Get started

SnapCenter Plug-in for VMware vSphere

NetApp
January 31, 2025

Table of Contents

Get started

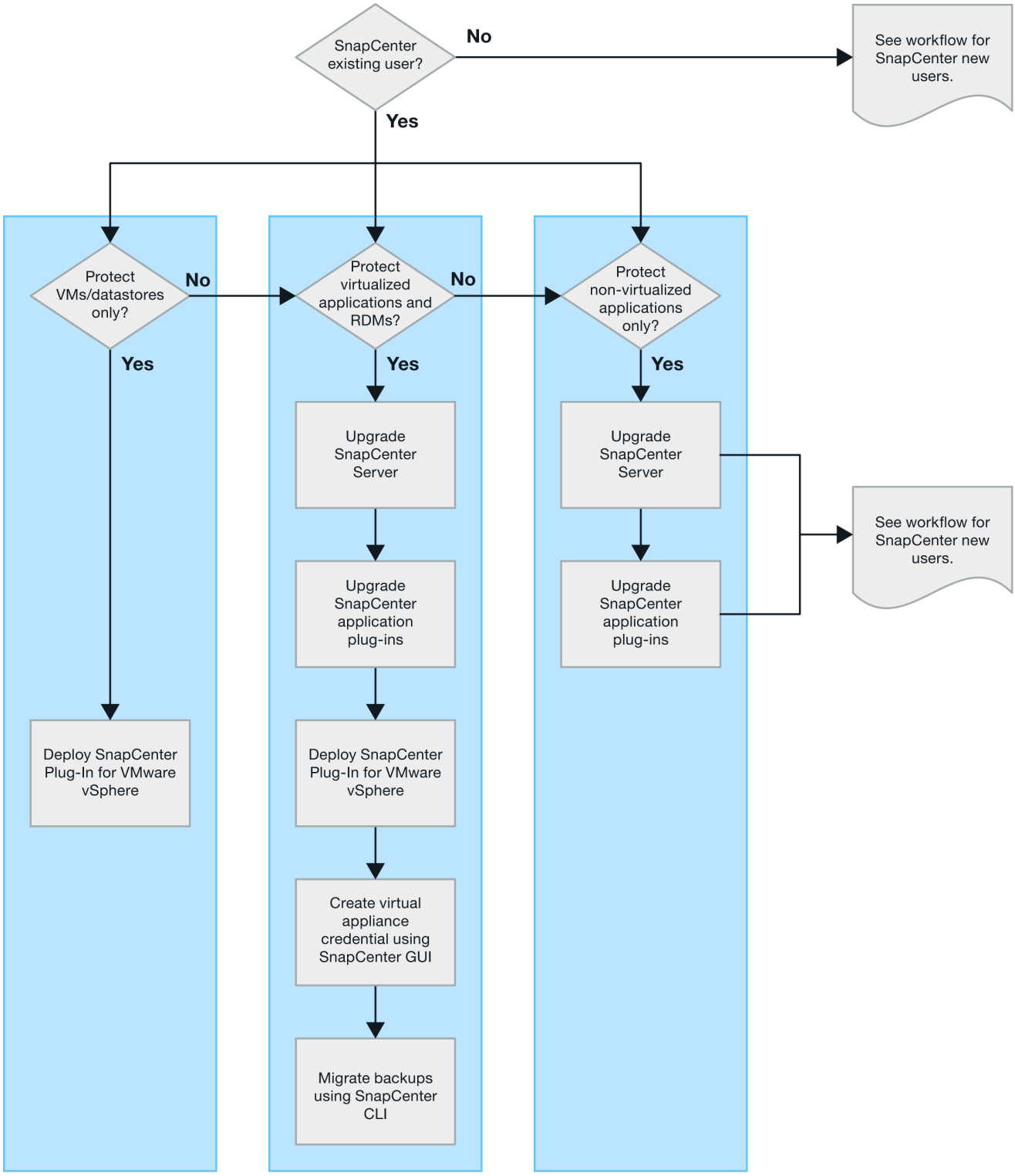
Deployment Overview

To use SnapCenter features to protect VMs, datastores, and application-consistent databases on virtualized machines, you must deploy SnapCenter Plug-in for VMware vSphere.

Existing SnapCenter users must use a different deployment workflow from new SnapCenter users.

Deployment workflow for existing users

If you are a SnapCenter user and have SnapCenter backups, then use the following workflow to get started.



Requirements for deploying SCV

Deployment planning and requirements

You should be aware of the deployment requirements before you deploy the virtual appliance. The deployment requirements are listed in the following tables.

