Installation Guide for Cisco Evolved Programmable Network Manager 4.1

First Published: 2020-05-29

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

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.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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: https://www.cisco.com/c/en/us/about/legal/trademarks.html. 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. (1721R)

© 2020 Cisco Systems, Inc. All rights reserved.

CONTENTS

Full Cisco Trademarks with Software License ?

CHAPTER 1 **Cisco EPN Manager 4.1 Installation** 1

- Installation Overview 1
- Installation Paths for Cisco EPN Manager 4.1 2
- Prerequisites for Cisco EPN Manager 4.1 Installation 2
  - Licensing 2
  - Disable Automatic Client Logout 3
- Install Cisco EPN Manager 4.1 in a Standard Environment (No HA) 3
  - Place the Cisco EPN Manager 4.1 Installation File on the Server 4
  - Install Cisco EPN Manager 4.1 (No HA) 4
  - Synchronize the Inventory of All Devices with the Database (Existing Deployments Only) 5
- Install Cisco EPN Manager 4.1 in a High Availability Environment 6
  - Perform the General and HA Installation Prerequisite Tasks 6
  - Remove the HA Configuration 6
  - Place the Cisco EPN Manager 3.1 Installation File on the Server (HA Deployment) 7
  - Install Cisco EPN Manager 4.1 on Primary and Secondary Servers (HA Deployment) 7
  - Check Readiness for HA Configuration 9

CHAPTER 2 **Cisco EPN Manager 4.1 High Availability** 13

- High Availability Overview 13
- High Availability Deployment Considerations 14
  - High Availability Deployment Models 14
  - Understand High Availability Limitations 15
  - Consider Whether You Can Use Virtual Addresses 15
  - Best Practices if Firewall is Used Between Primary and Secondary Servers 16

CHAPTER 3 **Upgrade to Cisco EPN Manager 4.1** 19

Valid Upgrade Paths 19

Upgrade to Cisco EPN Manager 4.1 (No HA) 20

Backup-Restore Upgrade (No HA) 20

Upgrade to Cisco EPN Manager 4.1 (High Availability) 20

Backup-Restore Upgrade (High Availability) 21

Post-Upgrade Tasks 22

CHAPTER 4 **Install Geo Map Resource Files for Offline Use** 25

Install Geo Map Resource Files (Standard Deployment) 25

Place the Geo Map Resource Files on the Cisco EPN Manager Server 25

Install the Geo Map Resource Files on the Cisco EPN Manager Server 26

Configure the Cisco EPN Manager Server to Use the Installed Map Resources 27

Verify that the Geo Maps Files Were Installed Successfully 27

Install Geo Map Resource Files (High Availability Deployment) 28

Update Geo Map Resource Files After Upgrading to Cisco EPN Manager 28

CHAPTER 5 **Supplementary Installation-Related Information and Procedures** 31

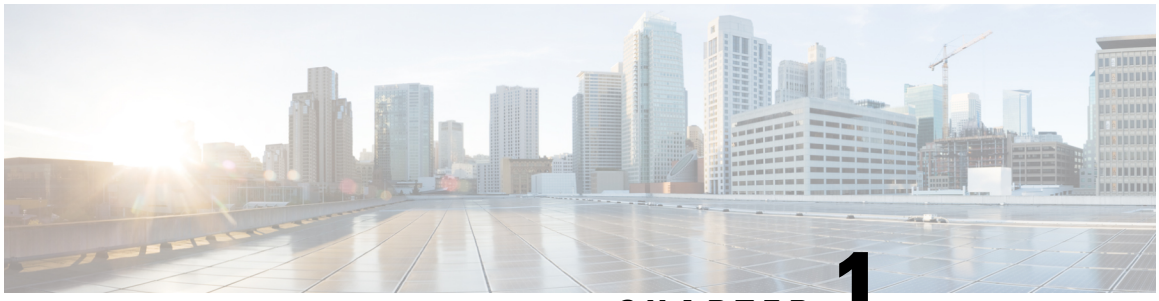
Log In and Out as the Linux CLI Users 31

Copy Files From a Client Machine to the Cisco EPN Manager Server 33

Synchronize the Hardware and NTP Clock 33

Log Into the Cisco EPN Manager Web GUI 35

Time Zones Supported by 36



CHAPTER 1

Cisco EPN Manager 4.1 Installation

This chapter provides the information required for planning your installation of Cisco EPN Manager 4.1 and ensuring that you meet all the prerequisites required for the installation. It also provides procedures for installing Cisco EPN Manager 4.1 in a standard, non-high availability environment. For high availability, see Cisco EPN Manager 4.1 High Availability, on page 13.

- Installation Overview, on page 1
- Installation Paths for Cisco EPN Manager 4.1 , on page 2
- Prerequisites for Cisco EPN Manager 4.1 Installation, on page 2
- Install Cisco EPN Manager 4.1 in a Standard Environment (No HA), on page 3
- Install Cisco EPN Manager 4.1 in a High Availability Environment, on page 6

Installation Overview

Cisco EPN Manager 4.1 can be installed as a fresh installation by following the given steps:

1. Install Cisco EPN Manager 4.0 either on a virtual machine or a bare metal server.

   You can refer to Cisco EPN Manager 4.0 Installation Guide

2. Install Cisco EPN Manager 4.1 UBF as explained in the steps in this guide

The following topics provide information and procedures for installing Cisco EPN Manager 4.1 UBF in standard and high availability deployments.

- Installation Paths for Cisco EPN Manager 4.1 , on page 2
- Prerequisites for Cisco EPN Manager 4.1 Installation, on page 2
- Install Cisco EPN Manager 4.1 (No HA), on page 4
- Install Cisco EPN Manager 4.1 on Primary and Secondary Servers (HA Deployment), on page 7

Note Before starting the installation procedure, please review the release notes for important information or issues relating to the installation.

Installation Paths for Cisco EPN Manager 4.1

The following table lists the valid paths for installing Cisco EPN Manager 3.1 from previous versions.

Current Cisco EPN Manager Version	Installation Path to Cisco EPN Manager 4.1
Cisco EPN Manager 4.0	**Cisco EPN Manager 4.0 > 4.1**
Cisco EPN Manager 4.0.1	**Cisco EPN Manager 4.0.1 > 4.1**

See the relevant installation guide for installation prerequisites and procedures for Cisco EPN Manager versions.

For point patch installation instructions, see the readme file supplied with the patch file on the on the Software Download site on Cisco.com.

Prerequisites for Cisco EPN Manager 4.1 Installation

Note Cisco EPN Manager 4.1 installation consists of Cisco EPN Manager 4.0 OVA/ISO installation followed by Cisco EPN Manager 4.1 UBF installation.

Before installing Cisco EPN Manager 4.1, you must perform the following tasks:

- Ensure that you have installed Cisco EPN Manager 4.0 either on a virtual machine or a bare metal server.

  You can refer to Cisco EPN Manager 4.0 Installation Guide:

- Licensing, on page 2
- Disable Automatic Client Logout

Licensing

Cisco EPN Manager includes a 90-day trial license that is automatically activated for first-time installations. To use the application beyond the trial period, you must obtain and install the necessary Cisco EPN Manager licenses for both production and non-production environments, as follows:

For a production environment:

- Base license (required)
- Standby license (optional)—Obtain this license if you will have a high availability deployment with two Cisco EPN Manager servers configured in a redundancy configuration.
- NBI license (optional)—Obtain this license if you will be using MTOSI or RESTCONF northbound interface features.
- Right-to-Manage licenses for the types and corresponding numbers of devices to be managed by Cisco EPN Manager.

For a non-production environment (e.g., lab validation or development environment), please obtain and install a Cisco EPN Manager lab license for each Cisco EPN Manager lab installation. The lab license covers all Cisco EPN Manager options, including redundancy (HA), and unlimited right-to-manage scope.

Do not make copies of licenses.

To purchase Cisco EPN Manager licenses, please contact your local sales representative.

For more information on the types of licenses available for Cisco EPN Manager, see the information on viewing and managing licenses in the Cisco Evolved Programmable Network Manager User and Administrator Guide.

Disable Automatic Client Logout

If the client is inactive for a certain period of time, you might be automatically logged out. To avoid being logged out during the installation, we recommend that you disable automatic logout of idle users in the system settings, as follows:

Procedure

Step 1 Go to **Administration** > **Settings** > **System Settings** > **Server**.

Step 2 In the Global Idle Timeout section, uncheck the **Logout all idle users** check box.

Step 3 Click **OK** in the displayed message reminding you to save your change to the system settings.

Step 4 Click **Save**.

Step 5 Click the **gear icon** at the top right of the web GUI window, then click **My Preferences**. Under User Idle Timeout, uncheck the **Logout idle user** check box.

Step 6 Click **Save**.

Step 7 Log out and then log back into Cisco EPN Manager.

Install Cisco EPN Manager 4.1 in a Standard Environment (No HA)

Follow these steps to install Cisco EPN Manager 4.1 in a standard environment (no high availability).

1. Make sure you have performed the tasks in Prerequisites for Cisco EPN Manager 4.1 Installation.
2. Place the Cisco EPN Manager 4.1 Installation File on the Server.
3. Install Cisco EPN Manager 4.1 (No HA).
4. Synchronize the Hardware and NTP Clock.
5. Perform an inventory collection for all devices to synchronize them with the database. See Synchronize the Inventory of All Devices with the Database (Existing Deployments Only).

