Performing Administrative Tasks

This chapter describes how to perform administrative tasks using Cisco CMX. Users who are assigned administration privileges can perform administrative tasks.

Cisco CMX User Accounts

Prior to Cisco CMX 10.2 all Cisco CMX processes ran under the Linux root user account. Cisco CMX 10.2 introduces two new user accounts (cmx and cmxadmin) to prevent any potential risks and secure the system.

- root: Root user account. Users should not use this account.

Note The password of the root account is now being set and maintained by the system owners, and no longer has a default password configured. This way, the account is still available for special-case installation and tackling debugging issues, and the root user will be owned by the end-user. Password recovery is accomplished through the use of the single user login process. For more information see Resetting Password - Cisco CMX Release 10.6 and Later with CentOS 7.0, on page 6.

- cmx: A no login account that now owns all the CMX processes with the exception of postgress.

- cmxadmin: Primary account used for the performance of all administrative tasks using CLI. User will *sudo* from this account to perform tasks requiring root-level access. This account is used to upgrade Cisco CMX 10.2 to a future release using GUI.
- admin: Admin user account for configuring maps, and Cisco WLCs, and restart services using Cisco CMX Web UI.
- normal user accounts: User-defined accounts. Use the **cmxos apiserver user** command to create/modify the Cisco CMX API users for this account.

Note From Cisco CMX Release 10.5.0, you must install the root patch to access root user account. For more information about transferring and installing patches, see Transferring and installing patches on CMX 10.6 and above.

Unlocking Users

You can unlock CMX access for a command line interface (CLI) or graphical user interface (GUI) user after they have been locked out, using the **cmxctl users unlock** command. For caveats and full details, refer to see the *Release Notes for Cisco CMX* at:

https://www.cisco.com/c/en/us/support/wireless/connected-mobile-experiences/products-release-notes-list.html

Before you begin

You must have root access credentials to modify these settings.

Procedure

Step 1 Connect to CMX via SSH, or through the console if FIPS or UCAPL is enabled.

Step 2 Enter one of the following commands to unlock a CMX user:

- **cmxctl users unlock cli** *username* to unlock a CLI user.
- **cmxctl users unlock gui** *username* to unlock a GUI user.

The user can log in again from the user interface you unlocked.

Setting Strong Password Authentication

You can enable strong password authentication with or without enabling FIPS or UCAPL mode. If you do plan to enable FIPS or UCAPL, set the correct minimums for that mode.

Before you begin

You must have CMX root user credentials to modify these settings.

If FIPS or UCAPL is enabled, you must connect directly from the console, or access the console through VMware VSphere client.

Procedure

Step 1 Connect to CMX via SSH, or through the console if FIPS or UCAPL is enabled.

Step 2 Enter the **cmxctl config auth settings** command to set password authentication settings.

Step 3 Respond to the following prompts:

Prompt	Action
Enable strong password [yes / no] [yes]:	Enable strong password authentication. Default is yes. CMX default: Not required. FIPS: Yes. UCAPL: Yes. **Note** If **Enable strong password** is set to **Yes**, you can extend the password upto 127 characters. However, we recommend you to ensure that password should have minimum one lower case, one upper case, one digit and a special character.
Minimum password length [8-20] [8]:	Set minimum password length. Range is 8-20 characters. Default is 8 characters. CMX default: 8 characters. FIPS: 8-20 characters. UCAPL: 15-20 characters.
Maximum password lifetime [1-9999] [9999]:	Duration after which password will expire. You must change password before the password expires. Range is 1-9999 days. CMX default: 9999 days. characters. UCAPL: 60 days.

Prompt	Action
Password Expiry Warning Period [1-30] [14]:	Password expiry warning period duration. Range is 1-30 days. CMX default: 14 days. characters. UCAPL: 7 days. **Note** If the password of Cisco CMX user is going to expire within the duration specified, then a warning message is displayed about the password expiry immediately following the login. On the Cisco CMX GUI, an alert window is displayed showing when the password is going to expire. If you are logging into Cisco CMX using SSH and the Cisco CMX CLI account for which the password is going to expire within the specified warning period, a warning message is printed just after the login successful message and before the command prompt. If password is already expired, then you will be redirected to change the password immediately after the login.
Unsuccessful login attempts before account lock [3-5] [3]:	Set the number of times a user can attempt to login before they are locked out for 30 minutes. Range is 3-5. Default is 3. CMX default: Not required. FIPS: 3-5. UCAPL: 3.
Fail interval in minutes [1-120] [15] :	Set the fail interval time in minutes. Range is 1-120. Default is 15. Fail interval time is automatically set to 15 minutes when UCPAL mode is enabled.
Account lockout interval in minutes [1-120] [30] :	Set the account locakout interval time in minutes. Range is 1-120. Default is 30.
Set session timeout in minutes [1-720] [30] :	Set the number of minutes a user can be inactive on the system before CMX times out. Range is 10-120 minutes. There is no default session timeout. CMX default: Not required. FIPS: 30 minutes or less. UCAPL: 10 minute timeout required.

