Configuring Cisco UCS Director PowerShell Agent

This chapter contains the following sections:

Adding PowerShell Agent to Cisco UCS Director

After PowerShell Agent is installed and running, you must add it to Cisco UCS Director. You must set up the virtual account (for example, an SCVMM account) to use the PowerShell Agent for inventory collection and other management functions.

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

Step 2 Click **Add**. In the **Add Agent** dialog box, complete the following fields.

Name	Description
Agent name field	The name of the PowerShell Agent.
Agent Address field	The IP address or FQDN (Fully Qualified Domain name) of the PowerShell Agent.

Name	Description
Agent Access Port field	The port assigned to the PowerShell Agent.
	Note The default port address is 43891. These values are pre-populated with default values. The PowerShell Agent is pre-configured to use these values and UCS Director must have matching values. These values can be changed on the Agent, but UCS Director must always use them as well.
Access key field	The default access key assigned to the PowerShell Agent.
	Note These values are prepopulated with default values. The PowerShell agent is preconfigured to use these values and Cisco UCS Director must have matching values. These values can be changed on the PowerShell Agent, but Cisco UCS Director must always use them as well.
Description field	The description of the PowerShell Agent.

Step 3   Click **Submit**.

What to Do Next

Verify connectivity between Cisco UCS Director and the PowerShell Agent.

Verifying Connectivity with Cisco UCS Director

After the PowerShell Agent is added, you can check the connectivity between Cisco UCS Director and the PowerShell Agent.

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

Step 2   Click the **Test Connect** icon.
Cisco UCS Director displays a success message if it can communicate with the PowerShell Agent.

If Cisco UCS Director cannot communicate with the PowerShell Agent, see

What to Do Next

Execute the Cisco UCS Director PowerShell command on the target server.

Troubleshooting Connectivity with Cisco UCS Director

Problem

You can experience a failed test connection with Cisco UCS Director. This problem can occur even though you successfully installed and configured the PowerShell Agent, and there is no issue with the network connectivity between PowerShell Agent and Cisco UCS Director.

Note This problem can happen with Windows Server 2012 R2 or other versions that use advanced cipher suites for https communication.

Symptom

When you check the PowerShell Agent logs in the PowerShell Agent server, you will find an **SSPI failed with inner exception** error. See a sample error message below:

2014-08-20 14:44:16,832 [6] ERROR cuic.ClientConnection[null] - Exception: A call to SSPI failed, see inner exception.
2014-08-2014:44:16,832 [6] DEBUG cuic.ClientConnection[null] - Inner exception: The message received was unexpected or badly formatted.
2014-08-2014:44:16,832 [6] DEBUG cuic.ClientConnection[null] - Authentication failed - closing the connection.

Cause

The test connection fails because of the Microsoft update, in which, new TLS cipher suites are added and cipher suite priorities are changed in Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2. See Microsoft kb article 2929281 for further information on this update.

Solution

To resolve the problem, you must modify the SSL cipher suite group policy setting. Follow the steps listed below:

1 At a command prompt, enter `gpedit.msc` to open your group policy editor.

2 Expand **Computer Configuration** > **Administrative Templates** > **Network**, and then click **SSL Configuration Settings**.

3 Under **SSL Configuration Settings**, click the **SSL Cipher Suite Order** setting.

4 In the **SSL Cipher Suite Order** pane, scroll to the bottom of the pane.

5 Follow the instructions labeled **How to modify this setting**.

It is necessary to restart the computer after modifying this setting for the changes to take effect.

Executing a Cisco UCS Director PowerShell Command on a Target Server

Cisco UCS Director provides a mechanism to test connectivity to a target server through the PowerShell Agent (end-to-end connectivity).

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

Step 2   Click the **Execute Command** icon.

Step 3   In the **Execute PowerShell Command** dialog box, complete the following fields:

Name	Description
Target Machine IP field	The IP address of the target machine.
User ID field	The unique ID assigned to the user.
Password field	The assigned password.
Domain field	The current server domain.
Commands/Script field	The field to enter your command to execute. **Note** Commands/scripts up to 64 kb in size are allowed.
Command Output field	The results of the execution appear in this field.

Step 4   Click **Execute**. The **Command Output** window displays the execution results.

Step 5   Click **Close**.

Example: Executing a PowerShell Agent Command on a Target Server

PowerShell Agent commands can be used in a workflow orchestration in Cisco UCS Director. A workflow can use a task that executes PowerShell commands against a target server.

A workflow, for example, can consist of the following Orchestrator elements:

- Start icon

- Execute PowerShell Command task icon

- Both Completed (Success) task and Competed (Failed)-task icons

The Execute PowerShell Command, for example, could use the following inputs:

- PowerShell Agent

- Target Server's credentials (IP address, username and password, and domain)

- Commands or Scripts of up to 64 kb.

Note Alternatively, you can provide the path to a PowerShell script on the target server (for example: `C:\scripts\DoSomething.ps1`) instead of providing a series of commands. The PowerShell Agent executes the script as long as it exists at the specified path on the target server.

In the above example, the PowerShell command is mapped to a user input, while the rest of the inputs are pre-configured within the task itself. When you execute the workflow in Cisco UCS Director, you are prompted to enter the PowerShell Agent commands to run on a target server. Use a ";" to separate multiple commands (for example, Hostname; Get-Process). Cisco UCS Director runs the commands against the target server and displays the output as an XML string in a service request log window.

Example: Setting Up PowerShell Agent and Running a Test Task

The following example outlines how you can set up PowerShell Agent on a Windows server and run a test task.

Step 1 Create a Microsoft Windows Server 2008 R2 or 2012 R2 VM.

Step 2 Make sure that the VM has the required .NET Framework and Windows PowerShell versions.

Step 3 Open a web browser and log on to Cisco UCS Director.

Step 4 From the **Administration > Virtual Accounts > PowerShell Agents** tab, download the PowerShell Agent and install it on the VM.

Step 5 In Windows Firewall, open the port that has been configured for the PowerShell Agent (the default port is 43891) or stop the firewall.

Step 6 Open PowerShell and run the following commands:
Enable-PSRemoting -Force

Set-Item WSMan:\localhost\Client\TrustedHosts -Value "*" -Force

Restart-Service WinRM

Set-ExecutionPolicy unrestricted -Force

Step 7 On the PowerShell Agent tab in Cisco UCS Director, click **Execute Command** option. In the **Execute PowerShell Command** dialog box, in addition to providing the IP address, user credentials of the VM, and the server domain, enter the following command in the Commands/Scripts field:
Echo "Import-ActiveDirectory" > c:\test.ps1

Step 8 Check the output for the test task on the C drive of the VM.