If you are using external authentication and authorization, after installation you must export the user task information to your AAA server in order to pick up the latest updates. See the Cisco Evolved Programmable Network Manager User and Administrator Guide for more information.

Place the Cisco EPN Manager 4.1 Installation File on the Server

This procedure explains how to download the ubf installation file to your local machine, then upload it from your local machine to the Cisco EPN Manager server.

Note You need an account on Cisco.com in order to download the installation file.

Procedure

Step 1 Make sure you have performed the tasks in Prerequisites for Cisco EPN Manager 3.1 Installation.

Step 2 Download the required ubf file to your local machine.

a. Go to the Software Download site on Cisco.com.

b. Locate the Cisco EPN Manager Minor Release file (in the format **cepnm3.1-build560.ubf**).

c. Download the file to your local machine.

Step 3 After the file is downloaded to the local server, make sure to compare the checksum (MD5) with the one available on Cisco.com.

Step 4 Log into the Cisco EPN Manager web GUI as a user with Administrator privileges.

Step 5 Upload the ubf file from your local machine to the Cisco EPN Manager server.

a. From the left sidebar menu, choose **Administration > Software Update**.

b. Click the blue **Upload** link at the top of the page

.

c. In the Upload Update dialog box, click **Browse** and navigate to the file you downloaded previously.

d. Click **OK** to upload the file to the server.

After the successful upload of Cisco EPN Manager 4.1, the software will appear under the Files tab.

Install Cisco EPN Manager 4.1 (No HA)

Follow this procedure to install Cisco EPN Manager 4.1 in a standard environment with no high availability.

Procedure

Step 1 From the left sidebar, choose **Administration** > **Software Update**.

Step 2 Click the **Install** button associated with EPN Manager 4.1 on the Software Update page.

Step 3 Click **Yes** in the confirmation message pop-up window to proceed with the installation.

Note
The server will restart when the installation is complete.

Step 4 If you are asked whether to overwrite an existing file, click **Yes**.

After successful installation, the status will change to **Installed**. Cisco EPN Manager will auto-restart and the Cisco EPN Manager web GUI will not be accessible for some time.

Step 5 Check the status of the Cisco EPN Manager services.

a. Start an SSH session with the Cisco EPN Manager server and log in as the Cisco EPN Manager CLI admin user.
b. Run the **ncs status** command to ensure that, at a minimum, the following services are up and running: Health Monitor, Database, NMS, SAM Daemon, DA Daemon, Compliance Engine. Note that for optimal Cisco EPN Manager functionality, all services should be up and running.

Step 6 When the Cisco EPN Manager web GUI is accessible, log in and check that the Cisco EPN Manager Minor Release's status is “Installed” in the Software Update page.

a. From the left sidebar, choose **Administration** > **Software Update**.
b. Verify that **Cisco EPN Manager Minor Release** is listed as Installed under the Updates tab. Also verify that the ubf file (in the format **cepnm3.1-build560.ubf**) is listed in the Files tab and that the In Use status is **Yes**.

What to do next

Go to Synchronize the Hardware and NTP Clock.

Note The service restart in the Synchorization Clock operation can be ignored as the installation of Cisco EPN Manager Minor Release restarts the Cisco EPN Manager.

Synchronize the Inventory of All Devices with the Database (Existing Deployments Only)

If you have already been using a previous version of Cisco EPN Manager (i.e., this is not a fresh installation), you need to perform a Sync operation on the devices. The Sync operation instructs Cisco EPN Manager to collect device physical and logical inventory and save the information to the database.

Procedure

Step 1 Choose **Monitor** > **Network Devices**.

Step 2 Select all devices, then click **Sync**.

Install Cisco EPN Manager 4.1 in a High Availability Environment

Follow these steps to install Cisco EPN Manager 4.1 in a HA environment.

1. Perform the General and HA Installation Prerequisite Tasks.
2. Remove the HA Configuration.
3. Place the Cisco EPN Manager 4.1 Installation File on the Server (HA Deployment).
4. Install Cisco EPN Manager 4.1 on Primary and Secondary Servers (HA Deployment).
5. Synchronize the Hardware and NTP Clock.
6. Synchronize the Inventory of All Devices with the Database (Existing Deployments Only).

Note If you are using external authentication and authorization, after installation you must export the user task information to your AAA server in order to pick up the latest updates.

Perform the General and HA Installation Prerequisite Tasks

Before starting the HA installation, do the following:

1. Perform the tasks in Prerequisites for Cisco EPN Manager 3.1 Installation on both primary and secondary servers.

Remove the HA Configuration

Note This process is required only if the servers are associated with HA configuration.

Procedure

Step 1 Make sure you have performed the tasks in Prerequisites for Cisco EPN Manager 3.1 Installation.

Step 2 Log into the Cisco EPN Manager web GUI on the primary server as a user with Administrator privileges.

Step 3 From the left sidebar, choose **Administration** > **Settings** > **High Availability**.

Step 4 Click **HA Configuration** on the left.

Step 5 Click **Remove**.

Step 6 When the remove operation completes, confirm that the Configuration Mode field displays **HA Not Configured**.

Place the Cisco EPN Manager 3.1 Installation File on the Server (HA Deployment)

Before You Begin

Make sure you have the password (authentication key) that was created when HA was enabled. You will need it to install the patch on the secondary server.

Procedure

Step 1 Make sure you have removed the HA configuration as described in Remove the HA Configuration.

Step 2 On the primary server, upload the Cisco EPN Manager 3.1 ubf file. Follow the procedure in Place the Cisco EPN Manager 3.1 Installation File on the Server.

Step 3 Upload the Cisco EPN Manager 3.1 ubf file to the secondary server. (You will use the same file that was uploaded and installed on the primary server.)

a. Log into the secondary server's HM web page by entering the following URL in your browser:

`https://`*serverIP*`:8082`

Where *serverIP* is the IP address or host name of the secondary server.

a. Enter the authentication key and click **Login**.

b. Click **Software Update** at the top right of the Health Monitor window to open the Secondary Server Software Update window.

c. Enter the authentication key and click **Login**.

d. Click the **Upload** link under the window title, browse to the ubf file, and click **OK**.

After the successful upload of the ubf file, the file will appear under the Files tab.

What to do next

Install Cisco EPN Manager 3.1 on Primary and Secondary Servers (HA Deployment).

Install Cisco EPN Manager 4.1 on Primary and Secondary Servers (HA Deployment)

Before You Begin

- Make sure you have the password (authentication key) that was created when HA was enabled. You will need it to install the Cisco EPN Manager Minor Release file on the secondary server.
- Make sure no backups are in progress.

This ensures that the compliance server will be up and running on the secondary server after failover.

Procedure

Step 1 Install Cisco EPN Manager 4.1 on the primary server and verify the installation, as described in Install Cisco EPN Manager 4.1 (No HA). After the installation, the primary server automatically restarts and the web GUI will not be accessible for some time.

Step 2 Synchronize the hardware and NTP clocks on both the primary and secondary servers as described in Synchronize the Hardware and NTP Clock, then check that the clocks on each server are synchronized with one another.

Note
The service restart in the Synchorization Clock operation can be ignored as the installation of Cisco EPN Manager Minor Release restarts the Cisco EPN Manager.

Step 3 Install Cisco EPN Manager 4.1 on the secondary server.

a. Log into the secondary server's HM web page by entering the following URL in your browser: **`https://`***serverIP*`:8082`

Where *serverIP* is the IP address or host name of the secondary server.

b. Enter the authentication key and click **Login**.
c. Click **Software Update** at the top right of the Health Monitor window to open the Secondary Server Software Update window.
d. Enter the authentication key and click **Login**.
e. Click the **Install** button associated with Cisco EPN Manager Minor Release on the Software Update page.
f. Click **Yes** in the confirmation message pop-up window to proceed with the installation. On successful installation, the status will change to **Installed** and the secondary server will restart automatically.

Step 4 After the secondary server has restarted, verify the installation on the secondary server.

a. Start an SSH session with the secondary server and log in as the Cisco EPN Manager CLI admin user.
b. Run the **ncs status** command to ensure that, at a minimum, the following services are up and running: Health Monitor, Database, NMS, SAM Daemon, DA Daemon, Compliance Engine. Note that for optimal Cisco EPN Manager functionality, all services should be up and running.
c. Once the web GUI is accessible, verify the installation and version in the secondary server's HM web page. Enter the following URL in your browser: **`https://`***serverIP*`:8082`

Where **`serverIP`** is the IP address or host name of the secondary server.

d. Enter the authentication key and click **Login** .
e. Click **Software Update** at the top right of the Health Monitor window to open the Secondary Server Software Update window.
f. Enter the authentication key and click **Login** .
g. In the Files tab, verify that the Cisco EPN Manager Minor Release file (in the format **cepnm3.1-build560.ubf**) is listed and that the In Use status is **Yes**.

Step 5 Ensure that all services are up and running by running this command:

```
ncs status
```

Step 6 On the primary server, enable high availability and verify that the primary server's HA status is Primary Active.

a. Enable high availability.

