Tech refresh

SnapCenter Software 6.0

NetApp
December 19, 2024

Table of Contents

Tech refresh

Tech refresh of SnapCenter Server host

When the SnapCenter Server host requires refresh, you can install the same version of SnapCenter Server on the new host and then run the APIs to backup the SnapCenter from old server and restore it in on the new server.

Steps

1. Deploy the new host and perform the following tasks:
   a. Install the same version of the SnapCenter Server.
   b. (Optional) Configure CA certificates and enable two-way SSL. For more information, refer to Configure CA Certificate and Configure and enable two-way SSL.
   c. (Optional) Configure multi-factor authentication. For more information, refer to Enable multi-factor authentication.
2. Log in as the SnapCenter Admin user.
3. Create a backup of the SnapCenter Server on the old host using either the API: `/<snapcenter_version>/server/backup` or the cmdlet: *New-SmServerBackup*.

   Before taking the backup, suspend all the scheduled jobs and ensure that no jobs are running.

   If you want to restore the backup on the SnapCenter Server that is running on a new domain, before taking a backup you should add the new domain user in the old SnapCenter host and assign the SnapCenter admin role.

4. Copy the backup from the old host to new host.
5. Restore the backup of the SnapCenter Server on the new host using either the API: `/<snapcenter_version>/server/restore` or the cmdlet: *Restore-SmServerBackup*.

   Restore will update the new SnapCenter Server URL in all the hosts by default. If you want to skip the update, use the *-SkipSMSURLInHosts* attribute and separately update the server URL by running using either the API: `/<snapcenter_version>/server/configureurl` or the cmdlet: *Set-SmServerConfig*.

   If the plug-in host is not able to resolve the server hostname, log in to each of the plug-in host and add the *etc/host* entry for the new IP in the <New IP> SC_Server_Name format.

   The server *etc/host* entries will not be restored. You can restore it manually from the old server.

   If the backup is restored on the SnpCenter Server that is running on a new domain and if you want to continue to use the old domain users, you should register the old domain in the new SnapCenter Server.

   If you have manually updated the web.config file in old SnapCenter host, the updates will not be copied to the new host. You should manually make the same changes in the web.config file of the new host.

6. If you have skipped updating the SnapCenter Server URL or any of the host was down during the restore process, update the new server name in all the hosts or specified hosts that are managed by the SnapCenter using either the API: `/<snapcenter_version>/server/configureurl` or the cmdlet: *Set-SmServerConfig*.
7. Activate the scheduled jobs on all the hosts from the new SnapCenter Server.

Tech refresh of a node in F5 cluster

You can do tech refresh of any node in the F5 cluster by removing the node and adding the new node. If the node that needs to be refreshed is active, make another node of the cluster as active and then remove the node.

For information on how to add a node to F5 cluster, refer to Configure SnapCenter Servers for High Availability using F5.

If the url of the F5 cluster changes, the url can be updated in all the hosts using either the API: `/<snapcenter_version>/server/configureurl` or the cmdlet: *Set-SmServerConfig*.

Decommissioning the old SnapCenter Server host

You can remove the old SnapCenter Server host after verifying that the new SnapCenter Server is up and running and all the plug-in hosts are able to communicate with the the new SnapCenter Server host.

Rollback to the old SnapCenter Server host

In case of any issues, you can bring back the old SnapCenter Server host by updating the SnapCenter Server URL in all the hosts using either the API: `/<snapcenter_version>/server/configureurl` or the cmdlet: *Set-SmServerConfig*.

Disaster recovery

Disaster recovery of standalone SnapCenter host

You can perform disaster recovery by restoring the server backup to the new host.

Before you begin

Ensure that you have a backup of the old SnapCenter Server.

Steps

1. Deploy the new host and perform the following tasks:
   a. Install the same version of the SnapCenter Server.
   b. Configure CA certificates and enable two-way SSL. For more information, refer to Configure CA Certificate and Configure and enable two-way SSL.
2. Copy the old SnapCenter Server backup to the new host.
3. Log in as the SnapCenter Admin user.
4. Restore the backup of the SnapCenter Server on the new host using either the API: `/<snapcenter_version>/server/restore` or the cmdlet: *Restore-SmServerBackup*.

   Restore will update the new SnapCenter Server URL in all the hosts by default. If you want to skip the

update, use the *-SkipSMSURLInHosts* attribute and separately update the server URL by using either the API: `/<snapcenter_version>/server/configureurl` or the cmdlet: *Set-SmServerConfig*.

