Migrate to the Linux-based SnapCenter Plug-in for VMware vSphere

SnapCenter Plug-in for VMware vSphere 4.4

NetApp
December 17, 2020

Table of Contents

Migrate to the Linux-based SnapCenter Plug-in for VMware vSphere

Overview

You use the SnapCenter Windows PowerShell cmdlets to migrate SnapCenter Plug-in for VMware vSphere metadata from the Windows-based SnapCenter Server to the Linux-based SnapCenter Plug-in for VMware vSphere virtual appliance.

There are two migration options:

- Migrating from SnapCenter

  You must migrate metadata for the following from Windows-based SnapCenter:

  - VM-consistent backups performed by the SnapCenter Plug-in for VMware vSphere when the plug-in was running as a Windows-based component of SnapCenter.
  - Application-consistent data protection metadata of virtualized databases or file systems performed by a SnapCenter application-based plug-in with support from the SnapCenter Plug-in for VMware vSphere when the plug-in was running as a Windows-based component of SnapCenter.

    To migrate, you use the Windows SnapCenter PowerShell cmdlet `invoke-SCVOVAMigration.`

    You can only migrate metadata from SnapCenter 4.0 or later.

- Migrating from VSC

  You can migrate VSC 6.2.x (SMVI) metadata for backup jobs that are not integrated with SnapCenter.

  To migrate, you use the NetApp ToolChest: NetApp Import Utility for SnapCenter and Virtual Storage Console. Make sure to select the VSC to SnapCenter migration option.

  You can only migrate metadata for existing backups. For example, if you do not have existing backups, then you cannot migrate policies only.

Supported migration paths

See the SnapCenter Plug-in for VMware vSphere Release Notes for information on supported upgrade and migration paths.

Migration overview

- The migration command migrates metadata from SnapCenter 4.0, 4.1, and 4.1.1 only. If you are using an earlier version of SnapCenter then you must first upgrade before you can migrate.
  - What is migrated:

    SnapCenter metadata, which includes storage systems, customized throttles, and email settings in the SnapCenter configuration file, policies, resource groups, backup metadata, and mounts. (the migration fails when it encounters prescripts or postscripts)

- What is not migrated:

  Pre- and post-scripts that are configured for resource groups

  Active guest file restore sessions, guest file restore credentials, and proxy VMs

  If you begin migration when a guest file restore session is active, the session is deleted and the attached disk is not unmounted. You might have to delete the attached disk manually.

  `scbr.override` configuration file

- To ensure migration success, the migration command suspends all hosts that are registered with SnapCenter. After the migration process finishes successfully, SnapCenter hosts are resumed.
- You must use the Windows Powershell cmdlet `invoke-SCVOVAMigration` for each instance of the SnapCenter VMware plug-in that is registered with SnapCenter. The cmdlet does the following:
  - Suspends all schedules to prevent job failures during the migration. After a successful migration, schedules are automatically re-enabled.
  - Migrates storage connections and metadata.
  - Creates backup schedules for post-migration backups.
  - Uninstalls the existing SnapCenter Plug-in for VMware vSphere from the Windows host.

    If the SnapCenter VMware plug-in is installed on the SnapCenter Server host and protection is configured for the SnapCenter repository, then the migration process also uninstalls the Windows-based plug-in package that contains the SnapCenter Plug-in for VMware vSphere and the SnapCenter Plug-in for Windows, and then reinstalls the latest version of SnapCenter Plug-in for Windows to support the repository protection. The host type in the SnapCenter GUI changes from “vsphere” to “Windows”.

  - Removes the vSphere host and resource groups from the Windows SnapCenter Server.
  - Activates the backup jobs on the Linux-based SnapCenter VMware plug-in.
  - Registers the vSphere host for the SnapCenter VMware plug-in `with SnapCenter to support application-based backups of virtualized databases and file systems (application over VMDK backups).
- Metadata for application-based VMDK backups is stored in the SnapCenter Server repository. Metadata for VM and datastore backups is stored in the SnapCenter VMware plug-in MySQL repository.

Prerequisites for migration

- You must be running SnapCenter Server 4.2 or later.
- You must use Admin credentials.
- The SnapCenter Plug-in for VMware vSphere virtual appliance must be deployed with the SnapCenter VMware plug-in enabled and registered on vCenter.
- On the SnapCenter VMware plug-in dashboard, the status for SnapCenter Plug-in for VMware vSphere must be “connected.”
- You must have created a Linux type Run As credential using the account that was specified during the deployment of the SnapCenter VMware plug-in.
- All guest file restore sessions must be deleted.
- SnapCenter hosts must be configured with IP addresses, not fully qualified domain names (FQDN).

In a Linked Mode environment, you must migrate all linked nodes together.

