Cisco UCS Director PowerShell Agent Installation and Configuration Guide

First Published: September 06, 2013

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
     800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-30461-01
THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© Cisco Systems, Inc. All rights reserved.
CONTENTS

Preface v
  Audience v
  Conventions v
  Related Documentation vii
  Documentation Feedback vii
  Obtaining Documentation and Submitting a Service Request vii

CHAPTER 1 Overview 1
  About Cisco UCS Director 1
  About Cisco UCS Director PowerShell Agent 2
  Prerequisites 2
  System Requirements 2

CHAPTER 2 Installation of Cisco UCS Director PowerShell Agent 3
  Installing Cisco UCS Director PowerShell Agent 3
  Updating Authentication Properties 4
  Configuring the Firewall 4
  Enabling WinRM and WinRS 5

CHAPTER 3 Configuring Cisco UCS Director PowerShell Agent 7
  Configuring Cisco UCS Director PowerShell Agent 7
  Adding PowerShell Agent to Cisco UCS Director 7
    Verifying Connectivity with Cisco UCS Director 8
  Executing a Cisco UCS Director PowerShell Command on a Target Server 9
  Executing a PowerShell Agent Command on a Target Server 9
Preface

This preface contains the following sections:

- Audience, page v
- Conventions, page v
- Related Documentation, page vii
- Documentation Feedback, page vii
- Obtaining Documentation and Submitting a Service Request, page vii

Audience

This guide is intended primarily for data center administrators who use Cisco UCS Director and who have responsibilities and expertise in one or more of the following:

- Server administration
- Storage administration
- Network administration
- Network security

Conventions

<table>
<thead>
<tr>
<th>Text Type</th>
<th>Indication</th>
</tr>
</thead>
<tbody>
<tr>
<td>GUI elements</td>
<td>GUI elements such as tab titles, area names, and field labels appear in this font. Main titles such as window, dialog box, and wizard titles appear in this font.</td>
</tr>
<tr>
<td>TUI elements</td>
<td>In a Text-based User Interface, text the system displays appears in this font.</td>
</tr>
<tr>
<td>Text Type</td>
<td>Indication</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>System output</td>
<td>Terminal sessions and information that the system displays appear in this</td>
</tr>
<tr>
<td></td>
<td>font.</td>
</tr>
<tr>
<td>CLI commands</td>
<td>CLI command keywords appear in this font. Variables in a CLI command appear</td>
</tr>
<tr>
<td></td>
<td>in this font.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Elements in square brackets are optional.</td>
</tr>
<tr>
<td>{x</td>
<td>y</td>
</tr>
<tr>
<td>[x</td>
<td>y</td>
</tr>
<tr>
<td>string</td>
<td>A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.</td>
</tr>
<tr>
<td>&lt; &gt;</td>
<td>Nonprinting characters such as passwords are in angle brackets.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Default responses to system prompts are in square brackets.</td>
</tr>
<tr>
<td>!, #</td>
<td>An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.</td>
</tr>
</tbody>
</table>

**Note**

Means reader take note. Notes contain helpful suggestions or references to material not covered in the document.

**Tip**

Means the following information will help you solve a problem. The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.

**Caution**

Means reader be careful. In this situation, you might perform an action that could result in equipment damage or loss of data.

**Timesaver**

Means the described action saves time. You can save time by performing the action described in the paragraph.
IMPORTANT SAFETY INSTRUCTIONS

Warning

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

Related Documentation

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to ucs-director-docfeedback@cisco.com. We appreciate your feedback.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation.

Subscribe to the What's New in Cisco Product Documentation as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.
Overview

This chapter contains the following sections:

- About Cisco UCS Director, page 1
- About Cisco UCS Director PowerShell Agent, page 2
- Prerequisites, page 2
- System Requirements, page 2

About Cisco UCS Director

Cisco UCS Director (formerly Cisco Cloupia Unified Infrastructure Controller) is a 64-bit appliance that uses the following standard templates:

- Open Virtualization Format (OVF) for VMware vSphere
- Virtual Hard Disk (VHD) for Microsoft Hyper-V

Cisco UCS Director delivers unified, highly secure management for the industry's leading converged infrastructure solutions, which are based on the Cisco UCS and Cisco Nexus platforms.

