



Protect your data using the SnapCenter Service 1.0

Manage SAP HANA Systems

NetApp
August 2021

Learn about the SnapCenter Service

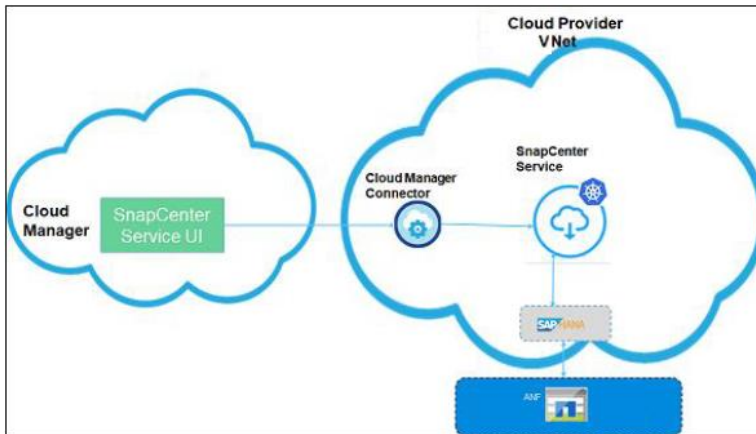
The SnapCenter Service provides data protection capabilities for applications running on NetApp® Cloud Storage. SnapCenter Service enabled within NetApp Cloud Manager offers efficient, application consistent, policy-based backup and restore of SAP HANA® Systems residing on Azure NetApp Files (ANF).

SnapCenter Service architecture

The architecture of SnapCenter Service include the following components.

- SnapCenter UI is integrated with Cloud Manager UI.
The SnapCenter UI is served from the Cloud Manager SAAS framework managed by NetApp that offers multiple storage and data management capabilities.
- Cloud Manager Connector is a component from Cloud Manager that manages the life cycle of the SnapCenter and several other services.
- SnapCenter Service is a set of data protection services hosted on Azure Kubernetes Service(AKS) that orchestrates the data protection workflows.

The following diagram shows the relationship between each component of SnapCenter Service:



The SnapCenter Service UI communicates with the Cloud Manager Connector for user-initiated request. The Connector then communicates to SnapCenter Service and SnapCenter Service invokes ANF management APIs and HANA system commands to perform data protection operations.

SnapCenter Service can be deployed in the same VNet as that of the HANA system, or in a different one. If SnapCenter Service and HANA systems are on different network, network connectivity is required between them.

Supported functionalities

- Adding SAP HANA systems
- Creating on-demand backup of SAP HANA systems
- Protecting SAP HANA systems using system-defined policies or create a custom policy for scheduled backups
- Retaining backups based on the policy
- Restoring SAP HANA systems

- Monitoring jobs
- Displaying the protection summary, configuration details, and job status on the Dashboard
- Sending alerts through email

Limitations

- Internationalization is not supported, ensure to use English browsers.
- Only a Cloud Manager user with “Account Admin” role can enable the SnapCenter Service.
- High availability cluster configuration is not supported.

Get started with SnapCenter Service

1. Create an Azure Connector in your cloud account for your region.
2. Deploy SnapCenter Service.
SnapCenter Service will be deployed in the same subnet and same resource group as that of the Connector.
3. Install the HDBSQL client.
4. Add SAP HANA systems.
5. Protect SAP HANA systems using system-defined or custom policies.

Deploy SnapCenter Service

Deploying SnapCenter Service for Azure NetApp Files (ANF) environment includes the following tasks:

1. Create an Azure Connector in Cloud Manager
2. Enable the SnapCenter Service

Create an Azure Connector in Cloud Manager

An Account Admin should deploy a *Connector* before you can use the Cloud Manager features. The Connector enables Cloud Manager to manage resources and processes within your public cloud environment.

What you'll need:

- Ensure that the subnet chosen for the Connector should not overlap with the following IP address ranges reserved for Azure Kubernetes Service (AKS): 169.254.0.0/16, 172.30.0.0/16, 172.31.0.0/16, and 192.0.2.0/24.
- Ensure that there are no AKS running in the chosen subnet.
- Ensure that the chosen subnet has outbound network connectivity to the internet.
- Ensure that the chosen subnet can access the SAP HANA systems on the respective ports.
- If the VNet of the chosen subnet is different from the VNet of the SAP HANA systems, ensure that the VNets can communicate with each other through VPN gateway, peering, or other means.
- Ensure that the VNet of the chosen subnet is configured with default (Azure provided) DNS Server.

