

SAP HANA on AWS Operations Overview Guide

December 2017



Notices

This document is provided for informational purposes only. It represents AWS's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Contents

Introduction	1
Administration	1
Starting and Stopping EC2 Instances Running SAP HANA Hosts	2
Tagging SAP Resources on AWS	2
Monitoring	4
Automation	4
Patching	5
Backup/Recovery	7
Creating an Image of an SAP HANA System	8
AWS Services and Components for Backup Solutions	9
Backup Destination	11
AWS Command Line Interface	12
Backup Example	13
Scheduling and Executing Backups Remotely	14
Restoring SAP HANA Backups and Snapshots	19
Networking	21
EBS-Optimized Instances	22
Elastic Network Interfaces (ENIs)	22
Security Groups	23
Network Configuration for SAP HANA System Replication (HSR)	24
Configuration Steps for Logical Network Separation	25
SAP Support Access	26
Support Channel Setup with SAProuter on AWS	26
Support Channel Setup with SAProuter On-Premises	28
Security	29
OS Hardening	29

Disabling HANA Services	29
API Call Logging	29
Notifications on Access	30
High Availability and Disaster Recovery	30
Conclusion	30
Contributors	30
Appendix A – Configuring Linux to Recognize Ethernet Devices for Multiple ENIs	31
Notes	33

Abstract

Amazon Web Services (AWS) offers you the ability to run your SAP HANA systems of various sizes and operating systems. Running SAP systems on AWS is very similar to running SAP systems in your data center. To a SAP Basis or NetWeaver administrator, there are minimal differences between the two environments. There are a number of AWS Cloud considerations relating to security, storage, compute configurations, management, and monitoring that will help you get the most out of your SAP HANA implementation on AWS. This whitepaper provides the best practices for deployment, operations, and management of SAP HANA systems on AWS. The target audience for this whitepaper is SAP Basis and NetWeaver administrators who have experience running SAP HANA systems in an on-premises environment and want to run their SAP HANA systems on AWS.

Introduction

This guide provides best practices for operating SAP HANA systems that have been deployed on Amazon Web Services (AWS) either using the [SAP HANA Quick Start reference deployment process](#)¹ or manually following the instructions in [Setting up AWS Resources and the SLES Operating System for SAP HANA Installation](#).² This guide is not intended to replace any of the standard SAP documentation. See the following SAP guides and notes:

- [SAP Library \(help.sap.com\) - SAP HANA Administration Guide](#)³
- [SAP installation guides](#)⁴ (These require SAP Support Portal access.)
- [SAP notes](#)⁵ (These require SAP Support Portal access.)

This guide assumes that you have a basic knowledge of AWS. If you are new to AWS, read the following guides before continuing with this guide:

- [Getting Started with AWS](#)⁶
- [What is Amazon EC2?](#)⁷

In addition, the following SAP on AWS guides can be found [here](#):⁸

- [SAP on AWS Implementation and Operations Guide](#) provides best practices for achieving optimal performance, availability, and reliability, and lower total cost of ownership (TCO) while running SAP solutions on AWS.⁹
- [SAP on AWS High Availability Guide](#) explains how to configure SAP systems on Amazon Elastic Compute Cloud (Amazon EC2) to protect your application from various single points of failure.¹⁰
- [SAP on AWS Backup and Recovery Guide](#) explains how to back up SAP systems running on AWS, in contrast to backing up SAP systems on traditional infrastructure.¹¹

Administration

This section provides guidance on common administrative tasks required to operate an SAP HANA system, including information about starting, stopping, and cloning systems.

Starting and Stopping EC2 Instances Running SAP HANA Hosts

At any time, you can stop one or multiple SAP HANA hosts. Before stopping the EC2 instance of an SAP HANA host, first stop SAP HANA on that instance. When you resume the instance, it will automatically start with the same IP address, network, and storage configuration as before. You also have the option of using the [EC2 Scheduler](#) to schedule starts and stops of your EC2 instances.¹² The EC2 Scheduler relies on the native shutdown and start-up mechanisms of the operating system. These native mechanisms will invoke the orderly shutdown and startup of your SAP HANA instance. Here is an architectural diagram of how the EC2 Scheduler works:

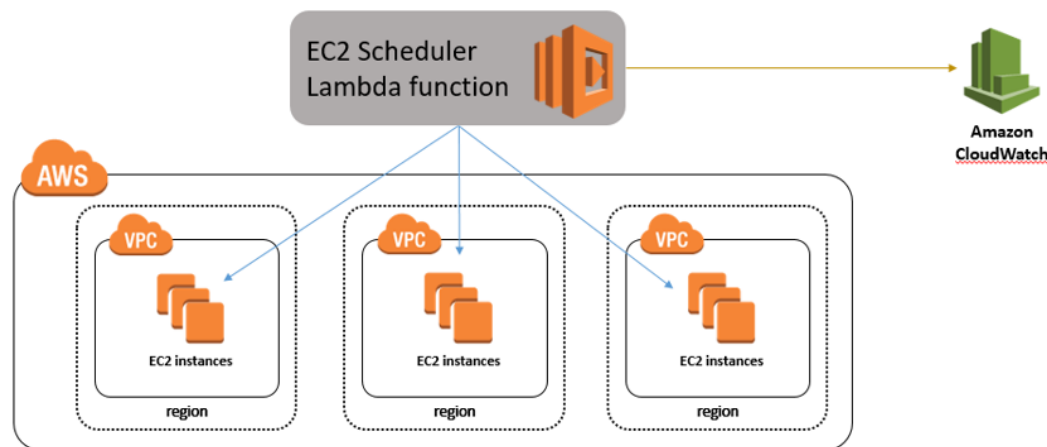


Figure 1: EC2 Scheduler

Tagging SAP Resources on AWS

Tagging your SAP resources on AWS can significantly simplify identification, security, manageability, and billing of those resources. You can tag your resources using the AWS Management Console or by using the `create-tags` functionality of the AWS Command Line Interface (AWS CLI). This table lists some example tag names and tag values:

Tag Name	Tag Value
Name	SAP server's virtual (host) name

Tag Name	Tag Value
Environment	SAP server's landscape role, such as: SBX, DEV, QAT, STG, PRD, etc.
Application	SAP solution or product, such as: ECC, CRM, BW, PI, SCM, SRM, EP, etc.
Owner	SAP point of contact
Service Level	Known uptime and downtime schedule

After you have tagged your resources, you can then apply specific security restrictions to them, for example, access control, based on the tag values. Here is an example of such a policy from our [AWS blog](#):¹³

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LaunchEC2Instances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:Describe*",
        "ec2:RunInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowActionsIfYouAreTheOwner",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StopInstances",
        "ec2:StartInstances",
        "ec2:RebootInstances",
        "ec2:TerminateInstances"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/PrincipalId" :
            "${aws:userid}"
        }
      }
    }
  ]
}
```