- Names for storage VMs must resolve to management LIFs.If you added `etc` host entries for storage VM names in SnapCenter, you must verify that they are also resolvable from the virtual appliance.

Migrate from SnapCenter backup metadata to the virtual appliance

You use the SnapCenter Windows PowerShell cmdlets to migrate SnapCenter VM-consistent backup metadata and SnapCenter application-consistent for virtualized data backup metadata to the SnapCenter Plug-in for VMware vSphere virtual appliance.

Steps

1. Back up the MySQL database and then copy and move that backup to a different location to make sure it does not get deleted due to the retention policy.

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

2. Log on to the VMware vSphere web client and verify that no jobs are running.
3. Log on to the SnapCenter GUI using the SnapCenter Admin username.

   Do not use any other username to log in, even if that username has all permissions, because it might cause a migration error.

4. In the Windows SnapCenter GUI left navigation pane, click **Settings**, then click the **Credential** tab, and then click **Add** to add credentials for the virtual appliance.
5. Create the name of the Run As credential to be used in the `invoke-SCVOVAMigration `cmdlet.

   You must select Linux for the Authentication field.

   This step adds the credentials that SnapCenter Server uses to access the virtual appliance during the migration.

6. Open a Windows PowerShell window and run the following cmdlets:

   ```
   Open-SmConnection

   invoke-SCVOVAMigration -SourceSCVHost old-SCV-host-IP -DestinationSCVOVAHost new-appliance-IP -OVACredential appliance-credentials -ByPassValidationCheck -Overwrite -ContinueMigrationOnStorageError -ScheduleOffsetTime time-offset
   ```

   The migration command suspends job schedules before migrating metadata and registers the virtual appliance with SnapCenter Server.

   Use the ScheduleOffsetTime parameter if the source SnapCenter host and the destination SnapCenter VMware virtual appliance host are in different time zones. The value can be a positive or negative time offset to adjust scheduled backup run times. Specify the time difference in the format hh: mm:ss; for example, 06:00:00, or -06:00:00 for a negative value.

Post-migration

- Migration log bundle

  Download the migration log bundle from the `App_Data/MigrationLog` directory in the SnapCenter installation folder. Keep the migration log bundle until you are sure that the migration was successful.

- Job details on the Dashboard

  Information on the migrated backups is listed in the VMware vSphere web client recent jobs pane but detailed information is not displayed in the Dashboard until backups are performed after the migration.

- Authentication errors

  If you do not use Admin credentials, you might encounter an authentication error.

  Manage authentication errors

- Backup names

  Backup names before migration have the format RGName `_HostName_Timestamp`. For example, `-NAS_DS_RG_perf1server_07-05-2019_02.11.59.9338`.

  Backup names after migration have the format `RGName_Timestamp`.

  For example, `-NAS_VM_RG_07-07-2019_21.20.00.0609`.

- Pre- and post-scripts

  Scripts that are configured for resource groups are not migrated. Because scripts written for Windows systems might not run on the Linux-based virtual appliance, you might need to recreate all or part of the scripts and add those scripts after migration. For example, file paths in Windows do not exist in Linux, and an invoke for a .bat batch file does not work in Linux.

  One solution is to put an existing Windows-based script on the Linux-based virtual appliance and test whether the script works with no changes. If it does not work correctly, then replace each Windows-based command in the script with a corresponding Linux compatible command.

- Guest file restore credentials

  Guest file restore credentials are not migrated. Therefore, you must create new guest file credentials after the migration.

- `scbr.override` configuration file

  If you have customized settings in the `scbr.override` configuration file, then you must move that file to the SnapCenter VMware plug-in virtual appliance and restart the web client service.

- Upgrade SnapCenter application-based plug-ins

  If you use the SnapCenter VMware plug-in to support other SnapCenter plug-ins, then you must update those plug-ins to 4.2 or later.

- Uninstall SnapCenter Server

If you use SnapCenter only for VM-consistent or crash-consistent data protection, then after all VM backups are migrated to the SnapCenter VMware plug-in, you can uninstall SnapCenter Server on the Windows host

Correct “Bad Gateway” errors during migration

There are several reasons why you might encounter a “Bad Gateway” error.

Scenario 1

You manually added files or other content to the SnapCenter Plug-in for VMware vSphere and then tried to migrate. In this scenario, there is not enough space in the appliance for the migration process.

To correct this error, remove any manually added files.

Scenario 2

The SnapCenter Plug-in for VMware vSphere connection was stopped, or the service was stopped during the migration.

The SnapCenter Plug-in for VMware vSphere connection status must be “connected” during the migration process. You can also manually update the time out configuration in the virtual appliance.

Manage authentication errors

If you do not use the Admin credentials, you might receive an authentication error after deploying the 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 VMware plug-in management GUI using the format `https://<OVA-IP-address>:8080`.
2. Restart the service.