1. Log into the Cisco EPN Manager web GUI as a user with Administrator privileges.
2. From the left sidebar menu, choose **Administration > Settings > High Availability**.
3. Click **HA Configuration** on the left, then enter the secondary server's IP address, the secondary server's authentication key, and an email address to which Cisco EPN Manager should send HA state change notifications.
4. If you are using virtual IP addressing in your HA setup (if the primary and secondary servers are in the same subnet), check the Enable Virtual IP check box and enter the virtual IP address(es).
5. Check Readiness for HA by following the process mentioned in section Check Readiness for HA Configuration.
6. Click **Save**, then wait until the servers are synchronized.
7. Verify that the Configuration Mode is **HA Enabled**.

b. Verify the primary server's HA status.

1. Click **HA Status** on the left.
2. Check that the Current State Mode displays **Primary Active**.

Step 7 Verify that the secondary server's HA status is Secondary Syncing.

a. Log into the secondary server's HM web page by entering the following URL in your browser:
`https://`*serverIP*`:8082`

Where **`serverIP`** is the IP address or host name of the secondary server.

b. Enter the authentication key and click **Login** .

c. Verify that the Current State Mode is **Secondary Syncing** (with a green check mark).

Check Readiness for HA Configuration

During the HA configuration, other environmental parameters related to HA like system specification, network configuration and bandwidth between the servers determine the HA configuration.

15 checks are run in the system to ensure the HA configuration completion without any error or failure. The checklist name and the corresponding status with recommendations if any, will be displayed when you run the Check Readiness feature.

Note The **Check Readiness** does not block the HA configuration. You can configure HA even if some of the checks do not pass.

To check readiness for HA configuration, follow these steps:

Procedure

Step 1 Log in to Cisco EPN Manager with a user ID and password that has administrator privileges.

Step 2 From the menu, select **Administration** > **Settings** > **High Availability**. Cisco EPN Manager displays the HA status page.

Step 3 Select **HA Configuration**.

Step 4 Provide the secondary server IP address in the **Secondary Server** field and secondary Authentication Key **Authentication Key** field .

Step 5 Click **Check Readiness**.

A pop up window with the system specifications and other parameters will be displayed. The screen will show the Checklist Item name, Status, Impact and Recommendation details.

Below, is the list of checklist test name and the description displayed for Check Readiness:

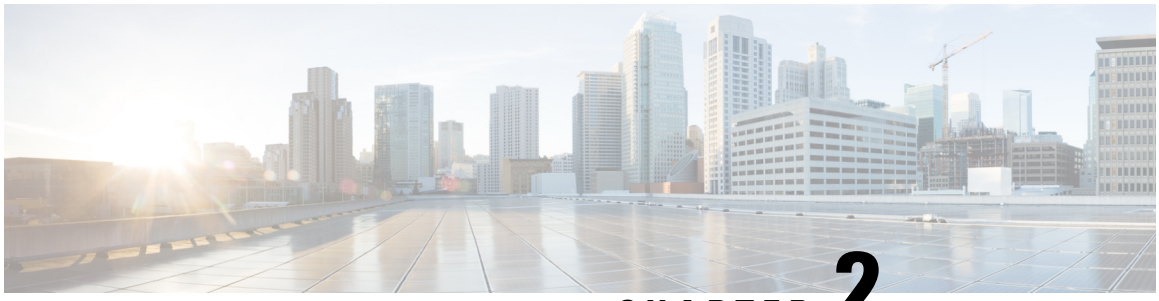
Table 1: Checklist name and description

Checklist Test Name	Test Description
SYSTEM - CHECK CPU COUNT	Checks the CPU count in both the primary and secondary servers. The CPU count in both servers must meet the requirements.
SYSTEM - CHECK DISK IOPS	Checks the disk speed in both the primary and secondary servers. The minimum expected disk speed is 200 MBps.
SYSTEM - CHECK RAM SIZE	Checks the RAM size of both the primary and secondary servers. The RAM size of both servers must meet the requirements.
SYSTEM - CHECK DISK SIZE	Checks the disk size of both the primary and secondary servers. The disk size of both servers must meet the requirements.
SYSTEM - CHECK SERVER PING REACHABILITY	Checks that the primary server can reach the secondary server through ping.
SYSTEM - CHECK OS COMPATABILITY	Checks that the primary server and secondary servers have the same OS version.
SYSTEM - HEALTH MONITOR STATUS	Checks whether the health monitor process is running in both the primary and secondary servers.

NETWORK - CHECK NETWORK INTERFACE BANDWIDTH	Checks if the speed of interface eth0 matches the recommended 100 Mbps in both primary and secondary severs. This test will not measure network bandwidth by transmitting data between primary and secondary server.
NETWORK - CHECK FIREWALL FOR DATABASE PORT ACCESSIBILITY	Checks if the database port 1522 is open in the system firewall. If the port is disabled, the test will grant permission for 1522 in the iptables list.
DATABASE - CHECK ONLINE STATUS	Checks if the database files status is online and accessible in both primary and secondary servers.
DATABASE - CHECK MEMORY TARGET	Checks for "/dev/shm" database memory target size for HA setup.
DATABASE - LISTENER STATUS	Checks if the database listeners are up and running in both primary and secondary servers. If there is a failure the test will attempt to start the listener and report the status.
DATABASE - CHECK LISTENER CONFIG CORRUPTION	Checks if all the database instances exist under database listener configuration file "listener.ora"
DATABASE - CHECK TNS CONFIG CORRUPTION	Checks if all the “WCS” instances exist under database TNS listener configuration file “tnsnames.ora"
DATABASE - TNS REACHABILITY STATUS	Checks if TNSPING is successful in both primary and secondary server.

Step 6 Once the check is completed for all the parameters, check their status and click **Clear** to close the window.

Note
Failback and failover events during **Check Readiness** are forwarded to the Alarms and Events page. Configuration failure events are not present in the Alarms and Events list.



CHAPTER 2

Cisco EPN Manager 4.1 High Availability

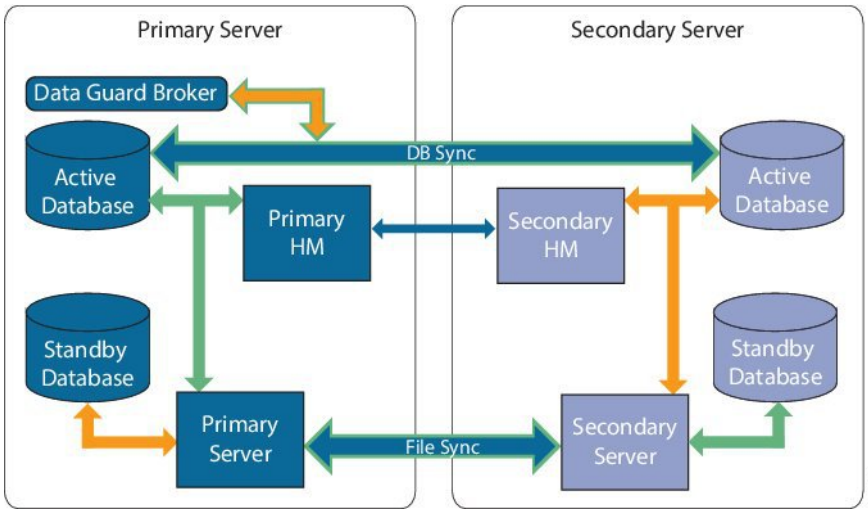
This chapter provides information about Cisco EPN Manager in a high availability environment:

- High Availability Overview, on page 13
- High Availability Deployment Considerations, on page 14

High Availability Overview

The Cisco EPN Manager high availability (HA) system ensures continued system operation in case of failure. HA uses a pair of linked, synchronized Cisco EPN Manager servers to minimize or eliminate the impact of application or hardware failures that may take place on either server.

The following figure shows the main components and process flows for a high availability deployment.



A high availability deployment consists of a primary and a secondary server with Health Monitor (HM) instances (running as application processes) on both servers. When the primary server fails (due to a problem or because it is manually stopped), the secondary server takes over and manages the network while you restore access to the primary server. If the deployment is configured for automatic failover, the secondary server takes over the active role within two to three minutes after the primary server failure.

When issues on the primary server are resolved and the server is in a running state, it remains in standby mode and begins syncing its data with the active secondary server. When failback is triggered, the primary server

again takes over the active role. This role switching between the primary and secondary servers generally takes approximately two to three minutes unless the primary server was reinstalled after failure, in which case it would take longer (based on the size of your setup).

For more information about HA, see the High Availability sections in the Cisco Evolved Programmable Network Manager User and Administrator Guide.

High Availability Deployment Considerations

- High Availability Deployment Models
- Understand High Availability Limitations
- Consider Whether You Can Use Virtual Addresses

High Availability Deployment Models

Cisco EPN Manager supports the following High Availability (HA) deployment models.