> If the plug-in host is not able to resolve the server hostname, log in to each of the plug-in host and add the *etc/host* entry for the new IP in the <New IP> SC_Server_Name format.

> The server *etc/host* entries will not be restored. You can restore it manually from the old server.

5. If you have skipped updating the URL or any of the host was down during the restore process, update the new server name in all the hosts or specified hosts that are managed by the SnapCenter using either the API: `/<snapcenter_version>/server/configureurl` or the cmdlet: *Set-SmServerConfig*.

Disaster recovery of SnapCenter F5 cluster

You can perform disaster recovery by restoring the server backup to the new host and then converting the standalone host to a cluster.

Before you begin

Ensure that you have a backup of the old SnapCenter Server.

Steps

1. Deploy the new host and perform the following tasks:
   a. Install the same version of the SnapCenter Server.
   b. Configure CA certificates and enable two-way SSL. For more information, refer to Configure CA Certificate and Configure and enable two-way SSL.
2. Copy the old SnapCenter Server backup to the new host.
3. Log in as the SnapCenter Admin user.
4. Restore the backup of the SnapCenter Server on the new host using either the API: `/<snapcenter_version>/server/restore` or the cmdlet: *Restore-SmServerBackup*.

   Restore will update the new SnapCenter Server URL in all the hosts by default. If you want to skip the update, use the *-SkipSMSURLInHosts* attribute and separately update the server URL by using either the API: `/<snapcenter_version>/server/configureurl` or the cmdlet: *Set-SmServerConfig*.

   > If the plug-in host is not able to resolve the server hostname, log in to each of the plug-in host and add the *etc/host* entry for the new IP in the <New IP> SC_Server_Name format.

   > The server *etc/host* entries will not be restored. You can restore it manually from the old server.

5. If you have skipped updating the URL or any of the host was down during the restore process, update the new server name in all the hosts or specified hosts that are managed by the SnapCenter using either the API: `/<snapcenter_version>/server/configureurl` or the cmdlet: *Set-SmServerConfig*.
6. Convert the standalone host to F5 cluster.

   For information on how to configure F5, refer to Configure SnapCenter Servers for High Availability using F5.

Related information

For information on the APIs, you need to access the Swagger page. see How to access REST APIs using the swagger API web page.

The information regarding the parameters that can be used with the cmdlet and their descriptions can be obtained by running *Get-Help command_name*. Alternatively, you can also refer the SnapCenter Software Cmdlet Reference Guide.

Tech refresh of SnapCenter plug-in hosts

When the SnapCenter plug-in hosts require refresh, you should move the resources from old host to new host. When the new host is added to SnapCenter, it will discover all the resources but will be treated as new resources.

About this task

You should run the API or cmdlet which will take old host name and new host name as input, compare the resources by name, and relink the objects of matching resources from old host to new host. The matching resources will be marked as protected.

- The *IsDryRun* parameter is set to True by default and this identifies the matching resources of the old and new host.

  After verifying the matching resources, you should set the *IsDryRun* parameter to False to relink the objects of the matching resources from the old host to new host.

- The *AutoMigrateManuallyAddedResources* parameter is set to True by default and this automatically copies the manually added resources from old host to the new host.

  The *AutoMigrateManuallyAddedResources* parameter is applicable only for Oracle and SAP HANA resources.

- The *SQLInstanceMapping* parameter should be used if the instance name is different between old host and new host. If it is a default instance then use *default_instance* as instance name.

Tech refresh is supported for the following SnapCenter Plug-ins:

- SnapCenter Plug-in for Microsoft SQL Server
  - If the SQL databases are protected at instance level and as part of host tech refresh only partial resources are moved to new host, then the existing instance level protection will be converted to resource group protection and instances from both the hosts will be added to the resource group.
  - If a SQL host (for example host1) is used as either scheduler or verification server for resources of another host (for example host2), then while performing tech refresh on host1, the schedule or the verification details will not be migrated and will continue to run on host1. If you have to modify, then you should manually change it in the respective hosts.
  - If you are using SQL Failover Cluster Instances (FCI) setup, you can perform the tech refresh by adding the new node to the FCI cluster and refreshing the plug-in host in SnapCenter.
  - If you are using SQL Availability Group (AG) setup, tech refresh is not required. You can add the new node to AG and refresh the host in SnapCenter.
- SnapCenter Plug-in for Windows
- SnapCenter Plug-in for Oracle Database

If you are using Oracle Real Application Cluster (RAC) setup, you can perform the tech refresh by adding the new node to the RAC cluster and refreshing the plug-in host in SnapCenter.

