Protect data

SnapCenter Plug-in for VMware vSphere 6.2

NetApp
October 28, 2025

Table of Contents

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.

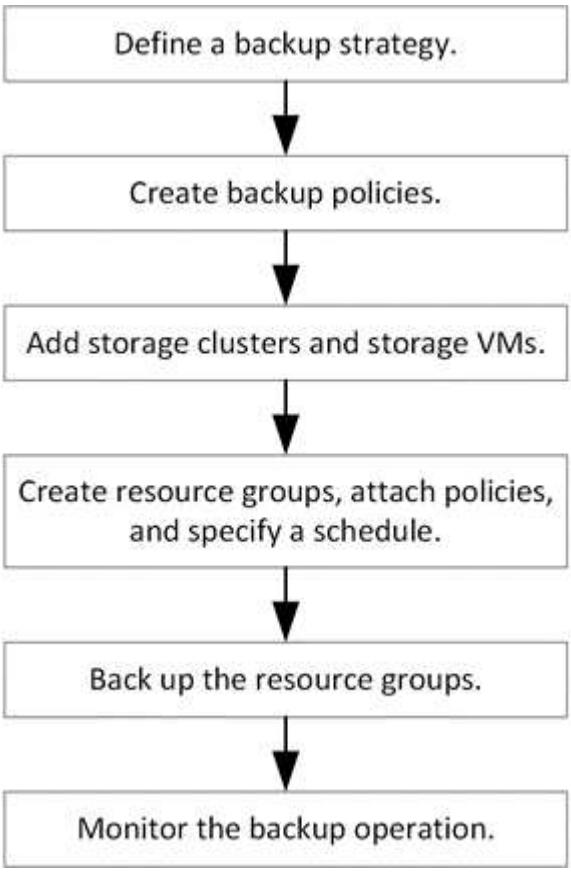
Backup and restore operations cannot be performed simultaneously on the same resource group.

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

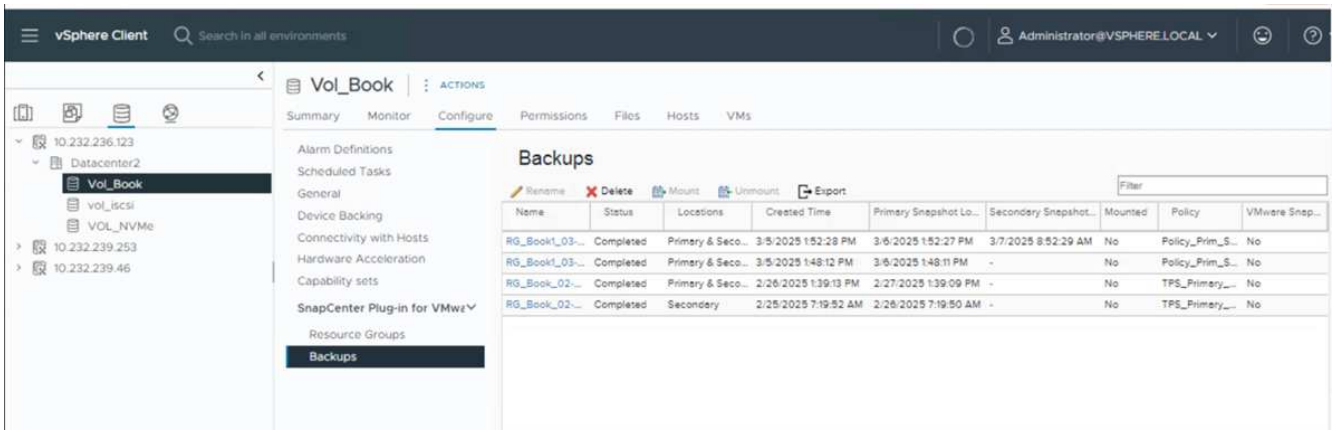
When preparing to back up or restore a VM or datastore, you might want to see all the backups available for that resource and view the details of those backups.