```
        "Resource" : [
            "*"
        ]
    }
]
```

The AWS Identity and Access Management (IAM) policy only allows specific permissions based on the tag value. In this scenario, the current user ID must match the tag value in order to be granted permissions. For more information on tagging, refer to our [AWS documentation](#) and our [AWS blog](#).^{14, 15}

Monitoring

There are various AWS, SAP, and third-party solutions that you can leverage for monitoring your SAP workloads. Here are some of the core AWS monitoring services:

- Amazon [CloudWatch](#) – CloudWatch is a monitoring service for AWS resources.¹⁶ It's critical for SAP workloads where it's used to collect resource utilization logs and create alarms to automatically react to changes in AWS resources.
- AWS [CloudTrail](#) – CloudTrail keeps track of all API calls made within your AWS account. It captures key metrics about the API calls and can be useful for automating trail creation for your SAP resources.

Configuring CloudWatch detailed monitoring for SAP resources is mandatory for getting AWS and SAP support. You can use native AWS monitoring services in a complementary fashion with the SAP Solution Manager. Third-party monitoring tools can be found on [AWS Marketplace](#).¹⁷

Automation

AWS offers multiple options for programmatically scripting your resources to operate or scale them in a predictable and repeatable manner. You can leverage AWS CloudFormation to automate and operate SAP systems on AWS. Here are some examples for automating your SAP environment on AWS:

Area	Activities	AWS Services
Infrastructure Deployment	Provision new SAP environment	AWS CloudFormation ¹⁸
	SAP system cloning	AWS CLI ¹⁹
Capacity Management	Automate scale-up/scale-out of SAP application servers	AWS Lambda ²⁰ AWS CloudFormation
	SAP backup automation (see the Backup Example)	Amazon CloudWatch Amazon EC2 Systems Manager
Operations	Performing monitoring and visualization	

Patching

There are two ways for you to patch your SAP HANA database with alternatives for minimizing cost and/or downtime. With AWS, you can provision additional servers as needed to minimize downtime for patching in a cost-effective manner. You can also minimize risks by creating on-demand copies of your existing production SAP HANA databases for life-like production readiness testing.

This table summarizes the tradeoffs of the two patching methods:

Patching Method	Benefits	Technologies Available
Patch an existing server	<ul style="list-style-type: none"> [x] Patch existing OS and DB [x] Longest downtime to existing server and DB [✓] No costs for additional on-demand instances [✓] Lowest levels of relative complexity and setup tasks involved 	Native OS patching tools Patch Manager ²¹ Native SAP HANA patching tools ²²
Provision and patch a new server	<ul style="list-style-type: none"> [✓] Leverage latest AMIs (only DB patch needed) [✓] Shortest downtime to existing server and DB [✓] Can patch and test OS and DB separately and together [x] More costs for additional on-demand instances [x] More complexity and setup tasks involved 	Amazon Machine Image (AMI) ²³ AWS CLI ²⁴ AWS CloudFormation ²⁵ SAP HANA System Replication ²⁶ SAP HANA System Cloning ²⁷ SAP HANA backups ²⁸ SAP Notes: 1984882 ²⁹ - Using HANA System Replication for Hardware Exchange with minimum/zero downtime

Patching Method	Benefits	Technologies Available
		1913302 ³⁰ - HANA: Suspend DB connections for short maintenance tasks

The first method (patch an existing server) involves patching the operating system (OS) and database (DB) components of your SAP HANA server. The goal of the method is to minimize any additional server costs and avoid any tasks needed to set up additional systems or tests. This method may be most appropriate if you have a well-defined patching process and are satisfied with your current downtime and costs. With this method you must use the correct OS update process and tools for your Linux distribution. See this [SUSE](#) blog³¹ and [Red Hat](#) FAQ page³² or check each vendor's documentation for their specific processes and procedures.

In addition to patching tools provided by our Linux partners, AWS offers a [free of charge patching service](#)³³ called [Patch Manager](#).³⁴ At the time of this writing, Patch Manager supports [Red Hat](#).³⁵ Patch Manager is an automated tool that helps you simplify your OS patching process. You can scan your EC2 instances for missing patches and automatically install them, select the timing for patch rollouts, control instance reboots, and many other tasks. You can also define auto-approval rules for patches with an added ability to black-list or white-list specific patches, control how the patches are deployed on the target instances (e.g., stop services before applying the patch), and schedule the automatic rollout through maintenance windows.

The second method (provision and patch a new server) involves provisioning a new EC2 instance that will receive a copy of your source system and database. The goal of the method is to minimize downtime, minimize risks (by having production data and executing production-like testing), and have repeatable processes. This method may be most appropriate if you are looking for higher degrees of automation to enable these goals and are comfortable with the trade-offs. This method is more complex and has a many more options to fit your requirements. Certain options are not exclusive and can be used together. For example, your AWS CloudFormation template can include the latest Amazon Machine Images (AMIs), which you can then use to automate the provisioning, set up, and configuration of a new SAP HANA server.

Here is an example of a process that can be used to automate OS/HANA patching/upgrade:

1. Download the AWS CloudFormation template offered in the [SAP HANA Quick Start](#).³⁶
2. Update the CloudFormation template with the latest OS AMI ID and execute the updated template to provision a new SAP HANA server. The latest OS AMI ID has the specific security patches that your organization needs. As part of the provisioning process, you need to provide the latest SAP HANA installation binaries to get to the required version. This allows you to provision on a new HANA system with the required OS version and security patches along with SAP HANA software versions.
3. After the new SAP HANA system is available, use one of the following methods to copy the data from the original SAP HANA instance to the newly created system:
 - SAP HANA native backup/restore
 - Use SAP HANA System Replication (HSR) technology to replicate the data and then perform an HSR take-over.
 - Take snapshots of the old system's Amazon Elastic Block Store (Amazon EBS) volumes and create new EBS volumes from it. Mount them in the new environment. (Make sure that the HANA SID stays the same for minimal post-processing.)
 - Use new SAP HANA 2.0 functionality such as [SAP HANA Cloning](#).³⁷ The new system will become a clone of the original system.

At the end of this process, you will have a new SAP HANA system that is ready to test.

SAP Note [1984882](#)³⁸ (*Using HANA System Replication for Hardware Exchange with Minimum/Zero Downtime*) has specific recommendations and guidelines on the process for promoting to production.

Backup and Recovery

This section provides an overview of the AWS services used in the backup and recovery of SAP HANA systems and provides an example backup and recovery scenario. This guide does not include detailed instructions on how to execute

database backups using native HANA backup and recovery features or third-party backup tools. Please refer to the standard OS, SAP, and SAP HANA documentation or the documentation provided by backup software vendors. In addition, backup schedules, frequency, and retention periods might vary with your system type and business requirements. See the following standard SAP documentation for guidance on these topics. (SAP notes require SAP Support Portal access.)

Note: Both general and advanced backup and recovery concepts for SAP systems on AWS can be found in detail in the [SAP on AWS Backup and Recovery Guide](#).³⁹

SAP Note	Description
1642148 ⁴⁰	FAQ: SAP HANA Database Backup & Recovery
1821207 ⁴¹	Determining required recovery files
1869119 ⁴²	Checking backups using <code>hdbbackupcheck</code>
1873247 ⁴³	Checking recoverability with <code>hdbbackupdiag --check</code>
1651055 ⁴⁴	Scheduling SAP HANA Database Backups in Linux
2484177 ⁴⁵	Scheduling backups for multi-tenant SAP HANA Cockpit 2.0

Creating an Image of an SAP HANA System

You can use the AWS Management Console or the command line to create your own [AMI](#) based on an existing instance.⁴⁶ For more information, see the [AWS documentation](#).⁴⁷ You can use an AMI of your SAP HANA instance for the following purposes:

- **To create a full offline system backup** (of the OS /usr/sap, HANA shared, backup, data, and log files) – AMIs are automatically saved in multiple Availability Zones within the same Region.
- **To move a HANA system from one Region to another** – You can create an image of an existing EC2 instance and move it to another Region by following the instructions in the [AWS documentation](#).⁴⁸ Once the AMI has been copied to the target Region, the new instance can be launched there.

- **To clone an SAP HANA system** – You can create an AMI of an existing SAP HANA system to create an exact clone of the system. See the following section for additional information.

Note – See the [restore section](#) later in this whitepaper to view the recommended restore steps for production environments.

Tip: The SAP HANA system should be in a consistent state before you create an AMI. To do this, stop the SAP HANA instance before creating the AMI or by following the instructions in SAP Note [1703435](#) (requires SAP Support Portal access).⁴⁹

AWS Services and Components for Backup Solutions

AWS provides a number of services and options for storage and backup, including Amazon Simple Storage Service (Amazon S3), AWS Identity and Access Management (IAM), and Amazon Glacier.

Amazon S3

[Amazon S3](#) is the center of any SAP backup and recovery solution on AWS.⁵⁰ It provides a highly durable storage infrastructure designed for mission-critical and primary data storage. It is designed to provide 99.999999999% durability and 99.99% availability over a given year. See the [Amazon S3 documentation](#) for detailed instructions on how to create and configure an S3 bucket to store your SAP HANA backup files.⁵¹

AWS IAM

With [IAM](#), you can securely control access to AWS services and resources for your users.⁵² You can create and manage AWS users and groups and use permissions to grant user access to AWS resources. You can create roles in IAM and manage permissions to control which operations can be performed by the entity, or AWS service, that assumes the role. You can also define which entity is allowed to assume the role.

During the deployment process, CloudFormation creates an IAM role that allows access to get objects from and/or put objects into Amazon S3. That role is

subsequently assigned to each EC2 instance that is hosting SAP HANA master and worker nodes at launch time as they are deployed.

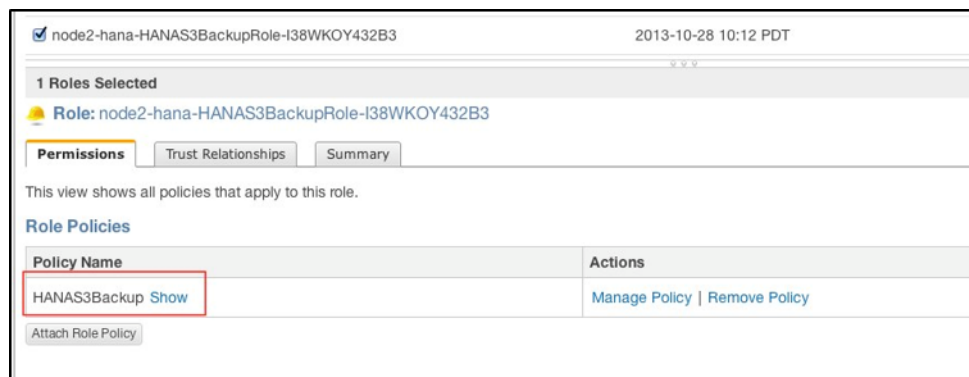


Figure 2: IAM role example

To ensure security that applies the principle of least privilege, permissions for this role are limited only to actions that are required for backup and recovery.