Host requirements

Before you begin deployment of SnapCenter Plug-in for VMware vSphere (SCV), you should be familiar with the host requirements.

- SnapCenter Plug-in for VMware vSphere is deployed as a Linux VM regardless of whether you use the plug-in to protect data on Windows systems or Linux systems.
- You should deploy the SnapCenter Plug-in for VMware vSphere on the vCenter Server.

  Backup schedules are executed in the time zone in which the SnapCenter Plug-in for VMware vSphere is deployed. vCenter reports data in the time zone in which the vCenter is located. Therefore, if the SnapCenter Plug-in for VMware vSphere and vCenter are in different time zones, data in the SnapCenter Plug-in for VMware vSphere Dashboard might not be the same as the data in the reports.

- You must not deploy the SnapCenter Plug-in for VMware vSphere in a folder that has a name with special characters.

  The folder name should not contain the following special characters: $!@#%^&()_+{}';.,*?"<>|

- You must deploy and register a separate, unique instance of the SnapCenter Plug-in for VMware vSphere for each vCenter Server.
  - Each vCenter Server, whether or not it is in Linked Mode, must be paired with a separate instance of the SnapCenter Plug-in for VMware vSphere.
  - Each instance of the SnapCenter Plug-in for VMware vSphere must be deployed as a separate Linux VM.

    For example, if you want to perform backups from six different instances of the vCenter Server, then you must deploy the SnapCenter Plug-in for VMware vSphere on six hosts and each vCenter Server must be paired with a unique instance of the SnapCenter Plug-in for VMware vSphere.

- To protect vVol VMs (VMs on VMware vVol datastores), you must first deploy ONTAP tools for VMware vSphere. ONTAP tools provisions and configures storage for vVols on ONTAP and on the VMware web client.

  For more information, refer to the ONTAP tools for VMware vSphere documentation. Additionally, refer to NetApp Interoperability Matrix Tool for latest information about the supported versions on ONTAP tools.

- SnapCenter Plug-in for VMware vSphere provides limited support of shared PCI or PCIe devices (for example, NVIDIA Grid GPU) due to a limitation of the virtual machines in supporting Storage vMotion. For more information, see the vendor's document Deployment Guide for VMware.
  - What is supported:

    Creating resource groups

    Creating backups without VM consistency

    Restoring a complete VM when all the VMDKs are on an NFS datastore and the plug-in does not need to use Storage vMotion

    Attaching and detaching VMDKs

    Mounting and unmounting datastores

    Guest file restores

- What is not supported:

  Creating backups with VM consistency

  Restoring a complete VM when one or more VMDKs are on a VMFS datastore.

- For a detailed list of the SnapCenter Plug-in for VMware vSphere limitations, refer to SnapCenter Plug-in for VMware vSphere Release Notes.

License requirements

You must provide licenses for…	License requirement
ONTAP	One of these: SnapMirror or SnapVault (for secondary data protection regardless of the type of relationship)
Additional products	vSphere Standard, Enterprise, or Enterprise Plus A vSphere license is required to perform restore operations, which use Storage vMotion. vSphere Essentials or Essentials Plus licenses do not include Storage vMotion.
Primary destinations	SnapCenter Standard: required to perform application-based protection over VMware SnapRestore: required to perform restore operations for VMware VMs and datastores only FlexClone: used for mount and attach operations on VMware VMs and datastores only
Secondary destinations	SnapCenter Standard: used for failover operations for application-based protection over VMware FlexClone: used for mount and attach operations on VMware VMs and datastores only

Software support

Item	Supported versions
vCenter vSphere	7.0U1 and above.
ESXi Server	7.0U1 and above.
IP addresses	IPv4, IPv6
VMware TLS	1.2, 1.3
TLS on the SnapCenter Server	1.2, 1.3 The SnapCenter Server uses this to communicate with the SnapCenter Plug-in for VMware vSphere for application over VMDK data protection operations.
VMware application vStorage API for Array Integration (VAAI)	SnapCenter Plug-in for VMware vSphere uses this to improve performance for restore operations. It also improves performance in NFS environments.

Item	Supported versions
ONTAP tools for VMware	SnapCenter Plug-in for VMware vSphere uses this to manage vVol datastores (VMware virtual volumes). For supported versions, refer to NetApp Interoperability Matrix Tool.

For the latest information about supported versions, refer to NetApp Interoperability Matrix Tool.

