open`

```
RMAN> SET ENCRYPTION ALGORITHM 'AES256' ;
RMAN> SET DECRYPTION IDENTIFIED BY passw0rd;
RMAN> recover database ;
```

After cataloging the FINAL incremental backup pieces the recovery needs to be up to the *date/time* determined in the backup

After this final recovery action no further changes are expected to be applied to the database from a recovery perspective. Set the time and date format with:

```
RMAN> alter session set nls_date_format='DD-MM-YYYY HH24:mi:SS' ;
```

You will find an example date range here:

```
RMAN> recover database until time '13-01-2024 11:52:12';
```

Starting the database

After all interim archived REDO logs and the final RMAN increment level 1 have been cataloged and recovered as described, the database can be opened.

Run sql plus as user `oracle`:

```
$ sqlplus "/ as sysdba"
SQL> alter database open resetlogs ;
```

Checking the database mode

Check to make sure that after the database has been restored that the *Archive Mode* is now enabled.

As user `oracle` execute sqlplus command:

```
$ sqlplus "/ as sysdba"
```

And double check the archive logs list:

```
SQL> archive log list;
```

This concludes the Restore/Recover approach to database migration to Power Virtual Server.

Migrating SAP ERP 6.0 with IBM Db2 to IBM Power Virtual Server

Use the following guide to migrate your SAP Enterprise Resource Planning 6 (ERP) system from an IBM Db2 to an IBM Power Virtual Server. You have different options to migrate IBM Db2 databases to a target system.

IBM Db2 SAP migration options

For SAP ERP with IBM Db2, you have two migration options:

- [Migration option 1 - Back up and restore](#) is based on standard administrative tasks such as start, stop, backup, and restore. It is a less complicated approach, but it requires downtime during migration.
- [Migration option 2 - IBM Db2 high availability and disaster recovery \(HADR\)](#) is a downtime-optimized approach for SAP production systems. It is based on IBM Db2 High Availability and Disaster Recovery (IBM Db2 HADR) Database Synchronization and an online back

up. The system downtime is minimized, but the method requires a higher configuration approach compared to option 1.

Migration option 1 - Back up and restore

Back up and restore is a typical option to migrate development or test SAP systems. This migration option is based on a backup of the database from the source system and a database *restore* to fill the database on a preinstalled target system.

The following steps are required to complete the migration:

1. [Preparing for migration](#)
2. [Shutting down the SAP application and deactivating the database on the source server](#)
3. [Using the IBM Db2 offline backup on the source system](#)
4. [Transferring the backup files](#)
5. [Restoring the database on the target system](#)
6. [Starting the SAP target system](#)

Characteristics of the *Migration Option 1 - Back up and Restore* approach:

- *Downtime*: a planned downtime of the SAP system is required because the SAP system is not available during the migration process.
- *Fallback*: no changes were made to the source SAP system. The fallback action if required, stops the migration and restarts the source SAP system.
- *Complexity*: is based on standard administrative tasks. This migration option is the least complicated.

Preparing for migration

Use the following steps to prepare for the migration.

You need all the defined environment variables on both the source and target server. Save the commands to a temporary text file while you run them on the source SAP server. The exact same commands are required on the target server as shown in chapter [Restoring the database on the target system](#).

Set the following environment variables according to your needs.

1. Start a C shell session as `root` user on the source system:

```
$ csh
```

The command syntax for defining environment variables depends on the shell type. Default shell type for Db2 and SAP administrator users `db2<sid>` and `<sid>adm` is the C shell. When using the same shell, you can copy the command examples and paste them into your session environment.

2. Define the hostname of the target migration system (example: `cdb6ecc1`) and replace it with your target hostname:

```
$ set TARGETSERVER=cdb6ecc1
```

Make sure that the same versions of SAP ERP Software and IBM Db2 database are running on the source and target SAP systems.

3. Define the SAP instance administrator (this example is for the SAP instance `th1`) and change it to match your system.

```
$ set SIDADM=th1adm
```

4. Define the IBM Db2 database name - again `th1` is the example, and change it to match your system:

```
$ set DBNAME=th1
```

5. Define the IBM Db2 database administrator:

```
$ set DB2ADM=db2th1
```

6. Define a directory to store the backup files:

```
$ set BACKUPDIR=/db2/backup
```

7. Create the following directory if it does not exist:

```
$ mkdir -p $BACKUPDIR
```

and transfer the ownership of the backup directory to the Db2 administrator:

```
$ chown $DB2ADM $BACKUPDIR
```



Tip: This backup directory needs enough space to store the compressed backup files. Determine the current IBM Db2 database size by calling the `GET_DBSIZE_INFO` procedure. For more information, see the [GET_DBSIZE_INFO procedure](#).

Shutting down the SAP application and deactivating the database on the source server

Use the following steps to shut down the SAP application and deactivate the database on the source server.

1. To start or stop the SAP system, use the SAP instance administrator account `$SIDADM`:

```
$ su - $SIDADM
```

2. To stop the SAP system and keep the database running, use the following command:

```
$ stopsap r3
```

Optionally, you can check whether the SAP is in the required state by running the following command:

```
$ stopsap check
```

The expected output looks like the following example:

```
Checking db6 Database
Database is running
-----
Checking SAP TH1 Instance ASCS01
-----
Instance ASCS01 is not running
Checking SAP TH1 Instance D00
-----
Instance D00 is not running
```

3. For the Db2 commands, end the `$SIDADM` user session:

```
$ exit
```

4. Switch to the `$DB2ADM` user:

```
$ su - $DB2ADM
```

Optionally, you can check whether any applications are still connected to the database before you deactivate the database by running the following command:

```
$ db2 list applications
```

The following example is the expected output.

```
SQL1611W No data was returned by Database System Monitor.
```



Tip: If applications are still listed, stop the applications and check again. Only if the external applications still don't stop, try disconnecting applications from the database server with `db2 force applications all`.

5. Define the environment variables for the DB2ADM user again:

```
$ set DBNAME=th1
```

```
$ set BACKUPDIR=/db2/backup
```

6. The IBM Db2 offline backup requires that the database is deactivated. Use the following command to deactivate the database:

```
$ db2 deactivate database $DBNAME
```

The following output is expected.

```
DB20000I The DEACTIVATE DATABASE command completed successfully.
```

Using the IBM Db2 offline backup on the source system

Use the following steps to use the Db2 offline backup on the source system.

A backup directory to store the compressed offline backup was created in the preparation step [Preparation for Migration](#).

1. Verify that the backup directory offers sufficient available space to store backup files:

```
$ df -m $BACKUPDIR
```

2. Start the IBM Db2 offline backup:

```
$ db2 backup database $DBNAME to $BACKUPDIR compress
```

This command runs for a long time, depending on the database size.



Tip: Backup progress can be tracked with the command `db2 list utilities show detail`



Note: You can find a timestamp at the end of the backup command output. This timestamp is required to [Restoring the database on the target system](#).

Example output:

```
Backup successful. The timestamp for this backup image is : 20240730170709
```

Memorize this timestamp, you need to refer to it in the next two steps.

3. Use an environment variable to store the timestamp:

```
$ set TIMESTAMP=<your timestamp>
```

The IBM Db2 backup timestamp has the format YYYYMMDDHHMMSS (Year-Month-Day-Hour-Minute-Second) and looks like `20240730170709`. This timestamp is needed on the target SAP server again. Append this `TIMESTAMP` definition command to the list of saved commands that are from [Preparation for Migration](#).

4. Change to the backup folder by using the following command:

```
$ cd $BACKUPDIR
```

5. Check for files that contain your timestamp in their name:

```
$ ls -l *$TIMESTAMP*
```

Example output:

```
TH1.0.db2th1.DBPART000.20240730170709.001
```

Files that are listed in the output are the backup files that are transferred to the target system in the next step.

Transferring the backup files

Use the following step to transfer the backup files.

1. Copy the backup files from the source SAP system to the target:

```
$ scp ${BACKUPDIR}/*${TIMESTAMP}* \
${TARGETSERVER}:${BACKUPDIR}
```

This example uses secure copy (SCP), a slower version of data transfer. You can transfer backup files either directly to an IBM AIX LPAR in Power Virtual Server, or to IBM Cloud Object Storage. If you use SCP or SFTP with IBM Cloud Object Storage, it assumes that you are using an IBM FileManage Gateway service or installed and configured an SFTP server within or next to the target IBM Power Virtual Server environment to receive the transfer.

The faster option is IBM's high-performance Aspera product for data transfer. In many situations, IBM Aspera can transfer data several times faster than traditional TCP-based protocols. For more information, see [IBM Aspera Technologies](#).



Note: This reference also contains the [Accelerated network transfer migration guide](#).

Restoring the database on the target system

Use the following steps to restore a database on the target system.

1. Log in to the target server to start the restore procedure:

```
$ ssh $DB2ADM@$TARGETSERVER
```

The target server can't know the environment variables that are defined on the source system. But variables `$DBNAME`, `$TIMESTAMP` and `$SIDADM` are needed on the target system. To define these variables, run the list of commands that you saved in step [Preparing for migration](#) and [Using the IBM Db2 offline backup on the source system](#) or define the environment variables again.

2. The full restore procedure requires a deactivated IBM Db2 database. Use the same steps as before on the preinstalled target SAP system:

```
$ db2 list applications
```

The following output is expected:

```
SQL1611W No data was returned by Database System Monitor.
```

3. Deactivate the IBM Db2 database:

```
$ db2 deactivate database $DBNAME
```

4. Do a full database restore:

```
$ db2 restore database $DBNAME \
  from $BACKUPDIR \
  taken at $TIMESTAMP
```



Tip: Appending `replace existing` to the restore command avoids the overwrite prompt.

5. Db2 command asks if you want to overwrite the existing database by restoring the backup:

```
SQL2523W Warning! Restoring to an existing database that is different from the database on the backup image, but have matching names. The target database is overwritten by the backup version. The Roll-forward recovery logs associated with the target database is deleted.
```

```
Do you want to continue ? (y/n)
```

Enter `y` and press Enter.

The following output is expected:

```
DB20000I The RESTORE DATABASE command completed successfully.
```



Tip: If the restore did not succeed, drop the database on the target system in advance with `db2 drop database $DBNAME` and redo the restore command.

6. To complete the restore, use the following command:

```
$ db2 rollforward db $DBNAME to end of backup and stop
```

The target database now contains the source system data.

Starting SAP target system

Use the following steps to start the target system,

1. Switch to the SAP instance administrator:

```
$ login $SIDADM
```

2. Start the SAP application:

```
$ startsap
```

The following example is the expected output:

```
Checking db6 Database
Database is running
-----
Starting Startup Agent sapstartsrv
OK
Instance Service on host <TARGET> started
-----
starting SAP Instance ASCS01
Startup-Log is written to /home/th1adm/startsap_ASCS01.log
-----
/usr/sap/TH1/ASCS01/exe/sapcontrol -prot NI_HTTP -nr 01 -function Start
Instance on host <TARGET> started
Starting Startup Agent sapstartsrv
OK
Instance Service on host <TARGET> started
-----
starting SAP Instance D00
Startup-Log is written to /home/th1adm/startsap_D00.log
-----
/usr/sap/TH1/D00/exe/sapcontrol -prot NI_HTTP -nr 00 -function Start
Instance on host <TARGET> started
```



Important: Adjust the SAP system DNS record to point to the target SAP server to make sure that client systems (the running SAP Logon GUI) are connected to the target server.

The migration is complete.

- SAP system on the source server is down
- SAP system on the target server is up and running

Migration option 2 - IBM Db2 high availability and disaster recovery (HADR)

Migration option 2 is a downtime-optimized procedure. It is a combination of backup, recovery, and synchronization of the databases on both sides by using IBM Db2 HADR. If databases are in sync and the environment is prepared for migration, the core migration switches to the preinstalled target SAP server.

If the source system uses an IBM Db2 cluster or has IBM Db2 HADR enabled, migration extends the existing HADR configuration. [Special case - Migrating a source IBM Db2 cluster](#) describes and links to the required steps.

If IBM Db2 HADR is not enabled on the source side, the following steps are required:

1. [Preparing for migration](#)

2. [Making sure that IBM Db2 archive logging is enabled](#)
3. [Creating an online backup from the source system database](#)
4. [Transferring backup files to the target system](#)
5. [Restoring the target system](#)
6. [Defining HADR local and remote service ports on the target and source system](#)
7. [Configuring HADR on the target and source systems](#)
8. [Starting HADR and checking the synchronized data](#)
9. [Running the core migration step](#)

Characteristics of *Migration Option 2 -IBM Db2 HADR* :

- *Downtime, general*: it has a short downtime when the server switches from source to target. Before the switch, the source SAP system is running. After the switch, the target SAP system takes over.
- *Downtime, circular logging*: HADR requires that the IBM Db2 database is in **archive logging** mode. If your IBM Db2 database is in **circular logging** mode, you need to migrate the IBM Db2 database to **archive logging** mode before you use HADR. This step enforces a one-time database downtime.
- *Fallback*: means that the source SAP system is running during the complete migration until it switches. Before you make the switch, no special fallback option is required. If steps before or after the switch are unsuccessful, you can reverse the steps to bring the source SAP system up and running again.

Special case - Migrating a source IBM Db2 cluster

If the source SAP system is an IBM Db2 HADR cluster, the HADR configuration needs to extend to include the target server. The steps are easier in this case.

Most of the configuration steps that are described are already set up. The target system needs to be added as an auxiliary node to the existing IBM Db2 HADR configuration. For more information, see the [Steps for adding a new Auxiliary Standby to an existing Db2 HADR Pair](#) IBM Db2 Support Article.

Preparing for migration

Use the following steps to prepare the SAP system for migration.

Keep the following information in mind as you prepare for the migration.

- You need to define two TCP port numbers to use in your setup.
- Synchronizing with HADR requires two open network ports:
 - A local port for outgoing traffic
 - A remote port for incoming traffic
- Both port are configured on each of the two IBM Db2 systems, but with interchanged order. This example uses port number **5920/tcp** and **5921/tcp**, but you can adapt these ports to your needs.
- Firewalls must allow TCP traffic between the source and target system. Make sure that the required firewall rules are configured on all involved firewalls and on the source and target system.

Set the following environment variables according to your configuration.

All environment variables that are defined are needed on both the source and target server. Save the commands while you run them on the source SAP server to a temporary text file. The same commands are required on the target server as noted in [Restoring the database on the target system](#).

1. Define the hostname for the target migration system. **cdb6ecc1** is an example and replace it with your target hostname by using the following command:

```
$ set TARGETSERVER=cdb6ecc1
```

Make sure that your target server is running SAP ERP Software and IBM Db2 database with the same version as the source SAP system.

2. Define the SAP instance administrator and change it to match your system by using the following command (this example is for the SAP instance **th1**):

```
$ set SIDADM=th1adm
```

3. Define the IBM Db2 database name - again `th1` is an example. Change it to match your system:

```
$ set DBNAME=th1
```

4. Define the IBM Db2 database administrator:

```
$ set DB2ADM=db2th1
```

5. Define a directory to store backup files:

```
$ set BACKUPDIR=/db2/backup
```

6. Create the following directory if it does not exist:

```
$ mkdir -p $BACKUPDIR
```

and transfer the ownership of the backup directory to the Db2 administrator:

```
$ chown $DB2ADM $BACKUPDIR
```

 **Tip:** This backup directory needs enough space to store the compressed backup files. Determine the current IBM Db2 database size by calling the `GET_DBSIZE_INFO` procedure. For more information, see [GET_DBSIZE_INFO procedure](#).

Making sure that IBM Db2 archive logging is enabled

IBM Db2 High Availability and Disaster Recovery (HADR) requires `archive logging` to be enabled. `circular logging` is enabled by default after you install IBM Db2 HADR. Most SAP systems with IBM Db2 have `archive logging` enabled.

Checking the archive logging methods

To check which logging method is configured, use the following steps.

1. Switch to the IBM Db2 database admin:

```
$ su - $DB2ADM
```

2. Retrieve both log archive method configuration options:

```
$ db2 get db cfg for th2 | grep LOGARCHMET
```

3. Continue with the next section, if at least one of the log archive methods is set to `ON`. Make sure that both are not set to `OFF`. This example shows what the output for enabled archive logging looks like:

First log archive method	(LOGARCHMETH1) = DISK:/db2/logarch/
Second log archive method	(LOGARCHMETH2) = OFF

4. If both log archive methods are `OFF`, you need to configure archive logging first. The following example is the output:

First log archive method	(LOGARCHMETH1) = OFF
Second log archive method	(LOGARCHMETH2) = OFF

Configuring archive logging

Archive logging is required for IBM Db2 HADR. If `LOGARCHMETH1` and `LOGARCHMETH2` are set to `OFF`, use the following steps to enable archive logging.

A downtime is required to enable archive logging.

1. Start as SAP admin user to stop the SAP system:

```
$ su - $SIDADM
```

2. Stop the SAP system, but leave the database running:

```
$ stopsap r3
```

3. Quit the SAP administrative user:

```
$ exit
```

4. Switch to the IBM Db2 administration account:

```
$ su - $DB2ADM
```

5. Use the saved commands to ensure environment variables like `DBNAME` and `BACKUPDIR` are set.

6. Define a directory for log archive files:

```
$ set LOGARCHDIR=/db2/log_archive
```

⚠️ Important: If possible, create the log archive directory on a separate partition. The archive log partition depends on the LPARs disk setup, which is out of the scope of this document. Keep in mind that if the source system is an IBM Db2 cluster, the log archive is a shared directory between the nodes.

7. Create the log archive directory, at minimum with this command:

```
$ mkdir $LOGARCHDIR
```

8. Check the created directory:

```
$ ls -ld $LOGARCHDIR
```

Sample output:

```
drwxr-xr-x 7 db2th1 dbth1adm 256 Aug 30 11:24 /db2/log_archive
```

9. Verify whether the directory owner is the Db2 administrator, which is `db2th1` in sample output. Then, check that the owner has full permissions `rwx`.

10. Configure Db2 to use a disk device with this directory for archive logging method 1:

```
$ db2 "update db cfg for $DBNAME using LOGARCHMETH1 DISK:$LOGARCHDIR"
```

Expected output:

```
DB20000I The UPDATE DATABASE CONFIGURATION command completed successfully.
```

IBM Db2 database enforces a backup after this change:

```
$ db2 backup database $DBNAME to $BACKUPDIR compress
```

The backup takes a while to complete, depending on the database size.

11. Use the SAP admin account `$SIDADM` to start database and SAP system again:

```
$ su - $SIDADM
```

```
$ startsap
```

Creating an online backup from the source system database

To minimize SAP system downtime, create an online Db2 database backup.

1. Switch to the Db2 admin user:

```
$ su - $DB2ADM
```

2. Start the online backup, including log files:

```
$ db2 backup db $DBNAME online to $BACKUPDIR compress include logs
```

Keep in mind that the backup takes some time to complete.

When the backup is complete, a timestamp is printed:

```
Backup successful. The time stamp for this backup image is : 20240913091058
```

Memorize this timestamp. You need it in the next two steps.

3. Use an environment variable to store the timestamp:

```
$ set TIMESTAMP=<your timestamp>
```

The IBM Db2 backup timestamp uses the format YYYYMMDDHHMMSS (Year-Month-Day-Hour-Minute-Second) and looks like **20240913091058**. This timestamp is needed on the target SAP server again. Append this **TIMESTAMP** definition command to the list of saved commands from step [Preparation for Migration](#).

Transferring backup files to the target system

Use the following step to transfer the backup files to the target system.

1. Copy the backup files from the source SAP system to the target system:

```
$ scp ${BACKUPDIR}/*${TIMESTAMP}* \
${TARGETSERVER}:${BACKUPDIR}
```

Restoring the target system

Use the following steps to restore the target system.

1. The database restore is done on the target server:

```
$ ssh $DB2ADM@$TARGETSERVER
```

The target server cannot know the environment variables that are defined on the source system. But the variables **\$DBNAME**, **\$TIMESTAMP** and **\$SIDADM** are needed on the target system. To define these variables, run the list of commands that you saved in step [Preparing for migration](#) and [Creating an online backup from the source system database](#) or define the environment variables again.

2. Use the online backup to restore to the database.

```
$ db2 restore database $DBNAME \
from $BACKUPDIR \
taken at $TIMESTAMP
```

Db2 command asks if you want to overwrite the existing database by restoring the backup:

```
SQL2523W Warning! Restoring to an existing database that is different from the database on the backup image, but have matching names. The target database will be overwritten by the backup version. The Roll-forward recovery logs associated with the target database will be deleted. Do you want to continue? (y/n)
```

3. Enter **y** and press Enter.

The following example is the expected output:

```
DB20000I The RESTORE DATABASE command completed successfully.
```



Tip: If the recovery was not successful, drop the database on the target system in advance with **db2 drop database \$DBNAME** and redo the restore command.

In contrast to option 1, do not roll forward archive logs. HADR takes this state to synchronize changed data that is in the next step. If the source SAP system is operational, source data changes.

To transfer the latest changes, configure IBM Db2 HADR database synchronization.

Defining HADR local and remote service ports on the target and source system

Use the following steps to define HADR local and remote service ports on the target and source system.

HADR uses two TCP ports to synchronize data.

1. Check that `/etc/services` does not contain these TCP port numbers on both systems. Configure port numbers in this file on both servers.

 **Tip:** If local and remote HADR ports are configured in `/etc/services`, IBM Db2 configuration is more readable by using service names instead of numbers.

In the example, ports `5920/tcp` and `5921/tcp` are used, but you can define different ports.

Overview table of the port numbers to configure:

Services name	Value on source server	Value on target server	Comment
db2th1ha_l	5921/tcp	5920/tcp	Local port
db2th1ha_r	5920/tcp	5921/tcp	Remote port

TCP port assignment in `/etc/services` on both servers

2. Use your favorite editor to change `/etc/services` on both servers.

3. Review if the configuration files are correct, by using the following command:

```
$ grep -e '592[01]/' /etc/services
```

The following lines are the expected output on the source server:

```
db2th1ha_l      5921/tcp      # Db2 HADR local port
db2th1ha_r      5920/tcp      # Db2 HADR remote port
```

Port numbers must be enabled on the target server. The following example is the expected output on the target node:

```
db2th1ha_l      5920/tcp      # Db2 HADR local port
db2th1ha_r      5921/tcp      # Db2 HADR remote port
```

Configuring HADR on the target and source system

HADR needs the following set of configurations.

Db2 HADR parameter	Value on source server	Value on target server	Comment
HADR_LOCAL_HOST	<source hostname>	<target hostname>	Hostname of the system that you are on
HADR_LOCAL_SVC	db2th1ha_l	db2th1ha_l	Local port as defined in <code>/etc/services</code>
HADR_REMOTE_HOST	<target hostname>	<source hostname>	The other host's hostname
HADR_REMOTE_SVC	db2th1ha_r	db2th1ha_r	Remote port as defined in <code>/etc/services</code>
HADR_REMOTE_INST	<db2 instance name>	<db2 instance name>	The other node's IBM Db2 instance name (not the database name)

LOGINDEXBUILD	ON	ON	Set to ON on for both hosts
HADR_SYNCMODE	<a valid sync mode>	<a valid sync mode>	See HADR Synchronization Mode

HADR parameter overview, both servers

Local and remote hostnames (`HADR_LOCAL_HOST` and `HADR_REMOTE_HOST`) must be turned on for both systems. `HADR_LOCAL_HOST` is always the hostname of the node. The configuration command is run on and the remote host is the hostname of the respective other system.

Local and remote service entries (`HADR_LOCAL_SVC` and `HADR_REMOTE_SVC`) are identical because the switch is already configured in `/etc/services`.



Note: [High availability disaster recovery \(HADR\) synchronization mode](#) explains different IBM Db2 HADR synchronization options and their benefits.

Use the following commands to configure both systems:

1. Local host is the system that the `hostname` command reports to:

```
$ db2 "update db cfg for $DBNAME using HADR_LOCAL_HOST `hostname`"
```

2. Local port is the local port definition from `/etc/services`:

```
$ db2 "update db cfg for $DBNAME using HADR_LOCAL_SVC db2th1ha_l"
```

3. For the remote host, verify that `$TARGETSERVER` points to the other server:

```
$ db2 "update db cfg for $DBNAME using HADR_REMOTE_HOST $TARGETSERVER"
```

4. The remote port is the remote port definition from `/etc/services`:

```
$ db2 "update db cfg for $DBNAME using HADR_REMOTE_SVC db2th1ha_r"
```

5. Configure the remote IBM Db2 instance.

As orientation, if the database name is `th1`, then the instance name looks like `db2th1`:

```
$ db2 "update db cfg for $DBNAME using HADR_REMOTE_INST $DBINST"
```

6. Make sure that the log index build is set to ON on both systems:

```
$ db2 "update db cfg for $DBNAME using LOGINDEXBUILD ON"
```

7. Define the HADR synchronization mode. The value `async` is an example, change it to match the [HADR Synchronization Mode](#) suitable for your environment:

```
$ db2 "update db cfg for $DBNAME using HADR_SYNCMODE async"
```

Starting HADR and checking the synchronized data

Use the following steps to start HADR and to check whether the data is syncing.

1. Start HADR on the target server in standby. Switch to the target server as `$DB2ADM`, and run the following command:

```
$ db2 start hadr on db $DBNAME as standby
```

Expected output looks like the following example:

```
DB20000I The START HADR ON DATABASE command completed successfully.
```

2. Start HADR on the source server as the primary. Switch to the source server as `$DB2ADM` and run the following command:

```
$ db2 start hadr on db $DBNAME as primary
```

Expected output looks like the following example:

```
DB20000I The START HADR ON DATABASE command completed successfully.
```

3. Verify the HADR state with:

```
$ db2pd -d $DBNAME -hadr
```

And check for these fields:

Field	Source server	Target server
HADR_ROLE	PRIMARY	STANDBY
HADR_STATE	PEER	PEER
HADR_CONNECT_STATUS	CONNECTED	CONNECTED
HADR Status Values, both servers		

Running the core migration

Use the following steps to start migrating the SAP system from source server to the target server.

⚠ Important: Adjust the SAP system DNS record to point to the target SAP server. This adjustment makes sure that client systems (such as the system that runs the SAP logon GUI) connect to the target server.

1. Stop the source servers SAP system that includes the Db2 database.

On the source system login as `$SIDADM` and run the following command:

```
$ stopsap
```

Wait for the command to complete.

2. Switch to the target server as `$DB2ADM` and initiate a takeover by using the following command:

```
$ db2 takeover hadr on database $DBNAME
```

✓ Tip: The takeover command has an option `by force` that can help if the source system wasn't cleanly shut down. For more information, see [TAKEOVER HADR command](#).

3. As `$DB2ADM` on the target server. Verify that the IBM Db2 HADR role changed from `standby` to `primary` by using the following command:

```
$ db2pd -d th2 -hadr | grep ROLE
```

4. If the IBM Db2 HADR role is `primary` on the target server, you can start the SAP system on the target server. Switch to the `$SIDADM` user and run the following command:

```
$ startsap
```

The IBM Db2 database synchronization is still configured, although not active at this stage.

Leave HADR configuration as is if the target system is planned to migrate back (as for a disaster scenario). If the source system is removed after the migration, remove the HADR configuration as described in [How to remove existing HADR configuration](#).

The migration is complete.

- SAP system on the source server is down

- SAP system on the target server is up and running

Migration from SAP ERP 6.0 to S/4HANA to IBM Power Virtual Server considerations

Migrating from SAP ERP 6.0 to SAP S/4HANA is called a heterogeneous migration. Upgrading the SAP software version and changing the database engine during the transition of the SAP system to IBM Power Virtual Server is complex.

The following items are best practices for a heterogeneous SAP migration.

- Either sign a contract for [RISE with SAP on IBM Power Virtual Server](#). The IBM RISE contract includes the service to migrate your SAP system to IBM Power Virtual Server.
- Or contact [IBM consulting](#) for more help with SAP migration service options.

This information does not replace required expert advice or support. It is intended for educational purposes as an example outline of the migration steps.

The migration process is based on the SAP product "Software Update Manager" (SUM) and the "Database Migration Option" (DMO) - which is not an IBM product. For more information, see [Database Migration Option: Target Database SAP HANA](#).

Target audience and intent

The described steps are targeted for solution and infrastructure architects, technology consultants, and implementation teams for SAP system migrations.

The information is to help with your project plans and provides an overview of database migration procedures that use DMO. Each migration project has a unique migration scenario with different challenges in terms of deployment, configuration, and available resources.

The following information explains the steps to migrate an SAP Business Suite server from on-premises to IBM Power Virtual Server. It is important to use the most recent version of the "Database Migration Option" (DMO) within the "Software Update Manager" (SUM).

The DMO function offers various methods to migrate. Installing the recent Service or Enhancement Pack Updates on the source system in advance is the method that is used in this description.

The following steps are verified with a proof of concept (POC) project migration:

- From the source system, use SAP ERP 6.0 EhP8 SP30 (ECC) system with Oracle 19c database on AIX
- To the target system, use SAP S/4HANA 2023 on RHEL 9.4 running on IBM Power Virtual Server

Whereas the overall steps are similar, migration steps that involve other operating systems or other databases are different. SAP offers individual SAP Notes for each operating system and database version.

DMO basics

Understand the naming conventions provided by SAP.

Software Update Manager (SUM)

SUM updates the SAP systems that are based on AS ABAP and AS Java™.

Database Migration Option (DMO)

DMO is an option of SUM for a migration scenario. It is not a tool.

Software Provisioning Manager (SWPM)

Software Provisioning Manager is a tool for SAP system installation or copy.

You can use SWPM for the heterogeneous SAP system copy, which is a typical migration path.

SAPup

SAPup runs as a background service for the migration.

SAPup processes handle requests from the SAP host agent and trigger tools such as `R3trans`, `tp`, or `R3load` when needed during the migration.

Maintenance Planner (MPO)

The SAP Solution Manager cloud-based Maintenance Planner enables an easier and more efficient planning of all changes in your SAP system landscape.

- [Maintenance Planner Link](#)

Technical Downtime Optimization App (TDOA)

TDOA gives a detailed analysis and evaluation of a previous SUM maintenance task or action. This information provides information on optimization potential, which can help to optimize the next SUM operation. If detailed planning is required for business downtime, TDOA can help minimize downtime and helps provide a more simple maintenance experience.

[SAP Note 2881515 - Introduction to the Technical Downtime Optimization App](#)

[SAP Community Blog - TDOA](#)

Disclaimer

SAP systems are typically customized and integrated with other systems and tools.

Every migration project must consider multiple dependencies that are not in the scope for this information. The following items are an example of out-of-scope dependencies.

- Specific procedures for operating and maintaining nonproduction and production systems
- Helps makes sure that the system is available for maintenance and reconfiguration
- Plan, schedule, and communicate downtimes
- Review and adjust migration procedures to the local system and environment

The migration options that are described are not necessarily specific to IBM PowerVS migrations. SAP basis and SAP functional admins are expected to understand the full scope of SAP Upgrades and the migration option that uses SUM/DMO - including details that are not explicitly stated.

SAP Software Update Manager is an SAP product. For more information, see [Database Migration Option: Target Database SAP HANA](#).

Migration considerations

It is important to understand the implications of a migration action and evaluate the necessary tasks. The following sections outline these considerations.

The following information also highlights some of the migration steps. The following items are verified with a migration.

- Source system: SAP ERP 6.0 EhP8 SP30 (ECC) system with Oracle 19c database on AIX
- Target system: SAP S/4HANA 2023 on RHEL 9.4 that is running on IBM Power Virtual Server

The overall steps are similar to other databases and operating systems.

Use this information, together with and not *limited* to SAP certified business practices, processes, and publicized tools. Links are included at the foot of the chapter.

 **Tip:** You can't upgrade of SAP source system during DMO with a system move. Instead, do a system copy, if the source system upgrade is required. To retain a fallback option, upgrade the copied SAP system. You can decommission the source SAP system after the migration.

Prerequisites and limitations

- The source SAP system must be Unicode
- The minimum SAP Version is at least SAP ERP 6.0 - also known as SAP ECC
- The ECC stack is ABAP only and not a dual ABAP and Java™ stack
- Update SPAM to version 77 or higher
- You can run the following checks in parallel (without the stack XML from MP)
 - Simplification item check
 - ABAP custom code checks

Dependency fulfillment

See the following list for the planning considerations for migrating to S/4HANA:

- Does ABAP custom code exist on your system that needs to be adapted?
- Which migration options are available for S/4HANA? For more information, see [Migration Objects for SAP S/4HANA](#).
- Are any business processes outdated?

