SnapCenter Plug-in for VMware vSphere documentation

SnapCenter Plug-in for VMware vSphere

NetApp
December 09, 2025

This PDF was generated from https://docs.netapp.com/us-en/sc-plugin-vmware-vsphere-61/index.html on December 09, 2025. Always check docs.netapp.com for the latest.

Table of Contents

SnapCenter Plug-in for VMware vSphere documentation . . . 1
Release notes . . . 2
SnapCenter Plug-in for VMware vSphere Release notes . . . 2
What's new in SnapCenter Plug-in for VMware vSphere 6.1 . . . 2
Upgrade paths . . . 2
Concepts . . . 4
Product overview . . . 4
Overview of the different SnapCenter GUIs . . . 5
Licensing . . . 6
Role-Based Access Control (RBAC) . . . 6
Types of RBAC for SnapCenter Plug-in for VMware vSphere users . . . 7
vCenter Server RBAC . . . 7
ONTAP RBAC . . . 7
Validation workflow for RBAC privileges . . . 8
ONTAP RBAC features in SnapCenter Plug-in for VMware vSphere . . . 8
Predefined roles packaged with SnapCenter Plug-in for VMware vSphere . . . 9
How to configure ONTAP RBAC for SnapCenter Plug-in for VMware vSphere . . . 10
Get started . . . 12
Deployment Overview . . . 12
Deployment workflow for existing users . . . 12
Requirements for deploying SCV . . . 13
Deployment planning and requirements . . . 13
ONTAP privileges required . . . 18
Minimum vCenter privileges required . . . 22
Download the Open Virtual Appliance (OVA) . . . 23
Deploy SnapCenter Plug-in for VMware vSphere . . . 24
Post deployment required operations and issues . . . 27
Required operations after deployment . . . 27
Deployment issues you might encounter . . . 28
Manage authentication errors . . . 28
Register SnapCenter Plug-in for VMware vSphere with SnapCenter Server . . . 28
Log in to the SnapCenter VMware vSphere client . . . 29
Quick start . . . 31
Overview . . . 31
Deploy SnapCenter Plug-in for VMware vSphere . . . 31
Add storage . . . 33
Create backup policies . . . 33
Create resource groups . . . 33
Monitor and report . . . 34
View status information . . . 34
Monitor jobs . . . 35
Download job logs . . . 36
Access reports . . . 37

Types of reports from the VMware vSphere client . . . 37
Generate a support bundle from the SnapCenter Plug-in for VMware vSphere GUI . . . 39
Generate a support bundle from the maintenance console . . . 40
Audit logs . . . 41
Data Protection Events . . . 42
Maintenance Console Events . . . 43
Admin Console Events . . . 43
Configure syslog servers . . . 43
Change audit log settings . . . 44
Manage storage . . . 45
Add storage . . . 45
Manage storage systems . . . 47
Modify storage VMs . . . 47
Remove storage VMs . . . 48
Modify the configured storage timeout . . . 48
Protect data . . . 49
Data protection workflow . . . 49
View VM and datastore backups . . . 50
Create backup policies for VMs and datastores . . . 50
Create resource groups . . . 55
Manage compatibility check failures . . . 61
Prescripts and postscripts . . . 62
Supported script types . . . 62
Script path location . . . 62
Where to specify scripts . . . 62
When scripts are executed . . . 63
Environment variables passed to scripts . . . 63
Script timeouts . . . 64
Example PERL script #1 . . . 64
Example PERL script #2 . . . 64
Example shell script . . . 65
Add a single VM or datastore to a resource group . . . 65
Add multiple VMs and datastores to a resource group . . . 65
Restore backup of renamed storage . . . 66
Back up resource groups on demand . . . 67
Back up the SnapCenter Plug-in for VMware vSphere MySQL database . . . 68
Manage resource groups . . . 69
Suspend and resume operations on resource groups . . . 69
Modify resource groups . . . 70
Delete resource groups . . . 70
Manage policies . . . 71
Detach policies . . . 71
Modify policies . . . 71
Delete policies . . . 72
Manage backups . . . 72

Rename backups . . . 72
Delete backups . . . 73
Mount and unmount datastores . . . 74
Mount a backup . . . 74
Unmount a backup . . . 75
Restore backups . . . 76
Restore overview . . . 76
How restore operations are performed . . . 76
Search for backups . . . 78
Restore VMs from backups . . . 78
Restore deleted VMs from backups . . . 81
Restore VMDKs from backups . . . 82
Restore the most recent backup of the MySQL database . . . 84
Restore a specific backup of the MySQL database . . . 84
Attach and detach VMDKs . . . 85
Attach VMDKs to a VM or vVol VM . . . 85
Detach a virtual disk . . . 87
Restore guest files and folders . . . 88
Workflow, prerequisites, and limitations . . . 88
Guest restore workflow . . . 88
Prerequisites for restoring guest files and folders . . . 88
Guest file restore limitations . . . 89
Restore guest files and folders from VMDKs . . . 90
Set up proxy VMs for restore operations . . . 93
Configure credentials for VM guest file restores . . . 94
Extend the time of a guest file restore session . . . 95
Guest file restore scenarios you might encounter . . . 95
Guest file restore session is blank . . . 95
Guest file restore attach disk operation fails . . . 96
Guest email shows ?????? for the file name . . . 96
Backups are not detached after guest file restore session is discontinued . . . 96
Manage SnapCenter Plug-in for VMware vSphere appliance . . . 97
Restart the VMware vSphere client service . . . 97
Restart the VMware vSphere client service in a Linux vCenter . . . 97
Access the maintenance console . . . 97
Modify the SnapCenter Plug-in for VMware vSphere password from the maintenance console . . . 99
Create and import certificates . . . 100
Unregister SnapCenter Plug-in for VMware vSphere from vCenter . . . 100
Disable and enable SnapCenter Plug-in for VMware vSphere . . . 101
Remove SnapCenter Plug-in for VMware vSphere . . . 102
Manage your configuration . . . 103
Modify the time zones for backups . . . 103
Modify the logon credentials . . . 104
Modify the vCenter logon credentials . . . 104
Modify the network settings . . . 105

Modify configuration default values . . . 106
Create the scbr.override configuration file . . . 107
Properties you can override . . . 107
Enable SSH for SnapCenter Plug-in for VMware vSphere . . . 112
REST APIs . . . 114
Overview . . . 114
Access REST APIs using the Swagger API web page . . . 115
REST API workflows to add and modify storage VMs . . . 115
REST API workflows to create and modify resource groups . . . 116
REST API workflow to back up on demand . . . 117
REST API workflow to restore VMs . . . 118
REST API workflow to restore deleted VMs . . . 118
REST API workflow to restore VMDKs . . . 119
REST API workflows to attach and detach VMDKs . . . 121
To attach VMDKs, follow this workflow: . . . 121
To detach VMDKs, follow this workflow: . . . 122
REST API workflows to mount and unmount datastores . . . 123
To mount datastores, follow this workflow: . . . 123
To unmount datastores, follow this workflow: . . . 124
REST APIs to download jobs and generate reports . . . 124
Use the following REST APIs in the Jobs section to get detailed information on jobs: . . . 124
Use the following REST API in the Jobs section to download job logs: . . . 124
Use the following REST APIs in the Reports section to generate reports: . . . 124
REST API workflow to modify built-in schedules . . . 125
REST API to mark stuck jobs as failed . . . 125
REST APIs to generate audit logs . . . 126
Upgrade . . . 127
Upgrade from an earlier release of SnapCenter Plug-in for VMware vSphere . . . 127
Upgrade paths . . . 127
Upgrade to a new patch of the same release of SnapCenter Plug-in for VMware vSphere . . . 128
Steps for clearing the cache . . . 129
Information not displayed after upgrading to a new patch of the same release . . . 129
Workaround if you already upgraded before clearing the cache . . . 130
Legal notices . . . 131
Copyright . . . 131
Trademarks . . . 131
Patents . . . 131
Privacy policy . . . 131
Open source . . . 131

SnapCenter Plug-in for VMware vSphere documentation

Release notes

SnapCenter Plug-in for VMware vSphere Release notes

Learn about the new and enhanced features available in SnapCenter Plug-in for VMware vSphere 6.1.

For details about known issues, limitations, and fixed issues, see SnapCenter Plug-in for VMware vSphere 6.1 Release Notes. You must sign in with your NetApp account or create an account to access the Release Notes.

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

What's new in SnapCenter Plug-in for VMware vSphere 6.1

Support for VMs and VMFS datastore on ASA r2 systems

The SnapCenter plug-in for VMware vSphere 6.1 release supports the provisioning of virtual machines (VMs) and VMFS datastore on ASA r2 systems. ASA r2 systems deliver a unified hardware and software solution that creates a simplified experience specific to the needs of SAN-only customers. SnapCenter Plug-in for VMware vSphere 6.1 supported features for VMs, datastores, and Virtual Machine Disk format (VMDK) on ASA r2 systems include:

- Consistency group provisioning for primary protection
- Consistency group-based backup
- Clone workflows
- Restore workflows
- Secondary protection provisioning when you're creating or modifying the resource group.

The secondary protection is supported only on ONTAP 9.16.1 and later versions

Support for secondary Tamperproof Snapshots (TPS)

SnapCenter Plug-in for VMware vSphere introduces support for secondary TPS, ensuring that secondary snapshot copies are protected from deletion or alteration by ransomware attackers or rogue administrators and making them available even after an attack.

Upgrade paths

The version of SnapCenter Plug-in for VMware vSphere (SCV) that you can upgrade to depends on the version that you're currently running.

Upgrade to SnapCenter Plug-in for VMware vSphere (SCV) 4.8 and above is supported only on VMware vCenter server 7 update 1 and later versions. For VMware vCenter server prior to version 7 update 1, you should continue to use SCV 4.7.

If you are on SCV version…	You can directly upgrade SCV to…
SCV 6.0	SCV 6.1
SCV 5.0	SCV 6.0 and SCV 6.1
SCV 4.9	SCV 5.0 and SCV 6.0
SCV 4.8	SCV 4.9 and SCV 5.0
SCV 4.7	SCV 4.8 and SCV 4.9

For virtualized databases and file systems that are integrated with SnapCenter, this is the upgrade path:

If you are using	If your VMware plug-in is…	You can directly upgrade to…
SnapCenter 6.1	SCV 6.0	SCV 6.1
SnapCenter 6.0	SCV 5.0	SCV 6.0
SnapCenter 5.0	SCV 4.9	SCV 5.0
SnapCenter 4.9	SCV 4.8	SCV 4.9
SnapCenter 4.8	SCV 4.7	SCV 4.8

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

Concepts

Product overview

SnapCenter Plug-in for VMware vSphere is a standalone virtual appliance (Open Virtual Appliance format) that provides data protection services for VMs and datastores, and supports data protection services for SnapCenter application-based plug-ins. This document describes how to deploy and use SnapCenter Plug-in for VMware vSphere and includes quick start information.

SnapCenter Plug-in for VMware vSphere is deployed as a Linux-based virtual appliance.

SnapCenter Plug-in for VMware vSphere adds the following functionality to your environment:

- Support for VM-consistent and crash-consistent data protection operations.

  You can use the VMware vSphere client GUI in vCenter for all backup and restore operations of VMware virtual machines (traditional VMs and vVol VMs), VMDKs, and datastores. For vVol VMs (VMs in vVol datastores), only crash-consistent backups are supported. You can also restore VMs and VMDKs and restore files and folders that reside on a guest OS.

  When backing up VMs, VMDKs, and datastores, the plug-in does not support RDMs. Backup jobs for VMs ignore RDMs. If you need to back up RDMs, you must use a SnapCenter application-based plug-in.

  SnapCenter Plug-in for VMware vSphere includes a MySQL database that contains the SnapCenter Plug-in for VMware vSphere metadata. For VM-consistent and crash-consistent data protection, you do not need to install SnapCenter Server.

- Support for application-consistent (application over VMDK/RDM) data protection operations.

  You can use the SnapCenter GUI and the appropriate SnapCenter application plug-ins for all backup and restore operations of databases and filesystems on primary and secondary storage on VMs.

  SnapCenter natively leverages the SnapCenter Plug-in for VMware vSphere for all data protection operations on VMDKs, raw device mappings (RDMs), and NFS datastores. After the virtual appliance is deployed, the plug-in handles all interactions with vCenter. SnapCenter Plug-in for VMware vSphere supports all SnapCenter application-based plug-ins.

  SnapCenter does not support single snapshots of databases and VMs together. Backups for VMs and databases must be scheduled and run independently, which creates separate snapshots, even if the databases and VMs are hosted in the same volume. Schedule the database application backups using the SnapCenter GUI; schedule the VM and datastore backups using the VMware vSphere client GUI.

- VMware tools is required for VM consistent snapshots

  If VMware tools is not installed and running, the file system is not quiesced and a crash-consistent snapshot is created.

- VMware Storage vMotion is required for restore operations in SAN (VMFS) environments

  The restore workflow for VMware file system (VMFS) utilizes the VMware Storage vMotion feature. Storage vMotion is a part of the vSphere Standard License but is not available with the vSphere Essentials or Essentials Plus licenses.

Most restore operations in NFS environments use native ONTAP functionality (for example, Single File SnapRestore) and do not require VMware Storage vMotion.

- ONTAP tools for VMware vSphere is required to configure VMware vVol VMs.

  You use ONTAP tools to provision and configure storage for vVols in ONTAP and in 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 is deployed as a virtual appliance in a Linux VM

  Although the virtual appliance must be installed as a Linux VM, the SnapCenter Plug-in for VMware vSphere supports both Windows-based and Linux-based vCenters. SnapCenter natively uses this plug-in without user intervention to communicate with your vCenter to support SnapCenter application-based plug-ins that perform data protection operations on Windows and Linux virtualized applications.

In addition to these major features, the SnapCenter Plug-in for VMware vSphere also provides support for iSCSI, Fiber Channel, FCoE, NFS 3.0/4.1, VMFS 5.0/6.0, NVMe over FC, and NVMe over TCP.

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

For information about NFS protocols and ESXi host, refer to the vSphere Storage documentation that is provided by VMware.

For information about SnapCenter data protection, refer to data protection information for your SnapCenter plug-in in the SnapCenter Documentation.

For information about supported upgrade and migration paths, refer to SnapCenter Plug-in for VMware vSphere Release Notes.

Overview of the different SnapCenter GUIs

In your SnapCenter environment, you must use the appropriate GUI to perform data protection and management operations.

SnapCenter Plug-in for VMware vSphere is a standalone plug-in that is different from other SnapCenter plug-ins. You must use the VMware vSphere client GUI in vCenter for all backup and restore operations for VMs, VMDKs, and datastores. You also use the web client GUI Dashboard to monitor the list of protected and unprotected VMs. For all other SnapCenter plug-in (application-based plug-ins) operations like backup and restore and job monitoring, you use the SnapCenter GUI.

To protect VMs and datastores, you use the VMware vSphere client interface. The web client GUI integrates with NetApp snapshot technology on the storage system. This enables you to back up VMs and datastores in seconds and restore VMs without taking an ESXi host offline.

There is also a management GUI to perform administrative operations on the SnapCenter Plug-in for VMware vSphere.

The following table shows the operations that the SnapCenter GUI performs.

Use this GUI…	To perform these operations…	And to access these backups…
SnapCenter vSphere client GUI	VM and datastore backup VMDK attach and detach Datastore mount and unmount VM and VMDK restore Guest file and folder restore	Backups of VMs and datastores using the VMware vSphere client GUI.
SnapCenter GUI	Backup and restore of databases and applications on VMs, including protecting databases for Microsoft SQL Server, Microsoft Exchange, and Oracle. Database clone	Backups performed using the SnapCenter GUI.
SnapCenter Plug-in for VMware vSphere management GUI	Modify the network configuration Generate a support bundle Modify NTP server settings Disable/enable the plug-in	N.A.
vCenter GUI	Add SCV roles to vCenter Active Directory users Add resource access to users or groups	N.A.

For VM-consistent backup and restore operations, you must use the VMware vSphere client GUI. Although it is possible to perform some operations using VMware tools, for example, mounting or renaming a datastore, those operations will not be registered in the SnapCenter repository and are not recognized.

SnapCenter does not support single snapshots of databases and VMs together. Backups for VMs and databases must be scheduled and run independently, which creates separate snapshots even if the databases and VMs are hosted in the same volume. Application-based backups must be scheduled by using the SnapCenter GUI; VM-consistent backups must be scheduled by using the VMware vSphere client GUI.

Licensing

SnapCenter Plug-in for VMware vSphere is a free product if you are using the following storage systems:

- On-premises ONTAP clusters (FAS, AFF, and ASA systems)
- Cloud Volumes ONTAP
- ONTAP Select

It is recommended, but not required, that you add SnapCenter Standard licenses to secondary destinations. If SnapCenter Standard licenses are not enabled on secondary systems, you cannot use SnapCenter after performing a failover operation. However, a FlexClone license on secondary storage is required to perform mount and attach operations. A SnapRestore license is required to perform restore operations.

Role-Based Access Control (RBAC)

SnapCenter Plug-in for VMware vSphere provides an additional level of RBAC for managing virtualized resources. The plug-in supports both vCenter Server RBAC and

ONTAP RBAC.

SnapCenter and ONTAP RBAC applies only to SnapCenter Server application-consistent (application over VMDK) jobs. If you use the SnapCenter Plug-in for VMware vSphere to support SnapCenter application-consistent jobs, you must assign the SnapCenterAdmin role; you cannot change the permissions of the SnapCenterAdmin role.

SnapCenter Plug-in for VMware vSphere ships with predefined vCenter roles. You must use the vCenter GUI to add these roles to vCenter Active Directory users to perform SnapCenter operations.

You can create and modify roles and add resource access to users at any time. However, when you are setting up the SnapCenter Plug-in for VMware vSphere for the first time, you should at least add Active Directory users or groups to roles, and then add resource access to those users or groups.

Types of RBAC for SnapCenter Plug-in for VMware vSphere users

If you are using the SnapCenter Plug-in for VMware vSphere, the vCenter Server provides an additional level of RBAC. The plug-in supports both vCenter Server RBAC and ONTAP RBAC.

vCenter Server RBAC

This security mechanism applies to all jobs performed by the SnapCenter Plug-in for VMware vSphere, which includes VM-consistent, VM crash-consistent, and SnapCenter Server application-consistent (application over VMDK) jobs. This level of RBAC restricts the ability of vSphere users to perform SnapCenter Plug-in for VMware vSphere tasks on vSphere objects, such as virtual machines (VMs) and datastores.

SnapCenter Plug-in for VMware vSphere deployment creates the following roles for SnapCenter operations on vCenter:

```
SCV Administrator
SCV Backup
SCV Guest File Restore
SCV Restore
SCV View
```

The vSphere administrator sets up vCenter Server RBAC by doing the following:

- Setting the vCenter Server permissions on the root object (also known as the root folder). You can then refine the security by restricting child entities that do not need those permissions.
- Assigning the SCV roles to Active Directory users.

  At a minimum, all users must be able to view vCenter objects. Without this privilege, users cannot access the VMware vSphere client GUI.

ONTAP RBAC

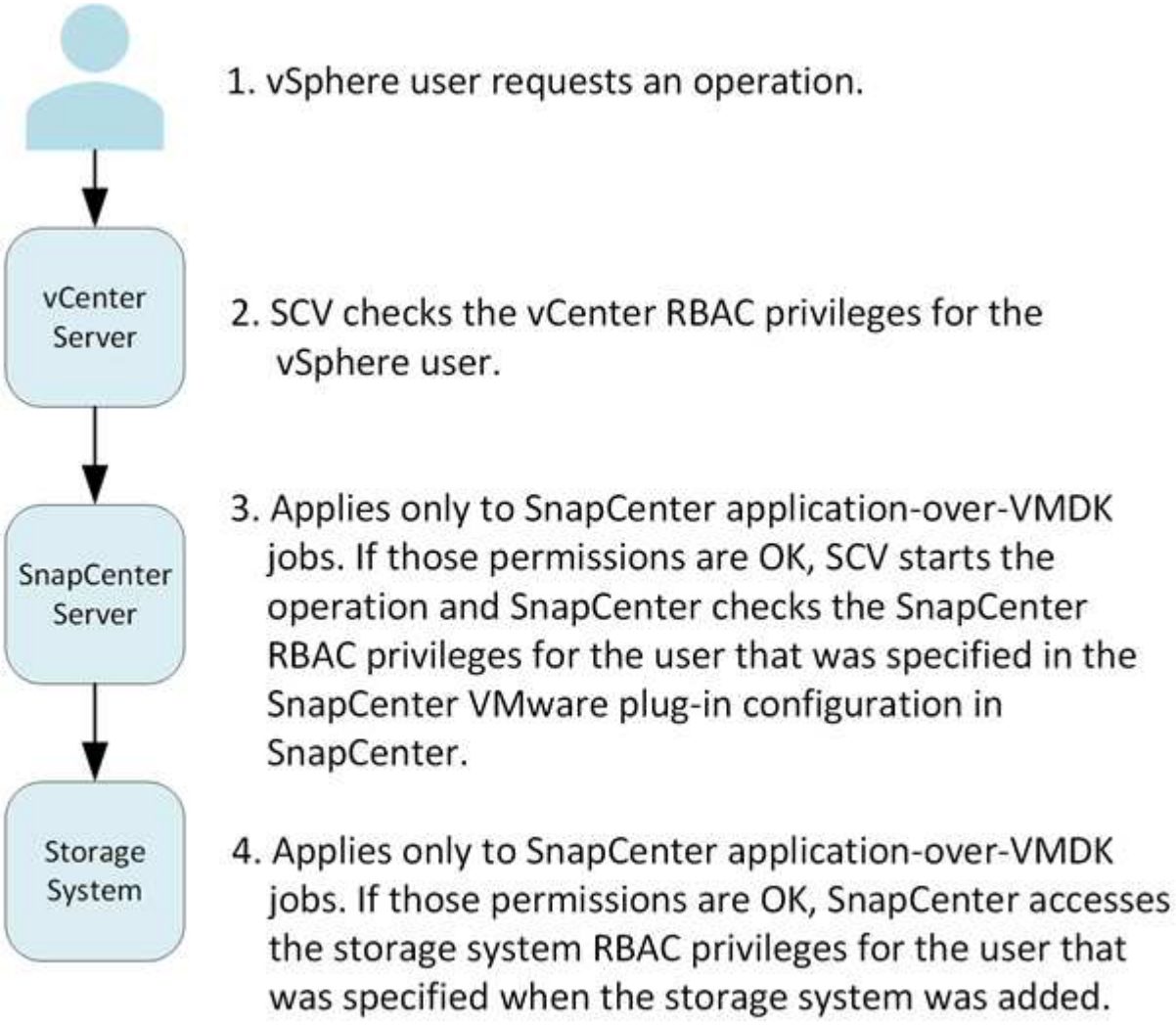
This security mechanism applies only to SnapCenter Server application-consistent (application over VMDK) jobs. This level restricts the ability of SnapCenter to perform specific storage operations, such as backing up storage for datastores, on a specific storage system.

Use the following workflow to set up ONTAP and SnapCenter RBAC:

1. The storage administrator creates a role on the storage VM with the necessary privileges.
2. Then the storage administrator assigns the role to a storage user.
3. The SnapCenter administrator adds the storage VM to the SnapCenter Server, using that storage username.
4. Then the SnapCenter administrator assigns roles to SnapCenter users.

Validation workflow for RBAC privileges

The following figure provides an overview of the validation workflow for RBAC privileges (both vCenter and ONTAP):



*SCV=SnapCenter Plug-in for VMware vSphere

ONTAP RBAC features in SnapCenter Plug-in for VMware vSphere

ONTAP RBAC applies only to SnapCenter Server application-consistent (application over VMDK) jobs.

ONTAP role-based access control (RBAC) enables you to control access to specific storage systems and the actions a user can perform on those storage systems. SnapCenter Plug-in for VMware vSphere works with vCenter Server RBAC, SnapCenter RBAC (when needed to support application-based operations), and ONTAP RBAC to determine which SnapCenter tasks a specific user can perform on objects on a specific storage system.

SnapCenter uses the credentials that you set up (username and password) to authenticate each storage system and determine which operations can be performed on that storage system. SnapCenter Plug-in for VMware vSphere uses one set of credentials for each storage system. These credentials determine all tasks that can be performed on that storage system; in other words, the credentials are for SnapCenter, not an individual SnapCenter user.

ONTAP RBAC applies only to accessing storage systems and performing SnapCenter tasks related to storage, such as backing up VMs. If you do not have the appropriate ONTAP RBAC privileges for a specific storage system, you cannot perform any tasks on a vSphere object hosted on that storage system.

Each storage system has one set of ONTAP privileges associated with it.

Using both ONTAP RBAC and vCenter Server RBAC provides the following benefits:

- Security

  The administrator can control which users can perform which tasks on both a fine-grained vCenter Server object level and a storage system level.

- Audit information

  In many cases, SnapCenter provides an audit trail on the storage system that lets you track events back to the vCenter user who performed the storage modifications.

- Usability

  You can maintain controller credentials in one place.

Predefined roles packaged with SnapCenter Plug-in for VMware vSphere

To simplify working with vCenter Server RBAC, the SnapCenter Plug-in for VMware vSphere provides a set of predefined roles that enable users to perform SnapCenter tasks. There is also a read-only role that allows users to view SnapCenter information, but not perform any tasks.

The predefined roles have both the required SnapCenter-specific privileges and the native vCenter Server privileges to ensure that tasks are completed correctly. In addition, the roles are set up to have the necessary privileges across all supported versions of vCenter Server.

As an administrator, you can assign these roles to the appropriate users.

SnapCenter Plug-in for VMware vSphere returns these roles to their default values (initial set of privileges) each time you restart the vCenter web client service or modify your installation. If you upgrade the SnapCenter Plug-in for VMware vSphere, the predefined roles are automatically upgraded to work with that version of the plug-in.

You can see the predefined roles in the vCenter GUI by selecting **Menu > Administration > Roles** as shown in the following table.

Role	Description
SCV Administrator	Provides all native vCenter Server and SnapCenter-specific privileges necessary to perform all SnapCenter Plug-in for VMware vSphere tasks. Beginning with SCV 6.1 release, a new privilege to create secondary protection is added to this role.
SCV Backup	Provides all native vCenter Server and SnapCenter-specific privileges necessary to back up vSphere objects (virtual machines and datastores). The user also has access to the configure privilege. The user cannot restore backups. Beginning with SCV 6.1 release, a new privilege to create secondary protection is added to this role.
SCV Guest File Restore	Provides all native vCenter Server and SnapCenter-specific privileges necessary to restore guest files and folders. The user cannot restore VMs or VMDKs.
SCV Restore	Provides all native vCenter Server and SnapCenter-specific privileges necessary to restore vSphere objects that have been backed up using the SnapCenter Plug-in for VMware vSphere and to restore guest files and folders. The user also has access to the configure privilege. The user cannot back up vSphere objects.
SCV View	Provides read-only access to all the SnapCenter Plug-in for VMware vSphere backups, resource groups, and policies.

How to configure ONTAP RBAC for SnapCenter Plug-in for VMware vSphere

ONTAP RBAC applies only to SnapCenter Server application-consistent (application over VMDK) jobs.

> 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. For information on creating or modifying login accounts, refer to Worksheets for administrator authentication and RBAC configuration.

You must configure ONTAP RBAC on the storage system if you want to use it with the SnapCenter Plug-in for

VMware vSphere. From within ONTAP, you must perform the following tasks:

- Create a single role.

  Administrator authentication and RBAC

- Create a username and password (storage system credentials) in ONTAP for the role.

  This storage system credential is needed to allow you to configure the storage systems for the SnapCenter Plug-in for VMware vSphere. You do this by entering the credentials in the plug-in. Each time you log in to a storage system using these credentials, you are presented with the set of SnapCenter functions that you set up in ONTAP when you created the credentials.

You can use the administrator or root login to access all the SnapCenter tasks; however, it is a good practice to use the RBAC feature provided by ONTAP to create one or more custom accounts with limited access privileges.

For more information, refer to Minimum ONTAP privileges required.