Requirements for NVMe over TCP and NVMe over FC protocols

The minimum software requirements for NVMe over TCP and NVMe over FC protocol support are:

- vCenter vSphere 7.0U3
- ESXi 7.0U3
- ONTAP 9.10.1

Space and sizing requirements

Item	Requirements
Operating system	Linux
Minimum CPU count	4 cores
Minimum RAM	Minimum: 12 GB Recommended: 16 GB
Minimum hard drive space for the SnapCenter Plug-in for VMware vSphere, logs, and MySQL database	100 GB

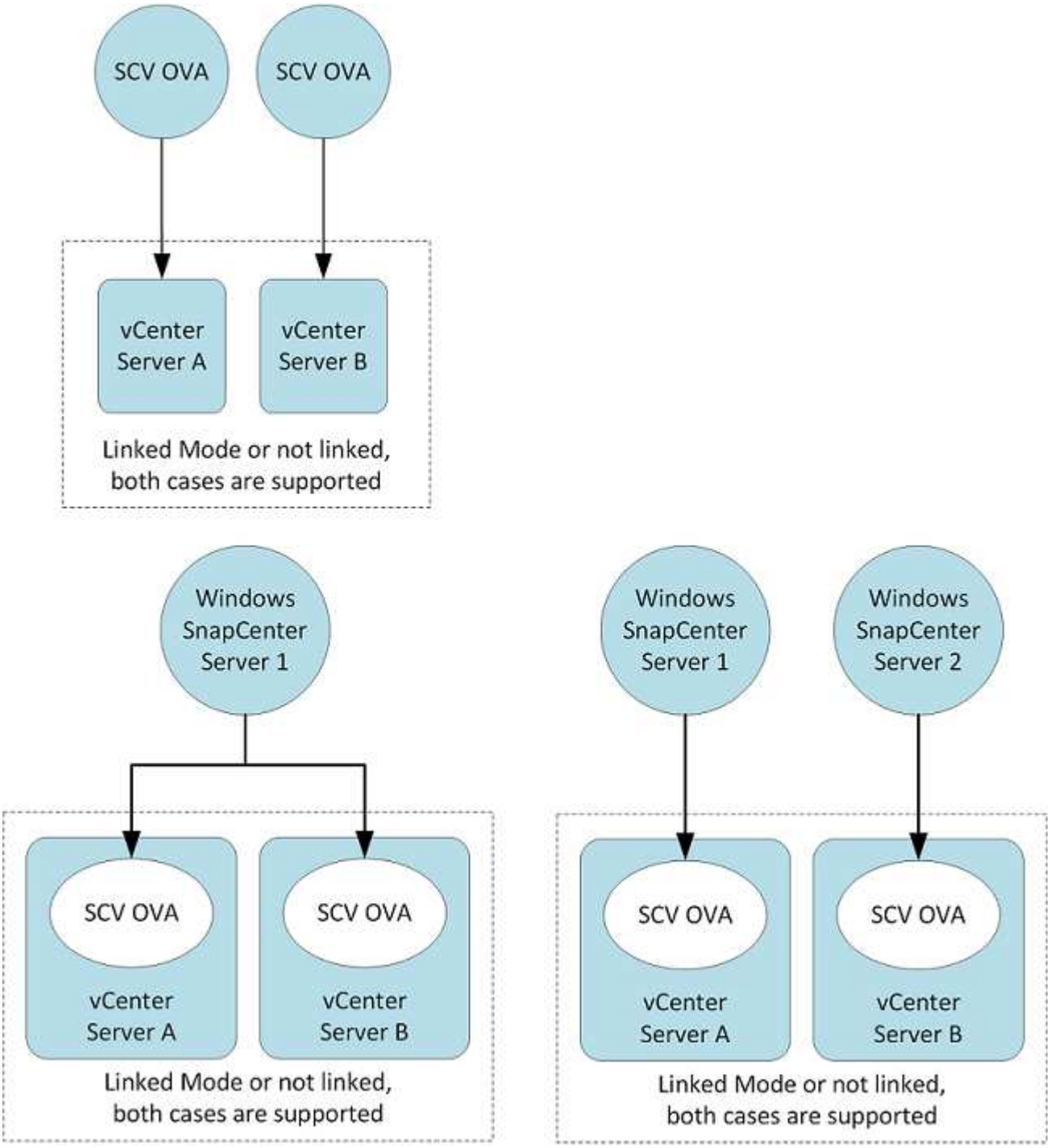
Connection and port requirements

Type of port	Preconfigured port
VMware ESXi Server port	443 (HTTPS), bidirectional The Guest File Restore feature uses this port.
SnapCenter Plug-in for VMware vSphere port	8144 (HTTPS), bidirectional The port is used for communications from the VMware vSphere client and from the SnapCenter Server. 8080 bidirectional This port is used to manage virtual appliances. Note: Custom port for addition of SCV host to SnapCenter is supported.
VMware vSphere vCenter Server port	You must use port 443 if you are protecting vVol VMs.