- How long is the acceptable system downtime?
- Are you aware of the new transaction codes that are available and which codes are obsolete?
- Migrating to S/4HANA requires database schema changes. Implementing SAP customer vendor integration (CVI) on the source system is mandatory.
- Do any ad-on dependencies exist?
- Does SAP Fiori have dependencies?
- Are external data source connections used?
- Are data cleanup and database consistency checks in place?
- Is warm and cold SAP data clearly defined?
- Is the source system configured to run the "SAP Readiness Check" by using the most recent "Simplification Check"?

These considerations are just some of the questions that you need to address during the migration planning phase.

You can see details on how to activate and run the "SAP Readiness Check" with the most recent Simplification Check.

SAP readiness check for SAP S/4HANA

The "SAP Readiness Check" for SAP S/4HANA is a tool that analyzes the source system and determines steps that are required to convert from SAP ERP 6.0 to SAP S/4HANA. The "SAP Readiness Check" is a useful tool for the planning stage of your migration project. It also provides important assistance to scope and plan the project.

The "SAP Readiness Check" tool has different feature versions.

- SAP BW/4HANA
- SAP S/4HANA Upgrades
- SAP Customer Experience Solutions, and more

Read the subsections of this SAP support article to get the full list of variants: [Feature Scope Description - SAP Readiness Check](#).

You need to implement SAP notes to install the "SAP Readiness Check for SAP S/4HANA" tool. These notes are listed in the section [Associated SAP notes and documentation for the SAP readiness check](#). The data collector framework together with the data collectors are implemented on the source system. These collectors are then activated to collect statistical data and collect a limited set of configuration data from your system.

Make sure that you choose the correct target version of SAP S/4HANA for the "SAP Readiness Check" report.

Download the "Simplification Item Catalog" from the download site "Simplification Item Catalog":

- [SAP Simplification Catalog](#) - Make sure to use the correct version for the planned S/4HANA conversion target.

Instruction videos and guidance on how to set up and run the "SAP Readiness Check" are provided in the following section.

Associated SAP notes and documentation for the SAP readiness check

- The central SAP documentation landing page for the "SAP Readiness Check": [SAP Tutorial overview - SAP Readiness Check for SAP S/4HANA](#)
- Overview video tutorial for the "S/4HANA Readiness Check" tool: [SAP Video Tutorial - SAP Readiness Check for SAP S/4HANA](#)
- The SAP Readiness Check Analysis Upload Page: [SAP Readiness Analysis Upload page](#)
- The central SAP Note for the "SAP Readiness Check" for SAP S/4HANA: [SAP Note 2913617 - SAP Readiness Check for SAP S/4HANA](#)
- Instructions about how to solve authorization issues: [SAP Note 3310759 - Revised Authorization Concept for SAP Readiness Check](#)
- Important updates for the SAP Notes Assistant (Mandatory): [SAP Note 1668882 - Note Assistant: Important notes for SAP BASIS 730, 731, 740, 750, ...](#) and [SAP Note 2971435 - SNOTE - Delta calculation Issue when 'mod unit' positions are changed](#)

Compare business data before the SAP migration

Use the Data Transition Validation (DTV) tool to compare business data before and after a system conversion from SAP ECC to SAP S/4HANA. It can also serve as a data validation check during updates and upgrades.

Sizing the target SAP system

It is highly recommended that you implement the most recent SAP patches for SPAM, ST-PI, ST/A-PI on the source system. These updates contain the most recent version of the ABAP sizing reports.

To view the current SAP version, start an SAP GUI session:

1. Log in to the SAP GUI.
2. Use SAP Transaction "SPAM" to see the Support Package Manager version.
3. Record the version number and collect the version numbers for the additional software.
4. Click **System**, then select **Status** when the dialog box appears.
5. Go to **SAP System Data**.
6. Click the magnifying glass and
7. Click the **Installed Software Component Versions** tab and check for the following components: * ST-PI * ST-A/PI
8. Compare the current version with the new versions that are available for download by using [Tools For Support Service Sessions](#).

Sizing considerations for the brownfield approach

 **Tip:** SAP recommends that you archive as much data as possible from the source database before you start the conversion to SAP S/4HANA.

Use the following steps to determine the version of the "ABAP HANA Sizing report" that is installed on your source system.

1. Log in to the SAP GUI.
2. Use the SAP Transaction "SE38".
3. Select report [/SDF/HDB_SIZING](#).
4. Leave the "Subobjects" field to "Source Code".
5. Click **Display**.
6. Check the "VALUE" that is in Line 10. This value is of the current report version.

You can use the ABAP Sizing report to correctly size for brownfield configurations. For more information, see [SAP Note 1872170 - ABAP on HANA sizing report \(S/4HANA, Suite on HANA\)](#).

The following link demonstrates how to run a sizing report:

- [How to install and run the ABAP on HANA Sizing report](#)

Consider the system growth factors, the data-aging residence time in days, and the maximum age of database statistics. They are the typical criteria in the report to plan for system growth.

After the report is complete, it displays the recommended core, memory, SAPS, and storage requirements for your target system. Use the following links to compare the SAP Sizing report recommendations with the current IBM Power Virtual Server profile offerings and select the profile that aligns with the sizing report recommendation.

- [SAP Note 2947579 - SAP HANA on IBM Power Virtual Servers\)](#)
- [IBM Power Virtual Server certified profiles for SAP HANA IBM® Power® Virtual Server](#)

SAP maintains a list of certified and supported SAP HANA® hardware. Certified IBM Power Virtual Server profiles and certified IBM server hardware are listed in the [SAP Certified and Supported SAP HANA® Hardware Directory](#).

Source database health

Database consistency is an important part of the pre-migration step because issues with the source database can break the migration process. Your source database needs to be checked for inconsistencies, fragmentation, and general health in advance. Review the existing migration documentation for your database software version and implement all required checks.

Preparing the target system landscape

Use the following steps to prepare the target system landscape.

1. Access the most recent version of "Database Migration Option: Target Database SAP HANA" from [Database Migration Option: Target Database SAP HANA](#), then select **Download Link**.



Note: This migration scenario uses the "System Move" option. A single stack SAP Netweaver DB/Application is moved to a separate S/4HANA 2023 Application Server and a dedicated server for the SAP HANA database.

2. Make sure that an active network connection between source and target systems with sufficient line speed is available. [Hybrid Cloud](#)

[Network Considerations for SAP applications on IBM® Power® Virtual Server](#). Keep in mind that SAP demands a network latency less than 20 ms, and a bandwidth higher than 400 Mbps for this migration scenario.

Requirements for using the system move option

See the following requirement for using System Move.

- Install the target database and target PAS before you start the migration.
- Make sure that both target systems use a different <SID>. For example, if <DB_SID> is assigned to the target SAP HANA database, the target application server must then use a different ID like <AS_SID>.
- During a "DMO with System Move" run, dump files are created in the SUM folder. These files contain the source database data and tables in compressed form.
 - The dump files are transferred from the source to the target system in a later step.
 - Because the entire source database is exported, make sure that enough free disk space is available on both systems.

Source database is Oracle - suppressing long-running phases in SUM

During the update with DMO, the EU_CLONE_DT_SIZES and EU_CLONE_UT_SIZES phases can be long-running.

In these phases, the system updates the database statistics. Correct statistics for table space usage helps to better distribute the tables during the system cloning. Before the update is started, follow this procedure to suppress long-running phases:

1. Log in to the host where the Oracle database instance is running. Use user <ora<dbsid>> for UNIX™ system or user <sapsid>adm for Windows™.
2. Open a command line and run the following command:

```
$ brconnect -u / -c -f stats -o <schema_owner> -t all -f allsel,collect,space -p <Number of Processors>
```

The <-p> flag defines the number of CPU processors that your hardware has, if the source system has, e. g. 8 processors, then the value needs to be changed to 8. To find the schema owner, use the following SQL statement in <sqlplus>.

```
SQL> select username from dba_users;
```

This query provides all database usernames. For ABAP systems, the common schema owner is typically <SAPSR3>.

The following SQL query lists the database schemas:

```
SQL> select distinct owner from dba_objects;
```

3. The file <SAPup_add.par> is located in the <bin> subdirectory of the SUM folder. It is typically part of the "Software Update Manager" archive.
4. Add the following line to the file <SAPup_add.par>:

```
/ORA/update_spacestat = 0
```

If the <SAPup_add.par> file does not exist yet, create one.

Checking database parameterization for source Oracle databases

If your source database is Oracle, make sure that the database parameterization is properly configured regarding parameter parallel_max_server. For more information, see [SAP Note 936441 - Oracle settings for R3load based system copy](#).

Index-organized tables for source Oracle databases

The following information is about Oracle index-organized tables.

The "Database Migration Option" is able to work with index-organized tables on the source database Oracle. The primary key is used to split index-organized tables automatically. No special action or preparatory activity is necessary from your side. For more information about index-organized tables, check this SAP Note:

- [SAP Note 641435 - FAQ: Oracle index-organized tables \(IOTs\)](#)

Make sure that the release version and the patch level of the SUM tools are identical in both the source and the target system.

- Download the same SUM version for both systems, even if different operating system platforms are involved.
- Check that the most recent version is used on source and target SAP systems.

POC project SAP system landscape

This description is based on a proof of concept (POC) project. The project migrates to two target SAP servers in IBM Power Virtual Server:

- IBM Power Systems Virtual Server - model S1022 for the S/4HANA Application Layer
- IBM Power Systems Virtual Server - model E1080 for the HANA Database Layer

Both Servers are provisioned with the recommended values that are outlined in the SAP HANA sizing report, and installed with the OS RHEL 9x. Storage Architecture and configuration are aligned with the current TDI recommendations.

Details for SAP HANA and supported Operating Systems including RHEL and SLES. The second SAP Note also includes recommended OS settings for both product versions. You can apply settings manually or automatically by running an Ansible™ playbook on IBM Power Virtual Servers. For SAP HANA on RHEL 9, SAP recommends the following OS settings:

- [SAP Note 2235581 - SAP HANA: Supported Operating Systems](#)
- [SAP Note 3108302 - SAP HANA DB: Recommended OS Settings for RHEL 9](#)

Before you can start the installation of the most recent GA version of SAP HANA Database, you need to make sure that the required GCC compiler is installed on the OS. If the correct Compiler version isn't installed, the SAP HANA Database installation experiences errors.

If you plan to install SAP HANA database version 2.00.082, a newer compiler version is needed. For more information, see [SAP Note 3449186 - Linux: Running SAP applications compiled with GCC 13.x](#).

For earlier versions of the SAP HANA Database, see [SAP Note 3216146 - Linux: Running SAP applications compiled with GCC 11.x](#).

Next steps before installing the SAP HANA database

Before you install SAP HANA Database, make sure that you perform the following items.

- Configure storage
- Apply OS recommendations
- Prepare the target servers
- Test network connectivity between both source and target servers

In the next phase, the stack and software packaging XML file is required, which defines two things:

- Which upgrades are required on the source SAP system.
- Which software stack to apply to prepare the target servers.

Using SAP Maintenance Planner to create the system software stack

If the source system is already registered in the SAP "Solution Manager Landscape", continue with the next section.

If the current SAP server is not registered in a Solution Manager environment, use SAP Maintenance Planner to update the software stack information from the source SAP server with these steps:

1. Start a dialog session on the SAP source system.
2. Use SAP Transaction "SPAM".
3. Select **Utilities** from the menu.
4. Click **Generate System information XML**.
5. Save the XML file with name `sysinfo_<SID>`.



Note: The XML file contains all details of installed software levels and SAP modules currently in your system.

6. Open the [SAP Maintenance Planner](#) website.
7. Click **Access Maintenance Planner**, which opens the [SAP Maintenance Planner](#).
8. In the **Plan and Execute** section, click **Explore Systems**.
9. If the system is not on the list, click **Add System**.

10. Accept the SAP advisory and click **Next**.
11. Use browse in the **Select System Information XML** section and upload the system XML file that was generated in the previous section.
12. Click **Next** after the system message "Valid system information XML, choose Next" appears.
13. Double check the *SID*, *Host*, and *System Type* and click **Next**.
14. If a question why the system was manually uploaded occurs, verify whether "no active SAP SOLMAN in the landscape" is a valid answer in your environment.
15. Click **OK**. The system appears in the **Explore Systems** list.

Creating the maintenance plan

Use the instructions that are outlined in the following links to create your maintenance plan for your conversion to S/4HANA.

1. Follow the steps that are in the [SAP Maintenance Planner - Central Repository](#).
2. Use the [Manual Conversion to SAP S/4HANA System](#) as a guide.



Tip: Consider that in the scenario of an OS/DB migration you need the OS-dependent files for source and your target systems. Remember to include all relevant software packages for the conversion to S/4HANA.

Backing up the source SAP system

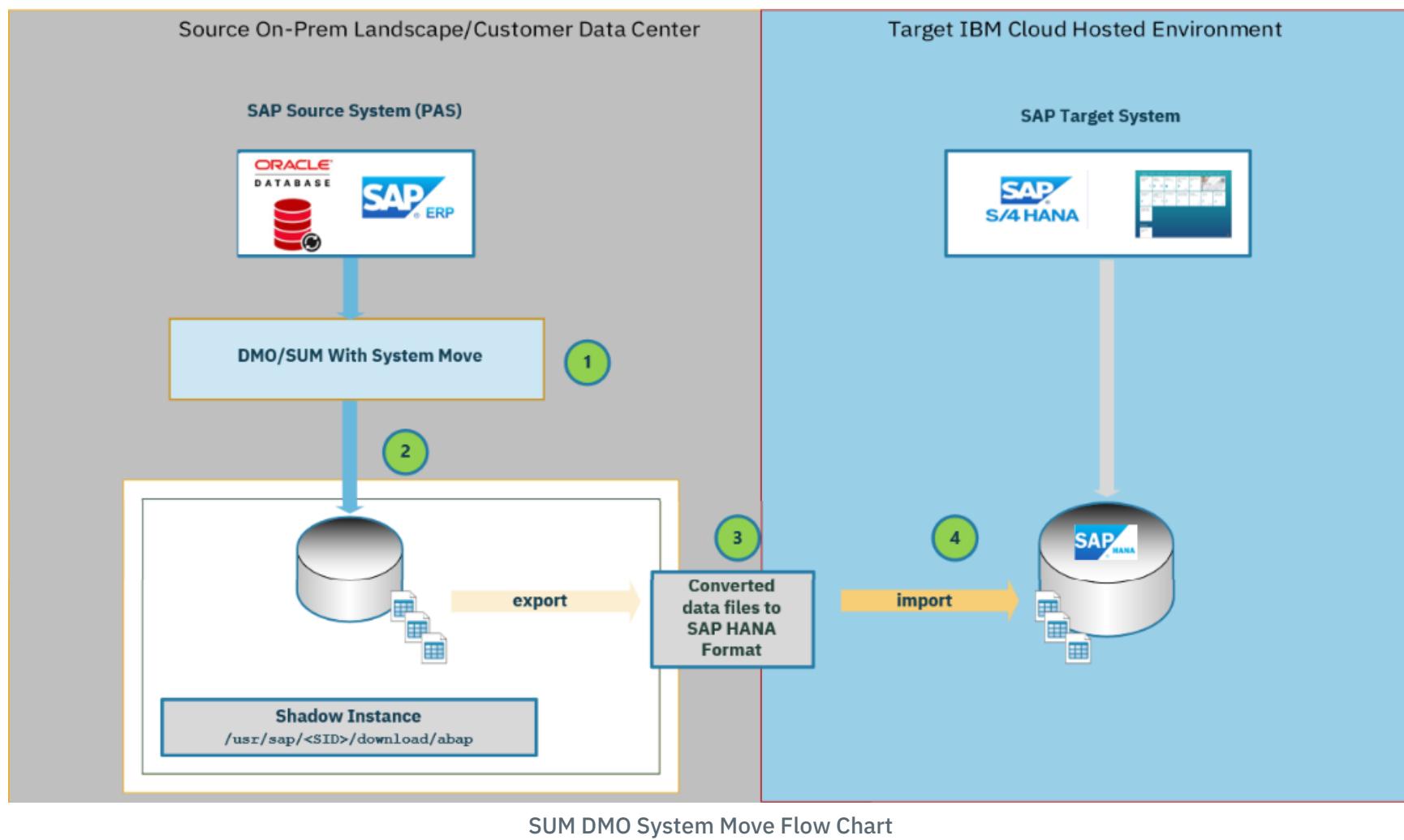
Backup the source SAP system before the SAP migration is started by using the following steps.

1. Create a full database backup (preferably an offline backup).
2. Back up your SAP Profiles (`DEFAULT.PFL`, `Dxx`, and `ASCSXX`) to a backup directory.
3. Create a backup folder in the `/home/<sid>adm` directory.
4. Copy all SAP and AnyDB environment files to the backup folder, including the following files.
 - `.profile`
 - `.sapenv.*`
 - `.dbenv.*`
 - `.sapsrc_<hostname>.*`

Enabling DMO with system migration

See the following overview for the SAP "System Move": Enabling DMO with System Migration

[Enabling DMO with System Move](#)



Legend

- As sidadm user, start SUM - Scenario DMO Without System Update - Standard Configuration.
- DMO initiates the cloning of the source DB files to the shadow instance.
- Converted files are then exported.
- Import the SAP HANA Format files into the Target SAP HANA Database. SUM/DMO drops the shadow instance upon export/import completion.

Post-migration actions

Comparing Business Data before and after conversion from SAP ERP (ECC) to SAP S/4HANA:

- [SAP Note Data Transition Validation \(DTV Tool\)](#)

Post Activities must include an assessment and acceptance phase.

The following link provides an overview of follow-up activities to complete after a successful migration.

- [DMO - Follow Up Activities Section](#)

One of the follow up activities is [Backing up the SAP HANA Database](#). Include a label that indicates a post DMO backup for both backups:

- Full SAP HANA SYSTEMDB database backup
- Full SAP HANA MDC database backup

For additional information on enabling or disabling HANA encryption, including backup encryption, refer to: [SAP Note 3498202 - Enabling or Disabling HANA Encryption](#)

For encrypted backups of SYSTEMDB or MDC, create a backup of the *ROOT ENCRYPTION KEYS* to a secure location. Without these keys, a backup cannot be restored. The SAP documentation describes how to [Back Up Root Keys](#).

Compare business data after migration

Comparison of business data after conversion from SAP ERP (ERP) to SAP S/4HANA:

- [SAP Note Data Transition Validation \(DTV Tool\)](#)

Perform SQL optimizations

The SQL Monitor grants transparency on all ABAP functions that run SQL statements. Use SQL Monitor to find any SQL performance-related issues, and to identify areas and statements that you can optimize. For more information, see [SQL Monitor](#).

Links for the database migration option

DMO user guides for different target database systems are available.

- [Database Migration Option of Software Update Manager 2.0](#)
- [SAP Note 1912445 - ABAP custom code migration for SAP HANA - recommendations](#)

Links for the SAP Software Update Manager data migration option

- [Database Migration Option: Target Database SAP HANA](#)
- [SAP Note 3474707 - Database Migration Option \(DMO\) of SUM 2.0 SP21](#)
 - This SAP Note contains prerequisites for source and target SAP systems. The version of the SAP Software Update Manager depends on the target SAP system version. Restrictions and in-depth information about the available types of DMO options are explained.
 - The "attachment" section contains a PDF file worth mentioning. It contains a PDF file that graphically shows SAP supported update and upgrade paths.
- [SAP Note 3391209 - Central SAP Note Software Update Manager 2.0 SP20](#)
- [SAP Note 2547309 - Downtime-optimized DMO with SUM 2.0](#)

Extra DMO information

The following links provide extra DMO information



Note: An SAP S-User access is required to access the following links.

- [Database Migration Option \(DMO of SUM in a nutshell\)](#)
- *Downtime-Optimized DMO: Introduction* PDF file attached to [SAP Note 2547309 - Downtime-optimized DMO with SUM 2.0](#)

The following document outlines the DMO steps for a migration of an SAP system from anyDB to an SAP HANA Database.

- [Database Migration Option: Target Database SAP HANA](#)
- [Software Logistics Toolset](#)

Links for sizing SAP servers

For reference only, the new sizing report for SAP BW/4HANA:

- [SAP Note 2296290 - New Sizing Report for SAPBW/4HANA](#)

The official SAP sizing webpage:

- SAP [Sizing](#) webpage

Monitoring

Automating SAP workload HA deployment on IBM Cloud VPC with Terraform and Ansible

You can use Terraform to automate IBM Cloud® VPC provisioning. The VPC provisioned includes virtual server instances with high network performance. The VPC infrastructure contains various Infrastructure-as-a-Service (IaaS) offerings, including virtual servers. After the VPC is provisioned, the scripts use the Ansible Playbooks to install the SAP system.

IBM Cloud VPC introduction

VPC is a public cloud offering that an enterprise uses to establish its own private cloud-like computing environment on shared [public cloud](#) infrastructure. VPC gives an enterprise the ability to define and control a virtual network that is logically isolated from all other public cloud tenants, creating a private and secure place on the public cloud.

Imagine that a cloud provider's infrastructure is a residential apartment building and multiple families live inside. A public cloud tenant is a kind of sharing an apartment with a few roommates. In contrast, having a VPC is like having your own private condominium; no one else has the key, and no one can enter the space without your permission.

VPC's logical isolation is implemented by using virtual network functions and security features that give the enterprise customer granular control over which IP addresses or applications can access particular resources. It is analogous to the "friends-only" or "public/private" controls on social media accounts used to restrict who can or can't see your otherwise public posts.

With IBM Cloud VPC, you can use the UI, CLI, and API to manually provision virtual server instances for VPC with high network performance. VPC infrastructure contains various Infrastructure-as-a-Service (IaaS) offerings including virtual servers for VPC.

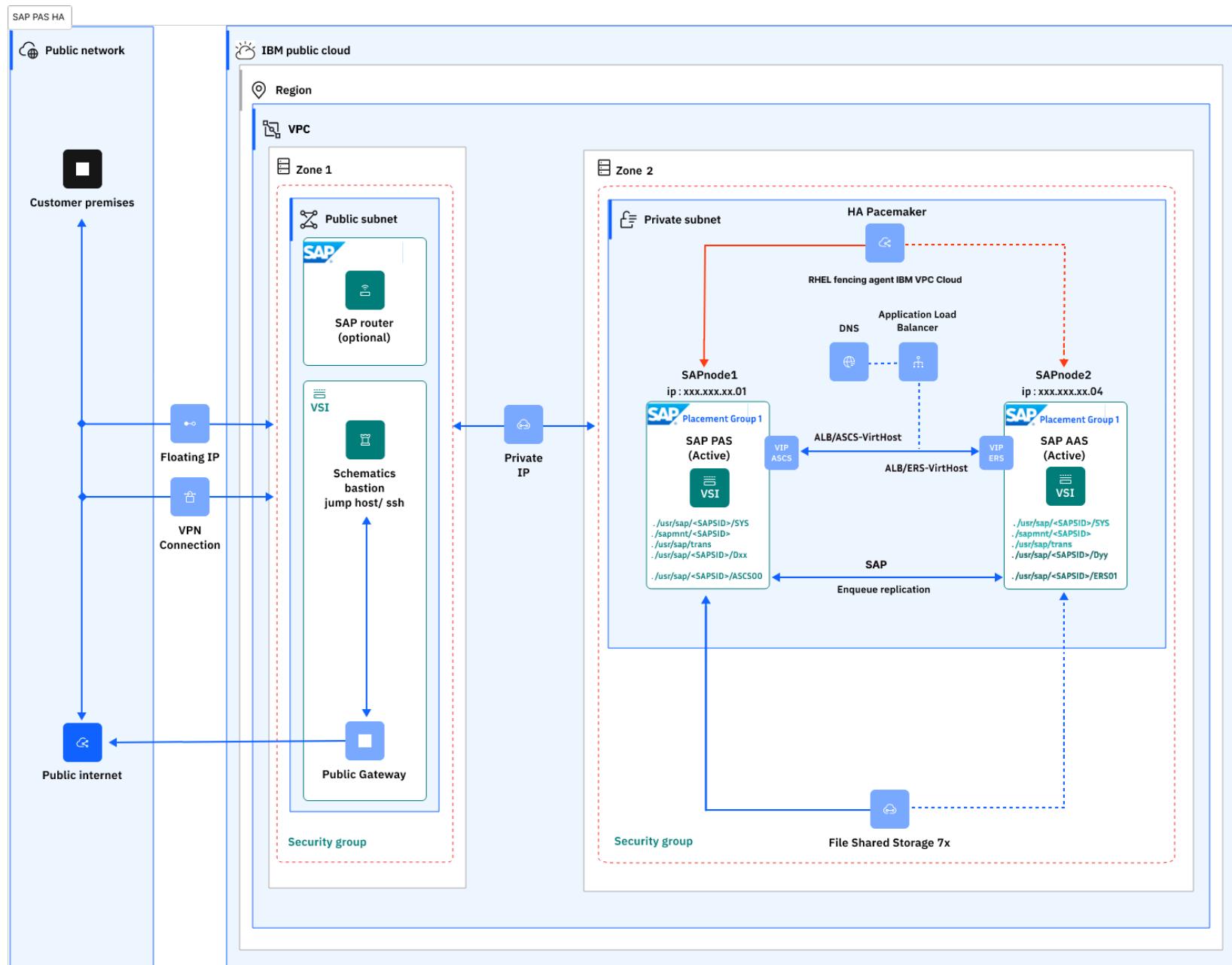
Use the following information to understand a simple use-case for planning, creating, and configuring resources for your VPC, and learn more about VPC overviews and VPC tutorials. For more information about the VPC, see [Getting started with Virtual Private Cloud \(VPC\)](#).

SAP products architecture on IBM Cloud VPC

A [Virtual Private Cloud \(VPC\)](#) contains one of the most secure and reliable cloud environments for SAP applications within your own VPC with virtual server instances. This represents an Infrastructure-as-a-Service (IaaS){: external} within IBM Cloud that offers all the benefits of isolated, secure, and flexible virtual cloud infrastructure from IBM. In comparison, the IBM Cloud classic infrastructure virtual servers offering uses virtual instances with native and VLAN networking to communicate with each other within a data center; however, the instances are restricted in one well-working pod by using subnet and VLAN networking as a gap scale up of virtual resources should rely between the pods. The IBM Cloud VPC network orchestrator layer concept eliminates the pod boundaries and restrictions, so this new concept handles all the networking for every virtual instance running within VPC across regions and zones.

Highly available system for SAP NetWeaver on IBM Cloud VPC

In a Highly Available (HA) system, every instance can run on a separate IBM Cloud virtual server instance. The cluster HA configuration for the SAP application server consists of two virtual server instances, each of them located in the same zone within the region by using placement groups. Placement groups assure that both cluster resources and cloud resources are also located in different compute nodes as specified in the following placement groups section:



SAP HA for SAP applications cluster nodes PAS (Active) and AAS (Active)

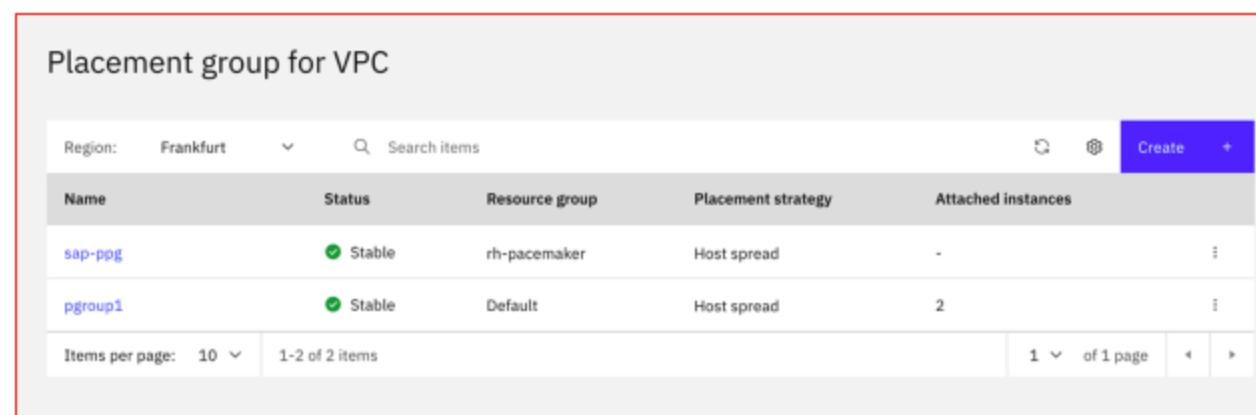
Placement groups on IBM Cloud VPC for SAP HA architecture

Placement Groups (PG) for VPC have two different anti-affinity strategies for high availability. By using the placement strategies, you minimize the chance of service disruption with virtual server instances that are placed on different hosts or into an infrastructure with separate power and network supplies.

The design of placement groups for IBM Cloud virtual servers solves this issue. Placement groups give a measure of control over the host on which a new public virtual server is placed. In this release, a “spread” rule is implemented, which means that the virtual servers within a placement group are spread onto different hosts. You can build a highly available application within a data center and know that your virtual servers are isolated from each other.

Placement groups with the spread rule are available to create in selected IBM Cloud data centers. After a spread rule is created, you can provision a virtual server into that group and ensure that it is not on the same host as any of your other virtual servers. This feature comes with no cost.

You can create your placement group and assign up to four new virtual server instances. With the spread rule, each of your virtual servers are provisioned on different physical hosts. In the following configuration example, the “Power Spread” option is used:



Placement groups host spread

Placement group for VPC					
Name	Status	Resource group	Placement strategy	Attached instances	
sapha-poc	Stable	wes-ic4sap-resourcegroup	Power spread	4	
Items per page: 10 1 item 1 of 1 page					

Placement groups power spread

Following are the SAP instances that are required for HA scenario:

- ABAP SAP Central Services (ASCS) instance - contains the ABAP message server and the ABAP enqueue server.
- Enqueue Replication Server (ERS) instance for the ASCS instance.
- Database instance
- Primary Application Server (PAS) instance on node 1.
- Additional Application Server (AAS) instance on node 2.



Note: It is recommended to run both the ASCS instance and the ERS instance in a switchover cluster infrastructure.

IBM Cloud File Storage for VPC for SAP HA architecture

[IBM Cloud File Storage for VPC](#) technology is used to make the SAP directories available to the SAP system. The technologies of choice are NFS, shared disks, and cluster file system. If you have decided to use the HA solution for your SAP system, make sure that you properly address the HA requirements of the SAP file systems in your SAP environment.

File shares for VPC								
Name	Status	Resource groups	Location	Mount targets	Size	Replication role	Encryption type	
usrsap-as1-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-as2-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-sapscs-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-sapers-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-sapmnt-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-sapsys-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	20 GB	None	Provider managed	
usrsap-trans-poc	Stable	wes-ic4sap-resourcegroup	Frankfurt 2	1	80 GB	None	Provider managed	

File shares for VPC

- File shares that are mounted as NFS permanent file systems on both cluster nodes for SAP HA application:
 - `/usr/sap/<SAPSID>/SYS`
 - `/sapmnt<SAPSID>`
 - `/usr/sap/trans`
- Cluster-managed file systems for SAP HA application: ASCS
 - `/usr/sap/<SAPSID>/ASCS00`
 - `/usr/sap/<SAPSID>/ERS01`
- Permanent NFS mount on SAP HA application node 1 PAS instance:
 - `/usr/sap/<SAPSID>/Dxx`
- Permanent NFS mount on SAP HA application node 2 dialog instance:
 - `/usr/sap/<SAPSID>/Dyy`

Prerequisites

You need to install the hardware (hosts, disks, and network) and decide how to distribute the database, SAP instances, and if required, the Network File System (NFS) server over the cluster nodes.

Context

Following are the types of SAP directories:

- Physically shared directories: `/<sapmnt>/<SAPSID>` and `/usr/sap/trans`

- Logically shared directories that are bound to a node, such as `/usr/sap`, with the following local directories:
 - `/usr/sap/<SAPSID>`
 - `/usr/sap/<SAPSID>/SYS`
 - `/usr/sap/hostctrl`
- Local directories that contain the SAP instances such as `/usr/sap/<SAPSID>/ASCS<Instance_Number>`
- The global transport directory may reside on a separate SAP transport host as a standard three systems transport layer configuration.

You need at least two nodes and a shared file system for distributed ASCS and ERS instances. The assumption is that the rest of the components are distributed on other nodes.