Get started

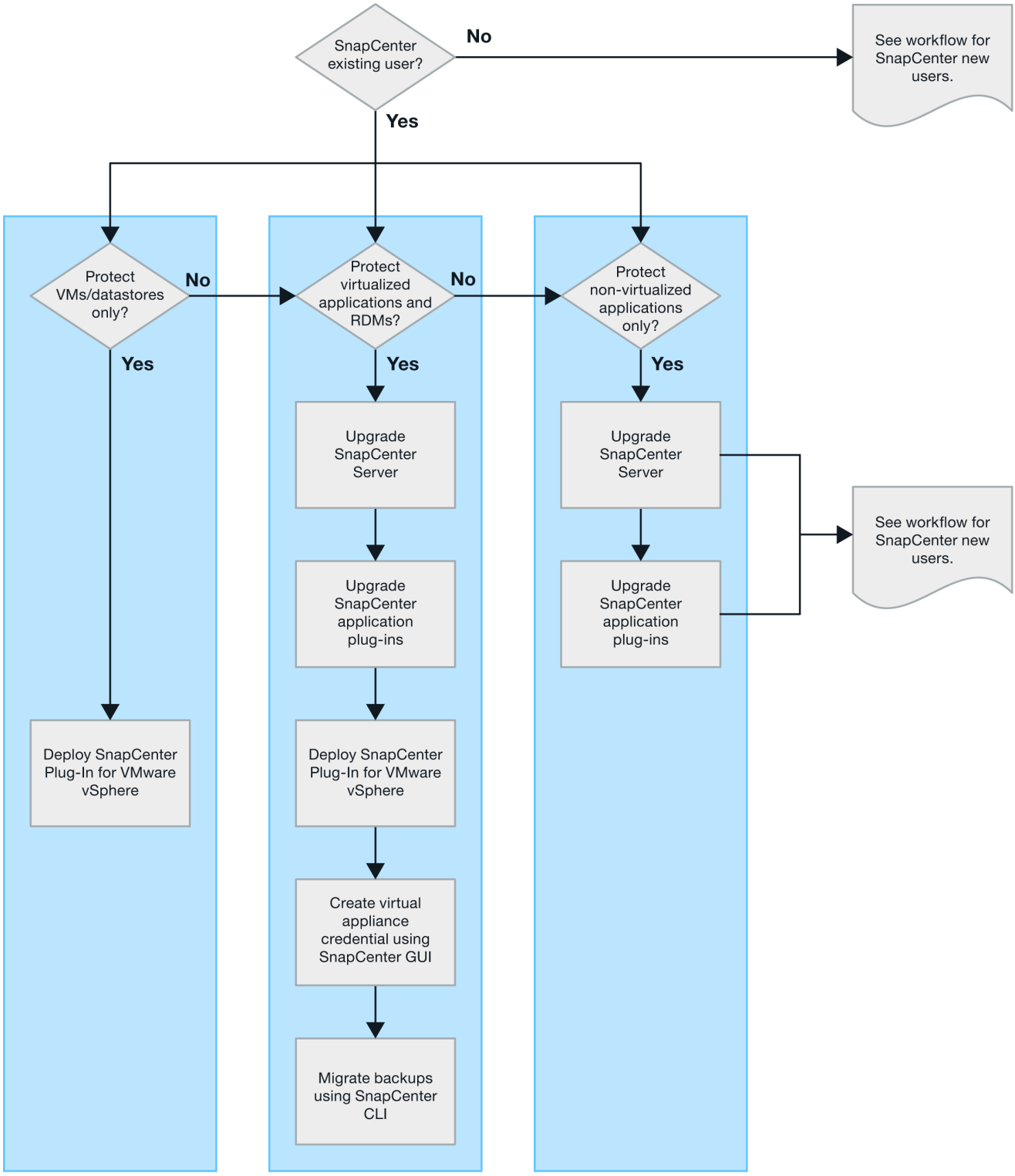
Deployment Overview

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 familiar with the following requirements before you begin deploying the SnapCenter Plug-in for VMware vSphere (SCV).

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 it is used to protect data on Windows 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, and vCenter reports data in the time zone in which it 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 with a name that contains 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 in Linked Mode or not, 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, suppose you want to perform backups from six different instances of the vCenter Server. In that case, 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 using 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, sizing, and scaling requirements

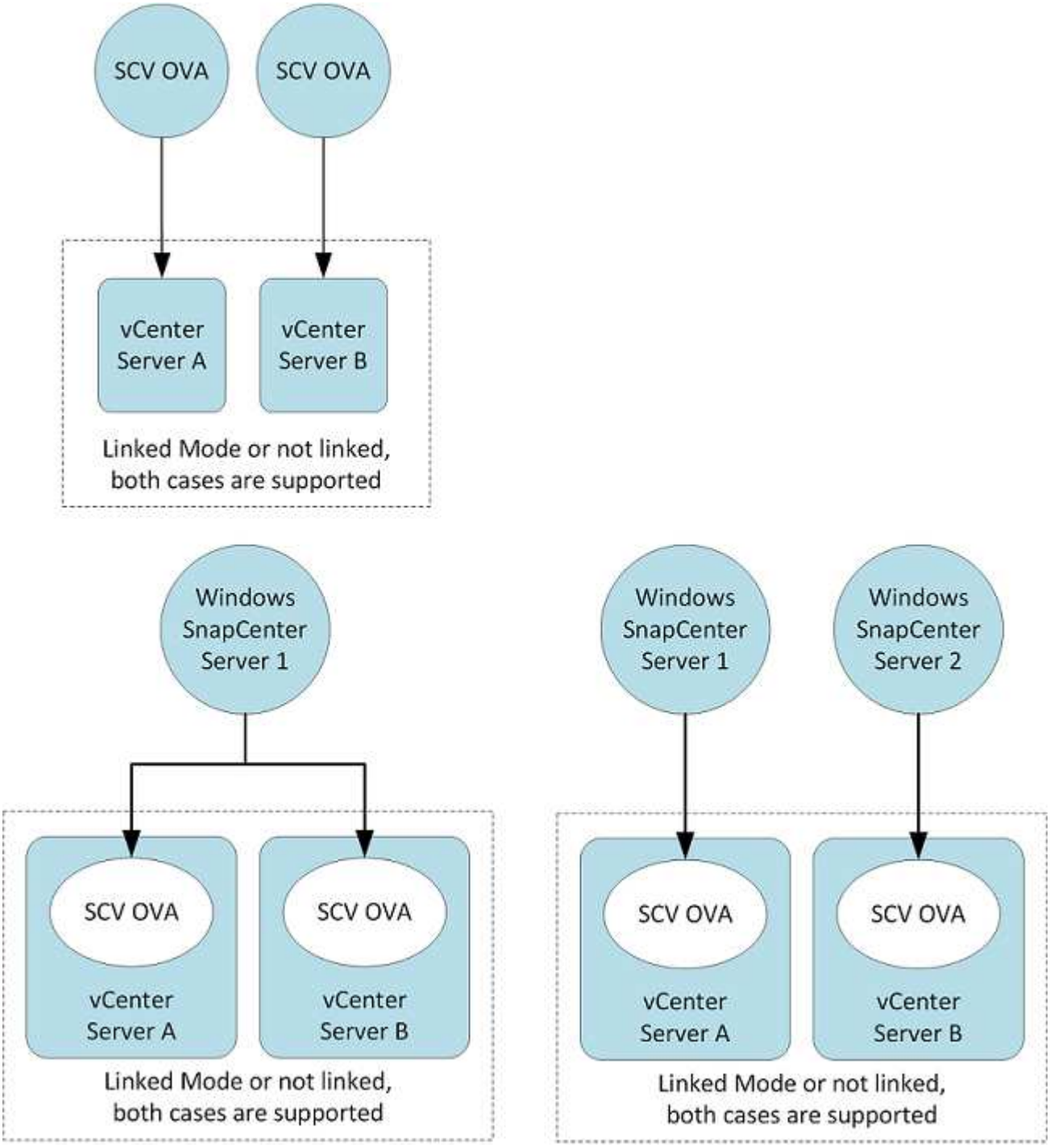
Item	Requirements
Recommended CPU count	8 cores
Recommended RAM	24 GB
Minimum hard drive space for the SnapCenter Plug-in for VMware vSphere, logs, and MySQL database	100 GB

Connection and port requirements

Type of port	Pre-configured 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 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.
Storage cluster or storage VM port	443 (HTTPS), bidirectional 80 (HTTP), bidirectional The port is used to communicate between the virtual appliance and the storage VM or the cluster containing the storage VM.

Configurations supported

Each plug-in instance supports only one vCenter Server, which is in linked mode. However, 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 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 ONTAP privileges.
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 status
volume clone split stop
volume create
volume delete
volume destroy
volume file clone create
volume file show-disk-usage
volume offline
volume online
volume managed-feature
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 modify-snaplock-expiry-time
volume snapshot rename
volume snapshot restore
volume snapshot restore-file
volume snapshot show
volume snapshot show-delta
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 create vserver nvme subsystem delete vserver nvme subsystem host vserver nvme subsystem host show vserver nvme subsystem host add vserver nvme subsystem host remove vserver nvme subsystem map vserver nvme subsystem map show vserver nvme subsystem map add vserver nvme subsystem map remove vserver nvme subsystem modify vserver nvme subsystem show vserver nvme namespace create vserver nvme namespace delete vserver nvme namespace modify vserver nvme namespace show network interface network interface failover-groups

Read-only Commands: Minimum ONTAP Privileges
cluster identity show network interface show vserver vserver peer vserver show

All-access commands: Minimum ONTAP privileges
consistency-group storage-unit 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

- 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 select 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**, select **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 address 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. Select **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 select **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 select **Next**.
9. On the **Review details** page, verify the `.tar` template details and select **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 select **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 address fields, or both, if appropriate. If you are using both IPv4 and IPv6 addresses, 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 select **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 select the **Summary** tab, and then select 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 select **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 address 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 select **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, select **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. Select **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. Select **Submit**.

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

6. In the left navigation pane, select **Settings**, then select 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.

   Select 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, select Menu in the toolbar, and then select **SnapCenter Plug-in for VMware vSphere**.

Quick start

Overview

The quick start documentation provides a condensed set of instructions for deploying the SnapCenter Plug-in for VMware vSphere virtual appliance and enabling the SnapCenter Plug-in for VMware vSphere. These instructions are intended for customers who do not have SnapCenter already installed and who want to protect only VMs and datastores.

Before you begin, refer to Deployment planning and requirements.

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.
The Download the Open Virtual Appliance (OVA) page provides instructions to download the OVA files.

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

3. Log in to the **VMware vCenter Single Sign-On page**.
4. On the Navigation pane, right-click any inventory object that is a valid parent object of a virtual machine, such as a datacenter, folder, cluster, or host, and select **Deploy OVF Template** to start the VMware deploy wizard.
5. On the **Select an OVF template** page, specify the location of the `.ova` file (as listed in the following table) and select **Next**.

On this wizard page…	Do this…
Select a name and folder	Enter a unique name for the VM or vApp and select a deployment location.
Select a resource	Select a resource where you want to run the deployed VM template.
Review details	Verify the `.ova` template details.
License agreements	Select the checkbox for **I accept all license agreements**.
Select storage	Define where and how to store the files for the deployed OVF template.
Select networks	Select a source network and map it to a destination network.

On this wizard page…	Do this…
Customize template	In **Register to existing vCenter**, enter the vCenter credentials. In **Create SnapCenter Plug-in for VMware vSphere credentials**, enter the SnapCenter Plug-in for VMware vSphere credentials. 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 at a later time. In the **Setup Network Properties** section, enter the network information. In the **Setup Date and Time** section, select the time zone where the vCenter is located.
Ready to complete	Review the page and select **Finish**.

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

6. Navigate to the VM where SnapCenter Plug-in for VMware vSphere was deployed, then select the **Summary** tab, and then select the **Power On** box to start the SnapCenter Plug-in for VMware vSphere.
7. 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 select **Install VMware tools**.

   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.

   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.

8. Log in to the SnapCenter Plug-in for VMware vSphere management GUI using the IP address displayed on the deployment screen 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.

9. Log in to vCenter HTML5 client, then select **Menu** in the toolbar, and then select **SnapCenter Plug-in for VMware vSphere**

Add storage

Follow the steps in this section to add storage.

1. In the left navigator pane of the SCV plug-in, select **Storage Systems** and then select **Add** option.
2. On the Add Storage System dialog box, enter the basic SVM or cluster information, and select **Add**.

Create backup policies

Follow the instructions given below to create backup policies

1. In the left navigator pane of the SCV plug-in, select **Policies**, and then select **New Policy**.
2. On the **New Backup Policy** page, enter the policy configuration information, and then select **Add**.

Create resource groups

Follow the steps below to create resource groups.

1. In the left navigator pane of the SCV plug-in, select **Resource Groups**, and then select **Create**.
2. Enter the required information on each page of the Create Resource Group wizard, select VMs and datastores to be included in the resource group, and then select the backup policies to be applied to the resource group. Add the remote secondary protection details and specify the backup schedule.

Backups are performed as specified in the backup policies that are configured for the resource group.

You can perform a backup on demand from the **Resource Groups** page by selecting **Run Now**.

Monitor and report

View status information

You can view status information on the vSphere client Dashboard. Status information is updated once an hour.

Steps

1. From the vCenter client shortcut page, select SnapCenter Plug-in for VMware vSphere (SCV).
2. In the left navigation pane of SCV, select **Dashboard** > **Status**.
3. View overview status information or select a link for more details, as listed in the following table.

This dashboard tile…	Displays the following information…
Recent job activities	The three to five most recent backup, restore, and mount jobs. • Select on a job ID to see more details about that job. • Select **See all** to go to the Job Monitor tab for more details on all jobs.
Jobs	A count of each job type (backup, restore, and mount) performed within the selected time window. Hover the cursor over a section of the chart to see more details for that category.

This dashboard tile…	Displays the following information…
Latest Protection Summary	Summaries of the data protection status of primary and secondary VMs or datastores within the selected time window. • Select the drop-down menu to select **VMs** or **Datastores**. • For secondary storage, select **SnapVault** or **SnapMirror**. • Hover the cursor over a section of a chart to see the count of VMs or Datastores in that category. In the Successful category, the most recent backup is listed for each resource. • You can change the time window by editing the configuration file. The default is 7 days. For more information, refer to Customize your configuration. • Internal counters are updated after each primary or secondary backup. The dashboard tile is refreshed every six hours. The refresh time cannot be changed. Note: If you use a mirror-vault protection policy, then the counters for the protection summary are displayed in the SnapVault summary chart, not in the SnapMirror chart.
Configuration	The total number of each type of object managed by the SnapCenter Plug-in for VMware vSphere.
Storage	The total number of snapshots, SnapVault, and SnapMirror snapshots, generated and the amount of storage used for primary and secondary snapshots. The line graph separately plots primary and secondary storage consumption on a day-by-day basis over a rolling 90-day period. Storage information is updated once every 24 hours at 1:08 A.M. Storage Savings is the ratio of logical capacity (snapshot savings plus storage consumed) to the physical capacity of primary storage. The bar chart illustrates the storage savings. Hover the cursor over a line on the chart to see detailed day-by-day results.

Monitor jobs

After performing any data protection operation using the VMware vSphere client, you can

monitor the job status from the Job Monitor tab in the Dashboard and view job details.

Steps

1. From the vCenter client shortcut page, select SnapCenter Plug-in for VMware vSphere (SCV).
2. In the left navigation pane of SCV, select **Dashboard**.
3. When two or more vCenters are configured in linked mode, select the SCV plug-in instance and select **Job Monitor** tab.
   The Job Monitor tab lists each job and its status, start time, and end time. If the job names are long, you might need to scroll to the right to view the start and end times. The display is refreshed every 30 seconds.
   - Select the refresh icon in the toolbar to refresh the display on-demand.
   - Select the filter icon to choose the time range, type, tag, and status of jobs you want displayed. The filter is case sensitive.
   - Select the refresh icon in the Job Details window to refresh the display while the job is running.

If the Dashboard does not display job information, refer to KB article: SnapCenter vSphere client dashboard does not display jobs.

Download job logs

You can download the job logs from the Job Monitor tab on the Dashboard of the SnapCenter VMware vSphere client.

If you encounter unexpected behavior while using the VMware vSphere client, you can use the log files to identify the cause and resolve the problem.

> The default value for retaining job logs is 30 days; the default value for retaining jobs is 90 days. Job logs and jobs that are older than the configured retention are purged every six hours. You can use the Configuration `jobs/cleanup` REST APIs to modify how long jobs and job logs are retained. You cannot modify the purge schedule.

Steps

1. From the vCenter client shortcut page, select SnapCenter Plug-in for VMware vSphere (SCV).
2. In the left navigation pane of SCV, select **Dashboard** > **Job Monitor**.
3. Select the download icon in the Job Monitor title bar.

   You might need to scroll to the right to see the icon.

   You can also double-click a job to access the Job Details window and then select **Download Job Logs**.

Result

Job logs are located on the Linux VM host where the SnapCenter Plug-in for VMware vSphere is deployed. The default job log location is `/var/log/netapp`.

If you tried to download job logs but the log file named in the error message has been deleted, you might encounter the following error: `HTTP ERROR 500 Problem accessing /export-scv-logs`. To correct this error, check the file access status and permissions for the file named in the error message and correct the access problem.

Access reports

You can request reports for one or more jobs from the dashboard.

The Reports tab contains information on the jobs that are selected on the Jobs page in the Dashboard. If no jobs are selected, the Reports tab is blank.

Steps

1. From the vCenter client shortcut page, select SnapCenter Plug-in for VMware vSphere (SCV).
2. In the left navigation pane of SCV, select **Dashboard** > **Reports** tab.
3. For Backup Reports, you can do the following:
   a. Modify the report

      Select the filter icon to modify the time range, job status type, resource groups, and policies to be included in the report.

   b. Generate a detailed report

      Double-click any job to generate a detailed report for that job.
4. Optional: On the Reports tab, select **Download** and select the format (HTML or CSV).

   You can also select the download icon to download plug-in logs.

Types of reports from the VMware vSphere client

The VMware vSphere client for SnapCenter provides customizable report options that provide you with details about your data protection jobs and plug-in resource status. You can generate reports for primary protection only.

> Backup schedules are executed in the time zone in which 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 the vCenter are in different time zones, data in the VMware vSphere client Dashboard might not be the same as the data in the reports.

The Dashboard displays information on migrated backups only after backups post-migration are performed.

Report type	Description
Backup Report	Displays overview data about backup jobs. Select a section/status on the graph to see a list of jobs with that status on the **Reports** tab. For each job, the report lists the job ID, corresponding resource group, backup policy, start time and duration, status, and job details which includes the job name (snapshot name) if the job completed, and any warning or error messages. You can download the Report table in HTML or CSV format. You can also download the Job Monitor job logs for all the jobs (not just the jobs in the report). Deleted backups are not included in the report.
Mount Report	Displays overview data about mount jobs. Select a section/status on the graph to see a list of jobs with that status on the Reports tab. For each job, the report lists the job ID, job status, job name, and job start and end times. The job name includes the snapshot name. For example: `Mount Backup <snapshot-copy-name>` You can download the Report table in HTML or CSV format. You can also download the Job Monitor job logs for all the jobs (not just the jobs in the report).
Restore Report	Displays overview status information about restore jobs. Select a section/status on the graph to see a list of jobs with that status on the Reports tab. For each job, the report lists the job ID, job status, job name, and job start and end times. The job name includes the snapshot name. For example: `Restore Backup <snapshot-copy-name>` You can download the Report table in HTML or CSV format. You can also download the Job Monitor job logs for all the jobs (not just the jobs in the report).

Report type	Description
Last Protection Status of VMs or Datastores Report	Displays overview information about the protection status, during the configured number of days, for VMs and datastores managed by the SnapCenter Plug-in for VMware vSphere. The default is 7 days. To modify the value in the properties file, refer to Modify configuration default values. Select a section/status on the primary protection chart to see a list of VMs or datastores with that status on the **Reports** tab. The VM or Datastores Protection Status Report for protected VMs and datastores displays the names of VMs or datastores that have been backed up during the configured number of days, the latest snapshot name, and the start and end times for the latest backup run. The VM or Datastores Protection Status Report for unprotected VMs or datastores displays the names of VMs or datastores that do not have any successful backups during the configured number of days. You can download the Report table in HTML or CSV format. You can also download the Job Monitor job logs for all the jobs (not just the jobs in the report). This report is refreshed every hour when the plug-in cache is refreshed. Therefore, the report might not display VMs or datastores that were recently backed up.

Generate a support bundle from the SnapCenter Plug-in for VMware vSphere GUI

Before you begin

To log on to the SnapCenter Plug-in for VMware vSphere management GUI, you must know the IP address and the log in credentials. You must also note down the MFA token generated from the maintenance console.

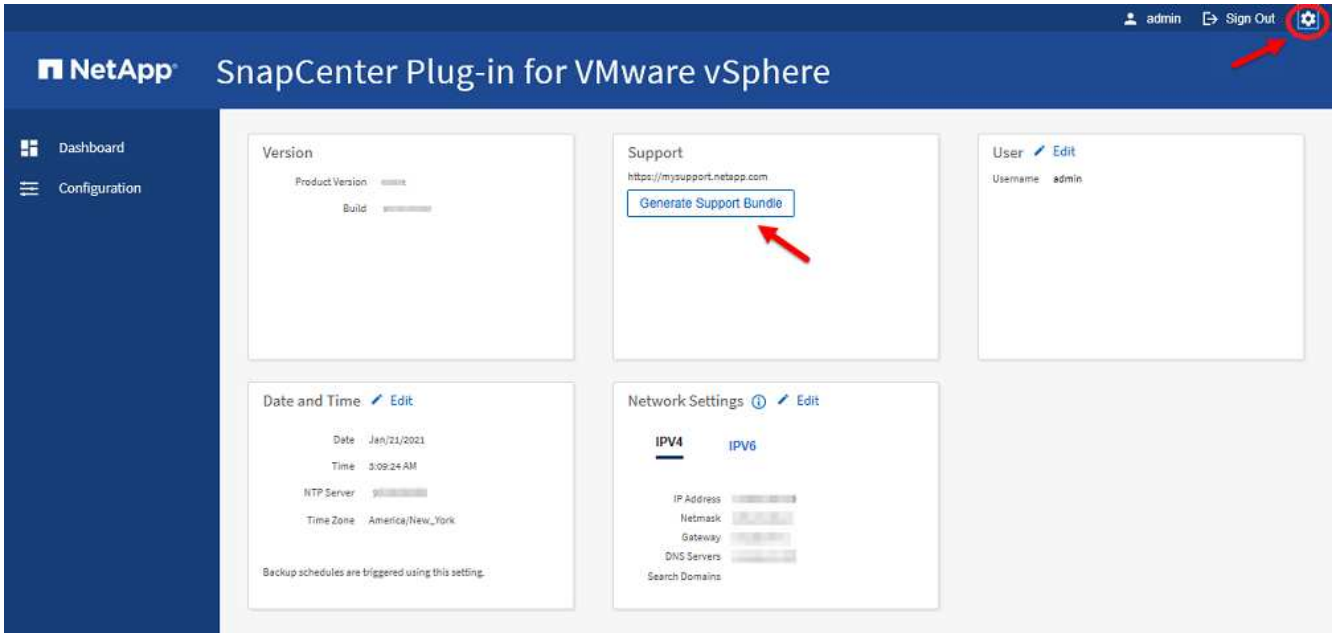
- The IP address was displayed when the SnapCenter Plug-in for VMware vSphere was deployed.
- Use the log in credentials provided during the deployment of the SnapCenter Plug-in for VMware vSphere or as later modified.
- Generate a 6-digit MFA token using the maintenance console System Configuration options.

Steps

1. Log in to the SnapCenter Plug-in for VMware vSphere GUI.

   Use the format `https://<OVA-IP-address>:8080`.

2. Select the Settings icon in the top toolbar.



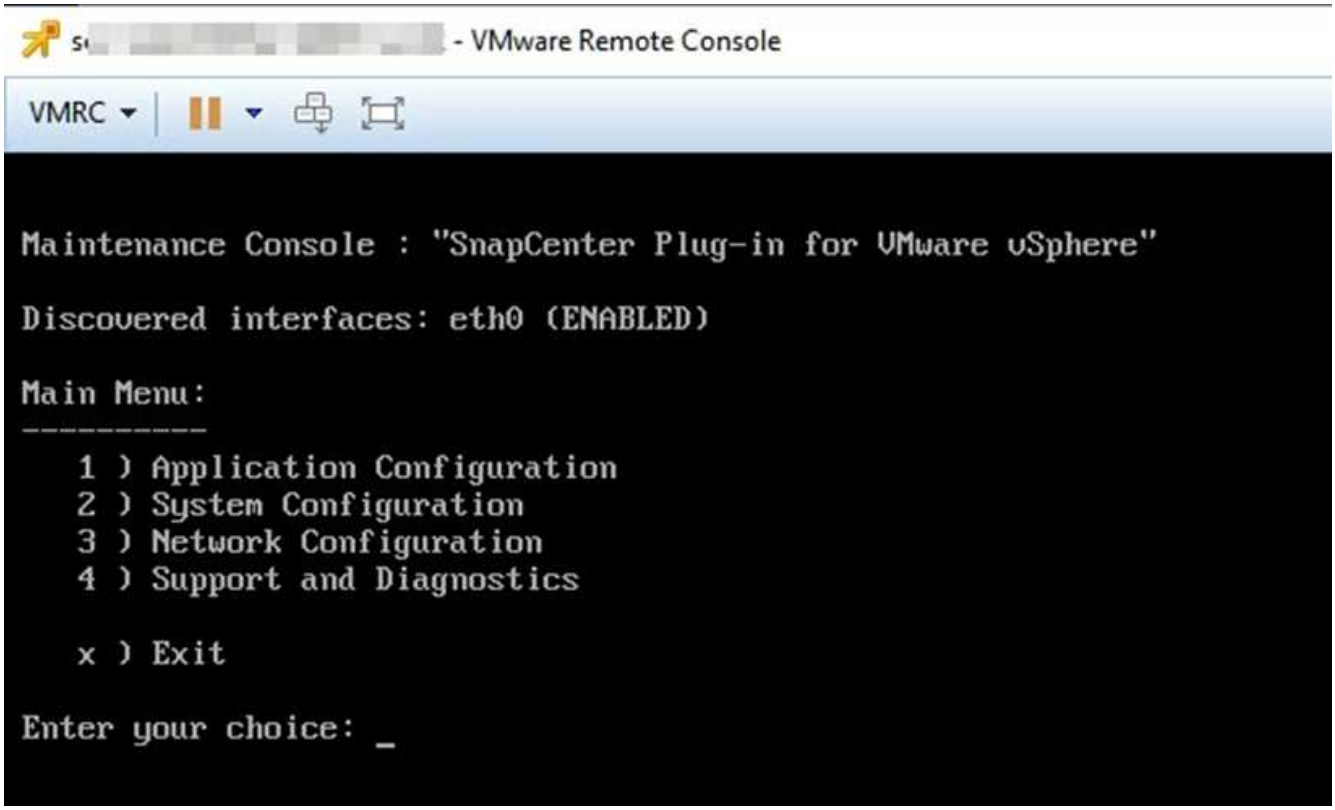
3. On the **Settings** page, in the **Support** section, select **Generate Support** Bundle.
4. After the support bundle is generated, select the link that is provided to download the bundle to NetApp.

Generate a support bundle from the maintenance console

Steps

1. From the VMware vSphere client, select the VM where the SnapCenter Plug-in for VMware vSphere is located.
2. In the **Summary** tab of the virtual appliance select **Launch Remote Console or Launch Web Console** to open a maintenance console window, and then log on.

   For information on accessing and logging on to the maintenance console, refer to Access the Maintenance Console.



3. From the Main Menu, enter option **4) Support and Diagnostics**.
4. From the Support and Diagnostics Menu, enter option **1) Generate support bundle**.

To access the support bundle, on the Support and Diagnostics Menu enter option **2) Access Diagnostic Shell**. In the console, navigate to `/support/support/<bundle_name>.tar.gz`.

Audit logs

An audit log is a collection of events in chronological order, which is written to a file within the appliance. The audit log files are generated at `/var/log/netapp/audit` location, and the file names follow one of the below naming conventions:

- audit.log: Active audit log file that is in use.
- audit-%d{yyyy-MM-dd-HH-mm-ss}.log.gz: Rolled over audit log file. The date and time in the file name indicates when the file was created, for example: audit-2022-12-15-16-28-01.log.gz.

In the SCV plug-in user interface, you can view and export the audit log details from **Dashboard** > **Settings** > **Audit Logs** Tab
You can view operation audit in the audit logs. The audit logs are downloaded with the Support bundle.

If Email settings are configured, SCV sends an Email notification in the event of an Audit Log Integrity Verification failure. An Audit Log Integrity Verification failure can happen when one of the files is tampered with or deleted.

The default configurations of the audit files are:

- Audit log file in use can grow to a maximum of 10 MB

- A maximum of 10 audit log files are retained

Rolled over audit logs are periodically verified for integrity. SCV provides REST APIs to view logs and verify their integrity. A built-in schedule triggers and assigns one of the following integrity statuses.