Type of port	Preconfigured port
Storage cluster or storage VM port	443 (HTTPS), bidirectional 80 (HTTP), bidirectional The port is used for communication between the virtual appliance and the storage VM or the cluster that contains the storage VM.

Configurations supported

Each plug-in instance supports only one vCenter Server. vCenters in linked mode are supported. Multiple plug-in instances can support the same SnapCenter Server as shown in the following figure.



RBAC privileges required

The vCenter administrator account must have the required vCenter privileges, as listed in the following table.

To do this operation…	You must have these vCenter privileges…
Deploy and register the SnapCenter Plug-in for VMware vSphere in vCenter	Extension: Register extension
Upgrade or remove the SnapCenter Plug-in for VMware vSphere	Extension • Update extension • Unregister extension
Allow the vCenter Credential user account registered in SnapCenter to validate user access to the SnapCenter Plug-in for VMware vSphere	sessions.validate.session
Allow users to access the SnapCenter Plug-in for VMware vSphere	SCV Administrator SCV Backup SCV Guest File Restore SCV Restore SCV View The privilege must be assigned at the vCenter root.

AutoSupport

SnapCenter Plug-in for VMware vSphere provides a minimum of information for tracking its usage, including the plug-in URL. AutoSupport includes a table of installed plug-ins that is displayed by the AutoSupport viewer.

ONTAP privileges required

The minimum ONTAP privileges that are required vary according to the SnapCenter plug-ins you are using for data protection.

Beginning with SnapCenter Plug-in for VMware (SCV) 5.0, you need to add applications of type HTTP and ONTAPI as user login methods for any ONTAP users with customized role-based access to the SCV. Without access to these applications, backups will fail. You need to restart the SCV service to recognize changes to ONTAP user login methods.

Minimum ONTAP privileges required

All SnapCenter plug-ins require the following minimum privileges.

All-access commands: Minimum privileges required for ONTAP 8.3 and later.
event generate-autosupport-log
job history show job show job stop

lun lun create lun delete lun igroup add lun igroup create lun igroup delete lun igroup rename lun igroup show lun mapping add-reporting-nodes lun mapping create lun mapping delete lun mapping remove-reporting-nodes lun mapping show lun modify lun move-in-volume lun offline lun online lun persistent-reservation clear lun resize lun serial lun show
snapmirror list-destinations snapmirror policy add-rule snapmirror policy modify-rule snapmirror policy remove-rule snapmirror policy show snapmirror restore snapmirror show snapmirror show-history snapmirror update snapmirror update-ls-set
Version

volume clone create
volume clone show
volume clone split start
volume clone split stop
volume create
volume delete
volume destroy
volume file clone create
volume file show-disk-usage
volume offline
volume online
volume modify
volume qtree create
volume qtree delete
volume qtree modify
volume qtree show
volume restrict
volume show
volume snapshot create
volume snapshot delete
volume snapshot modify
volume snapshot rename
volume snapshot restore
volume snapshot restore-file
volume snapshot show
volume unmount

vserver cifs vserver cifs share create vserver cifs share delete vserver cifs shadowcopy show vserver cifs share show vserver cifs show vserver export-policy vserver export-policy create vserver export-policy delete vserver export-policy rule create vserver export-policy rule show vserver export-policy show vserver iscsi vserver iscsi connection show vserver nvme subsystem controller vserver nvme subsystem controller show vserver nvme subsystem map vserver nvme subsystem map show vserver nvme subsystem map add vserver nvme subsystem map remove vserver nvme subsystem host show vserver nvme subsystem host add vserver nvme subsystem host remove vserver nvme subsystem show vserver nvme subsystem delete vserver nvme namespace show network interface network interface failover-groups

Read-only Commands: Minimum Privileges Required for ONTAP 8.3 and Later
cluster identity show network interface show vserver vserver peer vserver show

You can ignore the *cluster identity show* cluster level command when creating a role to associate with the data vServer.

You can ignore the warning messages about the unsupported vServer commands.

Additional ONTAP information

- If you are running ONTAP 8.2.x:

  You must login as `vsadmin` on the storage VM to have the appropriate privileges for SnapCenter Plug-in for VMware vSphere operations.