Cisco CMX then restarts its authorization services.

Resetting Cisco CMX GUI Administrator Password

The GUI admin user password can be reset to the default of admin from the Cisco MSE CLI using the following command:

cmxctl users passwd username

Note You should know the cmxadmin user password for CLI access. If you do not know the current cmxadmin password, follow the guidelines to reset the root password. For more information, see and Resetting Root Password - Cisco CMX Release 10.4 and Earlier with CentOS 6.0, on page 5 and Resetting Password - Cisco CMX Release 10.6 and Later with CentOS 7.0, on page 6.

Resetting Root Password - Cisco CMX Release 10.4 and Earlier with CentOS 6.0

Cisco CMX uses a single user mode to reset the root/cmxadmin user passwords.

To enter into the single user mode you require:

- A (non-SSH) console connection to the Cisco Mobility Services Engine (Cisco MSE).
- A power-cycle of the Cisco MSE appliance

For Cisco CMX Release 10.4 and below with CentOS 6.0 operating system to reset the root or cmxadmin password, perform the following tasks:

Procedure

Step 1 Establish console access.

Step 2 Power on the Cisco MSE.

Step 3 Press the Up arrow key within 6 seconds of the first text appearing on window.

Step 4 When the GRUB menu is displayed:

a) Verify if the first entry is highlighted.
b) Press the **e** key to edit.

Step 5 Use the Down arrow key to highlight the entry that begins with the word *kernel*.

a) Press the **e** key to edit the entry.
b) Press the space bar, type the word **single**, and then press Enter.
c) Press the **b** key to boot the selected entry.

Step 6 After the system boots and you are at the # prompt:

a) Enter **passwd** <*username*> and press Enter.
b) When prompted, enter the new password for the user (root/cmxadmin) and press Enter.
c) Re-enter the password to verify.

Step 7 Type **reload** and press **Enter** to reboot the system and load the Cisco CMX services.

Resetting Password - Cisco CMX Release 10.6 and Later with CentOS 7.0

To recover a password, console access is mandatory. Console access can be a VM console or a physical console depending on the type of appliance used in the deployment.

Procedure

Step 1 Establish console access.

Step 2 Break the boot sequence on the GRUB screen.

Step 3 Choose the entry for the **Rescue** mode and then press the e.key to edit.

If prompted for username or password, enter the credentials as username: **root** password: **password** (not the configured root password).

Step 4 In the code, navigate to the line **linux16** and remove the last 2 parameters for **rhgb** and **quiet**.

Step 5 Add **rd.break enforcing=0** in the same **linux16** line.

Step 6 Press **Ctrl+X** to restart with the new parameters. After the system reboots, you are at the **switch_root:/**# prompt.

Step 7 Use the **# mount -o remount,rw /sysroot** command to mount the partition in read/write mode.

Step 8 Use **# chroot /sysroot** option to change the filesystem root.

Step 9 Use the **# passwd** command and enter the new root password.

Step 10 Use the **# mount -o remount,ro /** command to re-mount the partition in read-only mode.

Step 11 Enter the **exit** command twice to reboot the system and load the Cisco CMX services. The root password is successfully reset.

Setting Up External Server Authentication

Cisco CMX supports external AAA server authentication. Use external AAA authentication servers, such as Radius Server, and AD and allow Cisco CMX to delegate CMX's authentication functionality to the external AAA server. With this, CMX users can be directly managed, added, and deleted directly in the AAA server.

Note Cisco CMX does not support Terminal Access Controller Access-Control System (TACACS) protocol.

When the feature is enabled, the local user management for CMX GUI users is suspended and local GUI users are deleted. When a CMX user tries to log in to the CMX GUI, CMX authenticates the user against the credentials stored in this external AAA server. After the user is authenticated, CMX provides access to the GUI based on the user's role in CMX. From end-user perspective, this authentication by the AAA server is transparent and there is no change in the GUI behavior.

Procedure

Step 1 To configure external RADIUS authentication, run the **cmxctl config authserver** command.

Step 2 Use these subcommads as required:

a) **cmxctl config authserver delete**: Removes the external RADIUS authentication server.

b) **cmxctl config authserver settings**: Sets the external RADIUS authentication server.

c) **cmxctl config authserver show**: Shows the external server configuration.

Configuring Cisco CMX Users in the External Authentication Server

Before enabling this feature, the passwords and roles of the Cisco CMX GUI users should be configured in the external authentication server. A Cisco CMX user's ID and the role should be configured exactly as expected by Cisco CMX in this external authentication server.

Apart from this, a secret shared key should also be configured on the external authentication server. Later,the same shared key should be configured on Cisco CMX.

Configuring an External Authentication Server in Cisco CMX

You can configure an external authentication server using the **cmxctl config authserver settings** command. Provide the server IP address, shared secret key (which is already configured in the external authentication server, as described earlier), the local user name as a **`Last Resort`** user and the password.