ASCS and ERS installation

In order for the ASCS and ERS instances to be able to move from one node to the other, they need to be installed on a shared file system and use virtual hostnames based on the virtual IP.

In this VPC-based SAP HA solution, the shared file system that is required by the cluster is replaced by the NFS-mounted file storage, and the virtual IP is replaced by the Application Load Balancer for VPC (ALB).

In this scenario, three ALBs are used, one for each Single Point of Failure (SPOF) component in order to replace the virtual IP requirement: ALB for ASCS, ALB for ERS, and ALB for ASE Sybase. Each ALB is configured as a backend for the corresponding cluster servers and redirects all of the communication that is received on the front-end ports to the active server in the backend pool.

Load balancers for VPC						
Region:	Frankfurt	▼	Search: poc	X		
Name	Status	Family	Resource group	Type	Hostname	Location
db-alb-hana-poc	Active	Application	wes-ic4sap-resourcegroup	Private	20bdd130-eu-de.lb.appdomain.cloud	Frankfurt
sap-alb-ers-poc	Active	Application	wes-ic4sap-resourcegroup	Private	3941d983-eu-de.lb.appdomain.cloud	Frankfurt
sap-alb-ascs-poc	Active	Application	wes-ic4sap-resourcegroup	Private	56a9190d-eu-de.lb.appdomain.cloud	Frankfurt

Application load balancer management of HA IPs mechanism

Private application load balancer

A [private application load balancer](#) is accessible through your private subnets that you configured to create the load balancer.

Similar to a public application load balancer, your private application load balancer service instance is assigned an FQDN; however, this domain name is registered with one or more private IP addresses.

IBM Cloud operations change the number and value of your assigned private IP addresses over time, based on maintenance and scaling activities. The backend virtual server instances that host your application must run in the same region and under the same VPC.

Use the assigned ALB FQDN to send traffic to the private application load balancer to avoid connectivity problems to your applications during system maintenance or scaling down activities.

Each ALB sends traffic to the cluster node where the application (ASCS, ERS, ASE Sybase DB) is running. During the cluster failover, the ALB redirects all the traffic to the new node where the resources are up and running.



Note: DNS-as-a-Service (DNSaaS) is the management IBM Cloud VPC DNS service of HA and FQDN (IPs) mechanism.



Note: The ALB has a default of 50 seconds for client and server timeout, so after 50 seconds of inactivity, the connection is closed. To support SAP connections through ALB and not lose connection after 50 seconds, you need to request a change this value to a minimum of 300 seconds (client-side idle connection = minimum 300s and server-side idle connection = minimum 300s). To request this change, open a support ticket. This is an account-wide change that affects all of the ALBs in your account. For more information, see [Connection timeouts](#).

DNS Services with VPC

[IBM Cloud DNS Services](#) provide private DNS to VPC users. Private DNS zones are resolvable only on IBM Cloud and from explicitly [permitted networks](#) in an account. To get started, create a DNS Services instance by using the IBM Cloud console.

DNS Services allows you to:

- Create the private DNS zones that are collections for holding the domain names.
- Create the DNS resource records under these DNS zones.
- Specify the access controls used for the DNS resolution of resource records on a zone-wide level.

DNS Services also maintains its own worldwide set of DNS resolvers. Instances that are provisioned under IBM Cloud on an IBM Cloud network can use resource records that are configured through IBM Cloud DNS Services by querying DNS Services resolvers.

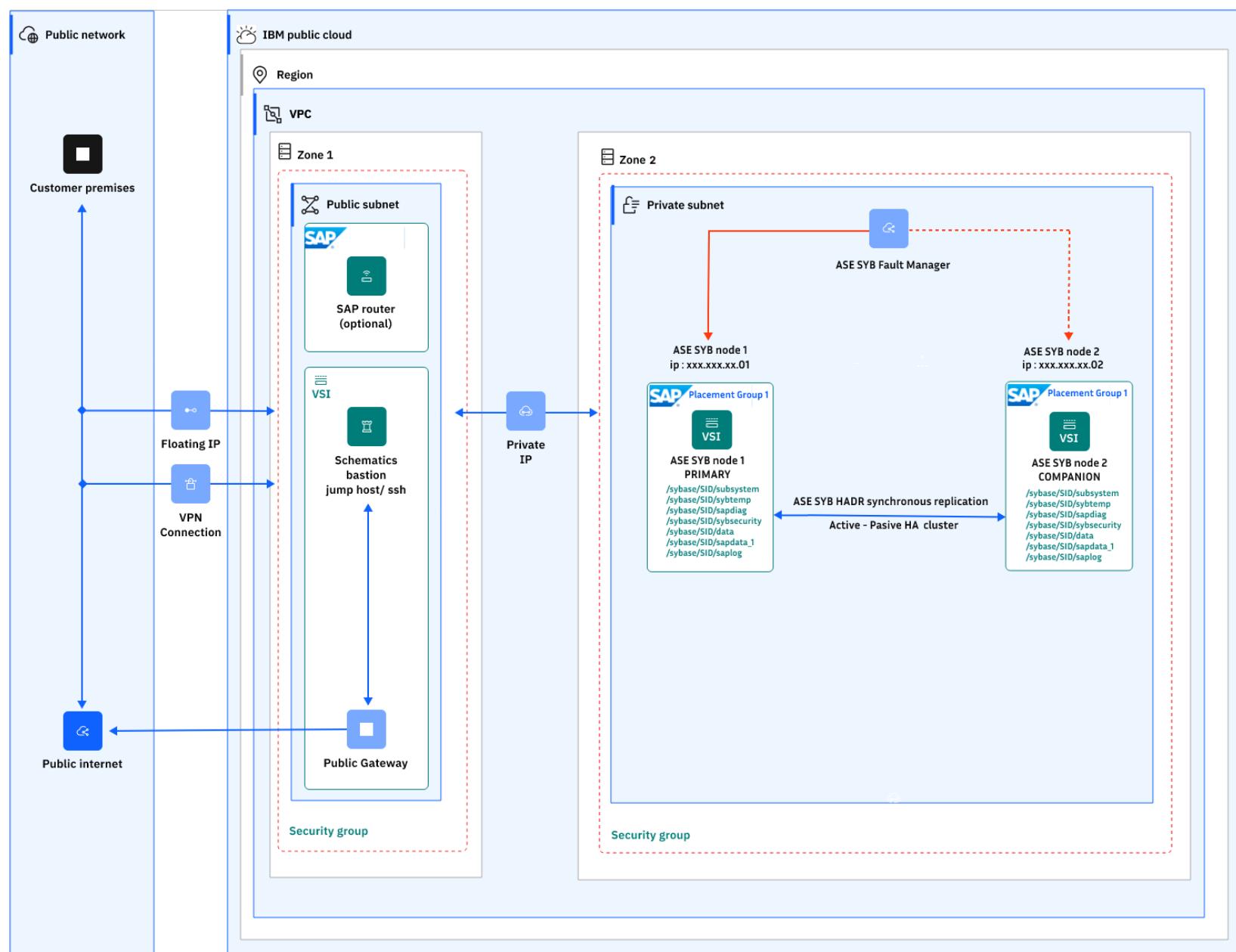
Resource records and zones that are configured through DNS Services are:

- Separated from the wider public DNS, and their publicly accessible records.
- Hidden from the system outside of and not part of the IBM Cloud private network.
- Accessible only from the system that you authorize on the IBM Cloud private network.
- Resolvable only via the resolvers provided by the service.

The DNS service maps the FQDN of each ALB to the virtual hostnames of the ASCS, ERS, and ASE Sybase that are used by SAP applications.

Type	Name	Value	TTL
CNAME	dbpochana	is an alias of 20bdd130-eu-de.lb.appdomain.cloud	12 hr
CNAME	sappocers	is an alias of 3941d983-eu-de.lb.appdomain.cloud	12 hr
CNAME	sappocases	is an alias of 56a9190d-eu-de.lb.appdomain.cloud	12 hr

Highly available system for SAP ASE Sybase database with HADR system



SAP HA for ASE Sybase DB instances cluster nodes primary (Active) and Secondary (Companion)

At the most basic level, a standard HA ASE Sybase cluster in an active(primary)-passive(companion) configuration has two nodes: one is the primary node and the other is the standby node. This means that the primary node is actively serving the active SAP DB instances (Primary and Companion), while the standby node is waiting to jump in if there is any failure.

The cluster is set with a virtual hostname IP (hostname is mapped to the FQDN of the ASE Sybase ALB through DNS, which is the same as

explained previously for SAP ASCS and ERS instances). Application instances (PAS and AAS) are used on the SAP profiles to call that particular component. The cluster assigns the virtual IP to the active node and uses a heartbeat monitor to confirm the availability of the components. If the primary node stops responding, it triggers the automatic failover mechanism that calls the standby node to step up to become the primary node. The ALB detects the change, redirects the traffic to the new active node, and assigns the virtual IP to it, restoring the component availability. Once fixed, the failed node comes online as a standby node.

SAP Sybase HADR system supports synchronous replication

The SAP Sybase HADR system supports synchronous replication between the primary and standby servers for high availability. An active-active setup is a two-node configuration where both nodes in the cluster include SAP ASE managing independent workloads, capable of taking over each others workload in the event of a failure.

The SAP ASE server that takes over the workload is called a secondary companion, and the SAP ASE server that fails is called the primary companion. Together they are companion servers. This movement from one node to another is called failover. After the primary companion is ready to resume its workload, it is moved back to its original node. This movement is called a failback.

When a system fails over, clients that are connected to the primary companion and use the failover property automatically reestablish their network connections to the secondary companion. You must tune your operating system to successfully manage both servers during fail over. See your operating system documentation for information about configuring your system for high availability. An SAP ASE configured for failover in an active-active setup can be shut down using the shutdown command only after you have suspended SAP ASE from the companion configuration, at both the server level and the platform level.

The always-on option in a High Availability and Disaster Recovery (HADR) system consists of two SAP ASE servers:

- Primary on which all transaction processing takes place.
- Warm standby (referred to as a "standby server" in DR mode, and as a "companion" in HA mode) for the primary server, and contains copies of designated databases from the primary server.



Note: The HADR feature that is shipped with SAP ASE version 16.0 SP02 supports only a single-companion server.

Some high-availability solutions (for example, the SAP Adaptive Server Enterprise Cluster Edition) share or use common resources between nodes. However, the HADR system is a "shared nothing" configuration, each node has separate resources including disks.

In an HADR system, servers are separate entities and data is replicated from the primary server to the companion server. If the primary server fails, a companion server is promoted to the role of primary server either manually or automatically. Once the promotion is complete, clients can reconnect to the new primary server, and see all committed data, including data that was committed on the previous primary server.

Servers can be separated geographically, which makes an HADR system capable of withstanding the loss of an entire computing facility.



Note: The HADR system includes an embedded SAP Replication Server, which synchronizes the databases between the primary and companion servers. SAP ASE uses the Replication Management Agent (RMA) to communicate with Replication Server and SAP Replication Server uses Open Client connectivity to communicate with the companion SAP ASE.

The Replication Agent detects any data changes made on the primary server and sends them to the primary SAP Replication Server. In the figure above, the unidirectional arrows indicate that, although both SAP Replication Servers are configured, only one direction is enabled at a time.

The HADR system supports synchronous replication between the primary and standby servers for high availability so the two servers can keep in sync with Zero Data Loss (ZDL). This requires a network link that is fast enough between the primary and standby server so that synchronous replication can keep up with the primary servers workload. Generally, this means that the network latency is approximately the same speed as the local disk IO speed, a few (fewer than 10) milliseconds. Anything longer than a few milliseconds may result in a slower response to write operations at the primary.

The HADR system supports asynchronous replication between the primary and standby servers for disaster recovery. The primary and standby servers by using asynchronous replication can be geographically distant, meaning they can have a slower network link. With asynchronous replication, Replication Agent Thread captures the primary servers workload, which is delivered asynchronously to SAP Replication Server. The SAP Replication Server applies these workload change to the companion server.

The most fundamental service that is offered by the HADR system is the failover; planned or unplanned from the primary to the companion server, which allows maintenance activity to occur on the old primary server, while applications continue on the new primary.

The HADR system provides protection in the event of a disaster. If the primary server is lost, the companion server can be used as a replacement. Client applications can switch to the companion server, and the companion server is quickly available for users. If the SAP Replication Server was in synchronous mode before the failure of the primary server, the Fault Manager automatically initiates failover with

zero data loss.

Fault Manager installation on the SAP ASCS node

The required parameters are asked during the installation process to create a profile for the fault manager and then adds it to the instance start profile. It is also possible to run the installation by using an existing profile: `sybdbfm install pf=<SYBHA.PFL>` In this case, the installation process will only ask for profile parameters missing in the profile.



Note: Fault manger is integrated with ASCS on same SAP PAS/AAS cluster (start/stop/move together).

There may be some data loss if the SAP Replication Server was in asynchronous mode and you must use manual intervention to failover for disaster recovery.

Connection attempts to the companion server without the necessary privileges are silently redirected to the primary companion via the login redirection mechanism, which is supported by Connectivity libraries. If login redirection is not enabled, client connections fail and are disconnected.

The SAP ASE HADR option installs the below components:

- SAP ASE
- SAP Replication Server
- Replication Management Agent (RMA)
- SAP Host Agent
- Fault Manager
- SAP ASE Cockpit



Note: This automation is offered at no cost; however, the provisioned infrastructure comes at cost.

Prerequisites



Note: Prerequisite is a running SAP HANA system. This guide doesn't detail the installation of SAP HANA database and SAP NetWeaver solution.

This document outlines the necessary steps a user must follow to successfully implement a monitoring solution for SAP.

Gather SAP parameters

Gather the below parameter values from an existing SAP system running in IBM cloud. These values are required by the [SAP HANA DB exporter](#) which will be installed and configured on the x86_64 Virtual Server Instance running in IBM Cloud VPC.

For more information, see [Determine SAP Parameters](#).

Parameters from HANA DB server

1. **IPv4 address** of the SAP HANA DB server.
2. [SQL access port](#) to the system database on the SAP HANA server.
3. [HTTP port](#) of the sapstartsrv web service on the SAP HANA server.
4. **SQL user credentials** of the system database. If you want to create a user with `ReadOnly` permissions, see [Creating a Read only system user](#)

Parameters from SAP NetWeaver server

1. **IPv4 address** of server where the SAP ASCS instance is running.
2. **IPv4 address** of server where the SAP PAS instance is running.
3. **IPv4 address** of server where the SAP AAS instance is running (if any).
4. [HTTP port](#) of the sapstartsrv web service on the server where the SAP ASCS instance is running (for ENQ and MSG services).
5. [HTTP port](#) of the sapstartsrv web service on the server where the SAP PAS instance is running.
6. [HTTP port](#) of the sapstartsrv web service on the server where the SAP AAS instance is running(if any).

The following port numbers will be exposed from the **x86_64 virtual server instance** running in IBM Cloud VPC which servers as a **monitoring**

host. The corresponding services are based on the [SAP HANA Database exporter](#) variables.

Exposed port numbers	Service description
5<sap_monitoring_nr>01	Prometheus agent
5<sap_monitoring_nr>02	hanadb_exporter
5<sap_monitoring_nr>03	sap_host_exporter for the SAP HANA database.
5<sap_monitoring_nr>04	sap_host_exporter for the ABAP Central Service (ASCS) server.
5<sap_monitoring_nr>05	sap_host_exporter is the primary or first SAP Application Server.
5<sap_monitoring_nr>06	sap_host_exporter is the second SAP Application Server.
5<sap_monitoring_nr>07	sap_host_exporter is the third SAP Application Server.

Exposed ports for services



Note: If you have multiple SAP systems, you need to differentiate between them. This means that you have to adjust the configuration file names. That is, the names of the `systemd` processes and the numbers of the locally exposed HTTP ports.

Check firewall settings on the SAP system

IBM Cloud® provides configured ACLs (Access Control Lists) and security groups for each subnet.

- On each SAP system, the local operating system firewall and SELinux/AppArmor are disabled by default.
- If the operating system firewall is enabled, check the firewall settings on each SAP system for SQL ports and SAP instance ports.
- If you decide to use the firewalld service, open the ports that are used on the SAP system and on the monitoring host(x86_64 Virtual Server Instance running in IBM Cloud VPC).
- Use the following commands to allow additional ports in the firewalld service.

```
$ firewall-cmd --zone=public --permanent --add-port ${port_number}/tcp
```

```
$ systemctl reload firewalld
```

Creating an SAP HANA database monitoring user with ReadOnly permission(Optional)

Skip this step if you already have a read only user and you are okay to use the same SAP HANA database user for monitoring role.

Do not use a user with administrator privileges for monitoring of the SAP HANA database.

To create a new SAP HANA database user with `ReadOnly` permissions for a monitoring role run the following commands

1. as the SAP HANA database system administrator user.
2. using the SAP HANA command line tool `hdbsql`.

For more information, see the section [Determine SAP Parameters](#).

```
$ CREATE USER <sap_hana_sql_systemdb_user> PASSWORD <sap_hana_sql_systemdb_password> \
NO FORCE_FIRST_PASSWORD_CHANGE;
CREATE ROLE HANADB_EXPORTER_ROLE;
GRANT MONITORING TO HANADB_EXPORTER_ROLE;
GRANT HANADB_EXPORTER_ROLE TO <sap_hana_sql_systemdb_user>;
```

Setting Up passwordless authentication for SAP monitoring

Configure your SAP System to allow the monitoring queries without user and password authentication.

By default, all `sapstartsrv` methods that can modify the status of an instance or the system are classified as protected methods. These

methods can only be executed after successful user authentication. To enable monitoring without authentication, configure the `sapstartsrv` service so that the methods required for monitoring queries are treated as unprotected.

```
SDEFAULT -GetQueueStatistic -ABAPGetWPTable -EnqGetStatistic -GetProcessList -GetEnvironment -ABAPGetSystemWPTable
```

Configure this setting for the following SAP instances:

- `HDB<ID>` on the SAP HANA database host
- `ASCS<ID>` on the SAP Application Server host
- `D<ID>` on all corresponding SAP Application Server hosts

Follow these steps for all `sapstartsrv` services.

1. List the instances and instance numbers.

```
$ /usr/sap/hostctrl/exe/lssap
```

2. Show the operating system user of the `sapstartsrv` service.

```
$ ps aux|grep sapstart
```

3. Switch the shell to `sapstartsrv` operating system user.

```
$ su - <OS-user of sapstartsrv>
```

4. List the configured web methods by using the instance numbers that were extracted with lssap.

```
$ sapcontrol -nr <ID> -function ParameterValue service/protectedwebmethods
```

5. If the output shows the following result,

```
SDEFAULT
```

then, the following configuration is required.

Add a line to the SAP default profile:

1. List the configuration files.

```
$ sapcontrol -nr <ID> -function ListConfigFiles
```

2. Edit the file named `/usr/sap/<sid>/SYS/profile/<sid>_<instance-name>_<host-name>`

3. Add a line at the end or change the existing line, if the entry `service/protectedwebmethods` exists.

```
#IBM SAP monitoring
service/protectedwebmethods = SDEFAULT -GetQueueStatistic -ABAPGetWPTable -EnqGetStatistic -GetProcessList -
GetEnvironment -ABAPGetSystemWPTable
```

4. Save the configuration file without changing the file name.

5. Restart the corresponding services.

```
$ sapcontrol -nr <ID> -function RestartService
```

The restart might take some time.

6. Check the status by running the following command.

```
$ sapcontrol -nr <ID> -function GetSystemInstanceList
```

The status shows `GREEN/ GRAY /YELLOW`.

If the service does not return to `GREEN`, see the troubleshooting section.

7. Verify that the configuration change was successful.

```
$ sapcontrol -nr <ID> -function ParameterValue service/protectedwebmethods
```

The following output is shown, if successful:

```
SDEFAULT -GetQueueStatistic -ABAPGetWPTable -EnqGetStatistic -GetProcessList -GetEnvironment -ABAPGetSystemWPTable
```

Next steps

After the prerequisites are met, you can proceed to the next step [Creating an IBM Cloud Monitoring Instance](#).

Creating an IBM Cloud Monitoring instance

Use the following information to create a monitoring instance.

Step 1: Managing user access

To get started with IBM Cloud® Monitoring for SAP systems, you need an IBM Cloud account and an [Administrator IAM role](#). For more information, see [Getting started with IBM Cloud® Monitoring](#).

Verify that the Virtual Routing and Forwarding (VRF) service endpoints are enabled in your Identity and Access Management (IAM) account settings. If VRF service endpoints are not enabled, enable the setting in your IAM account. For more information, see [Enabling VRF and service endpoints](#).

Step 2: Provisioning a IBM Cloud Monitoring instance

To create a IBM Cloud Monitoring instance by using the IBM Cloud UI, use the following steps. For more information, see [Provision an instance of the Monitoring service](#).

1. Log in to the [IBM Cloud® console](#).
2. Click **Navigation menu > Observability > Monitoring**.
3. Click **Create +**.
4. Select and complete the following settings for the monitoring instance:
 - Select the same location as the monitoring host and the deployed SAP systems.
 - Select the resource group of your deployable architecture (DA).
 - Enter a name or keep the default name.
 - Select the **Graduated Trier** pricing plan.
 - When you are ready to enable metrics, set the IBM platform metrics to **Enabled**.

Step 3: Collecting monitoring metrics

Retrieve the authorization credentials after you create the IBM Cloud Monitoring instance. These credentials will be used by the Prometheus remote write application running on **x86_64 VSI in IBM Cloud VPC** to send metrics data to the dashboard hosted on IBM Cloud Monitoring instance.

1. In the IBM Cloud® console, select **Observability > Monitoring** or go to [Monitoring](#).
2. Select your monitoring instance from the table and click **Open dashboard**.
3. Click **Get started**. Your credential values are in the dashboard.
4. Click **Optional: Connect your Prometheus Servers** to find the yaml-code with authorization credentials.
5. From this yaml code, you only need the URL value and the credentials values. The yaml code looks like the following example.

```
remote_write:  
- url: "https://ingest.prws.eu-de.monitoring.cloud.ibm.com/prometheus/remote/write"  
  authorization:  
    credentials: "123-abcdh-xxx-456"
```

6. In the URL, replace the string `ingest.prws` with `ingest.prws.private` as the private ingestion endpoint.

The new URL looks like the following example.

```
https://ingest.prws.private.<region>.monitoring.cloud.ibm.com/prometheus/remote/write
```

7. For a list of all private ingestion endpoints per region, refer to the IBM Cloud documentation that is described in [Collecting metrics by using Prometheus remote write](#).

Step 4: Next steps

Configure a monitoring host and send the SAP metrics data to the IBM Cloud® monitoring instance. For more information, see [Setting up and configuring a monitoring host](#).

Setting up and configuring a monitoring host

A monitoring agent collects the metrics from an SAP system and forwards them to the dashboard of the monitoring instance.

Deploying VPC virtual server instance host for a monitoring agent

Use Prometheus exporters to collect the metrics. The section about [Collecting metrics](#) explains details about metrics, labels, and monitoring agents.

The Prometheus exporter is based on the GitHub open source project [SAP HANA DB exporter](#).

Before you begin, check out the IBM Cloud® documentation about [Creating virtual server instances](#) to create a monitoring host by using the IBM Cloud® UI.

Monitoring host consideration

Consider the following settings for the monitoring host.

- The monitoring host must be deployed in the same region and zone as the monitored SAP system.
- Make sure that you select the correct resource group that corresponds to your deployable architecture (DA).
- You must deploy the `ibm-sles-15-5-amd64-sap-applications-<version>` image - SUSE Linux Enterprise Server 15 SP5 for SAP Applications (AMD64) - with the smallest available size of 2 cores.
- Add your appropriate SSH keys as described in [Managing SSH keys](#).

Verifying ACLs and security groups

After you create your monitoring agent host, go to your **ACLs and security groups** to verify that the settings are correct.



Note: If you are using ingestion endpoints other than the country location of the monitoring host, you must adjust the IBM Cloud® network ACL settings for a corresponding Private REST API endpoint. For more information, see [Collecting metrics by using Prometheus remote write](#).

Exporting SAP variables as bash variables

Use the following command to export SAP variables as Bash variables.

```
export sap_monitoring_nr=<sap_monitoring_nr>
export sap_hana_ip=<sap_hana_ip>
export sap_ascs_ip=<sap_ascs_ip>
export sap_app_server_ip_01=<sap_app_server_ip_01>
export sap_app_server_port_01=<sap_app_server_port_01>
export sap_ascs_http_port=<sap_ascs_http_port>
export sap_hana_http_port=<sap_hana_http_port>
export sap_hana_sql_systemdb_port=<sap_hana_sql_systemdb_port>
export sap_hana_sql_systemdb_user=<sap_hana_sql_systemdb_user>
export sap_hana_sql_systemdb_password=<sap_hana_sql_systemdb_password>
export ibmcloud_monitoring_instance_url=<ibmcloud_monitoring_instance_url>
export ibmcloud_monitoring_authorization_credentials=<ibmcloud_monitoring_authorization_credentials>
```

Checking connectivity for the database port and SAP instance ports

Install the netcat tool by using the following command.

```
$ sudo zypper install netcat
```

Use netcat to check connectivity to the database port and SAP instance ports on the monitoring host.

```
$ nc -vz ${sap_hana_ip} ${sap_hana_sql_systemdb_port}
```

Check connectivity from the SAP HANA database server to the HTTP port of the sapstartsrv web service on the SAP HANA server.

```
$ nc -vz ${sap_hana_ip} ${sap_hana_http_port}
```

Check connectivity from the SAP ASCS server to the HTTP port of the sapstartsrv web service of the ASCS on the SAP ASCS server.

```
$ nc -vz ${sap_asc_s_ip} ${sap_asc_s_http_port}
```

Check connectivity from IP address of the first SAP (primary) application server to the HTTP port of the sapstartsrv web service on the first application server.

```
$ nc -vz ${sap_app_server_ip_01} ${sap_app_server_port_01}
```

Checking the status of SLES operating system repositories

Make sure the appropriate **SLES OS** repositories are enabled by using the following command.

```
SLE-Module-SAP-Applications15-SP5-Updates  
SLE-Module-Packagehub-Subpackages15-SP5-Pool
```

If the repositories are not enabled, use the following commands to enable them.

```
$ sudo SUSEConnect -p sle-module-sap-applications/15.5/x86_64
```

```
$ sudo SUSEConnect -p PackageHub/15.5/x86_64
```

 **Tip:** If you are unable to activate these repositories, then you have installed the wrong version of the SLES operating system image.

Installing SLES Prometheus packages

Use the following steps to install SLES Prometheus packages.

1. Update all operating system packages to the latest version. Restart the host if necessary.

```
$ sudo zypper update
```

2. Install the following Prometheus packages.

```
$ sudo zypper install prometheus-sap_host_exporter
```

```
$ sudo zypper install prometheus-hanadb_exporter
```

```
$ sudo zypper install golang-github-prometheus-prometheus
```

3. Create the Prometheus data storage directory.

```
$ sudo mkdir /opt/prometheus
```

4. Change the user and group IDs of the Prometheus data storage directory to the Prometheus user.

```
$ sudo chown -R prometheus:prometheus /opt/prometheus
```

```
$ sudo chmod u+rwx /opt/prometheus
```

5. Copy the metric file `metrics.json` to the configuration directory `/etc/hanadb_exporter`.

```
$ sudo cp /usr/share/doc/packages/prometheus-hanadb_exporter/metrics.json /etc/hanadb_exporter/metrics.json
```

Installing the SAP Python driver hdbcli

Use the following steps to install the SAP Python driver `hdbcli`.

1. Access the SAP Download Center by using the [SAP S-user authentication](#).
2. Retrieve the SAP HANA Python driver by downloading the official SAP HANA Client. For more detailed information, see [Install the SAP HANA Client](#).
3. Install the SAP Python driver `hdbcli` as described in the [Installing the Python driver](#).
4. Choose the following SAP HANA Client package with the current `<version>` and `<patch>`.

```
SUPPORT PACKAGES & PATCHES - SAP HANA PLATFORM EDITION/ - SAP HANA PLATFORM EDITION 2.0/ - SAP HANA CLIENT 2.0 -  
LINUX ON X86_64 64BIT - IMDB_CLIENT20_<version>_<patch>-80002082.SAR
```

5. Download the `SAPCAR_*.EXE` package from the SAP download center.
6. Copy the two files `SAPCAR_*.EXE` and `IMDB_CLIENTXXX.SAR` to an arbitrary directory on the monitoring host.
7. As the root user, run the following command.

```
$ chmod 755 SAPCAR_*.EXE
```

8. Extract the SAP HANA Client from the SAR-file with SAPCAR.

```
$ ./SAPCAR_*.EXE -xvf IMDB_CLIENT20*.SAR
```



Note: The file name `SAPCAR_*.EXE` is a Linux binary file.

9. Use `hdbinst` to install the SAP HANA Client.

```
$ cd SAP_HANA_CLIENT
```

```
$ ./hdbinst
```

10. Enter the installation path: `[/usr/sap/hdbclient]: /usr/sap/hdbclient`.

11. Install the required pip package for Python 3.x.

```
$ sudo zypper install python3-pip
```

12. Install the SAP HANA Python driver.

```
$ pip install /usr/sap/hdbclient/hdbcli-*.tar.gz
```

Creating the hdbuserstore key

Use the following steps to create the `hdbuserstore` key.

1. Create the stored user key with the same Python user that runs the hanadb_exporter. Use the ReadOnly SQL user as `<sap_hana_sql_systemdb_user>`.

```
$ /usr/sap/hdbclient/hdbuserstore SET MONITORING-${sap_monitoring_nr}-KEY \  
"${sap_hana_ip}:${sap_hana_sql_systemdb_port}@SYSTEMDB" \
```

```
 ${sap_hana_sql_systemdb_user} ${sap_hana_sql_systemdb_password}
```

For more information, see [SAP HANA User Store \(hdbuserstore\)](#) and [hdbuserstore Commands](#).



Note: For the next steps, the `userkey` is added to the configuration file for the hanadb_exporter as `"userkey": "MONITORING-<sap_monitoring_nr>-KEY"`.

- Verify that your key was created successfully by listing all keys.

```
$ /usr/sap/hdbcclient/hdbuserstore list
```

- To list only your key, use the following command.

```
$ /usr/sap/hdbcclient/hdbuserstore list MONITORING-${sap_monitoring_nr}-KEY
```

Configuring the hanadb_exporter and activating the daemon

Use the following steps to configure the hanadb_exporter and activate the daemon.

The `hanadb_exporter` collects metrics from the SAP HANA database. All metrics from the database tenant SYSTEMDB are forwarded to the monitoring ingestion endpoint through Prometheus.

The GitHub repository and original documentation can be found at the following websites.

- [Hanadb exporter](#)
- [SAP monitoring](#)
- [Hanadb exporter metrics](#)

The configuration consists of two configuration files:

- `metrics.json` - contains all the SQL statements for querying the SAP HANA database
- `config.json` contains `sap_hana_ip`, `sap_hana_sql_systemdb_port`, and `hdbuserkey`

To avoid needing administrator privileges on the database, use the ReadOnly SQL user from the hdbuserstore. The specific parameters are added to the configuration file by replacing the placeholders `<...>`.

- Create the configuration file as user root with the file name `/etc/hanadb_exporter/config-<sap_monitoring_nr>-SQL.json` by using the following command:

```
{  
  "listen_address": "0.0.0.0",  
  "exposition_port": 5<sap_monitoring_nr>02,  
  "multi_tenant": false,  
  "_comment_multi_tenant": "true, if you want another 1000 metrics",  
  "timeout": 30,  
  "hana": {  
    "host": "<sap_hana_ip>",  
    "port": <sap_hana_sql_systemdb_port>,  
    "userkey": "MONITORING-<sap_monitoring_nr>-KEY",  
    "ssl": true,  
    "ssl_validate_cert": false  
  }  
}
```

- For the value of the `userkey` parameter, use the `hdbuserkey` name that you created earlier.

You can list the keys by using the following command.

```
$ /usr/sap/hdbcclient/hdbuserstore list
```

- Change the permissions of the configuration files so that only the root user can read them.

```
$ chmod 600 /etc/hanadb_exporter/config*
```

- Before you define the configuration of `sap_host_exporters` for the `systemd service`, test the exporters manually by using the

following command.

```
$ hanadb_exporter -c /etc/hanadb_exporter/config-${sap_monitoring_nr}-SQL.json -m  
/etc/hanadb_exporter/metrics.json
```

3. The process is blocking one terminal, so open a second terminal and verify that an exporter has correctly collected the metric. Run the following curl command.

```
$ curl http://localhost:5${sap_monitoring_nr}02/metrics
```

If you see the metrics, you should also see a status message. If the metrics are listed correctly, stop the exporter process.