- SnapCenter Plug-in for SAP HANA Database

The supported use cases are:

- Migrating resources from one host to another host.
- Migrating resources from multiple hosts to one or fewer hosts.
- Migrating resources from one host to multiple hosts.

The supported scenarios are:

- New host has a different name from the old host
- Existing host has been renamed

Before you begin

As this workflow modifies the data in SnapCenter repository, it is recommended to backup the SnapCenter repository. Incase of any data issues, SnapCenter repository can be reverted to old state using the backup.

For more information, refer to Back up the SnapCenter repository.

Steps

1. Deploy the new host and install the application.
2. Suspend the schedules of the old host.
3. Move the required resources from the old host to the new host.
   a. Bring up the required databases in the new host from the same storage.
      - Ensure that the storage is mapped to the same drive or same mount path as that of old host. If the storage is not mapped correctly, backups created in old host cannot be used for restore.

        By default, Windows auto assigns the next available drive.

      - If storage DR is enabled, the respective storage should be mounted in the new host.
   b. Check for the compatibility if there is a change in application version.
   c. Only for Oracle plug-in host, ensure that the UIDs and GIDs of Oracle and it's group users are same as that of old host.

      For information, refer to:

      - How to migrate SQL database from old host to new host
      - How to migrate Oracle database from old host to new host
      - How to bring up SAP HANA database onto new host
4. Add the new host to SnapCenter.
5. Verify if all the resources are discovered.
6. Run the host refresh API: `/<snapcenter_version>/techrefresh/host` or the cmdlet: *Invoke-SmTechRefreshHost*.

The dry run is enabled by default and the matching resources to be relinked are identified. You can verify the resources by running either the API: '/jobs/{jobid}' or the cmdlet *Get-SmJobSummaryReport*.

If you have migrated the resources from multiple hosts, you should run the API or the cmdlet for all the hosts. If the drive or mount path in the new host is not same as the old host, following restore operations will fail:

- SQL in-place restore will fail. However, RTAL feature can be leveraged.
- Restore of Oracle and SAP HANA databases will fail.

If you want to migrate to multiple hosts, you should perform all the steps from step 1 for all the hosts.

You can run the API or cmdlet on the same host multiple times, it will relink only if there is a new resource identified.

7. (Optional) Remove the old host or hosts from SnapCenter.

Related information

For information on the APIs , you need to access the Swagger page. see How to access REST APIs using the swagger API web page.

The information regarding the parameters that can be used with the cmdlet and their descriptions can be obtained by running *Get-Help command_name*. Alternatively, you can also refer the SnapCenter Software Cmdlet Reference Guide.

Tech refresh of storage system

When the storage is tech refreshed, the data is migrated to new storage and the application hosts are mounted with new storage. The SnapCenter backup workflow identifies the new storage and creates the snapshot if the new storage is registered in SnapCenter.

You can perform restore, mount, and clone on the new backups created after storage refresh. However these operations will fail when performed on the backups that were created before storage refresh because the backups has the old storage details. You should run the storage tech refresh API or cmdlet to update the old backups in SnapCenter with the new storage details.

Tech refresh is supported for the following SnapCenter Plug-ins:

- SnapCenter Plug-in for Microsoft SQL Server
- SnapCenter Plug-in for Windows
- SnapCenter Plug-in for Oracle Database
- SnapCenter Plug-in for SAP HANA Database
- SnapCenter Plug-in for Microsoft Exchange Server

The supported use cases are:

- Primary storage refresh

The storage tech refresh is supported for replacing the primary storage with new storage. You cannot convert the existing secondary storage to a primary storage.

- Secondary storage refresh

The other supported scenarios are:

- SVM name change
- Volume name change

Update the backups of the primary storage

When the storage is tech refreshed, you should run the storage tech refresh API or cmdlet to update the old backups in SnapCenter with the new storage details.

Before you begin

As this workflow modifies the data in SnapCenter repository, it is recommended to backup the SnapCenter repository. Incase of any data issues, SnapCenter repository can be reverted to old state using the backup.

For more information, refer to Back up the SnapCenter repository.

Steps

1. Migrate the data from old storage to new storage.

   For information on how to migrate, refer to:

   - How to migrate the data to new storage
   - How can I copy a volume and preserve all of the Snapshot copies?
2. Put the host to maintenance mode.
3. Mount the new storage in the respective hosts and bring up the databases.

   The new storage should be connected to host in the same way as before. For example, if it was connected as SAN, it needs to be connected as SAN.

   The new storage needs to be mounted on the same drive or path as that of the old storage.
4. Verify that all the resources are up and running.
5. Add the new storage in SnapCenter.