Custom DNS servers are not supported if you are planning to install the Connector without public IP.

- If you want to enable SnapCenter Service behind Azure firewall, you should perform the actions mentioned in [Appendix: Networking Requirements](#).

You should upfront decide whether you want to enable SnapCenter Service behind Azure firewall. After enabling SnapCenter Service, you cannot configure it to run behind Azure firewall. This is an AKS limitation.

Steps:

1. Sign up to NetApp Cloud Central so you can access NetApp's cloud services. [Learn more](#).
2. Log into Cloud Manager and create a Cloud Central account. [Learn more](#).

If you are using Cloud Manager, you can ask your existing Cloud Manager admin to associate you as an Account Admin.

Only an Account Admin can deploy the SnapCenter Service. However, both Account Admin and SnapCenter Admin can perform SnapCenter operations. [Learn more](#).

Note: You can use the default workspace created by the Cloud Manager.

3. Create a Connector.

If...	Then...
If user consent is enabled in your Azure active directory.	1. Create a Connector in Azure from the Cloud Manager UI. Learn more.
If user consent is disabled but you can get consent from the tenant admin.	1. Perform one of the following: <ol style="list-style-type: none"> If the admin consent workflow is configured in your active directory, click Request approval. Learn more. If admin consent workflow is not configured, you can construct the URL for granting tenant-wide admin consent and ask your tenant admin to run the URL in a browser, and provide his consent. <ul style="list-style-type: none"> You should specify the clientID as 989efff4-9a9e-46fa-9f17-de39e15714f9. This is the Cloud Manager Azure application ID named in the Cloud Manager wizard. After providing the consent, the page will display errors that can be ignored by your Admin. 2. Create a Connector in Azure from the Cloud Manager UI. Learn more.
If user consent is disabled and if you are not able to get consent from the tenant admin.	1. Create a Connector from Azure marketplace. Learn more. Note: <ul style="list-style-type: none"> Wherever Cloud Manager for Cloud Volumes ONTAP is specified, the same can be leveraged for SnapCenter Service. For the Cloud Manager Name specify your Connector VM name for better identification. This will be shown as connector name in the Cloud Manager UI. You can skip “Granting Azure permissions” section because that is not required for SnapCenter Service. Ensure that the Azure VM size meets the requirement specified at Connector host requirements. If you have configured firewall and created a route table for the subnet, to access the Connector machine you need to configure a jump host or create a DNAT rule in firewall to translate from the firewall public IP to the Connector private IP.

Note: The username and password or the key that was provided while creating the Connector would be required to connect to the machine.

4. Create an Azure NetApp Files working environment in Cloud Manager for ANF to create and manage NetApp accounts, capacity pools, volumes, and snapshots. [Learn more.](#)

Enable SnapCenter Service for ANF

You can enable the SnapCenter Service using the Cloud Manager UI. When the SnapCenter Service is enabled, Azure Kubernetes Service (AKS) cluster is created that will host the SnapCenter Service.

What you'll need:

- You should send your Connector ID to Debeesantosh.Prakash@netapp.com and Bernd.Herth@netapp.com for whitelisting the Connector because in the Preview builds, SnapCenter will not be available by default in the Cloud Manager UI.

Click **Connector > Manage Connectors**, select the connector Name, and copy the Connector ID.

- You should register the "Microsoft.ContainerService" resource provider in your Azure subscription. [Learnmore](#).

About this task:

The AKS cluster will be created in the same resource group and the same subnet that was chosen while creating the Connector. If your Connector is created without public IP address, then the AKS cluster will be created in private mode.

A user assigned managed identity with necessary permissions is required to create and manage AKS cluster. The user assigned managed identity should be assigned to the Connector VM.


Steps:

- Log into Cloud Manager.
- Select the Azure Connector that was created in the Cloud Manager.

Ensure that the Connector has the network connectivity to the SAP HANA systems to be protected.