If the connection to the external AAA server is lost due to some reason, a user can log in using this **Last Resort** user credentials, in which case, authentication is done by the Cisco CMX server itself. Thus, the system can function properly even if connectivity to the external AAA server is lost.

The following example shows how to configure an external RADIUS authentication server.

```
[cmxadmin@cmx]# cmxctl config authserver settings
Enter external RADIUS authentication server host : 1.2.3.4
Enter RADIUS server shared secret key : password
Configure local account. This account can be used if RADIUS server is not reachable.
Enter username : cmxadmin
Enter password :
Repeat for confirmation:
External RADIUS authentication server configured successfully
```

Configuring an External AAA Server with Cisco CMX

You can authenticate Cisco CMX users to connect with an external AAA server. For every authentication request, the server must sent Access-Accept or Access-Reject response packet depending upon the outcome of the authentication.

An external AAA server must be configured with the following details for AAA server and Cisco CMX to work together to perform external authentication. There are two types of AAA servers: Cisco ISE and freeradius.

Note In Cisco CMX Release 10.6.3, the External Authentication (AAA) feature is enabled without the Federal Information Processing Standard 140-2 (FIPS) or the U.S. Department of Defense Unified Capabilities Approved Products List (UCAPL) mode. Prior to Cisco CMX Release 10.6.3, the External Authentication (AAA) feature was only available with UCAPL mode enabled.

Procedure

Step 1 Access-Accept response must include the following Vendor Specific Attribute (VSA) information with value as appropriate role corresponding to the authenticated user.

a) Provide the **Attribute** value as **`Cisco-AVpair`**. For this VSA, provide **Type** as **`1`**.

b) Enter "shell:cmx-user-role=<ROLE>", wherein values for <ROLE> can be "Admin", "System", "Manage", "Location" and "Read Only".

Note Value string is case-sensitive.

Step 2 For **freeradius AAA server**, the sample string for role **Admin** in "users" is **`Cisco-AVPair = "shell:cmx-user-role=Admin"`**.

Step 3 For **Cisco ISE**, follow the steps:

a) In section **Policy> Policy Elements> Dictionaries > System> Radius> Radius Vendors** (if not configured already), add Vendor or Vendor specific attribute (VSA).

- **Vendor ID**: Enter the value as **`9 (Cisco Systems)`**.
- **VSA Type/ID**: Enter the value as **`1`**.

b) Add a Network Device Profile and associate correct vendor dictionary that contains VSA.

c) Add Cisco CMX as a Network Device and associate correct Network Device Profile.

d) Create authorization policies that sends Access-Accept packets in response to authentication requests.

- In the response, add Vendor Specific Attribute (Vendor ID=9 for Cisco Systems) named "cisco-avpair" (Type = 1) with a value of "shell:cmx-user-role=<ROLE>". <ROLE> can have the values "Admin", "System", "Manage", "Location" and "Read Only".

Note Value string is case-sensitive.

e) Create one authorization policy for every role that needs to be supported.

f) Create Policy Set with required authorization policies.

For more information on ISE configuration, see https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/215525-use-radius-for-device-administration-wit.html.

Note Along with UDP port 1812, UDP port 500 must be accessible from Cisco CMX to AAA/ISE when using IPSec.

Displaying External Authentication Server Settings

To display the settings of the currently configured external authentication server, run the **cmxctl config fips ucaplmode authserver show** command.

```
[cmxadmin@cmx]# cmxctl config fips ucaplmode authserver show
External RADIUS authentication server host : 1.2.3.4
RADIUS server shared secret key : password
Local user : cmxadmin
```

Deleting External Authentication Server Settings

To delete the currently configured external authentication server settings, run the **cmxctl config fips ucaplmode authserver delete** command.

When these settings are deleted, CMX reverts to local user management. Standard CMX UI users are re-created locally and their passwords are set to default. If new users were added to External Authentication Server, prior to disabling feature, you will need to configure those users in CMX UI as well.

Note If you have this feature enabled and later disable FIPS mode, this feature is also disabled and External Authentication Server details are deleted. Then CMX reverts to local user management as described above.

The following example shows how to delete the configured external authentication server settings.

```
[root@server]# cmxctl config fips ucaplmode authserver delete
External RADIUS authentication server is removed.
```

Setting Up Audit Logging

You can enable remote logging of system events, and specify which syslog events you want to log and view.

Before you begin

You must have CMX root user credentials to modify these settings.

If FIPS or UCAPL is enabled, you must connect directly from the console, or access the console through VMware VSphere client.

Procedure

Step 1 Connect to CMX via SSH, or through the console if FIPS or UCAPL is enabled.

Step 2 Enter the **cmxctl config audit settings** command.

Step 3 Respond to the following prompts. **Enter** selects the prompt default, shown in [brackets].

Prompt	Action
Enable or Disable Remote Syslogging [Enable / Disable] [Enable]:	Choose whether CMX should log system events. Options are Enable or Disable, and defaults to enable.