- If you are running ONTAP 8.3 and later:

  You must login as `vsadmin` or with a role that has the minimum privileges listed in the tables above.

- You need to be the cluster admin to create and manage user roles. You can associate the users either with Cluster storage VM or with storage VM.
- You need ONTAP 9.12.1 or later versions to use SnapMirror active sync feature.
- To use TamperProof Snapshot (TPS) feature:
  - You need ONTAP 9.13.1 and later versions for SAN
  - You need ONTAP 9.12.1 and later versions for NFS
- For NVMe over TCP and NVMe over FC protocol you need ONTAP 9.10.1 and later.

Beginning with ONTAP version 9.11.1, the communication to ONTAP cluster is through REST APIs. The ONTAP user should have http application enabled. However, if there are issues found with ONTAP REST APIs, the configuration key 'FORCE_ZAPI' helps the switchover to traditional ZAPI workflow. You may need to add or update this key using the config APIS and set it to true. Refer to KB article, How to use RestAPI to edit configuration parameters in SCV for more information.

Minimum vCenter privileges required

Before you begin deployment of SnapCenter Plug-in for VMware vSphere, you should make sure you have the minimum required vCenter privileges.

Required privileges for vCenter Admin role

Datastore.AllocateSpace
Datastore.Browse
Datastore.Delete
Datastore.FileManagement
Datastore.Move
Datastore.Rename
Extension.Register
Extension.Unregister
Extension.Update
Host.Config.AdvancedConfig
Host.Config.Resources
Host.Config.Settings
Host.Config.Storage
Host.Local.CreateVM
Host.Local.DeleteVM
Host.Local.ReconfigVM
Network.Assign
Resource.ApplyRecommendation
Resource.AssignVMToPool
Resource.ColdMigrate
Resource.HotMigrate
Resource.QueryVMotion
System.Anonymous
System.Read
System.View
Task.Create
Task.Update
VirtualMachine.Config.AddExistingDisk
VirtualMachine.Config.AddNewDisk

VirtualMachine.Config.AdvancedConfig
VirtualMachine.Config.ReloadFromPath
VirtualMachine.Config.RemoveDisk
VirtualMachine.Config.Resource
VirtualMachine.GuestOperations.Execute
VirtualMachine.GuestOperations.Modify
VirtualMachine.GuestOperations.Query
VirtualMachine.Interact.PowerOff
VirtualMachine.Interact.PowerOn
VirtualMachine.Inventory.Create
VirtualMachine.Inventory.CreateFromExisting
VirtualMachine.Inventory.Delete
VirtualMachine.Inventory.Move
VirtualMachine.Inventory.Register
VirtualMachine.Inventory.Unregister
VirtualMachine.State.CreateSnapshot
VirtualMachine.State.RemoveSnapshot
VirtualMachine.State.RevertToSnapshot

Required privileges specific to SnapCenter Plug-in for VMware vCenter

Privileges	Label
netappSCV.Guest.RestoreFile	Guest File Restore
netappSCV.Recovery.MountUnMount	Mount/Unmount
netappSCV.Backup.DeleteBackupJob	Delete Resource Group/Backup
netappSCV.Configure.ConfigureStorageSystems.Delete	Remove Storage Systems
netappSCV.View	View
netappSCV.Recovery.RecoverVM	Recover VM
netappSCV.Configure.ConfigureStorageSystems.AddUpdate	Add/Modify Storage Systems
netappSCV.Backup.BackupNow	Backup Now
netappSCV.Guest.Configure	Guest Configuration
netappSCV.Configure.ConfigureSnapCenterServer	Configure SnapCenter Server
netappSCV.Backup.BackupScheduled	Create Resource Group

Download the Open Virtual Appliance (OVA)

Before installing the Open Virtual Appliance (OVA), add the certificate to the vCenter. The .tar file contains the OVA and Entrust Root and Intermediate certificates, the certificates can be found within the certificates folder. The OVA deployment is supported in VMware vCenter 7u1 and above.

In VMware vCenter 7.0.3 versions and higher, the OVA signed by the Entrust certificate is no longer trusted. You need to perform the following procedure to resolve the issue.