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:

- Any combination of traditional VMs, traditional SAN datastores, and traditional NAS datastores. Traditional VMs cannot be combined with vVol VMs.
- A single FlexGroup datastore. SCV does not support spanning FlexGroup datastores. A FlexGroup datastore cannot be combined with traditional VMs or datastores.
- One or more FlexVol datastores. Spanning datastores are supported.
- One or more vVol VMs. vVol VMs cannot be combined with traditional VMs or datastores.
- All VMs and Datastores, excluding vVol Datastores, that have the specified vSphere tag.
- 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 storage systems. You cannot combine ASA r2 VMs and datastores with other VMs and datastores.

If you are using VMware vSphere Cluster Service (vCLS), do not add vCLS-managed VMs to 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. For supported versions, visit NetApp Interoperability Matrix Tool.

About this task

- You can add or remove resources from a resource group anytime.
- To back up a single resource, such as a VM, create a resource group that contains only that resource.
- To back up multiple resources, create a resource group that includes all the resources you want to protect.
- For FlexGroup volumes in MetroCluster environments, if you are using ONTAP 9.8 or 9.9, restart the SnapCenter Plug-in for VMware vSphere service and resynchronize SnapMirror relationships after a switchover or switchback before backing up resource groups. In ONTAP 9.8, backups might hang after a switchback; this is resolved in ONTAP 9.9.
- For optimal snapshot performance, group VMs and datastores on the same volume into a single resource group.

- You can create a resource group without a backup policy, but data protection requires at least one policy. Select an existing policy or create a new one during resource group creation.

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

- SnapCenter performs compatibility checks when you create a resource group.

  Manage compatibility check failures

- Create secondary protection for a resource group

  Secondary protection enables replication for the resources in the resource group. To use secondary protection, create a consistency group-based SnapMirror relationship from the primary to the preferred cluster and SVM using a specified policy. This feature is supported only for ASA r2 system-based datastores and virtual machines. Ensure that cluster and SVM peering are configured in advance. Only asynchronous SnapMirror policies are supported. When configuring secondary protection, you must specify a consistency group suffix.

Steps

1. In the left navigator pane of the SCV plug-in, select **Resource Groups**, then select **Create** to start the wizard.
   Alternatively, you can create a resource group for a single resource by doing 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**.
2. 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 maintains its own SnapCenter Plug-in for VMware vSphere repository. As a result, you can use the same resource group names in different vCenters.
Description	Enter a description of the resource group.

For this field…	Do this…
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.
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.

For this field…	Do this…
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. • By default, snapshot names follow the format `<ResourceGroup>_<Date-TimeStamp>`. You can customize the snapshot name by using variables such as $ResourceGroup, $Policy, $HostName, $ScheduleType, and $CustomText. Select the desired variables and their order from the drop-down list in the custom name field. If you include $CustomText, the format becomes `<CustomName>_<Date-TimeStamp>`. Enter your custom text in the provided field. [NOTE]: If you select the “_recent” suffix, ensure that your custom snapshot names are unique within the datastore by including the $ResourceGroup and $Policy variables in the name. • Special characters For special characters in names, follow the same guidelines given for the Name field.

3. 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.

For this field…	Do this…
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.

4. 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.