HA Deployment Model	Primary and Secondary Server Location	Example:
Local	On the same subnet (Layer 2 proximity)	Servers located in same data center
Campus	Different subnets connected via LAN	Servers located in same campus, city, state, or province
Remote	Different subnets connected via WAN	Servers are geographically dispersed

Consider the following factors when deciding whether to use the Local, Campus, or Remote HA deployment model:

- Exposure to disaster—The more distributed the deployment model, the less risk to the business as a result of a natural disaster. Remote HA deployments are least likely to be affected by natural disaster, allowing for a less complex and costly business continuity model. Local HA deployments are most vulnerable to disaster because of server co-location.
- Whether you can use a virtual IP address—Only Local HA deployments can use virtual IP addresses. A virtual IP address is a single IP address that will always point to the active server, even after a failover and failback. It also allows both the primary and secondary servers to share a common management IP address.
- Bandwidth/latency—Bandwidth would be highest and latency would be lowest in Local HA deployments because the primary and secondary servers are connected by short network links that have high bandwidth and low latency. Campus HA deployments may have lower bandwidth and higher latency than Local HA deployments. Remote HA deployments have the least bandwidth and the highest latency.
- Administration—HA administration is simplest for Local HA deployments, with increasing complexity for Campus and Remote HA deployments. Remote HA deployments will require administrative remedying.
- Configuration of device event forwarding—Configuring event forwarding can be simplest with Local HA deployments because you can use a virtual IP address, and then configure your devices to forward events to that single virtual IP address. Without a virtual IP address, you must configure your devices to forward events to both the primary and secondary servers.

For more details about HA, see the Cisco Evolved Programmable Network Manager User and Administrator Guide.

Understand High Availability Limitations

The Cisco EPN Manager HA system is subject to the following limiting factors (this applies to all HA deployment models):

- The HA system requires a minimum of 500 Mbps (Mega bit per second) or higher of network bandwidth to handle HA operations. These operations include (but are not restricted to) HA registration, database and file synchronization, and triggering failback. Because Cisco EPN Manager uses a single physical port for all its networking needs, there can be occurrences of insufficient bandwidth which in turn will affect HA performance.
- The HA system requires low latency (maximum 100 ms, preferably under 70 ms.) across network links between the primary and secondary servers. Irrespective of the physical proximity of these two servers, high latency on these links can affect how Cisco EPN Manager maintains sessions between the primary and secondary servers. This is because larger databases require more synchronization transactions which require lower latency and higher bandwidth. If you are managing a relatively small network using Cisco EPN Manager, your database would be smaller and therefore, HA might work with a higher network latency and less bandwidth.
- HA performance is always sensitive to the network throughput delivered by the network that connects the primary and secondary servers. This restriction applies (to some degree) to all of the deployment models. For example, in a geographically dispersed deployment, a Remote HA deployment is more likely to have problems due to low bandwidth and high latency. However, if Local and Campus HA deployments are not properly configured, they are highly susceptible to problems with latency that result from bandwidth limitations on high-usage networks.

For assistance in determining whether your network is suitable for any of the HA variations, please contact your Cisco representative.

Consider Whether You Can Use Virtual Addresses

Using virtual IP addresses in a Local HA deployment setup gives your users the ability to connect to the active server using a single IP address or web URL without having to know which server is actually active. Virtual IP addresses also allow both servers to share a common management IP address. During normal operation, the virtual IP address points to the primary server. If a failover occurs, the virtual IP address automatically points to the secondary server. When failback occurs, the virtual IP address automatically switches back to the primary server.

To use a virtual IP addresses, the following IP addresses must be on the same subnet:

- The virtual IP address
- The IP addresses of the primary and secondary servers
- The IP address of the gateway configured on both primary and secondary servers

The following example illustrates how virtual, primary, and secondary IP addresses should be assigned with respect to each other. If the primary and secondary servers have the following IP address assignments within the given subnet, the virtual IP address for both servers can be assigned as follows:

- Subnet mask: 255.255.255.224 (/32)
- Primary server IP address: 10.10.101.1
- Secondary server IP address: 10.10.101.2
- Virtual IP address: 10.10.101.[3-30] e.g., 10.10.101.3. Note that the virtual IP address can be any of a range of addresses that are valid for the given subnet mask.

If you do not use a virtual IP address, you must configure your devices to forward events to both the primary and secondary servers (for example, by forwarding them to a given subnet or range of IP addresses that includes both the primary and secondary server). To reduce (or eliminate) the chance of losing data, you must configure device event forwarding before a failover occurs. You do not need to make any changes to the secondary server during installation; simply provision the primary and secondary servers with their individual IP addresses.

Whether your HA deployment uses a single IP address or not, users should always connect to the Cisco EPN Manager web GUI using the active server IP address/URL.

Best Practices if Firewall is Used Between Primary and Secondary Servers

Firewalls between the primary and secondary servers should be configured to avoid short timeouts for TCP packets to allow enough time for HA registration and other processes.

Following is the procedure for changing the Oracle and OS timeouts, if necessary. Use this procedure if the failback operation fails repeatedly.

Before you Begin

Back up the files specified in the procedure below.

Note This procedure must be performed on both primary and secondary servers.

Procedure

Step 1 Open the following file:

/opt/oracle/base/product/12.1.0/dbhome_1/network/admin/sqlnet.ora

Step 2 Add the following parameters:

```
SQLNET.EXPIRE_TIME=2
DISABLE_OOB=on
SQLNET.INBOUND_CONNECT_TIMEOUT=600
```

Step 3 Open the following file:

/opt/CSCOlumos/bin/ha_dgmgrl.sh

Step 4 Add the following line under the register() function:

```
edit database $1 set property NetTimeout=1000
```

Following is an example excerpt of the file with the relevant line in bold:

```
connect $4/$5@$3
remove configuration;
create configuration $DGMGRL_CONFIG_NAME as primary database is $1 connect identifier is $1;
edit database $1 set property NetTimeout=1000
;
```

```
add database $2 as connect identifier is $2 maintained as physical;
enable configuration;
```

Step 5 Open the following file:

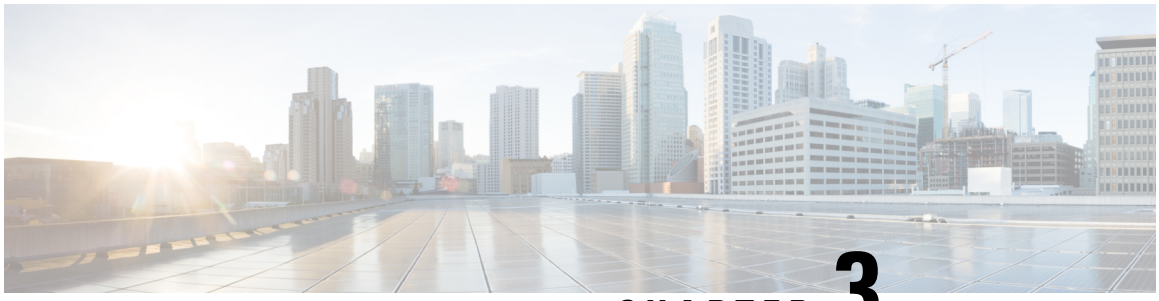
/etc/sysctl.conf

Add the following commands to the end of the file:

```
net.ipv4.tcp_keepalive_time = 80
net.ipv4.tcp_keepalive_probes = 7
net.ipv4.tcp_keepalive_intvl = 10
```

Step 6 Run the following command from the root shell:

```
sysctl -system
```



CHAPTER 3

Upgrade to Cisco EPN Manager 4.1

You can upgrade to Cisco EPN Manager 4.1 by following one of the Valid Upgrade Paths, on page 19.

This chapter provides instructions for upgrading to Cisco EPN Manager 4.1 using Backup-restore upgrade.

Backup-restore upgrade —Involves backing up all data from the currently installed version of Cisco EPN Manager, then installing Cisco EPN Manager 4.1 on a new server, then restoring the backed up data to the new Cisco EPN Manager 4.1 server.

Note Cisco EPN Manager 4.1 installation consists of Cisco EPN Manager 4.0 OVA/ISO installation followed by Cisco EPN Manager 4.1 UBF installation.

- Valid Upgrade Paths, on page 19
- Upgrade to Cisco EPN Manager 4.1 (No HA), on page 20
- Upgrade to Cisco EPN Manager 4.1 (High Availability), on page 20
- Post-Upgrade Tasks, on page 22

Valid Upgrade Paths

The following table lists the valid paths for installing/upgrading to Cisco EPN Manager 4.1 from previous versions.

Current Cisco EPN Manager Version	Installation Path to Cisco EPN Manager 4.1
Cisco EPN Manager 4.0	**Cisco EPN Manager 4.0 > 4.1**
Cisco EPN Manager 4.0.1	**Cisco EPN Manager 4.0.1 > 4.1**

See the relevant installation guide for installation prerequisites and procedures for Cisco EPN Manager versions.

For point patch installation instructions, see the readme file supplied with the patch file on the on the Software Download site on Cisco.com.

Upgrade to Cisco EPN Manager 4.1 (No HA)

These topics explain how to upgrade to Cisco EPN Manager 4.1 from an earlier version of Cisco EPN Manager in a standard deployment (no high availability).

- Backup-Restore Upgrade
- Post-Upgrade Tasks

If you are performing an upgrade in a high availability deployment, see Upgrade to Cisco EPN Manager 4.1 (High Availability), on page 20.

Backup-Restore Upgrade (No HA)

Backup-restore upgrade involves backing up all data from the currently installed version of Cisco EPN Manager, then installing Cisco EPN Manager 4.1 on a new server, then restoring the backed up data to the new Cisco EPN Manager 4.1 server. This is the recommended upgrade method.