   Ensure that you have an unique SVM name across clusters in SnapCenter. If you are using the same SVM name in the new storage and if all the volumes of the SVM can be migrated before executing the storage refresh, then it is recommended to delete the SVM in old cluster and rediscover the old cluster in SnapCenter which will remove the SVM from cache.
6. Put the host in production mode.
7. In SnapCenter, create a backup of the resources whose storage is migrated. A new backup is necessary for SnapCenter to identify the latest storage footprint, and it will be used to update the metadata of existing old backups.

Whenever a new LUN is attached to host, it will have a new serial number. During discovery of Windows File System, SnapCenter will treat every unique serial number as new resource. During storage tech refresh when the LUN from new storage is attached to host with the same drive letter or path, the discovery of Windows File System in SnapCenter will mark the existing resource as deleted even if it is mounted with same drive letter or path and display the new LUN as new resource. As the resource is marked as deleted, it will not be considered for storage tech refresh in SnapCenter and all the backups of the old resource will be lost. When ever storage refresh happens, for Windows file system resources, resource discovery should not be performed before executing storage refresh API or cmdlet.

8. Run either the storage refresh API: `/<snapcenter_version>/techrefresh/primarystorage` or the cmdlet: *Invoke-SmTechRefreshPrimaryStorage*.

   If the resource is configured with a replication enabled policy, the latest backup after the storage refresh should have details of the secondary storage.

   a. If you are using SQL Failover Cluster Instances (FCI) setup, the backups are maintained at cluster level. You should provide the cluster name as input for storage tech refresh.
   b. If you are using SQL Availability Group (AG) setup, the backups are maintained at node level. You should provide the node name as input for storage tech refresh.
   c. If you are using Oracle Real Application Clusters (RAC) setup, you can perform storage tech refresh on any node.

      The *IsDryRun* attribute is set to True by default. It will identify the resources for which the storage is refreshed. You can view the resource and the changed storage details by running either the API: '<snapcenter_version>/jobs/{jobid}' or the cmdlet *Get-SmJobSummaryReport*.

9. After verifying the storage details, set the *IsDryRun* attribute to False and run the storage refresh API: `/<snapcenter_version>/techrefresh/primarystorage` or the cmdlet: *Invoke-SmTechRefreshPrimaryStorage*.

   This will update the storage details in the older backups.

   You can run the API or cmdlet on the same host multiple times, it will update the storage details in the older backups only if the storage is refreshed.

   The clone hierarchy cannot be migrated in ONTAP. If the storage being migrated has any clone metadata in SnapCenter, then the cloned resource will be marked as independent resource. Clones of clone metadata will be removed recursively.

10. (Optional) If all the snapshots are not moved from old primary storage to new primary storage, run the following API: `/<snapcenter_version>/hosts/primarybackupsexistencecheck` or the cmdlet *Invoke-SmPrimaryBackupsExistenceCheck*.

    This will perform the snapshot existence check on the new primary storage and mark the respective backups not available for any operation in SnapCenter.

Update the backups of the secondary storage

When the storage is tech refreshed, you should run the storage tech refresh API or cmdlet to update the old backups in SnapCenter with the new storage details.

Before you begin

As this workflow modifies the data in SnapCenter repository, it is recommended to backup the SnapCenter repository. Incase of any data issues, SnapCenter repository can be reverted to old state using the backup.

For more information, refer to Back up the SnapCenter repository.

Steps

1. Migrate the data from old storage to new storage.

   For information on how to migrate, refer to:

   - How to migrate the data to new storage
   - How can I copy a volume and preserve all of the Snapshot copies?

2. Establish the SnapMirror relationship between the primary storage and new secondary storage, and make sure relationship state is healthy.
3. In SnapCenter, create a backup of the resources whose storage is migrated.

   A new backup is necessary for SnapCenter to identify the latest storage footprint and it will be used to update the metadata of existing old backups.

   > You should wait until this operation is completed. If you proceed to the next step before completion, SnapCenter will loose old secondary snapshot metadata completely.

4. After successfully creating backup of all the resources in a host, run either the secondary storage refresh API: `/<snapcenter_version>/techrefresh/secondarystorage` or the cmdlet: *Invoke-SmTechRefreshSecondaryStorage*.

   This will update the secondary storage details of the older backups in the given host.

   If you want to run this at resource level, click **Refresh** for each resource to update the secondary storage metadata.

5. After successfully updating the older backups, you can break the old secondary storage relationship with primary.

Copyright information

Trademark information