Status	Description
TAMPERED	Audit log file content is modified
NORMAL	Audit log file is unmodified
ROLLOVER DELETE	- Audit log file is deleted based on retention - By default, only 10 files are retained
UNEXPECTED DELETE	Audit log file is deleted
ACTIVE	- Audit log file is in use - Only applicable to audit.log

Events are categorize into three major categories:

- Data Protection Events
- Maintenance Console Events
- Admin Console Events

Data Protection Events

The resources in SCV are:

- Storage System
- Resource Group
- Policy
- Backup
- Subscription
- Account

The following table lists the operations that can be performed on each resource:

Resources	**Operations**
Storage System	Created, Modified, Deleted
Subscription	Created, Modified, Deleted
Account	Created, Modified, Deleted
Resource Group	Created, Modified, Deleted, Suspended, Resumed
Policy	Created, Modified, Deleted
Backup	Created, Renamed, Deleted, Mounted, Unmounted, Restored VMDK, Restored VM, Attach VMDK, Detach VMDK, Guest File Restore

Maintenance Console Events

The administrative operations in the maintenance console are audited.
Available maintenance console options are:

1. Start / Stop services
2. Change username & password
3. Change MySQL password
4. Configure MySQL Backup
5. Restore MySQL Backup
6. Change 'maint' user password
7. Change time zone
8. Change NTP Server
9. Disable SSH access
10. Increase jail disk size
11. Upgrade
12. Install VMware Tools (We are working on replace this with open-vm tools)
13. Change IP address settings
14. Change domain name search settings
15. Change static routes
16. Access diagnostic shell
17. Enable remote diagnostic access

Admin Console Events

The following operations in the Admin Console UI are audited:

- Settings
  - Change admin credentials
  - Change timezone
  - Change NTP Server
  - Change IPv4/IPv6 address settings
- Configuration
  - Change vCenter Credentials
  - Plug-in Enable / Disable

Configure syslog servers

Audit logs are stored within the appliance and are periodically verified for integrity. Event forwarding allows the you to obtain events from the source or forwarding computer and store it in a centralized computer, which is the Syslog Server. Data is encrypted in transit between the source and the destination.

Before you begin

You must have administrator privileges.

About this task

This task helps you to configure the syslog server.

Steps

1. Log in to the SnapCenter Plug-in for VMware vSphere.
2. In the left navigation pane, select **Settings** > **Audit Logs** > **Settings**.
3. In the **Audit Log Settings** pane, select **Send audit logs to Syslog server**
4. Enter the following details:
   - Syslog Server IP
   - Syslog Server Port
   - RFC format
   - Syslog Server Certificate
5. Select **SAVE** to save the Syslog server settings.

Change audit log settings

You can change the default configurations of the log settings.

Before you begin

You must have administrator privileges.

About this task

This task helps you to change the default audit log settings.

Steps

1. Log in to the SnapCenter Plug-in for VMware vSphere.
2. In the left navigation pane, select **Settings** > **Audit Logs** > **Settings**.
3. In the **Audit Log Settings** pane, enter the Maximum number of audit log files and Audit log file size limit.
4. Select **Send audit logs to Syslog server** option if you choose to send the logs to syslog server. Enter the details of the server.
5. Save the settings.

Manage storage

Add storage

Before you can backup or restore VMs, you must add storage clusters or storage VMs. Adding storage enables the SnapCenter Plug-in for VMware vSphere to recognize and manage backup and restore operations in vCenter.

- Which GUI to use

  Use the VMware vSphere client to add storage.

- Large LUNs

  SnapCenter Plug-in for VMware vSphere 4.5 and later supports datastores on large LUN sizes up to 128 TB on ASA aggregates. For large LUNs, SnapCenter only supports thick provisioned LUNs to avoid latency.

- VMware virtual volumes (vVols)

  You must add Storage Clusters to SnapCenter Plug-in for VMware vSphere and ONTAP tools for VMware vSphere for vVol DataProtection to work.

  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.

Before you begin

The ESXi server, the SnapCenter Plug-in for VMware vSphere, and each vCenter must be synchronized to the same time. If you try to add storage but the time settings for your vCenters are not synchronized, the operation might fail with a Java certificate error.

About this task

SnapCenter Plug-in for VMware vSphere performs backup and restore operations on directly connected storage VMs and on storage VMs in a storage cluster.

> If you are using the SnapCenter Plug-in for VMware vSphere to support application-based backups on VMDKs, then you must use the SnapCenter GUI to enter storage authentication details and register storage systems.

- For vCenters in linked mode, you must separately add storage systems to each vCenter.
- If you are adding SVM, names for storage VMs must resolve to management LIFs.

  If you have added entries to the *etc\hosts* file for storage VM names in SnapCenter, you must ensure that these are also resolvable from the virtual appliance. If they are not, you should add similar entries to the *etc/hosts* file within the appliance.

  If you add a storage VM with a name that cannot resolve to the management LIF, then scheduled backup jobs fail because the plug-in is unable to discover any datastores or volumes on that storage VM. If this occurs, either add the storage VM to SnapCenter and specify the management LIF or add a cluster that contains the storage VM and specify the cluster management LIF.

- Storage authentication details are not shared between multiple instances of the SnapCenter Plug-in for VMware vSphere or between Windows SnapCenter Server and the SnapCenter plug-in on vCenter.

Steps

1. From the vCenter client shortcut page, select SnapCenter Plug-in for VMware vSphere (SCV).
2. In the left navigation pane of SCV, select **Dashboard** > **Storage Systems**.
3. On the Storage Systems page, select **Add** option.
4. In the **Add Storage System** wizard, enter the basic storage VM or cluster information as listed in the following table:

For this field…	Do this…
Storage system	Enter the FQDN or Management LIF's IP address of a storage cluster or a storage VM. SnapCenter Plug-in for VMware vSphere does not support multiple storage VM's with the same name on different clusters.
Authentication Method	Select either Credentials or Certificate. Two types of certificates are supported: - Self signed certificate - CA signed certificate.
Username	This field is visible when you select Credentials as your authentication method. Enter the ONTAP username that is used to log on to the storage VM or the cluster.
Password	This field is visible when you select Credentials as your authentication method. Enter the storage VM or cluster login password.
Certificate	This field is visible when you select Certificate as your authentication method. Browse to select the certificate file.
Private Key	This field is visible when you select Certificate as your authentication method. Browse to select the private Key file.
Protocol	Select storage protocol.
Port	Port that the storage system accepts. - 443 for HTTPS connection - 80 for HTTP connection
Timeout	Enter the number of seconds SnapCenter Plug-in for VMware vSphere should wait before timing out the operation. The default is 60 seconds.
Preferred IP address	If the storage VM has more than one management IP address, check this box and enter the IP address that you want SnapCenter Plug-in for VMware vSphere to use. **Note:** Do not use square brackets ([]) when entering the IP address.

For this field…	Do this…
Event Management System(EMS) & AutoSupport Setting	If you want to send EMS messages to the storage system syslog or if you want to have AutoSupport messages sent to the storage system for applied protection, completed restore operations, or failed operations, select the appropriate checkbox. Select the **Send AutoSupport Notification for failed operations to storage system** checkbox and the **Log SnapCenter Server events to syslog** checkbox to enable AutoSupport notifications.
Log SnapCenter Server events to syslog	Check the box to log events for the SnapCenter Plug-in for VMware vSphere.
Send AutoSupport Notification for failed operation to storage system	Check the box if you want AutoSupport notification for failed data protection jobs. You must also enable AutoSupport on the storage VM and configure the AutoSupport email settings.

5. Select **Add**.

   If you added a storage cluster, all storage VMs in that cluster are automatically added. Automatically added storage VMs (sometimes called “implicit” storage VMs) are displayed on the cluster summary page with a hyphen (-) instead of a username. Usernames are displayed only for explicit storage entities.

Manage storage systems

Before you can back up or restore VMs or datastores using the VMware vSphere client, you must add the storage.

Modify storage VMs

You can use the VMware vSphere client to modify the configurations of clusters and storage VMs that are registered in SnapCenter Plug-in for VMware vSphere and used for VM data protection operations.

If you modify a storage VM that was automatically added as part of a cluster (sometimes called an implicit storage VM), then that storage VM changes to an explicit storage VM and can be separately deleted without changing the rest of the storage VMs in that cluster. On the Storage Systems page, the username is displayed as N/A when the authentication method is through the certificate; usernames are displayed only for explicit storage VMs in the cluster list and have the ExplicitSVM flag set to true. All storage VMs are always listed under the associated cluster.

If you added storage VMs for application-based data protection operations using the SnapCenter GUI, you must use the same GUI to modify those storage VMs.

Steps

1. In the left navigator pane of the SCV plug-in, select **Storage Systems**.
2. On the **Storage Systems** page, select the storage VM to be modified and then select **Edit**.
3. On the **Edit Storage System** window, enter the new values, and then select **Update** to apply the changes.

Remove storage VMs

You can use the VMware vSphere client to remove storage VMs from the inventory in vCenter.

If you added storage VMs for application-based data protection operations using the SnapCenter GUI, you must use the same GUI to modify those storage VMs.

Before you begin

You must unmount all datastores in the storage VM before you can remove the storage VM.

About this task

If a resource group has backups that reside on a storage VM that you remove, then subsequent backups for that resource group fail.

Steps

1. In the left navigator pane of the SCV plug-in, select **Storage Systems**.
2. On the **Storage Systems** page, select the storage VM to be removed and then select **Delete**.
3. In the **Remove Storage System** confirmation box, check the box for **Delete storage system(s)** and then select **Yes** to confirm.
   Note: Only ESXi host 7.0U1 and later releases are supported.

   Restart the VMware vSphere client service.

Modify the configured storage timeout

Even though backups have run successfully in the past, they might start failing during the time that the SnapCenter Plug-in for VMware vSphere must wait for the storage system to exceed the configured timeout period. If this condition occurs, you can increase the configured timeout.

You might encounter the error `Unable to discover resources on SCV: Unable to get storage details for datastore <xxx>…`

Steps

1. In the left navigator pane of the SCV plug-in, select **Storage Systems**.
2. On the Storage Systems page, select the storage system to be modified and select **Edit**.
3. In the Timeout field, increase the number of seconds.

   180 seconds is recommended for large environments.

Protect data

Data protection workflow

Use the SnapCenter vSphere client to perform data protection operations for VMs, VMDKs, and datastores. All backup operations are performed on resource groups, which can contain any combination of one or more VMs and datastores. You can back up on demand or according to a defined protection schedule.

When you back up a datastore, you are backing up all the VMs in that datastore.

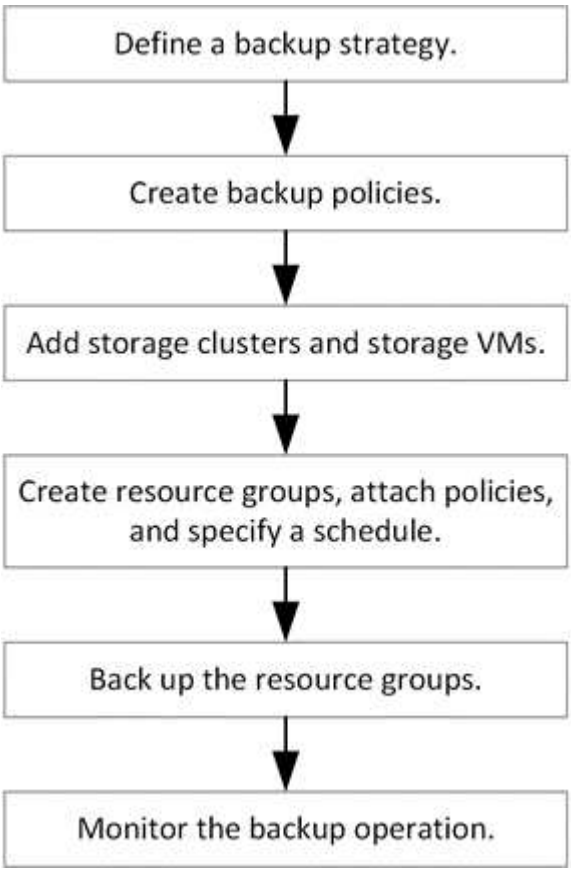
Backup and restore operations cannot be performed simultaneously on the same resource group.

You should review the information on what the SnapCenter Plug-in for VMware vSphere does and does not support.
Deployment planning and requirements

In MetroCluster configurations:

- SnapCenter Plug-in for VMware vSphere might not be able to detect a protection relationship after a failover. Refer to KB article: Unable to detect SnapMirror or SnapVault relationship after MetroCluster failover for more information.
- If backups fail with the error `Unable to discover resources on SCV: <xxx>...` for NFS and VMFS VMs after switchover/switch back, restart the SnapCenter VMware services from the maintenance console.

The following workflow figure shows the sequence in which you must perform backup operations:



View VM and datastore backups

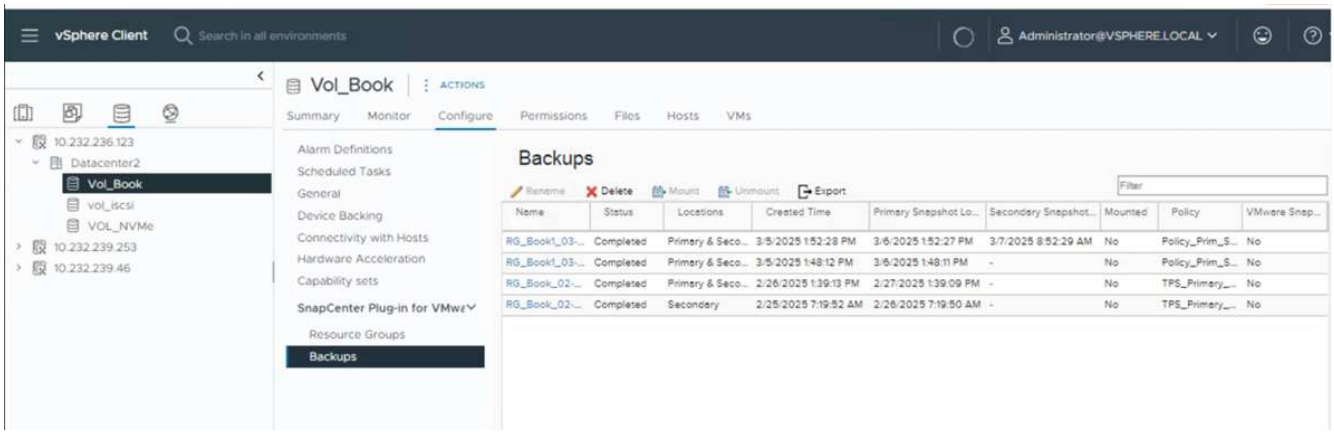
When preparing to back up or restore a VM or datastore, you might want to see all the backups available for that resource and view the details of those backups.

About this task

Browsing large file folders, such as 10k file folders, might take one or more minutes the first time. Subsequent browsing sessions take less time.

Steps

1. Log in to the vCenter Server.
2. Navigate to the **Inventory** page and select a datastore or a VM.
3. In the right pane, select **Configure** > **SnapCenter Plug-in for VMware vSphere** > **Backups**.



If the **Enable Secondary Snapshot Locking** option is not selected during the policy creation stage, it takes the value set for the **Enable Primary Snapshot Locking** option by default. In the backups list, the hyphen in the **Secondary Snapshot Lock Expiration** field indicates that both primary and secondary locking periods are the same.

4. Select the backup that you want to view.

Create backup policies for VMs and datastores

You must create backup policies before you use the SnapCenter Plug-in for VMware vSphere to back up VMs and datastores.

Before you begin

- You must have read the prerequisites.
- You must have secondary storage relationships configured.
  - If you are replicating snapshots to a mirror or vault secondary storage, the relationships must be configured and the SnapCenter administrator must have assigned the storage VMs to you for both the source and destination volumes.
  - To successfully transfer snapshots to secondary storage for Version-FlexibleMirror relationships on a NFS or VMFS datastore, make sure that the SnapMirror policy type is Asynchronous Mirror and that the "all_source_snapshots" option is checked.

- When the number of snapshots on the secondary storage (mirror-vault) reaches the maximum limit, the activity to register backup and apply retention in the backup operation fails with the following error: `This snapshot is currently used as a reference snapshot by one or more SnapMirror relationships. Deleting the snapshot can cause future SnapMirror operations to fail.`

  To correct this issue, configure the SnapMirror retention policy for secondary storage to avoid reaching the maximum limit of snapshots.

  For information about how administrators assign resources to users, refer to SnapCenter information on using role-based access control.

- If you want VM-consistent backups, you must have VMware tools installed and running. VMware tools is needed to quiesce VMs. VM-consistent backups are not supported for vVol VMs.
- SnapMirror active sync enables business services to continue operating even through a complete site failure, supporting applications to fail over transparently using a secondary copy.

  SnapMirror active sync is supported only for VMFS Datastores.

  To protect a VMFS datastore on a SnapMirror active sync deployment, as SnapCenter administrator you need to:

  - Configure clusters and mediator as described in the technical report: Configure the ONTAP Mediator and clusters for SnapMirror active sync.
  - Add the volume associated with the VMFS datastore to the consistency group and create a data protection relationship using *AutomatedFailOver* or *AutomatedFailOverDuplex* protection policy between two ONTAP storage systems. *AutomatedFailOverDuplex* policy is supported from ONTAP 9.15.1 release onwards.

In fan-out configuration, consistency group is not supported for tertiary site.

About this task

Most of the fields on these wizard pages are self-explanatory. The following information describes some of the fields for which you might require guidance.

Steps

1. In the left navigator pane of the SCV plug-in, select **Policies**.
2. On the **Policies** page, select **Create** to start the wizard.
3. On the **New Backup Policy** page enter the policy name and a description.
   - Linked mode

     In linked mode, each vCenter has a separate virtual appliance. Therefore, you can use duplicate names across vCenters. However, you must create the policy in the same vCenter as the resource group.

   - Unsupported characters

     Do not use the following special characters in VM, datastore, cluster, policy, backup, or resource group names: % & * $ # @ ! \ / : * ? " < > - | ; ' , and space.

     An underscore character (_) is allowed.

4. Specify the frequency settings.

   The policy specifies the backup frequency only. The specific protection schedule for backing up is defined in the resource group. Therefore, two or more resource groups can share the same policy and backup frequency but have different backup schedules.

5. Select **Locking Period** checkbox to enable snapshot locking. You can select the primary and secondary snapshot locking periods as Days/Months/Years.

   Irrespective of the retention value set in the ONTAP SnapMirror policy, the secondary snapshot copy is not deleted before the specified secondary snapshot locking period.

6. Specify the retention settings.

   You should set the retention count to 2 backups or higher if you plan to enable SnapVault replication. If you set the retention count to 1 backup to keep, the retention operation can fail. This is because the first snapshot is the reference snapshot for the SnapVault relationship until the newer snapshot is replicated to the target.

   The maximum retention value is 1018 backups. Backups will fail if retention is set to a value higher than what the underlying ONTAP version supports. This is also true for spanning datastores.

1. In the **Replication** fields, specify the type of replication to secondary storage, as shown in the following table:

For this field…	Do this…
Update SnapMirror after backup	Select this option to create mirror copies of backup sets on another volume that has a SnapMirror relationship to the primary backup volume. If a volume is configured with a mirror-vault relationship, you must select only the **Update SnapVault after backup** option if you want backups copied to the mirror-vault destinations. This option is supported for datastores in FlexGroup volumes in SnapCenter Plug-in for VMware vSphere 4.5 and later. To protect VMFS datastore on SnapMirror active sync deployment, you need to complete the prerequisites mentioned in the *Before you begin* section and enable **Update SnapMirror after backup**.

For this field…	Do this…
Update SnapVault after backup	Select this option to perform disk-to-disk backup replication on another volume that has a SnapVault relationship to the primary backup volume. If a volume is configured with a mirror-vault relationship, you must select only this option if you want backups copied to the mirror-vault destinations. This option is supported for datastores in FlexGroup volumes in SnapCenter Plug-in for VMware vSphere 4.5 and later.
Snapshot label	Enter an optional, custom label to be added to SnapVault and SnapMirror snapshots created with this policy. The snapshot label helps to distinguish snapshots created with this policy from other snapshots on the secondary storage system. A maximum of 31 characters is allowed for snapshot labels.

2. Optional: In the **Advanced** fields, select the fields that are needed. The Advanced field details are listed in the following table.

For this field…	Do this…
VM consistency	Check this box to quiesce the VMs and create a VMware snapshot each time the backup job runs. This option is not supported for vVols. For vVol VMs, only crash-consistent backups are performed. You must have VMware tools running on the VM to perform VM consistent backups. If VMware tools is not running, a crash-consistent backup is performed instead. When you check the VM consistency box, backup operations might take longer and require more storage space. In this scenario, the VMs are first quiesced, then VMware performs a VM consistent snapshot, then SnapCenter performs its backup operation, and then VM operations are resumed. VM guest memory is not included in VM consistency snapshots.
Include datastores with independent disks	Check this box to include in the backup any datastores with independent disks that contain temporary data.
Scripts	Enter the fully qualified path of the prescript or postscript that you want the SnapCenter Plug-in for VMware vSphere to run before or after backup operations. For example, you can run a script to update SNMP traps, automate alerts, and send logs. The script path is validated at the time the script is executed. Prescripts and postscripts must be located on the virtual appliance VM. To enter multiple scripts, press **Enter** after each script path to list each script on a separate line. The character ";" is not allowed.

3. Select **Add.**

   You can verify that the policy is created and review the policy configuration by selecting the policy in the Policies page.

Create resource groups

A resource group is the container for VMs, datastores, vSphere Tags, and vSphere VM Folders that you want to protect.

A resource group can contain the following:

- Traditional VMs and datastores

  Any combination of traditional VMs, traditional SAN datastores, and traditional NAS datastores. Traditional VMs cannot be combined with vVol VMs.

- Flexgroup datastores

  A single FlexGroup datastore. Spanning Flexgroup datastores are not supported. A FlexGroup datastore cannot be combined with traditional VMs or datastores.

- FlexVol datastores

  One or more FlexVol datastores. Spanning datastores are supported.

- vVol VMs

  One or more vVol VMs. vVol VMs cannot be combined with traditional VMs or datastores.

- vSphere tag

  All VMs and Datastores, excluding vVol Datastores, that have the specified vSphere tag.

- vVol VMs in a folder

  All vVols in a single, specified vVol folder. If the folder contains a mix of vVol VMs and traditional VMs, SnapCenter Plug-in for VMware vSphere backs up the vVol VMs and skips the traditional VMs.

- VMs and datastores on ASA r2

  You cannot combine ASA r2 VMs and datastores with other VMs and datastores.

For all resource groups:

If you are using VMware vSphere Cluster Service (vCLS), do not include VMs managed by vCLS in SnapCenter Plug-in for VMware vSphere resource groups.

For more information, refer to SCV unable to backup vCLS VMs after updating vCenter to 7.0.x

SnapCenter Plug-in for VMware vSphere 4.5 and later supports datastores on large LUNs and files up to 128 TB with volumes up to 300 TB. If you are protecting large LUNs, use only thick provisioned LUNs to avoid latency.

Do not add VMs that are in an inaccessible state. Although it is possible to create a resource group that contains inaccessible VMs, backups for that resource group will fail.

Before you begin

ONTAP tools for VMware must be deployed before you create a resource group that contains vVol VMs.

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.

About this task

You can add or remove resources from a resource group at any time.

- Backing up a single resource

  To back up a single resource (for example, a single VM), you must create a resource group that contains that single resource.

- Backing up multiple resources

  To back up multiple resources, you must create a resource group that contains multiple resources.

- Resource groups that contain FlexGroup volumes in MetroCluster environments

  If you are running on ONTAP 9.8 or ONTAP 9.9, then after a switchover or switchback, you must restart the SnapCenter Plug-in for VMware vSphere service and resynchronize the SnapMirror relationships before you back up resource groups in MetroCluster environments.

  In ONTAP 9.8, the backups hang after the switchback. This issue is fixed in ONTAP 9.9.

- Optimizing snapshots

  To optimize snapshots, you should group the VMs and datastores that are associated with the same volume into one resource group.

- Backup policies

  While you can create a resource group without a backup policy, data protection operations are only possible when at least one policy is attached to the resource group. You have the option to use an existing policy or create a new one during the resource group creation process.

  > If you are selecting a backup policy with snapshot locking period, you need to select ONTAP 9.12.1 or later version.

- Compatibility checks

  SnapCenter performs compatibility checks when you create a resource group.

  Manage compatibility check failures

- Create secondary protection for a resource group

  Secondary protection takes care of creating replication relationship for the resources added in resource group. You need to create a consistency group-based SnapMirror relationship in the preferred cluster and SVM using a specified policy from the primary. The secondary protection is supported only for ASA r2 system based datastore and virtual machines. The cluster peering and SVM peering should be pre-configured. Secondary protection only allows asynchronous SnapMirror policies. You need to provide consistency group suffix when creating the secondary protection.

Secondary protection takes care of creating replication relationship for the resources added in resource group.

Steps

1. In the left navigator pane of the SCV plug-in, select **Resource Groups**, then select **Create** to start the wizard.

This is the easiest way to create a resource group. However, you can also create a resource group with one resource by performing one of the following:

- To create a resource group for one VM, on the shortcuts page, select **Hosts and Clusters**, then right-click a VM, select **SnapCenter Plug-in for VMware vSphere** > **Create Resource Group**.
- To create a resource group for one datastore, on the shortcuts page, select **Hosts and Clusters**, then right-click a datastore, select **SnapCenter Plug-in for VMware vSphere** > **Create Resource Group**.
  1. On the **General Info & Notification** page in the wizard, do the following:

For this field…	Do this…
vCenter Server	Select a vCenter server.
Name	Enter a name for the resource group. Do not use the following special characters in VM, datastore, policy, backup, or resource group names: % & * $ # @ ! \ / : * ? " < > - [vertical bar] ; ' , and space. An underscore character (_) is allowed. VM or datastore names with special characters are truncated, which makes it difficult to search for a specific backup. In linked mode, each vCenter has a separate SnapCenter Plug-in for VMware vSphere repository. Therefore, you can use duplicate names across vCenters.
Description	Enter a description of the resource group.
Notification	Select when you want to receive notifications about operations on this resource group: Error or warnings: Send notification for errors and warnings only Errors: Send notification for errors only Always: Send notification for all message types Never: Do not send notification
Email send from	Enter the email address you want the notification sent from.
Email send to	Enter the email address of the person you want to receive the notification. For multiple recipients, use a comma to separate the email addresses.
Email subject	Enter the subject you want for the notification emails.

For this field…	Do this…
Latest snapshot name	If you want the suffix "_recent" added to the latest snapshot, then check this box. The "_recent" suffix replaces the date and timestamp. A `_recent` backup is created for each policy that is attached to a resource group. Therefore, a resource group with multiple policies will have multiple `_recent` backups. Do not manually rename `_recent` backups. ASA r2 storage system does not support renaming of snapshots and as a result SCV's rename backup and _recent snapshot naming features are not supported.
Custom snapshot format	If you want to use a custom format for the snapshot names, then check this box and enter the name format. • By default, this feature is disabled. • The default snapshot names use the format `<ResourceGroup>_<Date-TimeStamp>` However, you can specify a custom format using the variables $ResourceGroup, $Policy, $HostName, $ScheduleType, and $CustomText. Use the drop-down list in the custom name field to select which variables you want to use and the order in which they are used. If you select $CustomText, the name format is `<CustomName>_<Date-TimeStamp>`. Enter the custom text in the additional box that is provided. [NOTE]: If you also select the "_recent" suffix, you must make sure that the custom snapshot names will be unique in the datastore, therefore, you should add the $ResourceGroup and $Policy variables to the name. • Special characters For special characters in names, follow the same guidelines given for the Name field.

2. On the **Resources** page, do the following:

For this field…	Do this…
Scope	Select the type of resource you want to protect: * Datastores (all traditional VMs in one or more specified datastores). You cannot select a vVol datastore. * Virtual Machines (individual traditional or vVol VMs; in the field you must navigate to the datastore that contains the VMs or vVol VMs). You cannot select individual VMs in a FlexGroup datastore. * Tags Tag-based datastore protection is supported only for NFS and VMFS datastores, as well as for virtual machines and vVol Virtual Machines. * VM Folder (all vVol VMs in a specified folder; in the popup field you must navigate to the datacenter in which the folder is located)
Datacenter	Navigate to the VMs or datastores or folder that you want to add. VM and Datastore names in a resource group must be unique.
Available entities	Select the resources you want to protect, then select **>** to move your selections to the Selected entities list.

When you select **Next**, the system first checks that SnapCenter manages and is compatible with the storage on which the selected resources are located.

If the message `Selected <resource-name> is not SnapCenter compatible` is displayed, then a selected resource is not compatible with SnapCenter.

To globally exclude one or more datastores from backups, you must specify the datastore name(s) in the `global.ds.exclusion.pattern` property in the `scbr.override` configuration file. Refer to Properties you can override.