Prompt	Action
If logs size goes beyond l gb, drop or overwrite messages? [drop / overwrite] [overwrite]	Select CMX behavior when log size exceeds 1 gigabyte. Options are drop and overwrite, and defaults to overwrite.
Please enter rsyslog port [514]:	Optional. Enter the port number of a remote syslog server if you want to enable remote audit logging. The default is port number 514.
Please enter rsyslog DNS:	Optional. If your system uses a domain name server (DNS) for authentication, enter the DNS address here. There is no default. For example, *yoursyslogserver.yourco.com*
Please enter the email IDs (comma separated) for mail alerts:	List email IDs which need to receive important email alerts about audit logging.

A confirmation message displays.

```
Remote Audit Logging = Enabled
```

Step 4 Select the events you want Cisco CMX to log. Yes logs all events. No prompts you to select the event types you want to log, and confirms the update.

```
Show all logs [yes/no] [yes]: no
Enter day [today(1)/yesterday(2)/last week(3)/last month(4)/all(5)] [5]:
Enter event type [MGMT_EVENT(1)/CONN_EVENT(2)/AUTH_EVENT(3)/CONF_EVENT(4)/ALL(5) [5]:
Enter identity [root(1)/admin(2)/all(3)] [3]:
Enter status [success(1)/failure(2)/all(3) [3]:

Settings saved.
```

Note In Cisco CMX, audit logging is not enabled for user-related activities such as modifying a user and monitoring the user modification activities. Audit logging is not available for the **Settings** option and associated actions such as filtering probing clients or tracking parameters.

CMX then restarts the affected loggers.

Example

This example shows how to log everything except Connection, Management, and Misc events.

```
[root@server]# cmxctl config audit settings enable

Enable or Disable Audit Logging [Enable / Disable] [Enable]:enable
If logs size goes beyond lgb, drop or overwrite messages? [drop / overwrite]
[overwrite]:overwrite
Please enter rsyslog IP: 168.172.1.20
Please enter rsyslog port [514]: 514
Please enter rsyslog DNS: sls1296@wowco.com
Please enter the email IDs (comma separated) for mail alerts: email@example.com

Remote Audit Logging = Enabled

Please select the events to be logged
All Events [yes/no] [yes]: no
```

```
Connection Events [yes/no] [yes]:no
Management Events [yes/no] [yes]:no
Auth Events [yes/no] [yes]:
Configuration Events [yes/no] [yes]:
Security Configuration Events [yes/no] [yes]:
Security Events [yes/no] [yes]:
Misc Events [yes/no] [yes]:no
Settings saved.
```

Performing Scheduled Backup for Cisco CMX

You can use SSH File Transfer Protocol (SFTP) or Secure copy protocol (SCP) commands for backing up and restoring data on Cisco CMX 10.x. We recommend you to follow the below best practice for data backup automation.

Note Cisco CMX does not support File Transfer Protocol (FTP) commands for managing data.

Procedure

To schedule a Cisco CMX backup capability, run the **cmxos backupsched** command.

For more information, see the Cisco CMX command reference guide.

Performing Manual Backup for Cisco CMX

After you install and run Cisco CMX successfully, you can take a backup to avoid losing any data.

You may lose data on your CMX server, if:

- The hard disk in your CMX server fails
- The data on your CMX server is corrupted while upgrading

Therefore, backing up your data enables you to restore it to the original state. You can back up data on either /tmp or /opt partition. The /tmp folder is allocated 25 GB storage.

If Cisco CMX contains huge amount of saved data, the backup operation will take up extra disk space. In that case, you can consider the following:

- Back up to an external drive if there is not enough space on the Cisco CMX server. You can perform this operation by plugging in a removable hard disk or a mounted hard disk.
- After the backup operation, move the backup file (using scp) to a different server and remove it from the Cisco CMX server.

You can backup data such as location history, current client location, floor maps, and licenses.

Note We recommend that you backup database, floormaps, license and setup components to be compliant with General Data Protection Regulation (GDPR).

The following components are included in the backup:

- Database—Stores configuration data, such as, maps, controllers, location, and aggregated analytics data.
- Cache—Stores analytics repeat visits.
- Cassandra—Stores location history data and analytics raw visits.
- Influxdb—Stores metrics data for systems.
- Consul—Stores Consul configurations.
- Floormaps—Stores floor images for UI display.
- Licenses—Stores Cisco CMX license information.
- Setup—Stores CMX setup data.
- Conf—Stores node configurations.

Procedure

To perform a backup operation, run the **cmxos backup** command using the cmxadmin (non-root user) account.

You can include the -i (for example, cmxos backup -i database) parameter with the backup so that you can choose the components that you want to include in the backup.

The other backup options available are:

- **--all**—Include influxdb in the backup. The default is without influxdb and only includes postgres and Cassandra data.
- **--path**—Specify a location for the backup file. The default location is /tmp.
- **--online**—Perform the backup without stopping cmx services.
- **--offline**—Stop cmx services first and then perform the backup.

Note
- The destination directory for backup file requires rwx permission. When you specify a backup directory other than /tmp, ensure that the directory has "r/w/x" permission by user:cmx.
- If High Availability is enabled on Cisco CMX, online backup is supported only on primary and not secondary. If High Availability is disabled, online and offline backups are supported on both primary and secondary.