Cisco UCS Director extends the unification of computing and network layers through Cisco UCS to provide data center administrators with comprehensive visibility and management capability. It supports NetApp FlexPod and ExpressPod, EMC VSPEx, and VCE Vblock systems, based on the Cisco UCS and Cisco Nexus platforms.

Cisco UCS Director automates the provisioning of resource pools across physical, virtual, and bare-metal environments. It delivers native, automated monitoring for health, status, and resource utilization. For example, you can do the following using Cisco UCS Director:

- Create, clone, and deploy service profiles and templates for all servers and applications
- Monitor organizational usage, trends, and capacity across a converged infrastructure on a continuous basis, such as by viewing heat maps that show virtual machine (VM) utilization across all your data centers
- Deploy and add capacity to ExpressPod and FlexPod infrastructure in a consistent, repeatable manner
- Manage, monitor, and report on Cisco UCS domains and their components
• Extend virtual service catalogs to include physical infrastructures services
• Manage secure multitenant environments to accommodate virtualized workloads that run with nonvirtualized workloads

About Cisco UCS Director PowerShell Agent

Cisco UCS Director PowerShell Agent (PSA) is a lightweight, Microsoft Windows service application that provides the ability to manage applications that expose Windows PowerShell based northbound API calls. The PowerShell Agent acts as an interfacing layer between Cisco UCS Director and applications such as Xen Desktop Controller, that is managed through Windows PowerShell. Once the PowerShell Agent is installed and started, you can manage it from Cisco UCS Director.

Note
The PowerShell Agent consumes minimum memory or CPU cycles because it just relays the requests and responses back and forth between Cisco UCS Director and XenDesktop Controller (or other PowerShell enabled applications).

Prerequisites

Installation requirements for Cisco UCS Director PowerShell Agent

• Microsoft Windows Server 2008 R2 64-bit
• .NET Framework 4.0 (Full Package) or higher

Note
Cisco UCS Director executes scripts (commandlets) on the target server via remote execution. It is assumed that the target server’s north-bound PowerShell APIs support remote invocation.

System Requirements

<table>
<thead>
<tr>
<th>Element</th>
<th>Minimum Supported Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco UCS Director</td>
<td>Release 4.0</td>
</tr>
</tbody>
</table>
CHAPTER 2

Installation of Cisco UCS Director PowerShell Agent

This chapter contains the following sections:

- Installing Cisco UCS Director PowerShell Agent, page 3
- Updating Authentication Properties, page 4
- Configuring the Firewall, page 4
- Enabling WinRM and WinRS, page 5

Installing Cisco UCS Director PowerShell Agent

The installer for Cisco UCS Director PowerShell Agent can be downloaded from Cisco UCS Director directly.

Before You Begin

System administrator privileges.

Step 1
Choose Start > Administration > Virtual Accounts.

Step 2
Choose the PowerShell Agents tab.

Step 3
Click the Download Installer button.
The Download Agent Installer dialog box appears listing the installation requirements.

Step 4
Click Submit.
The executable file (PSASetup.exe) is downloaded to your machine.

Step 5
Copy the executable file to your target machine.

Step 6
Double-click the PSASetup.exe file. The Preparing to Install... dialog box appears.

Step 7
Click Next. The Ready to Install the Program dialog box appears.

Step 8
Click Install. The Installing Cisco PSA Service dialog box appears.
When the installation is completed, the InstallShield Wizard Completed dialog box appears.
Step 9  Click **Finish**. The PowerShell Agent is installed into the C:\Program Files (x86)\Cisco Systems\Cisco PSA Service folder (known as %AGENT_INSTALL_FOLDER% for the remainder of the document).