Steps

1. To download the SnapCenter Plug-in for VMware:
   - Log in to the NetApp Support Site (https://mysupport.netapp.com/products/index.html).
   - From the list of products, select **SnapCenter Plug-in for VMware vSphere**, then click the **Download Latest Release** button.
   - Download the SnapCenter Plug-in for VMware vSphere `.tar` file to any location.
2. Extract the contents of the tar file. The tar file contains the OVA and certs folder. The certs folder contains the Entrust Root and Intermediate certificates.
3. Log in with the vSphere Client to the vCenter Server.
4. Navigate to **Administration > Certificates > Certificate Management**.
5. Next to **Trusted Root certificates**, click **Add**
   - Go to the *certs* folder.
   - Select the Entrust Root and Intermediate certificates.
   - Install each certificate one at a time.
6. The certificates are added to a panel under **Trusted Root Certificates**.
   Once the certificates are installed, OVA can be verified and deployed.

If the downloaded OVA is not tampered, then the **Publisher** column displays **Trusted certificate**.

Deploy SnapCenter Plug-in for VMware vSphere

To use SnapCenter features to protect VMs, datastores, and application-consistent databases on virtualized machines, you must deploy SnapCenter Plug-in for VMware vSphere.

Before you begin

This section lists all the necessary actions you should do before you begin the deployment.

The OVA deployment is supported in VMware vCenter 7u1 and above.

- You must have read the deployment requirements.
- You must be running a supported version of vCenter Server.
- You must have configured and set up your vCenter Server environment.
- You must have set up an ESXi host for the SnapCenter Plug-in for VMware vSphere VM.
- You must have downloaded the SnapCenter Plug-in for VMware vSphere .tar file.
- You must have the login authentication details for your vCenter Server instance.
- You must have a certificate with valid Public and Private Key files. For more information, refer to articles under Storage Certificate Management section.
- You must have logged out of and closed all browser sessions of vSphere client and deleted the browser cache to avoid any browser cache issue during the deployment of the SnapCenter Plug-in for VMware vSphere.

- You must have enabled Transport Layer Security (TLS) in vCenter. Refer to the VMware documentation.
- If you plan to perform backups in vCenters other than the one in which the SnapCenter Plug-in for VMware vSphere is deployed, then the ESXi server, the SnapCenter Plug-in for VMware vSphere, and each vCenter must be synchronized to the same time.
- To protect VMs on vVol datastores, you must first deploy ONTAP tools for VMware vSphere. For the latest information about supported versions of ONTAP tools, refer to NetApp Interoperability Matrix Tool. ONTAP tools provisions and configures storage on ONTAP and on the VMware web client.

Deploy the SnapCenter Plug-in for VMware vSphere in the same time zone as the vCenter. Backup schedules are executed in the time zone in which the SnapCenter Plug-in for VMware vSphere is deployed. vCenter reports data in the time zone in which the vCenter is located. Therefore, if the SnapCenter Plug-in for VMware vSphere and vCenter are in different time zones, data in the SnapCenter Plug-in for VMware vSphere Dashboard might not be the same as the data in the reports.

Steps

1. For VMware vCenter 7.0.3 and later versions, follow the steps in Download the Open Virtual Appliance (OVA) to import the certificates to vCenter.
2. In your browser, navigate to VMware vSphere vCenter.

   For IPv6 HTML web clients, you must use either Chrome or Firefox.

3. Log in to the **VMware vCenter Single Sign-On** page.
4. On the navigator pane, right-click any inventory object that is a valid parent object of a virtual machine, such as a datacenter, cluster, or host, and select **Deploy OVF Template** to start the VMware deploy wizard.
5. Extract the .tar file, which contains the .ova file onto your local system. On the **Select an OVF template** page, specify the location of the `.ova` file inside the .tar extracted folder.
6. Click **Next**.
7. On the **Select a name and folder** page, enter a unique name for the VM or vApp, and select a deployment location, and then click **Next**.

   This step specifies where to import the `.tar` file into vCenter. The default name for the VM is the same as the name of the selected `.ova` file. If you change the default name, choose a name that is unique within each vCenter Server VM folder.

   The default deployment location for the VM is the inventory object where you started the wizard.

8. On the **Select a resource** page, select the resource where you want to run the deployed VM template, and click **Next**.
9. On the **Review details** page, verify the `.tar` template details and click **Next**.
10. On the **License agreements** page, select the checkbox for **I accept all license agreements**.
11. On the **Select storage** page, define where and how to store the files for the deployed OVF template.
    a. Select the disk format for the VMDKs.
    b. Select a VM Storage Policy.

       This option is available only if storage policies are enabled on the destination resource.

    c. Select a datastore to store the deployed OVA template.

The configuration file and virtual disk files are stored on the datastore.

Select a datastore large enough to accommodate the virtual machine or vApp and all associated virtual disk files.