The following is a sample output from the **cmxos backup** command:

```
[cmxadmin@test ~]$ cmxos backup
Please enter the path for backup file [/tmp]: /tmp
[17:01:30] Preparing for backup...
```

```
Data size 287388806
Available disk space 139165282304
Pre-backup took: 0.0118758678436 seconds
['database', 'cache', 'cassandra', 'influxdb', 'consul', 'floormaps', 'licenses' , 'setup',
 'conf']
[17:01:30] Backup Database...
Backup database took: 1.15777993202 seconds
[17:01:32] Backup Cache...
Backup cache took: 0.383176088333 seconds
[17:01:32] Backup Cassandra...
Backup Cassandra DB took: 2.99715185165 seconds
[17:01:35] Backup InfluxDb...
Backup Influx DB took: 0.0846002101898 seconds
[17:01:35] Backup Consul...
Backup Consul took: 0.0185141563416 seconds
[17:01:35] Backup Floormaps...
Backup floor maps took: 0.000938892364502 seconds
[17:01:35] Backup licenses...
Backup licenses took: 0.000122785568237 seconds
[17:01:35] Backup setup...
Backup setup took: 0.000464200973511 seconds
[17:01:35] Backup node configuration...
Backup configuration took: 0.476609945297 seconds
[17:01:35] Creating tar file..
Post backup took: 16.3115179539 seconds
[17:01:52] Done Backup. Created backup file
/tmp/cmx_backup_test.cisco.com_2015_07_28_17_01.tar.gz
[cmxadmin@test ~]$
```

What to do next

You can automate the backing up process. For more information, see Performing Scheduled Backup for Cisco CMX, on page 11.

Increasing the Hard Disk Space

You can increase the hard disk space if your Virtual Machine that runs Cisco CMX is run out of disk space for backup.

Procedure

Step 1 Stop all the Cisco CMX services by entering the following commands:

cmxctl stop

cmxctl stop -a

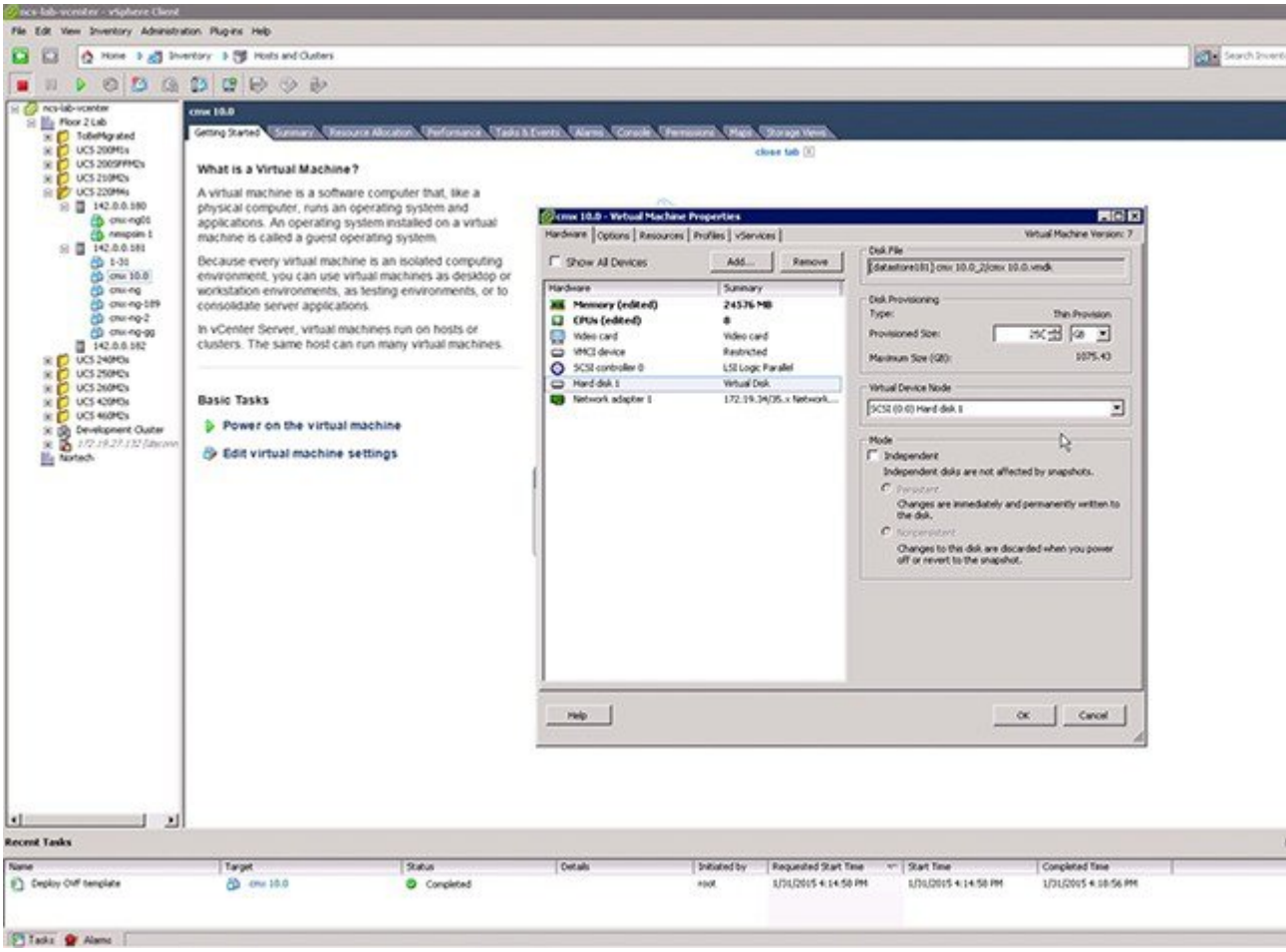
Step 2 Shutdown the virtual machine by entering the following command:

Shutdown –h now

Step 3 Edit the virtual machine settings and increase the hard disk space.

Note You cannot increase the hard disk space if the virtual machine was ever restored from snapshot.

Figure 1: Virtual Machine Settings



Step 4 Reboot the virtual machine.

After performing these steps, you can back up Cisco CMX.

You can enter the **cmxctl status** command to verify the status of CMX services. If any of the services is not running, you may need to restart it by entering the **cmxctl restart** <*service name*> command.

Restoring Data

After the backup, you can save the backup file in a safe location. If required, you can restore from this location.

To restore data, the Cisco CMX server must have free disk space which is 4 times the size of the backup file. If there is not enough disk space in the Cisco CMX server, you must increase the disk space. For more information, see Increasing the Hard Disk Space.

Note

- The restore of backup data on a third-party server is not allowed.
- Restoring Cisco CMX data must be done on a device that has the same local time as the device from which the data is collected.
- Otherwise, you will not be able to correctly access the analytics data. In addition, the data will result in errors or zero values on reports.

Procedure

To restore the data, enter the **cmxos restore** command using the cmxadmin (non-root user) account.

You can include the -i (for example, cmxos restore -i database) parameter with the **restore** command so that you can choose the components that you want to restore.

The following is a sample output from the **cmxos restore** command:

```
[cmxadmin@cmx~]# cmxos restore
Please enter the backup file path: /tmp/cmx_backup_test.cisco.com_2015_07_28_17_01.tar.gz
Please enter the path for untar backup file [/tmp]: /tmp
[17:08:54] Preparing for restore...
Restore size 27866720
Available disk space in /tmp is 139137040384
Available disk space is 139424529077
[17:08:54] Untarring backup file...
[17:08:55] Stopping all services...
Pre restore took: 26.4669179916 seconds
[17:09:21] Restoring Database...
Created database mse
Running command /usr/bin/sudo -u postgres  pg_restore -d mse -Fc
/tmp/cmx_backup_test.cisco.com_2015_07_28_17_01/postgres/mse.dump
Restored database mse
Restarting database...
Restore database took: 18.3071520329 seconds
[17:09:39] Restoring Cache...
Stopping cache_6383...
Restarting cache_6383...
Stopping cache_6380...
Restarting cache_6380...
..............
Stopping cache_6382...
Restarting cache_6382...
Stopping cache_6379...
Restarting cache_6379...
Stopping cache_6381...
Restarting cache_6381...
Stopping cache_6378...
Restarting cache_6378...
Restore Cache took: 46.7663149834 seconds
[17:10:26] Restoring Cassandra...
Stopping Cassandra...
Starting casandra
Creating cassandra scehma
..............
Restore Cassandra took: 29.5983269215 seconds
[17:10:56] Restoring Influxdb...
Stopping Influxdb...
```

```
Restarting Influxdb...
Restore Influx DB took: 13.9934449196 seconds
[17:11:10] Restoring consul...
Restore Consul took: 0.761927843094 seconds
[17:11:10] Restoring floormaps...
Restore floor maps took: 0.0269021987915 seconds
[17:11:10] Restoring licenses...
Restore licenses took: 0.00019907951355 seconds
[17:11:10] Restoring setup...
Restore setup took: 0.000532150268555 seconds
[17:11:10] Running Post Restore Tasks...
[17:11:10] Migrating Schemas...
[17:11:11] Migrating Cassandra schemas...
[17:11:12] Restarting all services...
stopping cassandra
Post restore took: 6.64956212044 seconds
[17:11:17] Starting all services...
..............
[17:12:45] Done
$
```

Encrypting the CMX /opt Directory

You can elect to encrypt CMX data in one of two ways:

- **CMX installation.** You have the option to encrypt the `/opt` partition of the disk as part of the installation process, or to skip it. Refer to *Cisco Mobility Services Engine Virtual Appliance Installation Guide for Cisco CMX, release 10.6* for more details.
- The **cmxos encryptdisk** command. You have the option to run the encryption command after installation. The following task uses this option. Refer to *Cisco CMX Command Reference, release 10.6* for more details.

