Cisco UCS Director Multi-Node Installation and Configuration Guide, Release 6.8

First Published: 2021-03-17

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

CONTENTS

Preface

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
- Virtualization and virtual machines

Conventions

Text Type	Indication
GUI elements	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**.
Document titles	Document titles appear in *this font*.
TUI elements	In a Text-based User Interface, text the system displays appears in `this font`.
System output	Terminal sessions and information that the system displays appear in `this font`.

Text Type	Indication
CLI commands	CLI command keywords appear in **this font**. Variables in a CLI command appear in *this font*.
[ ]	Elements in square brackets are optional.
{x | y | z}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

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

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

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.

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Warning IMPORTANT SAFETY INSTRUCTIONS

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

Cisco UCS Director Documentation Roadmap

For a complete list of Cisco UCS Director documentation, see the *Cisco UCS Director Documentation Roadmap* available at the following URL: http://www.cisco.com/en/US/docs/unified_computing/ucs/ucs-director/doc-roadmap/b_UCSDirectorDocRoadmap.html.

Cisco UCS Documentation Roadmaps

For a complete list of all B-Series documentation, see the *Cisco UCS B-Series Servers Documentation Roadmap* available at the following URL: http://www.cisco.com/go/unifiedcomputing/b-series-doc.

For a complete list of all C-Series documentation, see the *Cisco UCS C-Series Servers Documentation Roadmap* available at the following URL: http://www.cisco.com/go/unifiedcomputing/c-series-doc.

Note The *Cisco UCS B-Series Servers Documentation Roadmap* includes links to documentation for Cisco UCS Manager and Cisco UCS Central. The *Cisco UCS C-Series Servers Documentation Roadmap* includes links to documentation for Cisco Integrated Management Controller.

Documentation Feedback

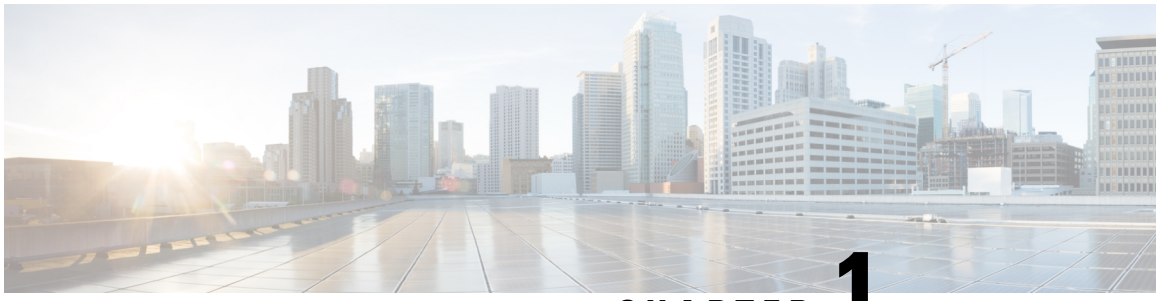
To provide technical feedback on this document, or to report an error or omission, please send your comments to ucs-director-docfeedback@cisco.com. We appreciate your feedback.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.



CHAPTER 1

Overview

This chapter contains the following sections:

About the Optimized Multi-Node Setup

In Cisco UCS Director versions prior to Release 6.7.4.x, the multi-node setup included the following nodes:

- One primary node
- One or more service nodes
- One monitoring database
- One inventory database

Similar to 6.7.4.x release, 6.8.0.0 also support same capabilities and scale with the following nodes:

- One database node
- One primary node

Note After upgrading to release 6.7.4.x, since the multi-node configuration requires only 2 VMs, you can claim the freed up VMs.

Minimum System Requirements for Optimized Multi-Node Setup

System Requirements for the Primary Node

Number of VMs	vCPU Allocation	Memory Allocation (GB)	Memory Reservation (GB)	Disk Size (GB)	Inframgr Memory Allocation (GB)
1 - 5000	4	16	16	100	8
5001 - 10000	4	22	22	100	12
10001 - 15000	4	28	28	100	12
15001 - 20000	4	34	34	100	16
20001 - 25000	8	40	40	100	16
25001 - 30000	8	46	46	100	24
30001 - 35000	8	52	52	100	24
35001 - 40000	8	58	58	100	28
40001 - 45000	8	64	64	100	28
45001 - 50000	8	64	64	100	32

You can configure the Inframgr memory allocation in the `/opt/infra/bin/inframgr.env` file.

