Backing Up and Restoring Prime Network Services Controller

This section includes the following topics:

Note For information about exporting or importing, see the Cisco Prime Network Services Controller 3.0 User Guide.

Overview

Note We recommend that you use backup and restore as a disaster recovery mechanism. To migrate configuration data from one Prime Network Services Controller server to another, see the Cisco Prime Network Services Controller 3.0 User Guide.

Prime Network Services Controller enables you to back up and restore data for the same Prime Network Services Controller version. That is, the following backup and restore operations are supported:

- Backing up VNMC 2.0 and restoring to VNMC 2.0.
- Backing up Prime Network Services Controller 3.0 and restoring to Prime Network Services Controller 3.0.

Backing up one version and restoring to another version (such as backing up VNMC 2.0 and restoring to Prime Network Services Controller 3.0) is not supported.

> **Note** Do not use TFTP for backup and restore operations.

The following topics describe how to back up data and restore data for Prime Network Services Controller 3.0:

- Backing Up Prime Network Services Controller, on page 2
- Restoring the Previous Version, on page 2

Backing Up Prime Network Services Controller

Prime Network Services Controller enables you to perform a backup using either the GUI or the CLI. You can back up and restore data for the same Prime Network Services Controller version. Backing up one version and restoring to another (such as backing up VNMC 2.0 and restoring to Prime Network Services Controller 3.0) is not supported.

We recommend the following:

- That you do not perform a backup when any of the following tasks are running on the system:
  - Image import
  - Migration of a VM to the cloud
  - Deployment of an InterCloud Switch
  - Creation of an InterCloud link

- That you use backup and restore as a disaster recovery mechanism. To save a state for recovery purposes, perform a backup via the GUI or CLI, using one of the following methods:
  - CLI—See Backing Up Data.
  - GUI—See the Cisco Prime Network Services Controller 3.0 User Guide.

Restoring the Previous Version

> **Note** Do not use TFTP to update data.

Before You Begin

Temporarily disable the CSA on the remote file server.

Procedure

Step 1 Using the console, log in to Prime Network Services Controller as admin.

> **Note** We recommend that you access the CLI via the console instead of SSH. If the SSH session should disconnect, you will not be able to access the VM.

Step 2   Connect to local-mgmt:

```
connect local-mgmt
```

Step 3   (Optional) Check the current version of Prime Network Services Controller:

```
show version
```

Step 4   Download the required image from a remote file server:

```
copy scp://imageURLtoBinFile bootflash:/
```

Step 5   Enter the **update** command:

```
update bootflash:/nsc.3.0.0.XXXX.bin force
```

Step 6   Restore the previous version:

```
restore scp://user@host-ip-address/tmp/backup-file.tgz
```

where:

- *user* is the username for accessing the remote host.
- *host-ip-address* is the IP address of the remote host with the backup file.
- */tmp/backup-file.tgz* is the path and filename for the backup file.

Step 7   Restart the server:

```
service restart
```

Step 8   (Optional) Confirm that the Prime Network Services Controller server is operating as desired:

```
service status
```

Step 9   (Optional) Verify that the Prime Network Services Controller software version has been restored:

```
show version
```

Step 10   To confirm that Prime Network Services Controller is fully accessible, log in via the GUI.

What to Do Next

Perform the post-restoration tasks described in .

Post-Restoration Tasks

After you successfully restore Prime Network Services Controller, complete the following procedures to reestablish the previous environment:

- Update VM Managers—See Updating VM Managers, on page 4.

- Reimport InterCloud and VM images—See Reimporting InterCloud and VM Images, on page 4.

- Verify InterCloud status—See Verifying InterCloud Status, on page 5.

Updating VM Managers

You must update any configured VM Managers after you upgrade or restore Prime Network Services Controller.

Procedure

Step 1 Choose **InterCloud Management > Enterprise > VM Managers**.

Step 2 For existing vCenters that you wish to retain, reimport the vCenter Extension plugin. For more information, see the Cisco Prime Network Services Controller 3.0 User Guide.

Step 3 Check and delete any stale VM Manager entries.

Reimporting InterCloud and VM Images

Prime Network Services Controller does not restore InterCloud or VM images that were previously imported. After you restore Prime Network Services Controller, complete the following procedure to reimport any required InterCloud or VM images.

Before You Begin

Successfully restore Prime Network Services Controller as described in Restoring the Previous Version, on page 2.

Procedure

Step 1 Log into the Prime Network Services Controller GUI.

Step 2 Review the imported images in the following screens:

- VM Images—Choose **InterCloud Management > Enterprise > VM Images**.

- Infrastructure Images—Choose **InterCloud Management > InterCloud Link > Infrastructure Images**.

- InterCloud Agent Images—Choose **InterCloud Management > InterCloud Link > InterCloud Agent Images**.

Step 3 For each image that you want to reimport, note the image details, such as the image name, operating system, location, and version. If desired, you can delete images that you no longer use or need.