5. On the **Policies** page, select or create one or more backup policies, as shown in the following table:

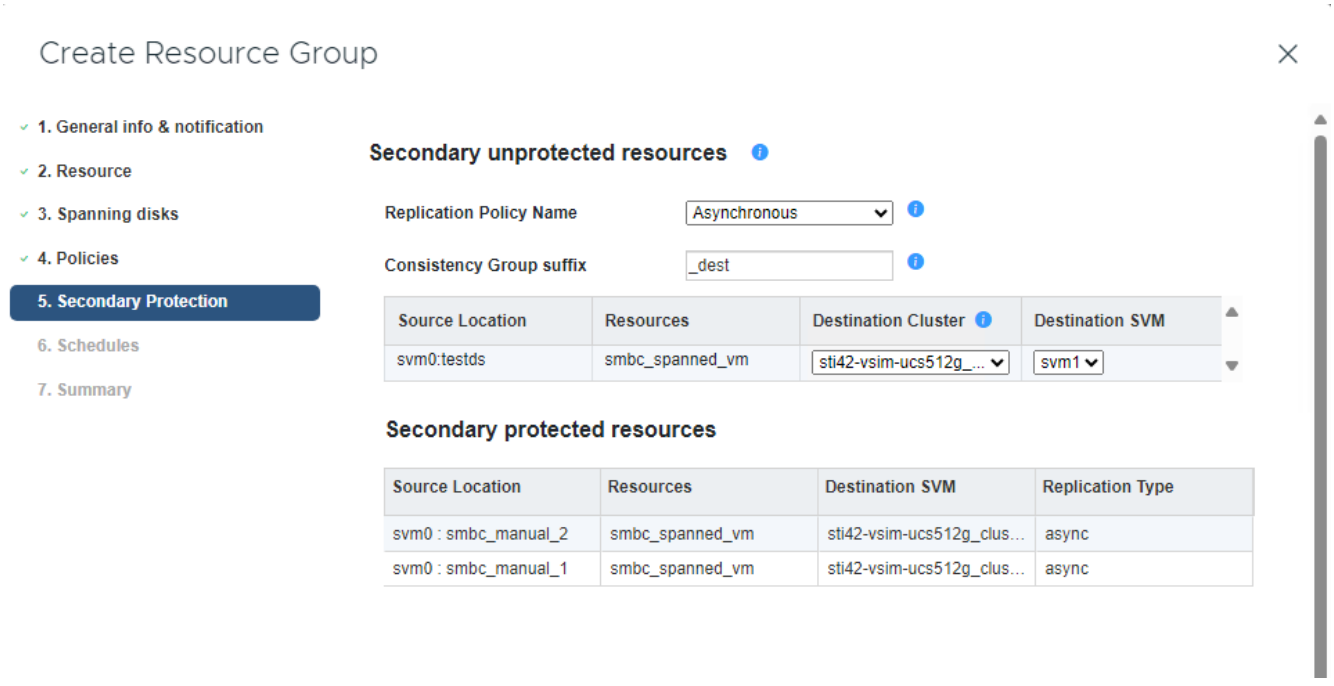
To use…	Do this…
An existing policy	Select one or more policies from the list. Secondary protection is applicable to existing and new policies where you have selected both SnapMirror and SnapVault updates.
A new policy	1. Select **Create**. 2. Complete the New Backup Policy wizard to return to the Create 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.

6. On the **Secondary protection** page, you see the selected resources along with their current protection status. To enable protection for any unprotected resources, choose the replication policy type, enter a consistency group suffix, and select the destination cluster and destination SVM from the dropdown menus. When the resource group is created, SCV starts a separate job for secondary protection. You can monitor this job in the job monitor window.

Fields	Description
Replication policy name	Name of the SnapMirror policy. Only **Asynchronous** and **Mirror and Vault** secondary policies are supported.

Fields	Description
Consistency group suffix	Enter a suffix to append to the primary consistency group name when creating the destination consistency group. For example, if the primary consistency group name is `sccg_2024-11-28_120918` and you enter `_dest` as the suffix, the secondary consistency group will be named `sccg_2024-11-28_120918_dest`. This suffix is used only for unprotected consistency groups.
Destination cluster	For all unprotected storage units, SCV displays the names of peered clusters in the dropdown menu. If the storage is added to SCV with SVM scope, the cluster ID is shown instead of the cluster name due to ONTAP limitations.
Destination SVM	For all unprotected storage units, SCV displays the names of peered SVMs. When you select a storage unit that is part of a consistency group, the corresponding cluster and SVM are automatically selected for all other storage units in that 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.



7. On the **Schedules** page, set up 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`.

If you select a value in the **Every** field (for example, **Every 2 days**), backups will run on the first day of the month and then repeat at the specified interval (day 1, 3, 5, 7, so on.) for the rest of the month, regardless of whether the starting date is even or odd.