Configure the systemd application for the `hanadb_exporter`.



Note: The `systemd` configuration file for the `hanadb_exporter` is included in the installation package. No changes to this configuration file are required. The systemd service can start any process with the configuration name (without the JSON extension as the file name).

1. To enable the `systemd` service for the `hanadb_exporter`, use the following commands.

```
$ sudo systemctl start prometheus-hanadb_exporter@config-${sap_monitoring_nr}-SQL
```

```
$ sudo systemctl enable prometheus-hanadb_exporter@config-${sap_monitoring_nr}-SQL
```

2. To show the status of the `hanadb_exporter` run the command below.

```
$ sudo systemctl status prometheus-hanadb_exporter@config-${sap_monitoring_nr}-SQL
```

Configuring the `sap_host_exporter` and activating the daemon

Use the following information to configure the `sap_host_exporter` and activate the daemon.

Prometheus `sap_host_exporter` uses stateless HTTP protocol to collect metrics from the SAP system instances. For more information, see the [official GitHub repository](#).

The SAP exporter configuration contains all the parameters for the connection and the HTTP port. Note that you need to create a separate configuration file for each connection.

Create the configuration files in the `/etc/sap_host_exporter/` directory. Name the configuration files according to the SAP instance by using the following command.

Use the following templates for the configuration files.

1. As the root user, create the SAP HANA configuration file with the file name `/etc/sap_host_exporter/sap_host_exporter-${sap_monitoring_nr}-HANA.yaml`.

```
# The listening TCP/IP address and port.  
address: "0.0.0.0"  
port: "5${sap_monitoring_nr}03"  
log-level: "info"  
sap-control-url: "http://<sap_hana_ip>:<sap_hana_http_port>"
```

2. As the root user, create the SAP ASCS configuration file with the file name `/etc/sap_host_exporter/sap_host_exporter-${sap_monitoring_nr}-ASCS.yaml`.

```
# The listening TCP/IP address and port.  
address: "0.0.0.0"  
port: "5${sap_monitoring_nr}04"  
log-level: "info"  
# ASCS instance  
sap-control-url: "http://<sap_ascs_ip>:<sap_ascs_http_port>"
```

3. As the root user, create the first SAP application server (PAS) configuration file with the name `/etc/sap_host_exporter/sap_host_exporter-${sap_monitoring_nr}-DI-01.yaml`.

```

# The listening TCP/IP address and port.
address: "0.0.0.0"
port: "5<sap_monitoring_nr>05"
log-level: "info"
# DI instance (metrics dispatcher server + resources)
sap-control-url: "http://<sap_app_server_ip_01>:<sap_app_server_port_01>"
```

- As the root user, create the second SAP application server (AAS) configuration file with the name `/etc/sap_host_exporter/sap_host_exporter-<sap_monitoring_nr>-DI-02.yaml`.

```

# The listening TCP/IP address and port.
address: "0.0.0.0"
port: "5<sap_monitoring_nr>06"
log-level: "info"
# DI instance (metrics dispatcher server + resources)
sap-control-url: "http://<sap_app_server_ip_02>:<sap_app_server_port_02>"
```

 **Note:** If there are multiple application servers, then create more configuration files for each SAP application server. Make sure that you increment the number of each configuration file.

- Test each `sap_host_exporter` configuration.

```
$ sap_host_exporter -c /etc/sap_host_exporter/sap_host_exporter-<sap_monitoring_nr>-HANA.yaml
```

- The process is blocking the terminal, so open a second terminal and run the following command.

```
$ curl http://localhost:5<sap_monitoring_nr>03/metrics
```

- Verify that the metric data is displayed. If no metrics are displayed, you should see some error messages.

- Repeat the same test with other exporter configurations:

```
$ /etc/sap_host_exporter/sap_host_exporter-<sap_monitoring_nr>-ASCS.yaml
```

```
$ /etc/sap_host_exporter/sap_host_exporter-<sap_monitoring_nr>-DI-01.yaml
```

If all of the exporters are working correctly, continue with the `systemd` configuration.

Configure the `systemd` server for the `sap_host_exporter`.

 **Note:** Only one extra `systemd` configuration file is required for all `sap_host_exporters`. The `systemd` service can start any process with the configuration name (without the JSON extension as file name).

- Create a file `sap_host_exporter@.service` as user root in the system directory.

```
/etc/systemd/system/sap_host_exporter@.service
```

- Add the following content without making any changes.

```

[Unit]
Description=Prometheus sap_host_exporter for Netweaver clusters metrics
After=network.target
Documentation=https://github.com/SUSE/sap_host_exporter
[Service]
Type=simple
Restart=always
ExecStart=/usr/bin/sap_host_exporter --config /etc/sap_host_exporter/%i.yaml
ExecReload=/bin/kill -HUP $MAINPID
[Install]
WantedBy=multi-user.target
DefaultInstance=default
```

- Run the following command as user root to reload the systemd configuration.

```
$ systemctl daemon-reload
```

4. As user root, start and enable the service for all configured `sap_host_exporter`.

```
$ systemctl enable --now sap_host_exporter@sap_host_exporter-${sap_monitoring_nr}-HANA
```

```
$ systemctl enable --now sap_host_exporter@sap_host_exporter-${sap_monitoring_nr}-ASCS
```

```
$ systemctl enable --now sap_host_exporter@sap_host_exporter-${sap_monitoring_nr}-DI-01
```

```
$ systemctl enable --now sap_host_exporter@sap_host_exporter-${sap_monitoring_nr}-DI-02
```

5. As user root, check the status of `systemd processes`.

```
$ systemctl status sap_host_exporter@sap_host_exporter-${sap_monitoring_nr}-ASCS
```

```
$ systemctl status sap_host_exporter@sap_host_exporter-${sap_monitoring_nr}-HANA
```

```
$ systemctl status sap_host_exporter@sap_host_exporter-${sap_monitoring_nr}-DI-01
```

```
$ systemctl status sap_host_exporter@sap_host_exporter-${sap_monitoring_nr}-DI-02
```

6. Enable `systemd autostart`.

```
$ sudo systemctl enable sap_host_exporter@sap_host_exporter-${sap_monitoring_nr}-ASCS
```

```
$ sudo systemctl enable sap_host_exporter@sap_host_exporter-${sap_monitoring_nr}-HANA
```

```
$ sudo systemctl enable sap_host_exporter@sap_host_exporter-${sap_monitoring_nr}-DI-01
```

Next steps

If the setup and configuration of the monitoring host was successful, continue with [Configuration of Prometheus server metric forwarding](#).

Configuring Prometheus server metric forwarding

The Prometheus metrics exporters, `sap_host_exporter` and `hanadb_exporter`, are configured to collect metrics from SAP HANA and the SAP system instances. Each Prometheus exporter collects metrics from the SAP system and exposes the metrics to a local HTTP port. Use a different HTTP port for each process and use a port number greater than 9600.

A Prometheus server, available from the package `golang-github-prometheus-prometheus`, is configured to forward the collected metrics from the local HTTP port to the monitoring ingestion endpoints.

All these services are installed as `systemd` services to keep them running permanently.

The Prometheus server is used to forward the metrics to the IBM Cloud® monitoring. You can configure all exporter processes of `hanadb_exporter` and `sap_host_exporter` in one `prometheus.yml` file.

The Prometheus server in agent mode performs the following functions.

- Collects metrics from HTTPS endpoints.
- Forwards the metrics to a remote endpoint.

Use the following steps to configure metric forwarding for the Prometheus server.

1. Create a Prometheus configuration file as described in [Configuring Prometheus remote write](#).

All metrics from all exporter processes are collected by defining `targets`.

The template for this configuration includes the following placeholders:

- `<ibmcloud_monitoring_instance_url>` determines the IBM Cloud® instance rewrite destination.
- `<ibmcloud_monitoring_authorization_credentials>` is the authentication token for the IBM Cloud® monitoring instance.

- <sap_monitoring_nr> is the SAP system number where the exposed metrics are collected.
- As the Prometheus user, run the following command to create the configuration file with the file name /etc/prometheus/<sap_monitoring_nr>.yml

```

global:
  scrape_interval: 15s
  evaluation_interval: 20s
  remote_write:
    - url: "<ibmcloud_monitoring_instance_url>"
      authorization:
        credentials: "<ibmcloud_monitoring_authorization_credentials>"
      write_relabel_configs:
        - target_label: instance
          replacement: 'SAP-<sap_monitoring_nr>-<sap_monitoring_solution_name>'
  scrape_configs:
    - job_name: "hanadb_exporter"
      static_configs:
        - targets: ['localhost:5<sap_monitoring_nr>02']
      relabel_configs:
        - target_label: domain
          replacement: 'SAP'
    - job_name: "sap_host_exporter"
      static_configs:
        - targets:
          ['localhost:5<sap_monitoring_nr>03', 'localhost:5<sap_monitoring_nr>04', 'localhost:5<sap_monitoring_nr>05']
          # 05 – n: as many as existing SAP Application server
      relabel_configs:
        - target_label: domain
          replacement: 'SAP'

```

 **Note:** Do not change the syntax of the Prometheus configuration file name: `/etc/prometheus/<sap_monitoring_nr>.yml`.

- Use the following commands to enforce Prometheus user permissions in all Prometheus configuration files.

```

$ sudo chown -R prometheus:prometheus /etc/prometheus

$ sudo chmod 0740 /etc/prometheus

$ sudo chmod 0640 /etc/prometheus/*

```

Test the Prometheus daemon manually.

```

$ sudo -H -u prometheus /usr/bin/prometheus \
--config.file=/etc/prometheus/${sap_monitoring_nr}.yml \
--storage.agent.path=/opt/prometheus/${sap_monitoring_nr} \
--enable-feature=agent --web.listen-address=localhost:5${sap_monitoring_nr}01

```

As the root user, set the systemd service parameters to run the Prometheus server in agent mode by using the following steps.

- Create and copy the following content to the `/etc/systemd/system/prometheus@.service` file.

```

[Unit]
Description=Prometheus
After=network.target
[Service]
User=prometheus
Group=prometheus
Type=simple
Restart=always
ExecStart=/usr/bin/prometheus --config.file=/etc/prometheus/%i.yml \
--storage.agent.path=/opt/prometheus/%i --enable-feature=agent \
--web.listen-address=localhost:5%i01
ExecReload=/bin/kill -HUP $MAINPID
TimeoutStopSec=20s
SendSIGKILL=no
[Install]

```

```
WantedBy=multi-user.target
```

2. Use the following commands to activate the configuration and start and enable the Prometheus agent.

```
$ systemctl daemon-reload  
  
$ sudo systemctl start prometheus@${sap_monitoring_nr}  
  
$ sudo systemctl enable prometheus@${sap_monitoring_nr}
```

Check the status of the service:

```
$ systemctl status prometheus@${sap_monitoring_nr}
```

3. Restart the daemon after each update of the configuration in the file /etc/prometheus/<sap_monitoring_nr>.yml.

```
$ chown a+r /etc/prometheus/*  
  
$ systemctl reload prometheus@${sap_monitoring_nr}
```

 **Note:** It takes some time for the metrics to appear in your dashboard.

Next steps

To visualize the metrics that are collected by the Prometheus server, see [Launch the monitoring web UI and work with dashboards](#).

Launching the monitoring UI and working with dashboards

All metrics are sent to the IBM Cloud® monitoring instance. If monitoring metrics are received on the monitoring instance, two SAP Dashboards are visible in the dashboard library of the monitoring instance in the Dashboard library.

1. To view the Dashboard library, click the **Dashboard library** tab from [/Dashboard/Dashboard manager](#).
2. Copy both dashboards to **My Dashboards**, click the three dots on the right side and click: **Copy to My Dashboards**. The two SAP Dashboards are visible under the **Dashboard/Dashboard Manager/My Dashboards/My Dashboards**:

- **SAP HANA DB**
- **SAP SYSTEM**

 **Note:** All configured SAP systems are monitored by these dashboards.

3. To show all configured SAP system instances on the **SAP SYSTEM** dashboard, click the pen icon next to **Team Scope** on the panel.
4. Select **instance** from the first pull-down menu and select **in** from the second pull-down menu. Go to the third pull-down menu and select one or more available names with syntax **SAP<sap_monitoring_nr>**.
5. Click **Save**. For more information, see the [Sysdig dashboard documentation](#).

The official [SAP System Monitoring documentation](#) describes all metric details to clarify the visualized values.

Duplicating, editing, and publishing dashboards

Use the following information to duplicate, edit, and publish dashboards.

Duplicating dashboards

To duplicate a dashboard, use the following information.

1. Go to the **Dashboard Manager** and click the **My Dashboards** tab.
2. From the list of dashboards, find your dashboard and click the three dots icon, then click **Duplicate dashboard**.

Editing of Dashboards

You can change the dashboard layout by duplicating the dashboard. For more information, see [Dashboard panels](#).

Publishing dashboards

Public dashboard sharing allows external users to review a dashboard without an IBM Cloud® login. For more information about sharing dashboards publicly, see [Enabling Public Sharing](#).

Parameter harvesting, troubleshooting, and maintenance

Use the following information for SAP parameter determination, troubleshooting, and maintenance.

Determining SAP parameters

Use the following commands to determine SAP parameters on your SAP HANA database and SAP application servers.

List the sapstartsrv services and operating system user of the processes

As a user `root`, use the following command to list the `sapstartsrv` services and the operating system user.

```
$ ps aux|grep sapstartsrv
```

List details such as SID, Nr, Instance, SAPLOCALHOST, Version, DIR_EXECUTABLE

As a root user, use the following command to list SAP HANA database and SAP application server details.

```
$ /usr/sap/hostctrl/exe/lssap
```

Log in as an SAP administrator

Use the following command to log in as an SAP administrator.

```
$ su - <SID>adm
```

List HTTP/HTTPS ports of an SAP instance

As an SAP administrator, use the following command to list the HTTP/HTTPS ports of an SAP instance.

```
$ sapcontrol -nr <instance_nr> -function GetSystemInstanceList
```

The following details are displayed: hostname, instanceNr, httpPort, httpsPort, startPriority, features, and dispstatus.

Determine the SQL ports of the SAP SYSTEMDB and TenantDB

As an SAP administrator, use the following commands to determine the SQL ports of the SAP SYSTEMDB and TenantDB.

```
$ hdbsql -i <instance_nr> -d SYSTEMDB -u SYSTEM -p <sap_hana_sql_systemdb_password>
```

```
$ SELECT * FROM SYS_DATABASES.M_SERVICES
```

The following details are displayed: `DATABASE_NAME, HOST, PORT, SERVICE_NAME, PROCESS_ID, DETAIL, ACTIVE_STATUS, SQL_PORT, COORDINATOR_TYPE, IS_DATABASE_LOCAL`.

```
$ quit
```

Show the status of an SAP HANA database

As an SAP administrator, use the following commands to show the status of an SAP HANA database.

```
$ hbsql -i <instance_nr> -d SYSTEMDB -u SYSTEM -p <sap_hana_sql_systemdb_password>
```

```
$ SELECT * FROM SYS.M_DATABASES
```

The following details are displayed: `DATABASE_NAME, DESCRIPTION, ACTIVE_STATUS, ACTIVE_STATUS_DETAILS, OS_USER, OS_GROUP, RESTART_MODE, FALBACK_SNAPSHOT_CREATE_TIME`.

```
$ quit
```

Troubleshooting missing data on the monitoring dashboards

If you don't see any metric data on the dashboard and all exporters are configured and running, the missing data might be due to one of the following reasons.

- Network ports are not open due to firewall settings or VPC ACL settings.
- Incorrect port numbers or credentials.

Check whether the SAP HANA database is running

To check whether the SAP HAHA database is running, log in to the SAP HANA host and run the following commands.

```
$ su - <SID>adm
```

```
$ HDB info
```

```
$ ps aux|grep -i gdb
```

Check a connection to an SAP HANA database with `hbsql`

To check a connection to an SAP HANA database with `hbsql`, run the following command as an SAP administrator.

```
$ hbsql -i <instance_nr> -d SYSTEMDB -u SYSTEM -p <sap_hana_sql_systemdb_password>
```

List processes of the SAP Control instances and the `sapstartsrv` services

To list the processes of the SAP Control instances and the `sapstartsrv` services, run the following command as the root user.

```
$ ps aux|grep sapstartsrv
```

View listening ports of an SAP HANA host or application server

To show the listening ports of an SAP HANA host or application server, use the following command.

```
$ ss -tulpen | grep sap
```

Test the `hanadb_exporter` manually

To manually test the `hanadb_exporter`, use the following command.

```
$ hanadb_exporter -c /etc/hanadb_exporter/config-${sap_monitoring_nr}-SQL.json \
-m /etc/hanadb_exporter/metrics.json
```

View the status of the Prometheus daemons on the monitoring host

Use the following commands to show the status of the prometheus daemons on the monitoring host.

```
$ systemctl status prometheus@${sap_monitoring_nr}
```

```
$ systemctl status prometheus-hanadb_exporter@config-${sap_monitoring_nr}-SQL
```

```
$ systemctl status sap_host_exporter@sap_host_exporter-${sap_monitoring_nr}-HANA
```

```
$ systemctl status sap_host_exporter@sap_host_exporter-${sap_monitoring_nr}-ASCS
```

```
$ systemctl status sap_host_exporter@sap_host_exporter-${sap_monitoring_nr}-DI-01
```

View the status of `firewalld` service

To show the status of the `firewalld` service, use the following command.

```
$ systemctl status firewalld
```

Display SAP exporter metrics on the monitoring host

To show the SAP exporter metrics on the monitoring host, use the following command.

Use the variables `<sap_monitoring_nr>` and the last two digits (default: 01) for service "Prometheus agent" that are in [Table 2](#).

```
$ curl http://localhost:5${sap_monitoring_nr}01/metrics
```

List the HTTP/HTTPS ports of each SAP instance on the SAP systems

To list the HTTPS port of each SAP instance, use the following command.

```
$ sapcontrol -nr <instance_nr> -function GetSystemInstanceList
```

View details about each running SAP instance on the SAP systems

```
$ sapcontrol -nr <instance_nr> -function GetProcessList
```

You can also debug the status of SAP HANA database and application service by using the commands that are in [Determine SAP Parameters](#).

Remove monitoring for an SAP system

To remove monitoring for an SAP system, you must stop and remove the corresponding Prometheus exporter on the monitoring host. After you stop the exporter, the metrics will no longer be sent to the IBM Cloud® monitoring instance.

To stop the Prometheus server for an SAP system, use the following command.

```
$ sudo systemctl stop prometheus@${sap_monitoring_nr}
```

Remove the Prometheus server `systemd` configuration for an SAP system by using the following command.

```
$ sudo systemctl remove prometheus@${sap_monitoring_nr}
```

To delete the corresponding Prometheus configuration, use the following command.

```
$ sudo rm /etc/prometheus/${sap_monitoring_nr}.yml
```

To stop and remove the `hanadb_exporter systemd` configuration, use the following commands.

```
$ sudo systemctl stop prometheus-hanadb_exporter@config-${sap_monitoring_nr}-SQL
```

```
$ sudo systemctl remove prometheus-hanadb_exporter@config-${sap_monitoring_nr}-SQL
```

To delete the `hanadb_exporter` configuration, use the following command.

```
$ sudo rm /etc/hanadb_exporter/config-${sap_monitoring_nr}-SQL.json
```

To stop and remove the `sap_host_exporter systemd` configuration, use the following commands.

```
$ sudo systemctl stop sap_host_exporter@sap_host_exporter-${sap_monitoring_nr}-HANA
$ sudo systemctl remove sap_host_exporter@sap_host_exporter-${sap_monitoring_nr}-HANA
$ sudo systemctl stop sap_host_exporter@sap_host_exporter-${sap_monitoring_nr}-ASCS
$ sudo systemctl remove sap_host_exporter@sap_host_exporter-${sap_monitoring_nr}-ASCS
$ sudo systemctl stop sap_host_exporter@sap_host_exporter-${sap_monitoring_nr}-DI-01
$ sudo systemctl remove sap_host_exporter@sap_host_exporter-${sap_monitoring_nr}-DI-01
$ sudo systemctl stop sap_host_exporter@sap_host_exporter-${sap_monitoring_nr}-DI-02
$ sudo systemctl remove sap_host_exporter@sap_host_exporter-${sap_monitoring_nr}-DI-02
```

To delete the `sap_host_exporter` configurations, use the following commands.

```
$ sudo rm /etc/sap_host_exporter/sap_host_exporter-${sap_monitoring_nr}-HANA.yaml
$ sudo rm /etc/sap_host_exporter/sap_host_exporter-${sap_monitoring_nr}-ASCS.yaml
$ sudo rm /etc/sap_host_exporter/sap_host_exporter-${sap_monitoring_nr}-DI-01.yaml
$ sudo rm /etc/sap_host_exporter/sap_host_exporter-${sap_monitoring_nr}-DI-02.yaml
```

Optional changes to /etc/services

You can use the `/etc/services` file to map service names to port numbers on the local host. The current setup doesn't require any changes to this file, but you can add the following optional changes.

```
SAP_prometheus_agent_<sap_monitoring_nr> 5<sap_monitoring_nr>01/tcp  # SAP monitoring \ prometheus agent to
<sap_monitoring_nr>
SAP_prometheus_agent_<sap_monitoring_nr> 5<sap_monitoring_nr>01/udp  # SAP monitoring \ prometheus agent to
<sap_monitoring_nr>
SAP_hanadb_exporter_<sap_monitoring_nr> 5<sap_monitoring_nr>02/tcp  # SAP monitoring \ hanadb_exporter to
<sap_monitoring_nr>
SAP_hanadb_exporter_<sap_monitoring_nr> 5<sap_monitoring_nr>02/udp  # SAP monitoring \ hanadb_exporter to
<sap_monitoring_nr>
SAP_sap_host_exporter_HANA_<sap_monitoring_nr> 5<sap_monitoring_nr>03/tcp  # SAP monitoring \ sap_host_exporter HANA
to <sap_monitoring_nr>
SAP_sap_host_exporter_HANA_<sap_monitoring_nr> 5<sap_monitoring_nr>03/udp  # SAP monitoring \ sap_host_exporter HANA
to <sap_monitoring_nr>
SAP_sap_host_exporter_ASCS_<sap_monitoring_nr> 5<sap_monitoring_nr>04/tcp  # SAP monitoring \ sap_host_exporter ASCS
to <sap_monitoring_nr>
SAP_sap_host_exporter_ASCS_<sap_monitoring_nr> 5<sap_monitoring_nr>04/udp  # SAP monitoring \ sap_host_exporter ASCS
to <sap_monitoring_nr>
SAP_sap_host_exporter_DI_01_<sap_monitoring_nr> 5<sap_monitoring_nr>05/tcp  # SAP monitoring \ sap_host_exporter DI
01 to <sap_monitoring_nr>
SAP_sap_host_exporter_DI_01_<sap_monitoring_nr> 5<sap_monitoring_nr>05/udp  # SAP monitoring \ \ sap_host_exporter DI
01 to <sap_monitoring_nr>
SAP_sap_host_exporter_DI_n_<sap_monitoring_nr> 5<sap_monitoring_nr>06/tcp  # SAP monitoring \ sap_host_exporter DI 02
to <sap_monitoring_nr>
SAP_sap_host_exporter_DI_n_<sap_monitoring_nr> 5<sap_monitoring_nr>06/udp  # SAP monitoring \ sap_host_exporter DI 02
to <sap_monitoring_nr>
```

Backup strategies

Fast path of IBM Power Virtual Server

Use this collection of shortcuts for rapid access to key documentation about SAP solutions on IBM Power Virtual Server.

Overview

An Infrastructure-as-a-Service (IaaS) environment consists primarily of compute, storage, network, and virtualization components from a specified region (such as the US) and a designated zone or data center. For more information, see [Architecture for IBM Power Virtual Server in IBM data center](#). For information about the zones, see [IBM Cloud regions](#).

Planning

SAP solution architecture

Your business and functional requirements determine the scope for your SAP solutions. Consider your nonfunctional requirements in addition, and map the application components to the infrastructure components.

Refer to [Connectivity options within the IBM Power Virtual Server network, connection through IBM Cloud](#)

Deployment

- Compute
 - [Sizing process for SAP Systems](#)
 - [Mapping CPUs derived from SAPS to an IBM Power Virtual Server](#)
 - [SAP HANA certified instances on IBM Power Virtual Server](#)
 - [SAP NetWeaver certified instances on IBM Power Virtual Server](#)
 - [OS for IBM Power Virtual Servers](#)
 - [Bring-your-own-OS \(custom OS image and BYOL license\)](#)
- Storage
 - [General storage configurations on IBM Power Virtual Server Infrastructure](#)

High availability

- [Implementing high availability for SAP applications on IBM Power Virtual Server](#)

Disaster recovery

- [Planning Disaster Recovery for SAP solutions on IBM Cloud](#)

Tutorials

Deployment

- [Accessing File Storage for VPC from IBM Power Virtual Server instances](#)

How to

Deployment

- Preparing the deployment
 - [Planning your deployment](#)
 - [Deploying IBM Cloud VPC infrastructure for Power Virtual Server workloads](#)
 - [Deploying SAP Power Virtual Server workloads](#)
- Running the deployment

- [Deploying SAP applications on Power Virtual Server](#)
- [SAP license key with IBM Power Systems Virtual Servers](#)

High availability

- General preparation steps
 - [Creating instances for a high availability cluster](#)
- Cluster deployment in a single Power Virtual Server workspace
 - [Implementing a Red Hat Enterprise Linux High Availability Add-On cluster](#)
 - [Configuring SAP HANA scale-up system replication in a Red Hat Enterprise Linux High Availability Add-On cluster](#)
 - [Configuring SAP HANA cost-optimized scale-up system replication in a Red Hat Enterprise Linux High Availability Add-On cluster](#)
 - [Configuring SAP HANA active/active \(read enabled\) system replication in a Red Hat Enterprise Linux High Availability Add-On cluster](#)
 - [Configuring SAP HANA multitier system replication in a Red Hat Enterprise Linux High Availability Add-On cluster](#)
 - [Configuring SAP HANA multitarget system replication in a Red Hat Enterprise Linux High Availability Add-On cluster](#)
 - [Configuring high availability for SAP S/4HANA \(ASCS and ERS\) in a Red Hat Enterprise Linux High Availability Add-On cluster](#)
 - [Configuring an active-passive NFS server in a Red Hat Enterprise Linux High Availability Add-On cluster](#)
- Cluster deployment in a multizone region environment
 - [Implementing a Red Hat Enterprise Linux High Availability Add-On cluster in a multizone region environment](#)
 - [Configuring high availability for SAP S/4HANA \(ASCS and ERS\) in a Red Hat Enterprise Linux High Availability Add-On cluster in a multizone region environment](#)

Backup and restore

- [Backup strategies for SAP HANA on IBM Power Virtual Server](#)

Monitoring

- Overview
 - [Getting started with IBM Cloud Monitoring for SAP systems](#)
 - [Monitoring for IBM Power Systems Virtual Servers](#)
- Setting-up
 - [Prerequisites](#)
 - [Creating a monitoring instance in IBM Cloud®](#)
 - [Setup and configuration of a monitoring host](#)
 - [Configuration of Prometheus server metric forwarding](#)
 - [Launching the monitoring UI and working with dashboards](#)

Migration

- [Overview - Migrating SAP servers between on-premises and IBM Cloud® on IBM Power Virtual Server](#)
- [Hybrid Cloud Network Consideration for SAP applications on IBM Power Virtual Server](#)
- [Migrating SAP S/4HANA to IBM Power Virtual Server](#)
- [Migrating SAP ERP 6.0 with Oracle to IBM Power Virtual Server](#)
- [Migrating SAP ERP 6.0 with IBM Db2 to IBM Power Virtual Server](#)
- [Migrating from SAP ERP 6.0 to S/4HANA to IBM Power Virtual Server](#)

Help

- [Getting help and support from IBM Cloud or SAP](#)
- [SAP-certified IBM Power Virtual Servers](#)

Backup strategies for SAP HANA on IBM Power Virtual Server

IBM Cloud offers a robust Power Virtual Server infrastructure to run SAP HANA, and this document outlines the steps and best practices for

performing backups of SAP HANA database.

When deploying SAP HANA on Power Virtual Server instance, it is essential to implement a reliable and efficient backup strategy to ensure the availability and recoverability of your data. Two primary methods are available for performing backups of SAP HANA database running on Power Virtual Server instance:

1. [Secure automated backup with Compass for SAP HANA](#)
2. [SAP HANA Backint Agent for IBM Cloud Object Storage](#)

Both of these methods offer flexible, secure, and scalable solutions for backing up SAP HANA, and each has its own set of advantages based on your infrastructure and requirements.

Secure automated backup with Compass for Linux

The Backup Offering is powered by Cobalt Iron Compass and is accessible from the IBM Cloud [catalog](#). The Backup Offering provides enterprise-class backup and restore features in a cloud-centric SaaS solution. Compass capabilities and security features, along with many other security functions provides protection and self-assessments to protect enterprise data and applications.

For more information, see [Cobalt Iron documentation](#).

Cobalt Iron Compass protects various platforms, applications, and data classes. The Backup Offering includes the following unique features and functions for SAP HANA on Power Virtual Server:

1. HDBackInt-integrated backup and restore of SAP HANA databases
2. HDBackInt-integrated backup and restore of SAP HANA redo log files
3. Support for the SAP HANA Cockpit for configuration, monitoring, and scheduling of backups

The Backup Offering provides various integrated security and operational features that includes:

1. Alerting, notifications, and ticketing features and integration
2. Automated auditing and validation of backup server landscape
3. Backup server automation that includes hands-free automation of all backup server tasks
4. Centralized policy management
5. Complete governance
6. Data reduction through compression and deduplication
7. Data replication across regions in IBM Cloud
8. Encryption of data in all phases from in-transit, to-storage, and at-rest
9. Extensive support for encryption, data immutability, and other security access controls
10. Multitenancy and unlimited sub-organizations
11. Role-based access control management.

Network architecture for deploying the backup instance

To deploy the backup instance, use one of the following architectures:

- [Single copy Backup Offering](#)
- [Dual copy Backup Offering](#)

Single copy Backup Offering

Using a single copy Backup Offering, you can take a backup of your workload in a single data center.