3. On the **Spanning disks** page, select an option for VMs with multiple VMDKs across multiple datastores:
   - Always exclude all spanning datastores (This is the default for datastores.)
   - Always include all spanning datastores (This is the default for VMs.)
   - Manually select the spanning datastores to be included

     Spanning VMs are not supported for FlexGroup and vVol datastores.
4. On the **Policies** page, select or create one or more backup policies, as shown in the following table:

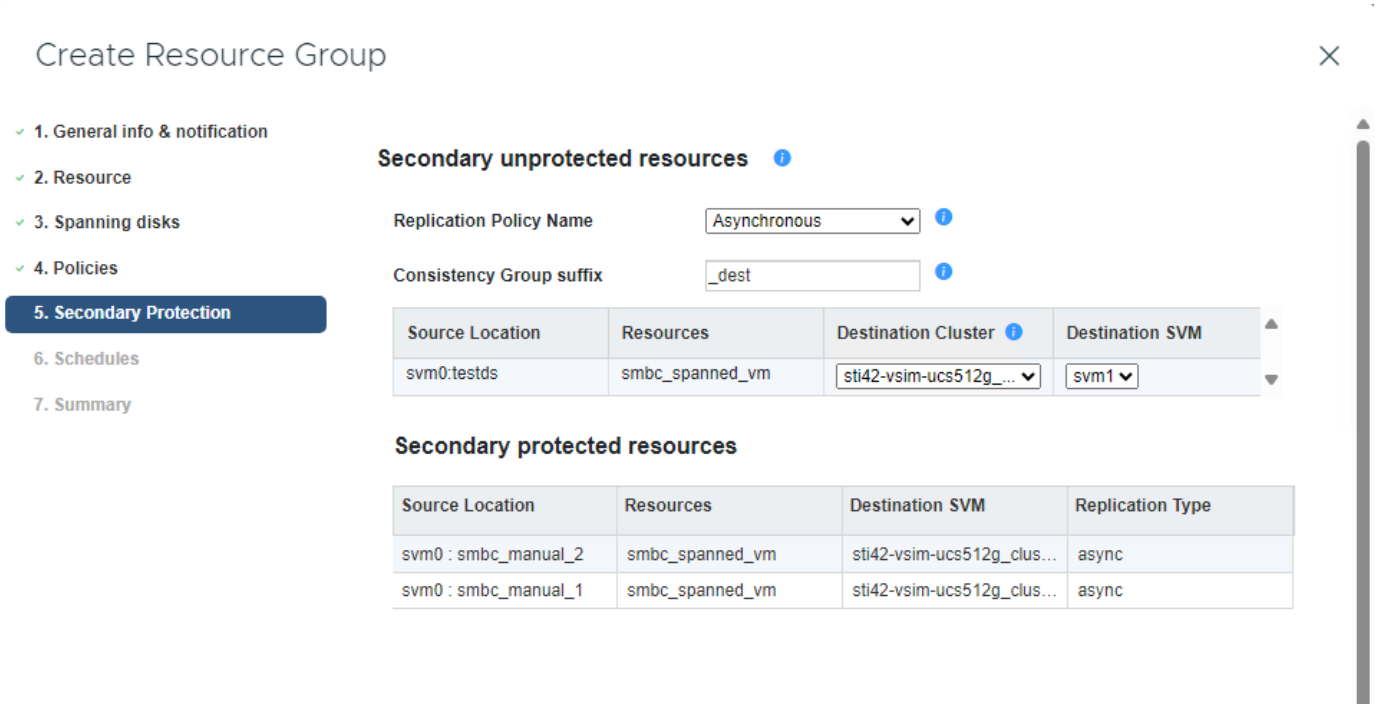
To use…	Do this…
An existing policy	Select one or more policies from the list. Secondary protection is applicable to existing and new policies where you have selected both SnapMirror and SnapVault updates.

To use…	Do this…
A new policy	1. Select **Create**. 2. Complete the New Backup Policy wizard to return to the Create Resource Group wizard.

In Linked Mode, the list includes policies in all the linked vCenters. You must select a policy that is on the same vCenter as the resource group.

5. On the **Secondary protection** page, the list of selected resources are displayed with their protection status. To protect the unprotected resources, select the replication policy type, consistency group suffix, destination cluster, and destination SVM from the dropdown. On creation of resource group a separate job is created for secondary protection and you can see it it in job monitor window.

Fields	Description
Replication policy name	Name of the SnapMirror policy. Only **Asynchronous** and **Mirror and Vault** secondary policies are supported.
Consistency group suffix	A destination setting used to append to the primary consistency group to form the destination consistency group name. For example: If the primary consistency group name is sccg_2024-11-28_120918 and you enter _dest as suffix then secondary consistency group will be created as sccg_2024-11-28_120918_dest. The suffix is applicable only for unprotected consistency groups.
Destination cluster	For all unprotected storage units, SCV displays peered cluster(s) names in the dropdown. If the storage added to SCV is in SVM scope, then due to ONTAP limitation, the cluster ID is displayed instead of the name.
Destination SVM	For all unprotected storage units, SCV displays Peered SVM(s) names. Cluster and SVM is automatically chosen when one of the storage units that is part of the consistency group is selected. The same is applied to all the other storage units in the same consistency group.
Secondary protected resources	For all the protected storage units of the resources that are added in the resources page, the secondary relationship details including cluster, SVM, and replication type are displayed.



1. On the **Schedules** page, configure the backup schedule for each selected policy.

   In the starting hour field, enter a date and time other than zero. The date must be in the format `day/month/year`.

   When you select a number of days in Every field, then backups are performed on day 1 of the month, and thereafter at every interval that is specified. For example, if you select the option **Every 2 days**, then backups are performed on day 1, 3, 5, 7, and so on throughout the month, regardless of whether the starting date is even or odd.

   You must fill in each field. SnapCenter Plug-in for VMware vSphere creates schedules in the time zone in which the SnapCenter Plug-in for VMware vSphere is deployed. You can modify the time zone by using the SnapCenter Plug-in for VMware vSphere GUI.

   Modify the time zones for backups.

2. Review the summary and then select **Finish**. Beginning with SCV 6.1 secondary protection for ASA r2 systems resources are visible in the summary page.

   Before you select **Finish**, you can go back to any page in the wizard and change the information.

   After you select **Finish**, the new resource group is added to the resource groups list.

   If the quiesce operation fails for any of the VMs in the backup, then the backup is marked as not VM- consistent even if the policy selected has VM consistency selected. In this case, it is possible that some of the VMs were successfully quiesced.

Manage compatibility check failures

SnapCenter performs compatibility checks when you attempt to create a resource group.
Always refer to NetApp Interoperability Matrix Tool (IMT) for the latest information about SnapCenter support.
Reasons for incompatibility might be:

- A shared PCI device is attached to a VM.
- The preferred IP address is not configured in SnapCenter.
- You have not added the storage VM (SVM) management IP address to SnapCenter.
- The storage VM is down.

To correct a compatibility error, perform the following:

1. Make sure the storage VM is running.
2. Make sure that the storage system on which the VMs are located has been added to the SnapCenter Plug-in for VMware vSphere inventory.
3. Make sure the storage VM is added to SnapCenter. Use the Add storage system option on the VMware vSphere client GUI.
4. If there are spanning VMs that have VMDKs on both NetApp and non-NetApp datastores, then move the VMDKs to NetApp datastores.

Prescripts and postscripts

You can use custom prescripts and postscripts as part of your data protection operations. These scripts enable automation either before your data protection job or after. For example, you might include a script that automatically notifies you of data protection job failures or warnings. Before you set up your prescripts and postscripts, you should understand some of the requirements for creating these scripts.

Supported script types

Perl and shell scripts are supported.
Shell scripts must start with `!/bin/bash`. (`!/bin/sh` is not supported.)

Script path location

Prescripts and postscripts are run by the SnapCenter Plug-in for VMware vSphere. Therefore, the scripts must be located in the SnapCenter Plug-in for VMware vSphere OVA, with executable permissions.

For example:
* A PERL script path might be `/support/support/script.pl`
* A shell script path might be `/support/support/script.sh`

The script path is validated at the time the script is executed.

Where to specify scripts

Scripts are specified in backup policies. When a backup job is started, the policy automatically associates the script with the resources being backed up.

To specify multiple scripts, press **Enter** after each script path to list each script on a separate line. Semicolons (;) are not allowed. You can specify multiple prescripts and multiple postscripts. A single script can be coded as both a prescript and a postscript and can call other scripts.

When scripts are executed

Scripts are executed according to the value set for BACKUP_PHASE.

- BACKUP_PHASE=PRE_BACKUP

  Prescripts are executed in the PRE_BACKUP phase of the operation.

  If a prescript fails, the backup completes successfully, and a warning message is sent.

- BACKUP_PHASE=POST_BACKUP or BACKUP_PHASE=FAILED_BACKUP

  Postscripts are executed in the POST_BACKUP phase of the operation after the backup completes successfully or in the FAILED_BACKUP phase if the backup does not complete successfully.

  If a postscript fails, the backup completes successfully, and a warning message is sent.

Check the following to verify that the script values are populated:
* For PERL scripts: `/support/support/log_env.log`
* For shell scripts: `/support/support/log_file.log`

Environment variables passed to scripts

You can use the environment variables shown in the following table in scripts.

Environment variable	Description
`BACKUP_NAME`	Name of the backup. Variable passed in postscripts only.
`BACKUP_DATE`	Date of the backup, in the format `yyyymmdd` Variable passed in postscripts only.
`BACKUP_TIME`	Time of the backup, in the format `hhmmss` Variable passed in postscripts only.
`BACKUP_PHASE`	The phase of the backup in which you want the script to run. Valid values are: `PRE_BACKUP, POST_BACKUP, and FAILED_BACKUP`. Variable passed in prescripts and postscripts.
`STORAGE_SNAPSHOTS`	The number of storage snapshots in the backup. Variable passed in postscripts only.
`STORAGE_SNAPSHOT.#`	One of the defined storage snapshots, in the following format: `<filer>:/vol/<volume>:<ONTAP-snapshot-name>` Variable passed in postscripts only.
`VIRTUAL_MACHINES`	The number of VMs in the backup. Variable passed in prescripts and postscripts.

Environment variable	Description
VIRTUAL_MACHINE.#	One of the defined virtual machines, in the following format: <VM name>[vertical bar]<VM UUID>[vertical bar]<power-state>[vertical bar]<VM snapshot>[vertical bar]<ip-addresses> <power-state> has the values POWERED_ON, POWERED_OFF, or SUSPENDED <VM snapshot> has the values true or false Variable passed in prescripts and postscripts.

Script timeouts

The timeout for backup scripts is 15 minutes and cannot be modified.

Example PERL script #1

The following example PERL script prints the environmental variables when a backup is run.

```
#!/usr/bin/perl
use warnings;
use strict;
my $argnum;
my $logfile = '/support/support/log_env.log';
open (FH, '>>', $logfile) or die $!;
foreach (sort keys %ENV) {
print FH "$_ = $ENV{$_}\n";
}
print FH "=========\n";
close (FH);
```

Example PERL script #2

The following example prints information about the backup.

```
#!/usr/bin/perl
use warnings;
use strict;

my $argnum;
my $logfile = '/support/support/log_env.log';
open (FH, '>>', $logfile) or die $!;

print FH "BACKUP_PHASE is $ENV{'BACKUP_PHASE'}\n";
print FH "Backup name $ENV{'BACKUP_NAME'}\n";
print FH "Virtual Machine $ENV{'VIRTUAL_MACHINES'}\n";
print FH "VIRTUAL_MACHINE # is $ENV{'VIRTUAL_MACHINE.1'}\n";
print FH "BACKUP_DATE is $ENV{'BACKUP_DATE'}\n";
print FH "BACKUP_TIME is $ENV{'BACKUP_TIME'}\n";
```

```
print FH "STORAGE_SNAPSHOTS is $ENV{'STORAGE_SNAPSHOTS'}\n";
print FH "STORAGE_SNAPSHOT # is $ENV{'STORAGE_SNAPSHOT.1'}\n";

print FH "PWD is $ENV{'PWD'}\n";
print FH "INVOCATION_ID is $ENV{'INVOCATION_ID'}\n";

print FH "=========\n";
close (FH);
```

Example shell script

```
===============================================
#!/bin/bash
echo Stage $BACKUP_NAME >> /support/support/log_file.log
env >> /support/support/log_file.log
===============================================
```

Add a single VM or datastore to a resource group

You can quickly add a single VM or datastore to any existing resource group managed by SnapCenter Plug-in for VMware vSphere.

About this task

You can add SAN and NAS datastores but not VSAN or VVOL datastores.

Steps

1. In the vSphere client GUI, select **Menu** in the toolbar, and navigate to the VM or datastore that you want to add.
2. In the left navigator pane, right-click on the VM or datastore, select **SnapCenter Plug-in for VMware vSphere** > **Add To Resource Group** from the secondary drop-down list.

   The system first checks that SnapCenter manages and is compatible with the storage system on which the selected VM is located and then displays the **Add to Resource Group** page. If the message `SnapCenter Compatibility Error` is displayed, then the selected VM is not compatible with SnapCenter and you must first add the appropriate storage VM to SnapCenter.

3. In the **Add To Resource Group** page, select a resource group, and then select **OK**.

   When you select **OK**, the system first checks that SnapCenter manages and is compatible with the storage on which the selected VMs or datastores are located.

   If the message `Selected <resource-name> is not SnapCenter compatible` is displayed, then a selected VM or datastore is not compatible with SnapCenter. Refer to Manage compatibility check failures for more information.

Add multiple VMs and datastores to a resource group

Using the SnapCenter VMware vSphere client Edit Resource Group wizard, you can add multiple resources to an existing resource group.

A resource group can contain one of the following:

- Any combination of traditional VMs and SAN and NAS datastores (vVol datastores not supported).
- One FlexGroup datastore (spanning VMs are not supported).
- One or more FlexVol datastores (spanning VMs are supported).
- One or more vVol VMs.
- All vVol VMs with a specified vSphere tag.
- All vVol VMs in a specified folder.

vVol VMs that span multiple vVol datastores are not supported because SnapCenter only backs up vVols in the primary, selected, vVol datastore.

Steps

1. In the left navigator pane of the SCV plug-in, select **Resource Groups**, then select a resource group, and then select **Edit Resource Group** to start the wizard.
2. On the **Resource** page, do the following:
   a. In the Datastores field, navigate to the VMs or datastores that you want to add.
   b. In the Available entities list, select one or more VMs or datastores you want to add to the resource group, then select **>** to move your selection to the Selected entities list. Select **>>** to move all the available entities.

      By default, the Available entities list displays the Datacenter object. You can select a datastore to view the VMs within the datastore and add them to the resource group.

      When you select **Next**, the system first checks that SnapCenter manages and is compatible with the storage on which the selected VMs or datastores are located. If the message `Some entities are not SnapCenter compatible` is displayed, then a selected VM or datastore is not compatible with SnapCenter. Refer to Manage compatibility check failures for more information.
3. Repeat Step 2 for each VM or datastore that you want to add.
4. Select **Next** until you reach the **Summary** page and then review the summary and select **Finish**.

Restore backup of renamed storage

When the storage is renamed, workflows using backups taken before the rename used to fail. With the introduction of the rename backup feature, which is exclusively accessible through REST API, it is now possible to use the backups that were taken prior to the storage renaming. The workflow and usage of the REST API are described below.

ASA r2 storage system does not support _recent snapshot naming feature.

Steps

1. Add or update the new storage connection, ensuring that the new Cluster or SVM name is reflected in SCV.
2. Restart the service to refresh the caches as described in the KB article: SCV backups fail after SVM rename

3. Create a new backup.
4. Use the backup details to find the old and new storage names.
5. In the **Backups** screen of the vSphere client, select the backup to see its details.
6. Access Swagger from the URL: `https://<SCV-IP>:8144/api/swagger-ui/index.html`

   Use the following API to rename the storage:

   PATCH
   /4.1/storage-system

   Example:
   {
   "existingSVM": {
   "name": "string"
   },
   "newSVM": {
   "name": "string"
   }
   }

   Response:

   {
   "statusMessage": "OK",
   "statusCode": 200,
   "responseMessage": [
   "Storage system renamed successfully."
   ]
   }

   After running this API you will be able to run all the workflows including the restore operation from the old backup.

Back up resource groups on demand

Backup operations are performed on all the resources defined in a resource group. If a resource group has a policy attached and a schedule configured, then backups occur automatically according to the schedule.

ASA r2 backup creates consistency group snapshots and provisions primary consistency group if the given resource does not already have it.

Before you begin

You must have created a resource group with a policy attached.

Do not start an on-demand backup job when a job to back up the SnapCenter Plug-in for VMware vSphere MySQL database is already running. Use the maintenance console to see the configured backup schedule for the MySQL database.

About this task

In earlier releases of Virtual Storage Console (VSC), you could perform an on-demand backup without having a backup job configured for a VM or datastore. However, for the SnapCenter Plug-in for VMware vSphere, VMs and datastores must be in a resource group before you can perform backups.

Steps

1. In the left navigator pane of the SCV plug-in, select **Resource Groups**, then select a resource group, and then select **Run Now** to start the backup.
2. If the resource group has multiple policies configured, then in the **Backup Now** dialog box, select the policy you want to use for this backup operation.
3. Select **OK** to start the backup.
4. Optional: Monitor the operation progress by selecting **Recent Tasks** at the bottom of the window or on the dashboard **Job Monitor** for more details.
   .Result

If the quiesce operation fails for any of the VMs in the backup, then the backup completes with a warning and is marked as not VM consistent even if the selected policy has VM consistency selected. In this case, it is possible that some of the VMs were successfully quiesced. In the job monitor, the failed VM details will show the quiesce as failed.

Back up the SnapCenter Plug-in for VMware vSphere MySQL database

SnapCenter Plug-in for VMware vSphere includes a MySQL database (also called an NSM database) that contains the metadata for all jobs performed by the plug-in. You should back up this repository regularly.

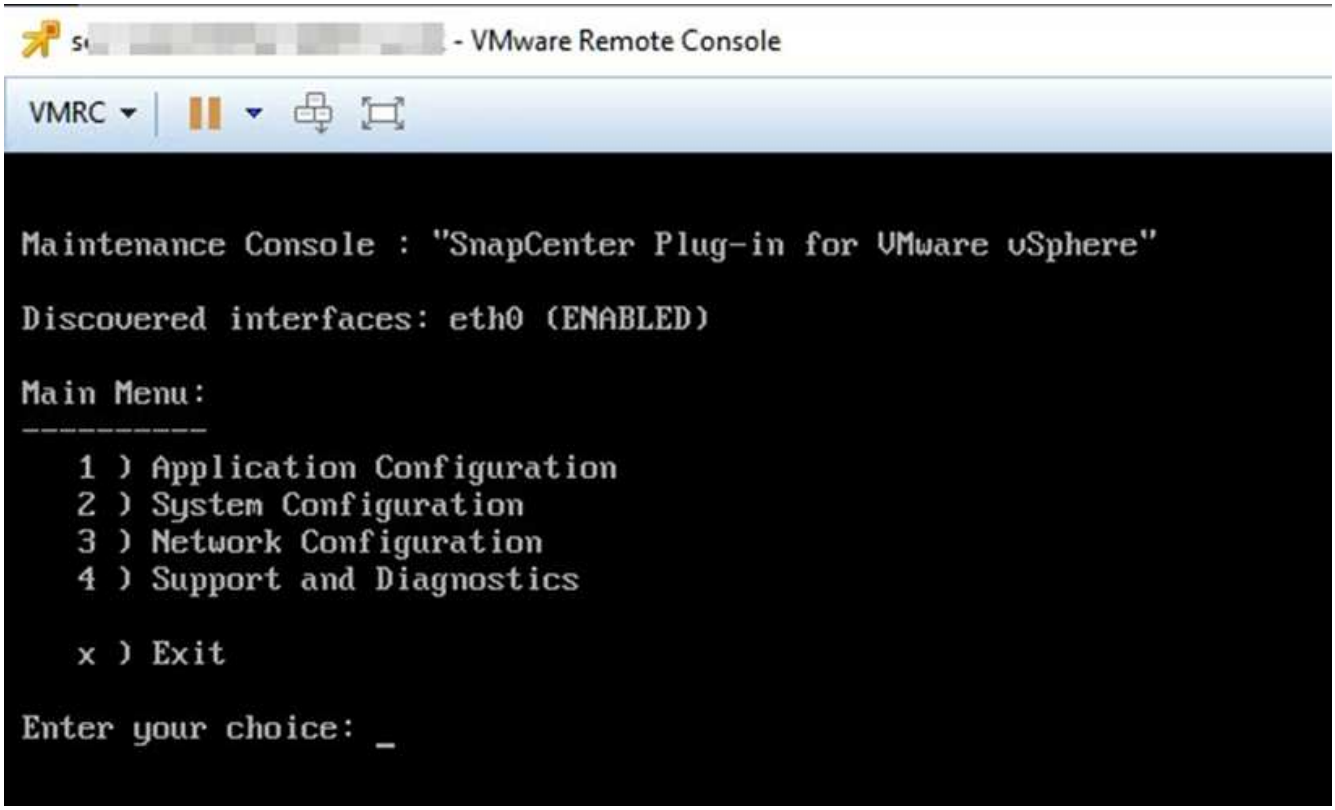
You should also back up the repository before performing migrations or upgrades.

Before you begin

Do not start a job to back up the MySQL database when an on-demand backup job is already running.

Steps

1. From the VMware vSphere client, select the VM where the SnapCenter Plug-in for VMware vSphere is located.
2. In the **Summary** tab of the virtual appliance select **Launch Remote Console or Launch Web Console** to open a maintenance console window.



3. From the Main Menu, enter option **1) Application Configuration.**
4. From the Application Configuration Menu, enter option **6) MySQL backup and restore.**
5. From the MySQL Backup and Restore Configuration Menu, enter option **1) Configure MySQL backup**.
6. At the prompt, enter the backup location for the repository, the number of backups to keep, and the time the backup should start.

   All inputs are saved when you enter them. When the backup retention number is reached, older backups are deleted when new backups are performed.

Repository backups are named "backup-<date>". Because the repository restore function looks for the "backup" prefix, you should not change it.

Manage resource groups

You can create, modify, and delete backup resource groups, and perform backup operations on resource groups.

Resource groups are called backup jobs in Virtual Storage Console (VSC).

Suspend and resume operations on resource groups

You can temporarily disable scheduled operations from starting on a resource group. Later when you want, you can enable those operations.

Steps

1. In the left navigator pane of the SCV plug-in, select **Resource Groups**, select a resource group and select **Suspend** (or select **Resume**).
2. In the confirmation box, select **OK** to confirm.

After you finish

On the Resource Groups page, the job status for the suspended resource is `Under_Maintenance`. You might need to scroll to the right of the table to see the Job Status column.

After backup operations are resumed, the Job Status changes to `Production`.

Modify resource groups

You can remove or add resources in resource groups in vCenter, detach or attach policies, modify schedules, or modify any other resource group option.

About this task

If you want to modify the name of a resource group, do not use the following special characters in VM, datastore, policy, backup, or resource group names:

% & * $ # @ ! \ / : * ? " < > - | ; ' , and space.
An underscore character (_) is allowed.

Steps

1. In the left navigator pane of the SCV plug-in, select **Resource Groups**, then select a resource group and select **Edit**.
2. On the left list in the **Edit Resource Group** wizard, select the category that you want to modify and enter your changes.

   You can make changes in multiple categories. You can also edit secondary protected resources in this option.

3. Select **Next** until you see the Summary page, and then select **Finish**.

Delete resource groups

You can delete a resource group in vCenter if you no longer need to protect the resources in the resource group. You must ensure that all resource groups are deleted before you remove SnapCenter Plug-in for VMware vSphere from vCenter.

About this task

All resource group delete operations are performed as force deletes. The delete operation detaches all policies from the vCenter resource group, removes the resource group from SnapCenter Plug-in for VMware vSphere, and deletes all backups and snapshots of the resource group.

> In a SnapVault relationship, the last snapshot cannot be deleted; therefore, the resource group cannot be deleted. Before deleting a resource group that is part of a SnapVault relationship, you must use either System Manager or use the ONTAP CLI to remove the SnapVault relationship, and then you must delete the last snapshot.

Steps

1. In the left navigator pane of the SCV plug-in, select **Resource Groups**, then select a resource group and

select **Delete**.

2. In the **Delete resource group** confirmation box, select **OK** to confirm.

Manage policies

You can create, modify, view, detach, and delete backup policies for SnapCenter Plug-in for VMware vSphere. Policies are required to perform data protection operations.

Detach policies

You can detach policies from a SnapCenter Plug-in for VMware vSphere resource group when you no longer want those policies to govern data protection for the resources. You must detach a policy before you can remove it or before you modify the schedule frequency.

About this task

The guidelines for detaching policies from the SnapCenter Plug-in for VMware vSphere resource groups differ from the guidelines for SnapCenter resource groups. For a VMware vSphere client resource group, it is possible to detach all policies, which leaves the resource group with no policy. However, to perform any data protection operations on that resource group, you must attach at least one policy.

Steps

1. In the left navigator pane of the SCV plug-in, select **Resource Groups**, then select a resource group and select **Edit**.
2. On the **Policies** page of the **Edit Resource Group** wizard, clear the check mark next to the policies you want to detach.

   You can also add a policy to the resource group by checking the policy.

3. Make any additional modifications to the resource group in the rest of the wizard, and then select **Finish**.

Modify policies

You can modify policies for a SnapCenter Plug-in for VMware vSphere resource group. You can modify the frequency, replication options, snapshot retention settings, or scripts information while a policy is attached to a resource group.

About this task

Modifying SnapCenter Plug-in for VMware vSphere backup policies differs from modifying backup policies for SnapCenter application-based plug-ins. You do not need to detach policies from resource groups when you modify the plug-in policies.

Before you modify the replication or retention settings, you should consider the possible consequences.

- Increasing replication or retention settings

  Backups continue to accumulate until they reach the new setting.

- Decreasing replication or retention settings

  Backups in excess of the new setting are deleted when the next backup is performed.

To modify a SnapCenter Plug-in for VMware vSphere policy schedule, you must modify the schedule in the plug-in resource group.

Steps

1. In the left navigator pane of the SCV plug-in, select **Policies**, then select a policy and select **Edit**.
2. Modify the policy fields.
3. When you are finished, select **Update**.

The changes take effect when the next scheduled backup is performed.

Delete policies

If you no longer require a configured backup policy for SnapCenter Plug-in for VMware vSphere, you might want to delete it.

Before you begin

You must have detached the policy from all resource groups in the virtual appliance for SnapCenter before you can delete it.

Steps

1. In the left navigator pane of the SCV plug-in, select **Policies**, then select a policy and select **Remove**.
2. In the confirmation dialog box select **OK**.

Manage backups

You can rename and delete backups performed by SnapCenter Plug-in for VMware vSphere. You can also delete multiple backups simultaneously.

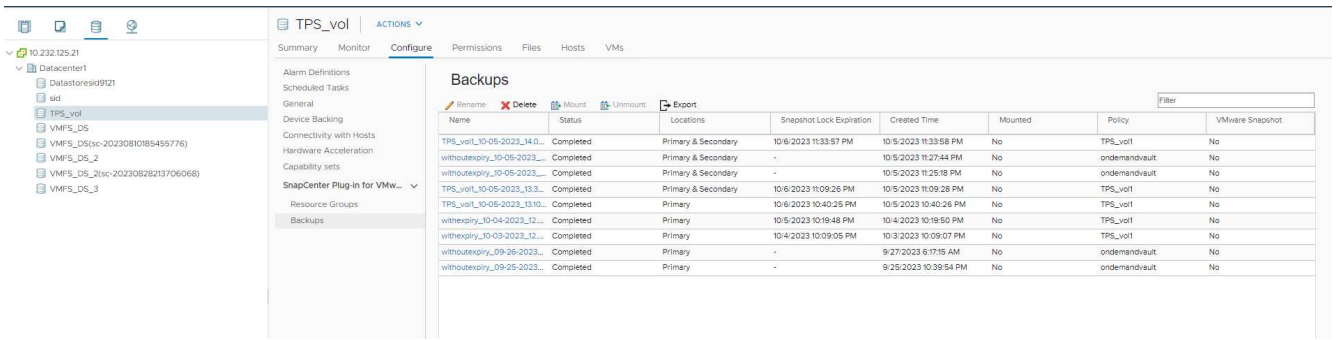
Rename backups

You can rename SnapCenter Plug-in for VMware vSphere backups if you want to provide a better name to improve searchability.

ASA r2 storage system does not support renaming of backups.

Steps

1. Select **Menu** and select the **Hosts and Clusters** menu option, then select a VM, then select the **Configure** tab, and then select **Backups** in the **SnapCenter Plug-in for VMware vSphere** section.



2. On the Configure tab, select a backup, and select **Rename**.
3. On the **Rename Backup** dialog box, enter the new name, and select **OK**.

   Do not use the following special characters in VM, datastore, policy, backup, or resource group names: & * $ # @ ! \ / : * ? " < > - | ; ' , and space. An underscore character (_) is allowed.

Delete backups

You can delete SnapCenter Plug-in for VMware vSphere backups if you no longer require the backup for other data protection operations. You can delete one backup or delete multiple backups simultaneously.

