HANA Backup using Azure Backup

v1.0

Contents

[1 Introduction 3](#_Toc97725978)

[1.1 Purpose 3](#_Toc97725979)

[1.2 Audience 3](#_Toc97725980)

[1.3 Assumptions 3](#_Toc97725981)

[2 Prerequisites 3](#_Toc97725982)

[3 Prerequisites for Network 4](#_Toc97725983)

[4 HANA Backup User Creation 6](#_Toc97725984)

[5 HANA Backup Prerequisites Script 8](#_Toc97725985)

[6 Discover the databases 10](#_Toc97725986)

[7 HA Systems HANA Backup 13](#_Toc97725987)

[8 Run an on-demand backup 14](#_Toc97725988)

[9 Run SAP HANA Studio backup on a database with Azure Backup enabled 14](#_Toc97725989)

[10 DB Backup Policy 15](#_Toc97725990)

[Revision History 15](#_Toc97725991)

# Introduction

SAP HANA databases are critical workloads that require a low recovery-point objective (RPO) and long-term retention. You can back up SAP HANA databases running on Azure virtual machines (VMs) by using Azure Backup. This article shows how to back up SAP HANA databases that are running on Azure VMs to an Azure Backup Recovery Services vault.

To this end, it is acknowledged that this is a living document, meant to reflect the design as new standards/changes come online within the environment.

## Purpose

The purpose of this document is to provides a guide for SAP HANA databases running on Azure virtual machines (VMs) by using Azure Backup.

## Audience

This document is for the Infrastructure-specific architectural design as it relates to the SAP infrastructure on Azure Cloud. The target audience is intended to be Azure Technologists, BASIS Administrators and SAP Technical Architects.

## Assumptions

The following assumptions have been made and the implementation of the ANF HANA snapshot backup has been taking these into consideration:

* Any items that are not explicitly mentioned In-Scope are considered Out of Scope.

# Prerequisites

* Identify or create a [Recovery Services vault](https://docs.microsoft.com/en-us/azure/backup/backup-sql-server-database-azure-vms#create-a-recovery-services-vault) in the same region and subscription as the VM running SAP HANA.
* Allow connectivity from the VM to the internet, so that it can reach Azure, as described in the [set up network connectivity](https://docs.microsoft.com/en-us/azure/backup/tutorial-backup-sap-hana-db#set-up-network-connectivity) procedure below.
* Ensure that the combined length of the SAP HANA Server VM name and the Resource Group name doesn't exceed 84 characters for Azure Resource Manager (ARM\_ VMs (and 77 characters for classic VMs). This limitation is because some characters are reserved by the service.
* A key should exist in the **hdbuserstore** that fulfills the following criteria:
  + It should be present in the default **hdbuserstore**. The default is the <sid>adm account under which SAP HANA is installed.
  + For MDC, the key should point to the SQL port of **NAMESERVER**. In the case of SDC, it should point to the SQL port of **INDEXSERVER**
  + It should have credentials to add and delete users
  + Note that this key can be deleted after running the pre-registration script successfully
* Run the SAP HANA backup configuration script (pre-registration script) in the virtual machine where HANA is installed, as the root user. [This script](https://aka.ms/scriptforpermsonhana) gets the HANA system ready for backup. Refer to the [What the pre-registration script does](https://docs.microsoft.com/en-us/azure/backup/tutorial-backup-sap-hana-db#what-the-pre-registration-script-does) section to understand more about the pre-registration script.
* If your HANA setup uses Private Endpoints, run the [pre-registration script](https://aka.ms/scriptforpermsonhana) with the -sn or --skip-network-checks parameter.



Note: - The script is attached here for reference only. During real-time activity, the script has to be downloaded from the MS website everytime,

# Prerequisites for Network

SAP HANA database running on an Azure VM requires connectivity to the Azure Backup service, Azure Storage, and Azure Active Directory. This can be achieved by using private endpoints or by allowing access to the required public IP addresses or FQDNs. Not allowing proper connectivity to the required Azure services may lead to failure in operations like database discovery, configuring backup, performing backups, and restoring data.

The following table lists the various alternatives you can use for establishing connectivity:

| **ESTABLISH NETWORK CONNECTIVITY** | | |
| --- | --- | --- |
| **Option** | **Advantages** | **Disadvantages** |
| Private endpoints | Allow backups over private IPs inside the virtual network  Provide granular control on the network and vault side | Incurs standard private endpoint [costs](https://azure.microsoft.com/pricing/details/private-link/) |
| NSG service tags | Easier to manage as range changes are automatically merged  No additional costs | Can be used with NSGs only  Provides access to the entire service |
| Azure Firewall FQDN tags | Easier to manage since the required FQDNs are automatically managed | Can be used with Azure Firewall only |
| Allow access to service FQDNs/IPs | No additional costs  Works with all network security appliances and firewalls | A broad set of IPs or FQDNs may be required to be accessed |
| Use an HTTP proxy | Single point of internet access to VMs | Additional costs to run a VM with the proxy software |

More details around using these options are shared below:

#### Private endpoints

Private endpoints allow you to connect securely from servers inside a virtual network to your Recovery Services vault. The private endpoint uses an IP from the VNET address space for your vault. The network traffic between your resources inside the virtual network and the vault travels over your virtual network and a private link on the Microsoft backbone network. This eliminates exposure from the public internet. Read more on private endpoints for Azure Backup [here](https://docs.microsoft.com/en-us/azure/backup/private-endpoints).