Note To find the original location of the image, right-click the image and choose **Edit**. The Edit dialog box includes the location and name of the source file.

Step 4   After noting the details, delete each image from Prime Network Services Controller.

Step 5   Reimport the images using the information that you collected in Step 3.

Verifying InterCloud Status

When a backup is performed, InterCloud-related tasks might be running but not completed. When the system is restored, Prime Network Services Controller starts the tasks from the point at which it was backed up. The following steps enable you to verify the status of InterCloud-related objects after you restore the system.

If a task fails for any reason, we recommend that you abort, terminate, or undeploy the task as appropriate, and then restart the task.

Before You Begin

Successfully restore Prime Network Services Controller as described in .

Procedure

Step 1   Choose **InterCloud Management > InterCloud Link > Provider Accounts** and confirm that the provider accounts are valid.

Step 2   Choose **InterCloud Management > InterCloud Link > VPCs >** *vpc* **>** *intercloud-link* and review the link status:

  • If an InterCloud link was deployed in the backed-up system, but is no longer deployed:

  1   Choose **Administration > Service Registry > Clients**.

  2   If the Oper State column contains *lost-visibility*, wait approximately 10 minutes to see if visibility is regained. If visibility is not regained after 10 minutes, continue with the next steps.

  3   In VMware vCenter, verify that the InterCloud Extender exists in the VM placement detail. The path in VMware is *vm-manager > datacenter > cluster/host > extender-vm >* **Edit > Placement**.

  4   In VMware vCenter, verify that the InterCloud Switch exists on the public cloud. The path in VMware is *vm-manager > datacenter > cluster/host > switch-vm >* **Edit > General**.

  5   If the InterCloud Extender or InterCloud Switch does not exist, undeploy and then delete the link.

  • If an InterCloud link was being deployed when the system was backed up and completed deployment after the backup, Prime Network Services Controller will attempt to deploy the link from the point at which the system was backed up. In this situation, do either of the following, as appropriate:

    • Because the InterCloud Extender and InterCloud Switch exist in the network, you can wait to see if the link will be deployed within a few minutes.

    • If the InterCloud link deployment task displays an error, undeploy the link and redeploy it.

Step 3   Choose **InterCloud Management > Public Cloud VPCs >** *vpc* **> VMs** and review cloud VM status:

- If a cloud VM was deployed and existed in the backed-up system but was deleted due to VM termination after the system backup:

  1 In the list of cloud VMs, obtain the cloud instance ID.

  2 Check the public cloud for the selected cloud instance.

  3 If the VM instance does not exist on the cloud, you can delete the VM.

- If a user created a cloud VM instance after the backup, the restored system will not have a record of it. There is no way to recover the cloud VM instance. You will need to create a new cloud VM.

- If a cloud VM was being instantiated when the system was backed up and completed deployment after the backup, Prime Network Services Controller will start the VM instantiation task from the point at which the system was backed up. In this situation, do either of the following, as appropriate:

  - Wait for a while to see if the cloud VM will be instantiated.

  - If the instantiation fails for any reason, terminate the VM instantiation process, and initiate a new cloud VM instantiation.

Step 4 Reconcile the InterCloud Switch and cloud VM public IP addresses.
If the InterCloud Switch and cloud VM public IP addresses are changed after the backup, you need to restore the IP addresses manually. This situation can occur if the InterCloud Switch or cloud VM is rebooted after the backup. To reconcile the IP addresses:

  1 If the InterCloud Switch is in lost-visibility state (**Administration > Service Registry > Clients**), reboot the InterCloud Switch by choosing **InterCloud Management > InterCloud Link > VPCs >** *vpc* > *intercloud-link* **> InterCloud Switch Tab >** *intercloud-switch* **> Reboot**.

  2 If the cloud VM tunnel is not *up* (**InterCloud Management > Public Cloud > VPCs >** *vpc* **> VMs**), reboot the cloud VM.

Step 5 Reconcile the InterCloud link and cloud VM that were created after the backup on Prime Network Services Controller, as follows:

  a) For InterCloud links that were created after the backup, do the following:

  1 Remove the InterCloud Extender in vCenter.

  2 Remove the InterCloud Switch in Amazon Web Services (AWS).

  3 Remove the cloud VMs from AWS.

  b) For Intercloud links that were deleted after the backup, perform the following steps in the Prime Network Services Controller GUI:

  1 Terminate the cloud VMs by choosing **InterCloud Management > InterCloud Link > VPCs > VMs tab >** *cloud-vm* **> Terminate**.

  2 Undeploy the InterCloud link by choosing **InterCloud Management > InterCloud Link > VPCs >** *vpc* > *intercloud-link* **> Undelploy**.

  3 Delete the InterCloud link by choosing **InterCloud Management > InterCloud Link > VPCs >** *vpc* > *intercloud-link* **> Delete**.