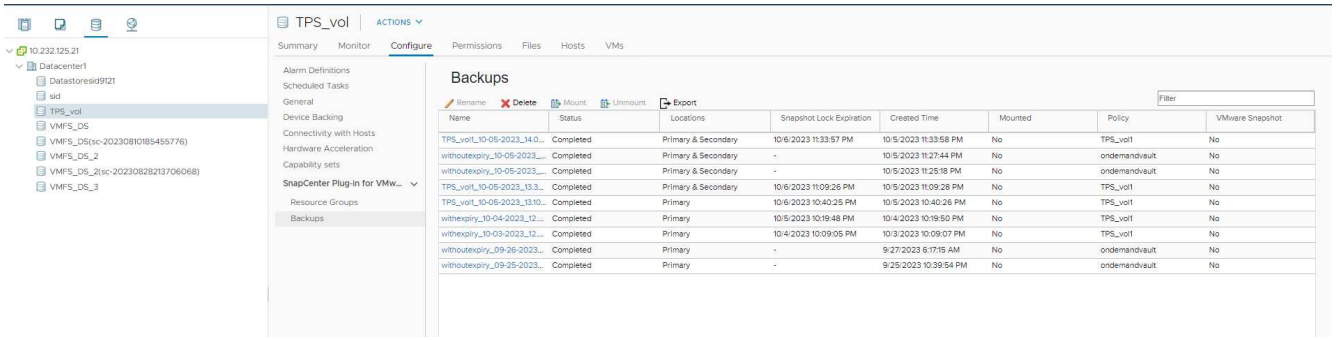
Before you begin

You cannot delete backups that are mounted. You must unmount a backup before you can delete it.

About this task

snapshots on secondary storage are managed by your ONTAP retention settings, not by the SnapCenter Plug-in for VMware vSphere. Therefore, when you use the SnapCenter Plug-in for VMware vSphere to delete a backup, snapshots on primary storage are deleted but snapshots on secondary storage are not deleted. If a snapshot still exists on secondary storage, the SnapCenter Plug-in for VMware vSphere retains the metadata associated with the backup to support restore requests. When the ONTAP retention process deletes the secondary snapshot, then the SnapCenter Plug-in for VMware vSphere deletes the metadata using a purge job, which is executed at regular intervals.

1. Select **Menu** and select the **Hosts and Clusters** menu option, then select a VM, then select the **Configure** tab, and then select **Backups** in the **SnapCenter Plug-in for VMware vSphere** section.



2. Select one or more backups and select **Delete**.

   You can select a maximum of 40 backups to delete.

3. Select **OK** to confirm the delete operation.
4. Refresh the backup list by selecting the refresh icon on the left vSphere menu bar.

Mount and unmount datastores

Mount a backup

You can mount a traditional datastore from a backup if you want to access files in the backup. You can either mount the backup to the same ESXi host where the backup was created or to an alternate ESXi host that has the same type of VM and host configurations. You can mount a datastore multiple times on a host.

You cannot mount a vVol datastore.

Before you begin

- Ensure alternate ESXi host can connect to the storage

  If you want to mount to an alternate ESXi host, you must ensure that the alternate ESXi host can connect to the storage and has the following:

  - Same UID and GID as that of the original host
  - Same virtual appliance for SnapCenter Plug-in for VMware vSphere version as that of original host
- When using the iSCSI protocol, ensure that the initiators for the storage system are mapped to the ESXi host. When using the NVMe protocol, add controllers to map the required subsystem to the ESXi host.
- Clean up stale LUN/Namespace

  Because the ESXi host can only discover one unique LUN/Namespace per datastore, the operation will fail if it finds more than one. This can occur if you start a mount operation before a previous mount operation has finished, or if you manually clone LUN/Namespace, or if clones are not deleted from storage during an unmount operation. To avoid discovery of multiple clones, you should clean up all stale LUN/Namespace on the storage.

About this task

A mount operation might fail if the storage tier of the FabricPool where the datastore is located is unavailable.

Steps

1. In the VMware vSphere client shortcuts page select **Storage**.
2. Right-click a datastore and select **SnapCenter Plug-in for VMware vSphere** > **Mount Backup**.
3. On the **Mount Datastore** page, select a backup and a backup location (primary or secondary), and then select **Finish**.
4. Optional: To verify that the datastore is mounted, perform the following:
   a. Select **Menu** in the toolbar, and then select **Storage** from the drop-down list.
   b. The left navigator pane displays the datastore you mounted at the top of the list.

      To prevent new snapshots from being created when you clone the volume, turn off the ONTAP schedule for the SnapVault volume. Previously existing snapshots are not deleted.

Unmount a backup

You can unmount a backup when you no longer need to access the files in the datastore.

If a backup is listed as mounted in the VMware vSphere client GUI, but it is not listed in the unmount backup screen, then you need to use the REST API `/backup/{backup-Id}/cleanup` to clean up the out-of-bound datastores and then try the unmount procedure again.

If you attempt to mount a backup copy of an NFS datastore on a storage VM (SVM) with the root volume in a load-sharing mirror relationship and you might encounter the error `You may have reached the maximum number of NFS volumes configured in the vCenter. Check the vSphere Client for any error messages.` To prevent this problem, change the maximum volumes setting by navigating to **ESX** > **Manage** > **Settings** > **Advance System Settings** and changing the NFS.MaxVolumes value. Maximum value is 256.

Steps

1. In the VMware vSphere client shortcuts page select **Storage**.
2. In the left navigator pane, right-click a datastore, then select **SnapCenter Plug-in for VMware vSphere** in the drop-down list, and then select **Unmount** in the secondary drop-down list.

   Make sure that you select the correct datastore to unmount. Otherwise, you might cause an impact on production work.

3. In the **Unmount Cloned Datastore** dialog box, select a datastore, select the **Unmount the cloned datastore** checkbox, and then select **Unmount**.

Restore backups

Restore overview

You can restore VMs, VMDKs, files, and folders from primary or secondary backups.

- VM restore destinations

  You can restore traditional VMs to the original host, or to an alternate host in the same vCenter Server, or to an alternate ESXi host managed by the same vCenter or any vCenter in linked mode.

  You can restore vVol VMs to the original host.

- VMDK restore destinations

  You can restore VMDKs in traditional VMs to either the original or to an alternate datastore.

  You can restore VMDKs in vVol VMs to the original datastore.

You can also restore individual files and folders in a guest file restore session, which attaches a backup copy of a virtual disk and then restores the selected files or folders.

You cannot restore the following:

- Datastores

  You cannot use the SnapCenter Plug-in for VMware vSphere to restore a datastore, only the individual VMs in the datastore.

- Backups of removed VMs

  You cannot restore backups of storage VMs that have been removed. For example, if you add a storage VM using the management LIF and then create a backup, and then you remove that storage VM and add a cluster that contains that same storage VM, the restore operation for the backup will fail.

How restore operations are performed

For VMFS environments, the SnapCenter Plug-in for VMware vSphere uses clone and mount operations with Storage VMotion to perform restore operations. For NFS environments, the plug-in uses native ONTAP Single File SnapRestore (SFSR) to provide greater efficiency for most restore operations. For vVol VMs, the plug-in uses ONTAP Single File snapshot Restore (ONTAP SFSR) and SnapMirror Restore for restore operations. The following table lists how restore operations are performed.

Restore operations	From	Performed using
VMs and VMDKs	Primary backups	NFS environments: ONTAP Single File SnapRestore VMFS environments: Clone and mount with Storage VMotion

Restore operations	From	Performed using
VMs and VMDKs	Secondary backups	NFS environments: ONTAP Single File SnapRestore VMFS environments: Clone and mount with Storage VMotion
Deleted VMs and VMDKs	Primary backups	NFS environments: ONTAP Single File SnapRestore VMFS environments: Clone and mount with Storage VMotion
Deleted VMs and VMDKs	Secondary backups	NFS environments: Clone and mount with Storage VMotion VMFS environments: Clone and mount with Storage VMotion
VMs and VMDKs	VM-consistent primary backups	NFS environments: ONTAP Single File SnapRestore VMFS environments: Clone and mount with Storage VMotion
VMs and VMDKs	VM-consistent secondary backups	NFS environments: ONTAP SnapMirror Restore VMFS environments: Clone and mount with Storage VMotion
vVol VMs	Crash-consistent primary backups	ONTAP Single File SnapRestore for all protocols
vVol VMs	Crash-consistent secondary backups	ONTAP SnapMirror Restore for all protocols
FlexGroup VMs	Primary backups	NFS environments: * ONTAP Single File SnapRestore if you are using ONTAP Version 9.10.1 and later * Clone and mount with Storage VMotion on ONTAP previous versions VMFS environments: Not supported for FlexGroups
FlexGroup VMs	Secondary backups	NFS environments: • ONTAP SnapMirror Restore if you are using ONTAP Version 9.10.1 and later • Clone and mount with Storage VMotion for ONTAP previous versions VMFS environments: Not supported for FlexGroups

You cannot restore a vVol VM after a vVol container rebalance.

Guest file restore operations are performed using clone and mount operations (not Storage VMotion) in both NFS and VMFS environments.

During a restore operation, you might encounter the error `Host unresolved volumes is null` or `Exception while calling pre-restore on SCV….Error mounting cloned LUN as datastore…` This occurs when the SnapCenter Plug-in for VMware vSphere attempts to resignature the clone. Due to VMware restrictions, the SnapCenter Plug-in for VMware vSphere cannot control the automatic resignature value in advanced ESXi host configurations.
For NVMe over TCP and NVMe over FC storage, SCV cannot add controllers dynamically when a new subsystem is added. You should make the necessary mapping before the mount operation.

Refer to KB article: SCV clone or restores fail with error 'Host Unresolved volumes is null for more information about the error.

Search for backups

You can search for and find a specific backup of a VM or datastore using the Restore wizard. After you locate a backup, you can then restore it.

Steps

1. In the VMware vSphere client GUI, select **Menu** in the toolbar, and then do one of the following:

To view backups for…	Do the following…
VMs	Select the **Hosts and Clusters** menu option, then select a VM, then select the **Configure** tab, and then select **Backups** in the **SnapCenter Plug-in for VMware vSphere section**.
Datastores	Select the **Storage** menu option, then select a datastore, then select the **Configure** tab, and then select **Backups** in the **SnapCenter Plug-in for VMware vSphere** section.

2. In the left navigator pane, expand the datacenter that contains the VM or datastore.
3. Optional: Right-click a VM or datastore, then select **SnapCenter Plug-in for VMware vSphere** in the drop-down list, and then select **Restore** in the secondary drop-down list.
4. In the **Restore** wizard enter a search name and select **Search**.

   You can filter the backup list by selecting the filter icon and selecting a date and time range, selecting whether you want backups that contain VMware snapshots, whether you want mounted backups, and the location. Select **OK**.

Restore VMs from backups

When you restore a VM, you can overwrite the existing content with the backup copy that

you select or you can make a copy of the VM.

You can restore VMs to the following locations:

- Restore to original location
  - To the original datastore mounted on the original ESXi host (this overwrites the original VM)
- Restore to alternate location
  - To a different datastore mounted on the original ESXi host
  - To the original datastore mounted on a different ESXi host that is managed by the same vCenter
  - To a different datastore mounted on a different ESXi host that is managed by the same vCenter
  - To a different datastore mounted on a different ESXi host that is managed by a different vCenter in linked mode

You cannot restore vVol VMs to an alternate host.

The following restore workflow is not supported: Add a storage VM, then perform a backup of that VM, then delete the storage VM and add a cluster that includes that same storage VM, and then attempt to restore the original backup.

For improved performance of restore operations in NFS environments, enable the VMware application vStorage API for Array Integration (VAAI).

Before you begin

- A backup must exist.

  You must have created a backup of the VM using the SnapCenter Plug-in for VMware vSphere before you can restore the VM.

  Restore operations cannot finish successfully if there are snapshots of the VM that were performed by software other than the SnapCenter Plug-in for VMware vSphere.

- The destination datastore must be ready.
  - The destination datastore for the restore operation must have enough space to accommodate a copy of all the VM files (for example: vmdk, vmx, vmsd).
  - The destination datastore must not contain stale VM files from previous restore operation failures. Stale files have the name format `restore_xxx_xxxxxx_<filename>`.
- The VM must not be in transit.

  The VM that you want to restore must not be in a state of vMotion or Storage vMotion.

- HA configuration errors

  Ensure there are no HA configuration errors displayed on the vCenter ESXi Host Summary screen before restoring backups to a different location.

- Restoring to a different locations
  - When restoring to a different location, SnapCenter Plug-in for VMware vSphere must be running in the vCenter that is the destination for the restore operation. The destination datastore must have sufficient

space.

- The destination vCenter in the Restore To alternate Location field must be DNS resolvable.

About this task

- VM is unregistered and registered again

  The restore operation for VMs unregisters the original VM, restores the VM from a backup snapshot, and registers the restored VM with the same name and configuration on the same ESXi server. You must manually add the VMs to resource groups after the restore.

- Restoring datastores

  You cannot restore a datastore, but you can restore any VM in the datastore.

- Restoring vVol VMs
  - vVol datastores that span VMs are not supported. Because attached VMDKs in a VM-spanning vVol datastore are not backed up, the restored VMs will contain only partial VMDKs.
  - You cannot restore a vVol to an alternate host.
  - vVol automatic rebalance is not supported.
- VMware consistency snapshot failures for a VM

  Even if a VMware consistency snapshot for a VM fails, the VM is nevertheless backed up. You can view the entities contained in the backup copy in the Restore wizard and use it for restore operations.

- A restore operation might fail if the storage tier of the FabricPool where the VM is located is unavailable.

Steps

1. In the VMware vSphere client GUI, select **Menu** in the toolbar, and then select **VMs and Templates** from the drop-down list.

   If you are restoring a deleted VM, the storage VM credentials that were added to the SnapCenter Plug-in for VMware vSphere must be `vsadmin` or a user account that has all the same privileges as `vsadmin`.

2. In the left navigator pane, right-click a VM, then select **SnapCenter Plug-in for VMware vSphere** in the drop-down list, and then select **Restore** in the secondary drop-down list to start the wizard.
3. In the **Restore** wizard, on the **Select Backup** page, select the backup snapshot that you want to restore.

   You can search for a specific backup name or a partial backup name, or you can filter the backup list by selecting the filter icon and selecting a date and time range, selecting whether you want backups that contain VMware snapshots, whether you want mounted backups, and the location. Select **OK** to return to the wizard.

4. On the **Select Scope** page, select **Entire virtual machine** in the **Restore scope** field, then select the restore location, and then enter the destination information where the backup should be mounted.

   In the **VM name** field, if the same VM name exists, then the new VM name format is `<vm_name>_<timestamp>`.

   When restoring partial backups, the restore operation skips the **Select Scope** page.

5. On the **Select Location** page, select the location for the restored datastore.

   In SnapCenter Plug-in for VMware vSphere 4.5 and later, you can select secondary storage for FlexGroup volumes.

6. Review the Summary page and then select **Finish**.
7. Optional: Monitor the operation progress by selecting **Recent Tasks** at the bottom of the screen.

   Refresh the screen to display updated information.

After you finish

- Change IP address

  If you restored to a different location, then you must change the IP address of the newly created VM to avoid an IP address conflict when static IP addresses are configured.

- Add restored VMs to resource groups

  Although the VMs are restored, they are not automatically added to their former resource groups. Therefore, you must manually add the restored VMs to the appropriate resource groups.

Restore deleted VMs from backups

You can restore a deleted VM from a datastore primary or secondary backup to an ESXi host that you select.

You can restore VMs to the following locations:

- Restore to original location
  - To the original datastore mounted on the original ESXi host (this makes a copy of the VM)
- Restore to alternate location
  - To a different datastore mounted on the original ESXi host
  - To the original datastore mounted on a different ESXi host that is managed by the same vCenter
  - To a different datastore mounted on a different ESXi host that is managed by the same vCenter
  - To a different datastore mounted on a different ESXi host that is managed by a different vCenter in linked mode

When restoring to a different location, SnapCenter Plug-in for VMware vSphere must be running in the linked vCenter that is the destination for the restore operation. The destination datastore must have sufficient space.

You cannot restore vVol VMs to an alternate location.

When restoring a deleted VM, any tags or folders that were originally assigned to the VM are not restored.

Before you begin

- The user account for the storage system, on the Storage Systems page in the VMware vSphere client, must have the Minimum ONTAP privileges required for ONTAP.
- The user account in vCenter must have the Minimum vCenter privileges required for SnapCenter Plug-in for VMware vSphere.
- A backup must exist.

  You must have created a backup of the VM using the SnapCenter Plug-in for VMware vSphere before you can restore the VMDKs on that VM.

For improved performance of restore operations in NFS environments, enable the VMware application vStorage API for Array Integration (VAAI).

About this task

You cannot restore a datastore, but you can restore any VM in the datastore.

A restore operation might fail if the storage tier of the FabricPool where the VM is located is unavailable.

Steps

1. In the vCenter Server, navigate to **Inventory** > **Datastores** and select a datastore.
2. Select the **Configure** > **Backups** in the SnapCenter Plug-in for VMware vSphere section.
3. Double-click on a backup to see a list of all VMs that are included in the backup.
4. Select the deleted VM from the backup list and select **Restore**.
5. In the **Restore** wizard, on the **Select Backup** page, select the backup copy that you want to restore from.

   You can search for a specific backup name or a partial backup name, or you can filter the backup list by selecting the filter icon and selecting a date and time range, selecting whether you want backups that contain VMware snapshots, whether you want mounted backups, and the location. Select **OK** to return to the wizard.

6. On the **Select Scope** page, select **Entire virtual machine** in the **Restore scope** field, then select the restore location, and then enter the Destination ESXi host information where the backup should be mounted.

   The restore destination can be any ESXi host that has been added to SnapCenter. This option restores the contents of the selected backup in which the VM resided from a snapshot with the specified time and date. The **Restart VM** check box is checked if you select this option and the VM will be powered on.

   If you are restoring a VM in an NFS datastore onto an alternate ESXi host that is in an ESXi cluster, then after the VM is restored, it is registered on the alternate host.

7. On the **Select Location** page, select the location of the backup that you want to restore from (primary or secondary).
8. Review the Summary page and then select **Finish**.

Restore VMDKs from backups

You can restore existing VMDKs, or deleted or detached VMDKs, from either a primary or secondary backup of traditional VMs or vVol VMs.

You can restore one or more virtual machine disks (VMDKs) on a VM to the same datastore.

For improved performance of restore operations in NFS environments, enable the VMware application vStorage API for Array Integration (VAAI).

Before you begin

- A backup must exist.

  You must have created a backup of the VM using the SnapCenter Plug-in for VMware vSphere.

- The VM must not be in transit.

  The VM that you want to restore must not be in a state of vMotion or Storage vMotion.

About this task

- If the VMDK is deleted or detached from the VM, then the restore operation attaches the VMDK to the VM.
- A restore operation might fail if the storage tier of the FabricPool where the VM is located is unavailable.
- Attach and restore operations connect VMDKs using the default SCSi controller.
  However, when VMDKs that are attached to a VM with a NVMe disk are backed up, the attach and restore operations use NVMe controller if available.

Steps

1. In the VMware vSphere client GUI, select **Menu** in the toolbar, and then select **VMs and Templates** from the drop-down list.
2. In the left navigator pane, right-click a VM, then select **SnapCenter Plug-in for VMware vSphere** in the drop-down list, and then select **Restore** in the secondary drop-down list.
3. In the **Restore** wizard, on the Select Backup page, select the backup copy that you want to restore from.

   You can search for a specific backup name or a partial backup name, or you can filter the backup list by selecting the filter icon and selecting a date and time range, selecting whether you want backups that contain VMware snapshots, whether you want mounted backups, and primary or secondary location. Select **OK** to return to the wizard.

4. On the **Select Scope** page, select the restore destination.

To restore to…	Specify the restore destination…
The original datastore	Select **Particular disk** from the drop-down list and then select **Next**. In the Datastore selection table, you can select or unselect any VMDKs.
An alternate datastore in an alternate location	Select the destination datastore and select a different datastore from the list.

5. On the **Select Location** page, select the snapshot that you want to restore (primary or secondary).
6. Review the Summary page and then select **Finish**.
7. Optional: Monitor the operation progress by selecting **Recent Tasks** at the bottom of the screen.
8. Refresh the screen to display updated information.

Restore the most recent backup of the MySQL database

You can use the maintenance console to restore the most recent backup of the MySQL database (also called an NSM database) for the SnapCenter Plug-in for VMware vSphere.

Steps

1. Open a maintenance console window.

   Access the Maintenance Console.

2. From the Main Menu, enter option **1) Application Configuration**.
3. From the Application Configuration Menu, enter option **6) MySQL backup and restore**.
4. From the MySQL Backup and Restore Configuration Menu, enter option **4) Restore MySQL backup**.
5. At the prompt “Restore using the most recent backup,” enter **y**, and then press **Enter**.

   The backup MySQL database is restored to its original location.

Restore a specific backup of the MySQL database

You can use the maintenance console to restore a specific backup of the MySQL database (also called an NSM database) for the SnapCenter Plug-in for VMware vSphere virtual appliance.

Steps

1. Open a maintenance console window.

   Access the Maintenance Console.

2. From the Main Menu, enter option **1) Application Configuration**.
3. From the Application Configuration Menu, enter option **6) MySQL backup and restore**.
4. From the MySQL Backup and Restore Configuration Menu, enter option **2) List MySQL backups**, and then make a note of the backup you want to restore.
5. From the MySQL Backup and Restore Configuration Menu, enter option **4) Restore MySQL backup**.
6. At the prompt “Restore using the most recent backup,” enter **n**.
7. At the prompt “Backup to restore from,” enter the backup name, and then press **Enter**.

   The selected backup MySQL database is restored to its original location.

Attach and detach VMDKs

Attach VMDKs to a VM or vVol VM

You can attach one or more VMDKs from a backup to the parent VM, or to an alternate VM on the same ESXi host, or to an alternate VM on an alternate ESXi host managed by the same vCenter or a different vCenter in linked mode. VMs in traditional datastores and in vVol datastores are supported.

This makes it easier to restore one or more individual files from a drive instead of restoring the entire drive. You can detach the VMDK after you have restored or accessed the files you need.

About this task

You have the following attach options:

- You can attach virtual disks from a primary or a secondary backup.
- You can attach virtual disks to the parent VM (the same VM that the virtual disk was originally associated with) or to an alternate VM on the same ESXi host.

The following limitations apply to attaching virtual disks:

- Attach and detach operations are not supported for Virtual Machine Templates.
- When more than 15 VMDKs are attached to an iSCSI controller, the virtual machine for SnapCenter Plug-in for VMware vSphere cannot locate VMDK unit numbers higher than 15 because of VMware restrictions.

  In this case, add the SCSi controllers manually and try the attach operation again.

- You cannot manually attach a virtual disk that was attached or mounted as part of a guest file restore operation.
- Attach and restore operations connect VMDKs using the default SCSi controller. However, when VMDKs that are attached to a VM with a NVMe disk are backed up, the attach and restore operations use NVMe controller if available.

Before you begin

Follow the steps below to add NVMe controller to the disk.

1. Log in to the vCenter client
2. Select the VM from the VMFS datastore
3. Right-click on the VM and go to **Edit settings**
4. In the edit settings window, select **Add new device** > **NVMe Controller**

Steps

1. In the VMware vSphere client GUI, select **Menu** in the toolbar, and then select **Hosts and clusters** from the drop-down list.
2. In the left navigation pane, right-click a VM, then select **SnapCenter Plug-in for VMware vSphere** > **Attach virtual disk(s)**.
3. On the **Attach Virtual Disk** window, in the **Backup** section, select a backup.

You can filter the backup list by selecting the filter icon and choosing a date and time range, selecting whether you want backups that contain VMware snapshots, whether you want mounted backups, and the location. Select **OK**.

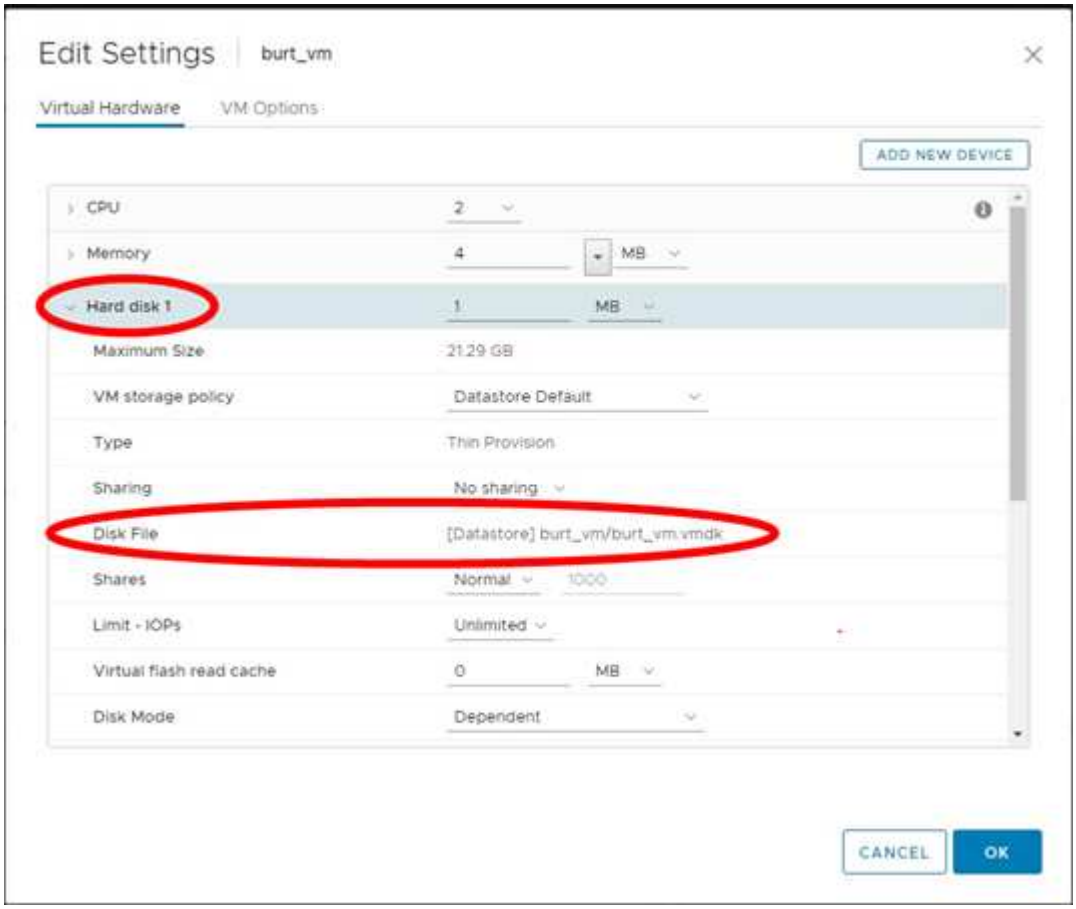
4. In the **Select Disks** section, select one or more disks you want to attach and the location you want to attach from (primary or secondary).

   You can change the filter to display primary and secondary locations.

5. By default, the selected virtual disks are attached to the parent VM. To attach the selected virtual disks to an alternate VM in the same ESXi host, select **Click here to attach to alternate VM** and specify the alternate VM.
6. Select **Attach**.
7. Optional: Monitor the operation progress in the **Recent Tasks** section.

   Refresh the screen to display updated information.

8. Verify that the virtual disk is attached by performing the following:
   a. Select **Menu** in the toolbar, and then select **VMs and Templates** from the drop-down list.
   b. In the left navigator pane, right-click a VM, then select **Edit settings** in the drop-down list.
   c. In the **Edit Settings** window, expand the list for each hard disk to see the list of disk files.



The Edit Settings page lists the disks on the VM. You can expand the details for each hard disk to see the list of attached virtual disks.

Result

You can access the attached disks from the host operating system and then retrieve the needed information from the disks.

Detach a virtual disk

After you have attached a virtual disk to restore individual files, you can detach the virtual disk from the parent VM.

Steps

1. In the VMware vSphere client GUI, select **Menu** in the toolbar, and then select **VMs and Templates** from the drop-down list.
2. In the left navigator pane, select a VM.
3. In the left navigation pane, right-click the VM, then select **SnapCenter Plug-in for VMware vSphere** in the drop-down list, and then select **Detach virtual disk** in the secondary drop-down list.
4. On the **Detach Virtual Disk** screen, select one or more disks you want to detach, then select the **Detach the selected disk(s)** checkbox, and select **DETACH**.

   Make sure that you select the correct virtual disk. Selecting the wrong disk might affect production work.

5. Optional: Monitor the operation progress in the **Recent Tasks** section.

   Refresh the screen to display updated information.

6. Verify that the virtual disk is detached by performing the following:
   a. Select **Menu** in the toolbar, and then select **VMs and Templates** from the drop-down list.
   b. In the left navigator pane, right-click a VM, then select **Edit settings** in the drop-down list.
   c. In the **Edit Settings** window, expand the list for each hard disk to see the list of disk files.

      The **Edit Settings** page lists the disks on the VM. You can expand the details for each hard disk to see the list of attached virtual disks.

Restore guest files and folders

Workflow, prerequisites, and limitations

You can restore files or folders from a virtual machine disk (VMDK) on a Windows guest OS.