#### NSG tags

If you use Network Security Groups (NSG), use the AzureBackup service tag to allow outbound access to Azure Backup. In addition to the Azure Backup tag, you also need to allow connectivity for authentication and data transfer by creating similar [NSG rules](https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview#service-tags) for Azure AD (AzureActiveDirectory) and Azure Storage(Storage). The following steps describe the process to create a rule for the Azure Backup tag:

1. In **All Services**, go to **Network security groups** and select the network security group.
2. Select **Outbound security rules** under **Settings**.
3. Select **Add**. Enter all the required details for creating a new rule as described in [security rule settings](https://docs.microsoft.com/en-us/azure/virtual-network/manage-network-security-group#security-rule-settings). Ensure the option **Destination** is set to Service Tag and **Destination service tag** is set to AzureBackup.
4. Select **Add** to save the newly created outbound security rule.

You can similarly create NSG outbound security rules for Azure Storage and Azure AD. For more information on service tags, see [this article](https://docs.microsoft.com/en-us/azure/virtual-network/service-tags-overview).

#### Azure Firewall tags

If you're using Azure Firewall, create an application rule by using the AzureBackup [Azure Firewall FQDN tag](https://docs.microsoft.com/en-us/azure/firewall/fqdn-tags). This allows all outbound access to Azure Backup.

#### Allow access to service IP ranges

If you choose to allow access service IPs, refer to the IP ranges in the JSON file available [here](https://www.microsoft.com/download/confirmation.aspx?id=56519). You'll need to allow access to IPs corresponding to Azure Backup, Azure Storage, and Azure Active Directory.

#### Allow access to service FQDNs

You can also use the following FQDNs to allow access to the required services from your servers:

| **ALLOW ACCESS TO SERVICE FQDNS** | |
| --- | --- |
| **Service** | **Domain names to be accessed** |
| Azure Backup | \*.backup.windowsazure.com |
| Azure Storage | \*.blob.core.windows.net  \*.queue.core.windows.net  \*.blob.storage.azure.net |
| Azure AD | Allow access to FQDNs under sections 56 and 59 according to [this article](https://docs.microsoft.com/en-us/office365/enterprise/urls-and-ip-address-ranges#microsoft-365-common-and-office-online) |

#### Use an HTTP proxy server to route traffic

When you back up an SAP HANA database running on an Azure VM, the backup extension on the VM uses the HTTPS APIs to send management commands to Azure Backup and data to Azure Storage. The backup extension also uses Azure AD for authentication. Route the backup extension traffic for these three services through the HTTP proxy. Use the list of IPs and FQDNs mentioned above for allowing access to the required services. Authenticated proxy servers aren't supported.

# HANA Backup User Creation

* Based on your Linux distribution, the script installs or updates any necessary packages required by the Azure Backup agent.
* It performs outbound network connectivity checks with Azure Backup servers and dependent services like Azure Active Directory and Azure Storage.
* It logs into your HANA system using the user key listed as part of the [prerequisites](https://docs.microsoft.com/en-us/azure/backup/tutorial-backup-sap-hana-db#prerequisites). The user key is used to create a backup user (AZUREWLBACKUPHANAUSER) in the HANA system and **the user key can be deleted after the pre-registration script runs successfully**.
* AZUREWLBACKUPHANAUSER is assigned these required roles and permissions:
  + For MDC: DATABASE ADMIN and BACKUP ADMIN (from HANA 2.0 SPS05 onwards): to create new databases during restore.
  + For SDC: BACKUP ADMIN: to create new databases during restore.
  + CATALOG READ: to read the backup catalog.
  + SAP\_INTERNAL\_HANA\_SUPPORT: to access a few private tables. Only required for SDC and MDC versions below HANA 2.0 SPS04 Rev 46. This is not required for HANA 2.0 SPS04 Rev 46 and above since we are getting the required information from public tables now with the fix from HANA team.
* The script adds a key to **hdbuserstore** for AZUREWLBACKUPHANAUSER for the HANA backup plug-in to handle all operations (database queries, restore operations, configuring and running backup).
* MD2:

SYSTEMKEY: backup\_key

SID: MH5

Instance Number: 06

USER: AZUREWLBACKUPHANAUSER

* DSD:

SYSTEMKEY: backup\_key

SID: DSD

Instance Number: 06

USER: AZUREWLBACKUPHANAUSER

* HD2:

SYSTEMKEY: backup\_key

SID: HDH

Instance Number: 06

USER: AZUREWLBACKUPHANAUSER

* RBD:

SYSTEMKEY: backup\_key

SID: RHD

Instance Number: 06

USER: AZUREWLBACKUPHANAUSER

* BDD:

SYSTEMKEY: backup\_key

SID: BDD

Instance Number: 06

USER: AZUREWLBACKUPHANAUSER

* BDP:

SYSTEM KEY: backup\_key

SID: BDP

Instance Number: 02

USER: AZUREWLBACKUPHANAUSER

* MDP:

SYSTEM KEY: backup\_key

SID: MDP

Instance Number: 02

USER: AZUREWLBACKUPHANAUSER

* DSP:

SYSTEM KEY: backup\_key

SID: DSP

Instance Number: 02

USER: AZUREWLBACKUPHANAUSER

* DSP: (DR)

SYSTEM KEY: backup\_key

SID: DSP

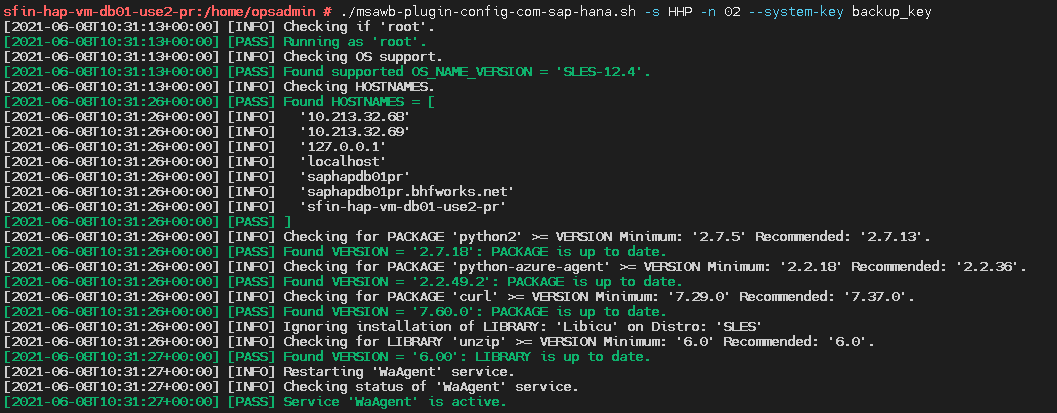
Instance Number: 02

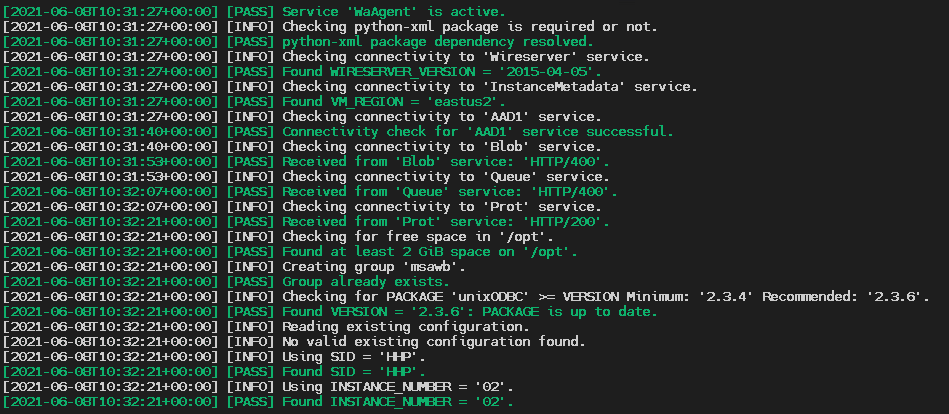
USER: AZUREWLBACKUPHANAUSER

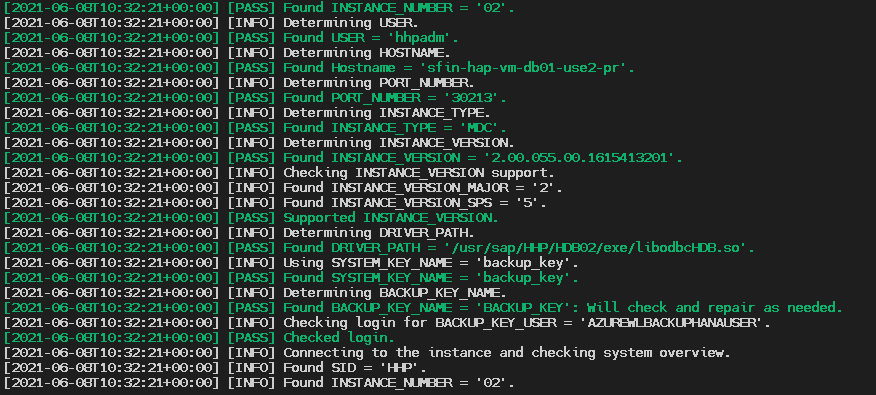
# HANA Backup Prerequisites Script

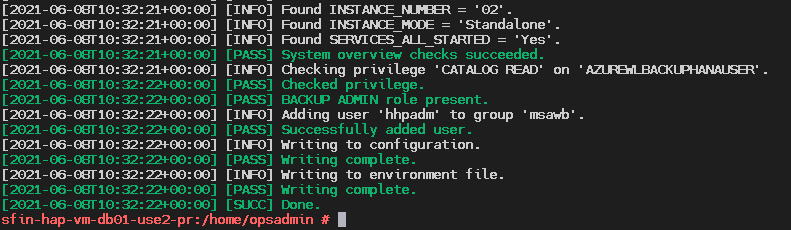
Command line to execute the script:

./msawb-plugin-config-com-sap-hana.sh -s <SID> -n <Instance number> --system-key <system-key-name>







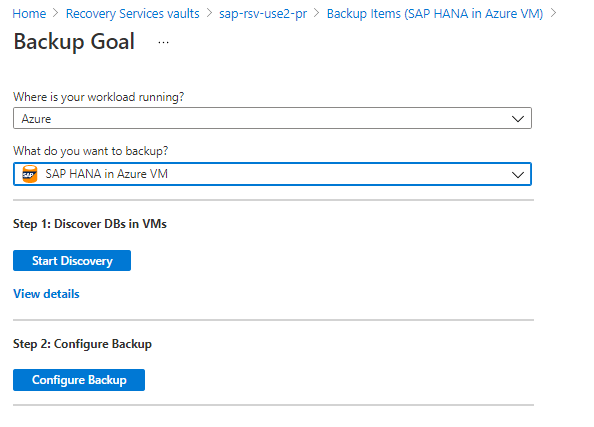


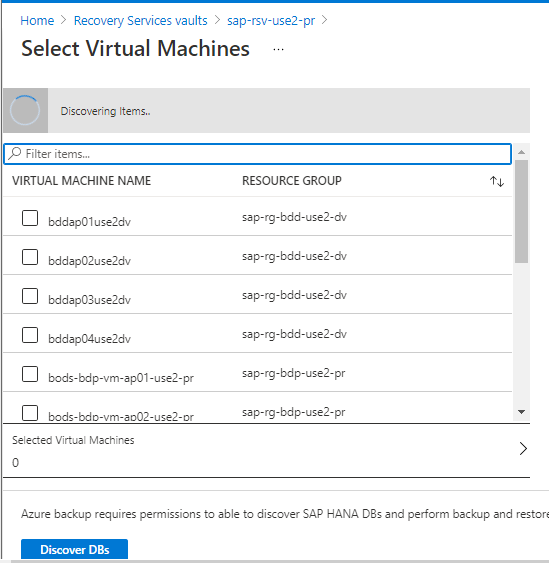
# Discover the databases

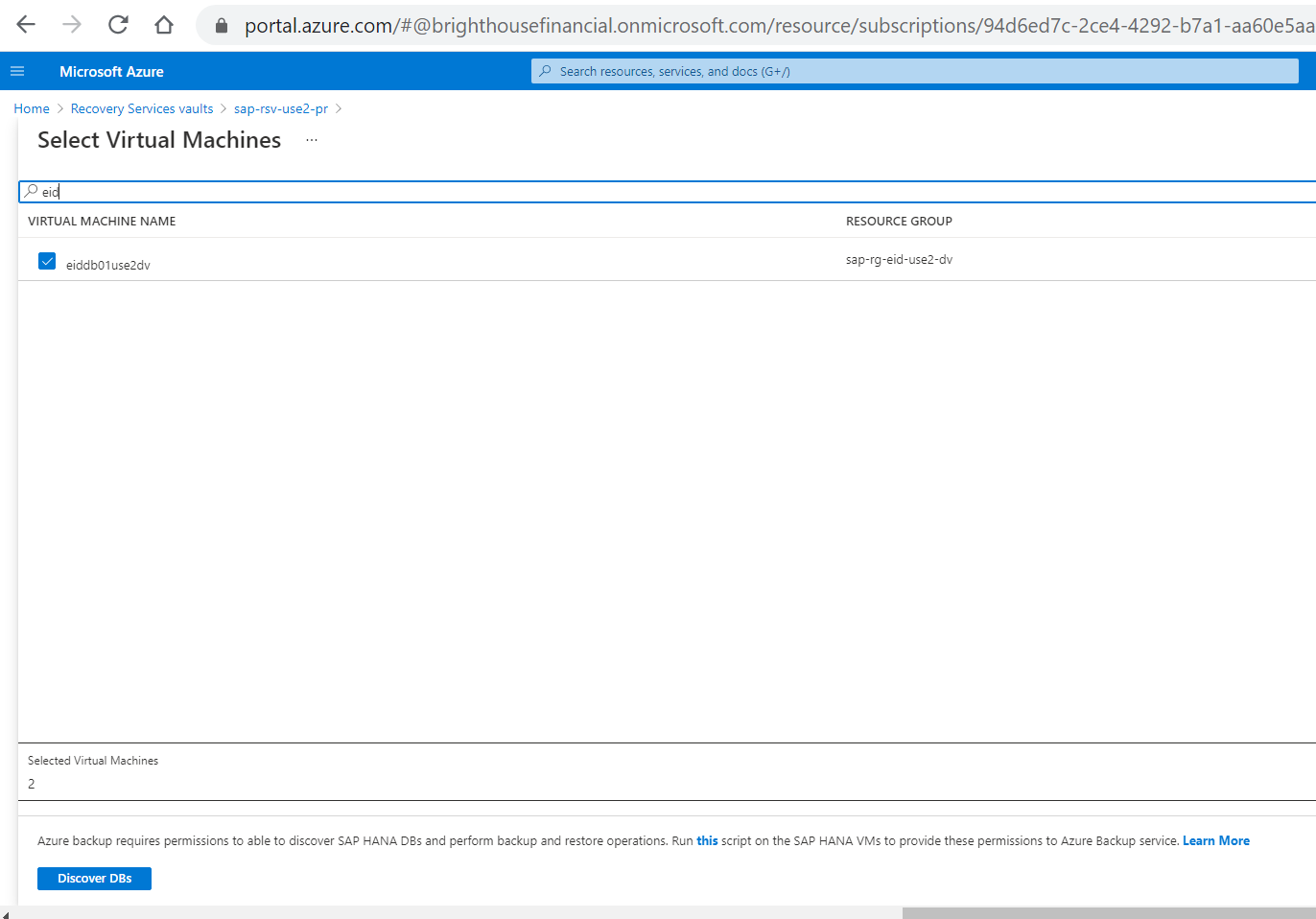
1. In the vault, in **Getting Started**, select **Backup**. In **Where is your workload running?**, select **SAP HANA in Azure VM**.
2. Select **Start Discovery**. This initiates discovery of unprotected Linux VMs in the vault region.
   * After discovery, unprotected VMs appear in the portal, listed by name and resource group.
   * If a VM isn't listed as expected, check whether it's already backed up in a vault.
   * Multiple VMs can have the same name but they belong to different resource groups.