```
{
  "Statement": [
    {
      "Resource": "arn:aws:s3::: <your-s3-bucket-name>/*",
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListBucket",
        "s3:Get*",
        "s3:List*"
      ],
      "Effect": "Allow"
    },
    {
      "Resource": "*",
      "Action": [
        "s3:List*",
        "ec2:Describe*",
        "ec2:AttachNetworkInterface",
        "ec2:AttachVolume",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:RunInstances",
        "ec2:StartInstances"
      ],
      "Effect": "Allow"
    }
  ]
}
```

To add functions later, you can use the AWS Management Console to modify the IAM role.

Amazon Glacier

[Amazon Glacier](#) is an extremely low-cost service that provides secure and durable storage for data archiving and backup.⁵³ Amazon Glacier is optimized for data that is infrequently accessed and provides multiple options like expedited, standard, and bulk methods for data retrieval. With standard and bulk retrievals, data is available in 3-5 hours or 5-12 hours, respectively.

However, with expedited retrieval, Amazon Glacier provides you with an option to retrieve data in 3-5 minutes, which can be ideal for occasional urgent requests. With Amazon Glacier, you can reliably store large or small amounts of data for as little as \$0.01 per gigabyte per month, a significant savings compared to on-premises solutions. You can use [lifecycle policies](#), as explained in the *Amazon S3 Developer Guide*, to push SAP HANA backups to Amazon Glacier for long-term archiving.⁵⁴

Backup Destination

The primary difference between backing up SAP systems on AWS compared with traditional on-premises infrastructure is the backup destination. Tape is the typical backup destination used with on-premises infrastructure. On AWS, backups are stored in Amazon S3. Amazon S3 has many benefits over tape, including the ability to automatically store backups “offsite” from the source system, since data in Amazon S3 is replicated across multiple facilities within the AWS Region.

SAP HANA systems provisioned using the [SAP HANA Quick Start reference deployment](#) are configured with a set of EBS volumes to be used as an initial local backup destination. HANA backups are first stored on these local EBS volumes and then copied to Amazon S3 for long-term storage.

You can use SAP HANA Studio, SQL commands, or the DBA Cockpit to start or schedule SAP HANA data backups. Log backups are written automatically unless disabled. The `/backup` file system is configured as part of the deployment process.

```
Have a lot of fun...
imdbmaster:~ # df
Filesystem                1K-blocks    Used Available Use% Mounted on
/dev/hda1                  20641404   9249976   10342908  48% /
udev                      126201160     148   126201012    1% /dev
tmpfs                     126201160      0   126201160    0% /dev/shm
/dev/xvds                  52403200   138964   52264236    1% /usr/sap
/dev/mapper/vghana-lvhanashared 255759296 12548240  243211056    5% /hana/shared
/dev/mapper/vghana-lvhanadata  767180800  2161216  765019584    1% /hana/data
/dev/mapper/vghana-lvhanalog   255759296  2497664  253261632    1% /hana/Log
/dev/mapper/vghana-lvhanaback 1073248192   33872 1073214320    1% /backup
imdbmaster:~ #
```

Figure 3: SAP HANA file system layout

The SAP HANA `global.ini` configuration file has been customized by the SAP HANA Quick Start reference deployment process as follows: database backups go directly to `/backup/data/<SID>`, while automatic log archival files go to `/backup/log/<SID>`.

```
[persistence]
basepath_shared = no
savepoint_intervals = 300
basepath_datavolumes = /hana/data/<SID>
basepath_logvolumes = /hana/log/<SID>
basepath_databackup = /backup/data/<SID>

basepath_logbackup = /backup/log/<SID>
```

Some third-party backup tools like Commvault, NetBackup, and TSM are integrated with Amazon S3 capabilities and can be used to trigger and save SAP HANA backups directly into Amazon S3 without needing to store the backups on EBS volumes first.

AWS Command Line Interface

The [AWS CLI](#), which is a unified tool to manage AWS services, is installed as part of the base image.⁵⁵ Using various commands, you can control multiple AWS services from the command line directly and automate them through scripts. Access to your S3 bucket is available through the IAM role assigned to the instance (discussed [earlier](#)). Using the AWS CLI commands for Amazon S3, you can list the contents of the previously created bucket, back up files, and restore files, as explained in the [AWS CLI documentation](#).⁵⁶

```
imdbmaster:/backup # aws s3 ls --region=us-east-1 s3://node2-
hana-s3bucket-gcynh5v2nqs3

Bucket: node2-hana-s3bucket-gcynh5v2nqs3
Prefix:
      LastWriteTime          Length Name
      -
      -----
```

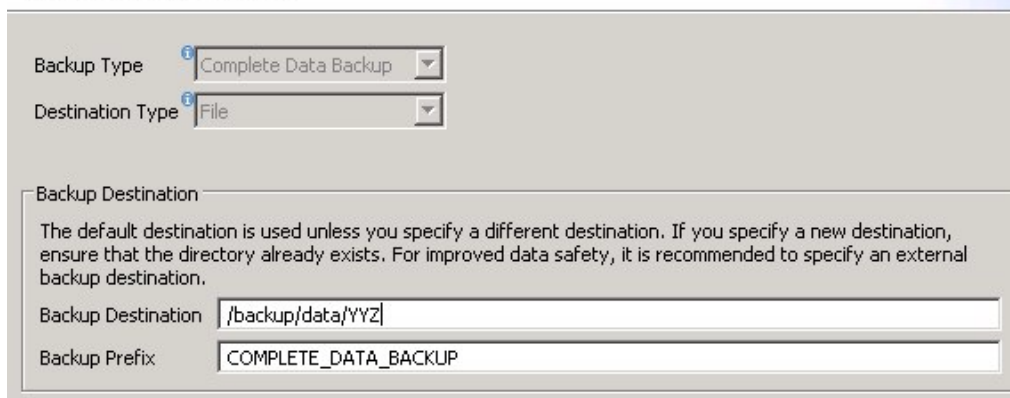
Backup Example

Here are the steps you might take for a typical backup task:

1. In the SAP HANA Backup Editor, choose **Open Backup Wizard**. You can also open the Backup Wizard by right-clicking the system that you want to back up and choosing **Back Up**.
 - a. Select destination type **File**. This will back up the database to files in the specified file system.
 - b. Specify the backup destination (`/backup/data/<SID>`) and the backup prefix.

Specify Backup Settings

Specify the information required for the data backup
Estimated backup size: 1.78 GB.



Backup Type: Complete Data Backup

Destination Type: File

Backup Destination: /backup/data/YYZ

Backup Prefix: COMPLETE_DATA_BACKUP

The default destination is used unless you specify a different destination. If you specify a new destination, ensure that the directory already exists. For improved data safety, it is recommended to specify an external backup destination.

Figure 4: SAP HANA backup example

- c. Choose **Next** and then **Finish**. A confirmation message will appear when the backup is complete.
 - d. Verify that the backup files are available at the OS level. The next step is to push or synchronize the backup files from the `/backup` file system to Amazon S3 by using the [aws s3 sync](#) command.⁵⁷