Step 10  From your PC, choose **Start** and enter services.msc into the text field.

Step 11  Press the **Enter** key. A list of currently services is displayed. Verify that the Cisco UCS Director PowerShell Agent service is listed and currently running.

---

**What to Do Next**

Configure Cisco UCS Director PowerShell Agent.

---

**Updating Authentication Properties**

The PowerShell Agent uses port 43891 (default) and it also uses a predefined authentication/access key to communicate with Cisco UCS Director. You can change these values, if needed, by modifying a properties file. The properties (XML) file is located in the following directory:

%AGENT_INSTALL_FOLDER%/props/properties.xml.

**Before You Begin**

You should download and successfully install the Cisco UCS Director PowerShell Agent installation program.

---

**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**  When the PowerShell Agent is added to Cisco UCS Director, the port number and access key values must match the values that are specified in the PowerShell Agent. Cisco UCS Director cannot able to communicate with the PowerShell Agent if the entries do not match.

**Step 5**  (Optional) 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**

Configure your firewalls.

---

**Configuring the Firewall**

The PowerShell Agent listens for incoming requests on port 43891 by default. Your machine's firewall needs to be configured so as to allow incoming TCP requests on port 43891 (or any port that you choose to use).
Enabling WinRM and WinRS

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

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

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.

Step 2
At the Make these changes [y/n] ? prompt, 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 winrmbest 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.

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.
Enabling WinRM and WinRS
CHAPTER 3

Configuring Cisco UCS Director PowerShell Agent

This chapter contains the following sections:

- Configuring Cisco UCS Director PowerShell Agent, page 7
- Executing a Cisco UCS Director PowerShell Command on a Target Server, page 9
- Executing a PowerShell Agent Command on a Target Server, page 9

Configuring Cisco UCS Director PowerShell Agent

Once Cisco UCS Director PowerShell Agent is installed and running on a Windows Server 2008 R2 machine, you need to add it to Cisco UCS Director. You must set up the virtual account (for example, XenDesktop Controller or Hyper-V SCVMM) to use the agent for inventory collection and other management functions.

Adding PowerShell Agent to Cisco UCS Director

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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent name field</td>
<td>The name of the PowerShell Agent.</td>
</tr>
<tr>
<td>Agent Address field</td>
<td>The IP address or FQDN (Fully Qualified Domain name) of the PowerShell Agent.</td>
</tr>
</tbody>
</table>
### 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.

---

**What to Do Next**

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target Machine IP</td>
<td>The IP address of the target machine.</td>
</tr>
<tr>
<td>User ID</td>
<td>The unique ID assigned to the user.</td>
</tr>
<tr>
<td>Password</td>
<td>The assigned password.</td>
</tr>
<tr>
<td>Domain</td>
<td>The current server domain.</td>
</tr>
<tr>
<td>Command</td>
<td>The field to enter your command to execute.</td>
</tr>
<tr>
<td>Command Output</td>
<td>The results of the execution appear in this field.</td>
</tr>
</tbody>
</table>

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

Step 5
Click Close.

Executing a PowerShell Agent Command on a Target Server

A workflow can use a task that executes PowerShell commands against a target server.

The workflow task Execute PowerShell Command uses the following inputs:

- PowerShell Agent
- Target Server's credentials (IP address, username and password, and domain)
- PowerShell command.
In addition, instead of a series of commands you can provide the path to a PowerShell script on the target server (for example: \scripts\DoSomething.ps1). The PowerShell Agent executes the script as long as it exists at the specified path on the target server.

The workflow consists of the following Orchestrator elements:

- Start icon
- Execute PowerShell Command task icon
- Both Completed (Success) task and Competed (Failed)-task icons

In the above example, the PowerShell command is mapped to a user input, while the rest of the inputs are preconfigured 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.