3. In **Select Virtual Machines**, select the link to download the script that provides permissions for the Azure Backup service to access the SAP HANA VMs for database discovery.
4. Run the script on each VM hosting SAP HANA databases that you want to back up.
5. After running the script on the VMs, in **Select Virtual Machines**, select the VMs. Then select **Discover DBs**.
6. Azure Backup discovers all SAP HANA databases on the VM. During discovery, Azure Backup registers the VM with the vault, and installs an extension on the VM. No agent is installed on the database.

Now enable backup.

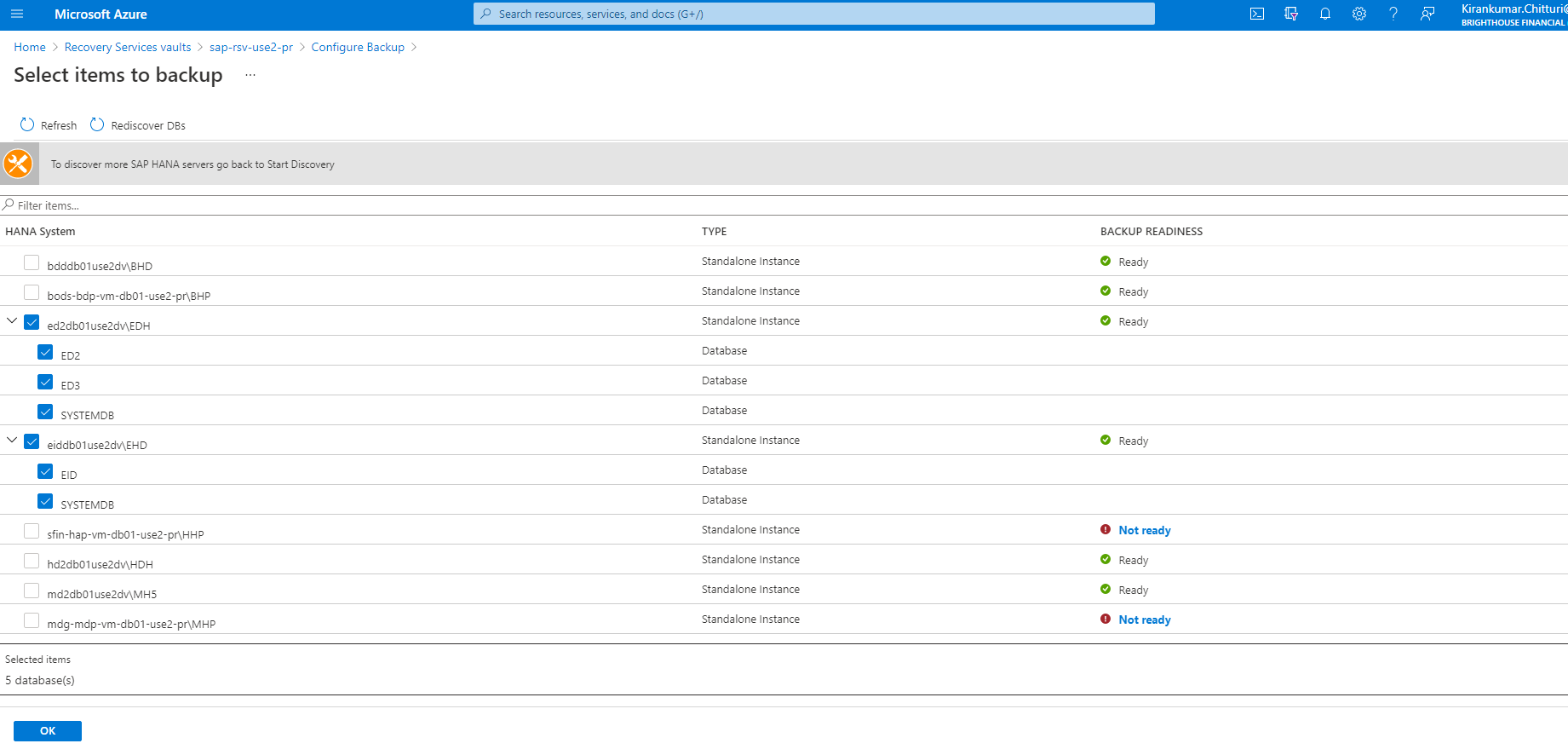
1. In Step 2, select **Configure Backup**.