All fields are required. SnapCenter Plug-in for VMware vSphere creates backup schedules based on the time zone where it is deployed. To change the time zone, use the SnapCenter Plug-in for VMware vSphere user interface.

Modify the time zones for backups.

8. 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 SCV marks the backup as not VM-consistent even if you selected a policy with VM consistency. 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 fix a compatibility error, do 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 user interface.
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.
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 user interface, 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.

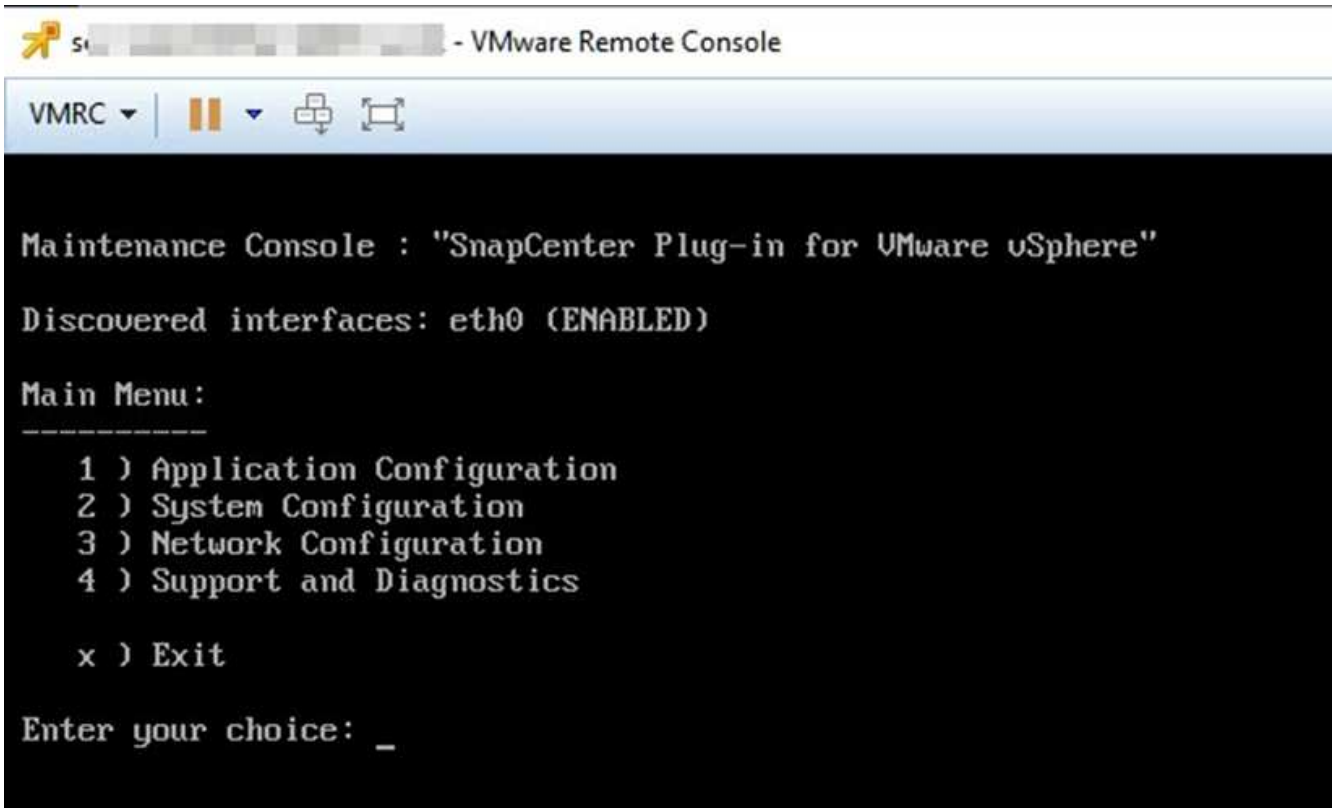
You should also back up the repository before performing migrations or upgrades.