Before You Begin

- Make sure you have completed the tasks in
- Make sure the new server has the same hardware specifications as the server from which the backup was taken.
- Note the location of the remote backup repository used by the old server. You will need it to configure the same backup location on the new server.

Procedure

Step 1 On the new server, install Cisco EPN Manager 4.1 by following the steps in Install Cisco EPN Manager 4.0 (No HA).

Step 2 Configure the new server to use the same remote backup repository as the old server, as explained in the remote backup repository topics in the Cisco Evolved Programmable Network Manager User and Administrator Guide .

Step 3 Restore the backup in the remote repository to the new server, as explained in the restore backup topics in the Cisco Evolved Programmable Network Manager User and Administrator Guide .

Upgrade to Cisco EPN Manager 4.1 (High Availability)

The following topic provides the procedure for upgrading to Cisco EPN Manager 4.1 in a high availability deployment:

Backup-Restore Upgrade (High Availability)

Note High availability will not be functional until the upgrade is complete.

Backup-Restore Upgrade (High Availability)

Backup-restore upgrade in an HA environment involves the following basic steps which are explained in detail in the procedure below:

1. Remove HA.
2. Back up your data to a remote repository.
3. Perform a fresh installation of Cisco EPN Manager on both the primary and secondary servers.
4. Restore the backup data on the primary server.
5. Reconfigure HA.

Before You Begin

- Make sure your deployment meets the general HA requirements.
- Make sure your deployment meets the upgrade-specific requirements listed in Prerequisites for Cisco EPN Manager 4.1 Installation, on page 2.
- Make sure the new server has at least the same hardware specifications as the server from which the backup was taken.
- Note the location of the remote backup repository used by the old server (if applicable). You will need it to configure the same backup location on the new server.
- Make sure that you have the password (authentication key) that was created when HA was enabled. You will need it to perform the Cisco EPN Manager 3.1 installation on the secondary server.

Procedure

Step 1 On the primary server, remove the High Availability configuration:

a. Log into Cisco EPN Manager as a user with Administrator privileges.
b. Choose **Administration > Settings > High Availability**.
c. Make a note of the HA configuration. You will need this information to reconfigure HA after the upgrade.
d. Choose **HA Configuration** in the left navigation area, then click **Remove**.
e. Wait for the remove operation to complete.
f. Click **HA Configuration** in the left navigation area and confirm that the Configuration Mode field displays **HA Not Configured**.

Step 2 Back up your data to the remote repository. For details, see the topics on backups in the Cisco Evolved Programmable Network Manager User and Administrator Guide.

Note
If you do not have a remote repository, configure one. See the topics on remote backup repositories in the Cisco Evolved Programmable Network Manager User and Administrator Guide.

Step 3 Install Cisco EPN Manager 4.1 on the two new servers as described in Install Cisco EPN Manager 4.1 in a High Availability Environment, on page 6.

Step 4 Once the installation is completed, configure the new primary server to use the same remote backup repository as the old primary server (which you used in *Step 2*). See the topics on remote backup repositories in the Cisco Evolved Programmable Network Manager User and Administrator Guide.

Step 5 On the primary server (only), restore the backup from the remote repository. See the topics on restoring data in the Cisco Evolved Programmable Network Manager User and Administrator Guide .

Note

You only need to perform the restore operation on the primary server. The secondary server will be synchronized with the primary server when HA is re-enabled.

Step 6 On the primary server:

a. Verify that the server is restarted.

b. Run the **ncs status** command and make sure that the Health Monitor process and other processes have restarted. Ensure that, at a minimum, the following services are up and running: Health Monitor, Database, NMS, SAM Daemon, DA Daemon, Compliance Engine. Note that for optimal Cisco EPN Manager functionality, all services should be up and running.

Step 7 If the **ncs status** output on the primary server lists **Compliance engine is stopped**, do the following:

a. Stop Cisco EPN Manager.

```
ncs stop
```

b. Log in as the Linux CLI root user (see Log In and Out as the Linux CLI Users).

c. Update the time zone using a soft link (the following command is one line):

```
ln -sf /usr/share/zoneinfo/$(grep ^clock /storedconfig/active/startup-config | cut -d " "  -f 3)
 /etc/localtime
```

Step 8 Once the restore is completed, perform the post-upgrade tasks on the primary server. See Post-Upgrade Tasks.

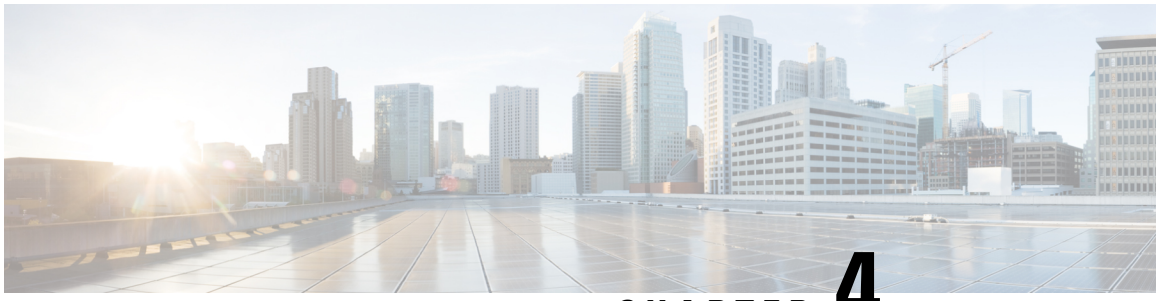
Step 9 Re-configure HA by registering the secondary server on the primary server. Use the information you saved in *Step 1*. The registration process must be performed from the primary server. For more information, see the section on registering the secondary server on the primary server, in the Cisco Evolved Programmable Network Manager User and Administrator Guide.

Post-Upgrade Tasks

- If you are using Cisco Smart Licensing, re-register Cisco EPN Manager with the Cisco Smart Software Manager (CSSM) on Cisco.com. Refer to the topics that describe managing licenses in the Cisco Evolved Programmable Network Manager User and Administrator Guide .
- Synchronize the inventory of all devices with the database, as follows:
  1. In the Cisco EPN Manager GUI, choose **Monitor > Network Devices**.
  2. Select all devices, then click **Sync**.
- Instruct users to clear the browser cache on all client machines that accessed an older version of Cisco EPN Manager before they try to connect to the upgraded Cisco EPN Manager server.
- If you were using external AAA before the upgrade, configure external authentication again. Refer to the user management topics in the Cisco Evolved Programmable Network Manager User and Administrator Guide.
- During the upgrade, the Cisco EPN Manager home page will be reset to the default home page (Getting Started page). Users can select their own default home page from the Getting Started page or from the Settings menu at the top right of the page.

New dashlets on existing tabs, will not be added automatically post upgrade. The user can manually add them from the dashboard menu Settings->Add Dashlet(s).

New dashboard tabs will be added automatically.



CHAPTER 4

Install Geo Map Resource Files for Offline Use

The network can be visualized on a topology map or on a geographical map (geo map). The geo map enables you to position your network devices on a world map and monitor them within their geographical context.

To display the geo map in the GUI, the system is set up by default to get the map tiles from a specific Mapbox URL through a direct Internet connection from the client or via the EPN Manager server which acts as a proxy. If you do not have an Internet connection, you must install the map resources locally and specify that you want the system to use the local map resources (i.e., offline use).

The topics below explain how to download and install geo maps for offline use in both HA and non-HA environments.

Note Geo map compressed files are very large. We recommend you save the files to a remote repository.

- Install Geo Map Resource Files (Standard Deployment), on page 25
- Install Geo Map Resource Files (High Availability Deployment), on page 28
- Update Geo Map Resource Files After Upgrading to Cisco EPN Manager , on page 28

Install Geo Map Resource Files (Standard Deployment)

Installing geo map resource files for offline use in a standard environment (no high availability) involves the following steps:

1. Place the Geo Map Resource Files on the Cisco EPN Manager Server.
2. Install the Geo Map Resource Files on the Cisco EPN Manager Server .
3. Configure the Cisco EPN Manager Server to Use the Installed Map Resources.
4. Verify that the Geo Maps Files Were Installed Successfully.

Place the Geo Map Resource Files on the Cisco EPN Manager Server

Before You Begin

- If you plan to use a remote repository (because geo map files are very large), make sure a remote repository has been configured. For more information, refer to the topics on using remote FTP backup repositories in the Cisco Evolved Programmable Network Manager User and Administrator Guide .
- Make sure SCP is enabled on your client machine and the required ports are open.

This procedure shows you how to download and copy the geo map resources to the default local repository on the Cisco EPN Manager server.

Procedure

Step 1 Download the geo map compressed files to a client machine.

a. Go to the Software Download site on Cisco.com .
b. Navigate to the files by choosing **All Releases >4.0**.
c. Identify the map you want to download and click **Download**.
d. Follow the instructions to save the file to the client machine.

Step 2 Copy the geo map compressed files from the local machine to the Cisco EPN Manager server's default local repository (/localdisk/defaultRepo).

In the following example, the Russia geo map file was downloaded to a /temp directory on the client machine. The user has logged into the Cisco EPN Manager server as the Linux CLI admin user and is retrieving the file from the client machine and copying it to /localdisk/defaultRepo on the server:

```
scp joesmith@123.456.789.101:/temp/Russia_GeoMap_CEPNM_3_1_0-bundle.tar.gz /localdisk/defaultRepo
```

What to do next

Install the geo map files as described in Install the Geo Map Resource Files on the Cisco EPN Manager Server .