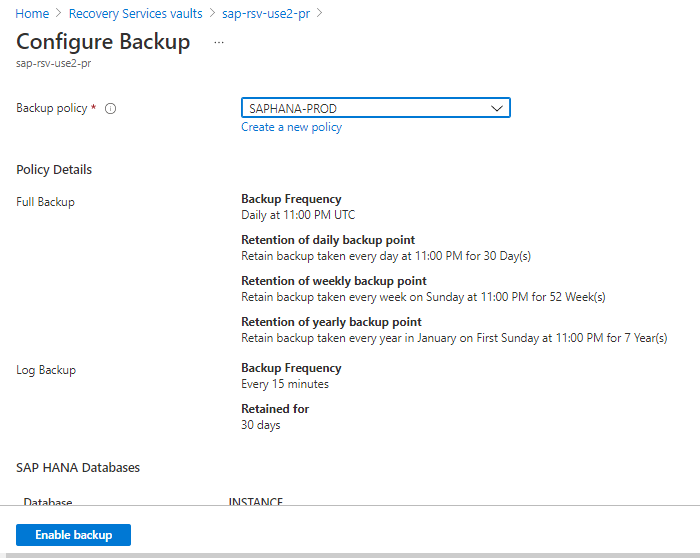




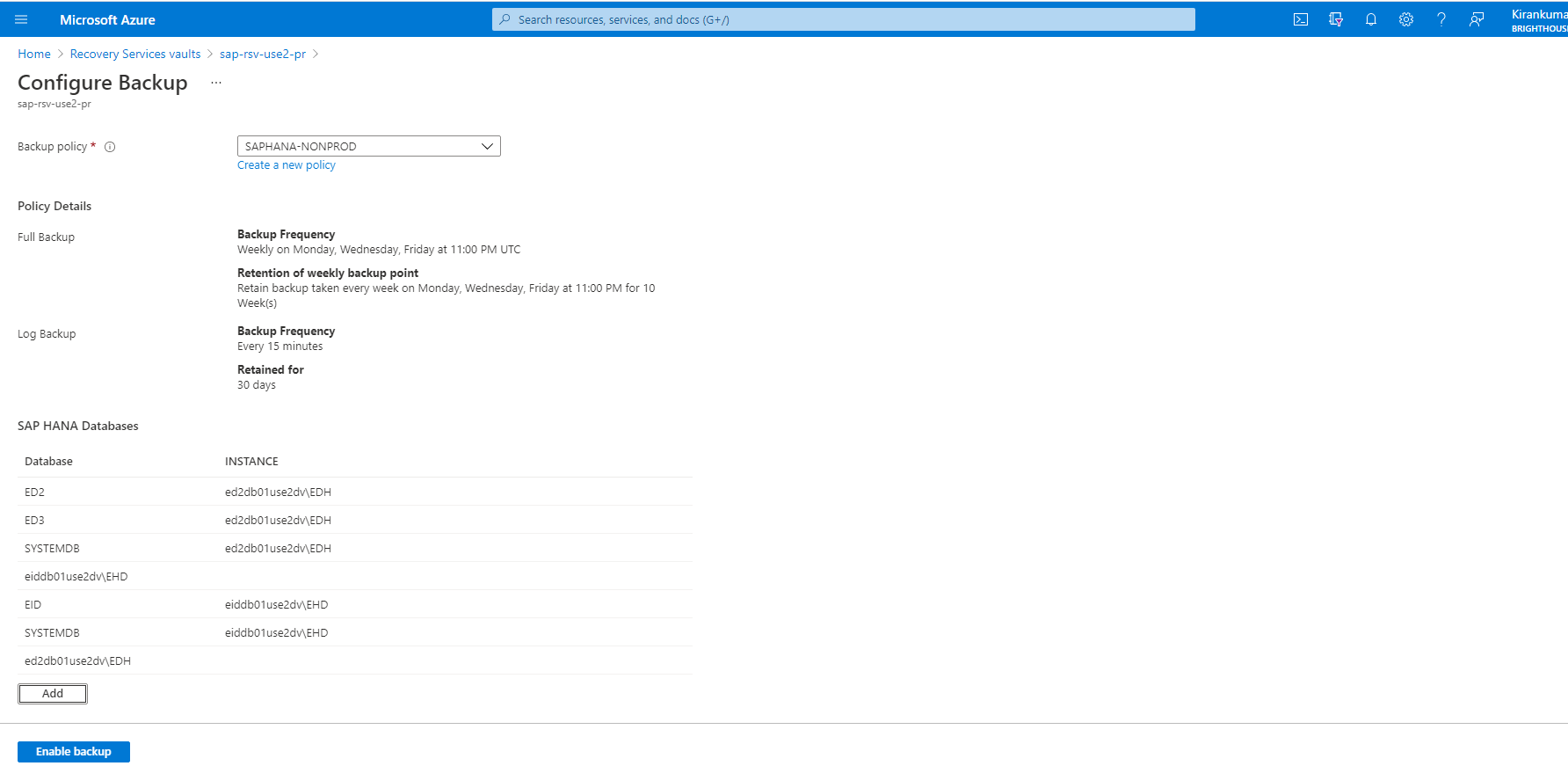
1. In **Select items to back up**, select all the databases you want to protect > **OK**.