System Requirements for the Database Node

Number of VMs	vCPU Allocation	Memory Allocation (GB)	Memory Reservation (GB)	Disk Read I/O Bandwidth (MBps)	Disk Write I/O Bandwidth (MBps)	Disk Size (GB)	MySQL InnoDB Buffer Pool (GB)
1 - 5000	4	12	12	4	4	100	8
5001 - 10000	4	16	16	6	6	100	12
10001 - 15000	4	28	28	8	8	100	24
15001 - 20000	4	40	40	10	10	200	36
20001 - 25000	8	52	52	12	12	200	48

Number of VMs	vCPU Allocation	Memory Allocation (GB)	Memory Reservation (GB)	Disk Read I/O Bandwidth (MBps)	Disk Write I/O Bandwidth (MBps)	Disk Size (GB)	MySQL InnoDB Buffer Pool (GB)
25001 - 30000	8	64	64	14	14	200	60
30001 - 35000	8	76	76	16	16	300	72
35001 - 40000	16	90	90	18	18	600	84
40001 - 45000	16	90	90	20	20	600	84
45001 - 50000	16	90	90	22	22	600	84

You can configure the MySQL InnoDB Buffer Pool parameter in the `/etc/my.cnf` file.

Note To determine the currently configured disk read I/O bandwidth and disk write I/O bandwidth, use the **Collect Diagnostics** option from the Cisco UCS Director Shell Admin menu.

MySQL Parameters

VMs	Thread Cache Size	Maximum Connections	innodb lock wait timeout	Query Cache Size (MB)	Maximum Connection Errors	Connection Timeout	innodb read I/O Threads	innodb write I/O Threads
1 - 5000	1000	1000	100	128	10000	20	64	64
5001 - 10000	1000	1000	100	128	10000	20	64	64
10001 - 15000	1000	1000	100	128	10000	20	64	64
15001 - 20000	1000	1000	100	128	10000	20	64	64
20001 - 25000	2000	2000	100	128	10000	20	64	64
25001 - 30000	2000	2000	100	128	10000	20	64	64
30001 - 35000	4000	2000	100	128	10000	20	64	64

VMs	Thread Cache Size	Maximum Connections	innodb lock wait timeout	Query Cache Size (MB)	Maximum Connection Errors	Connection Timeout	innodb read I/O Threads	innodb write I/O Threads
35001 - 40000	4000	4000	100	128	10000	20	64	64
40001 - 45000	4000	4000	100	128	10000	20	64	64
45001 - 50000	4000	4000	100	128	10000	20	64	64

Configure these parameters in the `/etc/my.cnf` file.

Guidelines and Limitations for Optimized Multi-Node Setup

Before you configure an optimized multi-node setup, review the following guidelines:

- Plan the locations and IP addresses of your nodes carefully. You cannot change the types of any nodes. For example, you cannot reconfigure a database node as a primary node or a primary node as a database node.
- Install licenses only on the primary node.
- After you configure the nodes, the list of operations available in the shelladmin changes for the database node and the primary node.
- If you modify your standalone configuration to a multi-node setup, you cannot revert to the standalone configuration unless you took a snapshot of the standalone configuration.
- Connector packs are installed only on the primary node, while Cisco UCS Director patch releases are installed on the database node. As a result, you may notice a discrepancy of software versions between the primary node and the database node.

Best Practices for an Optimized Multi-Node Setup

Before you configure a multi-node setup for Cisco UCS Director, consider the following best practices:

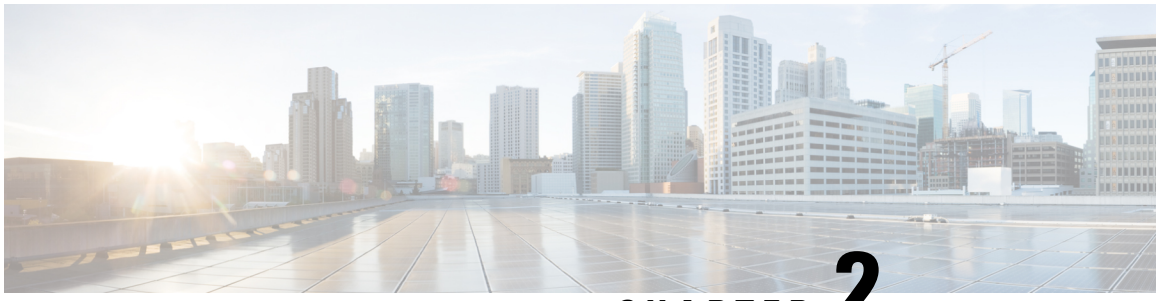
- To maximize output and minimize network latency, we recommend that the primary node and the database node reside on the same host.
- Network latency (average RTT) between the primary or service node and the physical, virtual compute, storage, and network infrastructures should be minimized. A lower average RTT results in increased overall performance.
- You can reserve more CPU cycles (MHz) and memory than recommended for better performance at system load.

  See System Requirements for the Primary Node, on page 2 and System Requirements for the Database Node, on page 2.

- You must configure passwordless authentication between the application node and the database node to:
  - Use the backup and restore feature available in Cisco Intersight on claimed UCS Director instances.
  - Enforce default password reset capability for SSH root and shelladmin users.

    You are prompted to reset the default SSH root user and shelladmin user passwords before logging into the Cisco UCS Director administrator interface. You will be prompted to reset these passwords only if you have not reset the passwords prior to upgrading to release 6.7(4.0). In an optimized multi-node environment, you must reset the password for these user accounts on the application node and the database node.

See Setting Up Passwordless Authentication, on page 9.