- Click **All Services > SnapCenter > Enable**.
- Perform one of the following:

If you have...	Tasks...
Created the Connector from Cloud Manager UI and if you have permissions to create and assign roles.	<p>The user assigned managed identity will be created automatically by SnapCenter.</p> <p>Ensure that the login account has the sufficient permissions.</p> <ol style="list-style-type: none">On the Get Ready page, Click Continue.Specify the Azure credentials.
Created the Connector from Azure marketplace or if you do not have permissions to create and assign roles.	<p>If you do not have sufficient permissions, contact your admin to perform the following steps to create the user assigned managed identity.</p> <ol style="list-style-type: none">Download the prerequisite_azure.sh script from https://docs.netapp.com/us-en/occm/media/prerequisite_azure.sh to your local system.Log into Microsoft Azure portal.

If you have...	Tasks...
	<ol style="list-style-type: none"> Click  to open the cloud shell and select the Bash console. Upload the script to Azure cloud shell. Assign the permission to run the script. <code>chmod +x ./prerequisite_azure.sh</code> Run the script. <pre>./prerequisite_azure.sh -s <subscription_ID> -g <connector_resourcegroup_name> -c <connector_VM_name></pre> The script displays the name of user assigned managed identity in the following format: SnapCenter-MSI-<connector_VM_Name>. After creating the user assigned managed identity, you should perform the following steps in the Cloud Manager UI: <ol style="list-style-type: none"> On the Get Ready page, click specify. Specify the name of the user-assigned managed identity that was created by the script. Click Save. Click Continue.

The user assigned managed identity will be assigned to a custom role with the below permissions at the scope of Connector resource group:

- "Microsoft.Resources/subscriptions/resourceGroups/read",
- "Microsoft.ContainerService/managedClusters/write",
- "Microsoft.ContainerService/managedClusters/read",
- "Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
- "Microsoft.ManagedIdentity/userAssignedIdentities/read",
- "Microsoft.ContainerService/managedClusters/delete",
- "Microsoft.Compute/virtualMachines/read",
- "Microsoft.Network/networkInterfaces/read",
- "Microsoft.ContainerService/managedClusters/listClusterUserCredential/action"

The user assigned managed identity will be assigned to a custom role with the below permissions at the scope of Connector's VNet:

- "Microsoft.Authorization/roleAssignments/read",
- "Microsoft.Network/virtualNetworks/subnets/join/action",
- "Microsoft.Network/virtualNetworks/subnets/read",
- "Microsoft.Network/virtualNetworks/read"

If route table is configured on the subnet for routing to firewall, then the user assigned managed identity will be assigned to a custom role with the below permissions at the scope of the route table.

- "Microsoft.Network/routeTables/**",
- "Microsoft.Network/networkInterfaces/effectiveRouteTable/action",
- "Microsoft.Network/networkWatchers/nextHop/action"

5. On the Cluster Configuration page, perform the following:


- i. Select the cluster configuration.
 - If you select **High Availability**, an Azure Kubernetes Service (AKS) cluster with 3 worker nodes will be created across available zones.
Note: For Preview builds, high availability cluster configuration is not supported.
 - If you select **Non-High Availability**, an AKS cluster with single node will be created.
- ii. Specify the Kubernetes Pod address range.

Ensure that the Kubernetes Pod address range does not overlap with IP ranges of your virtual network, peered virtual networks, and on-premises networks that are connected. Also, the range should not overlap with the Service address range and Docker bridge address.
- iii. Specify the Kubernetes Service address.

Ensure that the Kubernetes service address range does not overlap with the IP ranges of your virtual network, peered virtual networks, and on-premise networks that are connected. Also, the range should not overlap with the Pod address range and Docker bridge address.
- iv. Specify the Docker bridge network.

Ensure that the Docker Bridge address does not overlap with the IP ranges of your virtual network, peered virtual networks, and on-premise networks that are connected. Also, the range should not overlap with the Pod address range and Service address range.
- v. On the Review page, review the details and click **Continue**.

6. After the SnapCenter Service is successfully deployed, click **Finish**.

The AKS cluster details can be obtained by clicking .

Note: If the deployment fails, you can fix the issue and click **Retry** to enable SnapCenter Service.

Permissions required for Azure login account

Azure login account is used to create the user assigned managed identity, required roles, and assigning the identity to the Connector VM.

Note: The credentials of the login account is not stored anywhere in the SnapCenter Service and are not used to call APIs. The credentials are used only in the UI.

Steps:

1. Create a custom role using the **SnapCenter_Deployment_Role1.json** file available at:
https://docs.netapp.com/us-en/occm/media/SnapCenter_Deployment_Role1.json

You should replace the *<Subscription_ID>* in the SnapCenter_Deployment_Role1.json file with your Azure subscription ID.