```
imdbmaster:/ # aws s3 sync backup s3://node2-hana-s3bucket-
gcynh5v2nqs3 --region=us-east-1
```

2. Use the AWS Management Console to verify that the files have been pushed to Amazon S3. You can also use the `aws s3 ls` command shown previously in the [AWS Command Line Interface section](#).⁵⁸

Name	Storage Class	Size	Last Modified
COMPLETE_DATA_BACKUP_data...	Standard	160 KB	Mon Oct 28 12:56:07 GMT-700 2013
COMPLETE_DATA_BACKUP_data...	Standard	67.1 MB	Mon Oct 28 12:56:07 GMT-700 2013
COMPLETE_DATA_BACKUP_data...	Standard	954.5 MB	Mon Oct 28 12:56:08 GMT-700 2013
COMPLETE_DATA_BACKUP_data...	Standard	66 MB	Mon Oct 28 12:56:37 GMT-700 2013
COMPLETE_DATA_BACKUP_data...	Standard	96.8 MB	Mon Oct 28 12:56:39 GMT-700 2013
COMPLETE_DATA_BACKUP_data...	Standard	93.9 MB	Mon Oct 28 12:56:42 GMT-700 2013
COMPLETE_DATA_BACKUP_data...	Standard	66.2 MB	Mon Oct 28 12:56:44 GMT-700 2013
COMPLETE_DATA_BACKUP_data...	Standard	129.9 MB	Mon Oct 28 12:56:47 GMT-700 2013

Figure 5: Amazon S3 bucket contents after backup

Tip: The `aws s3 sync` command will only upload new files that don't exist in Amazon S3. Use a periodically scheduled cron job to sync, and then delete files that have been uploaded. See SAP Note [1651055](#) for scheduling periodic backup jobs in Linux, and extend the supplied scripts with `aws s3 sync` commands.⁵⁹

Scheduling and Executing Backups Remotely

The Amazon EC2 Systems Manager Run Command, along with Amazon CloudWatch Events, can be leveraged to schedule backups for your HANA SAP system remotely with the need to log in to the EC2 instances. You can also leverage cron or any other instance-level scheduling mechanism.

The Systems Manager Run Command lets you remotely and securely manage the configuration of your managed instances. A managed instance is any EC2 instance or on-premises machine in your hybrid environment that has been configured for Systems Manager. The Run Command enables you to automate common administrative tasks and perform ad hoc configuration changes at

scale. You can use the Run Command from the Amazon EC2 console, the AWS CLI, Windows PowerShell, or the AWS SDKs.

Systems Manager Prerequisites

Systems Manager has the following prerequisites.

Supported Operating System (Linux)	<p>Instances must run a supported version of Linux.</p> <p>64-bit and 32-bit systems:</p> <ul style="list-style-type: none">• Amazon Linux 2014.09, 2014.03 or later• Ubuntu Server 16.04 LTS, 14.04 LTS, or 12.04 LTS• Red Hat Enterprise Linux (RHEL) 6.5 or later• CentOS 6.3 or later <p>64-bit systems only:</p> <ul style="list-style-type: none">• Amazon Linux 2015.09, 2015.03 or later• Red Hat Enterprise Linux (RHEL) 7.x or later• CentOS 7.1 or later• SUSE Linux Enterprise Server (SLES) 12 or higher
Roles for Systems Manager	<p>Systems Manager requires an IAM role for instances that will process commands and a separate role for users executing commands. Both roles require permission policies that enable them to communicate with the Systems Manager API. You can choose to use Systems Manager managed policies or you can create your own roles and specify permissions. For more information, see Configuring Security Roles for Systems Manager.⁶⁰</p> <p>If you are configuring on-premises servers or virtual machines (VMs) that you want to configure using Systems Manager, you must also configure an IAM service role. For more information, see Create an IAM Service Role.⁶¹</p>
SSM Agent (EC2 Linux instances)	<p>SSM Agent processes Systems Manager requests and configures your machine as specified in the request. You must download and install SSM Agent to your EC2 Linux instances. For more information, see Installing SSM Agent on Linux.</p>

To schedule remote backups, here are the high-level steps:

1. Install and configure the Systems Manager agent on the EC2 instance. For detailed installation steps, please see <http://docs.aws.amazon.com/systems-manager/latest/userguide/ssm-agent.html#sysman-install-ssm-agent>.

2. Provide SSM access to the EC2 instance role that is assigned to the SAP HANA instance. For detailed information on how to assign SSM access to a role, please see <http://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-access.html>.
3. Create an SAP HANA backup script. A sample script is shown below. You can use this as a starting point and then modify it to meet your requirements.

```
#!/bin/sh
set -x
S3Bucket_Name=<<Name of the S3 bucket where backup files will be copied>>
TIMESTAMP=$(date +%F_%H%M)
exec 1>/backup/data/${SAPSYSTEMNAME}/${TIMESTAMP}_backup_log.out
2>&1
echo "Starting to take backup of Hana Database and Upload the backup files to S3"
echo "Backup Timestamp for $SAPSYSTEMNAME is $TIMESTAMP"
BACKUP_PREFIX=${SAPSYSTEMNAME}_${TIMESTAMP}
echo $BACKUP_PREFIX
# source HANA environment
source $DIR_INSTANCE/hdbenv.sh
# execute command with user key
hdbsql -U BACKUP "backup data using file ('$BACKUP_PREFIX')"
echo "HANA Backup is completed"
echo "Continue with copying the backup files in to S3"
echo $BACKUP_PREFIX
sudo -u root /usr/local/bin/aws s3 cp --recursive
/backup/data/${SAPSYSTEMNAME}/
s3://${S3Bucket_Name}/bkps/${SAPSYSTEMNAME}/data/ --exclude "*"
--in
clude "${BACKUP_PREFIX}*"
echo "Copying HANA Database log files in to S3"
sudo -u root /usr/local/bin/aws s3 sync
/backup/log/${SAPSYSTEMNAME}/
s3://${S3Bucket_Name}/bkps/${SAPSYSTEMNAME}/log/ --exclude "*" -
-include "log_backup*"
sudo -u root /usr/local/bin/aws s3 cp
/backup/data/${SAPSYSTEMNAME}/${TIMESTAMP}_backup_log.out
s3://${S3Bucket_Name}/bkps/${SAPSYSTEMNAME}
```

Note: This script takes into consideration that hdbuserstore has a key named **Backup**.

4. At this point you can test an one-time backup by executing an ssm command directly:

```
aws ssm send-command --instance-ids <<HANA Master Instance ID>>
--document-name AWS-RunShellScript --parameters commands="sudo -
u <HANA_SID>adm TIMESTAMP=$(date +%F\_%H\%M)
SAPSYSTEMNAME=<HANA_SID>
DIR_INSTANCE=/hana/shared/${SAPSYSTEMNAME}/HDB00 -i
/usr/sap/HDB/HDB00/hana_backup.sh"
```

Note: For this command to execute successfully, you will have to enable <sid>adm login using sudo.

5. Using CloudWatch Events, you can schedule backups remotely at any desired frequency. Navigate to the CloudWatch Events page and create a rule.

Step 1: Create rule

Create rules to invoke Targets based on Events happening in your AWS environment.

Event Source

Build or customize an Event Pattern or set a Schedule to invoke Targets.

☐ Event Pattern
 ☒ Schedule

☒ Fixed rate of

☐ Cron expression

[Learn more about CloudWatch Events schedules.](#)

► Show sample event(s)

Targets

Select Target to invoke when an event matches your Event Pattern or when schedule is triggered.

SSM Run Command

Document*

Target key*

Target value(s)*

A Run Command Target provides a way to specify which EC2 Instances to invoke SSM Run Command on. [Learn more](#)

▼ Configure parameter(s)

☐ No Parameter(s)
 ☒ Constant

Commands

```
aws ssm send-command --instance-ids <<HANA Master Instance ID>> --document-name AWS-RunShellScript --parameters commands="sudo -u <HANA_SID>adm TIMESTAMP=$(date +%F_%H%M) SAPSYSTEMNAME <HANA_SID> DIR_INSTANCE=/hana/shared/$(SAPSYSTEMNAME)/H -I /usr/sap/HDB/HDB00/hana_backup.sh"
```

WorkingDirectory

ExecutionTimeout

☐ Input Transformer

CloudWatch Events needs permission to call EC2 Run Command on your EC2 Instance(s). By continuing, you are allowing us to do so.

☒ Create a new role for this specific resource

☐ Use existing role

[Learn more about CloudWatch Events identity-based policies.](#)

* Required

Cancel

Figure 6: Amazon CloudWatch event rule creation

When configuring the rule:

- Choose **Schedule**.
- Select **SSM Run Command** as the Target.
- Select **AWS-RunShellScript (Linux)** as the Document type.
- Choose **InstanceIds** or **Tags** as Target Keys.

- Choose **Constant** under Configure Parameters, and type the run command.

Restoring SAP HANA Backups and Snapshots

Restoring SAP Backups

To restore your SAP HANA database from a backup, perform the following steps:

1. If the backup files are not already available in the /backup file system but are in Amazon S3, restore the files from Amazon S3 by using the [aws s3 cp](#) command.⁶² This command has the following syntax:

```
aws --region <region> cp <s3-bucket/path> --recursive <backup-prefix>*. 
```

For example:

```
imdbmaster:/backup/data/YYZ # aws --region us-east-1 s3 cp  
s3://node2-hana-s3bucket-gcynh5v2nqs3/data/YYZ . --recursive --  
include COMPLETE*
```

2. Recover the SAP HANA database by using the Recovery Wizard as outlined in the [SAP HANA Administration Guide](#).⁶³ Specify **File** as the Destination Type and enter the correct Backup Prefix.

Specify the Backup Files to Recover

Specify the data backup files to be recovered.

Destination Type:

Locate the Data Backup

Specify the destination of the data backup that you want to use to recover searched recursively.

Location:

Backup Prefix:

Figure 7: Restore example

3. When the recovery is complete, you can resume normal operations and clean up backup files from the `/backup/<SID>/*` directories.

Restoring EBS/AMI Snapshots

To restore EBS snapshots, perform the following steps:

1. Create a new volume from the snapshot:

```
aws ec2 create-volume --region us-west-2 --availability-zone us-west-2a --snapshot-id snap-1234abc123a12345a --volume-type gp2
```

2. Attach the newly created volume to your EC2 host:

```
aws ec2 attach-volume --region=us-west-2 --volume-id vol-4567c123e45678dd9 --instance-id i-03add123456789012 --device /dev/sdf
```

3. Mount the logical volume associated with SAP HANA data on the host:

```
mount /dev/sdf /hana/data
```

4. Start your SAP HANA instance.

Note: For large mission-critical systems, we highly recommend that you execute the volume initialization command on the database data and log volumes after the AMI restore but before starting the database. Executing the volume initialization command will help you avoid extensive wait times before the database is available. Here is the sample `fio` command that you can use:

```
sudo fio -filename=/dev/xvdf -rw=read -bs=128K -iodepth=32 -ioengine=libaio -direct=1 -name=volume-initialize
```

For more information about initializing Amazon EBS volumes, see the [AWS documentation](#).⁶⁴

Restoring AMI Snapshots

You can restore your HANA SAP AMI snapshots through the AWS Management Console. On the EC2 Dashboard, select **AMIs** in the left-hand navigation. Choose the AMI that you want to restore, expand **Actions**, and select **Launch**.

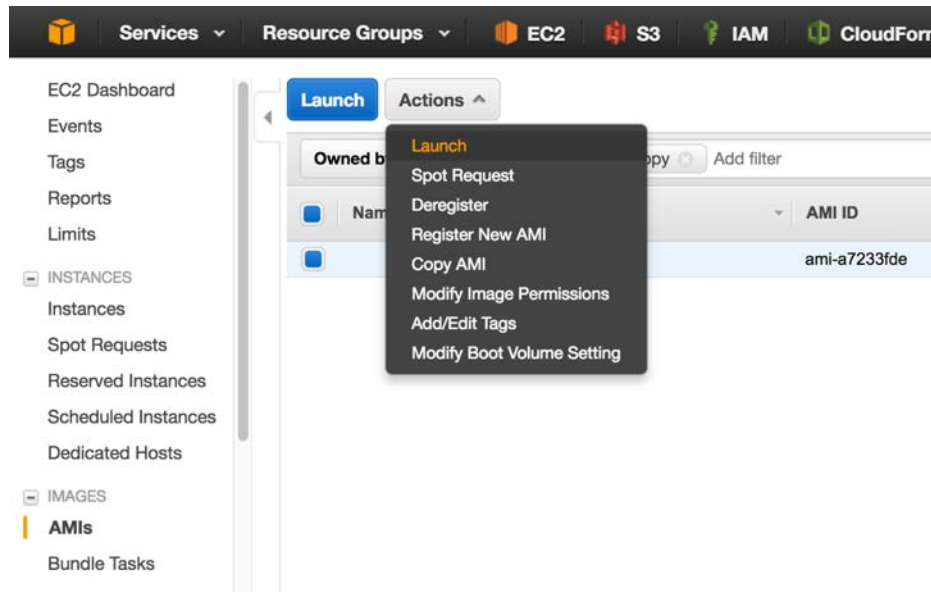


Figure 8: Restore AMI snapshot

Networking

SAP HANA components communicate over the following logical network zones:

- Client zone – to communicate with different clients such as SQL clients, SAP Application Server, SAP HANA Extended Application Services (XS), SAP HANA Studio, etc.
- Internal zone – to communicate with hosts in a distributed SAP HANA system as well as for SAP HSR
- Storage zone – to persist SAP HANA data in the storage infrastructure for resumption after start or recovery after failure

Separating network zones for SAP HANA is considered both an AWS and an SAP best practice because it enables you to isolate the traffic required for each communication channel.

In a traditional, bare-metal setup, these different network zones are set up by having multiple physical network cards or virtual LANs (VLANs). Conversely, on the AWS Cloud, this network isolation can be achieved simply through the use of elastic network interfaces (ENIs) combined with security groups. Amazon EBS-optimized instances can also be used for further isolation for storage I/O.

EBS-Optimized Instances

Many newer Amazon EC2 instance types such as the X1 use an optimized configuration stack and provide additional, dedicated capacity for Amazon EBS I/O. These are called [EBS-optimized instances](#).⁶⁵ This optimization provides the best performance for your EBS volumes by minimizing contention between Amazon EBS I/O and other traffic from your instance.

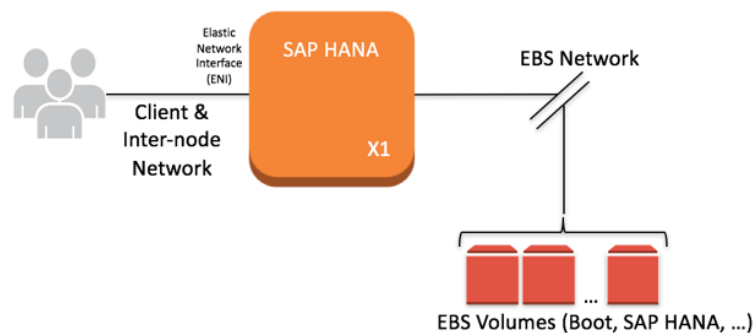


Figure 9: EBS-optimized instances

Elastic Network Interfaces (ENIs)

An ENI is a virtual network interface that you can attach to an EC2 instance in an Amazon Virtual Private Cloud (Amazon VPC). With ENIs, you can create different logical networks by specifying multiple private IP addresses for your instances.

For more information about ENIs, see the [AWS documentation](#).⁶⁶ In the following example, two ENIs are attached to each SAP HANA node as well as in separate communication channel for storage.

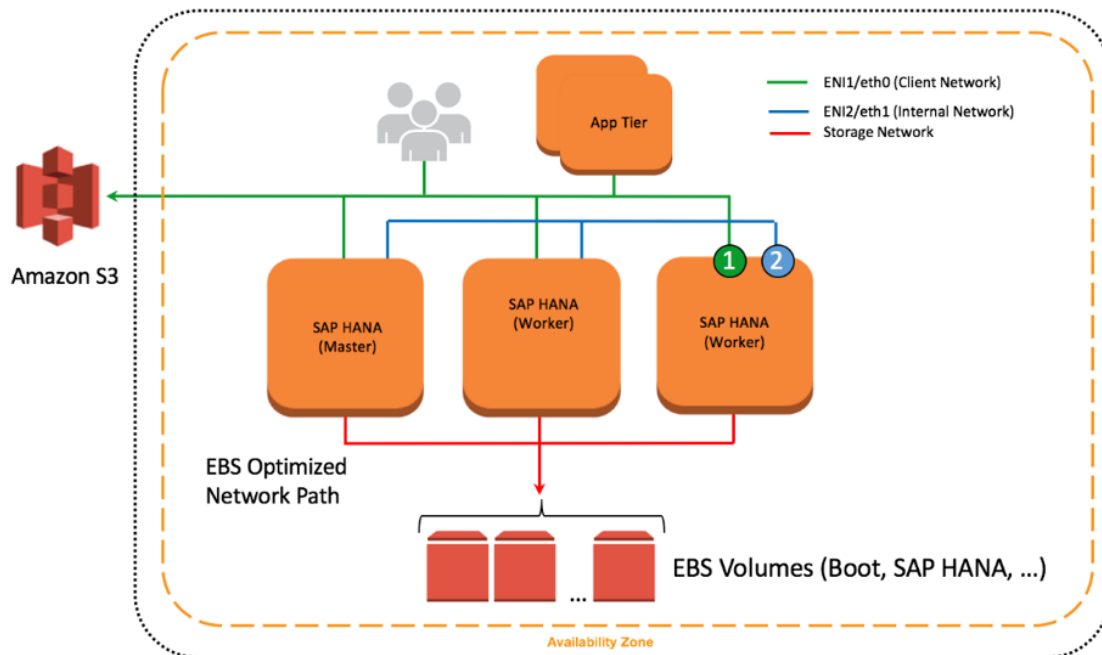


Figure 10: ENIs attached to SAP HANA nodes

Security Groups

A security group acts as a virtual firewall that controls the traffic for one or more instances. When you launch an instance, you associate one or more security groups with the instance. You add rules to each security group that allow traffic to or from its associated instances. You can modify the rules for a security group at any time. The new rules are automatically applied to all instances that are associated with the security group. To learn more about security groups, see the [AWS documentation](#).⁶⁷ In the following example, ENI-1 of each instance shown is a member of the same security group that controls inbound and outbound network traffic for the client network.

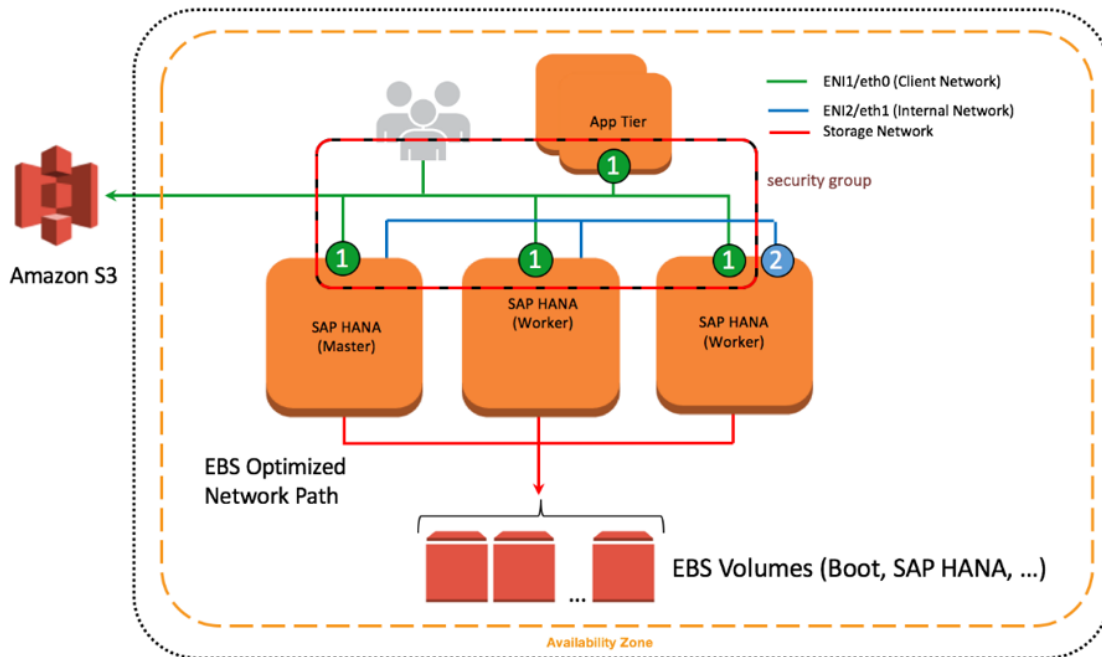


Figure 11: ENIs and security groups

Network Configuration for SAP HANA System Replication (HSR)

You can configure additional ENIs and security groups to further isolate inter-node communication as well as SAP HSR network traffic. In Figure 10, ENI-2 is dedicated for inter-node communication with its own security group (not shown) to secure client traffic from inter-node communication. ENI-3 is configured to secure SAP HSR traffic to another Availability Zone within the same Region. In this example, the target SAP HANA cluster would be configured with additional ENIs similar to the source environment, and ENI-3 would share a common security group.

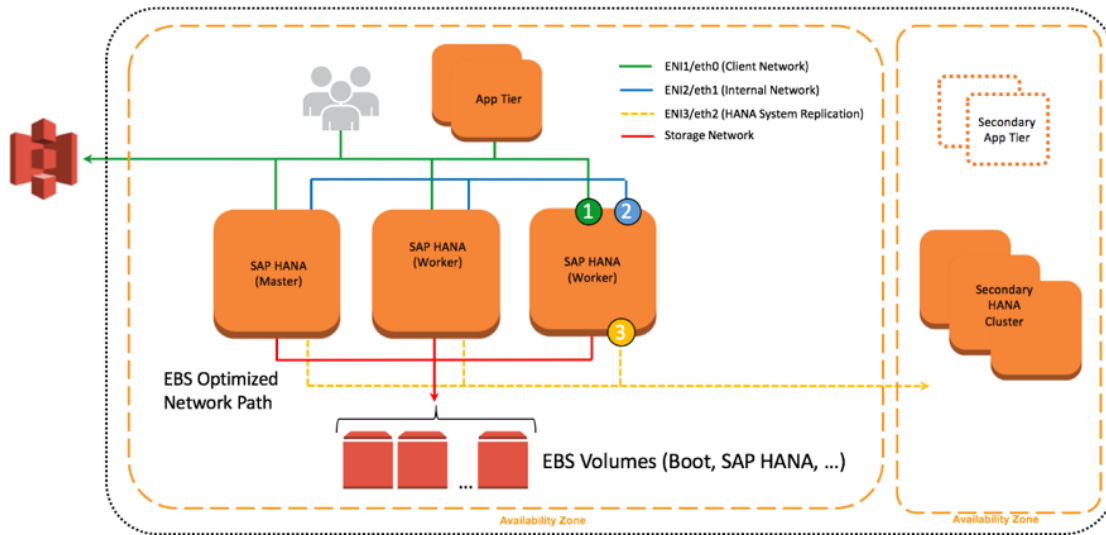


Figure 12: Further isolation with additional ENIs and security groups

Configuration Steps for Logical Network Separation

To configure your logical network for SAP HANA, follow these steps:

1. Create new security groups to allow for isolation of client, internal communication, and, if applicable, SAP HSR network traffic. See [Ports and Connections](#) in the SAP HANA documentation to learn about the list of ports used for different network zones.⁶⁸ For more information about how to create and configure security groups, see the [AWS documentation](#).⁶⁹
2. Use Secure Shell (SSH) to connect to your EC2 instance at the OS level. Follow the steps described in [Appendix A](#) to configure the OS to properly recognize and name the Ethernet devices associated with the new elastic network interfaces (ENIs) you will be creating.
3. Create new ENIs from the AWS Management Console or through the AWS CLI. Make sure that the new ENIs are created in the subnet where your SAP HANA instance is deployed. As you create each new ENI, associate it with the appropriate security group you created in step 1. For more information about how to create a new ENI, see the [AWS documentation](#).⁷⁰
4. Attach the ENIs you created to your EC2 instance where SAP HANA is installed. For more information about how to attach an ENI to an EC2 instance, see the [AWS documentation](#).⁷¹

5. Create virtual host names and map them to the IP addresses associated with client, internal, and replication network interfaces. Ensure that host name-to-IP-address resolution is working by creating entries in all applicable host files or in the Domain Name System (DNS). When complete, test that the virtual host names can be resolved from all SAP HANA nodes, clients, etc.
6. For scale-out deployments, configure SAP HANA inter-service communication to let SAP HANA communicate over the internal network. To learn more about this step, see [Configuring SAP HANA Inter-Service Communication](#) in the SAP HANA documentation.⁷²