Install the Geo Map Resource Files on the Cisco EPN Manager Server

Before You Begin

The installation process will extract the geo map files and install them in /opt/CSCOlumos/resources/offline_geo. To avoid storage constraints, consider mounting additional storage on the directory by editing the /etc/fstab file after logging in as a Linux CLI admin user. If you have high availability and need to mount additional storage, be sure to edit the /etc/fstab file on both the primary and secondary servers.

Procedure

Step 1 Start an SSH session with the Cisco EPN Manager server and log in as the Cisco EPN Manager CLI admin user.

Step 2 Install the geo map resource file that is located in /localdisk/defaultRepo.

Example:

```
application install filename defaultRepo
```

Where *filename* is the geo map resource file located in /localdisk/defaultRepo (this is the file you copied in Place the Geo Map Resource Files on the Cisco EPN Manager Server). For example:

Example:

```
application install Russia_GeoMap_CEPNM_3_1_0-bundle.tar.gz defaultRepo
Save the current ADE-OS running configuration? (yes/no) [yes] ? yes
Please ensure you have a backup of the system before proceeding.Proceed with the application install
 ? (yes/no) [yes] ? yes
```

The installation takes a few minutes to complete depending on the size of the map resources.

What to do next

Configure Cisco EPN Manager to use the installed geo map files, as described in Configure the Cisco EPN Manager Server to Use the Installed Map Resources.

Configure the Cisco EPN Manager Server to Use the Installed Map Resources

Procedure

Step 1 Choose **Administration** > **Settings** > **System Settings**, then choose **Maps** > **Network Topology**.

Step 2 Check **Enable Geo Maps**.

Step 3 Choose **Installed Map Resources** from the Map Provider drop-down list.

Step 4 Click **Save**.

You do not have to restart the Cisco EPN Manager server to apply your changes. A notification message informs you that the system is now working with the installed map resources.

What to do next

Verify that the geo map files have been installed, as described in Verify that the Geo Maps Files Were Installed Successfully.

Verify that the Geo Maps Files Were Installed Successfully

After installing the geo map files and configuring the system to use these geo map files, check that they have been successfully installed and that they are being displayed in the GUI.

Procedure

Check that the map is being displayed in the GUI:

a. Log in to the Cisco EPN Manager web GUI as a user with Administrator privileges.

b. From the left sidebar menu, choose **Maps** > **Topology Maps** > **Network Topology**.

c. Click the Geographical Map icon at the top right of the topology window to display the geo map.

d. Verify that the desired map is displayed. For example, if you installed the map of Russia, it should be displayed.

Install Geo Map Resource Files (High Availability Deployment)

For a high availability environment, you must install the offline map resources on both the primary and the secondary servers.

Note If a failure occurs on the primary server that requires you to reinstall Cisco EPN Manager on the primary server, you must reinstall the geo map resources on the primary server and restart the server.

Follow this workflow to install geo map files in a high availability deployment:

Procedure

Step 1 Place the geo map files on the primary server and on the secondary server, as described in Place the Geo Map Resource Files on the Cisco EPN Manager Server.

Step 2 Install the geo map files on the primary server, as described in Install the Geo Map Resource Files on the Cisco EPN Manager Server.

Step 3 Install the geo map files on the secondary server, as described in Install the Geo Map Resource Files on the Cisco EPN Manager Server.

Step 4 On the primary server, enable the use of installed map files, as described in Configure the Cisco EPN Manager Server to Use the Installed Map Resources.

Step 5 On the primary server, check that the geo map is displayed, as described in Verify that the Geo Maps Files Were Installed Successfully.

Update Geo Map Resource Files After Upgrading to Cisco EPN Manager

Geo map files must be reinstalled after upgrade.

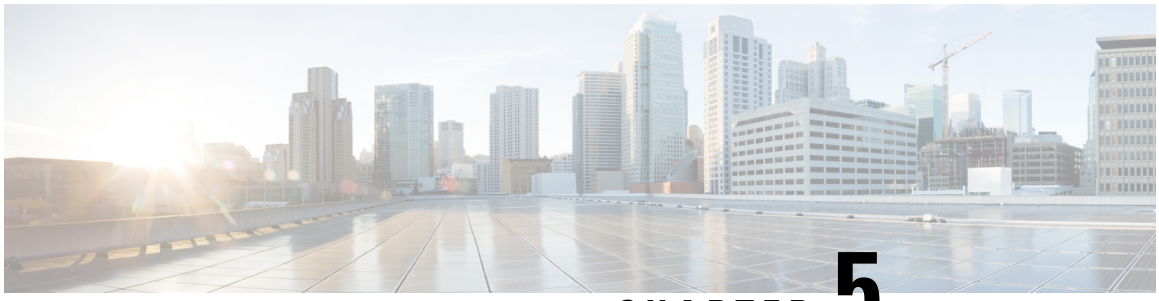
Procedure

Step 1 Download the required Cisco EPN Manager geo map files and reinstall them.

Step 2 Stop and restart the server(s).

Step 3 Clear the cache.

Step 4 Verify that the geo map files have been installed. See Verify that the Geo Maps Files Were Installed Successfully.



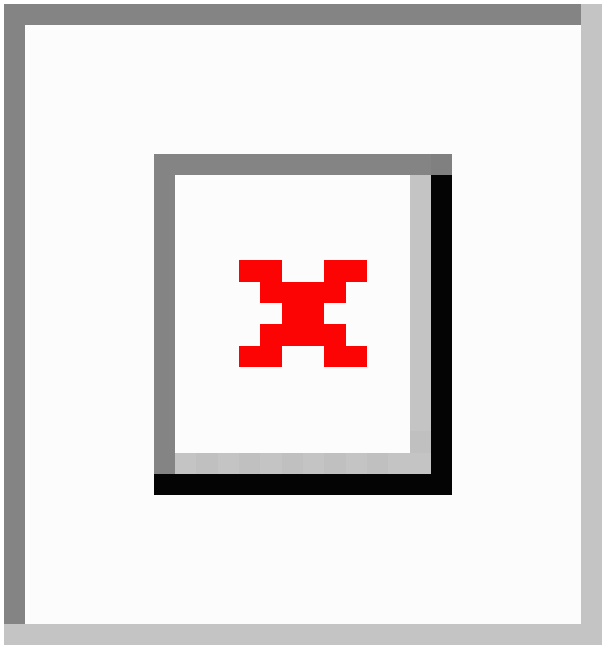
CHAPTER 5

Supplementary Installation-Related Information and Procedures

- Log In and Out as the Linux CLI Users, on page 31
- Copy Files From a Client Machine to the Cisco EPN Manager Server, on page 33
- Synchronize the Hardware and NTP Clock, on page 33
- Log Into the Cisco EPN Manager Web GUI, on page 35
- Time Zones Supported by , on page 36

Log In and Out as the Linux CLI Users

The Linux CLI has two shell users: One with administrative access (Linux CLI admin user), and another with root access (Linux CLI root user). The following diagram illustrates the flow for logging in and out as the various CLI users.



To log in as the Linux CLI root user, you will have to transition from being the Cisco EPN Manager **CLI admin user** to the **Linux CLI root user**. The following procedure gives you the exact steps you must follow to log in as these users. For more information on these users, refer to the Cisco Evolved Programmable Network Manager User and Administrator Guide.

Before You Begin

If the Linux CLI user is disabled, re-enable it. Refer to the user management procedures in the Cisco Evolved Programmable Network Manager User and Administrator Guide.

Procedure

Step 1 To log in as the Linux CLI root user:

a. Start an SSH session with the Cisco EPN Manager server and log in as the Cisco EPN Manager CLI admin user.

b. As the Cisco EPN Manager CLI admin user, log in as the Linux CLI admin user:

```
shell
Enter shell access password:
password
```

c. Log in as the Linux CLI root user:

```
sudo -i
```

By default, the Linux CLI shell prompt is the same for the Linux CLI admin and root user. You can use the **whoami** command to check the current user.

Step 2 To exit:

a. Log out as the Linux CLI root user.

```
exit
```

You are now logged in as the Linux CLI admin user.

b. Log out as the Linux CLI admin user:

```
exit
```

You are now logged in as the Cisco EPN Manager CLI admin user.

What to do next

For security purposes, disable the Linux CLI users. Refer to the user management procedures in the Cisco Evolved Programmable Network Manager User and Administrator Guide.

Copy Files From a Client Machine to the Cisco EPN Manager Server

Before You Begin

You can use SCP, FTP, or SFTP protocols to retrieve files from the client machine. Make sure the required protocol is enabled on your client machine and the required ports are open.

This procedure explains how to copy files from your client machine to the Cisco EPN Manager server.

Procedure

Step 1 Start an SSH session with the Cisco EPN Manager server and log in as the Cisco EPN Manager CLI admin user.

Step 2 Log in as the Linux CLI admin user (see Log In and Out as the Linux CLI Users).