2. Assign the role to the login account at the scope of Connector's resource group.
3. Create a custom role using the **SnapCenter_Deployment_Role2.json** file available at:
https://docs.netapp.com/us-en/occm/media/SnapCenter_Deployment_Role2.json

You should replace the *<Subscription_ID>* in the SnapCenter_Deployment_Role2.json file with your Azure subscription ID.

4. Assign the role to the login account at the scope of Connector's VNet or higher.

Protect SAP HANA systems

Install the HDBSQL client

After enabling the SnapCenter Service, install the HDBSQL client to perform data protection operations on SAP HANA databases. The HDBSQL client is used to communicate with the SAP HANA systems.

Steps:

1. Download HDB Client software from your SAP account.
It is an archive file with (.SAR) extension. Example: IMDB_CLIENT20_008_20-80002082.SAR
2. Download the latest SAPCAR utility from your SAP account.
Example: SAPCAR_1010-70006178.EXE
3. On the Cloud Manager UI, click **Connector** to obtain the connector name.
4. Log into [Microsoft Azure portal](#).
5. Click **Virtual machines**.
6. Search for the Cloud Manager Connector and copy the public IP address assigned to the Connector.

If the Connector does not have public IP enabled, you should use a jump host.

7. Copy the SAPCAR utility and HDB Client archive (.SAR) file to the Connector machine.
To copy the file to the Connector path, you need the credentials, or the key provided while creating the Connector.

```
scp <SAPCAR_utility> <username>@<IP_ADDRESS>:/home/<username>
scp <HDB_Client_archive> <username>@<IP_ADDRESS>:/home/<username>
```

The files are copied to **/home/<username>**.

For more information, see [how to use SCP to move files](#).

8. Log into the Connector VM with the ssh credentials or key.
9. Run the following commands in the Connector VM.
 - a.

```
sudo cp /home/<username>/<SAPCAR_utility>
/var/lib/docker/volumes/cloudmanager_snapcenter_volume/_data/
```
 - b.

```
sudo cp /home/<username>/<
HDB_Client_archive> /var/lib/docker/volumes/cloudmanager_snapcenter_volume/_da
ta/
```
 - c.

```
sudo docker exec -it cloudmanager_snapcenter /bin/bash
/opt/netapp/hdbclient/hdbclient.sh --archivefile <HDB_Client_archive> --
archiveutil <SAPCAR_utility>
```

Add SAP HANA systems

Manually add the SAP HANA systems. Auto discovery of SAP HANA system is not supported.

While adding the SAP HANA systems, you should add the HDB user store keys. The HDB secure user store key is used to store the connection information of SAP HANA systems securely on the client and HDBSQL client uses the secure user store key to connect to SAP HANA systems.

Steps:

1. On the SnapCenter Service page, click **SAP HANA Systems > Add**.
2. On the System Details page, perform the following actions:
 - i. Select the system type.
 - ii. Specify the SID of the SAP HANA system.
 - iii. Specify the SAP HANA system name.
 - iv. Click HDB Secure User Store Keys text box to add user store keys details.
Specify the key name, system details, username, and password.
 - v. Click **Add**.
Note: If you are adding a multi-host SAP HANA system, click **+** to add user store keys for each host.
3. Click **Continue**.
4. On the Storage Footprint page, perform the following:
 - i. Select the working environment and specify the NetApp account.
 - ii. Select the required volumes.
 - iii. Click **Add Storage**.
5. Click **Continue**.
6. Review all the details and click **Add**.

You can also edit or remove the SAP HANA systems that were added to the SnapCenter Service.

When you remove the SAP HANA system, all the associated backups will be deleted and no longer be protected.

Add non-data volumes

After adding the multitenant database container or single container type SAP HANA system, you can add the non-data volumes of the HANA system.

Steps:

1. On the SnapCenter Service page, click **SAP HANA Systems**.
All the systems added to the SnapCenter Service are displayed.
2. Click **...** corresponding to the multitenant database container or single container type system to which you want to add the non-data volumes.
3. Click **Add Non-Data Volumes**.
4. Click **Add New Storage**.

5. On the Storage Footprint page, perform the following:
 - i. Select the working environment and specify the NetApp account.
 - ii. Select the required volumes.
 - iii. Click **Add Storage**.
6. Click **Add**.