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

Pause scheduled operations on a resource group. Enable them again when needed.

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

Delete a resource group in vCenter if you do not need to protect the resources. Delete all resource groups before removing SnapCenter Plug-in for VMware vSphere.

About this task

All resource group delete operations are performed as force deletes. When you delete a resource group, the system 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, you cannot delete the last snapshot, therefore you cannot delete the resource group. Before deleting a resource group in a SnapVault relationship, use System Manager or ONTAP CLI to remove the relationship, then 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 dialog, select **OK** to confirm. Deleting a resource group does not remove secondary protection. If needed, use System Manager to delete secondary protection. Consistency groups created for the resource group are not automatically removed; you must manually delete them from ONTAP using System Manager or another supported interface.

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.

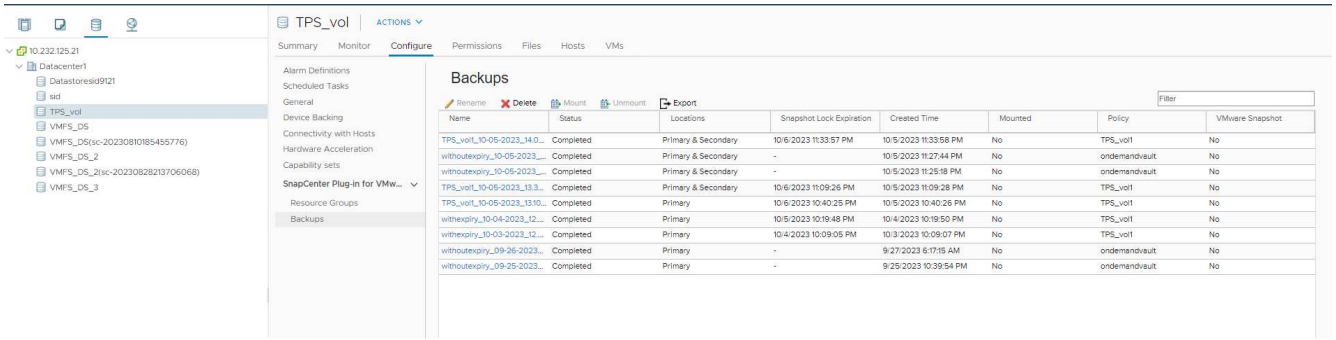
Rename backups

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.

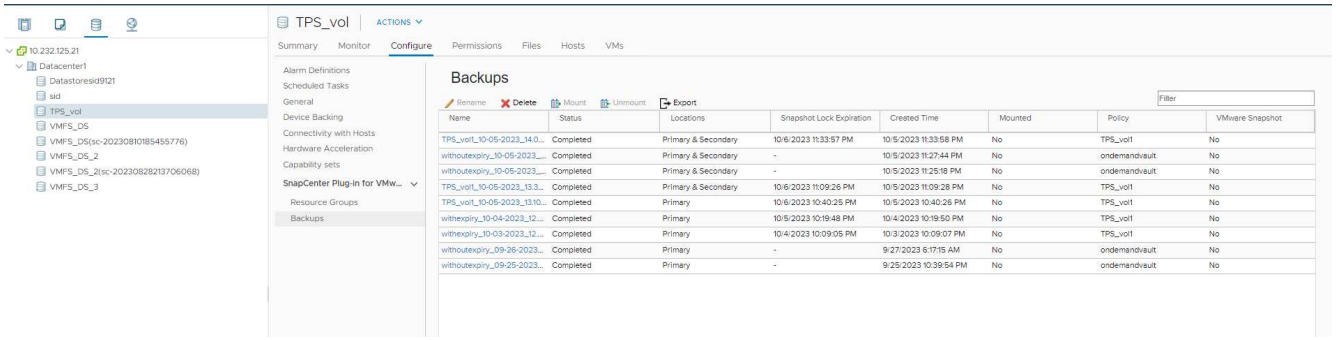
Before you begin

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.

Copyright information

Trademark information