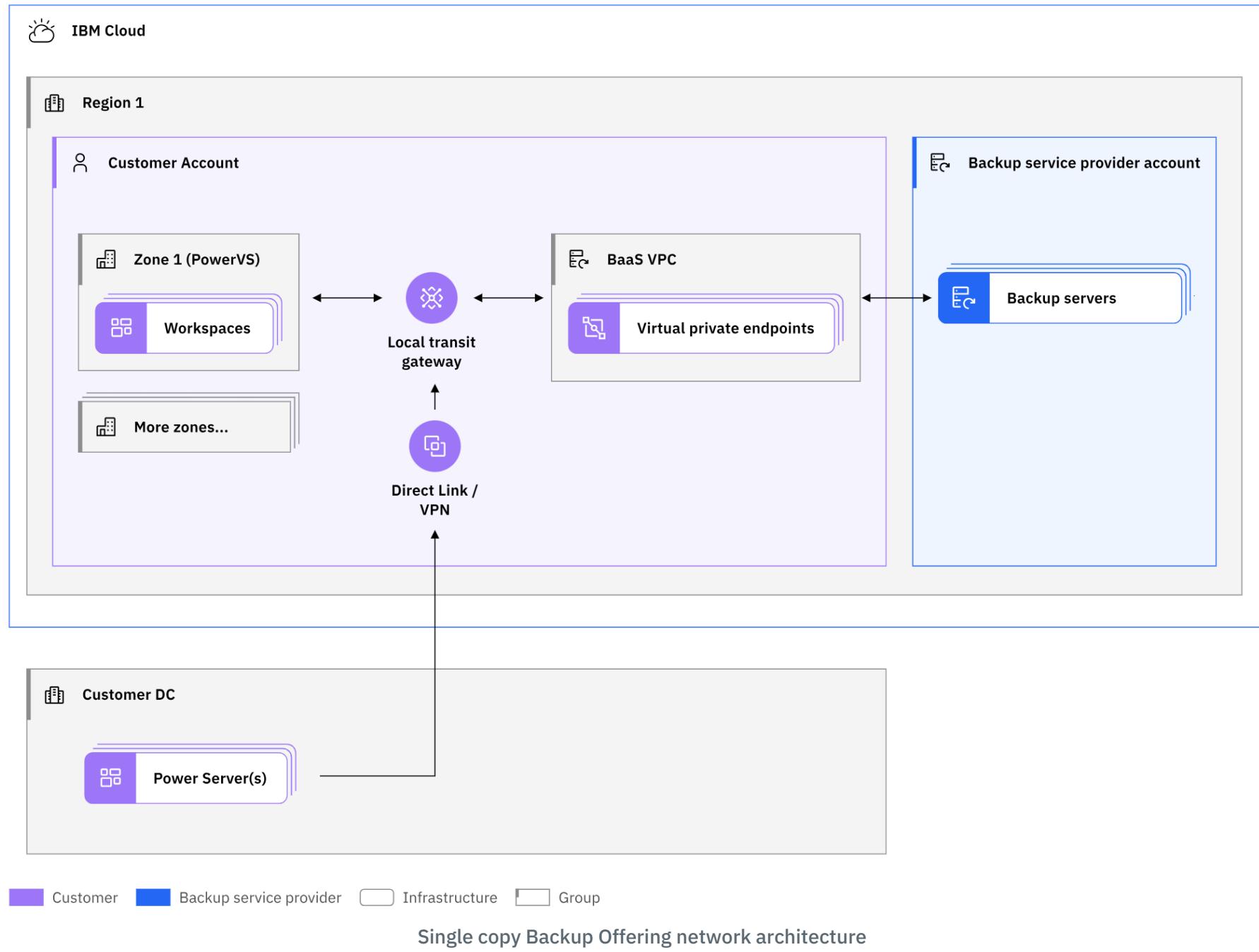
By studying the network architecture diagram of single copy Backup Offering, you can understand the following concepts:

- The architecture of single copy Backup Offering deployed in IBM data center
- The requirements for AIX and Linux VMs on Power to access the Compass backup servers through the IBM Cloud network

Compass Accelerator Vaults are backup server instances that are preconfigured in IBM Cloud data centers and are replicated across other regions.



Important: Do not deploy any additional resources to the Backup Offering VPC.



The Backup as a Service (BaaS) VPC is created when the Backup Offering is provisioned. The BaaS VPC enables Virtual Private Endpoints (VPEs) for private IP connectivity to the managed backup server instances. When you deploy the backup server instance, an automation process creates the following network segments:

- Local Transit Gateway, if it does not exist
- BaaS VPC for the dedicated use of the backup activity
- VPE for secure connectivity to each of the backup servers
- Security group with inbound rule, address prefix, and subnet

The Backup Offering VPC and the Power Virtual Server workspaces must exist in the same region and be connected by using the local Transit Gateway. You can connect your on-premises workloads to the Transit Gateway through the Direct Link connection. You can use VPN connection in place of a Direct Link connection.

Dual copy Backup Offering

Using a dual copy Backup Offering, you can take a backup of your workload in two different data center regions.

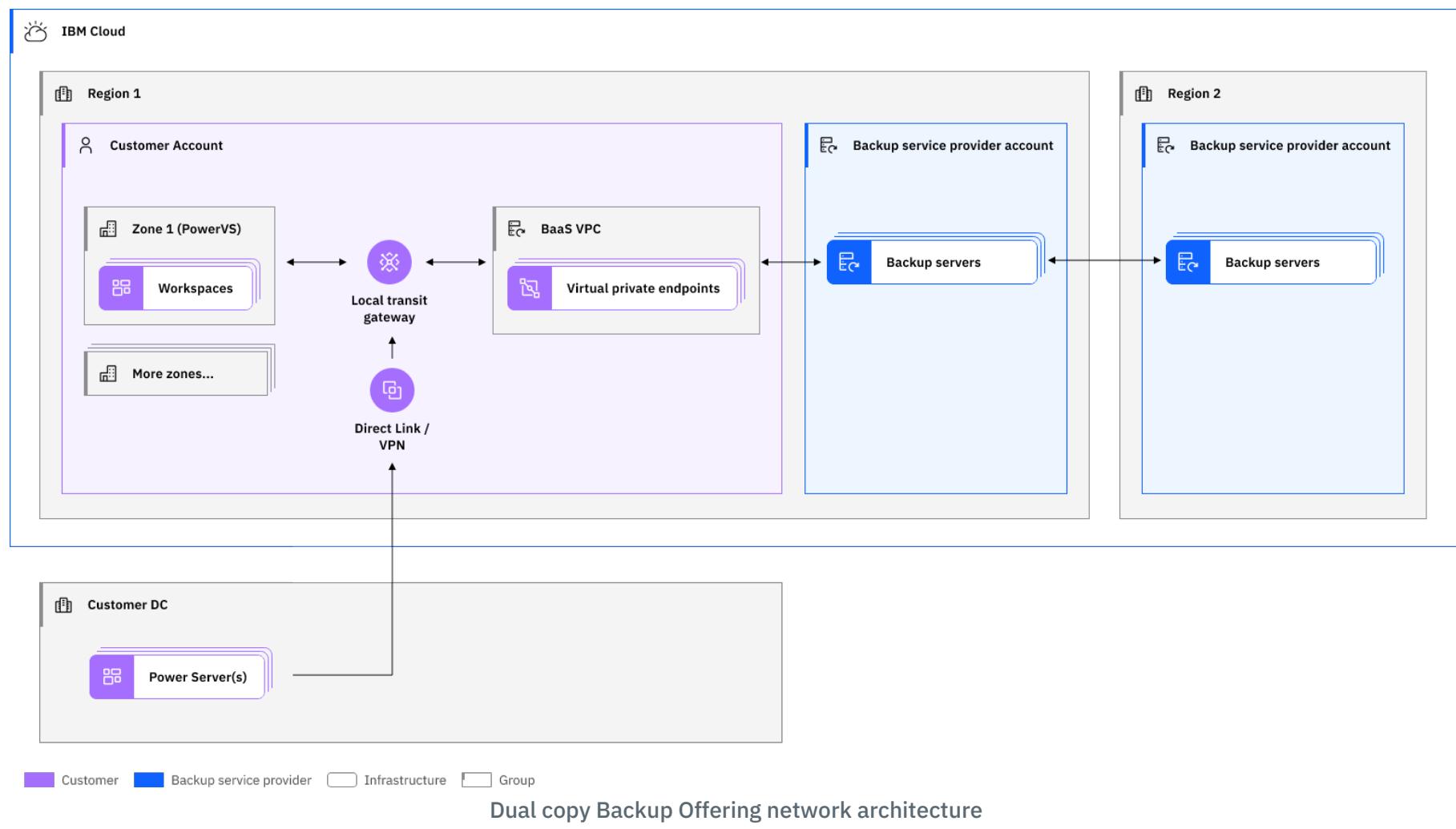
By studying the network architecture diagram of dual copy Backup Offering, you can understand the following concepts:

- The architecture of dual copy Backup Offering that is deployed in IBM data center
- The requirements for AIX and Linux VMs on Power to access the Compass backup servers through the IBM Cloud network

Compass backup servers are preconfigured in data centers and are also replicated across the other regions.



Important: Do not deploy any additional resources to the Backup Offering VPC.



The Backup Offering VPC is a managed backup server instance that is deployed when the Backup Offering is provisioned. When you deploy the backup server instance, an automation process creates the following network segments:

- Local Transit Gateway if it does not exist
- VPC for backup activity only
- VPE for each of the backup servers
- Security group with inbound rule, address prefix, and subnet

The Backup Offering VPC and the Power Virtual Server workspaces must exist in the same region and be connected by using the local Transit Gateway. You can connect your on-premises workloads to the Transit Gateway through the Direct Link connection. You can use VPN connection in place of a Direct Link connection.

Provisioning the backup instance in IBM data center

To create and deploy a backup server instance from the IBM Cloud catalog, complete the following steps:

1. Log in to the IBM Cloud [catalog](#) with your credentials.

Note: To create or edit VPC and Transit Gateway, you must have roles with permissions such as `writer` or `editor` for your IBM Cloud account.

2. In the search box, type *Compass Backup* and click **Secure Automated Backup with Compass** tile.

3. Select a deployment location for your backup instance.



Important: It is recommended not to deploy any additional resources to the Backup Offering VPC.

4. Define the fields – **Pricing plan**, **Service name**, **Resource group**, your **IBM Cloud API key**, and Compass organization name according to your business needs. Also, specify the VPC subnet IP range that you want to use to access the Compass Vaults.

5. Click **Create**.

6. Compass creates and connects the Backup VPC to the Power Virtual Server workspace that you want to back up by using the local Transit Gateway. A Transit Gateway is created if it does not exist.

For more information, see [Ordering IBM Cloud Transit Gateway](#) and [Using virtual private endpoints for VPC to privately connect to IBM Cloud Transit Gateway](#).

7. Click **Launch Compass UI** that will redirect you to the Cobalt Iron Compass Commander page where you need to complete the setup. For more information, see [Cobalt Iron documentation](#).



Tip: Connectivity between Power Virtual Server instances and the backup servers is established via a Transit Gateway connection to the

backup VPC. Name resolution is for the backup server connections, which is also required. You can accomplish this using the agent system's /etc/hosts file, or by adding CNAME entries to your agent system's DNS server. These elements need to be deployed in your account (Transit Gateway and VPC provisioning and setup happens through automation when the Backup Offering is provisioned).

Installation and configuration of agent on host

For detailed installation and configuration steps refer to the [SAP HANA agent setup process PDF](#).

Pricing

When you use the Backup Offering, you are billed monthly through IBM Cloud for the amount of data backed up for the region and are billed hourly. For more information about pricing plans, see [Cobalt Iron - Secure Automated Backup](#) page accessible from the IBM Cloud [catalog](#). You can generate an estimate of the cost based on your expected usage from the **Summary** pane.

Supported data centers

The single copy Backup Offering is available in the following data centers:

- DAL10
- DAL12
- FRA04
- FRA05
- MAD02
- MAD04
- OSA21
- SA001
- SA004
- SYD04
- SYD05
- TOK04
- WDC07
- WDC06

The dual copy Backup Offering is available in the following data center pairs:

Data Center 1	Data Center 2
DAL10	WDC07
DAL12	WDC06
MAD02	FRA04
MAD04	FRA05
SA001	SA004
OSA21	TOK04
SYD04	SYD05
DAL13	WDC04
LON04	LON06

Data center pair availability for Backup Offering

Additional support

Support for the Backup Offering is provided by Cobalt Iron.

- For more information about the offering, see the [Cobalt Iron documentation](#).
- For issues related to backup and restore, contact Cobalt Iron by opening a service ticket through support.cobaltiron.com.

SAP HANA Backint agent for IBM Cloud Object Storage

- The Backint agent for SAP HANA is a tool designed to integrate with third-party backup solutions. It allows SAP HANA backups to be offloaded to various backup storage systems, such as IBM Cloud Object Storage or to a local storage disk.
- The SAP HANA Backint Agent for IBM Cloud Object Storage is bundled as part of the **IMDB_SERVER*.SAR** installation file (SAP HANA database installation binary) and is essential for performing backups on SAP HANA in compliance with SAP's backup guidelines.
- SAP HANA Backint agent is supported both on SUSE Linux Enterprise Server (SLES) and RedHat platforms.

Prerequisites

Before you begin, ensure the following prerequisites are met:

1. It is required to have an IBM Cloud Object Storage (COS) instance. Within this instance, an Object Storage Bucket is required. Refer to [IBM Cloud Object Storage](#) for more details.
 - a. Log into **IBM Cloud Console** and create an instance of **IBM Cloud Object Storage**.
 - b. Create a **bucket** where backups will be stored.
 - c. Make sure to set the **bucket's permissions** properly to control access.
 - d. Obtain the **service credentials** (API key) required to authenticate your backups.
2. The **IMDB_SERVER*.SAR** file downloaded from [SAP Softwarecenter](#).

For better performance create an IBM Cloud VPC(VPC) and create a [virtual private endpoint gateway \(VPE\)](#) of type Cloud Object Storage. Add an entry in the **/etc/hosts** file on Power Virtual Server instance with the VPE IP which points to the direct endpoint of Cloud Object Storage. To reach the IP of VPE from the Power Virtual Server instance, the VPC and the Power Virtual Server Workspace must be connected to the same Transit Gateway.

Installation and configuration of agent on host

1. Extract the downloaded **IMDB_SERVER*.SAR** on the Power Virtual Server instance.
2. The backint agent installation package is available in [SAP_HANA_DATABASE/server/aws-s3-backint-<version>-linuxppc64le.tar.gz](#).
3. [SAP Note 2935898](#) describes how to install and configure the SAP HANA Backint Agent for IBM Cloud Object Storage.
4. Refer to [BACKUP DATA Statement \(Backup and Recovery\)](#).

Infrastructure reference architectures for SAP

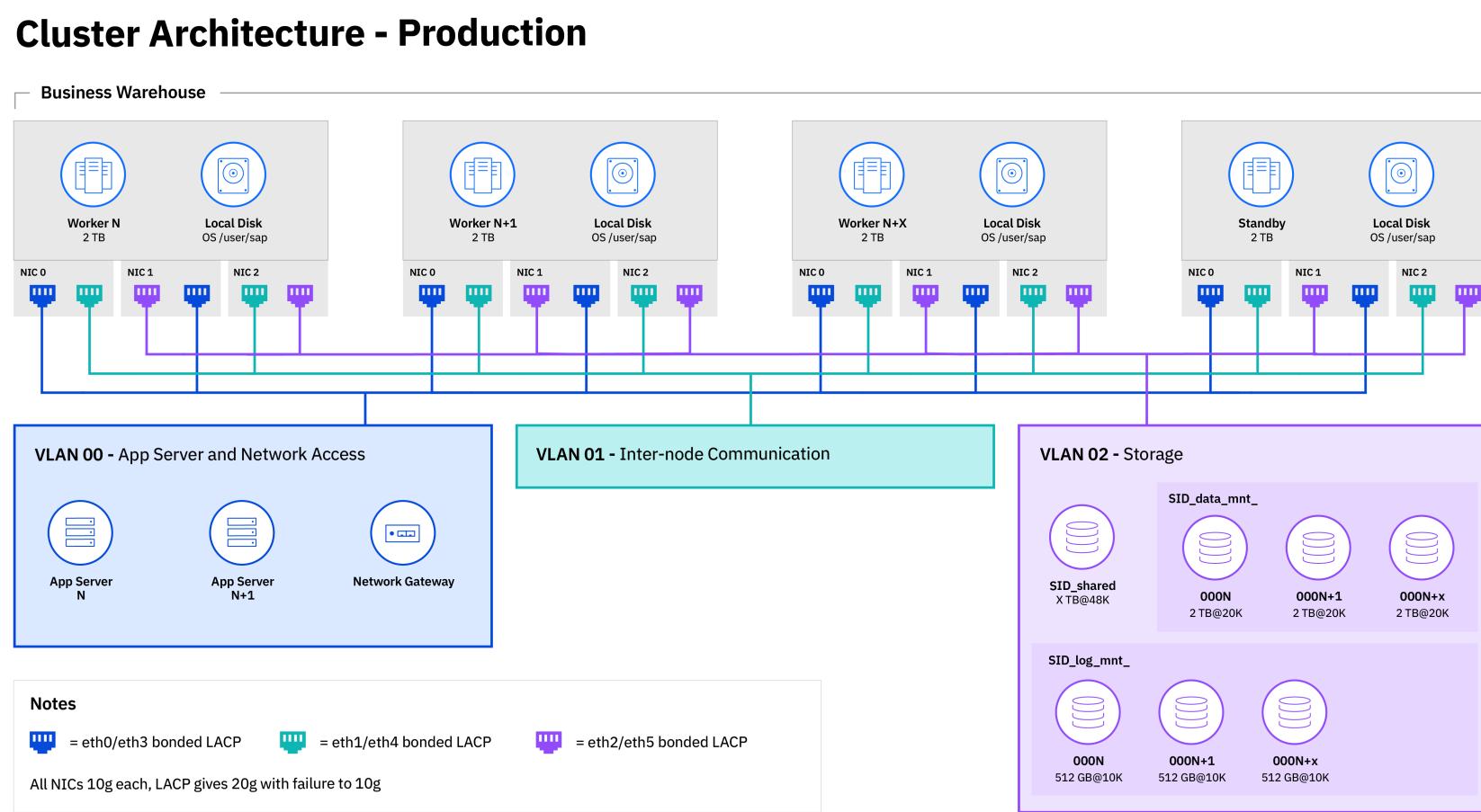
SAP HANA scale-out Reference Architecture

The IBM Cloud® architecture provides superior technical capabilities, such as a software definable environment critical to a cloud infrastructure, programmable interfaces, and hundreds of hardware and network configurations. It is designed to deliver a higher level of flexibility by mixing virtual and dedicated servers to fit various workloads, automation of interfaces, and hybrid deployment options. The IBM Cloud SAP-Certified Infrastructure offering for SAP HANA and SAP NetWeaver provides you with a best-fit selection. This selection includes bare metal and virtualization-based servers on which the SAP software stack is run.

Intel Bare Metal servers on Classic Infrastructure

Reviewing the network topology and storage layout

Figure 1 shows the network topology that is required for the IBM Cloud Classic Infrastructure as a Service SAP HANA TDI scale-out setup.



Available SAP HANA certified IBM Cloud configurations

For Intel Bare Metal, the following solutions are certified to serve as OLAP or OLTP scale-out configuration SAP HANA nodes:

OLTP:

- BI.S4.H8.12000

OLAP:

- BI.S4.H8.12000
- BI.S4.H8.6000
- BI.S4.H4.3000
- BI.S4.H4.6000
- BI.S4.H2.3000
- BI.S2.H8401
- BI.S2.H4101
- BI.S2.H4201

Check [SAP Certified and Supported SAP HANA Hardware Directory](#) for details of the supported configurations.

Network layout for Scale-out configurations

For Intel Bare Metal scale-out configurations, contact IBM Cloud support for assisting you to set-up the required networking. Depending on the hardware used, the choice of networks might be restricted, or special configurations might have to be adapted. See the following diagram, for the layout to use. The diagram describes the use of three fully redundant (LACP config), physically separate networks, for:

- Storage traffic,
- Internal SAP HANA inter-node communication
- Communication with the client(s), for example SAP ABAP application servers or SAP HANA Studio for administration purposes.

Use the network that holds the default route of your environment to pass the NFS traffic through it, the storage servers are reachable through that gateway, only.

Storage for Scale-out configurations

For scale-out configuration, the ability of storage volumes to be accessed from different server nodes is required for failover purposes. Thus, local storage is out of scope, and NFS volumes need to be deployed. The deployed volumes can vary in size and number (see details here: [Persistent Data Storage in the SAP HANA Database](#)). In any case, they have to comply with the TDI performance KPIs (see [SAP Note 2613646](#)) verified by [SAP HANA Hardware and Cloud Measurement Tools](#).

IBM Cloud recommends Endurance File Storage at 10 IOPS per GB or Performance File Storage with IOPS equal or greater than 10K. For the network configuration, use the primary network as storage network to guide the traffic to the NFS servers through it.

Intel Virtual Servers in VPC Infrastructure (Gen2)

Available SAP HANA certified IBM Cloud configurations

For Intel-based VSIs in VPC, the following configuration is available for OLAP scale-out configuration with SAP HANA:

OLAP:

- vx2-176x2464

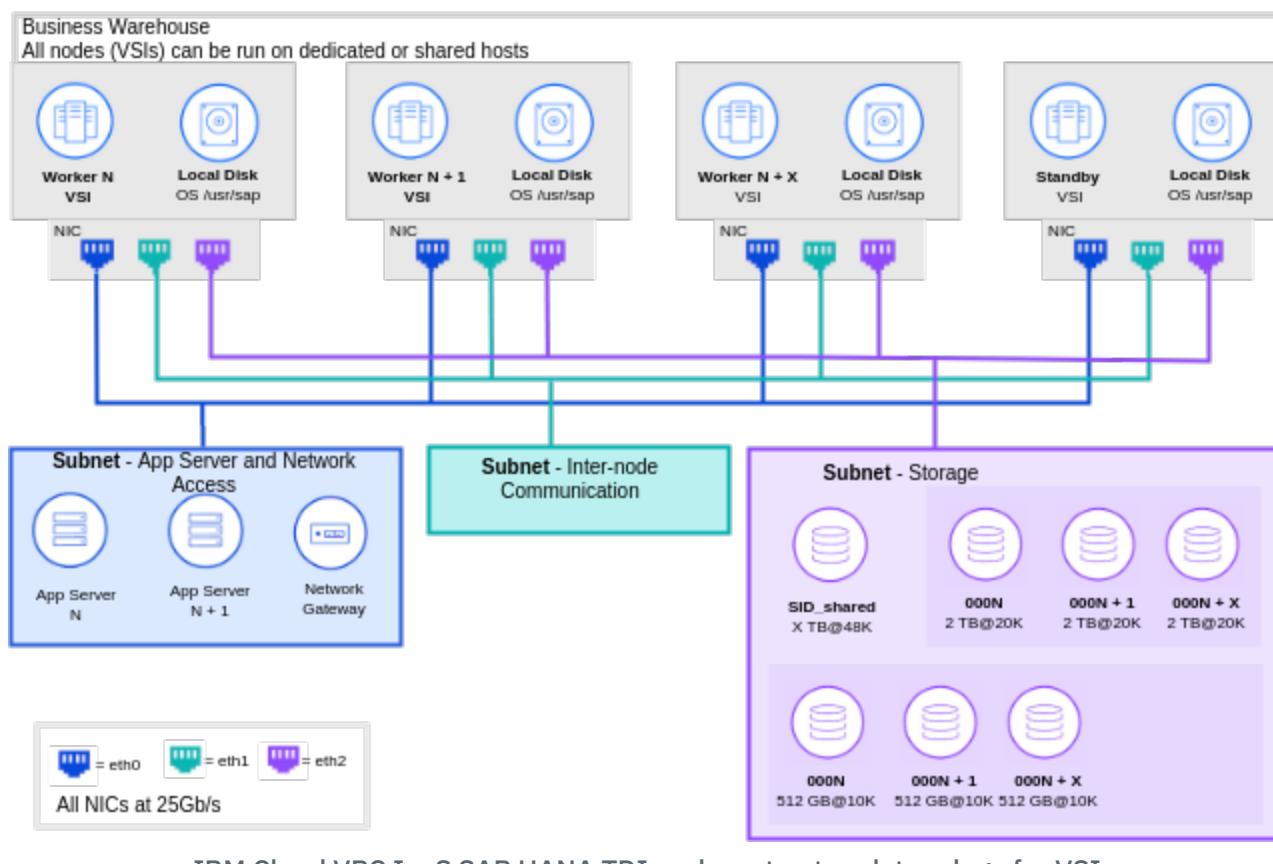
Check [SAP's Certified and Supported SAP HANA Hardware Directory](#) for details of the supported configurations.

These configurations can either be run on-top of dedicated hosts (DHs) or on shared hosts.

Network layout for Scale-out configurations

For Intel Bare Metal scale-out configurations, contact IBM Cloud support for assisting you to set-up the required networking. On the VPC (Gen2) infrastructure, underlying host systems are laid out for full redundancy, no matter if they are dedicated or shared hosts. As a result, VSIs in VPC do not require for redundant network adapter. Throughput for all VSI level adapters in one VSI is limited to 60 Gbps, by default. A single adapter is limited to 25 Gbps maximum throughput. Therefore, the HANA network layout for scale-out configurations requires three separate networks, 3 adapters to be configured with a throughput of 20 Gbps, each. See the following diagram for the network layout for VSIs. Read the following chapter on storage before you decide on the details of your storage layout and the according networks to use.

Figure 2 shows the network topology that is required for the IBM Cloud VPC Infrastructure as a Service SAP HANA TDI scale-out setup.



Storage for Scale-out configurations

For scale-out configuration, the ability of storage volumes to be accessed from different server nodes is required for failover purposes. Thus, local storage is out of scope, and NFS volumes need to be deployed. These shares are referred to as [file shares and their mount targets](#) in IBM Cloud VPC. The shares can vary in size and number (see details here: [Persistent Data Storage in the SAP HANA Database](#)). In any case, they must comply with the TDI performance KPIs (see [SAP Note 2613646](#)) verified by [SAP HANA Hardware and Cloud Measurement Tools](#).

IBM Cloud recommends 10 IOPS per GB or custom profile File Shares for meeting the SAP's KPIs.

Choose one subnet to connect the file shares to. Carefully design and configure your network and SAP HANA configuration in a way that this network is not used for client nor internal communication. For more information on creating file shares and mount targets, see [Planning your file shares](#).

SAP NetWeaver 7.x on UNIX with Sybase on IBM Cloud® VPC

Sybase is one of the many databases that can be run with SAP NetWeaver and that is supported on the IBM Cloud®. The most common architecture deployments are standard and distributed. IBM Cloud is certified for running SAP NetWeaver application servers ABAP, Java, and SAP products based on these application server stacks.

SAP NetWeaver architecture

SAP NetWeaver is the core foundation of the SAP technology stacks and is the platform that is used for Advanced Business Application Programming (ABAP) and Java applications. SAP NetWeaver components are built on the SAP NetWeaver Application Server and are written in ABAP or Java Platform, Enterprise Edition. ABAP systems, Java systems, and dual-stack systems are distinct systems.

Core platform features

SAP NetWeaver uses ABAP or Java core platforms to support the SAP applications. SAP NetWeaver:

- Has application lifecycle management capabilities.
- Provides the basic structure for the on-premises versions of SAP Business Suite and other applications, as an application server.
- Is the foundation for the on-premises SAP S/4HANA next-generation business suite, with SAP HANA serving as the sole underlying database.

SAP provides a list of the [SAP versions](#) to learn more about the versions available in IBM Cloud. Each support package stack has a leading software component version. The support package level of each component version is a key part of the stack and a unique identifier for the support package stack.

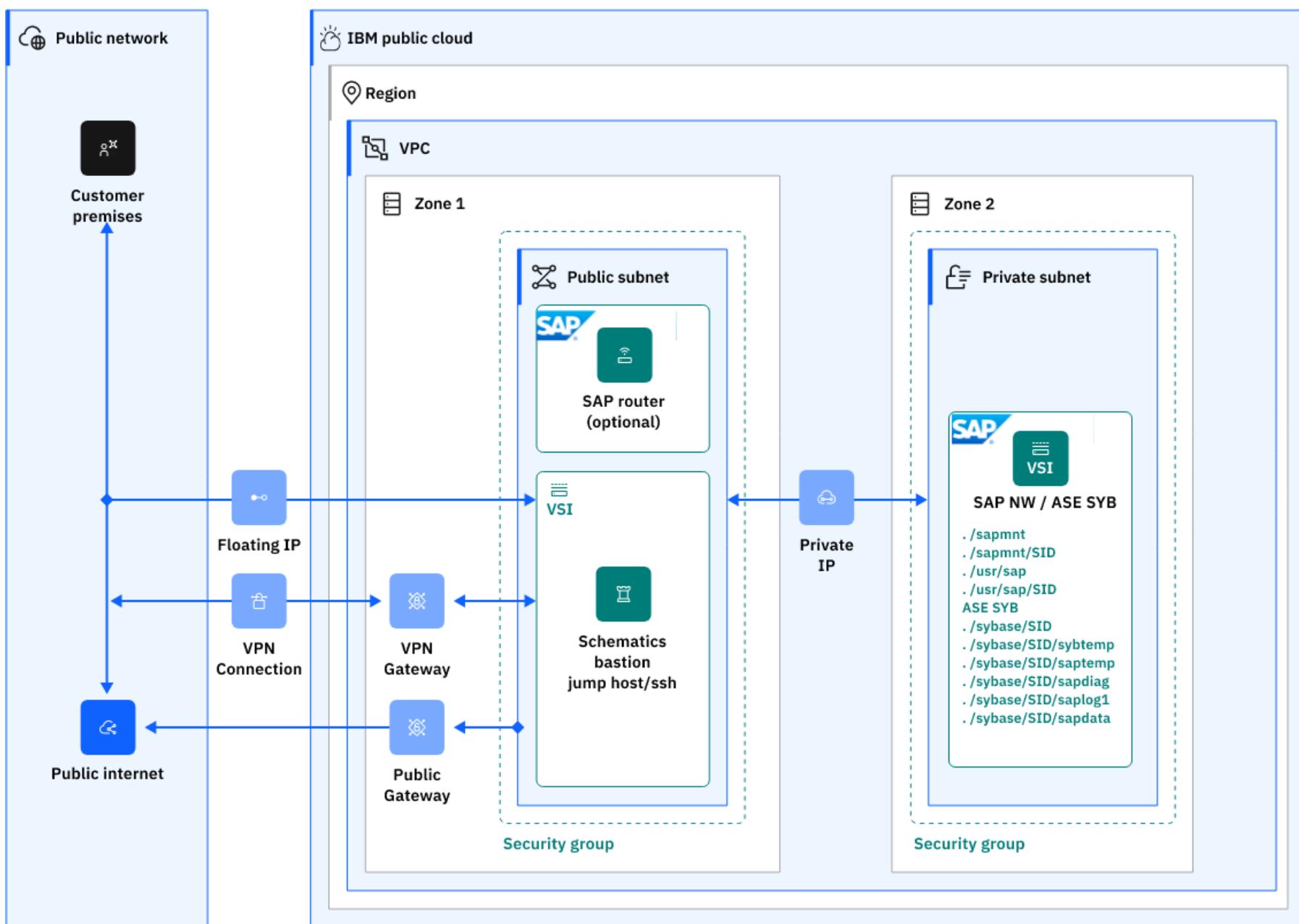
Installation types

The three installation types for SAP NetWeaver Application Server are:

- ABAP System – You can run ABAP programs and some SAP Java apps
- Java System – You can run only Java Platform, Enterprise Edition apps. No ABAP programs can be run on a Java system
- Dual Stack – You can run both ABAP and Java Platform, Enterprise Edition in separate instances

Architecture diagram

This diagram shows the SAP NetWeaver 7.X on Sybase DB integrated with IBM Cloud on the SAP NetWeaver 7.x architecture:



SAP NetWeaver 7.x with SYB standard installation with AAS on VSI to VPC IBM Cloud

Access from an external network

Clients on the customer facing network (CFN) use a floating IP to access virtual server instances within the IBM Cloud. Virtual server instances are hosted in availability zones (data centers) within geographic regions.

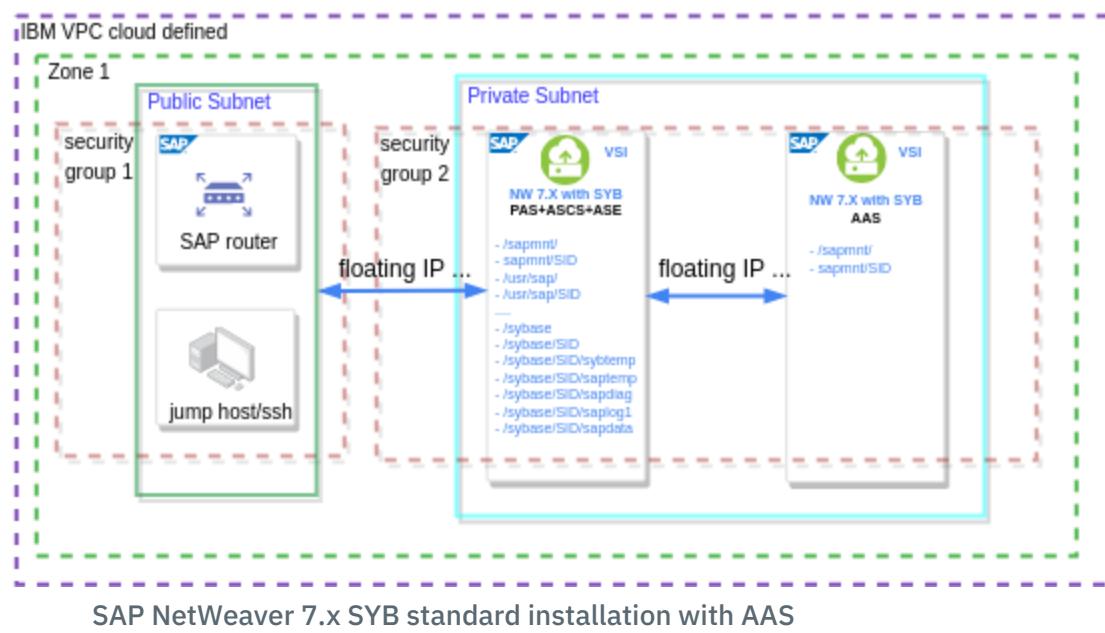
Within the Public Subnet, the [SAP router](#) and the jumphost provide secure connections to the virtual server instances. The SAP router is a software application that provides a remote connection between the customer's network and SAP. The SAP Router and jumphost are within a single security group with rules for inbound and outbound traffic between the private subnets in the zone. SAP routers are used with traditional SAP products and analytics solutions and offerings that are acquired from Sybase. For a comprehensive list of which SAP Business Analytics products benefits from SAP router connections, see [SAP Note 1478974](#).