Note We recommend that you enable encryption at installation, or as soon as possible afterward. The encryption process requires time proportional to the amount of data present on the `/opt` partition.

Important Encryption cannot be disabled or undone. It requires someone with root access credentials to manually enter the encrypted disk passphrase from the command line each time the device is rebooted or powered up.

Before you begin

You must have CMX root user credentials to modify these settings.

If FIPS or UCAPL is enabled, you must connect directly from the console, or access the console through VMware VSphere client.

Procedure

Step 1 Connect to CMX via SSH, or through the console if FIPS or UCAPL is enabled.

Step 2 Enter the **cmxos encryptdisk** command.

Step 3 At each of the following prompts, enter **y** to stop CMX and backup your data, or **N** to cancel. Data backup could take some time.

```
Have you closed all SSH sessions to this CMX? [y/N]:y
Are you sure you want to encrypt the /opt partition of the disk ? [y/N]:y

Checking disk space requirements for backing up /opt folder...
Looks Good.

Proceed with stopping all CMX services? [y/N]:y

Backing up /opt folder into /var ...
tar backup done.
Press Enter key to enter rescue mode and begin the encryption.
```

Step 4 Press **Enter** to continue. This process can take some time.

```
Shredding /opt ...
Shread: List of deleted folders
Shread: List of deleted folders
Shread: List of deleted folders
...
Formatting /opt ...

You will be prompted to set a passphrase for encrypted disk /opt.
Choose a passphrase, Enter and Verify it.

Note:
On every boot / power up, you will be prompted for this passphrase.
System will continue only if this passphrase is correct.
```

Step 5 Respond to the following prompt. If you enter **YES**, encryption is irreversable.

```
WARNING!
========
This will overwrite data on /dir/your_cmx/opt irrevocably.
Are you sure? (Type uppercase yes): YES
```

Step 6 Follow the prompts to select and confirm the encrypted disk passphrase.

```
Enter passphrase:
Verify passphrase:
Command successful.

Opening /opt ...
Enter passphrase for /dir/your_cmx/opt:
```

At this point, the encryption process begins in earnest. This process can take some time.

Step 7 When the process completes, press **Enter** at the prompt to reboot the disk.

```
Encryption of /opt is complete.

System will reboot now.
Upon (every) restart, when prompted to enter passphrase for /opt partition,
enter the passphrase you just set.

Press Enter to continue with reboot
```

Step 8 Once the system reboots, enter the encrypted disk passphrase at the prompt.

```
Please enter passphrase for disk device_name_opt on /opt!:
```

Step 9 Log into Cisco CMX command line.

Display a Login Banner

You can create a banner that displays when users log into CMX.

Before you begin

You must have CMX root user credentials to modify these settings.

If FIPS or UCAPL is enabled, you must connect directly from the console, or access the console through VMware VSphere client.

Procedure

Step 1 Connect to CMX via SSH, or through the console if FIPS or UCAPL is enabled.

Step 2 Enter the **cmxctl config banner edit** command.

If there is an existing banner, CMX displays the text [within brackets]. If none, the brackets are empty.

Step 3 Enter the banner text:

a) Type the text you want to display, and press **Enter**.

b) On the second line, type a period, and press **Enter**.

Your new banner will display the next time a user logs in from a browser or from the command line.

Note Use the **cmxctl config banner show** command to display the login banner.

Use the **cmxctl config banner disable** to disable the login banner.

For more information about the **cmxctl config banner** command, see https://www.cisco.com/c/en/us/td/docs/wireless/mse/10-6/cmx_command/cmxcli106.html.

Example

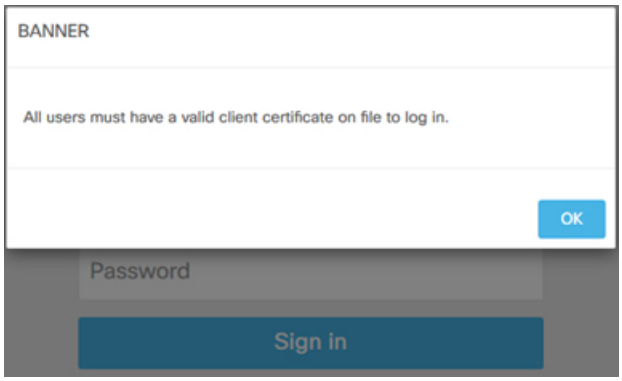
This example creates the following login banner: "All users must have a valid client certificate on file to log in."

```
Current Login Banner = []
Enter text to be displayed as login banner. Enter a single period on a line to
terminate.
```

```
All users must have a valid client certificate on file to log in.
.
starting /usr/sbin/sshd... \c
done.
```

When you opened CMX in a browser, you would see something similar to this:

Figure 2: Example of a login banner from a browser



Logging in from the command line, you would see something similar to this:

```
login as: cmxadmin
All users must have a valid client certificate on file to log in.
cmxadmin@192.168.1.20's password:
```

Managing NTP Servers

You can set up multiple Network Time Protocol (**NTP**) servers in Cisco CMX. You can add 2 types of NTP servers in Cisco CMX – unauthenticated NTP Server and and authenticated. You can add either a single unauthenticated NTP server or add up to 2 authenticated NTP servers.