Guest restore workflow

Guest OS restore operations include the following steps:

1. Attach

   Attach a virtual disk to a guest VM or proxy VM and start a guest file restore session.

2. Wait

   Wait for the attach operation to complete before you can browse and restore. When the attach operation finishes, a guest file restore session is automatically created and an email notification is sent.

3. Select files or folders

   Browse the VMDK in the Guest File Restore session and select one or more files or folders to restore.

4. Restore

   Restore the selected files or folders to a specified location.

Prerequisites for restoring guest files and folders

Before you restore one or more files or folders from a VMDK on a Windows guest OS, you must be aware of all the requirements.

- VMware tools must be installed and running.

  SnapCenter uses information from VMware tools to establish a connection to the VMware Guest OS.

- The Windows Guest OS must be running Windows Server 2008 R2 or later.

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

- Credentials for the target VM must specify the built-in domain administrator account or the built-in local administrator account. The username must be "Administrator." Before starting the restore operation, the credentials must be configured for the VM to which you want to attach the virtual disk. The credentials are required for both the attach operation and the subsequent restore operation. Workgroup users can use the built-in local administrator account.

  If you must use an account that is not the built-in administrator account, but has administrative privileges within the VM, you must disable UAC on the guest VM.

- You must know the backup snapshot and VMDK to restore from.

  SnapCenter Plug-in for VMware vSphere does not support searching of files or folders to restore. Therefore, before you begin you must know the location of the files or folders with respect to the snapshot and the corresponding VMDK.

- Virtual disk to be attached must be in a SnapCenter backup.

  The virtual disk that contains the file or folder you want to restore must be in a VM backup that was performed using the virtual appliance for SnapCenter Plug-in for VMware vSphere.

- To use a proxy VM, the proxy VM must be configured.

  If you want to attach a virtual disk to a proxy VM, the proxy VM must be configured before the attach and restore operation begins.

- For files with non-English-alphabet names, you must restore them in a directory, not as a single file.

  You can restore files with non-alphabetic names, such as Japanese Kanji, by restoring the directory in which the files are located.

- Restoring from a Linux guest OS is not supported

  You cannot restore files and folders from a VM that is running Linux guest OS. However, you can attach a VMDK and then manually restore the files and folders. For the latest information on supported guest OS, refer to NetApp Interoperability Matrix Tool (IMT).

Guest file restore limitations

Before you restore a file or folder from a guest OS, you should be aware of what the feature does not support.

- You cannot restore dynamic disk types inside a guest OS.
- If you restore an encrypted file or folder, the encryption attribute is not retained. You cannot restore files or folders to an encrypted folder.
- The Guest File Browse page displays the hidden files and folder, which you cannot filter.
- You cannot restore from a Linux guest OS.

  You cannot restore files and folders from a VM that is running Linux guest OS. However, you can attach a VMDK and then manually restore the files and folders. For the latest information on supported guest OS, refer to the NetApp Interoperability Matrix Tool (IMT).

- You cannot restore from a NTFS file system to a FAT file system.

  When you try to restore from NTFS-format to FAT-format, the NTFS security descriptor is not copied because the FAT file system does not support Windows security attributes.

- You cannot restore guest files from a cloned VMDK or an uninitialized VMDK.
- You cannot restore the directory structure for a file.

  If a file in a nested directory is selected to be restored, the file is not restored with the same directory structure. The directory tree is not restored, only the file. If you want to restore a directory tree, you can copy the directory itself at the top of the structure.

- You cannot restore guest files from a vVol VM to an alternate host.
- You cannot restore encrypted guest files.

Restore guest files and folders from VMDKs

You can restore one or more files or folders from a VMDK on a Windows guest OS.

About this task

By default, the attached virtual disk is available for 24 hours and then it is automatically detached. You can choose in the wizard to have the session automatically deleted when the restore operation completes, or you can manually delete the Guest File Restore session at any time, or you can extend the time in the **Guest Configuration** page.

Guest file or folder restore performance depends upon two factors: the size of the files or folders being restored; and the number of files or folders being restored. Restoring a large number of small-sized files might take a longer time than anticipated compared to restoring a small number of large-sized files, if the data set to be restored is of same size.

Only one attach or restore operation can run at the same time on a VM. You cannot run parallel attach or restore operations on the same VM.

The guest restore feature allows you to view and restore system and hidden files and to view encrypted files. Do not attempt to overwrite an existing system file or to restore encrypted files to an encrypted folder. During the restore operation, the hidden, system, and encrypted attributes of guest files are not retained in the restored file. Viewing or browsing reserved partitions might cause an error.

Steps

1. From the vSphere client shortcuts window, select **Hosts and Clusters** and select a VM.
2. Right-click on the VM and select **SnapCenter Plug-in for VMware vSphere** > **Guest File Restore**.
3. On the **Restore Scope** page, specify the backup that contains the virtual disk you want to attach by doing the following:
   a. In the **Backup Name** table, select the backup that contains the virtual disk that you want attach.
   b. In the **VMDK** table, select the virtual disk that contains the files or folders you want to restore.
   c. In the **Locations** table, select the location, primary or secondary, of the virtual disk that you want to attach.
4. On the **Guest Details** page, do the following.
   a. Choose where to attach the virtual disk:

Select this option…	If…
Use Guest VM	You want to attach the virtual disk to the VM that you right-clicked before you started the wizard, and then select the credential for the VM that you right-clicked. Credentials must already be created for the VM.
Use Guest File Restore proxy VM	You want to attach the virtual disk to a proxy VM, and then select the proxy VM. The proxy VM must be configured before the attach and restore operation begins.

b. Select the **Send email notification** option.

This option is required if you want to be notified when the attach operation finishes, and the virtual disk is available. The notification email includes the virtual disk name, the VM name, and the newly assigned drive letter for the VMDK.

Enable this option because a guest file restore is an asynchronous operation and there might be a time latency to establish a guest session for you.

This option uses the email settings that are configured when you set up the VMware vSphere client in vCenter.

5. Review the summary and then select **Finish**.

Before you select **Finish**, you can go back to any page in the wizard and change the information.

6. Wait until the attach operation completes.

You can view the progress of the operation in the Dashboard job monitor, or you can wait for the email notification.

7. To find the files that you want to restore from the attached virtual disk, select **SnapCenter Plug-in for VMware vSphere** from the vSphere client shortcuts window.
8. In the left navigator pane Select **Guest File Restore** > **Guest Configuration**.

In the Guest Session Monitor table, you can display additional information about a session by selecting *… *in the right column.

9. Select the guest file restore session for the virtual disk that was listed in the notification email.

All partitions are assigned a drive letter, including system reserved partitions. If a VMDK has multiple partitions, you can select a specific drive by selecting the drive in the drop-down list in the drive field at the top of the Guest File Browse page.

10. Select the **Browse Files** icon to view a list of files and folders on the virtual disk.

    When you double select a folder to browse and select individual files, there might be a time latency while fetching the list of files because the fetch operation is performed at run time.

    For easier browsing, you can use filters in your search string. The filters are case-sensitive, Perl expressions without spaces. The default search string is `.*`. The following table shows some example Perl search expressions.

This expression…	Searches for…
.	Any character except a newline character.
.*	Any string. This is the default.
a	The character a.
ab	The string ab.
a [vertical bar] b	The character a or b.
a*	Zero or more instances of the character a.
a+	One or more instances of the character a.
a?	Zero or one instance of the character a.
a{x}	Exactly x number of instances of the character a.
a{x,}	At least x number of instances of the character a.
a{x,y}	At least x number of instances of the character a and at most y number.
\	Escapes a special character.

    The Guest File Browse page displays all hidden files and folders in addition to all other files and folders.

11. Select one or more files or folders that you want to restore, and then select **Select Restore Location**.

    The files and folders to be restored are listed in the Selected File(s) table.

12. In the **Select Restore Location** page, specify the following:

Option	Description
Restore to path	Enter the UNC share path to the guest where the selected files will be restored. IPv4 address example: `\\10.60.136.65\c$` IPv6 address example: `\\fd20-8b1e-b255-832e—61.ipv6-literal.net\C\restore`

Option	Description
If original file(s) exist	Select the action to be taken if the file or folder to be restored already exists on the restore destination: Always overwrite or Always skip. If the folder already exists, then the contents of the folder are merged with the existing folder.
Disconnect Guest Session after successful restore	Select this option if you want the guest file restore session to be deleted when the restore operation completes.

13. Select **Restore**.

    You can view the progress of the restore operation in the Dashboard job monitor, or you can wait for the email notification. The time it takes for the email notification to be sent depends upon the length of time the restore operation takes to complete.

    The notification email contains an attachment with the output from the restore operation. If the restore operation fails, open the attachment for additional information.

Set up proxy VMs for restore operations

If you want to use a proxy VM for attaching a virtual disk for guest file restore operations, you must set up the proxy VM before you begin the restore operation. Although you can set up a proxy VM at any time, it might be more convenient to set it up immediately after the plug-in deployment completes.

Steps

1. From the vSphere client shortcuts window, select **SnapCenter Plug-in for VMware vSphere** under plug-ins.
2. In the left navigation select **Guest File Restore**.
3. In the **Run As Credentials** section, do one of the following:

To do this…	Do this…
Use existing credentials	Select any of the configured credentials.
Add new credentials	1. Select **Add**. 2. In the **Run As Credentials** dialog box, enter the credentials. 3. Select **Select VM**, then select a VM in the **Proxy VM** dialog box. Select **Save** to return to the **Run As Credentials** dialog box. 4. Enter the credentials. For Username, you must enter “Administrator”.

SnapCenter Plug-in for VMware vSphere uses the selected credentials to log into the selected proxy VM.

The Run As credentials must be the default domain administrator that is provided by Windows or the built-in local administrator. Workgroup users can use the built-in local administrator account.

4. In the **Proxy Credentials** section, select **Add** to add a VM to use as a proxy.
5. In the **Proxy VM** dialog box, complete the information, and then select **Save**.

You need to delete the proxy VM from the SnapCenter Plug-in for VMware vSphere UI before you can delete it from ESXi host.

Configure credentials for VM guest file restores

When you attach a virtual disk for guest file or folder restore operations, the target VM for the attach must have credentials configured before you restore.

About this task

The following table lists the credential requirements for guest restore operations.

	User access control enabled	User access control disabled
Domain user	A domain user with “administrator” as the username works fine. For example, “NetApp\administrator”. However, a domain user with “xyz” as the username that belongs to a local administrator group will not work. For example, you cannot use “NetApp\xyz”.	Either a domain user with “administrator” as the username or a domain user with “xyz” as the username that belongs to a local administrator group, works fine. For example, “NetApp\administrator” or “NetApp\xyz”.
Workgroup user	A local user with “administrator” as the username works fine. However, a local user with “xyz” as the username that belongs to a local administrator group will not work.	Either a local user with “administrator” as the username or a local user with “xyz” as the username that belongs to a local administrator group, works fine. However, a local user with “xyz” as the username that does not belong to local administrator group will not work.

In the preceding examples, “NetApp” is the dummy domain name and “xyz” is the dummy local username

Steps

1. From the vSphere client shortcuts window, select **SnapCenter Plug-in for VMware vSphere** under plug-ins.
2. In the left navigation select **Guest File Restore**.
3. In the **Run As Credentials** section, do one of the following:

To do this…	Do this…
Use existing credentials	Select any of the configured credentials.

To do this…	Do this…
Add new credentials	1. Select **Add**. 2. In the **Run As Credentials** dialog box, enter the credentials. For Username, you must enter “Administrator”. 3. Select **Select VM**, then select a VM in the **Proxy VM** dialog box. Select **Save** to return to the **Run As Credentials** dialog box. Select the VM that should be used to authenticate the credentials.

SnapCenter Plug-in for VMware vSphere uses the selected credentials to log on to the selected VM.

4. Select **Save**.

Extend the time of a guest file restore session

By default, an attached Guest File Restore VMDK is available for 24 hours and then it is automatically detached. You can extend the time in the **Guest Configuration** page.

About this task

You might want to extend a guest file restore session if you want to restore additional files or folders from the attached VMDK at a later time. However, because guest file restore sessions use a lot of resources, extending the session time should be performed only occasionally.

Steps

1. In the VMware vSphere client, select **Guest File Restore**.
2. Select a guest file restore session and then select the Extend Selected Guest Session icon in the Guest Session Monitor title bar.

   The session is extended for another 24 hours.

Guest file restore scenarios you might encounter

When attempting to restore a guest file, you might encounter any of the following scenarios.

Guest file restore session is blank

This issue occurs when you create a guest file restore session and while that session was active, the guest operating system is rebooted. When this occurs, VMDKs in the guest OS might remain offline. Therefore, when you try to browse the guest file restore session, the list is blank.

To correct the issue, manually put the VMDKs back online in the guest OS. When the VMDKs are online, the guest file restore session will display the correct contents.

Guest file restore attach disk operation fails

This issue occurs when you start a guest file restore operation, but the attach disk operation fails even though VMware tools is running and the Guest OS credentials are correct. If this occurs, the following error is returned:

```
Error while validating guest credentials, failed to access guest system using
specified credentials: Verify VMWare tools is running properly on system and
account used is Administrator account, Error is SystemError vix error codes =
(3016, 0).
```

To correct the issue, restart the VMware Tools Windows service on the Guest OS, and then retry the guest file restore operation.

Guest email shows ?????? for the file name

This issue occurs when you use the guest file restore feature to restore files or folders with non-English characters in the names and the email notification displays "??????" for the restored file names. The email attachment correctly lists the names of the restored files and folders.

Backups are not detached after guest file restore session is discontinued

This issue occurs when you perform a guest file restore operation from a VM-consistent backup. While the guest file restore session is active, another VM-consistent backup is performed for the same VM. When the guest file restore session is disconnected, either manually or automatically after 24 hours, the backups for the session are not detached.

To correct the issue, manually detach the VMDKs that were attached from the active guest file restore session.

Manage SnapCenter Plug-in for VMware vSphere appliance

Restart the VMware vSphere client service

If the SnapCenter VMware vSphere client starts to behave incorrectly, you might need to clear the browser cache. If the problem persists, then restart the web client service.

Restart the VMware vSphere client service in a Linux vCenter

Before you begin

You must be running vCenter 7.0U1 or later.

Steps

1. Use SSH to log in to the vCenter Server Appliance as root.
2. Access the Appliance Shell or BASH Shell by using the following command:

   ```
   shell
   ```

3. Stop the web client service by using the following HTML5 command:

   ```
   service-control --stop vsphere-ui
   ```

4. Delete all stale HTML5 scvm packages on vCenter by using the following shell command:

   ```
   etc/vmware/vsphere-ui/vc-packages/vsphere-client-serenity/

   rm -rf com.netapp.scv.client-<version_number>
   ```

   Do not remove the VASA or vCenter 7.x and later packages.

5. Start the web client service by using the following HTML5 command:

   ```
   service-control --start vsphere-ui
   ```

Access the maintenance console

You can manage your application, system, and network configurations using the maintenance console for SnapCenter Plug-in for VMware vSphere. You can change your administrator password, maintenance password, generate support bundles, and start remote diagnostics.

Before you begin

Before stopping and restarting SnapCenter Plug-in for VMware vSphere service, you should suspend all schedules.

About this task

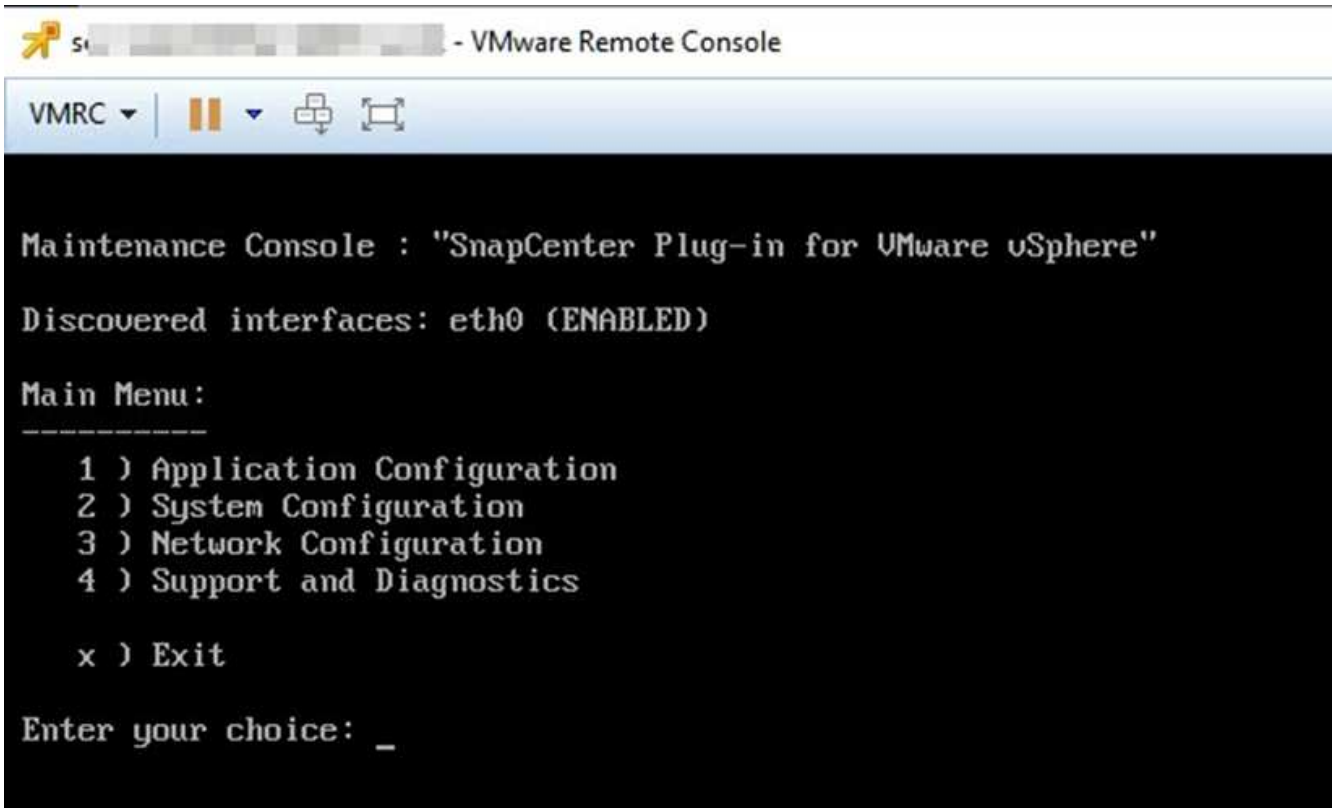
- In SnapCenter Plug-in for VMware vSphere 4.6P1, you must specify a password when you first install SnapCenter Plug-in for VMware vSphere. If you upgrade from release 4.6 or earlier to release 4.6P1 or later, the earlier default password is accepted.
- You must set a password for the “diag” user while enabling remote diagnostics.

  To obtain the root user permission to execute the command, use the sudo <command>.

Steps

1. From the VMware vSphere client, select the VM where SnapCenter Plug-in for VMware vSphere is located.
2. In the **Summary** tab of the virtual appliance select **Launch Remote Console** to open a maintenance console window.

   Log in using the default maintenance console username `maint` and password that you have set at the time of installation.



3. You can perform the following operations:
   - Option 1: Application Configuration

     Display a summary of SnapCenter Plug-in for VMware vSphere
     Start or stop SnapCenter Plug-in for VMware vSphere service
     Change login username or password for SnapCenter Plug-in for VMware vSphere
     Change MySQL password
     Backup and restore MySQL, configure and list MySQL backups

   - Option 2: System Configuration

     Reboot virtual machine
     Shut down virtual machine

Change 'maint' user password
Change time zone
Change NTP server
Enable SSH access
Increase jail disk size (/jail)
Upgrade
Install VMware Tools
Generate MFA Token

MFA is always enabled, you cannot disable MFA.

- Option 3: Network Configuration

  Display or change IP address settings
  Display or change domain name search settings
  Display or change static routes
  Commit changes
  Ping a host

- Option 4: Support and Diagnostics

  Generate support bundle
  Access diagnostic shell
  Enable remote diagnostic access
  Generate core dump bundle

Modify the SnapCenter Plug-in for VMware vSphere password from the maintenance console

If you do not know the admin password for the SnapCenter Plug-in for VMware vSphere management GUI, you can set a new password from the maintenance console.

Before you begin

Before stopping and restarting the SnapCenter Plug-in for VMware vSphere service, you should suspend all schedules.

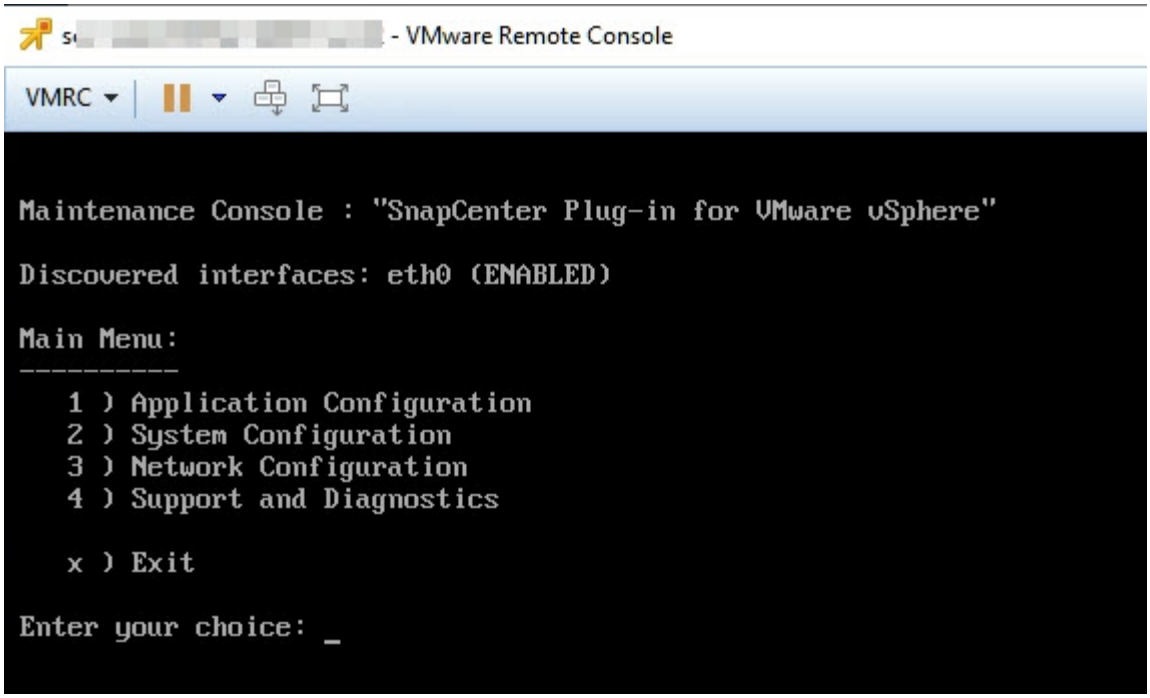
About this task

For information on accessing and logging on to the maintenance console, refer to Access the Maintenance Console.

Steps

1. From the VMware vSphere client, select the VM where the SnapCenter Plug-in for VMware vSphere is located.
2. In the **Summary** tab of the virtual appliance select **Launch Remote Console** to open a maintenance console window, and then log on.

   For information on accessing and logging on to the maintenance console, refer to Access the Maintenance Console.



3. Enter "**1**" for Application Configuration.
4. Enter "**4**" for Change username or password.
5. Enter the new password.

   The SnapCenter VMware virtual appliance service is stopped and restarted.

Create and import certificates

SnapCenter Plug-in for VMware vSphere employs SSL encryption for secure communication with the client browser. While this does enable encrypted data across the wire, creating a new self-signed certificate, or using your own Certificate Authority (CA) infrastructure or a third party CA, ensures that the certificate is unique for your environment.

Refer to KB article: How to create and/or import an SSL certificate to SnapCenter Plug-in for VMware vSphere for more information.

Unregister SnapCenter Plug-in for VMware vSphere from vCenter

If you stop the SnapCenter Plug-in for VMware vSphere service in a vCenter that is in Linked Mode, resource groups are not available in all the linked vCenters, even when the SnapCenter Plug-in for VMware vSphere service is running in the other linked vCenters.

You must unregister the SnapCenter Plug-in for VMware vSphere extensions manually.

Steps

1. On the linked vCenter that has the SnapCenter Plug-in for VMware vSphere service stopped, navigate to

the Managed Object Reference (MOB) manager.

2. In the Properties option, select **content** in the Value column, then in the next screen select **ExtensionManager** in the Value column to display a list of the registered extensions.
3. Unregister the extensions `com.netapp.scv.client` and `com.netapp.aegis`.

Disable and enable SnapCenter Plug-in for VMware vSphere

If you no longer need the SnapCenter data protection features, you must change the configuration of the SnapCenter Plug-in for VMware vSphere. For example, if you deployed the plug-in in a test environment, you might need to disable the SnapCenter features in that environment and enable them in a production environment.

Before you begin

- You must have administrator privileges.
- Make sure that no SnapCenter jobs are running.

About this task

When you disable the SnapCenter Plug-in for VMware vSphere, all resource groups are suspended and the plug-in is unregistered as an extension in vCenter.

When you enable the SnapCenter Plug-in for VMware vSphere, the plug-in is registered as an extension in vCenter, all resource groups are in production mode, and all schedules are enabled.

Steps

1. Optional: Back up the SnapCenter Plug-in for VMware vSphere MySQL repository in case you want to restore it to a new virtual appliance.

   Back up the SnapCenter Plug-in for VMware vSphere MySQL database.

2. Log in to the SnapCenter Plug-in for VMware vSphere management GUI using the format `https://<OVA-IP-address>:8080`. Login with the admin username and password set at the time of deployment and the MFA token generated using the maintenance console.

   The IP address of the SnapCenter Plug-in for VMware vSphere is displayed when you deploy the plug-in.

3. Select **Configuration** in the left navigation pane, and then unselect the Service option in the **Plug-in Details** section to disable the plug-in.
4. Confirm your choice.
   - If you only used the SnapCenter Plug-in for VMware vSphere to perform VM consistent backups

     The plug-in is disabled, and no further action is required.

   - If you used the SnapCenter Plug-in for VMware vSphere to perform application-consistent backups

     The plug-in is disabled and further cleanup is required.

     a. Log in to VMware vSphere.
     b. Power down the VM.
     c. In the left navigator screen, right-click the instance of the SnapCenter Plug-in for VMware vSphere

(the name of the `.ova` file that was used when the virtual appliance was deployed) and select **Delete from Disk**.

d. Log in to SnapCenter and remove the vSphere host.

Remove SnapCenter Plug-in for VMware vSphere

If you no longer need to use the SnapCenter data protection features, you must disable the SnapCenter Plug-in for VMware vSphere to unregister it from vCenter, then remove the SnapCenter Plug-in for VMware vSphere from vCenter, and then manually delete leftover files.

Before you begin

- You must have administrator privileges.
- Make sure that no SnapCenter jobs are running.

Steps

1. Log in to the SnapCenter Plug-in for VMware vSphere management GUI using the format `https://<OVA-IP-address>:8080`.

   The IP address of the SnapCenter Plug-in for VMware vSphere is displayed when you deploy the plug-in.

2. Select **Configuration** in the left navigation pane, and then unselect the Service option in the **Plug-in Details** section to disable the plug-in.
3. Log in to VMware vSphere.
4. In the left navigator screen, right-click the instance of the SnapCenter Plug-in for VMware vSphere (the name of the `.tar` file that was used when the virtual appliance was deployed) and select **Delete from Disk**.
5. If you used the SnapCenter Plug-in for VMware vSphere to support other SnapCenter plug-ins for application-consistent backups, log in to SnapCenter and remove the vSphere host.

After you finish

The virtual appliance is still deployed but the SnapCenter Plug-in for VMware vSphere is removed.

After removing the host VM for the SnapCenter Plug-in for VMware vSphere, the plug-in might remain listed in vCenter until the local vCenter cache is refreshed. However, because the plug-in was removed, no SnapCenter VMware vSphere operations can be performed on that host. If you want to refresh the local vCenter cache, first make sure the appliance is in a Disabled state on the SnapCenter Plug-in for VMware vSphere Configuration page, and then restart the vCenter web client service.

Manage your configuration

Modify the time zones for backups

When you configure a backup schedule for a SnapCenter Plug-in for VMware vSphere resource group, the schedule is automatically set for the time zone in which SnapCenter Plug-in for VMware vSphere is deployed. You can modify that time zone by using the SnapCenter Plug-in for VMware vSphere management GUI or maintenance console.

Before you begin

You must know the IP address and the log in credentials for the SnapCenter Plug-in for VMware vSphere management GUI. You must also note down the MFA token generated from the maintenance console.