A jumphost is used to access, manage, and administer SAP virtual server instances from the same customer ZONE directly from their premises. These SAP virtual server instances can be in a separate security zone but should be on same IBM Cloud region. The customer connection to the jumphost follows the same rules as the direct connection from customer premises to the virtual server instance SAP instances. The connection uses the CFN IP and security group 1 firewall rules from a designated public subnet. In this architecture, there are two security groups defined; this arrangement is the simplest method for separating the public and private subnets. You can add more security groups if you require more isolation.

Virtual server instances on SAP NetWeaver 7.x APAB stack, Java stack, and dual stack (ABAP+Java) architectural design on IBM Cloud® VPC on Unix

Standard system

In a standard system, all main instances run on a single virtual server instance within a private subnet. The virtual server instance has these components:



Architecture of SAP NetWeaver Application Server ABAP

SAP tools create a PAS instance and an ASCS instance. This method is the standard for Java Stack (System) and is now standard for ABAP Stack.

1. The Primary Application Server (PAS) - An instance is an administrative unit that contains various components of an SAP system. The components of an instance are parameterized in a shared instance profile. Each instance is identified by a system ID and an instance number and includes:

- [SAP Web Dispatcher](#) & Work Process (DIA,BTC,UPD,SPOOL) - The SAP Web Dispatcher lies between the internet and your SAP system. The SAP Web Dispatcher is the entry point for HTTP and HTTPS requests into your system, which consists of one or more SAP NetWeaver application servers. As a “software web switch”, the SAP Web dispatcher can reject or accept connections. When it accepts a connection, it balances the load to ensure an even distribution across the servers. The SAP Web Dispatcher contributes to security and also balances the load in your SAP system.

You can use the SAP Web Dispatcher in ABAP and Java systems, in pure Java systems, and in pure ABAP systems.

- [SAP Gateway Service](#) - The SAP Gateway carries out RFC services within the SAP world, which are based on [TCP/IP](#). These services enable SAP Systems and external programs to communicate with one another. RFC services can be used either in the ABAP program or for the external programs that use the interfaces. RFC can be used between processes of an instance or a system, or between systems.
- [ICM \(Internet Communication Manager\)](#) Service - Application server component that receives and dispatches Web requests (HTTP(S), SMTP, ...). ICM evaluates the URL and forwards requests to AS ABAP or AS Java.
- IGS (Internet Graphic Server)

2. The ABAP Central Services Instances (ASCS) – This instance contains the message server, the enqueue server, and a separate start. The ASCS instance cannot process any dialog requests. It is used to manage locks, exchange messages, and balance workload in the SAP system. The ASCS instance includes:

- [Message Server](#) - The SAP message server runs as a separate process, mostly on the same host as the central instance. If an SCS instance (SAP Central Services) or ASCS instance (ABAP SCS) is configured in the system, the message server is part of this instance.
- [Stand-alone Enqueue Server](#) - Part of the central instance (ABAP or Java) that manages the SAP locks. In combination with the enqueue replication server, this single point-of-failure can be made into a high availability solution.
- ABAP Central services instance (ASCS instance) - Contains the ABAP message server and the stand-alone Enqueue Server
- The enqueue replication server instance is only mandatory in a high-availability system.

Optionally, you can install the ASCS instance with an integrated:

- SAP Web Dispatcher. For more information, see [ASCS Instance with Embedded SAP Web Dispatcher](#).
- Gateway. For more information, see [ASCS Instance with Embedded Gateway](#).

Architecture of SAP NetWeaver Application Server Java

1. Java central instance ($J< nn >$ instance) – A Java instance is a unit in the AS Java cluster that is identified by its instance number. The elements that form an instance that is run on one physical machine. Also, it is possible to run several instances on one physical machine, but it is recommended that you split the different instances among different physical machines. An [AS Java Cluster Architecture](#) consists of:

- Internet Communication Manager (ICM) - The ICM is an element of the Java instance that handles requests coming from clients and dispatches them to the available server processes. Data is transferred from the ICM to the server processes and vice versa by using the Fast Channel Architecture (FCA), which allows fast and reliable communication between them
- One or several server processes - The server processes of AS Java run the Java application. They are responsible for processing incoming requests that are assigned to them by the ICM. Each server process is multi-threaded, and can therefore process many

requests simultaneously.

2. System Central Services instance (SCS instance) - Central services form the basis of communication and synchronization for the AS Java cluster. They are responsible for lock administration, message exchange, and load balancing within the cluster. Central services that are run on one physical machine and constitute a separate instance. This [SAP Central Services Instance \(SCS\)](#) comprises:

- Message Server - The message server keeps a list of all server processes in the AS Java cluster and provides information about their availability to Internet Communication Manager (ICM). It also represents the infrastructure for data exchange between the participating server processes.
- Enqueue Server - The enqueue server manages logical locks. The enqueue server runs on the Central Services instance of the Java cluster. It manages the lock table in the main memory and receives requests for setting or releasing locks. It maps the logical locks to the database.

Sybase for standard system

- Database instance (DB) - SAP Adaptive Server Enterprise (SAP ASE) in this case. The SAP systems in a landscape have specific requirements for servers, operating systems, network setup, and supported storage. Deployment of SAP AnyDB on IBM Cloud is similar to deployments with infrastructure with on-premises data centers. Therefore, use the information that is provided from SAP and the RDBMS providers. For more information, see [SAP AnyDB - SAP ASE](#) and [Infrastructure certified for SAP](#).
- Primary application server instance (PAS instance) - The global directories of the ASCS instance can be used as the global file system. That means that the host with the ASCS instance is the SAP global host. However, you can also separately install the global directories on any host of your SAP system landscape. You can also use the SAP transport host or the host with the global file system (SAP global host) as your primary application server instance host. Optionally, you can install one or more additional application server instances.
- Additional Application Server (AAS) - You can install one or more additional application server instances for an existing SAP system. Additional application server instances are optional and can be installed on separate hosts.

An additional application server instance can run on:

- The host of any instance of the existing SAP system
- On a dedicated host
- SAP Dialog Instance (DI) / Additional Application Instance (AAS) - Dialog Instance (DI) is an additional application instance on top of the Central Instance (CI). Normally the DI is set up on a different host.

Dialog instance consists of Gateway (GW), Internet Communication Manager (ICM), and Dispatcher Process (Disp) only. The DI has no Message Server and Enqueue Work Process.

DI always starts after the CI starts because the DI depends on CI as the main instance where message server and enqueue server exist. DI is used to balance the load and handle more workload rather than use only the Central Instance. The new name for DI is Additional Application Server (AAS).

Structure:

DI/AAS = GW + ICM + Disp

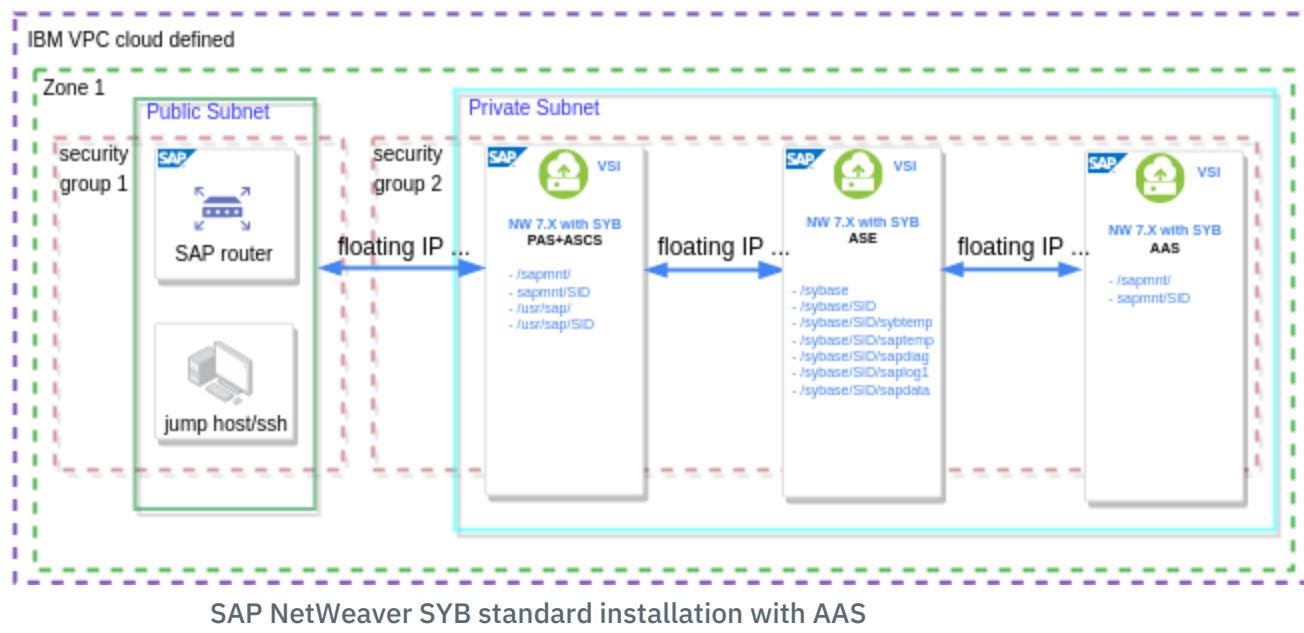
For more information about configuring and adding a AAS instance in heterogeneous SAP environment, see [SAP Note - 680617 INST: Appl. Server in Heterogeneous SAP System Environment](#).

The benefit of an AAS and DI is to balance the load from the PAS instance by distributing a significant percent of the workload, to an additional DI and AAS server. With help of SAP load balancer mechanism, the AAS and DI provide good performance. Having an AAS and additional DI increases the processing power as well, using the resources of its new server capacity for all system business workload.

For more information, see [SAP Note 26317 - Set up for LOGON group for autom load balancing](#).

Distributed system

In a distributed system, there are multiple virtual server instances and every instance can run on a separate host:



The components in a distributed system are the same as the components in a standard system, but there are restrictions as to which instances can go on which hosts.

The Sybase db and the ASE components must reside on the same virtual server instance. The SAP systems in a landscape have specific requirements for servers, operating systems, network setup, and supported storage. Deployment of SAP AnyDB on IBM Cloud is similar to deployments with infrastructure with on-premises data centers. Therefore, use the information that is provided from SAP and the RDBMS providers. To assist your project's planning phase, more design considerations are provided for SAP AnyDB - SAP ASE with IBM Cloud for SAP.

Related information

SAP One Support Notes that apply to this document:

- [SAP Note 84555 - Windows Server, Linux, and UNIX: Certified hardware](#)
- [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#)
- [SAP Note 2923773 - Linux on IBM Cloud \(IaaS\): Adaption of your SAP License](#)
- [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#)
- [SAP Note 2369910 - SAP Software on Linux: General information](#)
- [SAP Note 171380 - Released IBM hardware \(Intel processors\) and IBM cloud services offers](#)
- [SAP Note 1380654 - SAP support in IaaS environments](#)

This document is referenced by:

- [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#)
- [SAP Note 2588225 - SAP on IBM Cloud: Protect against speculative execution vulnerabilities](#)
- [SAP Note 1380654 - SAP support in IaaS environments](#)
- [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#)

SAP NetWeaver 7.x on UNIX with Db2 on IBM Cloud® VPC

Db2 is one of the many databases that can be run with SAP NetWeaver and deployed on the IBM Cloud®. The most common architecture deployments are standard and distributed. IBM Cloud is certified for running SAP NetWeaver application servers ABAP, Java, and SAP products based on these application server stacks.

SAP NetWeaver architecture

SAP NetWeaver is the core foundation of the SAP technology stacks and is the platform that is used for Advanced Business Application Programming (ABAP) and Java applications. SAP NetWeaver components are built on the SAP NetWeaver Application Server and are written in ABAP or Java Platform, Enterprise Edition. ABAP systems, Java systems, and dual-stack systems are distinct systems.

Core platform features

SAP NetWeaver uses ABAP or Java core platforms to support the SAP applications. SAP NetWeaver:

- Has application lifecycle management capabilities.
- Provides the basic structure for the on-premises versions of SAP Business Suite and other applications, as an application server.
- Is the foundation for the on-premises SAP S/4HANA next-generation business suite, with SAP HANA serving as the sole underlying database.

SAP provides a list of the [SAP versions](#) to learn more about the versions available in IBM Cloud. Each support package stack has a leading software

component version. The support package level of each component version is a key part of the stack and a unique identifier for the support package stack.

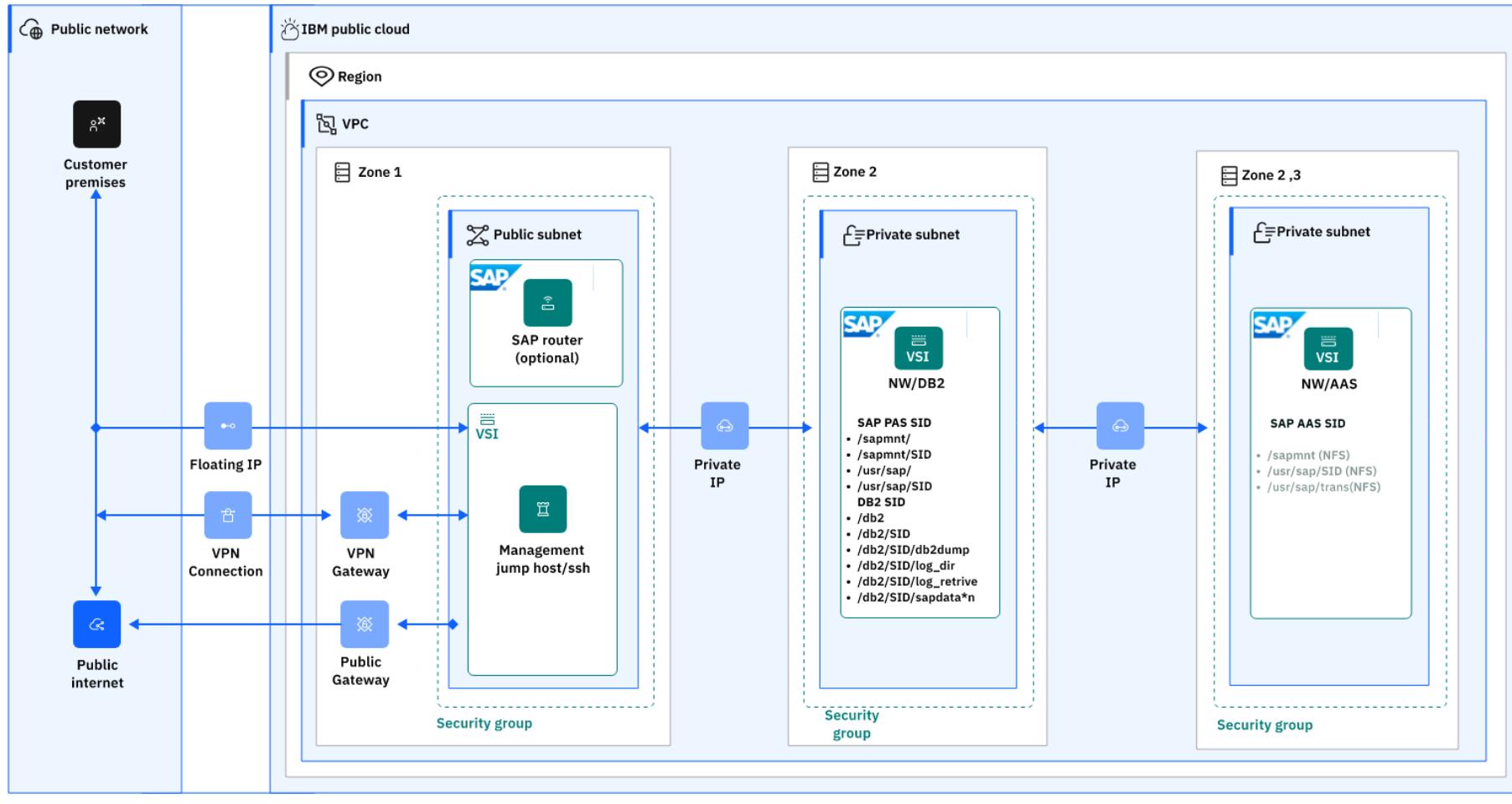
Installation types

The three installation types for SAP NetWeaver Application Server are:

- ABAP System – You can run ABAP programs and some SAP Java apps
- Java System – You can run only Java Platform, Enterprise Edition apps. No ABAP programs can be run on a Java system
- Dual Stack – You can run both ABAP and Java Platform, Enterprise Edition in separate instances

Architecture diagram

This diagram shows the SAP NetWeaver 7.X on Db2 integrated with IBM Cloud on the SAP NetWeaver 7.x architecture:



Access from an external network

Clients on the customer facing network (CFN) use a floating IP to access virtual server instances within the IBM Cloud. Virtual server instances are hosted in availability zones (data centers) within geographic regions. For more information about access, see [Connectivity to your SAP system landscape](#) and [Getting started with IBM Cloud Transit Gateway](#).

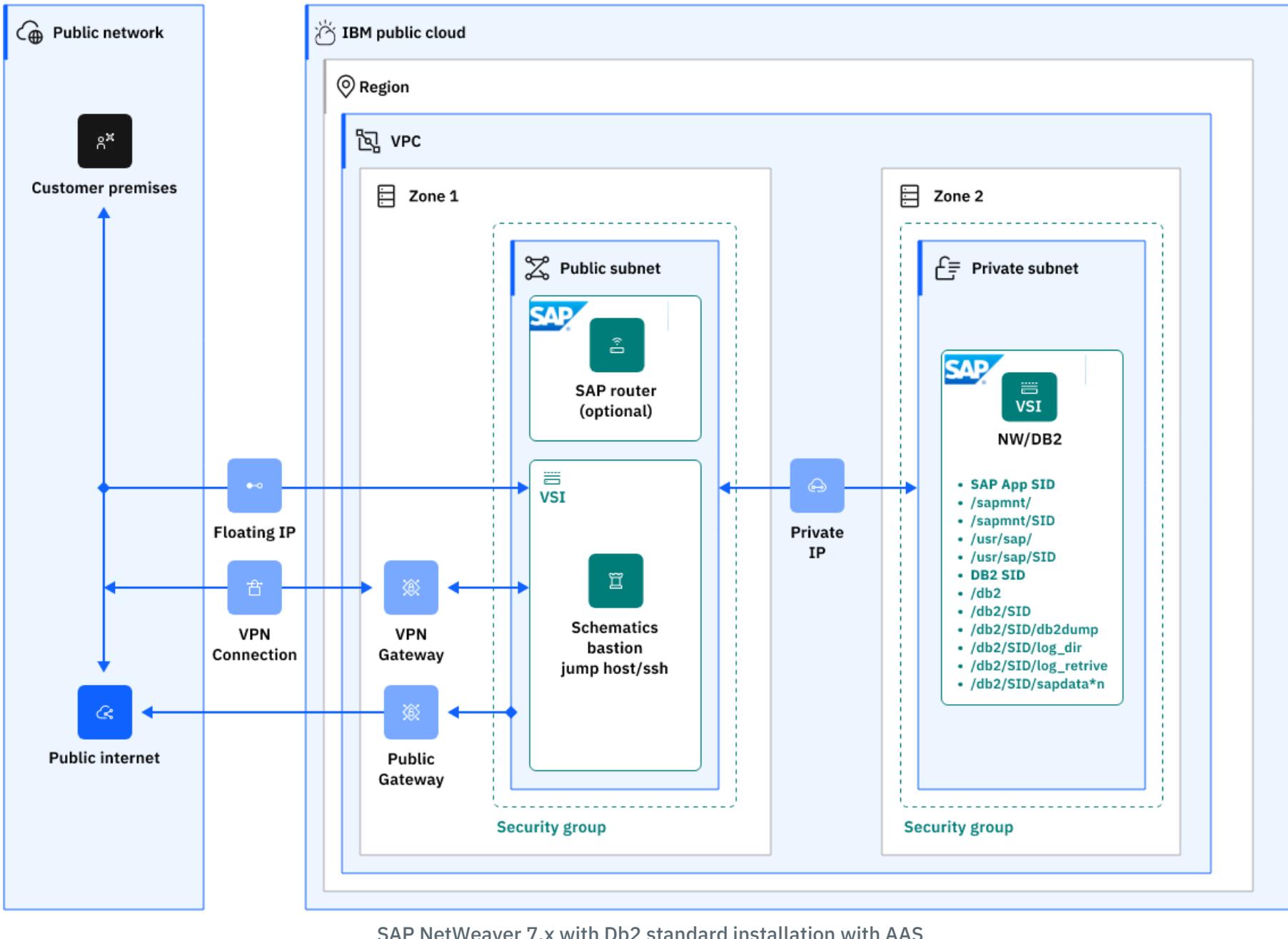
Within the Public Subnet, the [SAP router](#) and the jump host provide secure connections to the virtual server instances. The SAP router is a software application that provides a remote connection between the customer's network and SAP. The SAP Router and jump host are within a single security group with rules for inbound and outbound traffic between the private subnets in the zone. SAP routers are used with traditional SAP products and analytics solutions and offerings that are acquired from Sybase. For a comprehensive list of which SAP Business Analytics products benefits from SAP router connections, see [SAP Note 1478974](#).

A jump host is used to access, manage, and administer SAP virtual server instances from the same customer ZONE directly from their premises. These SAP virtual server instances can be in a separate security zone but must be on same IBM Cloud region. The customer connection to the jump host follows the same rules as the direct connection from customer premises to the virtual server instance SAP instances. The connection uses the CFN IP and security group 1 firewall rules from a designated public subnet. This architecture uses two defined security groups; this arrangement is the simplest method for separating the public and private subnets. You can add more security groups if you require more isolation.

Virtual server instances on SAP NetWeaver 7.x APAB stack, Java stack, and dual stack (ABAP+Java) architectural design on IBM Cloud® VPC on Unix

Standard system

In a standard system, all main instances run on a single virtual server instance within a private subnet. For more information, see [About virtual server instances for VPC](#). The virtual server instance has these components:



SAP NetWeaver 7.x with Db2 standard installation with AAS

Architecture of SAP NetWeaver Application Server ABAP

SAP tools create a PAS Instance and an ASCS Instance. This method is the standard for Java Stack (System) and is now standard for ABAP Stack.

1. The Primary Application Server (PAS) - An instance is an administrative unit that contains various components of an SAP system. The components of an instance are parameterized in a shared instance profile. Each instance is identified by a system ID and an instance number and includes:
 - [SAP Web Dispatcher](#) & Work Process (DIA,BTC,UPD,SPOOL) - The SAP Web Dispatcher lies between the internet and your SAP system. The SAP Web Dispatcher is the entry point for HTTP and HTTPS requests into your system, which consists of one or more SAP NetWeaver application servers. As a “software web switch”, the SAP Web dispatcher can reject or accept connections. When it accepts a connection, it balances the load to ensure an even distribution across the servers. The SAP Web Dispatcher contributes to security and also balances the load in your SAP system.

You can use the SAP Web Dispatcher in ABAP and Java systems, in pure Java systems, and in pure ABAP systems.
 - [SAP Gateway Service](#) - The SAP Gateway carries out RFC services within the SAP world, which are based on [TCP/IP](#). These services enable SAP Systems and external programs to communicate with one another. RFC services can be used either in the ABAP program or for the external programs that use the interfaces. RFC can be used between processes of an instance or a system, or between systems.
 - [ICM \(Internet Communication Manager\)](#) Service - Application server component that receives and dispatches Web requests (HTTP(S), SMTP, ...). ICM evaluates the URL and forwards requests to AS ABAP or AS Java.
 - IGS (Internet Graphic Server)
2. The ABAP Central Services Instances (ASCS) – This instance contains the message server, the enqueue server, and a separate start. The ASCS instance cannot process any dialog requests. It is used to manage locks, exchange messages, and balance workload in the SAP system. The ASCS instance includes:
 - [Message Server](#) - The SAP message server runs as a separate process, mostly on the same host as the central instance. If an SCS instance (SAP Central Services) or ASCS instance (ABAP SCS) is configured in the system, the message server is part of this instance.
 - [Stand-alone Enqueue Server](#) - Part of the central instance (ABAP or Java) that manages the SAP locks. In combination with the enqueue replication server, this single point-of-failure can be made into a high availability solution.
 - ABAP Central services instance (ASCS instance) - Contains the ABAP message server and the stand-alone Enqueue Server
 - The enqueue replication server instance is only mandatory in a high-availability system.

Optionally, you can install the ASCS instance with an integrated:

- SAP Web Dispatcher. For more information, see [ASCS Instance with Embedded SAP Web Dispatcher](#).
- Gateway. For more information, see [ASCS Instance with Embedded Gateway](#).

Architecture of SAP NetWeaver Application Server Java

1. Java central instance (J< nn > instance) – A Java instance is a unit in the AS Java cluster that is identified by its instance number. The elements that form an instance that is run on one physical machine. Also, it is possible to run several instances on one physical machine, but it is recommended that you split the different instances among different physical machines. A [AS Java Cluster Architecture](#) consists of:
 - Internet Communication Manager (ICM) - The ICM is an element of the Java instance that handles requests coming from clients and dispatches them to the available server processes. Data is transferred from the ICM to the server processes and vice versa by using the Fast Channel Architecture (FCA), which allows fast and reliable communication between them
 - One or several server processes - The server processes of AS Java run the Java application. They are responsible for processing incoming requests that are assigned to them by the ICM. Each server process is multi-threaded, and can therefore process many requests simultaneously.
2. System Central Services instance (SCS instance) - Central services form the basis of communication and synchronization for the AS Java cluster. They are responsible for lock administration, message exchange, and load balancing within the cluster. Central services that are run on one physical machine and constitute a separate instance. This [SAP Central Services Instance \(SCS\)](#) comprises:
 - Message Server - The message server keeps a list of all server processes in the AS Java cluster and provides information about their availability to Internet Communication Manager (ICM). It also represents the infrastructure for data exchange between the participating server processes.
 - Enqueue Server - The enqueue server manages logical locks. The enqueue server runs on the Central Services instance of the Java cluster. It manages the lock table in the main memory and receives requests for setting or releasing locks. It maps the logical locks to the database.

Db2 for standard system

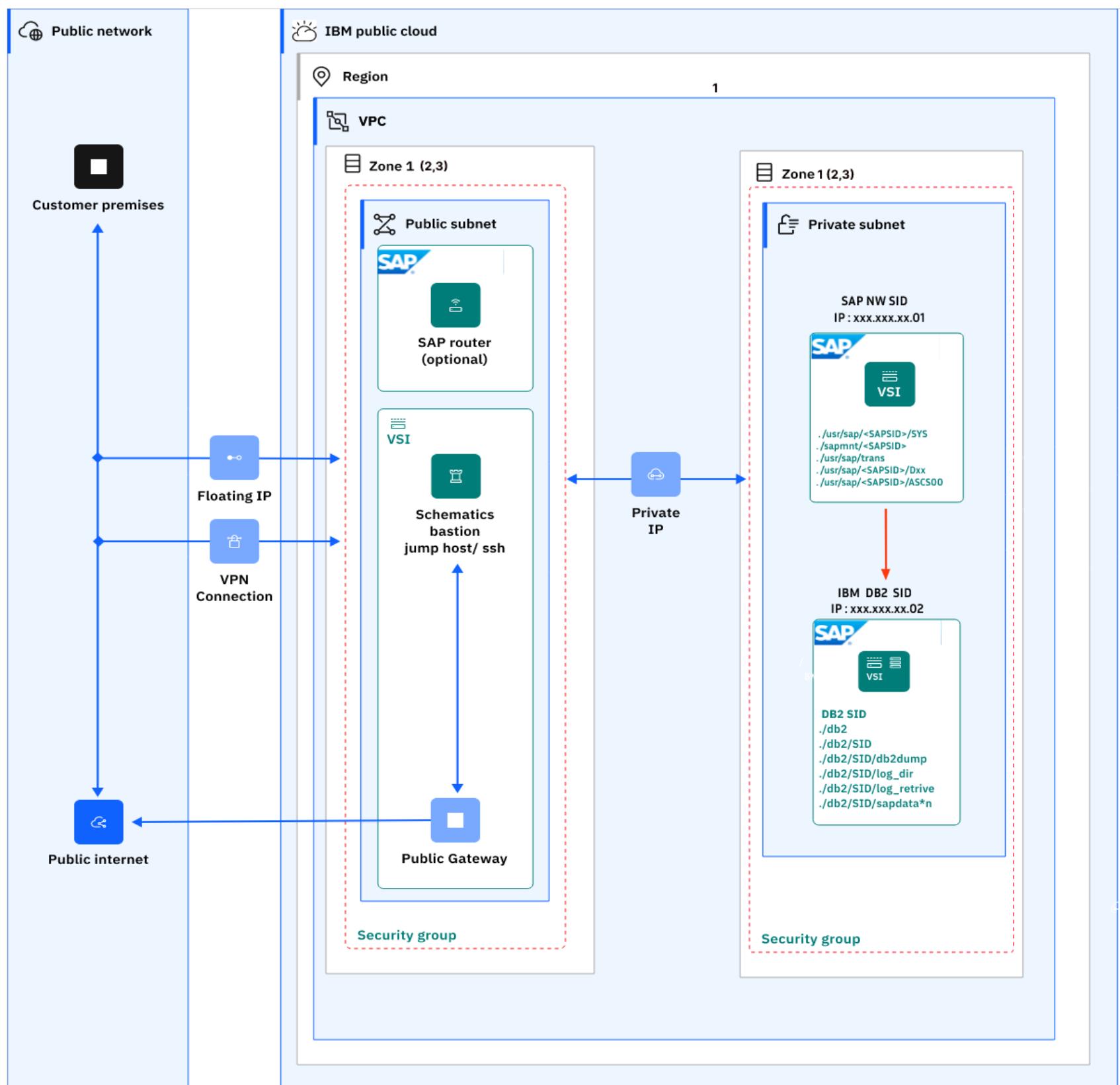
- Database instance (DB) - Db2 in this case. For more information, see [AnyDB - IBM Db2](#) and [Infrastructure certified for SAP](#).
- Primary application server instance (PAS instance) - The global directories of the ASCS instance can be used as the global file system. That means that the host with the ASCS instance is the SAP global host. However, you can also separately install the global directories on any host of your SAP system landscape. You can also use the SAP transport host or the host with the global file system (SAP global host) as your primary application server instance host. Optionally, you can install one or more extra application server instances.
- Additional Application Server (AAS) - You can install one or more extra application server instances for an existing SAP system. Additional application server instances are optional and can be installed on separate hosts.

An extra application server instance can run on:

- The host of any instance of the existing SAP system
- On a dedicated host

Distributed system

In a distributed system, there are multiple virtual server instances and every instance can run on a separate host:



SAP NetWeaver 7.x with Db2 distributed installation with AAS

The components in a distributed system are the same as the components in a standard system, but there are restrictions as to which instances can go on which hosts.

Related information

SAP One Support Notes that apply to this document:

- [SAP Note 84555 - Windows Server, Linux, and UNIX: Certified hardware](#)
- [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#)
- [SAP Note 2923773 - Linux on IBM Cloud \(IaaS\): Adaption of your SAP License](#)
- [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#)
- [SAP Note 2369910 - SAP Software on Linux: General information](#)
- [SAP Note 171380 - Released IBM hardware \(Intel processors\) and IBM cloud services offers](#)
- [SAP Note 1380654 - SAP support in IaaS environments](#)

This document is referenced by:

- [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#)
- [SAP Note 2588225 - SAP on IBM Cloud: Protect against speculative execution vulnerabilities](#)
- [SAP Note 1380654 - SAP support in IaaS environments](#)
- [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#)

SAP NetWeaver 7.x on Windows Servers with MS SQL on IBM Cloud® VPC

MS SQL Server is one of several databases that can be deployed on SAP NetWeaver in the IBM Cloud®. The most common architecture deployments are standard and distributed systems. IBM Cloud is certified for running SAP NetWeaver application servers ABAP, Java, and SAP products based on these application server stacks.