The **Add Non-Data Volumes** option is not available if non-data volumes are already added to the multitenant database container or single container database. If you want to add more non-data volumes, click **Edit System > Add Storage**, select **Non-Data Volumes**, and specify the details.

Back up SAP HANA systems

Create backup policies


Policies specify the backup type, backup frequency, schedules, retention type, retention count, and other characteristics of data protection operations. You can create policies using the Cloud Manager UI.

By default, two system-defined policies, one each for snapshot-based and file-based backup operations are available.

Steps:

1. On the SnapCenter Service page, click **Policies > Add**.
2. On the Create Backup Policy page, perform the following actions:
 - Specify a policy name.
 - Select the type of backup you want to create using this policy.
 - Specify the backup name.

The suffix timestamp is added by default. You can select the other suffixes that should be included in the backup name and define the order in which the suffixes should appear.
 - Specify the schedule frequency and the start and end time for the scheduled backups.
 - Specify the number of snapshot copies to be retained or specify the days for which the snapshot copies should be retained.
3. Click **Add**.


You can view, edit, or delete policies by clicking  corresponding to the policy.

Create on-demand backups

Create on-demand backups of SAP HANA systems either by associating a policy or by not associating any policy.

Steps:

1. On the SnapCenter Service page, click **SAP HANA Systems**.

All the systems added to the SnapCenter Service are displayed.
2. Click  corresponding to the system that you want to protect.
3. Click **On-Demand Backup**.

4. On the On-Demand Backup page, perform one of the following actions:
 - If you want to associate the backup to a policy, select the policy and click **Create Backup**.
 - If you do not want to associate the backup to a policy, perform the following actions:
 - i. In the **Policy** field, select **None**.
 - ii. Select the backup type.

If you are backing up a non-data volume, you can only select **Snapshot Based** as the backup type.
 - iii. Specify the retention period.
 - iv. Click **Create Backup**.

Create scheduled backups

Create scheduled backups by associating policies with the SAP HANA system.

Steps:

1. On the SnapCenter Service page, click **SAP HANA Systems**.

The systems added to the SnapCenter Service is displayed.
2. Click **...** corresponding to the system that you want to protect.
3. Click **Protect**.
4. Select the policies that you want to use to protect the SAP HANA system.
5. Click **Protect**.

Restore SAP HANA systems

In the event of data loss, restore the SAP HANA system from one of the backups of that system.

Only storage restore is supported. You should put the HANA system in recovery mode using SAP HANA Studio or SAP HANA Cockpit before restoring because recovery of HANA system is not supported.

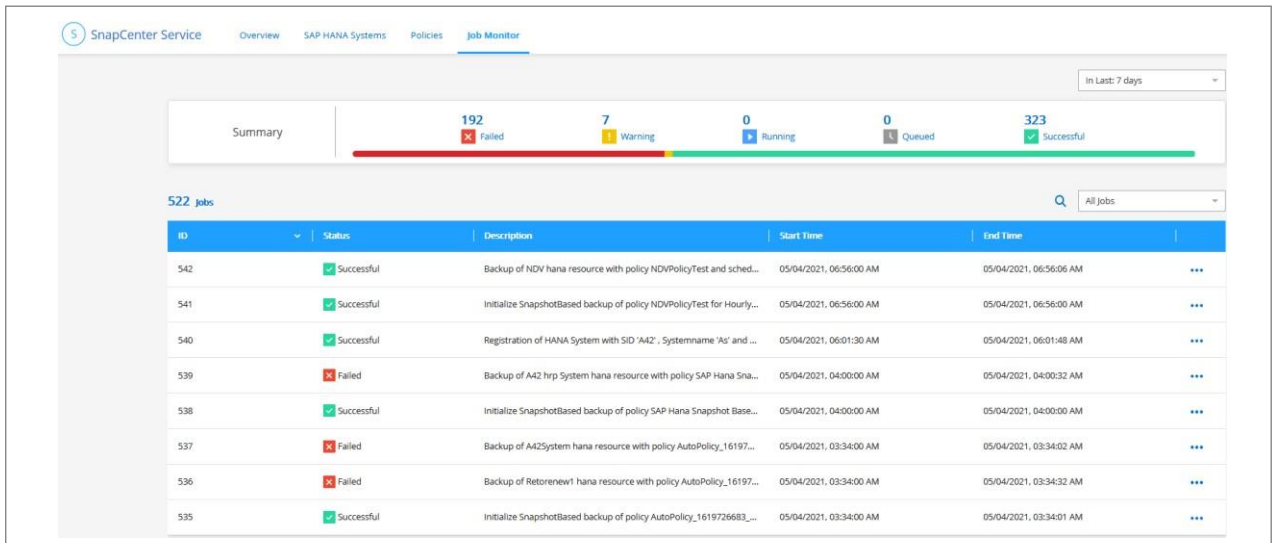
Steps:

1. On the SnapCenter Service page, click **SAP HANA Systems**.

The systems added to the SnapCenter Service are displayed.
2. Click **...** corresponding to the system that you want to restore.
3. Click **View Backups**.
4. In the Backups section, click **...** corresponding to the backup that you want to use to restore the system.
5. Click **Restore**.
6. Review the message and select **Yes, Restore** to confirm.

Monitor jobs

Click **Job Monitor** on the SnapCenter Service page to view the status of the jobs. The Job Monitor page displays an overall summary and lists all the jobs. You can then click ******* corresponding to a particular job to view the details.

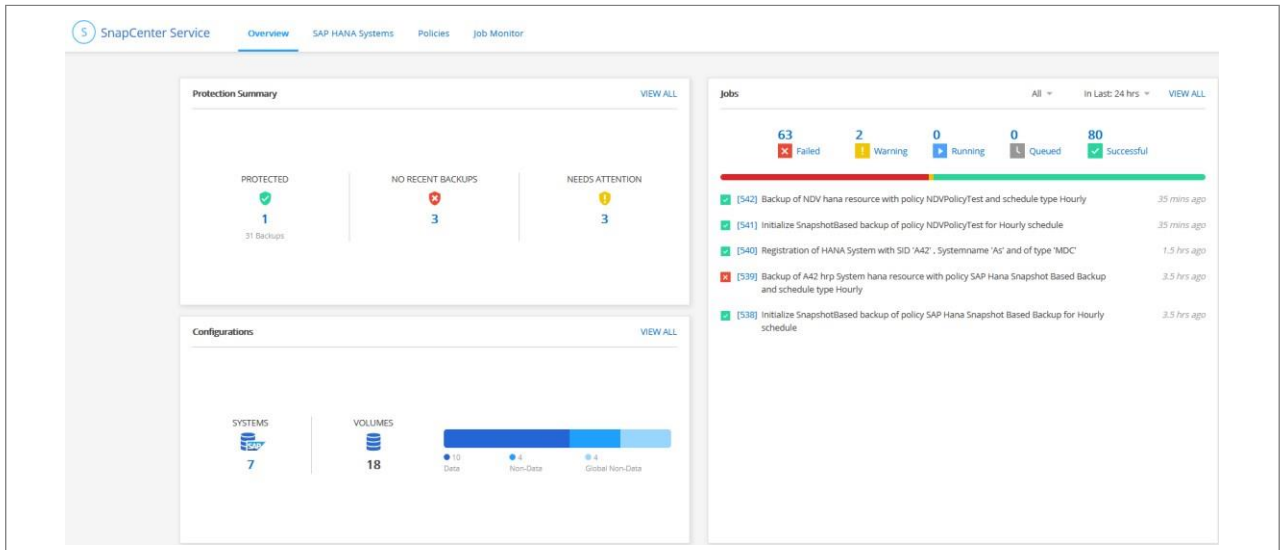


Email notification

The email notifications are sent by default for a failed on-demand backup, scheduled backup, and restore operations. Only a Cloud Manager user with “Account Admin” role will receive the email.

View dashboard

Click **Overview** on the SnapCenter Service page to view the protection summary, configuration details, and job status.



Appendix: Networking Requirements

Firewall configuration

If you want to enable SnapCenter Service behind Azure firewall, you should perform the actions.

- Add the below network rules to the firewall.

Destination Endpoint	Protocol	Port	Comments
ServiceTag - AzureCloud.<Region>:1194	UDP	1194	Not required if you are planning to have a private Connector and private SnapCenter Service cluster.
ServiceTag - AzureCloud.<Region>:9000	TCP	9000	Not required if you are planning to have a private Connector and private SnapCenter Service cluster.
*:123	UDP	123	Required for time synchronization in Azure virtual machines.
ServiceTag - AzureCloud.<Region>:443	TCP	443	Not required if you are planning to have a private Connector and private SnapCenter Service cluster.