Step 3 From the Cisco EPN Manager server, retrieve the file from the client machine. You can use SCP, FTP, or SFTP. This example uses the **scp** command, which has the following syntax:

```
scp clientUsername@clientIP:/fullpath-to-file-on-client
/server-directory
```

Where:

- *clientUsername* is your username on the client machine
- *clientIP* is the IP address of the client machine
- *fullpath-to-file-on-client* is the full path to the file on the client machine that you want to copy to the server
- *server-directory* is the path to the directory on the server to which you want to copy the file

In the following example, a file named **myfile** located in the /temp directory on the client machine is being copied to the /localdisk/defaultRepo on the Cisco EPN Manager server.

```
scp joesmith@123.456.789.101:/temp/myfile /localdisk/defaultRepo
```

Step 4 Log out as the Linux CLI admin user as described in Log In and Out as the Linux CLI Users.

Synchronize the Hardware and NTP Clock

This procedure synchronizes the hardware clock with the NTP clock using the **hwclock** command.

Procedure

Step 1 Log in as the Linux CLI root user as described in Log In and Out as the Linux CLI Users.

Step 2 Check the NTP service status and ensure that NTP has obtained a stable time reference using the following commands. The following includes examples of the output you should see.

a. Ensure that ntpd is running.

```
systemctl ntpd status
 ntpd (pid 3290) is running...
```

b. If ntpd (pid 3290) is not running, start it using the following command:

```
systemctl ntpd start
```

(Repeat *Step a* to ensure it is running.)

c. Ensure that NTP is receiving time from an NTP server.

```
ntpstat
 synchronised to NTP server (10.116.133.175) at stratum 3    time correct to within 62 ms
polling server every 1024 s
```

If you do not see output similar to this, then NTP synchronization has not yet occurred. Wait a few minutes and run **ntpstat** again. If synchronization does not happen within 10 minutes, contact your system administrator or Cisco support.

Step 3 Synchronize the hardware clock with NTP using the following command:

```
hwclock --systohc --debug
```

You should see output similar to the following:

```
hwclock from util-linux-ng 2.17.2
Using /dev interface to clock.
Last drift adjustment done at 1470117750 seconds after 1969
Last calibration done at 1470117750 seconds after 1969
Hardware clock is on local time
Assuming hardware clock is kept in local time.
Waiting for clock tick...
...got clock tick
Time read from Hardware Clock: 2016/08/02 16:03:30
Hw clock time : 2016/08/02 16:03:30 = 1470117810 seconds since 1969
1470117810.500000 is close enough to 1470117810.500000 (0.000000 < 0.001000)
Set RTC to 1470117810 (1470117810 + 0; refsystime = 1470117810.000000)
Setting Hardware Clock to 16:03:30 = 1470117810 seconds since 1969
ioctl(RTC_SET_TIME) was successful.
Not adjusting drift factor because it has been less than a day since the last calibration.
root$
```

Step 4 Verify that the hardware clock is synchronized with NTP.

```
echo "hwclock is: $(hwclock --show)" ; echo "linux clock is: $(date)";
```

Check the output and ensure that the two clocks are synchronized (to at least within a few seconds of each other):

```
Hwclock is: Tue 26 Jul 2016  06:11:40  PM AEST   -0.391028 secondslinux clock is: Tue Jul 26  18:11:40
  AEST 2016
```

Step 5 As the Linux CLI admin user, restart the Cisco EPN Manager services.

- If you are logged in as the Linux CLI root user, switch to the Linux CLI admin user.

```
exit
```

- Switch to the Cisco EPN Manager CLI admin user.

```
exit
```

- Stop and restart the Cisco EPN Manager services.

```
ncs stop
ncs start
```

Log Into the Cisco EPN Manager Web GUI

Follow these steps to log into the Cisco EPN Manager web GUI:

Procedure

Procedure

Step 1 On a client machine, launch one of the supported browsers.

Step 2 In the browser's address line, enter **`https://serverIP`**, where *serverIP* is the IP address of the server on which you installed Cisco EPN Manager. The login window is displayed.

When a client accesses the Cisco EPN Manager web GUI for the first time, the browser may display a warning that the site is untrusted. When this happens, follow the prompts to add a security exception and download the self-signed certificate from the Cisco EPN Manager server. After you complete this procedure, the browser will accept the Cisco EPN Manager server as a trusted site in all future login attempts.

Step 3 Enter the web GUI root username and password, as specified during the installation.

If any licensing problems occur, a message appears in an alert box. If you have an evaluation license, the number of days until the license expires is shown. You are also alerted about any expired licenses. (You have the option to go directly to the **Administration** > **Licenses and Software Updates** > **Licenses** page to address these problems.) For more information about licenses, refer to the Cisco Evolved Programmable Network Manager User and Administrator Guide .

Step 4 Click **Login** to log in to the Cisco EPN Manager web GUI. The home page appears and you can now use the web GUI. For information about the dashboards and dashlets, refer to the Cisco Evolved Programmable Network Manager User and Administrator Guide .

Step 5 For increased security, perform these steps:

a. Change the password for the web GUI root user by choosing **Administration** > **Users** > **Roles & AAA** > **Change Password**.

b. Create at least one Cisco EPN Manager web GUI user that has Admin or Super User privileges, then disable the web GUI root user. For information on disabling this user, refer to the user management topics in the Cisco Evolved Programmable Network Manager User and Administrator Guide .

c. If you have not done so already, disable the Linux CLI users. Refer to the Cisco Evolved Programmable Network Manager User and Administrator Guide .

What to do next

Perform setup tasks for server, user, fault, and web GUI management. For a detailed list of tasks, see the beginning of the administration section of the Cisco Evolved Programmable Network Manager User and Administrator Guide .

For information on Cisco EPN Manager user interfaces and user types, Cisco Evolved Programmable Network Manager User and Administrator Guide .

Time Zones Supported by

This table lists the available values for the system time zone.

Africa/Abidjan	America/St_Johns	Etc/GMT+6
Africa/Accra	America/St_Kitts	Etc/GMT+7
Africa/Addis_Ababa	America/St_Lucia	Etc/GMT+8
Africa/Algiers	America/St_Thomas	Etc/GMT+9
Africa/Asmara	America/St_Vincent	Etc/GMT0
Africa/Asmera	America/Swift_Current	Etc/GMT-0
Africa/Bamako	America/Tegucigalpa	Etc/GMT-1
Africa/Bangui	America/Thule	Etc/GMT-10
Africa/Banjul	America/Thunder_Bay	Etc/GMT-11
Africa/Bissau	America/Tijuana	Etc/GMT-12
Africa/Blantyre	America/Toronto	Etc/GMT-13
Africa/Brazzaville	America/Tortola	Etc/GMT-14
Africa/Bujumbura	America/Vancouver	Etc/GMT-2
Africa/Cairo	America/Virgin	Etc/GMT-3
Africa/Casablanca	America/Whitehorse	Etc/GMT-4
Africa/Ceuta	America/Winnipeg	Etc/GMT-5
Africa/Conakry	America/Yakutat	Etc/GMT-6
Africa/Dakar	America/Yellowknife	Etc/GMT-7

Africa/Dar_es_Salaam	Antarctica/Casey	Etc/GMT-8
Africa/Djibouti	Antarctica/Davis	Etc/GMT-9
Africa/Douala	Antarctica/DumontDUrville	Etc/Greenwich
Africa/El_Aaiun	Antarctica/Mawson	Etc/UCT
Africa/Freetown	Antarctica/McMurdo	Etc/Universal
Africa/Gaborone	Antarctica/Palmer	Etc/UTC
Africa/Harare	Antarctica/Rothera	Etc/Zulu
Africa/Johannesburg	Antarctica/South_Pole	Europe/Amsterdam
Africa/Kampala	Antarctica/Syowa	Europe/Andorra
Africa/Khartoum	Antarctica/Vostok	Europe/Athens
Africa/Kigali	Arctic/Longyearbyen	Europe/Belfast
Africa/Kinshasa	Asia/Aden	Europe/Belgrade
Africa/Lagos	Asia/Almaty	Europe/Berlin
Africa/Libreville	Asia/Amman	Europe/Bratislava
Africa/Lome	Asia/Anadyr	Europe/Brussels
Africa/Luanda	Asia/Aqtau	Europe/Bucharest
Africa/Lubumbashi	Asia/Aqtobe	Europe/Budapest
Africa/Lusaka	Asia/Ashgabat	Europe/Chisinau
Africa/Malabo	Asia/Ashkhabad	Europe/Copenhagen
Africa/Maputo	Asia/Baghdad	Europe/Dublin
Africa/Maseru	Asia/Bahrain	Europe/Gibraltar
Africa/Mbabane	Asia/Baku	Europe/Guernsey
Africa/Mogadishu	Asia/Bangkok	Europe/Helsinki
Africa/Monrovia	Asia/Beirut	Europe/Isle_of_Man
Africa/Nairobi	Asia/Bishkek	Europe/Istanbul
Africa/Ndjamena	Asia/Brunei	Europe/Jersey
Africa/Niamey	Asia/Calcutta	Europe/Kaliningrad
Africa/Nouakchott	Asia/Choibalsan	Europe/Kiev
Africa/Ouagadougou	Asia/Chongqing	Europe/Lisbon