The MS SQL Server database for SAP is supported only on Windows servers and using only the Enterprise Edition of the software. Other SQL Server editions are currently not supported.

SAP NetWeaver architecture

SAP NetWeaver is the core foundation of the SAP technology stacks and is the platform that is used for Advanced Business Application Programming (ABAP) and Java applications. SAP NetWeaver components are built on the SAP NetWeaver Application Server and are written in ABAP or Java Platform, Enterprise Edition. ABAP systems, Java systems, and dual-stack systems are distinct systems.

Core platform features

SAP NetWeaver uses ABAP or Java core platforms to support the SAP applications. SAP NetWeaver:

- Has application lifecycle management capabilities.
- Provides the basic structure for the on-premises versions of SAP Business Suite and other applications, as an application server.
- Is the foundation for the on-premises SAP S/4HANA next-generation business suite, with SAP HANA serving as the sole underlying database.

SAP provides a list of the [SAP versions](#) to learn more about the versions available in IBM Cloud. Each support package stack has a leading software component version. The support package level of each component version is a key part of the stack and a unique identifier for the support package stack.

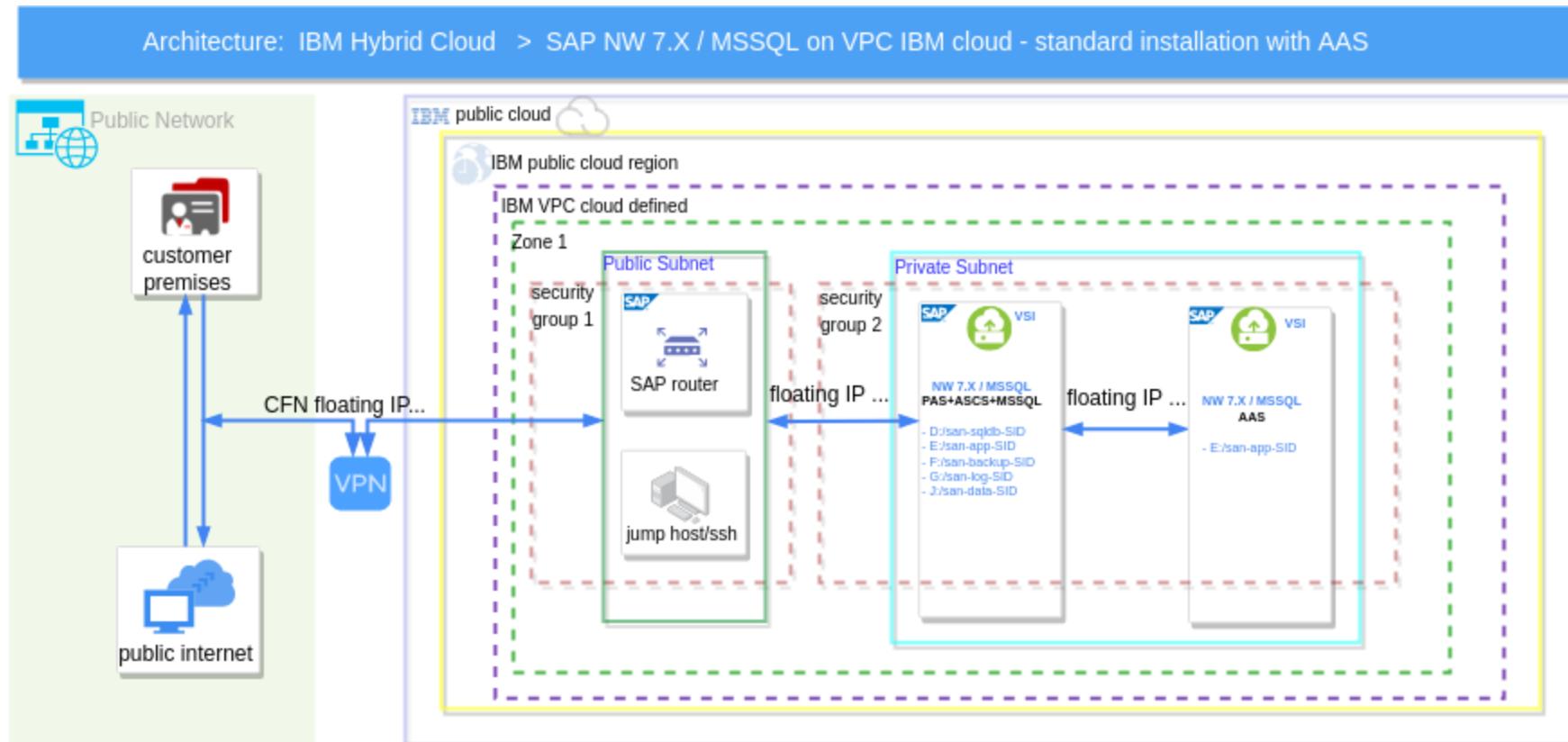
Installation types

The three installation types for SAP NetWeaver Application Server are:

- ABAP System – You can run ABAP programs and some SAP Java apps
- Java System – You can run only Java Platform, Enterprise Edition apps. No ABAP programs can be run on a Java system
- Dual Stack – You can run both ABAP and Java Platform, Enterprise Edition in separate instances

Architecture diagram

This diagram shows the SAP NetWeaver 7.X on MS SQL Server database integrated with IBM Cloud on the SAP NetWeaver 7.x architecture:



SAP NetWeaver 7.x with MS SQL Server standard installation with AAS

Access from an external network

Clients on the customer facing network (CFN) use a floating IP to access virtual server instances within the IBM Cloud. Virtual server instances are hosted in availability zones (data centers) within geographic regions.

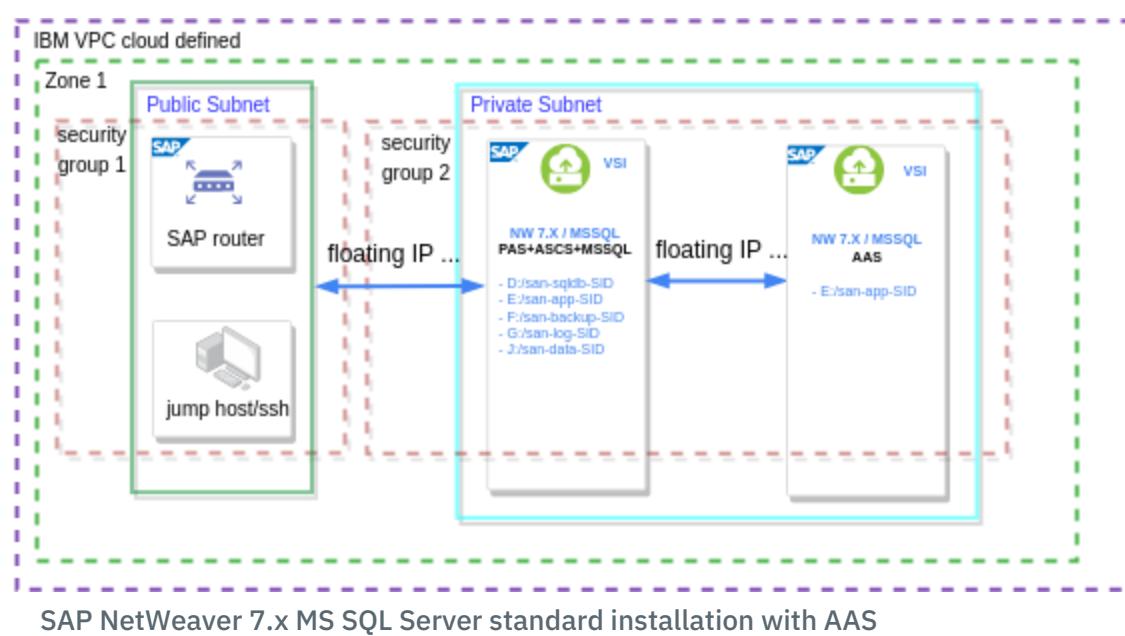
Within the Public Subnet, the [SAP router](#) and the jumphost provide secure connections to the virtual server instances. The SAP router is a software application that provides a remote connection between the customer's network and SAP. The SAP Router and jumphost are within a single security group with rules for inbound and outbound traffic between the private subnets in the zone. SAP routers are used with traditional SAP products and analytics solutions and offerings that are acquired from MS SQL Server database. For a comprehensive list of which SAP Business Analytics products benefit from SAP router connections, see [SAP Note 1478974](#).

A jumphost is used to access, manage, and administer SAP virtual server instances from the same customer ZONE directly from their premises. These SAP virtual server instances can be in a separate security zone but should be on same IBM Cloud region. The customer connection to the jumphost follows the same rules as the direct connection from customer premises to the virtual server instance SAP instances. The connection uses the CFN IP and security group 1 firewall rules from a designated public subnet. In this architecture, there are two security groups defined; this arrangement is the simplest method for separating the public and private subnets. You can add more security groups if you require more isolation.

Virtual server instances on SAP NetWeaver 7.x APAB stack, Java stack, and dual stack (ABAP+Java) stack on Windows Servers with MS SQL Server DB

Standard system

In a standard system, all main instances run on a single virtual server instance within a private subnet. The virtual server instance has these components:



Architecture of SAP NetWeaver Application Server ABAP

SAP tools create a PAS Instance and an ASCS Instance. This method is the standard for Java Stack (System) and is now standard for ABAP Stack.

1. The Primary Application Server (PAS) - An instance is an administrative unit that contains various components of an SAP system. The components of an instance are parameterized in a shared instance profile. Each instance is identified by a system ID and an instance number and includes:
 - [SAP Web Dispatcher](#) & Work Process (DIA,BTC,UPD,SPOOL) - The SAP Web Dispatcher lies between the internet and your SAP system. The SAP Web Dispatcher is the entry point for HTTP and HTTPS requests into your system, which consists of one or more SAP NetWeaver application servers. As a “software web switch”, the SAP Web dispatcher can reject or accept connections. When it accepts a connection, it balances the load to ensure an even distribution across the servers. The SAP Web Dispatcher contributes to security and also balances the load in your SAP system.
You can use the SAP Web Dispatcher in ABAP and Java systems, in pure Java systems, and in pure ABAP systems.
 - [SAP Gateway Service](#) - The SAP Gateway carries out RFC services within the SAP world, which are based on [TCP/IP](#). These services enable SAP Systems and external programs to communicate with one another. RFC services can be used either in the ABAP program or for the external programs that use the interfaces. RFC can be used between processes of an instance or a system, or between systems.
 - [ICM \(Internet Communication Manager\)](#) Service - Application server component that receives and dispatches Web requests (HTTP(S), SMTP, ...). ICM evaluates the URL and forwards requests to AS ABAP or AS Java.
 - IGS (Internet Graphic Server)
2. The ABAP Central Services Instances (ASCS) – This instance contains the message server, the enqueue server, and a separate start. The ASCS instance cannot process any dialog requests. It is used to manage locks, exchange messages, and balance workload in the SAP system. The ASCS instance includes:

- [Message Server](#) - The SAP message server runs as a separate process, mostly on the same host as the central instance. If an SCS instance (SAP Central Services) or ASCS instance (ABAP SCS) is configured in the system, the message server is part of this instance.
- [Stand-alone Enqueue Server](#) - Part of the central instance (ABAP or Java) that manages the SAP locks. In combination with the enqueue replication server, this single point-of-failure can be made into a high availability solution.
- ABAP Central services instance (ASCS instance) - Contains the ABAP message server and the stand-alone Enqueue Server
- The enqueue replication server instance is only mandatory in a high-availability system.

Optionally, you can install the ASCS instance with an integrated:

- SAP Web Dispatcher. For more information, see [ASCS Instance with Embedded SAP Web Dispatcher](#).
- Gateway. For more information, see [ASCS Instance with Embedded Gateway](#).

Architecture of SAP NetWeaver Application Server Java

1. Java central instance (J< nn > instance) – A Java instance is a unit in the AS Java cluster that is identified by its instance number. The elements that form an instance that is run on one physical machine. Also, it is possible to run several instances on one physical machine, but it is recommended that you split the different instances among different physical machines. An [AS Java Cluster Architecture](#) consists of:
 - Internet Communication Manager (ICM) - The ICM is an element of the Java instance that handles requests coming from clients and dispatches them to the available server processes. Data is transferred from the ICM to the server processes and vice versa by using the Fast Channel Architecture (FCA), which allows fast and reliable communication between them
 - One or several server processes - The server processes of AS Java run the Java application. They are responsible for processing incoming requests that are assigned to them by the ICM. Each server process is multi-threaded, and can therefore process many requests simultaneously.
2. System Central Services instance (SCS instance) - Central services form the basis of communication and synchronization for the AS Java cluster. They are responsible for lock administration, message exchange, and load balancing within the cluster. Central services that are run on one physical machine and constitute a separate instance. This [SAP Central Services Instance \(SCS\)](#) comprises:
 - Message Server - The message server keeps a list of all server processes in the AS Java cluster and provides information about their availability to Internet Communication Manager (ICM). It also represents the infrastructure for data exchange between the participating server processes.
 - Enqueue Server - The enqueue server manages logical locks. The enqueue server runs on the Central Services instance of the Java cluster. It manages the lock table in the main memory and receives requests for setting or releasing locks. It maps the logical locks to the database.

MS SQL for standard system

- Database instance (DB) - MS SQL Server in this case. The SAP systems in a landscape have specific requirements for servers, operating systems, network setup, and supported storage. Deployment of SAP AnyDB on IIBM Cloud is similar to deployments with infrastructure with on-premises data centers. Use the information that is provided from SAP and the RDBMS providers. For more information, see [AnyDB - Microsoft SQL Server](#) and [Infrastructure certified for SAP](#).
- Primary application server instance (PAS instance) - The global directories of the ASCS instance can be used as the global file system. That means that the host with the ASCS instance is the SAP global host. However, you can also separately install the global directories on any host of your SAP system landscape. You can also use the SAP transport host or the host with the global file system (SAP global host) as your primary application server instance host. Optionally, you can install one or more additional application server instances.
- Additional Application Server (AAS) - You can install one or more additional application server instances for an existing SAP system. Additional application server instances are optional and can be installed on separate hosts.

An additional application server instance can run on:

- The host of any instance of the existing SAP system
- On a dedicated host
- SAP Dialog Instance (DI) / Additional Application Instance (AAS) - Dialog Instance (DI) is an additional application instance on top of the Central Instance (CI). Normally the DI is set up on a different host.

Dialog instance consists of Gateway (GW), Internet Communication Manager (ICM), and Dispatcher Process (Disp) only. The DI has no Message Server and Enqueue Work Process.

DI always starts after the CI starts because the DI depends on CI as the main instance where message server and enqueue server exist. DI is used to balance the load and handle more workload rather than use only the Central Instance. The new name for DI is Additional Application Server (AAS).

Structure:

DI/AAS = GW + ICM + Disp

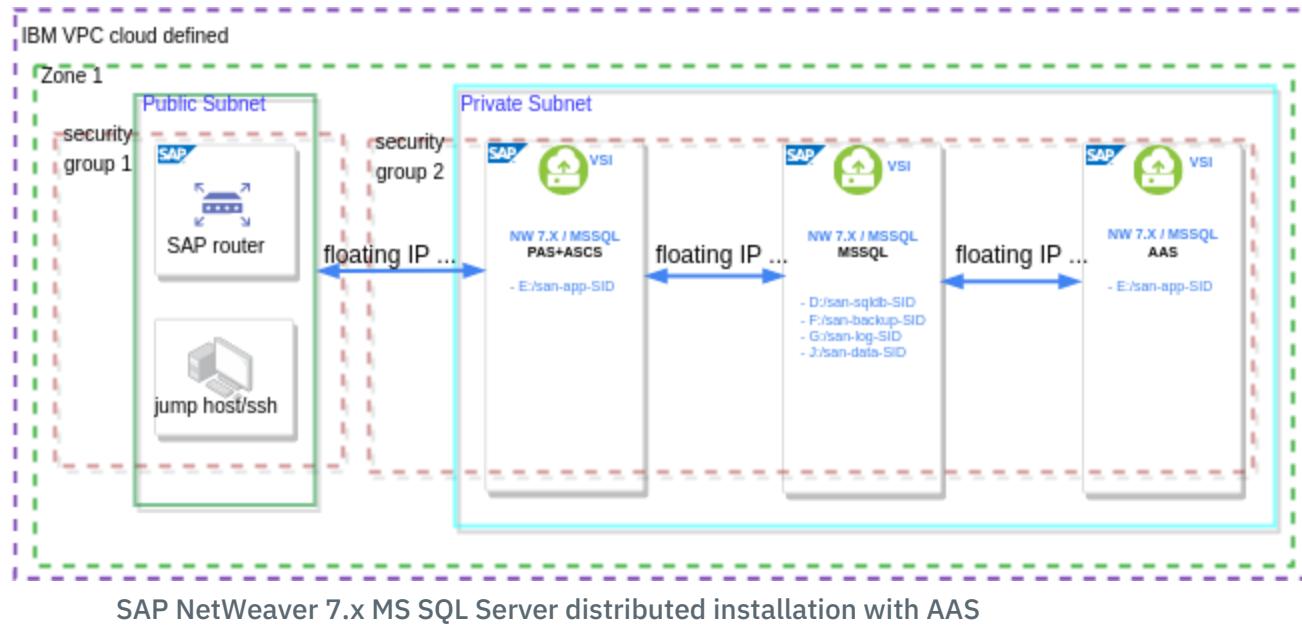
For more information about configuring and adding a AAS instance in heterogeneous SAP environment, see [SAP Note 680617 - INST: Appl. Server in Heterogeneous SAP System Environment](#).

The benefit of an AAS and DI is to balance the load from the PAS instance by distributing a significant percent of the workload, to an additional DI and AAS server. With help of SAP load balancer mechanism, the AAS and DI provide good performance. Having an AAS and additional DI increases the processing power as well, using the resources of its new server capacity for all system business workload.

For more information, see [SAP Note 26317 - Set up for LOGON group for autom load balancing](#).

Distributed system

In a distributed system, there are multiple virtual server instances and every instance can run on a separate host:



The components in a distributed system are the same as the components in a standard system, but there are restrictions as to which instances can go on which hosts.

Related information

SAP One Support Notes that apply to this document:

- [SAP Note 84555 - Windows Server, Linux, and UNIX: Certified hardware](#)
- [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#)
- [SAP Note 2923773 - Linux on IBM Cloud \(IaaS\): Adaption of your SAP License](#)
- [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#)
- [SAP Note 2369910 - SAP Software on Linux: General information](#)
- [SAP Note 171380 - Released IBM hardware \(Intel processors\) and IBM cloud services offers](#)
- [SAP Note 1380654 - SAP support in IaaS environments](#)

This document is referenced by:

- [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#)
- [SAP Note 2588225 - SAP on IBM Cloud: Protect against speculative execution vulnerabilities](#)
- [SAP Note 1380654 - SAP support in IaaS environments](#)
- [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#)

SAP NetWeaver 7.x with SAP HANA IBM Cloud® VPC

SAP HANA is one of several databases that can be deployed on SAP NetWeaver in the IBM Cloud®. SAP HANA is an in-memory database installed on a dedicated database server. The main architecture deployments for SAP HANA are single-host or multiple-host systems. IBM Cloud is certified for running SAP NetWeaver application servers ABAP, Java, and SAP products based on these application server stacks.

SAP NetWeaver architecture

SAP NetWeaver is the core foundation of the SAP technology stacks and is the platform that is used for Advanced Business Application Programming (ABAP) and Java applications. SAP NetWeaver components are built on the SAP NetWeaver Application Server and are written in ABAP or Java Platform, Enterprise Edition. ABAP systems, Java systems, and dual-stack systems are distinct systems.

Core platform features

SAP NetWeaver uses ABAP or Java core platforms to support the SAP applications. SAP NetWeaver:

- Has application lifecycle management capabilities.
- Provides the basic structure for the on-premises versions of SAP Business Suite and other applications, as an application server.
- Is the foundation for the on-premises SAP S/4HANA next-generation business suite, with SAP HANA serving as the sole underlying database.

SAP provides a list of the [SAP versions](#) to learn more about the versions available in IBM Cloud. Each support package stack has a leading software component version. The support package level of each component version is a key part of the stack and a unique identifier for the support package stack.

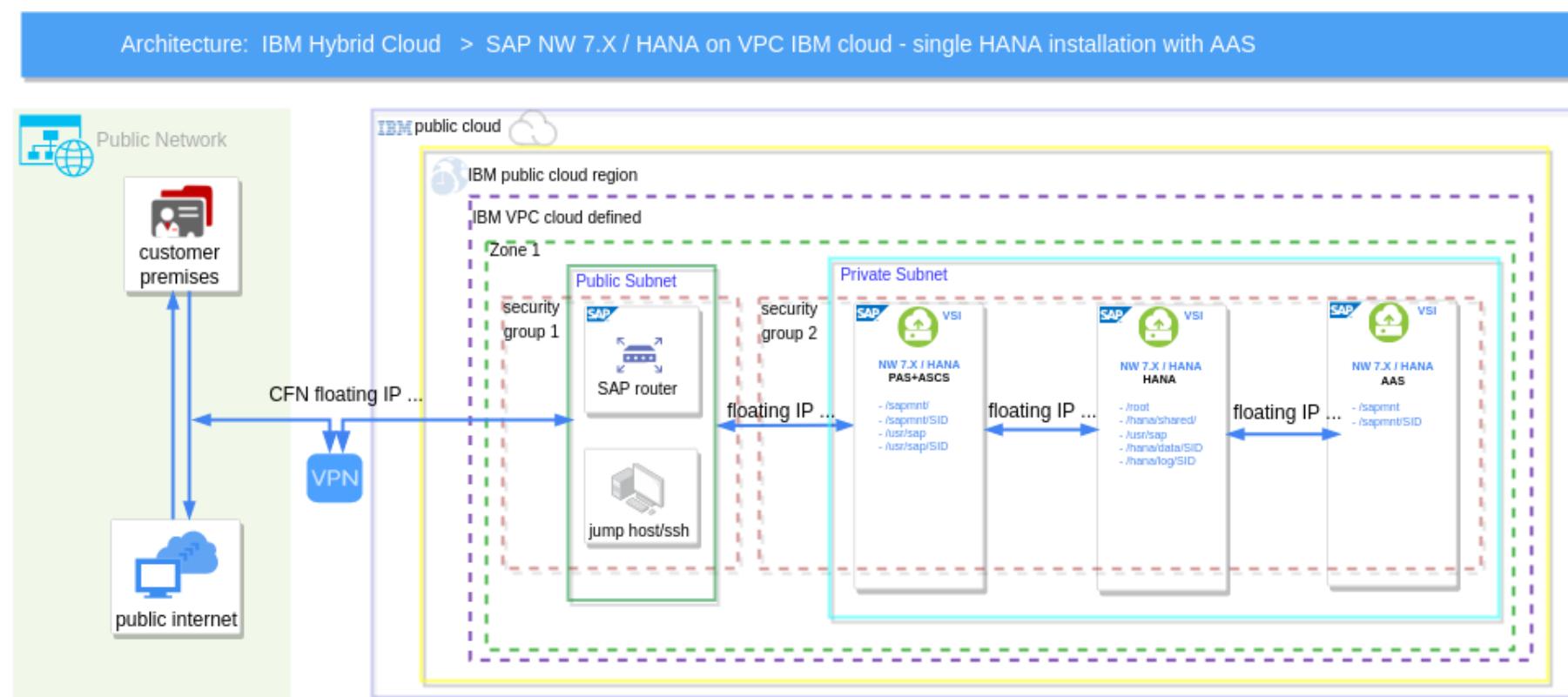
Installation types

The three installation types for SAP NetWeaver Application Server are:

- ABAP System – You can run ABAP programs and some SAP Java apps
- Java System – You can run only Java Platform, Enterprise Edition apps. No ABAP programs can be run on a Java system
- Dual Stack – You can run both ABAP and Java Platform, Enterprise Edition in separate instances

Architecture diagram

This diagram shows the SAP NetWeaver 7.X on SAP HANA Server database integrated with IBM Cloud on the SAP NetWeaver 7.x architecture:



SAP NetWeaver 7.x with SAP HANA database single-host installation with AAS

Access from an external network

Clients on the customer facing network (CFN) use a floating IP to access virtual server instances within the IBM Cloud. Virtual server instances are hosted in availability zones (data centers) within geographic regions.

Within the Public Subnet, the [SAP router](#) and the jumphost provide secure connections to the virtual server instances. The SAP router is a software application that provides a remote connection between the customer's network and SAP. The SAP Router and jumphost are within a single security group with rules for inbound and outbound traffic between the private subnets in the zone. SAP routers are used with traditional SAP products and analytics solutions and offerings that are acquired from MS SQL Server database. For a comprehensive list of which SAP Business Analytics products benefit from SAP router connections, see [SAP Note 1478974](#).

A jumphost is used to access, manage, and administer SAP virtual server instances from the same customer ZONE directly from their premises. These SAP virtual server instances can be in a separate security zone but should be on same IBM Cloud region. The customer connection to the jumphost follows the same rules as the direct connection from customer premises to the virtual server instance SAP instances. The connection uses the CFN IP and security group 1 firewall rules from a designated public subnet. In this architecture, there are two security groups defined; this arrangement is the simplest method for separating the public and private subnets. You can add more security groups if you require more isolation.

Virtual server instances on SAP NetWeaver 7.x with SAP HANA database

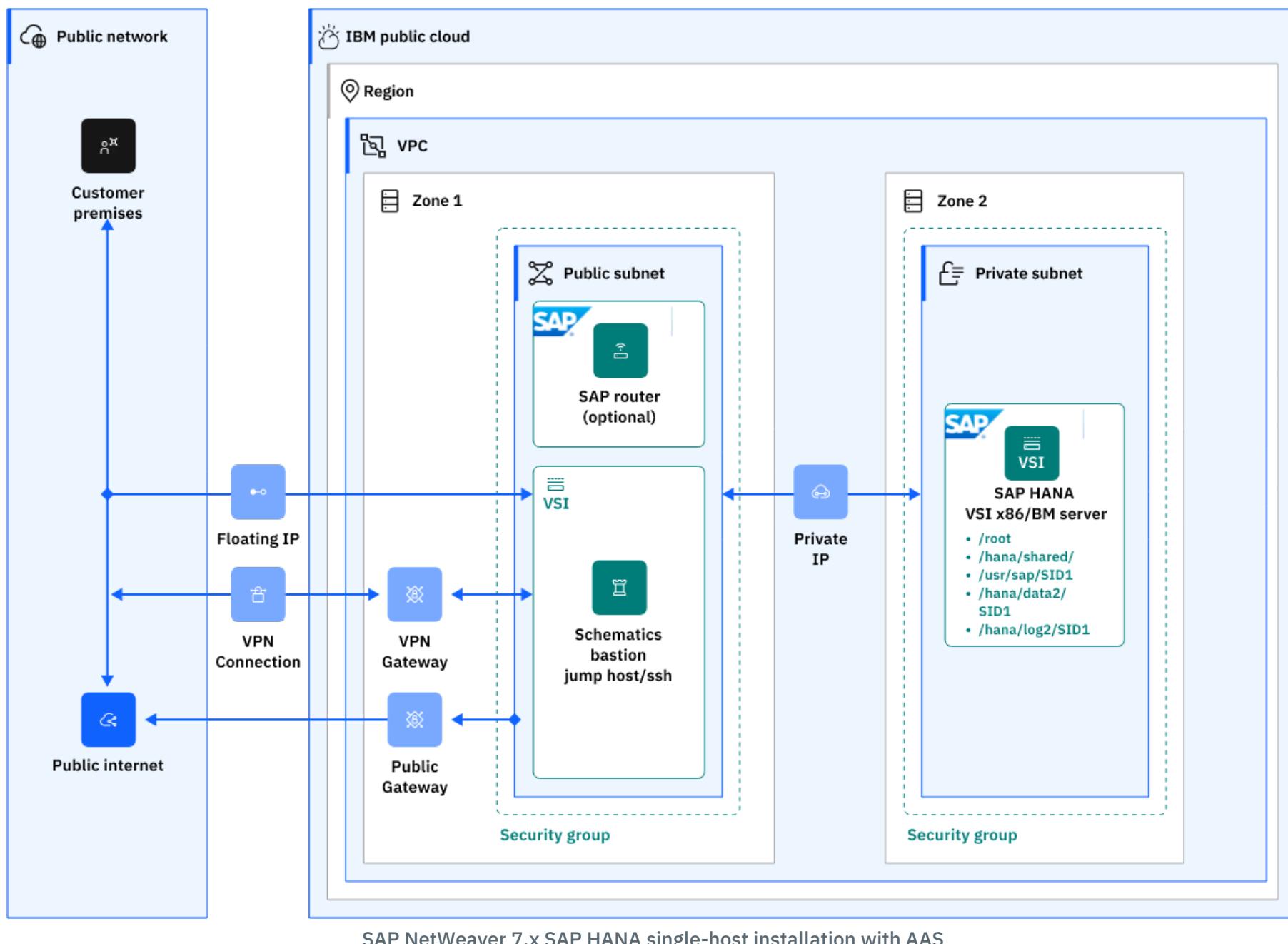
The number of hosts in an SAP HANA system landscape determines the SAP HANA system type.

An SAP HANA system can be configured as either:

- A single-host system - One SAP HANA instance on one host.
- A distributed system (multiple-host system) - Multiple SAP HANA instances distributed over multiple hosts,

Single-host HANA system

A single-host system is the simplest system installation type that runs an SAP HANA system entirely on one host. You can scale the system up as needed. The single-host system has these components:



Architecture of SAP NetWeaver Application Server ABAP

SAP tools create a PAS Instance and an ASCS Instance. This method is the standard for Java Stack (System) and is now standard for ABAP Stack.

1. The Primary Application Server (PAS) - An instance is an administrative unit that contains various components of an SAP system. The components of an instance are parameterized in a shared instance profile. Each instance is identified by a system ID and an instance number and includes:
 - [SAP Web Dispatcher](#) & Work Process (DIA,BTC,UPD,SPOOL) - The SAP Web Dispatcher lies between the internet and your SAP system. The SAP Web Dispatcher is the entry point for HTTP and HTTPS requests into your system, which consists of one or more SAP NetWeaver application servers. As a “software web switch”, the SAP Web dispatcher can reject or accept connections. When it accepts a connection, it balances the load to ensure an even distribution across the servers. The SAP Web Dispatcher contributes to security and also balances the load in your SAP system.
 - You can use the SAP Web Dispatcher in ABAP and Java systems, in pure Java systems, and in pure ABAP systems.
 - [SAP Gateway Service](#) - The SAP Gateway carries out RFC services within the SAP world, which are based on [TCP/IP](#). These services enable SAP Systems and external programs to communicate with one another. RFC services can be used either in the ABAP program or for the external programs that use the interfaces. RFC can be used between processes of an instance or a system, or between systems.
 - [ICM \(Internet Communication Manager\)](#) Service - Application server component that receives and dispatches Web requests (HTTP(S), SMTP, ...). ICM evaluates the URL and forwards requests to AS ABAP or AS Java.

- IGS (Internet Graphic Server)
2. The ABAP Central Services Instances (ASCS) – This instance contains the message server, the enqueue server, and a separate start. The ASCS instance cannot process any dialog requests. It is used to manage locks, exchange messages, and balance workload in the SAP system. The ASCS instance includes:
- [Message Server](#) - The SAP message server runs as a separate process, mostly on the same host as the central instance. If an SCS instance (SAP Central Services) or ASCS instance (ABAP SCS) is configured in the system, the message server is part of this instance.
 - [Stand-alone Enqueue Server](#) - Part of the central instance (ABAP or Java) that manages the SAP locks. In combination with the enqueue replication server, this single point-of-failure can be made into a high availability solution.
 - ABAP Central services instance (ASCS instance) - Contains the ABAP message server and the stand-alone Enqueue Server
 - The enqueue replication server instance is only mandatory in a high-availability system.

Optionally, you can install the ASCS instance with an integrated:

- SAP Web Dispatcher. For more information, see [ASCS Instance with Embedded SAP Web Dispatcher](#).
- Gateway. For more information, see [ASCS Instance with Embedded Gateway](#).