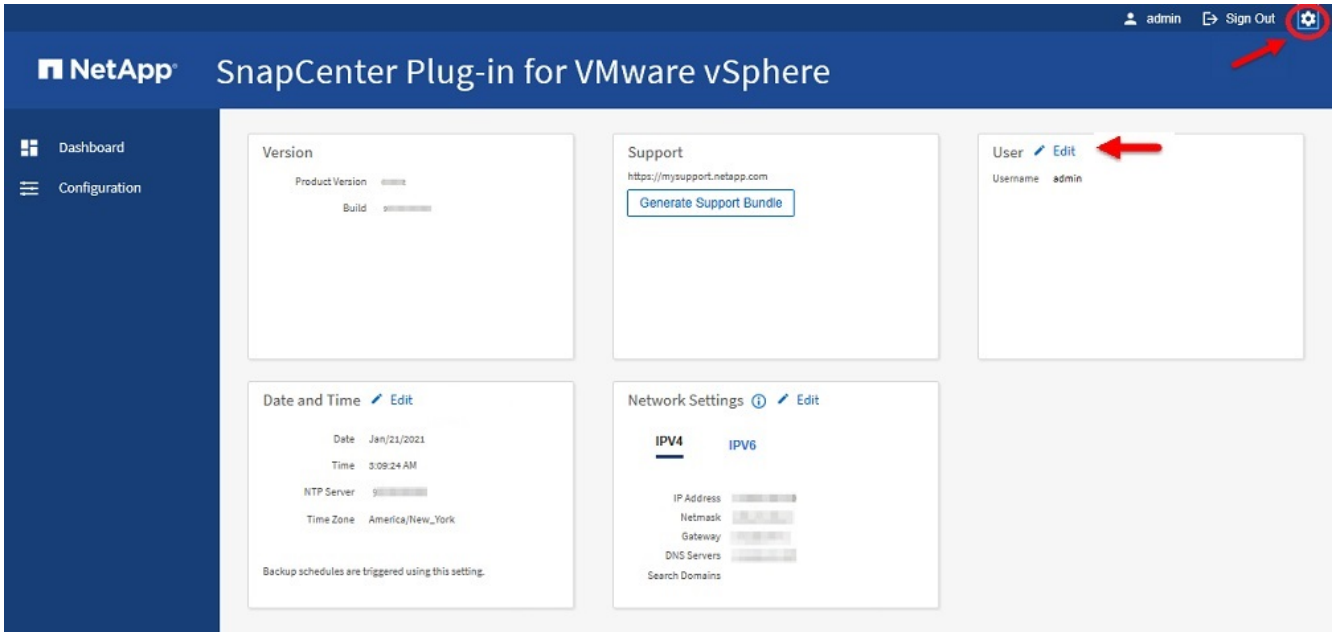
- The IP address was displayed when the SnapCenter Plug-in for VMware vSphere was deployed.
- Use the log in credentials provided during the deployment of the SnapCenter Plug-in for VMware vSphere or as later modified.
- Generate a 6-digit MFA token using the maintenance console System Configuration options.

Steps

1. Log in to the SnapCenter Plug-in for VMware vSphere management GUI.

   Use the format `https://<appliance-IP-address>:8080`

2. Select the Settings icon in the top toolbar.



3. On the **Settings** page, in the **Date and Time** section, select **Edit**.
4. Select the new time zone and select **Save**.

   The new time zone will be used for all backups performed by the SnapCenter Plug-in for VMware vSphere.

Modify the logon credentials

You can modify the logon credentials for the SnapCenter Plug-in for VMware vSphere management GUI.

Before you begin

You must know the IP address and the log on credentials for the SnapCenter Plug-in for VMware vSphere management GUI. You must also note down the MFA token generated from the maintenance console.

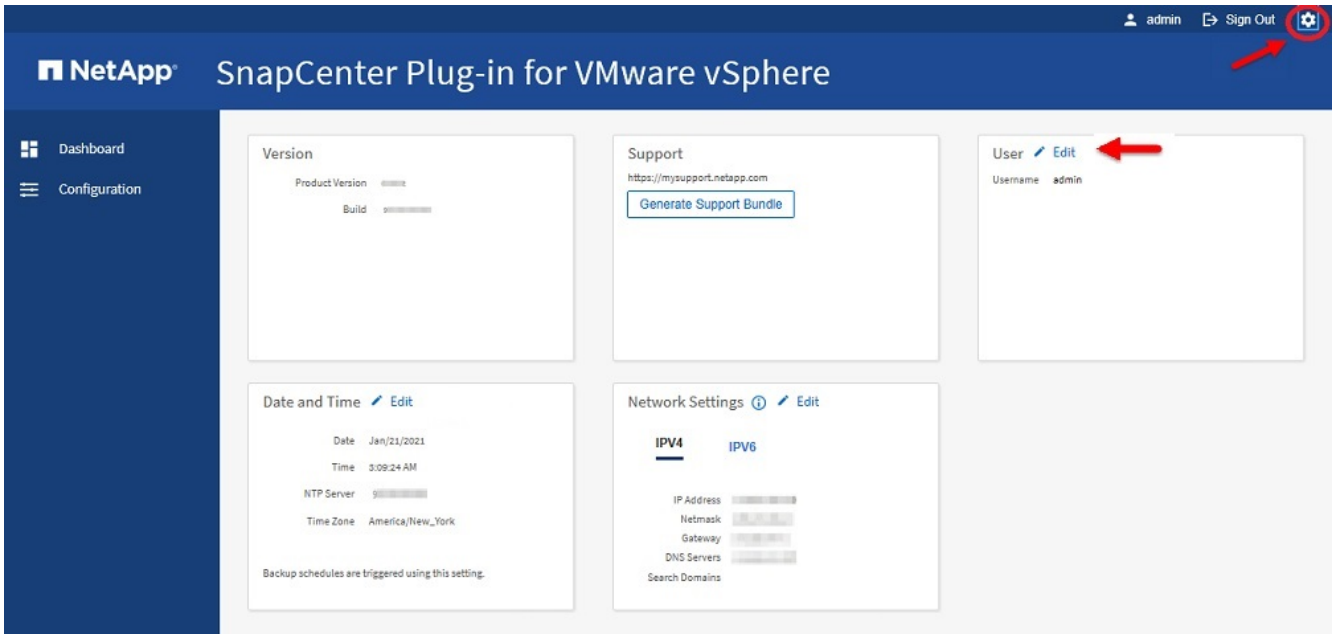
- The IP address was displayed when the SnapCenter Plug-in for VMware vSphere was deployed.
- Use the log in credentials provided during the deployment of the SnapCenter Plug-in for VMware vSphere or as later modified.
- Generate a 6-digit MFA token using the maintenance console System Configuration options.

Steps

1. Log in to the SnapCenter Plug-in for VMware vSphere management GUI.

   Use the format `https://<appliance-IP-address>:8080`

2. Select the Settings icon in the top toolbar.



3. On the **Settings** page, in the **User** section, select **Edit**.
4. Enter the new password and select **Save**.

   It might take several minutes before all the services come back up.

Modify the vCenter logon credentials

You can modify the vCenter logon credentials that are configured in SnapCenter Plug-in for VMware vSphere. These settings are used by the plug-in to access vCenter.
When you change the vCenter password, you need to unregister ONTAP tools for

VMware vSphere and re-registered it with the new password for the vVol backups to work seamlessly.

Before you begin

You must know the IP address and the log on credentials for the SnapCenter Plug-in for VMware vSphere management GUI. You must also note down the MFA token generated from the maintenance console.

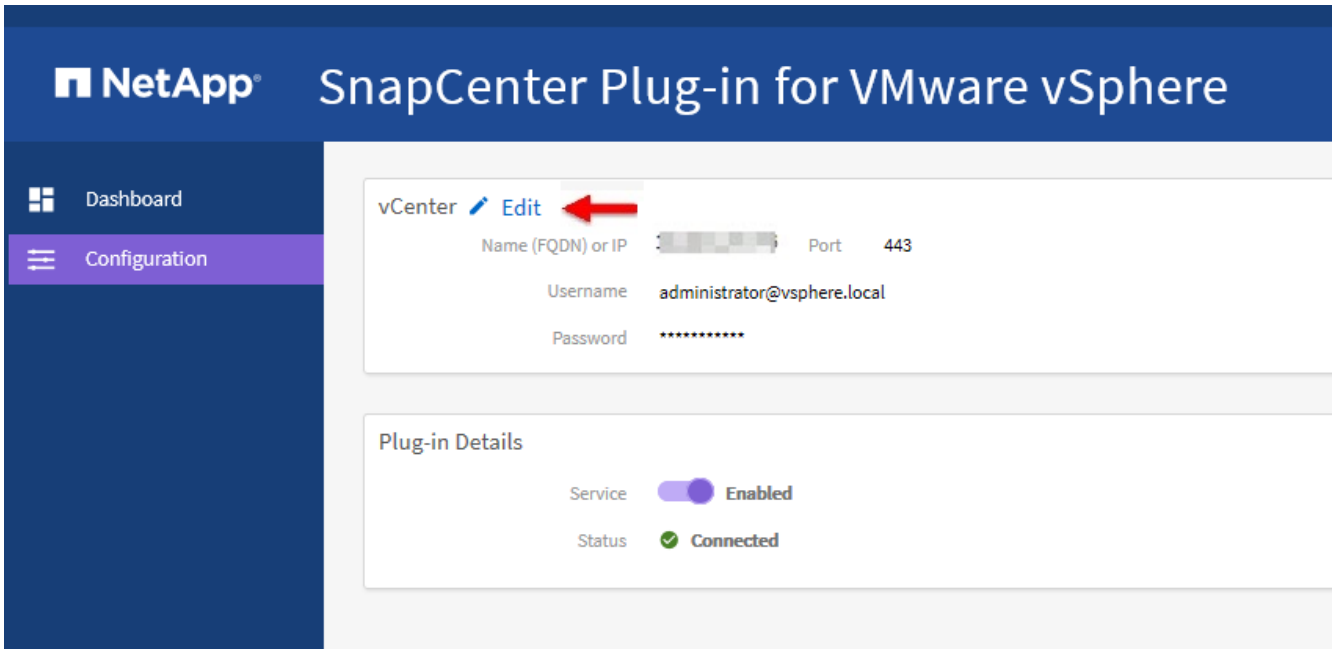
- The IP address was displayed when the SnapCenter Plug-in for VMware vSphere was deployed.
- Use the log in credentials provided during the deployment of the SnapCenter Plug-in for VMware vSphere or as later modified.
- Generate a 6-digit MFA token using the maintenance console System Configuration options.

Steps

1. Log in to the SnapCenter Plug-in for VMware vSphere management GUI.

   Use the format `https://<appliance-IP-address>:8080`

2. In the left navigation pane, select **Configuration**.



3. On the **Configuration** page, in the **vCenter** section, select **Edit**.
4. Enter the new password and then select **Save**.

   Do not modify the port number.

Modify the network settings

You can modify the network settings that are configured in SnapCenter Plug-in for VMware vSphere. These settings are used by the plug-in to access vCenter.

Before you begin

You must know the IP address and the log on credentials for the SnapCenter Plug-in for VMware vSphere

management GUI. You must also note down the MFA token generated from the maintenance console.

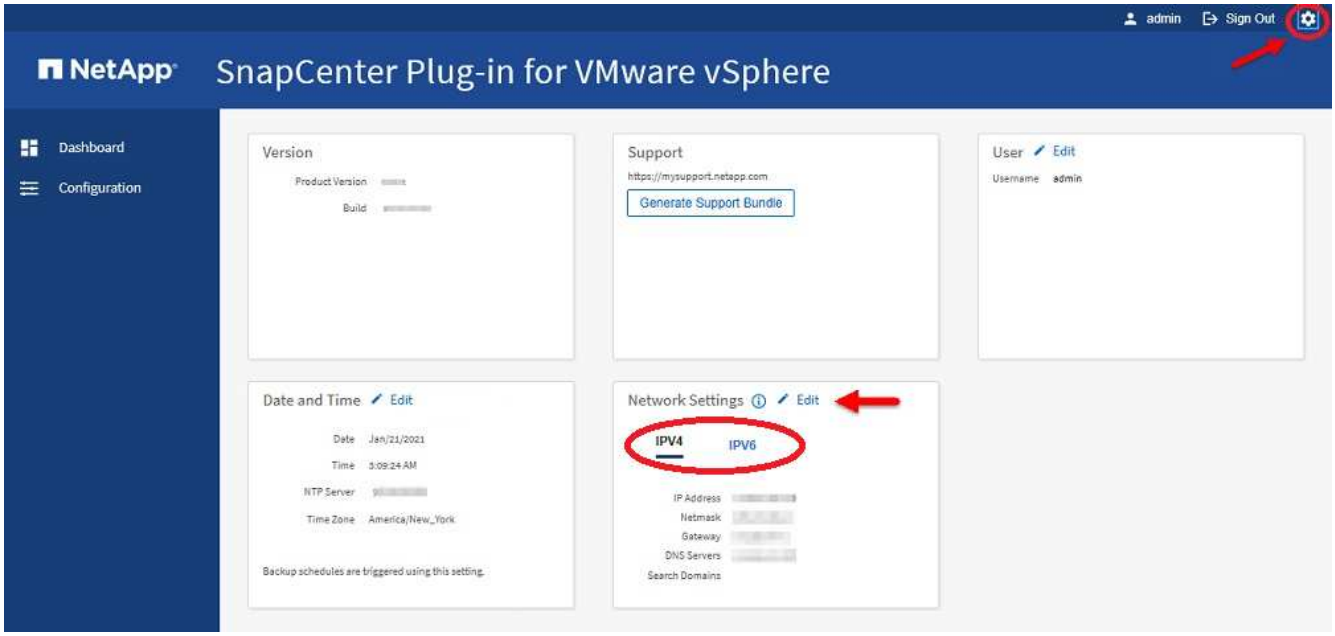
- The IP address was displayed when the SnapCenter Plug-in for VMware vSphere was deployed.
- Use the log in credentials provided during the deployment of the SnapCenter Plug-in for VMware vSphere or as later modified.
- Generate a 6-digit MFA token using the maintenance console System Configuration options.

Steps

1. Log in to the SnapCenter Plug-in for VMware vSphere management GUI.

   Use the format `https://<appliance-IP-address>:8080`

2. Select the Settings icon in the top toolbar.



3. On the **Settings** page, in the **Network Settings** section, select **IPv4** or **IPv6** address, and then select **Edit**.

   Enter the new information and select **Save**.

4. If you are removing a network setting, do the following:
   - IPv4: In the **IP Address** field, enter `0.0.0.0` and then select **Save**.
   - IPv6: In the **IP Address** field: enter `: :0` and then select **Save**.

> If you are using both IPv4 and IPv6 addresses, you cannot remove both network settings. The remaining network must specify the DNS Servers and Search Domains fields.

Modify configuration default values

To improve operational efficiency, you can modify the `scbr.override` configuration file to change default values. These values control settings such as the number of VMware snapshots that are created or deleted during a backup or the amount of time before a backup script stops running.

The `scbr.override` configuration file is used by the SnapCenter Plug-in for VMware vSphere in environments that support SnapCenter application-based data protection operations. If this file does not exist, then you must create it from the template file.

Create the scbr.override configuration file

The `scbr.override` configuration file is used by the SnapCenter Plug-in for VMware vSphere in environments that support SnapCenter application-based data protection operations.

1. Go to `/opt/netapp/scvservice/standalone_aegis/etc/scbr/scbr.override-template`.
2. Copy the `scbr.override-template` file to a new file called `scbr.override` in the `\opt\netapp\scvservice\standalone_aegis\etc\scbr` directory.

Properties you can override

You can use properties that are listed in the `scbr.override` configuration file to change default values.

- By default, the template uses hash symbol to comment the configuration properties. To use a property to modify a configuration value, you must remove the # characters.
- You must restart the service on the SnapCenter Plug-in for VMware vSphere host for the changes to take effect.

You can use the following properties that are listed in the `scbr.override` configuration file to change default values.

- **dashboard.protected.vm.count.interval=7**

  Specifies the number of days for which the dashboard displays VM protection status.

  The default value is "7".

- **disable.weakCiphers=true**

  Disables the following weakCiphers for the communication channel between SnapCenter Plug-in for VMware vSphere and SnapCenter, and any additional weakCiphers that are listed in `include.weakCiphers`:
  TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_128_GCM_SHA256
  TLS_RSA_WITH_AES_256_GCM_SHA384

- **global.ds.exclusion.pattern**

  Specifies one or more traditional or vVol datastores to be excluded from backup operations. You can specify the datastores using any valid Java regular expression.

  Example 1: The expression `global.ds.exclusion.pattern=.*21` excludes datastores that have a common pattern; for example `datastore21` and `dstest21` would be excluded.

Example 2: The expression `global.ds.exclusion.pattern=ds-.*|^vol123` excludes all datastores that contain `ds-` (for example `scvds-test`) or begin with `vol123`.

- **guestFileRestore.guest.operation.interval=5**

  Specifies the time interval, in seconds, that SnapCenter Plug-in for VMware vSphere monitors for completion of guest operations on the guest (Online Disk and Restore Files). The total wait time is set by `guestFileRestore.online.disk.timeout` and `guestFileRestore.restore.files.timeout`.

  The default value is "5".

- **guestFileRestore.monitorInterval=30**

  Specifies the time interval, in minutes, that the SnapCenter Plug-in for VMware vSphere monitors for expired guest file restore sessions. Any session that is running beyond the configured session time is disconnected.

  The default value is "30".

- **guestFileRestore.online.disk.timeout=100**

  Specifies the time, in seconds, that the SnapCenter Plug-in for VMware vSphere waits for an online disk operation on a guest VM to complete. Note that there is an additional 30-second wait time before the plug-in polls for completion of the online disk operation.

  The default value is "100".

- **guestFileRestore.restore.files.timeout=3600**

  Specifies the time, in seconds, that the SnapCenter Plug-in for VMware vSphere waits for a restore files operation on a guest VM to complete. If the time is exceeded, the process is ended and the job is marked as failed.

  The default value is "3600" (1 hour).

- **guestFileRestore.robocopy.directory.flags=/R:0 /W:0 /ZB /CopyAll /EFSRAW /A-:SH /e /NJH /NDL /NP**

  Specifies the extra robocopy flags to use when copying directories during guest file restore operations.

  Do not remove `/NJH` or add `/NJS` because this will break the parsing of the restore output.

  Do not allow unlimited retries (by removing the `/R` flag) because this might cause endless retries for failed copies.

  The default values are "`/R:0 /W:0 /ZB /CopyAll /EFSRAW /A-:SH /e /NJH /NDL /NP`".

- **guestFileRestore.robocopy.file.flags=/R:0 /W:0 /ZB /CopyAll /EFSRAW /A-:SH /NJH /NDL /NP**

  Specifies the extra robocopy flags to use when copying individual files during guest file restore operations.

  Do not remove `/NJH` or add `/NJS` because this will break the parsing of the restore output.

  Do not allow unlimited retries (by removing the `/R` flag) because this might cause endless retries for failed copies.

The default values are "`/R:0 /W:0 /ZB /CopyAll /EFSRAW /A-:SH /NJH /NDL /NP`".

- **guestFileRestore.sessionTime=1440**

  Specifies the time, in minutes, that SnapCenter Plug-in for VMware vSphere keeps a guest file restore session active.

  The default value is "1440" (24 hours).

- **guestFileRestore.use.custom.online.disk.script=true**

  Specifies whether to use a custom script for onlining disks and retrieving drive letters when creating guest file restore sessions. The script must be located at `[Install Path] \etc\guestFileRestore_onlineDisk.ps1`. A default script is provided with the installation. The values `[Disk_Serial_Number]`, `[Online_Disk_Output]`, and `[Drive_Output]` are replaced in the script during the attach process.

  The default value is "false".

- **include.esx.initiator.id.from.cluster=true**

  Specifies that the SnapCenter Plug-in for VMware vSphere should include iSCSI and FCP initiator IDs from all the ESXi hosts in the cluster in the application over VMDK workflows.

  The default value is "false".

- **include.weakCiphers**

  When `disable.weakCiphers` is set to `true`, specifies the weak ciphers that you want to be disabled in addition to the weak ciphers that `disable.weakCiphers` disables by default.

- **max.concurrent.ds.storage.query.count=15**

  Specifies the maximum number of concurrent calls that the SnapCenter Plug-in for VMware vSphere can make to the SnapCenter Server to discover the storage footprint for the datastores. The plug-in makes these calls when you restart the Linux service on the SnapCenter Plug-in for VMware vSphere VM host.

- **nfs.datastore.mount.retry.count=3**

  Specifies the maximum number of times the SnapCenter Plug-in for VMware vSphere tries to mount a volume as a NFS Datastore in vCenter.

  The default value is "3".

- **nfs.datastore.mount.retry.delay=60000**

  Specifies the time, in milliseconds, that the SnapCenter Plug-in for VMware vSphere waits between attempts to mount a volume as a NFS Datastore in vCenter.

  The default value is "60000" (60 seconds).

- **script.virtual.machine.count.variable.name= VIRTUAL_MACHINES**

  Specifies the environmental variable name that contains the virtual machine count. You must define the variable before you execute any user-defined scripts during a backup job.

For example, VIRTUAL_MACHINES=2 means that two virtual machines are being backed up.

- **script.virtual.machine.info.variable.name=VIRTUAL_MACHINE.%s**

  Provides the name of the environmental variable that contains information about the nth virtual machine in the backup. You must set this variable before executing any user defined scripts during a backup.

  For example, the environmental variable VIRTUAL_MACHINE.2 provides information about the second virtual machine in the backup.

- **script.virtual.machine.info.format= %s|%s|%s|%s|%s**

  Provides information about the virtual machine. The format for this information, which is set in the environment variable, is the following: `VM name|VM UUID| VM power state (on|off)|VM snapshot taken (true|false)|IP address(es)`

  The following is an example of the information you might provide:

  ```
  VIRTUAL_MACHINE.2=VM 1|564d6769-f07d-6e3b-
  68b1f3c29ba03a9a|POWERED_ON||true|10.0.4.2
  ```

- **storage.connection.timeout=600000**

  Specifies the amount of time, in milliseconds, that the SnapCenter Server waits for a response from the storage system.

  The default value is "600000" (10 minutes).

- **vmware.esx.ip.kernel.ip.map**

  There is no default value. You use this value to map the ESXi host IP address to the VMkernel IP address. By default, the SnapCenter Plug-in for VMware vSphere uses the management VMkernel adapter IP address of the ESXi host. If you want the SnapCenter Plug-in for VMware vSphere to use a different VMkernel adapter IP address, you must provide an override value.

  In the following example, the management VMkernel adapter IP address is 10.225.10.56; however, the SnapCenter Plug-in for VMware vSphere uses the specified address of 10.225.11.57 and 10.225.11.58. And if the management VMkernel adapter IP address is 10.225.10.60, the plug-in uses the address 10.225.11.61.

  ```
  vmware.esx.ip.kernel.ip.map=10.225.10.56:10.225.11.57,10.225.11.58;
  10.225.10.60:10.225.11.61
  ```

- **vmware.max.concurrent.snapshots=30**

  Specifies the maximum number of concurrent VMware snapshots that the SnapCenter Plug-in for VMware vSphere performs on the server.

  This number is checked on a per datastore basis and is checked only if the policy has "VM consistent" selected. If you are performing crash-consistent backups, this setting does not apply.

  The default value is "30".

- **vmware.max.concurrent.snapshots.delete=30**

Specifies the maximum number of concurrent VMware snapshot delete operations, per datastore, that the SnapCenter Plug-in for VMware vSphere performs on the server.

This number is checked on a per datastore basis.

The default value is "30".

- **vmware.query.unresolved.retry.count=10**

  Specifies the maximum number of times the SnapCenter Plug-in for VMware vSphere retries sending a query about unresolved volumes because of "…time limit for holding off I/O…" errors.

  The default value is "10".

- **vmware.quiesce.retry.count=0**

  Specifies the maximum number of times the SnapCenter Plug-in for VMware vSphere retries sending a query about VMware snapshots because of "…time limit for holding off I/O…" errors during a backup.

  The default value is "0".

- **vmware.quiesce.retry.interval=5**

  Specifies the amount of time, in seconds, that the SnapCenter Plug-in for VMware vSphere waits between sending the queries regarding VMware snapshot "…time limit for holding off I/O…" errors during a backup.

  The default value is "5".

- **vmware.query.unresolved.retry.delay= 60000**

  Specifies the amount of time, in milliseconds, that the SnapCenter Plug-in for VMware vSphere waits between sending the queries regarding unresolved volumes because of "…time limit for holding off I/O…" errors. This error occurs when cloning a VMFS datastore.

  The default value is "60000" (60 seconds).

- **vmware.reconfig.vm.retry.count=10**

  Specifies the maximum number of times the SnapCenter Plug-in for VMware vSphere retries sending a query about reconfiguring a VM because of "…time limit for holding off I/O…" errors.

  The default value is "10".

- **vmware.reconfig.vm.retry.delay=30000**

  Specifies the maximum time, in milliseconds, that the SnapCenter Plug-in for VMware vSphere waits between sending queries regarding reconfiguring a VM because of "…time limit for holding off I/O…" errors.

  The default value is "30000" (30 seconds).

- **vmware.rescan.hba.retry.count=3**

  Specifies the amount of time, in milliseconds, that the SnapCenter Plug-in for VMware vSphere waits between sending the queries regarding rescanning the host bus adapter because of "…time limit for holding off I/O…" errors.

The default value is "3".

- **vmware.rescan.hba.retry.delay=30000**

  Specifies the maximum number of times the SnapCenter Plug-in for VMware vSphere retries requests to rescan the host bus adapter.

  The default value is "30000".

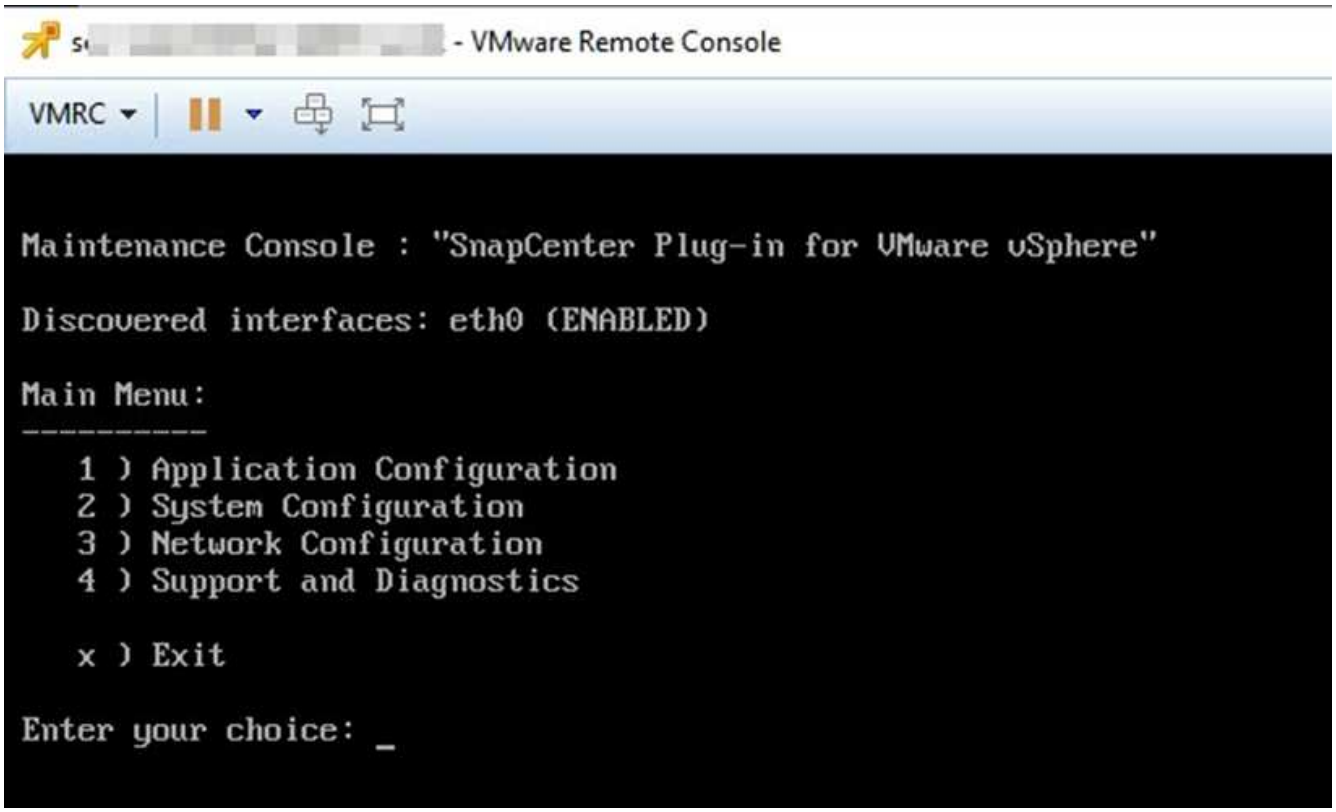
Enable SSH for SnapCenter Plug-in for VMware vSphere

When the SnapCenter Plug-in for VMware vSphere is deployed, SSH is disabled by default.