7. Configure SAP HANA hostname resolution to let SAP HANA communicate over the replication network for SAP HSR. To learn more about this step, see [Configuring Hostname Resolution for SAP HANA System Replication](#) in the SAP HANA documentation.⁷³

SAP Support Access

In some situations it may be necessary to allow an SAP support engineer to access your SAP HANA systems on AWS. The following information serves only as a supplement to the information contained in the “Getting Support” section of the [SAP HANA Administration Guide](#).⁷⁴

A few steps are required to configure proper connectivity to SAP. These steps differ depending on whether you want to use an existing remote network connection to SAP or you are setting up a new connection directly with SAP from systems on AWS.

Support Channel Setup with SAProuter on AWS

When setting up a direct support connection to SAP from AWS, consider the following steps:

1. For the SAProuter instance, create and configure a specific SAProuter security group, which only allows the required inbound and outbound access to the SAP support network. This should be limited to a specific IP address that SAP gives you to connect to, along with TCP port 3299. See the [Amazon EC2 security group documentation](#) for additional details about creating and configuring security groups.⁷⁵

2. Launch the instance that the SAProuter software will be installed on into a public subnet of the Amazon VPC and assign it an Elastic IP address (EIP).
3. Install the SAProuter software and create a `saprouttab` file that allows access from SAP to your SAP HANA system on AWS.
4. Set up the connection with SAP. For your internet connection, use **Secure Network Communication (SNC)**. For more information, see the [SAP Remote Support – Help](#) page.⁷⁶
5. Modify the existing SAP HANA security groups to trust the new SAProuter security group you have created.

Tip: For added security, shut down the EC2 instance that hosts the SAProuter service when it is not needed for support purposes.

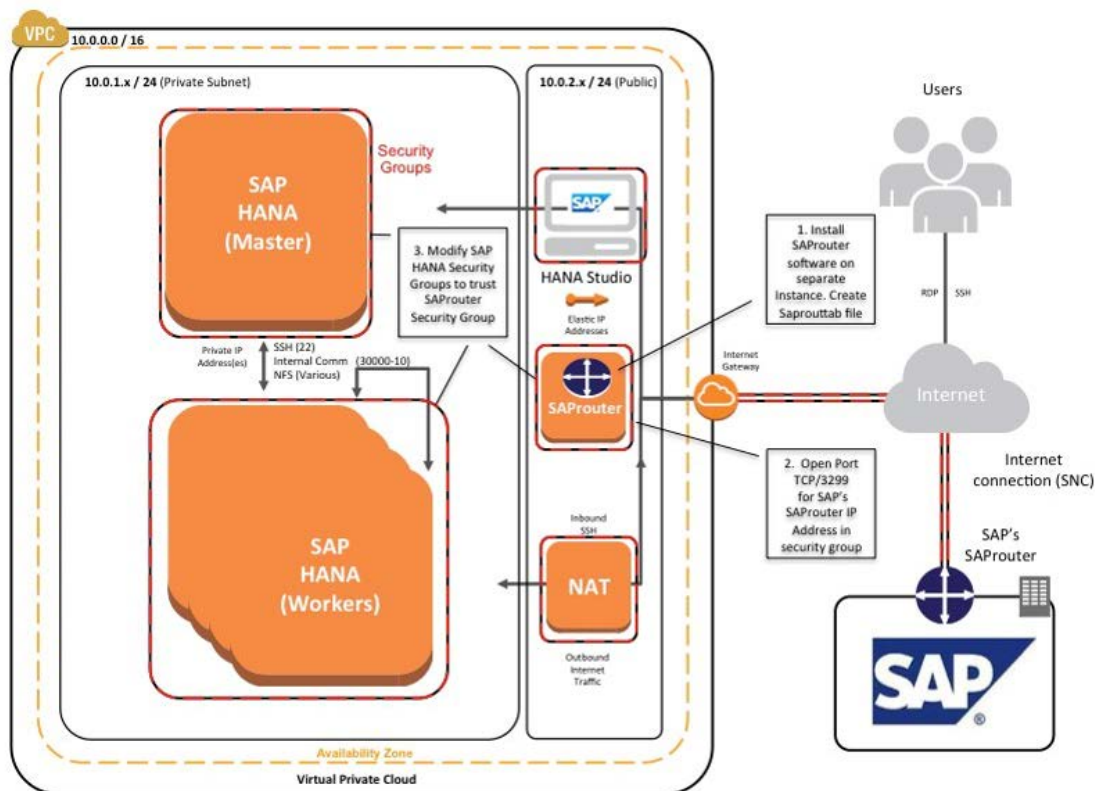


Figure 13: Support connectivity with SAProuter on AWS

Support Channel Setup with SAProuter On-Premises

In many cases, you may already have a support connection configured between your data center and SAP. This can easily be extended to support SAP systems on AWS. This scenario assumes that connectivity between your data center and AWS has already been established, either by way of a secure VPN tunnel over the internet or by using [AWS Direct Connect](#).⁷⁷

You can extend this connectivity as follows:

1. Ensure that the proper `saproutab` entries exist to allow access from SAP to resources in the Amazon VPC.
2. Modify the SAP HANA security groups to allow access from the on-premises SAProuter IP address.
3. Ensure that the proper firewall ports are open on your gateway to allow traffic to pass over TCP port 3299.

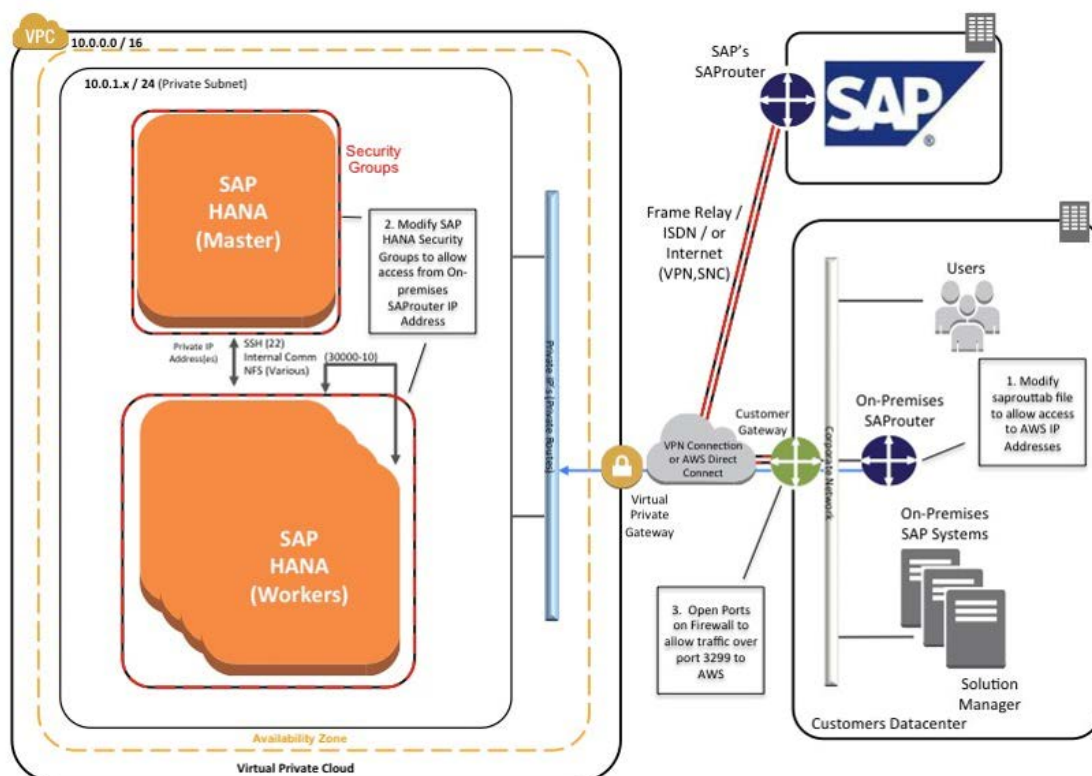


Figure 14: Support connectivity with SAProuter on-premises

Security

This section discusses additional security topics you may want to consider that are not covered in the [SAP HANA Quick Start reference deployment guide](#).

Here are additional AWS security resources to help you achieve the level of security you require for your SAP HANA environment on AWS:

- [AWS Cloud Security Center](#)⁷⁸
- [CIS AWS Foundation whitepaper](#)⁷⁹
- [AWS Cloud Security whitepaper](#)⁸⁰
- [AWS Cloud Security Best Practices whitepaper](#)⁸¹

OS Hardening

You may want to lock down the OS configuration further, for example, to avoid providing a DB administrator with root credentials when logging into an instance.

You can also refer to the following SAP notes:

- [1730999](#): *Configuration changes in HANA appliance*⁸²
- [1731000](#): *Unrecommended configuration changes*⁸³

Disabling HANA Services

HANA services such as HANA XS are optional and should be deactivated if they are not needed. For instructions, see SAP Note [1697613](#): *Remove XS Engine out of SAP HANA database*.⁸⁴ In case of service deactivation, you should also remove the TCP ports from the SAP HANA AWS security groups for complete security.

API Call Logging

[AWS CloudTrail](#) is a web service that records AWS API calls for your account and delivers log files to you.⁸⁵ The recorded information includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by the AWS service.

With CloudTrail, you can get a history of AWS API calls for your account, including API calls made via the AWS Management Console, AWS SDKs, command line tools, and higher-level AWS services (such as CloudFormation). The AWS API call history produced by CloudTrail enables security analysis, resource change tracking, and compliance auditing.

Notifications on Access

You can use [Amazon Simple Notification Service \(Amazon SNS\)](#) or third-party applications to set up notifications on SSH login to your email address or mobile phone.⁸⁶

High Availability and Disaster Recovery

For details and best practices for high availability and disaster recovery of SAP HANA systems running on AWS, see [High Availability and Disaster Recovery Options for SAP HANA on AWS](#).⁸⁷

Conclusion

This whitepaper discusses best practices for the operation of SAP HANA systems on the AWS cloud. The best practices provided in this paper will help you efficiently manage and achieve maximum benefits from running your SAP HANA systems on the AWS Cloud.

For feedback or questions, please contact us at sap-on-aws@amazon.com.

Contributors

The following individuals and organizations contributed to this document:

- Rahul Kabra, Partner Solutions Architect, AWS
- Somckit Khemmanivanh, Partner Solutions Architect, AWS
- Naresh Pasumarthy, Partner Solutions Architect, AWS

Appendix A – Configuring Linux to Recognize Ethernet Devices for Multiple ENIs

Follow these steps to configure the Linux operating system to recognize and name the Ethernet devices associated with the new elastic network interfaces (ENIs) created for logical network separation, which was discussed [earlier in this paper](#).

1. Use SSH to connect to your SAP HANA host as `ec2-user`, and `sudo` to `root`.
2. Remove the existing `udev` rule; for example:

```
hanamaster:# rm -f /etc/udev/rules.d/70-persistent-net.rules
```

Create a new `udev` rule that writes rules based on MAC address rather than other device attributes. This will ensure that on reboot, `eth0` is still `eth0`, `eth1` is `eth1`, and so on. For example:

```
hanamaster:# cat <<EOF > /etc/udev/rules.d/75-persistent-net-generator.rules
# Copyright (C) 2012 Amazon.com, Inc. or its affiliates.
# All Rights Reserved.
#
# Licensed under the Apache License, Version 2.0 (the
"License").
# You may not use this file except in compliance with the
License.
# A copy of the License is located at
#
# http://aws.amazon.com/apache2.0/
#
# or in the "license" file accompanying this file. This file is
# distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR
CONDITIONS
# OF ANY KIND, either express or implied. See the License for the
```

```

# specific language governing permissions and limitations under
the
# License.
# these rules generate rules for persistent network device
naming
SUBSYSTEM!="net", GOTO="persistent_net_generator_end"
KERNEL!="eth*", GOTO="persistent_net_generator_end"
ACTION!="add", GOTO="persistent_net_generator_end"
NAME=="?*", GOTO="persistent_net_generator_end"

# do not create rule for eth0
ENV{INTERFACE}=="eth0", GOTO="persistent_net_generator_end"
# read MAC address
ENV{MATCHADDR}="\${attr{address}}"
# do not use empty address
ENV{MATCHADDR}=="00:00:00:00:00:00",
GOTO="persistent_net_generator_end"
# discard any interface name not generated by our rules
ENV{INTERFACE_NAME}=="?*", ENV{INTERFACE_NAME}=""
# default comment
ENV{COMMENT}="elastic network interface"
# write rule
IMPORT{program}="write_net_rules"
# rename interface if needed
ENV{INTERFACE_NEW}=="?*", NAME="\${env{INTERFACE_NEW}}"
LABEL="persistent_net_generator_end"
EOF

```

3. Ensure proper interface properties. For example:

```

hanamaster:# cd /etc/sysconfig/network/

hanamaster:# cat <<EOF > /etc/sysconfig/network/ifcfg-ethN
BOOTPROTO='dhcp4'
MTU="9000"
REMOTE_IPADDR=' '
STARTMODE='onboot'
LINK_REQUIRED=no
LNIK_READY_WAIT=5
EOF

```

4. Ensure that you can accommodate up to seven more Ethernet devices/ENIs, and restart `wicked`. For example:

```
hanamaster:# for dev in eth{1..7} ; do
ln -s -f ifcfg-ethN /etc/sysconfig/network/ifcfg-${dev}
done

hanamaster:# systemctl restart wicked
```

5. Create and attach a new ENI to the instance.
6. Reboot.
7. After reboot, modify `/etc/iproute2/route`.

Important: Repeat the following for each ENI that you attach to your instance.

For example:

```
hanamaster:# cd /etc/iproute2
hanamaster:/etc/iproute2 # echo "2 eth1_rt" >> route
hanamaster:/etc/iproute2 # ip route add default via 172.16.1.122
dev eth1 table eth1_rt

hanamaster:/etc/iproute2 # ip rule
0:      from all lookup local
32766:  from all lookup main
32767:  from all lookup default

hanamaster:/etc/iproute2 # ip rule add from <ENI IP Address>
lookup eth1_rt prio 1000

hanamaster:/etc/iproute2 # ip rule
0:      from all lookup local
1000:   from <ENI IP address> lookup eth1_rt
32766:  from all lookup main
32767:  from all lookup default
```

Notes

- ¹ <http://docs.aws.amazon.com/quickstart/latest/sap-hana/> or <https://s3.amazonaws.com/quickstart-reference/sap/hana/latest/doc/SAP+HANA+Quick+Start.pdf>
- ² <http://d0.awsstatic.com/enterprise-marketing/SAP/SAP-HANA-on-AWS-Manual-Setup-Guide.pdf>
- ³ https://help.sap.com/hana/SAP_HANA_Administration_Guide_en.pdf
- ⁴ <http://service.sap.com/instguides>
- ⁵ <http://service.sap.com/notes>
- ⁶ <http://docs.aws.amazon.com/gettingstarted/latest/awsgsg-intro/intro.html>
- ⁷ <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/concepts.html>
- ⁸ <http://aws.amazon.com/sap/whitepapers/>
- ⁹ [http://d0.awsstatic.com/enterprise-marketing/SAP/SAP on AWS Implementation Guide.pdf](http://d0.awsstatic.com/enterprise-marketing/SAP/SAP_on_AWS_Implementation_Guide.pdf)
- ¹⁰ [http://d0.awsstatic.com/enterprise-marketing/SAP/SAP on AWS High Availability Guide v3.2.pdf](http://d0.awsstatic.com/enterprise-marketing/SAP/SAP_on_AWS_High_Availability_Guide_v3.2.pdf)
- ¹¹ <http://d0.awsstatic.com/enterprise-marketing/SAP/sap-on-aws-backup-and-recovery-guide-v2-2.pdf>
- ¹² <https://aws.amazon.com/answers/infrastructure-management/ec2-scheduler/>
- ¹³ <https://aws.amazon.com/blogs/security/how-to-automatically-tag-amazon-ec2-resources-in-response-to-api-events/>
- ¹⁴ http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_Tags.html
- ¹⁵ <https://aws.amazon.com/blogs/aws/new-aws-resource-tagging-api/>
- ¹⁶ <https://aws.amazon.com/cloudwatch/>
- ¹⁷ <https://aws.amazon.com/marketplace>
- ¹⁸ <http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/GettingStarted.html>
- ¹⁹ <http://docs.aws.amazon.com/cli/latest/userguide/cli-chap-welcome.html>
- ²⁰ <http://docs.aws.amazon.com/lambda/latest/dg/getting-started.html>
- ²¹ <https://aws.amazon.com/ec2/systems-manager/patch-manager/>

22

<https://help.sap.com/viewer/2c1988d620e04368aa4103bf26f17727/2.0.00/en-US/9731208b85fa4c2fa68c529404ffa75a.html>

23 <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AMIs.html>

24 <http://docs.aws.amazon.com/cli/latest/userguide/cli-ec2-launch.html>

25 <https://aws.amazon.com/cloudformation/>

26

<https://help.sap.com/viewer/6b94445c94ae495c83a19646e7c3fd56/2.0.00/en-US/38ad53e538ad41db9d12d22a6c8f2503.html>

27

<https://help.sap.com/viewer/6b94445c94ae495c83a19646e7c3fd56/2.0.00/en-US/c622d640e47e4c0ebca8cbe74ff9550a.html>

28

<https://help.sap.com/viewer/6b94445c94ae495c83a19646e7c3fd56/2.0.00/en-US/ea70213a0e114ec29724e4a10b6bb176.html>

29 <https://launchpad.support.sap.com/#/notes/1984882/E>

30 <https://launchpad.support.sap.com/#/notes/1913302/E>

31 <https://www.suse.com/communities/blog/upgrading-running-demand-instances-public-cloud/>

32 <https://aws.amazon.com/partners/redhat/faqs/>

33 <https://aws.amazon.com/about-aws/whats-new/2016/12/amazon-ec2-systems-manager-now-offers-patch-management/>

34 <https://aws.amazon.com/ec2/systems-manager/patch-manager/>

35 <http://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-patch.html>

36 <https://docs.aws.amazon.com/quickstart/latest/sap-hana/welcome.html>

37 <https://help.sap.com/doc/6b94445c94ae495c83a19646e7c3fd56/2.0.01/en-US/c622d640e47e4c0ebca8cbe74ff9550a.html>

38 <https://launchpad.support.sap.com/#/notes/1984882/E>

39 <http://d0.awsstatic.com/enterprise-marketing/SAP/sap-on-aws-backup-and-recovery-guide-v2-2.pdf>

40 <http://service.sap.com/sap/support/notes/1642148>

- 41 <http://service.sap.com/sap/support/notes/1821207>
- 42 <http://service.sap.com/sap/support/notes/1869119>
- 43 <http://service.sap.com/sap/support/notes/1873247>
- 44 <http://service.sap.com/sap/support/notes/1651055>
- 45 <http://service.sap.com/sap/support/notes/2484177>
- 46 <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AMIs.html>
- 47 <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/creating-an-ami-ebs.html>
- 48 <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/CopyingAMIs.html>
- 49 <https://service.sap.com/notes/1703435>
- 50 <http://aws.amazon.com/s3/>
- 51 <http://aws.amazon.com/documentation/s3/>
- 52 <http://aws.amazon.com/iam/>
- 53 <http://aws.amazon.com/glacier/>
- 54 <http://docs.aws.amazon.com/AmazonS3/latest/dev/object-archival.html>
- 55 <http://aws.amazon.com/cli/>
- 56 <http://docs.aws.amazon.com/cli/latest/reference/s3/>
- 57 <http://docs.aws.amazon.com/cli/latest/reference/s3/sync.html>
- 58 <http://docs.aws.amazon.com/cli/latest/reference/s3/ls.html>
- 59 <http://service.sap.com/sap/support/notes/1651055>
- 60 <http://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-access.html>
- 61 <http://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-managedinstances.html#sysman-service-role>
- 62 <http://docs.aws.amazon.com/cli/latest/reference/s3/cp.html>
- 63 https://help.sap.com/hana/SAP_HANA_Administration_Guide_en.pdf
- 64 <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-initialize.html>

65

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSOptimized.html>

66 <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html>

67

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html

68

https://help.sap.com/saphelp_hanaplatform/helpdata/en/a9/326f20b39342a7bc3d08acb8ffc68a/frameset.htm

69 <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html#creating-security-group>

70 http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html#create_eni

71 http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html#attach_eni_running_stopped

72

https://help.sap.com/saphelp_hanaplatform/helpdata/en/bb/cb76c7fa7f45b4adb99e60ad6c85ba/frameset.htm

73

http://help.sap.com/saphelp_hanaplatform/helpdata/en/9a/cd6482a5154b7e95ce72e83b04f94d/frameset.htm

74 https://help.sap.com/hana/SAP_HANA_Administration_Guide_en.pdf

75 <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html>

76 <https://support.sap.com/remote-support/help.html>

77 <http://aws.amazon.com/directconnect/>

78 <http://aws.amazon.com/security/>

79

https://d0.awsstatic.com/whitepapers/compliance/AWS_CIS_Foundations_Benchmark.pdf

80

<http://d0.awsstatic.com/whitepapers/Security/AWS%20Security%20Whitepaper.pdf>

- 81 <http://d0.awsstatic.com/whitepapers/aws-security-best-practices.pdf>
- 82 <https://service.sap.com/sap/support/notes/1730999>
- 83 <https://service.sap.com/sap/support/notes/1731000>
- 84 <https://service.sap.com/sap/support/notes/1697613>
- 85 <https://aws.amazon.com/cloudtrail/>
- 86 <https://aws.amazon.com/sns/>
- 87 <http://d0.awsstatic.com/enterprise-marketing/SAP/sap-hana-on-aws-high-availability-disaster-recovery-guide.pdf>