12. On the **Select networks** page, do the following:
    a. Select a source network and map it to a destination network,

       The Source Network column lists all networks that are defined in the OVA template.

    b. In the **IP Allocation Settings** section, select the required IP address protocol and then click **Next**.

       SnapCenter Plug-in for VMware vSphere supports one network interface. If you need multiple network adapters, you must set that up manually. Refer to KB article: How to create additional network adapters.

13. On the **Customize template** page, do the following:
    a. In the **Register to existing vCenter** section, enter the vCenter name and the vCenter credentials of the virtual appliance.

       In the **vCenter username** field, enter the username in the format `domain\username`.

    b. In the **Create SCV credentials** section, enter the local credentials.

       In the **Username** field, enter the local username; do not include the domain details.

       Make a note of the username and password that you specify. You need to use these credentials if you want to modify the SnapCenter Plug-in for VMware vSphere configuration later.

    c. Enter credentials for the maint user.
    d. In the **Setup Network Properties** section, enter the host name.
       i. In the **Setup IPv4 Network Properties** section, enter the network information such as IPv4 address, IPv4 Netmask, IPv4 Gateway, IPv4 Primary DNS, IPv4 Secondary DNS, and IPv4 Search Domains.
       ii. In the **Setup IPv6 Network Properties** section, enter the network information such as the IPv6 address, IPv6 Netmask, IPv6 Gateway, IPv6 Primary DNS, IPv6 Secondary DNS, and IPv6 Search Domains.

           Select the IPv4 or IPv6 fields, or both, if appropriate. If you are using both IPv4 and IPv6, then you need to specify the Primary DNS for only one of them.

           You can skip these steps and leave the entries blank in the **Setup Network Properties** section, if you want to proceed with DHCP as your network configuration.

    e. In **Setup Date and Time**, select the time zone where the vCenter is located.
14. On the **Ready to complete** page, review the page and click **Finish**.

All hosts must be configured with IP addresses (FQDN hostnames are not supported). The deploy operation does not validate your input before deploying.

You can view the progress of the deployment from the Recent Tasks window while you wait for the OVF import and deployment tasks to finish.

When the SnapCenter Plug-in for VMware vSphere is successfully deployed, it is deployed as a Linux VM, registered with vCenter, and a VMware vSphere client is installed.

15. Navigate to the VM where the SnapCenter Plug-in for VMware vSphere was deployed, then click the **Summary** tab, and then click the **Power On** box to start the virtual appliance.
16. While the SnapCenter Plug-in for VMware vSphere is powering on, right-click the deployed SnapCenter Plug-in for VMware vSphere, select **Guest OS**, and then click **Install VMware tools**.

    The VMware tools is installed on the VM where the SnapCenter Plug-in for VMware vSphere is deployed. For more information on installing VMware tools, see the VMware documentation.

    The deployment might take a few minutes to complete. Successful deployment is indicated when the SnapCenter Plug-in for VMware vSphere is powered on, the VMware tools is installed, and the screen prompts you to log in to the SnapCenter Plug-in for VMware vSphere. You can switch your network configuration from DHCP to static during the first reboot. However, switching from static to DHCP is not supported.

    The screen displays the IP address where the SnapCenter Plug-in for VMware vSphere is deployed. Make a note of the IP address. You need to log in to the SnapCenter Plug-in for VMware vSphere management GUI if you want to make changes to the SnapCenter Plug-in for VMware vSphere configuration.

17. Log in to the SnapCenter Plug-in for VMware vSphere management GUI using the IP address displayed on the deployment screen and using the credentials that you provided in the deployment wizard, then verify on the Dashboard that the SnapCenter Plug-in for VMware vSphere is successfully connected to vCenter and is enabled.

    Use the format `https://<appliance-IP-address>:8080` to access the management GUI.

    Login with the admin username and password set at the time of deployment and the MFA token generated using the maintenance console.

    If the SnapCenter Plug-in for VMware vSphere is not enabled, then refer to Restart the VMware vSphere client service.

    If the host name is 'UnifiedVSC/SCV, then restart the appliance. If restarting the appliance does not change the host name to the specified host name, then you must reinstall the appliance.

After you finish

You should complete the required post deployment operations.

Post deployment required operations and issues

After deploying the SnapCenter Plug-in for VMware vSphere, you must complete the installation.

Required operations after deployment

If you are a new SnapCenter user, you must add storage VMs to SnapCenter before you can perform any data protection operations. When adding storage VMs, specify the management LIF. You can also add a cluster and

specify the cluster management LIF. For information about adding storage, refer to Add storage.