Steps

1. From the VMware vSphere client, select the VM where the SnapCenter Plug-in for VMware vSphere is located.
2. In the **Summary** tab of the virtual appliance select **Launch Remote Console** to open a maintenance console window, and then log on.

   For information on accessing and logging on to the maintenance console, refer to Access the Maintenance Console.



3. From the Main Menu, select menu option **2) System Configuration**.
4. From the System Configuration Menu, select menu option **6) Enable SSH access** and then enter “**y**” at the confirmation prompt.
5. Wait for the message “Enabling SSH Access…” then press **Enter** to continue, and then enter **X** at the

prompt to exit Maintenance Mode.

REST APIs

Overview

You can use the SnapCenter Plug-in for VMware vSphere REST APIs to perform common data protection operations. The plug-in has different Swagger web pages from the Windows SnapCenter Swagger web pages.

- REST API workflows are documented for the following operations on VMs and datastores using the REST APIs for VMware vSphere:
  - Add, modify, and delete storage VMs and clusters
  - Create, modify, and delete resource groups
  - Backup VMs, scheduled and on-demand
  - Restore existing VMs and deleted VMs
  - Restore VMDKs
  - Attach and detach VMDKs
  - Mount and unmount datastores
  - Download jobs and generate reports
  - Modify built-in schedules
  - Configure secondary protection for ASA r2
- Operations that are not supported by the REST APIs for VMware vSphere
  - Guest file restore
  - Installation and configuration of the SnapCenter Plug-in for VMware vSphere
  - Assign RBAC roles or access to users
- `uri` parameter

  The `uri` parameter always returns a "null" value.

- Login timeout

  The default timeout is 120 minutes (2 hours). You can configure a different timeout value in the vCenter settings.

- Token management

  For security, REST APIs use a mandatory token that is passed with each request and is used in all API calls for client validation. The REST APIs for VMware vSphere use the VMware authentication API to obtain the token. VMware provides the token management.

  To obtain the token, use `/4.1/auth/login` REST API and provide the vCenter credentials.

- API version designations

  Each REST API name includes the SnapCenter version number in which the REST API was first released. For example, the REST API `/4.1/datastores/{moref}/backups` was first released in SnapCenter

4.1.

REST APIs in future releases will usually be backward compatible and will be modified to accommodate new features as needed.

Access REST APIs using the Swagger API web page

REST APIs are exposed through the Swagger web page. You can access the Swagger web page to display either the SnapCenter Server or the SnapCenter Plug-in for VMware vSphere REST APIs, as well as to manually issue an API call. Use SnapCenter Plug-in for VMware vSphere REST APIs to perform operations on VMs and datastores.

The plug-in has different Swagger web pages from the SnapCenter Server Swagger web pages.

Before you begin

For SnapCenter Plug-in for VMware vSphere REST APIs, you must know either the IP address or the host name of SnapCenter Plug-in for VMware vSphere.

The plug-in only supports REST APIs for the purpose of integrating with third party applications and does not support PowerShell cmdlets or a CLI.

Steps

1. From a browser, enter the URL to access the plug-in Swagger web page:

   `https://<SCV_IP>:8144/api/swagger-ui/index.html`

   Do not use the following characters in the REST API URL: +, . , %, and &.

   Example

   Access SnapCenter Plug-in for VMware vSphere REST APIs:

   `https://<SCV_IP>:8144/api/swagger-ui/index.html`

   `https://OVAhost:8144/api/swagger-ui/index.html`

   Log in use the vCenter authentication mechanism to generate the token.

2. Select an API resource type to display the APIs in that resource type.

REST API workflows to add and modify storage VMs

To perform add and modify storage VM operations using the SnapCenter Plug-in for VMware vSphere REST APIs, you must follow the prescribed sequence of REST API calls.

For each REST API, add `https://<server>:<port>` at the front of the REST API to form a complete endpoint.

To add storage VM operations, follow this workflow:

Step	REST API	Comments
1	`/4.1/storage-system`	`Add Storage System` adds the specified storage VM to SnapCenter Plug-in for VMware vSphere.

To modify storage VM operations, follow this workflow:

Step	REST API	Comments
1	`/4.1/storage-system`	`getSvmAll` gets the list of all available storage VMs. Note the **name** of the storage VM that you want to modify.
2	`/4.1/storage-system`	`Modify Storage System` modifies the specified storage VM. Pass the **name** from Step 1 in addition to all the other required attributes.

REST API workflows to create and modify resource groups

To perform create and modify resource group operations using the SnapCenter Plug-in for VMware vSphere REST APIs, you must follow the prescribed sequence of REST API calls.

For each REST API, add `https://<server>:<port>` at the front of the REST API to form a complete endpoint.

To create resource groups, follow this workflow:

Step	REST API	Comments
1	`/4.1/policies`	`Get Policies` gets the list of VMware vSphere client policies. Note the **policyId** that you want to use when creating the resource group and the policy **frequency**. If no policies are listed, then use the `Create Policy` REST API to create a new policy.
2	`/4.1/resource-groups`	`Create a Resource Group` creates a resource group with the specified policy. Pass the **policyId** from Step 1 and enter the policy **frequency** details in addition to all other required attributes. You can enable secondary protection using this REST API.

To modify resource groups, follow this workflow:

Step	REST API	Comments
1	`/4.1/resource-groups`	`Get List of Resource Groups` gets the list of VMware vSphere client resource groups. Note the **resourceGroupId** that you want to modify.
2	`/4.1/policies`	If you want to modify the assigned policies, `Get Policies` gets the list of VMware vSphere client policies. Note the **policyId** that you want to use when modifying the resource group and the policy **frequency**.
3	`/4.1/resource-groups/{resouceGroupId}`	`Update a Resource Group` modifies the specified resource group. Pass the **resourceGroupId** from Step 1. Optionally, pass the **policyId** from Step 2 and enter the **frequency** details in addition to all other required attributes.

REST API workflow to back up on demand

To perform backup operations on demand using the SnapCenter Plug-in for VMware vSphere REST APIs, you must follow the prescribed sequence of REST API calls.

For each REST API, add `https://<server>:<port>` at the front of the REST API to form a complete endpoint.

Step	REST API	Comments
1	`/4.1/resource-groups`	`Get List of Resource Groups` gets the list of VMware vSphere client resource groups. Note the **resourceGroupId** and the **policyId** for the resource group you want to back up.
2	`/4.1/resource-groups/backupnow`	`Run a backup on a Resource Group` backs up the resource group on demand. Pass the **resourceGroupId** and the **policyId** from Step 1.

REST API workflow to restore VMs

To perform restore operations for VM backups using the SnapCenter Plug-in for VMware vSphere REST APIs, you must follow the prescribed sequence of REST API calls.

For each REST API, add `https://<server>:<port>` at the front of the REST API to form a complete endpoint.

Step	REST API	Comments
1	Go to `http://<vCenter-IP>/mob`	Find the VM moref from the VMware Managed Objects URL. Note the **moref** for the VM that you want to restore.
2	`/4.1/vm/{moref}/backups`	`Get VM Backups` gets a list of backups for the specified VM. Pass the **moref** from Step 1. Note the **backupId** of the backup you want to restore.
3	`/4.1/vm/backups/{backupId}/snapshotlocations`	`Get snapshot locations` gets the location of the snapshot for the specified backup. Pass the **backupId** from Step 2. Note the **snapshotLocationsList** information.
4	`/4.1/vm/{moref}/backups/availableesxhosts`	`Get available ESX Hosts` gets the information for the host on which the backup is stored. Note the **availableEsxHostsList** information.
5	`/4.1/vm/{moref}/backups/{backupId}/restore`	`Restore a VM from a backup` restores the specified backup. Pass the information from Steps 3 and 4 in the **restoreLocations** attribute. If the VM backup is a partial backup, set the `restartVM` parameter to "false". You cannot restore a VM that is a template.

REST API workflow to restore deleted VMs

To perform restore operations for VM backups using the SnapCenter Plug-in for VMware

vSphere REST APIs, you must follow the prescribed sequence of REST API calls.

For each REST API, add `https://<server>:<port>` at the front of the REST API to form a complete endpoint.

Step	REST API	Comments
1	Go to `http://<vCenter-IP>/mob`	Find the VM UUID from the VMware Managed Objects URL. Note the **uuid** for the VM that you want to restore.
2	`/4.1/vm/{uuid}/backups`	`Get VM Backups` gets a list of backups for the specified VM. Pass the **uuid** from Step 1. Note the **backupId** of the backup you want to restore.
3	`/4.1/vm/backups/{backupId}/snapshotlocations`	`Get snapshot locations` gets the location of the snapshot for the specified backup. Pass the **backupId** from Step 2. Note the **snapshotLocationsList** information.
4	`/4.1/vm/{moref}/backups/availableesxhosts`	`Get available ESX Hosts` gets the information for the host on which the backup is stored. Note the **availableEsxHostsList** information.
5	`/4.1/vm/{uuid}/backups/{backupId}/restore`	`Restore VM from a backup using uuid or restore a deleted VM` restores the specified backup. Pass the **uuid** from Step 1. Pass the **backupId** from Step 2. Pass the information from Steps 3 and 4 in the **restoreLocations** attribute. If the VM backup is a partial backup, set the `restartVM` parameter to "false". **Note:** You cannot restore a VM that is a template.

REST API workflow to restore VMDKs

To perform restore operations for VMDKs using the SnapCenter Plug-in for VMware vSphere REST APIs, you must follow the prescribed sequence of REST API calls.

For each REST API, add `https://<server>:<port>` at the front of the REST API to form a complete endpoint.

Step	REST API	Comments
1	Go to `http://<vCenter-IP>/mob`	Find the VM moref from the VMware Managed Objects URL. Note the **moref** for the VM in which the VMDK is located.
2	`/4.1/vm/{moref}/backups`	`Get VM Backups` gets a list of backups for the specified VM. Pass the **moref** from Step 1. Note the **backupId** of the backup you want to restore.
3	`/4.1/vm/backups/{backupId}/snapshotlocations`	`Get snapshot locations` gets the location of the snapshot for the specified backup. Pass the **backupId** from Step 2. Note the **snapshotLocationsList** information.
4	`/4.1/vm/{moref}/backups/vmdklocations`	`Get Vmdk Locations` gets a list of VMDKs for the specified VM. Note the **vmdkLocationsList** information.
5	`/4.1/vm/{ moref}/backups/{backupId}/availabledatastores`	`Get Available Datastores` gets a list of datastores that are available for the restore operation. Pass the **moref** from Step 1. Pass the **backupId** from Step 2. Note the **DatastoreNameList** information.
6	`/4.1/vm/{moref}/backups/availableesxhosts`	`Get available ESX Hosts` gets the information for the host on which the backup is stored. Pass the **moref** from Step 1. Note the **availableEsxHostsList** information.

Step	REST API	Comments
7	`/4.1/vm/{moref}/backups/{backupId}/restorevmdks`	`Restore a VMDK from a backup` restores the specified VMDK from the specified backup. In the **esxHost** attribute, pass the information from **availableEsxHostsList** in Step 6. Pass the information from Steps 3 through 5 to the **vmdkRestoreLocations** attribute: • In the restoreFromLocation attribute, pass the information from snapshotLocationsList in Step 3. • In the vmdkToRestore attribute, pass the information from vmdkLocationsList in Step 4. • In the restoreToDatastore attribute, pass the information from DatastoreNameList in Step 5.

REST API workflows to attach and detach VMDKs

To perform attach and detach operations for VMDKs using the SnapCenter Plug-in for VMware vSphere REST APIs, you must follow the prescribed sequence of REST API calls.

For each REST API, add `https://<server>:<port>` at the front of the REST API to form a complete endpoint.

To attach VMDKs, follow this workflow:

Step	REST API	Comments
1	Go to `http://<vCenter-IP>/mob`	Find the VM moref from the VMware Managed Objects URL. Note the **moref** for the VM to which you want to attach a VMDK.
2	`/4.1/vm/{moref}/backups`	`Get VM Backups` gets a list of backups for the specified VM. Pass the **moref** from Step 1. Note the **backupId** of the backup you want to restore.

Step	REST API	Comments
3	`/4.1/vm/{moref}/backups/{backupId}/vmdklocations`	`Get VMDK Locations` gets a list of VMDKs for the specified VM. Pass the **backupId** from Step 2 and the **moref** from Step 1. Note the **vmdkLocationsList** information.
4	`/4.1/vm/{moref}/attachvmdks`	`Attach VMDKs` attaches the specified VMDK to the original VM. Pass the **backupId** from Step 2 and the **moref** from Step 1. Pass the **vmdkLocationsList** from Step 3 to the **vmdkLocations** attribute. To attach a VMDK to a different VM, pass the moref of the target VM in the alternateVmMoref attribute.

To detach VMDKs, follow this workflow:

Step	REST API	Comments
1	Go to `http://<vCenter-IP>/mob`	Find the VM moref from the VMware Managed Objects URL. Note the **moref** for the VM on which you want to detach a VMDK.
2	`/4.1/vm/{moref}/backups`	`Get VM Backups` gets a list of backups for the specified VM. Pass the **moref** from Step 1. Note the **backupId** of the backup you want to restore.
3	`/4.1/vm/{moref}/backups/{backupId}/vmdklocations`	`Get VMDK Locations` gets a list of VMDKs for the specified VM. Pass the **backupId** from Step 2 and the **moref** from Step 1. Note the **vmdkLocationsList** information.
4	`/4.1/vm/{moref}/detachvmdks`	`Detach VMDKs` detaches the specified VMDK. Pass the **moref** from Step 1. Pass the VMDK **vmdkLocationsList** details from Step 3 to the **vmdksToDetach** attribute.

REST API workflows to mount and unmount datastores

To perform mount and unmount operations for datastore backups using the SnapCenter Plug-in for VMware vSphere REST APIs, you must follow the prescribed sequence of REST API calls.

For each REST API, add `https://<server>:<port>` at the front of the REST API to form a complete endpoint.

To mount datastores, follow this workflow:

Step	REST API	Comments
1	Go to `http://<vCenter-IP>/mob`	Find the datastore moref from the VMware Managed Objects URL. Note the **moref** for the datastore that you want to mount.
2	`/4.1/datastores/{moref}/backups`	`Get the list of backups for a datastore` gets a list of backups for the specified datastore. Pass the **moref** from Step 1. Note the **backupId** that you want to mount.
3	`/4.1/datastores/backups/{backupId}/snapshotlocators`	`Get the list of Snapshot Locations` gets details about the location of the specified backup. Pass the **backupId** from Step 2. Note the **datastore** and the location from the **snapshotLocationsList** list.
4	`/4.1/datastores/{moref}/availableEsxHosts`	`Get the list of Available Esxi Hosts` gets the list of ESXi hosts that are available for mount operations. Pass the **moref** from Step 1. Note the **availableEsxHostsList** information.
5	`/4.1/datastores/backups/{backupId}/mount`	`Mount datastores for a backup` mounts the specified datastore backup. Pass the **backupId** from Step 2. In the **datastore** and **location** attributes, pass the information from `snapshotLocationsList` in Step 3. In the **esxHostName** attribute, pass the information from **availableEsxHostsList** in Step 4.

To unmount datastores, follow this workflow:

Step	REST API	Comments
1	`/4.1/datastores/backups/{backupId}/mounted`	`Get the list of mounted datastores.` Note the datastore **moref**(s) that you want to unmount.
2	`/4.1/datastores/unmount`	`UnMount datastores for a backup` unmounts the specified datastore backup. Pass the datastore **moref**(s) from Step 1.

REST APIs to download jobs and generate reports

To generate reports and download logs for VMware vSphere client jobs using the SnapCenter Plug-in for VMware vSphere REST APIs, you must use the REST API calls for VMware vSphere.

For each REST API, add `https://<server>:<port>` at the front of the REST API to form a complete endpoint.

Use the following REST APIs in the Jobs section to get detailed information on jobs:

REST API	Comments
`/4.1/jobs`	`Get all jobs` gets the job details for multiple jobs. You can narrow the scope of the request by specifying a job type, such as `backup`, `mountBackup`, or `restore`.
`/4.1/jobs/{id}`	`Get job details` gets detailed information for the specified job.

Use the following REST API in the Jobs section to download job logs:

REST API	Comments
`/4.1/jobs/{id}/logs`	`getJobLogsById` downloads the logs for the specified job.

Use the following REST APIs in the Reports section to generate reports:

REST API	Comments
`4.1/reports/protectedVM`	`Get Protected VM List` gets a list of the protected VMs during the last seven days.

REST API	Comments
`/4.1/reports/unProtectedVM`	`Get Unprotected VM List` gets a list of the unprotected VMs during the last seven days.

REST API workflow to modify built-in schedules

To modify built-in schedules for VMware vSphere client jobs using the SnapCenter Plug-in for VMware vSphere REST APIs, you must follow the prescribed sequence of REST API calls.

Built-in schedules are the schedules that are provided as part of the product; for example, the MySQL database dump schedule. You can modify the following schedules:
`Schedule-DatabaseDump`
`Schedule-PurgeBackups`
`Schedule-AsupDataCollection`
`Schedule-ComputeStorageSaving`
`Schedule-PurgeJobs`

For each REST API, add `https://<server>:<port>` at the front of the REST API to form a complete endpoint.

Step	REST API	Comments
1	`/4.1/schedules`	`Get all built-in schedules` gets a list of the job schedules that were originally provided in the product. Note the schedule name that you want to modify and the associated cron expression.
2	`/4.1/schedules`	`Modify any built-in schedule` changes the named schedule. Pass the schedule name from Step 1 and create a new cron expression for the schedule.

REST API to mark stuck jobs as failed

To find job IDs for VMware vSphere client jobs using the SnapCenter Plug-in for VMware vSphere REST APIs, you must use the REST API calls for VMware vSphere. These REST APIs were added in SnapCenter Plug-in for VMware vSphere 4.4.

For each REST API, add https://<server>:<port>` at the front of the REST API to form a complete endpoint.

Use the following REST API in the Jobs section to change jobs that are stuck in a running state to a failed state:

REST API	Comments
`/4.1/jobs/{id}/failJobs`	When you pass the IDs of jobs that are stuck in a running state, `failJobs` marks those jobs as failed. To identify jobs that are stuck in a running state, use the job monitor GUI to see the state of every job and the job ID.

REST APIs to generate audit logs

You can collect the audit log details from swagger rest APIs as well as the SCV plugin user interface.

Given below are the swagger rest APIs:

1. GET 4.1/audit/logs: Get audit data for all logs
2. GET 4.1/audit/logs/{filename}: Get audit data for a specific log file
3. POST 4.1/audit/verify: Trigger audit log verification.
4. GET 4.1/audit/config: Get the audit and syslog server config
5. PUT 4.1/audit/config: Update the audit and syslog server config

To generate audit logs for VMware vSphere client jobs using the SnapCenter Plug-in for VMware vSphere REST APIs, you must use the REST API calls for VMware vSphere.

For each REST API, add `https://<server>:<port>/api` at the front of the REST API to form a complete endpoint.

Use the following REST APIs in the Jobs section to get detailed information on jobs:

REST API	Comments
`4.1/audit/logs`	returns audit log files with integrity data
`4.1/audit/logs/{filename}`	get specific audit log file with integrity data
`4.1/audit/verify`	triggers audit verification
`4.1/audit/syslogcert`	updates the syslog server certificate

Upgrade

Upgrade from an earlier release of SnapCenter Plug-in for VMware vSphere

Upgrade to SCV 6.1 is supported only on VMware vCenter server 7 update 1 and later versions, for VMware vCenter server prior to version 7 update 1, you should continue to use SCV 4.7. The upgrade is disruptive on unsupported versions of VMware vCenter server.

If you are using the SnapCenter Plug-in for VMware vSphere virtual appliance, you can upgrade to a newer release.
The upgrade process unregisters the existing plug-in and deploys a plug-in that is compatible only with vSphere 7.0U1 and later versions.

Upgrade paths

If you are on SnapCenter Plug-in for VMware vSphere (SCV) version…	You can directly upgrade SnapCenter Plug-in for VMware vSphere to…
SCV 6.0	Upgrade to SCV 6.1
SCV 5.0	Upgrade to SCV 6.0 and SCV 6.1
SCV 4.9	Upgrade to SCV 5.0 and SCV 6.0
SCV 4.8	Upgrade to SCV 4.9 and SCV 5.0
SCV 4.7	Upgrade to SCV 4.8 and SCV 4.9
SCV 4.6	Upgrade to SCV 4.7 and SCV 4.8

Backup the SnapCenter Plug-in for VMware vSphere OVA before starting an upgrade.

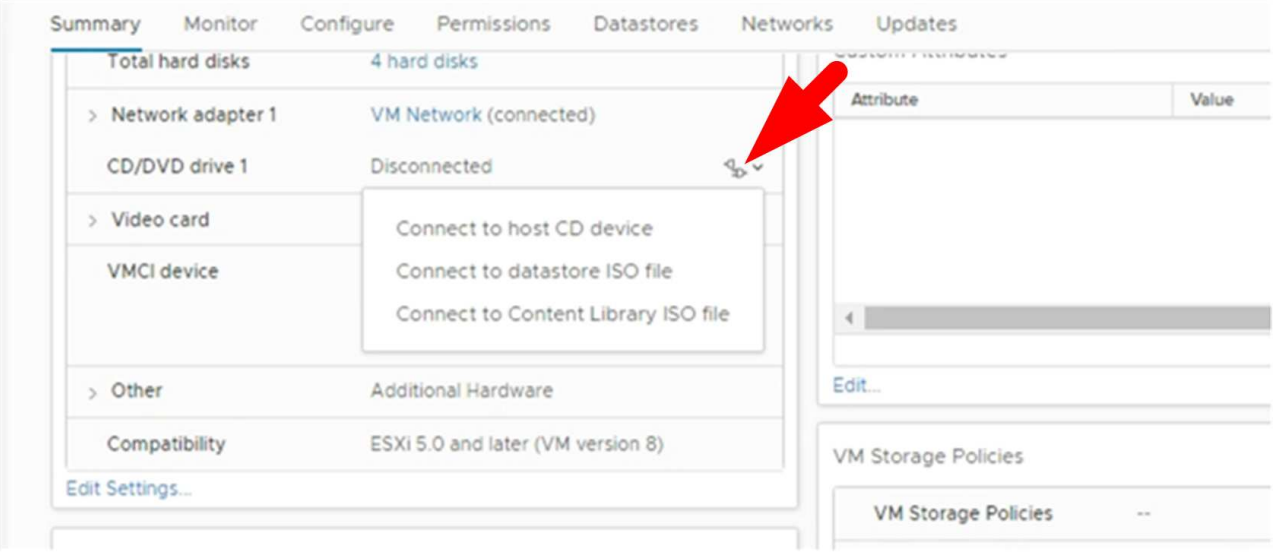
Switching your network configuration from static to DHCP is not supported.

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

Steps

1. Prepare for the upgrade by disabling SnapCenter Plug-in for VMware vSphere.
   a. Log in to the SnapCenter Plug-in for VMware vSphere management GUI.
   The IP address is displayed when you deploy the SnapCenter Plug-in for VMware vSphere.
   b. Select **Configuration** in the left navigation pane, and then select the **Service** option in the Plug-in Details section to disable the plug-in.
2. Download the upgrade `.iso` file.
   a. Log in to the NetApp Support Site (https://mysupport.netapp.com/products/index.html).
   b. From the list of products, select **SnapCenter Plug-in for VMware vSphere**, then select the **DOWNLOAD LATEST RELEASE** button.
   c. Download the SnapCenter Plug-in for VMware vSphere upgrade `.iso` file to any location.

3. Install the upgrade.
    a. In your browser, navigate to the VMware vSphere vCenter.
    b. On the vCenter GUI, select **vSphere client (HTML)**.
    c. Log in to the **VMware vCenter Single Sign-On** page.
    d. On the navigator pane, select the VM that you want to upgrade and then select the **Summary** tab.
    e. On the **Related Objects** pane, select on any datastore in the list and then select the **Summary** tab.
    f. On the **Files** tab for the selected datastore, select on any folder in the list, and then select **Upload files**.
    g. On the upload pop-up screen, navigate to the location where you downloaded the `.iso` file, then select on the `.iso` file image, and then select **Open**.
    The file is uploaded to the datastore.
    h. Navigate back to VM that you want to upgrade, and select the **Summary** tab.
    In the **VM Hardware** pane, in the CD/DVD field, the value should be “Disconnected”.
    i. Select the connection icon in the CD/DVD field and select **Connect to CD/DVD image on a datastore**.



    j. In the wizard, do the following:
        i. In the Datastores column, select the datastore where you uploaded the `.iso` file.
        ii. In the Contents column, navigate to the `.iso` file you uploaded, make sure “ISO image” is selected in the File Type field, and then select **OK**.
        Wait until the field shows the “Connected” status.
    k. Log onto the Maintenance console by accessing the **Summary** tab of the virtual appliance and then select the green run arrow to start the maintenance console.
    l. Enter **2** for System Configuration, then enter **8** for Upgrade.
    m. Enter **y** to continue and start the upgrade.

Upgrade to a new patch of the same release of SnapCenter Plug-in for VMware vSphere

If you are upgrading to a new patch of the same release, you must clear the SnapCenter

Plug-in for VMware vSphere cache on the vCenter Web Server and restart the server before the upgrade or registration.

If the plug-in cache is not cleared, then recent jobs are not displayed in the Dashboard and job monitor in the following scenarios:

- SnapCenter Plug-in for VMware vSphere was deployed using vCenter, and then later upgraded to a patch in the same release.
- The SnapCenter VMware virtual appliance was deployed in vCenter 1. Later, this SnapCenter Plug-in for VMware vSphere was registered to a new vCenter2. A new instance of the SnapCenter Plug-in for VMware vSphere is created with a patch and registered to vCenter1. However, because vCenter1 still has the cached plug-in from the first SnapCenter Plug-in for VMware vSphere without the patch, the cache needs to be cleared.

Steps for clearing the cache

1. Locate the `vsphere-client-serenity` folder, then locate the `com.netapp.scv.client-<release-number>` folder and delete it.

   The folder name changes for each release.

   Refer to VMware documentation for the location of the `vsphere-client-serenity` folder for your operating system.

2. Restart the vCenter Server.

   You can then upgrade the SnapCenter Plug-in for VMware vSphere.

Information not displayed after upgrading to a new patch of the same release

After upgrading SnapCenter Plug-in for VMware vSphere to a new patch of the same release, recent jobs or other information might not be displayed in the Dashboard and job monitor.

If you are upgrading to a new patch of the same release, you must clear the SnapCenter Plug-in for VMware vSphere cache on the vCenter Web Server and restart the server before the upgrade or registration.

If the plug-in cache is not cleared, then recent jobs are not displayed in the Dashboard and job monitor in the following scenarios:

- SnapCenter Plug-in for VMware vSphere was deployed using vCenter, and then later upgraded to a patch in the same release.
- The SnapCenter VMware virtual appliance was deployed in vCenter 1. Later, this SnapCenter Plug-in for VMware vSphere was registered to a new vCenter2. A new instance of the SnapCenter Plug-in for VMware vSphere is created with a patch and registered to vCenter1. However, because vCenter1 still has the cached plug-in from the first SnapCenter Plug-in for VMware vSphere without the patch, the cache needs to be cleared.

The cache is in the following locations, based on the type of server operating system:

- vCenter Server Linux Appliance

  `/etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity/`

- Windows OS

  `%PROGRAMFILES%/VMware/vSphere client/vc-packages/vsphere-client-serenity/`

Workaround if you already upgraded before clearing the cache

1. Log in to the SnapCenter Plug-in for VMware vSphere management GUI.

   The IP address is displayed when you deploy the SnapCenter Plug-in for VMware vSphere.

2. Select **Configuration** in the left navigation pane, and then select the Service option in the **Plug-in Details** section to disable the plug-in.

   SnapCenter Plug-in for VMware vSphere service is disabled, and the extension is unregistered in vCenter.

3. Locate the `vsphere-client-serenity` folder, then locate the `com.netapp.scv.client-<release-number>` folder and delete it.

   The folder name changes for each release.

4. Restart the vCenter Server.
5. Log in to VMware vSphere client.
6. Select **Configuration** in the left navigation pane, and then select the Service option in the **Plug-in Details** section to enable the plug-in.

   SnapCenter Plug-in for VMware vSphere service is enabled, and the extension is registered in vCenter.

Legal notices

Legal notices provide access to copyright statements, trademarks, patents, and more.

Copyright

https://www.netapp.com/company/legal/copyright/

Trademarks

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

https://www.netapp.com/company/legal/trademarks/

Patents

A current list of NetApp owned patents can be found at:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Privacy policy

https://www.netapp.com/company/legal/privacy-policy/

Open source

Notice files provide information about third-party copyright and licenses used in NetApp software.

Notice for SnapCenter Plug-in for VMware vSphere 6.1

Copyright information

Copyright © 2025 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.