System Requirements

This chapter lists the tested and supported hardware and software specifications for Cisco Prime Data Center Network Management (DCNM) server and client architecture. The application has been tested in English locales only.

Deployment Best Practices

Keep the following guidelines in mind when deploying Cisco Prime DCNM:

- Database
  - Deploy an Oracle database on a separate server from the Cisco DCNM application server.
  - Deploy an Oracle database when managing production or mission-critical environments.
  - If you plan to use an Oracle 11g or Oracle 12c database, configure the Oracle database as follows:
    - Increase the number of sessions and processes to 150 each from the default of 50.
    - Increase the number of open cursors to 1000 from the default of 300.

- We recommend that you deploy Oracle11g or Oracle 12c for mission-critical production environments.

Note The password for the database expires after 180 days.

You must change the default setting by performing the following steps:

1. Log in to the Oracle database.
2. Enter the commands, as shown in this example:

```
SQL> GRANT CONNECT,RESOURCE,UNLIMITED TABLESPACE TO username IDENTIFIED by password;
Grant succeeded.
SQL> select username,password from dba_users where username='username';
SQL> ALTER PROFILE DEFAULT LIMIT
2 FAILED_LOG_ATTEMPTS UNLIMITED
```

```
3 PASSWORD_LIFE_TIME UNLIMITED;
Profile altered.
SQL> EXIT
```

- Network Time Protocol
  - We recommend that the Cisco Prime DCNM server run the Network Time Protocol (NTP) to synchronize its clock with those of the managed devices.
- General Guidelines
  - Do not deploy Cisco Prime DCNM when network latency is more then 50 ms from the switch management subnet to the Cisco Prime DCNM server and Cisco Prime DCNM database.
  - Deploy Cisco Prime DCNM on high-performance tier storage (2 to 4 ms response time).
  - Create users with the same password digest and encryption algorithm in the device (for example, Digest, MD5) and encryption algorithm (for example, DES). Cisco Prime DCNM will not authenticate the devices with different digest and encryption passwords.
  - Deploy Cisco Prime DCNM-SAN in a federation configuration when either of the following conditions is met:
    - The switch count exceeds 150 switches
    - The port count exceeds 15,000 connected ports for every management server
- Windows Operating System
  - During the initial installation, disable all security and antivirus tools that are running on your Windows servers.
  - Do not run any other management applications on the Cisco Prime DCNM server or the Cisco Prime DCNM database server.
- Virtual Machines
  - When Cisco Prime DCNM is deployed as a virtual machine, do not share CPU and memory resources with other virtual machines on the virtual host, and the data store with other virtual machines.
  - CPU and memory resource must be reserved for virtual machines.

Installation Notes

The following installation notes apply to Cisco Prime DCNM, Release 7.1.x:

- The Cisco Prime DCNM Installer includes the Cisco Prime DCNM server and clients, Device Manager, SMI-S provider, PostgreSQL 8.4, and Strawberry Perl Version 5.10.
- The Cisco Prime DCNM virtual appliance includes the Cisco Prime DCNM server and clients, Device Manager, PostgreSQL, Cisco XCP, OpenLDAP, RabbitMQ, DHCPD, all of which are installed on a 64-bit CentOS.

- For Cisco Prime DCNM Open Virtual Appliance (OVA), upgrade support is available from Cisco Prime DCNM, Release 7.0(1), and Cisco Prime DCNM, Release 7.0(2), to Cisco Prime DCNM, Release 7.1(1).

  For Cisco Prime DCNM Windows and Linux installers, upgrade support is available from Cisco Prime DCNM, Release 6.3(2), to Cisco Prime DCNM, Release 7.1(1).

- For Cisco Prime DCNM Open Virtual Appliance (OVA), upgrade support is available from Cisco Prime DCNM, Release 7.0(2), and Cisco Prime DCNM, Release 7.1(1), to Cisco Prime DCNM, Release 7.1(2).

  For Cisco Prime DCNM ISO Virtual Appliance (ISO), upgrade support is available from Cisco Prime DCNM, Release 7.1(1), to Cisco Prime DCNM, Release 7.1(2).

  For Cisco Prime DCNM Windows and Linux installers, upgrade support is available from Cisco Prime DCNM, Release 6.3(2), and Cisco Prime DCNM, Release 7.1(1), to Cisco Prime DCNM, Release 7.1(2).

- SMI-S integration into Cisco Prime DCNM is disabled for Cisco Prime DCNM 7.1(1) Virtual Appliances (OVA and ISO images). However, it is available for RHEL and Windows DCNM 7.1.1 images.

  SMI-S integration with storage arrays is available on all Cisco Prime DCNM 7.1(1) images, including Open Virtual Appliances.

- From Cisco Prime DCNM, Release 7.1(2), SMI-S provider is available in both Cisco Prime DCNM installer and Cisco Prime DCNM virtual appliance.

- On the Cisco Prime DCNM Web Client, clicking the Evaluation License URL under the **Admin > General > License > Server License Files** tab results in an***Invalid Referrer*** error message being displayed. This occurs if you have not signed out correctly during the previous instance. To resolve this, highlight the URL address in the web browser menu bar and press the **Return** key. Clear the web browser cache for the URL to work.

For information about installing Cisco Prime DCNM Release 7.1.x, see the corresponding version of the *Cisco Prime DCNM Installation Guide* at:

http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-data-center-network-manager/products-installation-guides-list.html.