Managing SCVMM Infrastructure

This chapter contains the following sections:

Integrating SCVMM

To integrate SCVMM in Cisco UCS Director, perform the following actions:

- Install and configure the PowerShell agent (PSA).
- Add the PSA to Cisco UCS Director.
- Enable WinRM and WinRS on SCVMM and all SCVMM hosts.
- Make sure that the domain account used to connect SCVMM belongs to the local administrator group for SCVMM and SCVMM hosts.
- Ensure that a PowerShell Agent is added to the Hyper-V account when you create a Hyper-V account in Cisco UCS Director.

Configuring a PowerShell ExecutionPolicy Server

Step 1 Verify the current policy by executing Get-Executionpolicy cmdlet from the PowerShell command shell.

```
PS C:\Users\administrator\ Get-ExecutionPolicy Restricted
```

Note Make sure that you choose the correct policy type based on your infrastructure architecture. It is typically unrestricted.

Step 2 Type Set-ExecutionPolicy-ExecutionPolicy ExecutionPolicy unrestricted and press **Enter** to modify an existing execution policy.

```
PS C:\Users\administrator\ Set-ExecutionPolicy -ExecutionPolicy unrestricted

Execution Policy Change
```

```
The execution policy helps protect you from scripts that you do not trust.
Changing the execution policy might expose you to the security risks described in the about
_Execution_Policies help topic.
Do you want to change the execution policy?
[Y] Yes [N} No [S] Suspend [?] Help (default is "Y"): y
```

Enabling WinRM and WinRS

To accept remote PowerShell commands, you must enable Windows Remote Management (WinRM) for Windows Server 2008 R2, 2012 or 2012 R2. Once you enable the WinRM, the interoperability of hardware and operations systems is enabled to work with the Windows Remote Shell (WinRS) command-line tool on your target server and the target server hosts.

Before You Begin

The PowerShell Agent only executes the cmdlets and scripts on the target server in a PowerShell remote session. It requires the WinRM configuration to accept the remote session. This is a Windows PowerShell remote session requirement

Step 1 On your host(s), open a command prompt, and enter winrm quickconfig.

Note Configuring WinRM over HTTP or HTTPS depends on the requirements of the specific environment. HTTPS is only necessary if a secure connection is required. Instructions on configuring HTTPS communication is available at the following URL: https://blogs.technet.microsoft.com/meamcs/2012/02/24/how-to-force-winrm-to-listen-interfaces-over-https/

The following messages appear:

```
WinRM is not set up to allow remote access to this machine for management.
The following changes must be made:

Create a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine.
Enable the WinRM firewall exception.

Make these changes [y/n]?
```

Step 2 Enter **y**.

WinRM is updated for remote management, a listener is created to accept requests, and the firewall exception is enabled:

```
Make these changes [y/n]? y

WinRM has been updated for remote management.

Created a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine.
WinRM firewall exception enabled.
```

Step 3 Verify that WinRS is enabled by entering the winrm g winrm/config command at a command prompt.

Step 4 Configure the value `" * "` in the TrustedHosts table of WinRM by entering the winrm set winrm/config/client @{TrustedHosts="*"} command.

Note Adding the value " * " to the TrustedHosts table allows all hosts to be trusted or only add specific trusted IP addresses of target servers to the table.

What to Do Next

Make sure that the domain account used to connect the target server belongs to the local administrator group for the target server hosts.

Managing SCVMMs

In Cisco UCS Director, one SCVMM installation is considered as a cloud. Each cloud requires a unique name.

Step 1 On the menu bar, choose **Administration** > **Virtual Accounts**.
The virtual accounts available in Cisco UCS Director are displayed. The **Virtual Accounts** tab provides the following actions:

Action	Description
Refresh	Refreshes the current page.
Favorite	Adds this page to the **Favorites** tab which displays the page that you go to most often.
Add	Adds a virtual account to the Cisco UCS Director.

Step 2 Choose a virtual account to execute the following actions on the account:

Button Name	Description
View	Displays the cloud details.
Edit	Edits a cloud.
Delete	Deletes a cloud after confirmation.
Test Connectivity	Tests the connectivity of Cisco UCS Director to a cloud.
Manage Tag	Adds a tag to the cloud, edit the assigned tag, and delete the tag from the cloud. **Note** The tags that are assigned with the Taggable Entities as virtual accounts when you create a tag are displayed. For more information on the tab library, see Cisco UCS Director Administration Guide.
Add Tags	Adds a tag to the cloud. **Note** The tags that are assigned with the Taggable Entities as virtual accounts when you create a tag are displayed. For more information on the tab library, see Cisco UCS Director Administration Guide.

Button Name	Description
Delete Tags	Deletes one or more tags from the cloud. **Note** The tags that are assigned with the Taggable Entities as virtual accounts when you create a tag are displayed. For more information on the tab library, see Cisco UCS Director Administration Guide.

Adding a Cloud

In Cisco UCS Director, one SCVMM installation is considered as a cloud. Each cloud requires a unique name.

Step 1 On the menu bar, choose **Administration** > **Virtual Accounts**.

Step 2 In the **Virtual Accounts** pane, choose an SCVMM cloud.

Step 3 Click **Add**.