Architecture of SAP NetWeaver Application Server Java

1. Java central instance (J< nn > instance) – A Java instance is a unit in the AS Java cluster that is identified by its instance number. The elements that form an instance that is run on one physical machine. Also, it is possible to run several instances on one physical machine, but it is recommended that you split the different instances among different physical machines. An [AS Java Cluster Architecture](#) consists of:
 - Internet Communication Manager (ICM) - The ICM is an element of the Java instance that handles requests coming from clients and dispatches them to the available server processes. Data is transferred from the ICM to the server processes and vice versa by using the Fast Channel Architecture (FCA), which allows fast and reliable communication between them
 - One or several server processes - The server processes of AS Java run the Java application. They are responsible for processing incoming requests that are assigned to them by the ICM. Each server process is multi-threaded, and can therefore process many requests simultaneously.
2. System Central Services instance (SCS instance) - Central services form the basis of communication and synchronization for the AS Java cluster. They are responsible for lock administration, message exchange, and load balancing within the cluster. Central services that are run on one physical machine and constitute a separate instance. This [SAP Central Services Instance \(SCS\)](#) comprises:
 - Message Server - The message server keeps a list of all server processes in the AS Java cluster and provides information about their availability to Internet Communication Manager (ICM). It also represents the infrastructure for data exchange between the participating server processes.
 - Enqueue Server - The enqueue server manages logical locks. The enqueue server runs on the Central Services instance of the Java cluster. It manages the lock table in the main memory and receives requests for setting or releasing locks. It maps the logical locks to the database.

SAP HANA for standard system

- Primary application server instance (PAS) - The global directories of the ASCS instance can be used as the global file system. That means that the host with the ASCS instance is the SAP global host. However, you can also separately install the global directories on any host of your SAP system landscape. You can also use the SAP transport host or the host with the global file system (SAP global host) as your primary application server instance host. Optionally, you can install one or more additional application server instances.
- Database instance (DB) - To assist your project's planning phase, more design considerations are provided at SAP AnyDB – SAP HANA database with IBM Cloud for SAP. For more information, see [AnyDB - SAP HANA](#) and [Infrastructure certified for SAP](#).
- Additional Application Server (AAS) - You can install one or more additional application server instances for an existing SAP system. Additional application server instances are optional and can be installed on separate hosts.
- SAP Dialog Instance (DI) / Additional Application Instance (AAS) - Dialog Instance (DI) is an additional application instance on top of the Central Instance (CI). Normally the DI is set up on a different host.

Dialog instance consists of Gateway (GW), Internet Communication Manager (ICM), and Dispatcher Process (Disp) only. The DI has no Message Server and Enqueue Work Process.

DI always starts after the CI starts because the DI depends on CI as the main instance where message server and enqueue server exist. DI is used to balance the load and handle more workload rather than use only the Central Instance. The new name for DI is Additional Application Server (AAS).

Structure:

DI/AAS = GW + ICM + Disp

For more information about configuring and adding a AAS instance in heterogeneous SAP environment, see [SAP Note - 680617 INST: Appl. Server in Heterogeneous SAP System Environment](#).

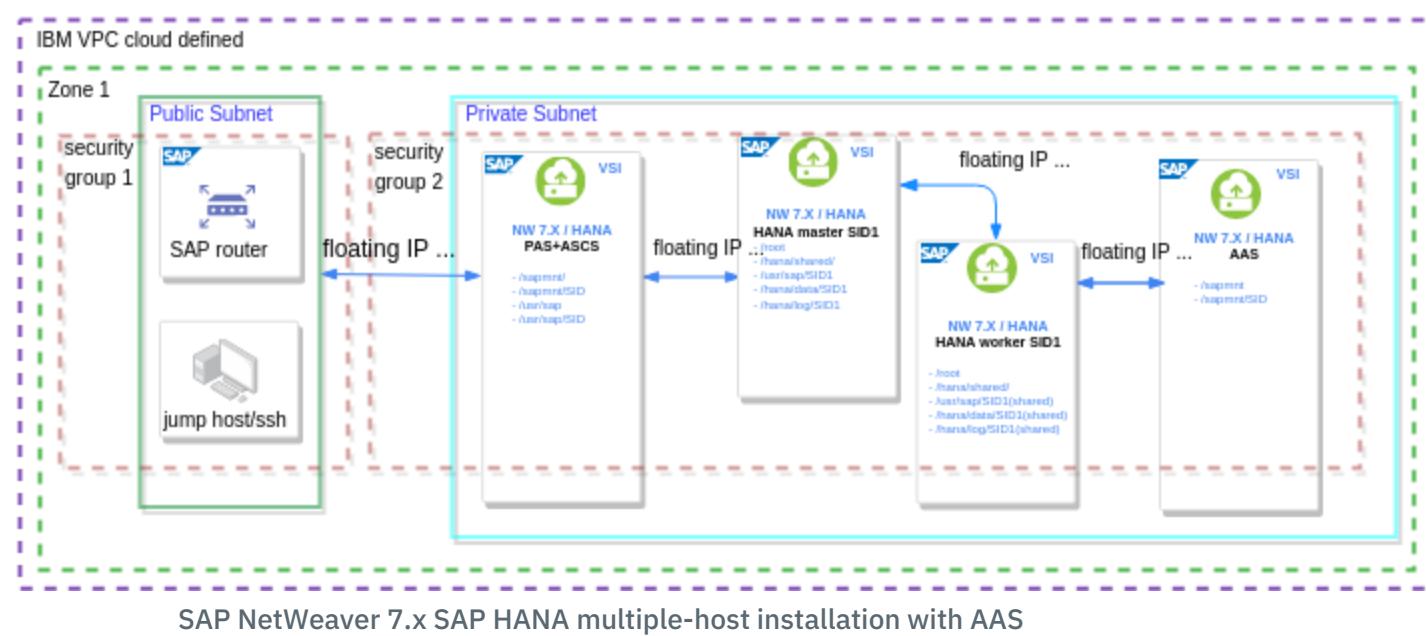
The benefit of an AAS and DI is to balance the load from the PAS instance by distributing a significant percent of the workload, to an additional DI and AAS server. With help of SAP load balancer mechanism, the AAS and DI provide good performance. Having an AAS and additional DI increases the processing power as well, using the resources of its new server capacity for all system business workload.

For more information, see [SAP Note 26317 - Set up for LOGON group for autom load balancing](#).

Multiple-host SAP HANA system

A multiple-host system is a system with more than one host, which can be configured as active worker hosts or idle standby hosts. The server software is based on a flexible architecture that enables a distributed installation in which loads are balanced between different hosts. The server software has to be installed in a shared file system. This file system has to be mounted by all hosts that are part of the system.

This diagram shows a multiple-host system configuration:



The SAP components in a multi-host SAP HANA system are the same as the components in a single-host SAP HANA system, the difference consists of multiple connected hosts for the SAP HANA database.

A multi-host SAP HANA system might be necessary to scale SAP HANA either by increasing RAM for a single server, or by adding hosts to the system to deal with larger workloads. This allows you to go beyond the limits of a single physical server.

When configuring a multiple-host system, the individual hosts must be defined as master, worker, slave, and standby depending on the task. Worker machines process data; standby machines do not handle any processing and instead just wait to take over processes in the case of worker machine failure.

Related information

SAP One Support Notes that apply to this document:

- [SAP Note 84555 - Windows Server, Linux, and UNIX: Certified hardware](#)
- [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#)
- [SAP Note 2923773 - Linux on IBM Cloud \(IaaS\): Adaption of your SAP License](#)
- [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#)
- [SAP Note 2369910 - SAP Software on Linux: General information](#)
- [SAP Note 171380 - Released IBM hardware \(Intel processors\) and IBM cloud services offers](#)
- [SAP Note 1380654 - SAP support in IaaS environments](#)

This document is referenced by:

- [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#)
- [SAP Note 2588225 - SAP on IBM Cloud: Protect against speculative execution vulnerabilities](#)
- [SAP Note 1380654 - SAP support in IaaS environments](#)
- [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#)

Getting help and support from IBM Cloud or SAP

If you experience problems with IBM Cloud, you have several options to get help with determining the cause of the problem and finding a solution.

Which support option depends on the level of support (and urgency), and whether the problem is with the Offering or running SAP Workloads using the Offering.

Options include:

- IBM Cloud Support Case, using the [IBM Cloud Support Center](#)
- SAP support incident, using the [SAP for Me](#)
- IBM Cloud Docs



Note: For previous users of IBM Cloud Classic Infrastructure (formerly Softlayer), please be aware these Support Cases were previously termed Support Tickets.

IBM Cloud Support

IBM Cloud Support handles any support questions and issues that might arise - available through live web chat, phone, and case-based support.

Each IBM Cloud account automatically comes with customer support at no cost and covers most cases which are placed each day; this is the Basic level of support.

The types of available and response time of support, depends on the support level of the account. Your support plan also determines the severity level that you can assign to support cases. For more information, see [Basic, Advanced, and Premium Support plans](#).

You can change your current support plan at any time by contacting IBM Cloud sales expert.

For full information about opening an IBM Cloud Support case, or about support levels and ticket severities, see [IBM Cloud Support documentation](#).



Tip: If you need support but are unable to log in to your account, start a chat by going to the [IBM Cloud Support](#) page and clicking **Let's talk**.

New support case with IBM Cloud Support

If you need to open a support case, collect as much information as possible to help the IBM Cloud Support team to analyze, triage and diagnose your problem as quickly as possible.

Requesting support for SAP-certified IBM Power Virtual Servers

All performance-related issues need to be checked by IBM Power Systems and IBM Cloud support first, to establish whether any infrastructure-related issues exist, before a case of the software stack (SAP Workloads) can be opened.

If the issue is operating system (OS) related, go the support portal of the distribution (AIX or Linux®) to open a case.



Tip: You can check whether the infrastructure is set up correctly by running a python script on Linux®: `python chk numa lpm.py`. For more information, see [SAP Note 2923962 -- Check SAP HANA NUMA Layout on IBM Power Systems Virtual Servers](#).

Requesting support for resources in the European Union

European Union (EU) support is available to customers who choose to enable the EU supported setting. EU Support is provided 24 hours a day and 7 days a week by engineers that are located in Europe.

Global teams provide support at the discretion of the EU support team. Global teams might be contacted, for example, when issues are not resolved by the Advanced Customer Support (ACS) team in the EU, and more expertise is needed.

You can specify that you want EU support for your account if the following criteria are true:

- The EU Supported setting is enabled for your account by the primary user or account owner. For more information, see [Enabling the EU Supported setting](#).
- Your resources are in the appropriate European data center. For more information, see [Data centers](#).
- You select the EU supported case level when you open the case.



Note: IBM Cloud offerings hosted in the Frankfurt location must be supported by a team that is physically located in Europe.

Enabling the EU Support setting for your account applies to all future cases that you open for issues on any service or data center that is hosted in the EU region. However, if you add resources outside of an EU location, issues for those resources are not necessarily handled by a support team in Europe. Any cases that are opened before you enable the EU Supported setting are not affected.

SAP ONE Support

You can also continue to create tickets through SAP Support that are related to your IBM Cloud IaaS and SAP products. For more information, see [SAP Support](#) and [SAP Note 2414820 - SAP on IBM Cloud: Support prerequisites](#).

The [SAP for Me](#) provides access to task-driven support resources from SAP, available with live web chat or incident tickets, and the following features:

- Knowledge Base for SAP Notes
- Incidents for connection with SAP Product Support teams
- Software Downloads
- Systems, Installations and License Keys

[Full information on SAP Support](#) provides additional details, including guidance on how to use the SAP ONE Support Launchpad.

SAP ONE Support process for IBM Power

If the issue is related to IBM Power and SAP, open a case by going to [support.sap.com](#) and click **Report an Incident**.

All performance-related issues must be checked by [IBM Cloud Customer Support](#) first to rule out any infrastructure-related issues before a case on the software stack is opened.

Provide details and run the following commands to attach the output to the case:

- For AIX:
 - `perfsap` on [SAP Note 1170252](#)
- For Linux:
 - `sapsysinfo` on [SAP Note 618104](#)
 - `supportconfig` on [SAP Note 1642802](#)
 - and for SAP HANA also use `full-system-info-dump` on [SAP Note 1732157](#)

Stack Overflow

The Stack Overflow forum provides a wide variety of searchable answers for your IBM Cloud questions. If you don't find an existing answer, ask a new question. Go to [Stack Overflow](#).

IBM Cloud development and support teams actively monitor Stack Overflow and follow the questions that are tagged with **ibm-cloud**. When you create a question, add the **ibm-cloud** tag to your question to ensure that it's seen by the IBM Cloud development and support teams.

FAQs

FAQ of IBM Cloud® for SAP

Introduction

This FAQ provides answers to questions about:

- [IBM Cloud® for SAP portfolio](#)
- [Licensing and pricing](#)
- [RISE with SAP Subscription Model](#)
- [SAP-certified IBM Power Virtual Servers](#)
- [SAP HANA database](#)
- [SAP NetWeaver and SAP applications](#)
- [SAP Notes for the IBM Cloud® for SAP portfolio](#)

Additional FAQs cover specific topics, such as:

- [Moving SAP Workloads](#)

IBM Cloud for SAP portfolio

Can SAP workloads run on any IBM Cloud server?

No, SAP HANA and SAP NetWeaver run only on SAP-certified instances on IBM Power Virtual Server® and IBM Cloud instances.

For proof of concept (POC) or evaluation, a non-certified instance can be used to explore IBM Cloud at a lower cost. However, SAP software may not function as designed on a non-certified server and is not supported by SAP.



Note: SAP considers both production and development/testing (dev/test) systems as productive systems, as specified in [SAP Note 2271345](#).

Can SAP software installation media and distributions be downloaded directly from IBM Cloud?

No, all SAP software installation media is available directly from SAP at [sap.com](#).



Note: SAP ID credentials are required to download SAP software installation media.

Who is responsible for deploying SAP software on IBM Cloud?

IBM Cloud offers two deployment models for running SAP workloads:

- RISE with SAP on Power Virtual Server – A software as a service (SaaS) offering from SAP.
- SAP as an infrastructure as a service (IaaS) on IBM Cloud – A customer-managed deployment model.

IBM Cloud's IaaS is a customer-managed environment, meaning the customer or a contracted Business Partner is responsible for all changes to the operating system and deployed applications. The installation and configuration of SAP software must align with SAP's guidance for the intended business scenario and usage.

Service providers for IBM Cloud for SAP

The following table outlines service types and the business partner categories that provide them:

Service type	Provided by	Description
Consulting, advisory, and implementation	SAP Global Systems Integrator (GSI) providers	Advise and manage SAP implementation and deployment projects.

Application management	SAP Application Management Services (AMS) providers	Maintain existing SAP deployments, including optional incremental functional or development changes.
End-to-end managed services	SAP Managed Services Providers (MSP)	Oversee SAP implementation, deployment, and management of infrastructure, OS, SAP technical applications, and SAP business applications. These services typically exclude incremental functional or development changes.

Services and Business Partner Types

For example, some of the services that are available in partnership between IBM Cloud and IBM Services include:

- [GSI and IBM Services: SAP consulting and implementation services](#)
- [AMS and IBM Services: SAP application management and development solutions](#)
- [MSP and IBM Services: Managed applications for SAP](#)

Do I need IBM Db2 to run SAP NetWeaver on IBM Cloud?

No, SAP NetWeaver supports multiple SAP AnyDB options and SAP HANA on IBM Cloud-certified infrastructure. IBM Db2 is not required.

Refer to [SAP Note 2414097 for SAP Applications on IBM Cloud Classic Infrastructure environment](#) and the [SAP Product Availability Matrix](#) for details.

For IBM Db2 information, see [SAP Note 2927211](#) and the SAP on IBM Db2 for Linux, UNIX, and Windows (LUW) page on [SAP Community page](#).

Why was IBM Db2 SaaS chosen for IBM Cloud certification?

IBM Db2 is seamlessly integrated into SAP and offers:

- Lower total cost of ownership
- High performance
- Simplified administration

IBM Systems has used IBM Db2 in benchmark tests for over four decades, continuing this tradition.

Can I split my distributed SAP environment between different data centers?

It is recommended to keep all nodes in the same location (for example, availability zone or datacenter) and networking constructs (for example, subnet, VPC, and VLAN) to avoid latency and timeouts that may affect system responsiveness.

Can I split my distributed SAP environment between IBM Cloud® Bare Metal and IBM Cloud® virtual servers?

RDBMS on Intel Bare Metal Servers in the IBM Cloud Classic Infrastructure that comply to [SAP Note 2414097](#) can be supported when connected to SAP application server on IBM Cloud Virtual Private Cloud (VPC), provided they are in the same datacenter or availability zone and use IBM Cloud transit gateway local routing.

Can I achieve SAP high availability as defined by SAP architecture?

High availability for SAP can be achieved for:

- SAP NetWeaver High Availability - [SAP NetWeaver design considerations for High Availability configuration](#)
- SAP HANA High Availability - [Implementing high availability for SAP applications on IBM Power Virtual Server](#) and [SAP Note 2057595](#)
- SAP AnyDB High Availability (for example, IBM Db2, MS SQL, and so on.)
 - [Db2](#)
 - MaxDB
 - [Oracle](#)
 - SQL Server

High availability can be configured at:

- SAP Technical Application layer (for example, system replication, system clustering)
- Hardware layer (for example, storage replication)

See the respective topics in the *Get Started* section for:

- [SAP HANA design considerations for High Availability and Disaster Recovery \(HA/DR\)](#)
- [SAP HANA backups - Storage impacts on Recovery Time Objective \(RTO\)](#)

How do I connect my SAP Systems running on IBM Cloud to my on-premises systems?

IBM Cloud provides multiple secure connectivity options. Refer to [Connectivity to your SAP system landscape](#).

Licensing and pricing

How does SAP licensing work with IBM Cloud for SAP infrastructure-as-a-service?

IBM Cloud SAP-certified infrastructure follows the Bring Your Own License (BYOL) model, a standard approach for SAP workloads used for decades. This model applies to:

- SAP business application licenses (for example, SAP S/4HANA, SAP ECC)
- SAP technical application licenses (for example, SAP HANA, SAP NetWeaver)
- SAP OEM licenses (for example, SAP AnyDB OEM, such as MS SQL)

How does operating system (OS) licensing work with IBM Cloud for SAP infrastructure-as-a-service?

The OS license cost, including applicable subscriptions for SAP-specific OS packages and support, is included when selecting the OS in the order form for an SAP-certified server.

How are the SAP-certified IBM Cloud servers priced?

Pricing is available through the IBM Cloud catalogue during the ordering process. Any applicable discounts, such as those from reserved instances pricing agreements or subscription accounts, are automatically calculated.

For SAP-certified bare metal servers certified as HANA appliances, pricing includes high-performance local storage.



Note: As a standard practice among cloud service providers, IBM Cloud for SAP virtual servers use redundant network block or file storage. These storage costs may not be included in the initial price estimate. Additionally, there are no network bandwidth charges for local network traffic between the virtual server host and the storage host on IBM Cloud.

RISE with SAP subscription model

In addition to the Bring Your Own License model, RISE with SAP is a Software as a Service offering on IBM Power Virtual Server. SAP provides the software as a subscription-based service.

- [RISE with SAP on IBM Power Virtual Server](#) – A new Hyperscaler offering where SAP delivers RISE with SAP as a SaaS solution running on IBM Power Virtual Server. IBM Consulting and Global Systems Integrator (GSI) partners provide advisory, implementation, and migration services within the RISE with SAP framework.
- [BREAKTHROUGH with IBM for RISE with SAP](#) – A single-partner solution where IBM offers SAP RISE on IBM Cloud, with IBM Consulting handling advisory, implementation, and migration services.

SAP-certified IBM Power Virtual Servers

What are the operating system (OS) requirements for Db2, AIX and SAP NetWeaver?

Refer to the following SAP Notes for OS requirements:

- [SAP Note 1780629 - AIX: Minimal OS requirements for SAP kernel](#)
- [SAP Note 2267287 - Using SAP systems with AIX 7.2](#)

Where is the `aioservers` setting in AIX 7.x for Oracle installs?

The smit fast path for aioservers is unavailable because the AIO server setting updates automatically when the kernel extension detects an aio sync operation request. View the `iocp` command pages for settings and examples. For details, see [Checking Asynchronous Input Output Processes AIX 64-Bit](#).

How do I activate the iocp device when it is "Defined" during an Oracle install?

Use `smitty iocp`, navigate to Change>Show Characteristics of I/O Completion Ports, and set the state to Available at system restart. This ensures the device remains active after reboot.

If using the command line, run: `mkdev -l iocp0` (activates the device until the next reboot) `mkdev -l iocp0 -P` (ensures activation persists after reboot by updating the ODM)

What should I do if the Oracle installer precheck lists failed items?

The Oracle RUNINSTALLER precheck ensures system requirements are met before installation. Common failures include:

- Insufficient `/tmp` space: Oracle 12.2 requires 5 GB of free space. Increase available space if needed.
- Insufficient paging space: Oracle requires 12 GB of paging space. You can:
 - Extend the `hd6` Paging Logical Volume.
 - Create a new paging space using `smit mklv`, setting the LV type to paging.

After making adjustments, rerun the precheck. If no errors appear, proceed with the installation.

Where can I find central SAP Notes for installing NetWeaver on Oracle and MaxDB?

Refer to the following SAP Notes for installation details:

- Oracle: [SAP Note 2172935 - installation - SAP Systems based on SAP NetWeaver: Oracle Database](#) provides hardware, storage requirements, and required file systems.
- MaxDB: [SAP Note 2365014 - Installation of SAP Systems Based on SAP NetWeaver: SAP MaxDB](#) outlines installation steps and key details for MaxDB users.

SAP HANA

What database virtualization, sharing, or isolation options are supported in IBM Cloud infrastructure?

IBM Cloud SAP-certified infrastructure does not include database virtualization, sharing, or isolation options such as Multitenant Database Containers (MDC) testing. Customers must follow SAP guidance to:

- Properly configure SAP HANA features and functions
- Maintain infrastructure compliance with SAP certification

Is scale-out supported for SAP HANA?

Yes. For OLTP (SAP S/4HANA) see [SAP S/4HANA - Scale-up/Scale-out](#), and for OLAP (BW/4HANA) see [SAP BW/4HANA - Scale-up/Scale-out](#).

How do I back up my SAP HANA-certified servers?

Server backup is not included with Cloud infrastructure-as-a-service. Options include:

- Ordering the Cobalt Iron backup option during provisioning. See [Backup for AIX and Linux instances](#) for details.
- Using the IBM backint agent to back up SAP HANA data to IBM Cloud Object Storage.

Is there a best practice configuration check for SAP HANA?

Yes, see [SAP Note 2903141 - Best practice configuration checks for SAP HANA](#).

How can I check parameters in SAP HANA?

See [SAP Note 2600030 - Parameter Recommendations in SAP HANA Environments](#)

How can I optimize my network for SAP HANA?

The OS image provided by IBM is preconfigured for network optimization. Adjustments can be made as needed. For details, see:

- [SAP Note 2382421 - Optimizing the Network Configuration on HANA- and OS-Level](#)
- [SAP Note 2477204 - FAQ: SAP HANA Services and Ports](#)

Where can I find information on SAP ports and services?

See [TCP/IP Ports of All SAP Products](#) for detailed explanations of SAP ports and services

How can I optimize my SAP HANA performance?

See [SAP Note 2000000 - FAQ: SAP HANA Performance Optimization](#)

How can I use SAP HANA Mini Checks to monitor and highlight potential issues with my HANA implementation?

See [SAP Note 1999993 - How-To: Interpreting SAP HANA Mini Check Results](#)

Why is SAP HANA using large SWAP memory?

See [SAP Note 2779331 - HANA services use large SWAP memory](#)

SAP NetWeaver

Which versions of SAP NetWeaver are supported?

SAP NetWeaver Application Server (ABAP or Java) versions 7.0 or later are supported across the IBM Cloud for SAP portfolio.

For a full updated list of SAP NetWeaver versions and SAP Kernel Patch Levels supported for the various IaaS options, see the following SAP Notes:

- [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#)
- [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#)
- [SAP Note 2855850 - SAP Applications on IBM Power Virtual Servers](#)

List of SAP Notes for the IBM Cloud® for SAP portfolio

IBM Cloud Classic Infrastructure

- [SAP Note 2414820 - SAP on IBM Cloud: Support prerequisites](#)
- [SAP Note 2414097 - SAP Applications on IBM Cloud Classic Infrastructure environment](#)
- [SAP Note 2279688 - SAP on IBM Cloud: Support for SAP BusinessObjects](#)
- [SAP Note 2686169 - Prerequisites for installing SAP Data Hub 2](#)

IBM Cloud VPC Infrastructure

- [SAP Note 2414820 - SAP on IBM Cloud: Support prerequisites](#)
- [SAP Note 2927211 - SAP Applications on IBM Cloud Virtual Private Cloud \(VPC\) Infrastructure environment](#)

IBM Power Infrastructure connected to IBM Cloud

- [SAP Note 2923984 - SAP on IBM Power Virtual Servers: Support prerequisites](#)
- [SAP Note 2947579 - SAP HANA on IBM Power Virtual Servers](#)
- [SAP Note 2855850 - SAP Applications on IBM Power Virtual Servers](#)
- [SAP Note 2932766 - SAP on IBM Power Virtual Servers: Key Monitoring Metrics](#)

Public Cloud and virtualized environments

- [SAP Note 1380654 - SAP support in IaaS environments](#)
- [SAP Note 1122387 - Linux: SAP Support in virtualized environments](#)
- [SAP Note 1409608 - Virtualization on Windows](#)
- [SAP Note 1409604 - Virtualization on Windows: Enhanced Monitoring](#)

- [SAP Note 2134316 - Can SAP ASE run in a cloud environment?](#)
- [SAP Note 2923773 - Linux on IBM Cloud \(IaaS\): Adaption of your SAP License](#)

IBM Cloud generic SAP Notes

- [SAP Note 2588225 - SAP on IBM Cloud: Protect against speculative execution vulnerabilities](#)

FAQ of Moving SAP Workloads

How do I move an existing SAP workload to IBM Cloud?

An existing IBM Cloud® for SAP workload can either be:

- Moved as-is, from on-premises data centers to Cloud IaaS. This method is often called "lift-and-shift"
- Migrating from one vendor or version to another:
 - Changing vendor or version of the database server (for example, IBM Db2 to SAP HANA)
 - Changing the version of the Application server (for example, SAP NetWeaver AS ABAP 7.0 to SAP NetWeaver AS ABAP 7.52)
 - Changing the version of the Business Application (for example, SAP ECC to SAP S/4HANA)

Moving workloads is an infrastructure-level change that affects the SAP systems because networking and storage changes are involved.

Migrating workloads is an application-level change that affects the SAP system installation because new software is being used.

- For VMware-based SAP workloads that are running in on-premises data centers, depending on the existing setup, the movement of these virtual machines into IBM Cloud for VMware may potentially be simplified with the usage of VMware HCX

How do I move an existing SAP HANA database or relational database to an SAP HANA-certified server in the IBM Cloud?

No move or migration services are included with Cloud Infrastructure-as-a-Service (IaaS).

Any move or migration activities are your responsibility.

While IBM Cloud does not provide SAP application-level services, the various IBM Cloud Business Partners (including IBM Services) do provide their service capabilities by using IBM Cloud® for SAP portfolio.

This table shows a brief list of services and the Business Partner types who can provide the services for IBM Cloud® for SAP:

Service	Provided by	Description
Partner type		
Consulting and advisory and implementation	SAP "Global Systems Integrator" (GSI) providers	These providers advise and run SAP implementation and deployment projects.
Application management	SAP "Application Management Services" (AMS) providers	These providers manage and maintain an existing deployment of SAP Applications (optional: incremental functional or development changes).
End-to-end managed services	SAP "Managed Services Providers" (MSP)	These providers run the SAP implementation and deployment and manage the Infrastructure, OS, SAP Technical Applications, and SAP Business Applications. These services often do not include incremental functional or development changes.
Services Partner types		

For example, some of the services that are available in partnership between IBM Cloud and IBM Services include:

- [GSI and IBM Services: SAP Consulting & Implementation Services](#)
- AMS and IBM Services: SAP Application Management and Development Solutions
- [MSP and IBM Services: Managed Applications for SAP](#)

At a high level, what are my options for moving and migrating an existing SAP system to Cloud?

This table is a high-level list of the options for moving and migrating existing SAP systems to cloud. For more information, see all of the necessary SAP documentation on moving and migrating SAP workloads, and liaise with your Systems Implementer for SAP.

Move and Description	Common Usage	Downtime	Pre/Post	Data Transfer	
Migrate SAP workloads approach			Migration Work		
Heterogeneous System Copy that uses SWPM	Move or Re-Platform to different CPU Architecture, OS, or database. Uses System Copy Export/Import of SWPM	Commonly used to change database server in preparation for more significant move; for example, move to SAP HANA DB with a Classical Migration approach	Yes	Significant preparation and post processing required.	System Copy Export dump
Homogeneous System Copy that uses SWPM (<i>Only option for System Copies that are running SAP HANA DB</i>)	Move or Re-Platform to more to newer OS or database version. Cannot be used to move between CPU Architecture or Endianness. Uses SAP Database Backup with SWPM.	Move to new SAP HANA target, or to move to new OS target with existing AnyDB. Also used to create fresh sandboxes of an existing system (with or without Logical System Name change).	Yes. Some reduction in downtime possible depending on preparation, change freeze, and delta change sync (of log files) in failover to target	Less preparation than heterogeneous System Copy; moderate to significant post processing required depending on scenario (in most cases, the Logical System Name is changed, for example, BDLS)	SAP Database Backup
SAP HANA System Replication (HSR) with replicated database mirror on cloud	Secondary failover site is hosted on cloud	HA and DR scenarios	Yes minimal, depends on design and failover factors (for example, cost-optimized or performance)	Using SAP Landscape Management (LaMa), set up and execution can be automated	Log or memory shipping; SYNCMEM, FULLSYNC, SYNC, or ASYNC modes
System Relocation that uses SAP LaMa to orchestrate move	Physically or virtually relocate running or shutdown instances. Uses SAP LaMa. Cannot relocate SAP HANA DB MDC Tenants.	Moving individual SAP instances to new infrastructure landscape that is already set up.	Yes minimal, running systems have downtimes as they are stopped, unprepared, then prepared and started	Using SAP LaMa, relocation can be automated	Package network transfer that uses LaMa or LaMa adapter for VMware
DMO for SUM with System Move execution (<i>Combines Migration, Unicode conversion, Upgrades, and more tasks</i>)	Supported for App Server (NetWeaver) upgrade or database conversion to SAP HANA. Moves the NW PAS + database server and upgrade - all at the same time.	Migrations to Business Suite on SAP HANA or part of SAP S/4HANA conversion migration (Brownfield)	Yes. Both PAS Target and database host in the target landscape (for example, IBM Cloud) needs to be ready before DMO for SUM with System Move execution.	Significant preparation is required.	System Export is performed in source landscape. Import is performed in target landscape. The export/import can also be done in parallel.

Selective Data Transition, with Shell Conversion	Create shell of SAP System with Customizing and Development only; then upgrade / conversion to either SAP ECC or SAP S/4HANA. Migrate selective data from ECC to the upgraded shell system	Used in Business split scenarios (e.g. Divestitures), and Transformation/Conversion projects with SAP S/4HANA	Yes minimal, the target can be built and tested in advance (repeatedly testing the conversion steps and remediation). Data can be replicated to target in advance, so downtime is only for the delta data synchronization and replacing the old system with target.	Significant preparation is required.	SAP Landscape Transformation Replication Server, handled through a direct SAP engagement
Selective Data Transition, with Mix & Match	Merge of two or more system configurations to create a new SAP System with required configuration; then upgrade / conversion to SAP S/4HANA	Used in Business merge scenarios (e.g. Acquisitions) or multiple SAP system consolidation (e.g. ERPs for each Geographic Region or Business Units), and Transformation/Conversion projects with SAP S/4HANA	Yes minimal, the target can be built and tested in advance (repeatedly testing the conversion steps and remediation). Data can be replicated to target in advance, so downtime is only for the delta data synchronization and replacing the old system with target.	Significant preparation is required.	SAP Landscape Transformation Replication Server, handled through a direct SAP engagement

List of Move and Migrate SAP workloads approaches

© Copyright IBM Corporation 2025

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
2025-06-03

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at <https://www.ibm.com/legal/copytrade>.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

