Installing Cisco UCS Director PowerShell Agent

This chapter contains the following sections:

Prerequisites

Before you install Cisco UCS Director PowerShell Agent, make sure that the following software has been installed on the machine:

- Supported Windows operating system.
- Supported .NET Framework (Full Package).
- Configure WinRM on any device that the PowerShell Agent communicates with.

For more information about the system requirements and supported software, see the Compatibility Matrix for Cisco UCS Director.

Enabling WinRM and WinRS

The PowerShell Agent executes cmdlets and scripts on the target server in a PowerShell remote session. To accept remote PowerShell commands, enable Windows Remote Management (WinRM), change the startup type to *Automatic*, create a "listener" to respond to WinRS commands, and start the service on each computer you want to work with. This provides connectivity to Windows Remote Shell (WinRS), the client side of WS-Management protocol.

To enable WinRM, run a configuration command. The command creates a "listener" and also opens an exception for WinRM in Windows Firewall.

Procedure

Step 1 Open a command prompt, and enter the command:
winrm quickconfig

You receive the following output:

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

Set the WinRM service type to delayed auto start.
Start the WinRM service.
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**.
You receive the following output:

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

WinRM has been updated for remote management.

WinRM service type changed successfully.
WinRM service started.
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 WinRM is enabled by executing the following command:
get-service winrm

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

When you are working with computers in workgroups or home groups, either use HTTPS as the transport or add the remote machine to the TrustedHosts configuration settings to enable authentication.

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. For more details, see https://blogs.technet.microsoft.com/meamcs/2012/02/24/how-to-force-winrm-to-listen-interfaces-over-https/ .

What to Do Next

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

Configuring the Firewall

The PowerShell Agent listens for incoming requests on port 43891. This is the default port. Configure your machine's firewall to allow incoming TCP requests on any other port of your choice.

Cisco UCS Director services create an access key, that is used for secure communication on that port. Copy that key from the main Cisco UCS Director interface and enter it into the PowerShell Agent host.

Downloading Cisco UCS Director PowerShell Agent

Download the installer for PowerShell Agent from Cisco UCS Director to your native Windows machine.

Procedure

Step 1 Choose **Administration** > **Virtual Accounts**.

Step 2 Click **PowerShell Agents**.

Step 3 Click **Download Installer**.

Step 4 Review the list of installation requirements on the **Download Agent Installer** page. Ensure that you have them available on the Windows machine where you plan to install the PowerShell Agent.

Step 5 Click **Submit**.
The `PSASetup.exe` file is downloaded to your native Windows machine default download folder.

What to Do Next

Install Cisco UCS Director PowerShell Agent on your Windows machine.

Installing Cisco UCS Director PowerShell Agent

Install the PowerShell Agent on your native Windows machine to enable the Cisco PSA service.

Installing a newer version of the PowerShell Agent requires that you uninstall the older version first. To remove the older version of PowerShell Agent, stop the Cisco PSA Service first and then uninstall the PowerShell agent. After uninstalling the PowerShell agent, navigate to the Cisco PSA Service folder (C:\Program Files (x86)\Cisco Systems\Cisco PSA Service) and check if any PSA files exist. If the PSA files remain in the Cisco PSA Service folder even after uninstallation, delete all the files.

Note If you get the **Error 1001** error message while uninstalling the PowerShell agent, delete the PSA registry folders.

To delete the PSA registry folders, do the following:

1. Open the Windows Registry Editor (**Start > Run> regedit.exe**).
2. In the left pane of the Registry Editor, right-click and choose **Find**.
3. In the **Find What** field, enter PSAServiceNew and click **Find Next** to view the PSA registry folders.
4. Right-click and choose **Delete** to delete the PSA registry folders.

Note If you do not install the current version of PowerShell Agent for Cisco UCS Director on the Windows machine, some tasks or options on the **PowerShell Agents** tab are not available.

Before You Begin

- You need system administrator privileges to complete this task.
- Enable WinRM.
- Configure Firewall.

Procedure

Step 1 If necessary, copy the `PSASetup.exe` file that you downloaded from Cisco UCS Director to your target Windows machine.

Step 2 Double-click the **PSASetup.exe** file.

Step 3 In the **Cisco PSA Service - InstallShield Wizard** screen, click **Next**.

Step 4 In the **Ready to install the Program** screen, click **Install**.
The **Installing Cisco PSA Service** screen displays during the installation. When the installation is complete, the **InstallShield Wizard Completed** message is displayed.

Step 5 Click **Finish**.
The PowerShell Agent is installed to the `C:\Program Files (x86)\Cisco Systems\Cisco PSA Service` folder. This folder is referred to as `%AGENT_INSTALL_FOLDER%` in the remainder of the document.

Step 6 Verify that the Cisco PSA Service is running on the Windows machine by checking the Resource Monitor.

Updating Ports and Authentication Properties for PowerShell Agent

By default, the PowerShell Agent uses port 43891 and it also uses a predefined authentication key to communicate with Cisco UCS Director. You can change these values by modifying the following file:

`%AGENT_INSTALL_FOLDER%/props/properties.xml`.

Before You Begin

Download and install the Cisco UCS Director PowerShell Agent service on your target server.

Procedure

Step 1 Use a text editor to open the *properties.xml* file.

Step 2 Edit the authKey entry.

Step 3 Edit the serverPort entry.

Step 4 Save the file.

Note The port number and access key values must match the values that are specified in the PowerShell Agent. Cisco UCS Director cannot communicate with the PowerShell Agent if the entries do not match.

Step 5 Restart the Cisco UCS Director PowerShell Agent service if you modify any of the properties in the *properties.xml* file. This can be done from the Services snap-in (**Start > Services.msc**)

What to Do Next

If you change the default port, configure the firewall to match the new port.