- Add an application rule in the firewall with the following FQDN tag and port details:
 - FQDN Tag – AzureKubernetesService
 - HTTPS:443
- Add an Application rule with the below endpoints as target FQDNs with protocol and port as HTTPS:443.

Endpoint	Purpose
<ul style="list-style-type: none">• https://management.azure.com• https://login.microsoftonline.com	Enables Cloud Manager to deploy and manage Cloud Volumes ONTAP in most regions.
<ul style="list-style-type: none">• https://management.microsoftazure.de• https://login.microsoftonline.de	Enables Cloud Manager to deploy and manage Cloud Volumes ONTAP in the Germany regions.
<ul style="list-style-type: none">• https://management.usgovcloudapi.net• https://login.microsoftonline.com	Enables Cloud Manager to deploy and manage Cloud Volumes ONTAP in the US Government regions.
<ul style="list-style-type: none">• https://api.services.cloud.netapp.com	Allows API requests to NetApp Cloud Central.
<ul style="list-style-type: none">• https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Provides access to software images, manifests, and templates.
<ul style="list-style-type: none">• https://cognito-idp.us-east-1.amazonaws.com• https://cognito-identity.us-east-1.amazonaws.com• https://sts.amazonaws.com	Enables the Connector to access and download manifests, templates, and Cloud Volumes ONTAP upgrade images.

Endpoint	Purpose
<ul style="list-style-type: none"> • https://cloud-support-netapp-com-accelerated.s3.amazonaws.com 	
<ul style="list-style-type: none"> • https://cloudmanagerinfraproduct.azurecr.io 	Provides access to software images of container components for an infrastructure that is running Docker and provides a solution for service integrations with Cloud Manager.
<ul style="list-style-type: none"> • https://kinesis.us-east-1.amazonaws.com 	Enables NetApp to stream data from audit records.
<ul style="list-style-type: none"> • https://cloudmanager.cloud.netapp.com 	Allows communication with the Cloud Manager service that includes Cloud Central accounts.
<ul style="list-style-type: none"> • https://netapp-cloud-account.auth0.com 	Allows communication with NetApp Cloud Central for centralized user authentication.
<ul style="list-style-type: none"> • https://support.netapp.com 	Allows communication with NetApp AutoSupport.
<ul style="list-style-type: none"> • https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com 	Allows communication with NetApp for system licensing and support registration.
<ul style="list-style-type: none"> • https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com • https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com 	Enables NetApp to collect information required to troubleshoot support issues.
<ul style="list-style-type: none"> • *.blob.core.windows.net 	Required for high availability when using a proxy.
<ul style="list-style-type: none"> • https://auth0.com 	Required for Auth0 authentication
<ul style="list-style-type: none"> • https://registry-1.docker.io • https://auth.docker.io • https://production.cloudflare.docker.com 	Retrieves the dependencies of SnapCenter's workflow engine.
<ul style="list-style-type: none"> • https://exteranl-log.cloudmanager.netapp.com 	Allows communication to transfer the logs to the Cloud Manager log repository.

- Choose the subnet where you are planning to install SnapCenter Service.
- Create a route table with routes:
 - to forward the traffic from the subnet to the firewall internal IP address
 - to forward the traffic from firewall public IP address to the internet.
- Attach the route table to the subnet.

For information on the networking requirements for Cloud Manager Connector, see [Networking requirements for the Connector](#).

For information on the outbound rules and FQDNs accessed by the AKS cluster for its regular operation, see [Required outbound network rules and FQDNs for AKS clusters](#).

Connectivity to HANA Systems

SnapCenter cluster needs to communicate with HANA systems in the user's network using HDBSQL command. The communication channel between SnapCenter cluster and HANA systems need to be allowed using various network architecture such as:

- Connector and SnapCenter cluster deployed in the same VNet as that of HANA systems
- Connector and SnapCenter cluster deployed in a different VNet as that of HANA systems, with communication established using VNet peering between the 2 VNets.
- Connector and SnapCenter cluster deployed in a different VNet as that of HANA systems, with communication established using VPN gateway between the 2 VNets.

Security Group configuration

If network security group (NSG) is configured in the HANA Systems, it should allow inbound communication from SnapCenter port to the port of HANA System as specified in User Store Key.

- Protocol: All TCP
- Subnet: SnapCenter AKS cluster subnet
- Purpose: To execute HDBSQL command

The HANA services running in the SnapCenter AKS cluster supports SSL communication with HANA systems which have SSL enabled.