CHAPTER 2

Configuring Optimized Multi-Node Setup

Database Node

The database node hosts the database service in a multi-node setup. While configuring a multi-node setup for the first time with Release 6.8.0.0, you must always first configure the database node.

If you are Migrating/Upgrading the existing 6.7.4.x to 6.8, please following the Cisco UCS Director Upgrade Guide, Release 6.8.

Primary Node

The primary node in the optimized multi-node setup runs the Cisco UCS Director software services, and also acts as the front-end user interface node. While configuring the optimized multi-node setup with release 6.8.0.0, you must first configure the database node, and then configure the primary node.

Configuring a Database Node

Procedure

Step 1 Login to the Cisco UCS Director Shell Admin Console on the node that you want to configure as the database node.

Step 2 From the menu, choose `Configure Multi-Node` and press **Enter**.

Step 3 When prompted, enter **y** to configure the multi- node setup.

Step 4 When prompted, enter **2** to configure the node as the database node.

Step 5 When prompted, enter **y** to confirm configuring the current node as the database node.

Step 6 When prompted, enter and confirm a new root password for the MySQL database.

Step 7 When prompted, enter and confirm the admin password for the MySQL database.

Step 8 When prompted, enter **y** to log out so that the changes can take effect.

Step 9 After you are logged out, log back on to the Cisco UCS Director shelladmin on the database node.

After you return to the Shell Admin, the menu options change to those available for a database node.

What to do next

Configure the primary node.

Configuring the Primary Node

Before you begin

You should have configured the database node. See Configuring a Database Node, on page 7.

Procedure

Step 1 Login to the Cisco UCS Director Shell Admin Console on the node that you want to configure as the primary node.

Step 2 From the menu, choose `Configure Multi-Node` and press **Enter**.

Step 3 When prompted, enter **y** to configure the multi-node setup.

Step 4 When prompted, enter **1** to configure the node as the primary node.

Step 5 When prompted, enter y to confirm configuring the current node as the primary node.

Step 6 When prompted, enter the database node IP address.

Note Do not configure multiple primary nodes with the same database node IP address. This will lead to data corruption. If the database node IP address of one multi-node configuration has to be configured for a primary node in a different multi-node configuration, then you must first stop the services running on the primary node.

Step 7 When prompted, enter the password for the mySQL root user and admin user for the database node.

Step 8 When prompted, enter **y** to log out so that the changes can take effect.

Step 9 After you are logged out, log back on to the Cisco UCS Director shelladmin on the primary node.

After you return to the Shell Admin, the menu options change to those available for a primary node.

Converting a Standalone Configuration to a Multi-Node Configuration

Complete the following procedure to convert your release 6.7 standalone configuration to a multi-node configuration.

Procedure

Step 1 Take a snapshot of the existing standalone VM.

Step 2 Deploy a new Cisco UCS Director VM, and configure it as the database node.

For more information, see Configuring a Database Node, on page 7.

Step 3 Take the backup of the database of the existing standalone VM.

Step 4 Configure the existing standalone VM as the primary node.

As part of this configuration, you will need to provide the IP address of the database node. For more information, see Configuring the Primary Node, on page 8.

Step 5 Restore the data from the database backup.

Step 6 If you have configured Bare Metal Agent accounts, run the following script in the primary node to re-configure the database IP configured in the BMA.

```
/opt/scalability/migration/updateDatabaseIPForBMAAccounts.sh
```

Step 7 Start the Cisco UCS Director services in the primary node.

Setting Up Passwordless Authentication

In an optimized multi-node setup, prior to installing or upgrading the base platform pack to version 6.7.3.1 and later or to Cisco UCS Director 6.7(4.0) and later, you must first configure passwordless authentication between the primary node and the database node. You need to configure this form of authentication only once and need not repeat it before upgrading to later versions.

Procedure

Step 1 Login to the primary node.

Step 2 Run the following command on the primary node: **cd /opt/scalability**.

Step 3 Run the **./passwordlessConnectivity** command to start the passwordless authentication setup.

Step 4 When prompted, enter the database node IP address.

Step 5 When prompted, enter **root** as the username for the database node.

Step 6 When prompted, enter **y** to generate the key.

Step 7 At the confirmation prompt, enter **yes**if you want to configure yet another node for passwordless connectivity.

Step 8 If you are installing a new version of Cisco UCS Director using the OVA, and if the default **root** user password of the database node is not reset already, you are prompted to change the password.

Step 9 When prompted, enter the password for the **root** user of the database node.

A confirmation message stating that passwordless authentication for the **root** user on the database node is displayed.

Step 10 Run the **chmod 600 ~/.ssh/id_rsa** command.
This completes the passwordless authentication setup.

Step 11 Run the **sudo ssh <<username>>@<<db nodeIp>>** command to verify the completion of the setup.

If you are logged in to the database node after running this command, then passwordless authentication is successfully configured.

Step 12 (Optional) If you cannot login to the database node without a password, login to the primary node and delete the entry of the database node from the `~/.ssh/id_rsa/known_hosts` file and repeat this procedure.