Deployment issues you might encounter

- After deploying the virtual appliance, the **Backup Jobs** tab on the Dashboard might not load in the following scenarios:
  - You are running IPv4 and have two IP addresses for the SnapCenter VMware vSphere host. As a result, the job request is sent to an IP address that is not recognized by the SnapCenter Server. To prevent this issue, add the IP address that you want to use, as follows:
    a. Navigate to the location where the SnapCenter Plug-in for VMware vSphere is deployed: `/opt/netapp/scvservice/standalone_aegis/etc`
    b. Open the file network- interface.properties.
    c. In the `network.interface=10.10.10.10` field, add the IP address that you want to use.
  - You have two NICs.
- After deploying the SnapCenter Plug-in for VMware vSphere, the MOB entry in vCenter for SnapCenter Plug-in for VMware vSphere might still show the old version number. This can occur when other jobs are running in the vCenter. vCenter will eventually update the entry.

To correct either of these issues, do the following:

1. Clear the browser cache and then check if the GUI is operating properly.

   If the problem persists, then restart the VMware vSphere client service

2. Log in to vCenter, then click **Menu** in the toolbar, and then select **SnapCenter Plug-in for VMware vSphere**.

Manage authentication errors

If you do not use the admin credentials, you might receive an authentication error after deploying SnapCenter Plug-in for VMware vSphere or after migrating. If you encounter an authentication error, you must restart the service.

Steps

1. Log on to the SnapCenter Plug-in for VMware vSphere management GUI using the format `https://<appliance-IP-address>:8080`. Use the admin username, password, and the MFA token details to login. MFA token can be generated from the maintenance console.
2. Restart the service.

Register SnapCenter Plug-in for VMware vSphere with SnapCenter Server

If you want to perform application-over-VMDK workflows in SnapCenter (application-based protection workflows for virtualized databases and file systems), you must register SnapCenter Plug-in for VMware vSphere with the SnapCenter Server.

Before you begin

- You must be running SnapCenter Server 4.2 or later.
- You must have deployed and enabled SnapCenter Plug-in for VMware vSphere.

About this task

- You register SnapCenter Plug-in for VMware vSphere with SnapCenter Server by using the SnapCenter GUI to add a “vsphere” type host.

  Port 8144 is predefined for communication within the SnapCenter Plug-in for VMware vSphere.

  You can register multiple instances of SnapCenter Plug-in for VMware vSphere on the same SnapCenter Server to support application-based data protection operations on VMs. You cannot register the same SnapCenter Plug-in for VMware vSphere on multiple SnapCenter Servers.

- For vCenters in Linked Mode, you must register the SnapCenter Plug-in for VMware vSphere for each vCenter.

Steps

1. In the SnapCenter GUI left navigation pane, click **Hosts**.
2. Verify that the **Managed Hosts** tab is selected at the top, then locate the virtual appliance host name and verify that it resolves from the SnapCenter Server.
3. Click **Add** to start the wizard.
4. On the **Add Hosts** dialog box, specify the host you want to add to the SnapCenter Server as listed in the following table:

For this field…	Do this…
Host Type	Select **vSphere** as the type of host.
Host name	Verify the IP address of the virtual appliance.
Credential	Enter the username and password for the SnapCenter Plug-in for VMware vSphere that was provided during the deployment.

5. Click **Submit**.

   When the VM host is successfully added, it is displayed on the Managed Hosts tab.

6. In the left navigation pane, click **Settings**, then click the **Credential** tab, and then select **Add** to add credentials for the virtual appliance.
7. Provide the credential information that was specified during the deployment of SnapCenter Plug-in for VMware vSphere.

   You must select Linux for the Authentication field.

After you finish

If the SnapCenter Plug-in for VMware vSphere credentials are modified, you must update the registration in SnapCenter Server using the SnapCenter Managed Hosts page.

Log in to the SnapCenter VMware vSphere client

When SnapCenter Plug-in for VMware vSphere is deployed, it installs a VMware vSphere client on vCenter, which is displayed on the vCenter screen with other vSphere clients.

Before you begin

Transport Layer Security (TLS) must be enabled in vCenter. Refer to the VMware documentation.

Steps

1. In your browser, navigate to VMware vSphere vCenter.
2. Log in to the **VMware vCenter Single Sign-On** page.

   Click the **Login** button. Due to a known VMware issue, do not use the ENTER key to log in. For details, refer to VMware documentation on ESXi Embedded Host Client issues.

3. On the **VMware vSphere client** page, click Menu in the toolbar, and then select **SnapCenter Plug-in for VMware vSphere**.

Copyright information

Trademark information