Africa/Porto-Novo	Asia/Chungking	Europe/Ljubljana
Africa/Sao_Tome	Asia/Colombo	Europe/London
Africa/Timbuktu	Asia/Dacca	Europe/Luxembourg
Africa/Tripoli	Asia/Damascus	Europe/Madrid
Africa/Tunis	Asia/Dhaka	Europe/Malta
Africa/Windhoek	Asia/Dili	Europe/Mariehamn
America/Adak	Asia/Dubai	Europe/Minsk
America/Anchorage	Asia/Dushanbe	Europe/Monaco
America/Anguilla	Asia/Gaza	Europe/Moscow
America/Antigua	Asia/Harbin	Europe/Nicosia
America/Araguaina	Asia/Ho_Chi_Minh	Europe/Oslo
America/Argentina/	Asia/Hong_Kong	Europe/Paris
America/Argentina/	Asia/Hovd	Europe/Podgorica
America/Argentina/Catamarca	Asia/Irkutsk	Europe/Prague
America/Argentina/Cordoba	Asia/Istanbul	Europe/Riga
America/Argentina/Jujuy	Asia/Jakarta	Europe/Rome
America/Argentina/La_Rioja	Asia/Jayapura	Europe/Samara
America/Argentina/Mendoza	Asia/Jerusalem	Europe/San_Marino
America/Argentina/Rio_Gallegos	Asia/Kabul	Europe/Sarajevo
America/Argentina/Salta	Asia/Kamchatka	Europe/Simferopol
America/Argentina/San_Juan	Asia/Karachi	Europe/Skopje
America/Argentina/San_Luis	Asia/Kashgar	Europe/Sofia
America/Argentina/Tucuman	Asia/Kathmandu	Europe/Stockholm
America/Argentina/Ushuaia	Asia/Katmandu	Europe/Tallinn
America/Aruba	Asia/Kolkata	Europe/Tirane
America/Asuncion	Asia/Krasnoyarsk	Europe/Tiraspol
America/Atikokan	Asia/Kuala_Lumpur	Europe/Uzhgorod
America/Atka	Asia/Kuching	Europe/Vaduz
America/Bahia	Asia/Kuwait	Europe/Vatican

America/Barbados	Asia/Macao	Europe/Vienna
America/Belem	Asia/Macau	Europe/Vilnius
America/Belize	Asia/Magadan	Europe/Volgograd
America/Blanc-Sablon	Asia/Makassar	Europe/Warsaw
America/Boa_Vista	Asia/Manila	Europe/Zagreb
America/Bogota	Asia/Muscat	Europe/Zaporozhye
America/Boise	Asia/Nicosia	Europe/Zurich
America/Buenos_Aires	Asia/Novosibirsk	Factory
America/Cambridge_Bay	Asia/Omsk	GB
America/Campo_Grande	Asia/Oral	GB-Eire
America/Cancun	Asia/Phnom_Penh	GMT
America/Caracas	Asia/Pontianak	GMT+0
America/Catamarca	Asia/Pyongyang	GMT0
America/Cayenne	Asia/Qatar	GMT-0
America/Cayman	Asia/Qyzylorda	Greenwich
America/Chicago	Asia/Rangoon	Hongkong
America/Chihuahua	Asia/Riyadh	HST
America/Coral_Harbour	Asia/Riyadh87	Iceland
America/Cordoba	Asia/Riyadh88	Indian/Antananarivo
America/Costa_Rica	Asia/Riyadh89	Indian/Chagos
America/Cuiaba	Asia/Saigon	Indian/Christmas
America/Curacao	Asia/Sakhalin	Indian/Cocos
America/Danmarkshavn	Asia/Samarkand	Indian/Comoro
America/Dawson	Asia/Seoul	Indian/Kerguelen
America/Dawson_Creek	Asia/Shanghai	Indian/Mahe
America/Denver	Asia/Singapore	Indian/Maldives
America/Detroit	Asia/Taipei	Indian/Mauritius
America/Dominica	Asia/Tashkent	Indian/Mayotte
America/Edmonton	Asia/Tbilisi	Indian/Reunion

America/Eirunepe	Asia/Tehran	Iran
America/El_Salvador	Asia/Tel_Aviv	Israel
America/Ensenada	Asia/Thimbu	Jamaica
America/Fort_Wayne	Asia/Thimphu	Japan
America/Fortaleza	Asia/Tokyo	Kwajalein
America/Glace_Bay	Asia/Ujung_Pandang	Libya
America/Godthab	Asia/Ulaanbaatar	MET
America/Goose_Bay	Asia/Ulan_Bator	Mexico/BajaNorte
America/Grand_Turk	Asia/Urumqi	Mexico/BajaSur
America/Grenada	Asia/Vientiane	Mexico/General
America/Guadeloupe	Asia/Vladivostok	Mideast/Riyadh87
America/Guatemala	Asia/Yakutsk	Mideast/Riyadh88
America/Guayaquil	Asia/Yekaterinburg	Mideast/Riyadh89
America/Guyana	Asia/Yerevan	MST
America/Halifax	Atlantic/Azores	MST7MDT
America/Havana	Atlantic/Bermuda	Navajo
America/Hermosillo	Atlantic/Canary	New_Salem
America/Indiana/Indianapolis	Atlantic/Cape_Verde	NZ
America/Indiana/Knox	Atlantic/Faeroe	NZ-CHAT
America/Indiana/Marengo	Atlantic/Faroe	Pacific/Apia
America/Indiana/Petersburg	Atlantic/Jan_Mayen	Pacific/Auckland
America/Indiana/Tell_City	Atlantic/Madeira	Pacific/Chatham
America/Indiana/Vevay	Atlantic/Reykjavik	Pacific/Easter
America/Indiana/Vincennes	Atlantic/South_Georgia	Pacific/Efate
America/Indiana/Winamac	Atlantic/St_Helena	Pacific/Enderbury
America/Indianapolis	Atlantic/Stanley	Pacific/Fakaofo
America/Inuvik	Australia/ACT	Pacific/Fiji
America/Iqaluit	Australia/Adelaide	Pacific/Funafuti
America/Jamaica	Australia/Brisbane	Pacific/Galapagos

America/Jujuy	Australia/Broken_Hill	Pacific/Gambier
America/Juneau	Australia/Canberra	Pacific/Guadalcanal
America/Kentucky/Louisville	Australia/Currie	Pacific/Guam
America/Kentucky/Monticello	Australia/Darwin	Pacific/Honolulu
America/Knox_IN	Australia/Eucla	Pacific/Johnston
America/La_Paz	Australia/Hobart	Pacific/Kiritimati
America/Lima	Australia/LHI	Pacific/Kosrae
America/Los_Angeles	Australia/Lindeman	Pacific/Kwajalein
America/Louisville	Australia/Lord_Howe	Pacific/Majuro
America/Maceio	Australia/Melbourne	Pacific/Marquesas
America/Managua	Australia/North	Pacific/Midway
America/Manaus	Australia/NSW	Pacific/Nauru
America/Marigot	Australia/Perth	Pacific/Niue
America/Martinique	Australia/Queensland	Pacific/Norfolk
America/Mazatlan	Australia/South	Pacific/Noumea
America/Mendoza	Australia/Sydney	Pacific/Pago_Pago
America/Menominee	Australia/Tasmania	Pacific/Palau
America/Merida	Australia/Victoria	Pacific/Pitcairn
America/Mexico_City	Australia/West	Pacific/Ponape
America/Miquelon	Australia/Yancowinna	Pacific/Port_Moresby
America/Moncton	Brazil/Acre	Pacific/Rarotong
America/Monterrey	Brazil/DeNoronha	Pacific/Saipan
America/Montevideo	Brazil/East	Pacific/Samoa
America/Montreal	Brazil/West	Pacific/Tahiti
America/Montserrat	Buenos_Aires	Pacific/Tarawa
America/Nassau	Canada/Atlantic	Pacific/Tongatapu
America/New_York	Canada/Central	Pacific/Truk
America/Nipigon	Canada/Eastern	Pacific/Wake
America/Nome	Canada/East-Saskatchewan	Pacific/Wallis

America/Noronha	Canada/Mountain	Pacific/Yap
America/North_Dakota/	Canada/Newfoundland	Poland
America/North_Dakota/Center	Canada/Pacific	Portugal
America/Panama	Canada/Saskatchewan	PRC
America/Pangnirtung	Canada/Yukon	PST8PDT
America/Paramaribo	CET	ROC
America/Phoenix	Chile/Continental	ROK
America/Port_of_Spain	Chile/EasterIsland	Singapore
America/Port-au-Prince	ComodRivadavia	Turkey
America/Porto_Acre	CST6CDT	UCT
America/Porto_Velho	Cuba	Universal
America/Puerto_Rico	EET	US/Alaska
America/Rainy_River	Egypt	US/Aleutian
America/Rankin_Inlet	Eire	US/Arizona
America/Recife	EST	US/Central
America/Regina	EST5EDT	US/Eastern
America/Resolute	Etc/GMT	US/East-Indiana
America/Rio_Branco	Etc/GMT+0	US/Hawaii
America/Rosario	Etc/GMT+1	US/Indiana-Starke
America/Santarem	Etc/GMT+10	US/Michigan
America/Santiago	Etc/GMT+11	US/Mountain
America/Santo_Domingo	Etc/GMT+12	US/Pacific
America/Sao_Paulo	Etc/GMT+2	US/Samoa
America/Scoresbysund	Etc/GMT+3	UTC
America/Shiprock	Etc/GMT+4	WET
America/St_Barthelemy	Etc/GMT+5	W-SU
		Zulu