Step 4 In the **Add Cloud** dialog box, complete the following fields:

Name	Description
Cloud Type drop-down list	Choose **Hyper-V** as the cloud type.
Cloud Name field	The name of the cloud. All reports refer to the cloud using this cloud name. **Note** The following special characters are not allowed in cloud name: **.**, **$**,**@**.
User Credential Policy check box	Check this check box to use the policy to assign credentials to the account.
Credential Policy field	This field appears only when the **User Credential Policy** check box is checked. Choose the credential policy.
PowerShell Agent drop-down list	Choose a PowerShell agent for Hyper-V.
Server Address field	The IP address of the SCVMM server.
Server User ID field	This field appears only when the **User Credential Policy** check box is unchecked. The user ID of the SCVMM server.
Server Password field	This field appears only when the **User Credential Policy** check box is unchecked. The password of the SCVMM server.
Domain field	The domain of the SCVMM server.

Name	Description
Description field	The description of the cloud.
Contact Email field	The email address that you can use to contact the administrator or other person responsible for this account.
Location field	The location of this account.
Pod drop-down list	Choose a pod to which this account belongs.
Service Provider field	(Optional) The name of the service provider associated with this account, if any.

Step 5 Click **Add**.

What to Do Next

Test the connectivity to the cloud account.

Testing Cloud Connectivity

Step 1 On the menu bar, choose **Administration** > **Virtual Accounts**.

Step 2 In the **Virtual Accounts** pane, choose an SCVMM cloud.

Step 3 Click **Test Connectivity**.
A connected cloud appears green.

What to Do Next

Verify that the cloud and the cloud data are being collected.

Verifying Cloud Discovery

Step 1 On the menu bar, choose **Virtual** > **Compute**.

Step 2 In the **Compute for All Clouds** pane, choose an SCVMM cloud.
It may take a few minutes to complete automatic discovery and populate all the data. Cisco UCS Director displays a set of tabs that contain information about the components of that account that it has discovered.

Viewing the Topology

You can view the topology of VM network, host network, and cluster network.

Step 1 On the menu bar, choose **Virtual** > **Compute**.

Step 2 In the **Compute** pane, choose an SCVMM cloud.

Step 3 To view the network connectivity of VMs, click the **VM** tab and do the following:

a) Choose a VM and click **View Details**.
b) Click the **VM Network Connectivity** tab.
c) Choose the VM network connectivity and click **View Connectivity**.
The **Topology View - VM Network Connectivity** dialog box is displayed with a view of the topology and connectivity of the devices in the VM.
d) If desired, you can modify the following view options:

- **View Mode** drop-down list—Adjusts the spacing and positioning of the devices. The mode determines which options are available for you to customize the topology view. You can choose between the following view modes:
    - **Hierarchical**
    - **Concentric**
    - **Circular**
    - **Force Directed**
- **Allow Item Spacing** check box—Increases the distance between devices for the Hierarchical view mode.
- **Distance** control—Adjusts the distance between devices for the Concentric view mode.
- **Radius** control—Changes the radius of the circle and therefore adjusts the distance between devices for the Circular view mode.
- **Rigidity** control—Adjusts the rigidity for the Force Directed view.
- **Force Distance** control—Adjusts the distance between devices for the Force Directed view.

e) Click **Close** to return to the **VM Network Connectivity** tab.
f) Click **Back**.

Step 4 To view the network connectivity of cluster network, click the **Clusters** tab and do the following:

a) Choose a cluster and click **View Details**.
b) Click the **Cluster Network Connectivity** tab.
c) Choose the network connectivity and click **View Connectivity**.
The **Topology View - Cluster Network Connectivity** dialog box is displayed with a view of the topology and connectivity of the devices in the cluster network.
d) If desired, you can modify the following view options:

- **View Mode** drop-down list—Adjusts the spacing and positioning of the devices. The mode determines which options are available for you to customize the topology view. You can choose between the following view modes:
    - **Hierarchical**
    - **Concentric**
    - **Circular**
    - **Force Directed**
- **Allow Item Spacing** check box—Increases the distance between devices for the Hierarchical view mode.
- **Distance** control—Adjusts the distance between devices for the Concentric view mode.
- **Radius** control—Changes the radius of the circle and therefore adjusts the distance between devices for the Circular view mode.
- **Rigidity** control—Adjusts the rigidity for the Force Directed view.
- **Force Distance** control—Adjusts the distance between devices for the Force Directed view.

e) Click **Close** to return to the **Cluster Network Connectivity** tab.
f) Click **Back**.

Step 5 To view the network connectivity of host, click the **Host Nodes** tab and do the following:

a) Choose a host node and click **View Details**.
b) Click the **Host Network Topology** tab.
c) Choose the host network topology and click **View Connectivity**.
The **Topology View - Cluster Network Connectivity** dialog box is displayed with a view of the topology and connectivity of the devices in the cluster network.
d) If desired, you can modify the following view options:

- **View Mode** drop-down list—Adjusts the spacing and positioning of the devices. The mode determines which options are available for you to customize the topology view. You can choose between the following view modes:
    - **Hierarchical**
    - **Concentric**
    - **Circular**
    - **Force Directed**
- **Allow Item Spacing** check box—Increases the distance between devices for the Hierarchical view mode.
- **Distance** control—Adjusts the distance between devices for the Concentric view mode.
- **Radius** control—Changes the radius of the circle and therefore adjusts the distance between devices for the Circular view mode.
- **Rigidity** control—Adjusts the rigidity for the Force Directed view.
- **Force Distance** control—Adjusts the distance between devices for the Force Directed view.

e) Click **Close** to return to the **Host Network Topology** tab.
f) Click **Back**.