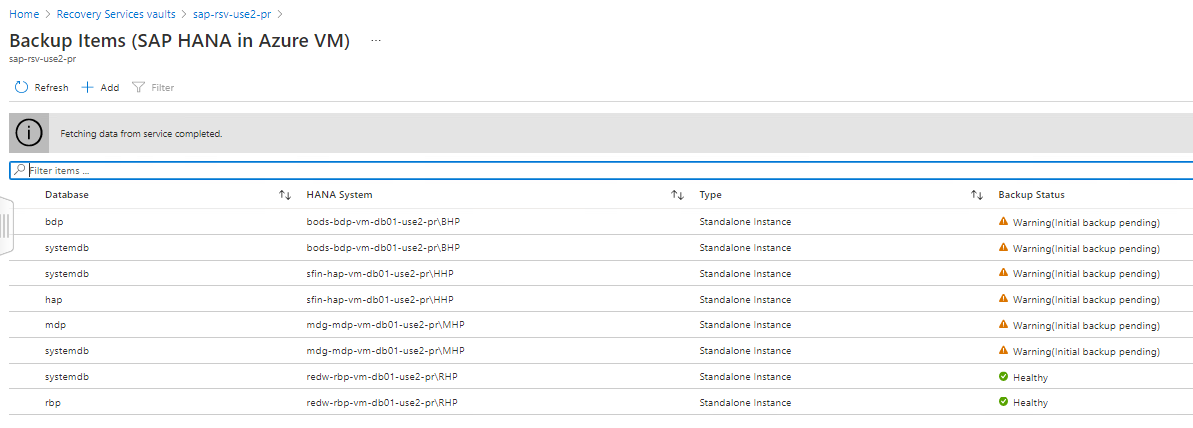
1. In **Backup Policy** > **Choose backup policy**, create a new backup policy for the databases, in accordance with the instructions below.



1. After creating the policy, on the **Backup** menu, select **Enable backup**.



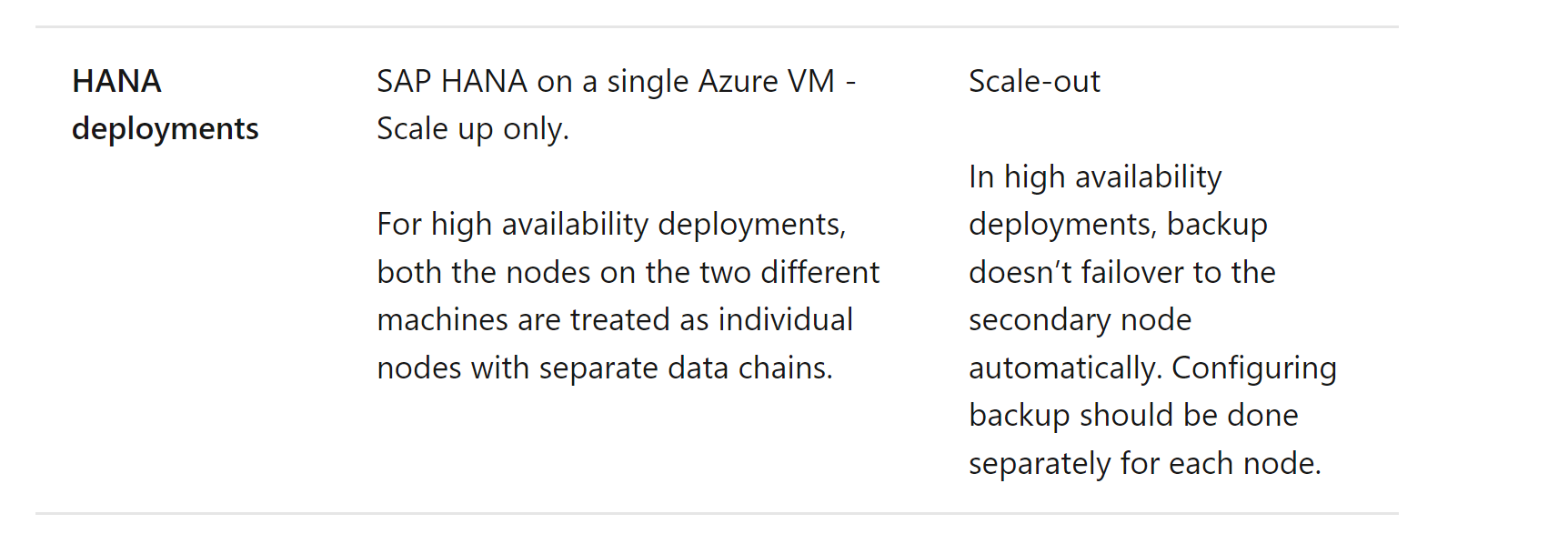
1. Track the backup configuration progress in the **Notifications** area of the portal.



# HA Systems HANA Backup

For the HA systems:

* We were able to onboard only the node which is running the master DB.
* We had made the other node to run as Master DB to get it onboarded.
* DB backups are taken successfully only on the node which is running master DB. So for other node DB backup jobs will be failing.



[https://docs.microsoft.com/en-us/azure/backup/sap-hana-backup-support-matrix](https://urldefense.proofpoint.com/v2/url?u=https-3A__docs.microsoft.com_en-2Dus_azure_backup_sap-2Dhana-2Dbackup-2Dsupport-2Dmatrix&d=DwMFAg&c=eIGjsITfXP_y-DLLX0uEHXJvU8nOHrUK8IrwNKOtkVU&r=elOmiZ-zk66z_OBY7I1pYQYEqhCHMQkFolXRaLkTQRo&m=h5VwN9hnxnhvS5D0jx6M4gRzVd-Cds1tG0IMBYiRvVY&s=DlZTJz0WN_mvC7O0I54YGbVnZb7FS2s6Gh9K3xzwtS0&e=)

# Run an on-demand backup

Backups run in accordance with the policy schedule. You can run a backup on-demand as follows:

1. In the vault menu, select **Backup items**.
2. In **Backup Items**, select the VM running the SAP HANA database, and then select **Backup now**.
3. In **Backup Now**, choose the type of backup you want to perform. Then select **OK**. This backup will be retained for 45 days.
4. Monitor the portal notifications. You can monitor the job progress in the vault dashboard > **Backup Jobs** > **In progress**. Depending on the size of your database, creating the initial backup may take a while.

By default, the retention of on-demand backups is 45 days.

# Run SAP HANA Studio backup on a database with Azure Backup enabled

If you want to take a local backup (using HANA Studio) of a database that's being backed up with Azure Backup, do the following:

1. Wait for any full or log backups for the database to finish. Check the status in SAP HANA Studio / Cockpit.
2. Disable log backups, and set the backup catalog to the file system for relevant database.
3. To do this, double-click **systemdb** > **Configuration** > **Select Database** > **Filter (Log)**.
4. Set **enable\_auto\_log\_backup** to **No**.
5. Set **log\_backup\_using\_backint** to **False**.
6. Set **catalog\_backup\_using\_backint** to **False**.
7. Take an on-demand full backup of the database.
8. Wait for the full backup and catalog backup to finish.
9. Revert the previous settings back to those for Azure:
   * Set **enable\_auto\_log\_backup** to **Yes**.
   * Set **log\_backup\_using\_backint** to **True**.
   * Set **catalog\_backup\_using\_backint** to **True**.

# DB Backup Policy

|  |  |  |
| --- | --- | --- |
|  | **Production** | **Non Prod(DEV and QA)** |
|  | **HANA Database** | **HANA Database** |
| Backup Policy Name | SAPHANA-PROD | SAPHANA-NONPROD |
| **Daily** | Retain backup taken every day at 11:00 PM for 30 Day(s) | Retain backup taken every 3 days at 11:00 PM for 10 iterations |
| **Weekly** | Retain backup taken every week on Sunday at 11:00 PM for 52 Week(s) | NA |
| **Yearly** | Retain backup taken every year in January on First Sunday at 11:00 PM for 7 Year(s) | NA |
| **Log Backup** | Retain backup taken every 15 minutes 30days retention | Retain backup taken every 15 minutes 30 days retention |

# Revision History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Approvers** | **Changes** |
| **1.0** | 29/11/2021 | Sunil Ramachandra/ Senthil Vel Murugan | Sasikumar Sampath | Initial Draft |