Configuring Authenticated NTP Server

Before you begin

You need to decide on a local password for CMX's NTP client.

Procedure

Step 1 On NTP Server, run the **ntp-keygen -e -c RSA-SHA1 -p <server_password> -q <client_password>** command to export an IFF Key. Note that you must use the local password of the CMX NTP client for executing this command.

The command output is displayed as follows:

```
[cmxadmin@cmx]# ntp-keygen -e -c RSA-SHA1 -p <server_password> -q <client_password>
Using OpenSSL version OpenSSL 1.0.1e-fips 11 Feb 2013
Using host test group ntpserver
Using host key ntpkey_RSAhost_ntpserver.3747444855
```

```
Using host key as sign key
Using IFF keys ntpkey_IFFkey_ntpserver.37474448555
Writing IFF parameters ntpkey_iffpar_ntpserver.3747444855 to stdout
# ntpkey_iffpar_ntpserver.3747444855
# Mon Oct  1 21:54:15 2018

-----BEGIN PRIVATE KEY-----
MIG0AgEAMIGpBgcqhkjOOAQBMIGdAkEAvi39ekol/VjRa5J8D329KUY+U6V63XBE
6xOFGlSFIii/3j87ZEy5U7M6aJte8N0RFrR/HNdXl2HUAsEPyYXjmwIVALVEPtki
j4NB7b7lDgq7VWwhIcwDAkEAnMdvYaA4AA4DCeiszaTecVAtRnuZlajE8r7+hq64
hR+/ircsjjICmrgCdJXrgv+NDRi6L48LBGHyCbrsK5TiNAQDAgEB
-----END PRIVATE KEY-----
Writing IFF keys ntpkey_iffkey_ntpserver.3747444855 to stdout
# ntpkey_iffkey_ntpserver.3747444855
# Mon Oct  1 21:54:15 2018

-----BEGIN ENCRYPTED PRIVATE KEY-----
MIH9MEAGCSqGSIb3DQEFDTAzMBsGCSqGSIb3DQEFDDAOBAj8r+RVOkTclgICCAAw
FAYIKoZIhvcNAwcECGQosPZ3xNr9BIG4AozI6FFAlP1M+O9JI3SA+iDmamB7ONwl
iXzmVJgspncg5NXwU3AJYxhNHvRN+/ENWdiUev3vRcCdvFHOF5HDiAHYSx0OTtQE
749FmolxuWq+Fsy6KDDH+EmcgKOEjFtnNu7z7Y7dBeGlrFxBnctAtbyhjzZVMnCf
jIwaSyySquA38OlMii7LEuCVuUBzJvcOjLHqVOpIphZUUnMPs9+cthzlIC3HChGB
nYHFkDVUvuLIcRiUDILb/g==
-----END ENCRYPTED PRIVATE KEY-----
```

Step 2 From the command output, copy or export the the ENCRYPTED PRIVATE KEY block along with preceding 2 comment lines into a file.

Step 3 SCP the file to Cisco CMX server.

Step 4 Connect to CMX command line either from a console, or from a VMWare vSphere console.

Step 5 To delete all the NTP configurations, run the **cmxos ntp clear** command.

Step 6 To configure authenticated NTP server, run the **cmxos ntp type** command, followed by the IP addresses of the NTP server.

```
[cmxadmin@cmx]$ cmxos ntp type
Current NTP Type = <Not Set>
Select NTP Type [1] Unauthenticated, [2] Authenticated or [3] Skip [3]: 2

Changing the NTP Type = Authenticated
Enter local password:
Repeat for confirmation:
Password changed and host key/cert file generated successfully.

Enter hostname / IP for NTP Server #1 (blank to skip) []: 172.19.28.54
Please enter complete path of exported IFF (encrypted) key file: /tmp/iffkey
Checking if server 172.19.28.54 is reachable ...
OK
Key file successfully saved as ntpkey_iffkey_cmx-vmdev334.3747444855
NTP Server added successfully

Enter hostname / IP for NTP Server #2 (blank to skip) []:
```

Step 7 Repeat step 6 to add the second NTP server.

Note that you need to wait for a few minutes for the NTP servers to sysnchronize.

Step 8 (Optional) To verify the status of the NTP server configuration, run the **cmxos ntp status** command. Add **--verbose** to get detailed status.

```
[cmxadmin@cmx]# cmxos ntp status
NTP Type = Authenticated
Status   = Synchronized
```

```
[cmxadmin@cmx-vmdev281 ~]$ cmxos ntp status --verbose
NTP Type = Authenticated
Status   = Synchronized

synchronised to NTP server (1.2.3.4) at stratum 3
   time correct to within 990 ms
   polling server every 64 s

     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*1.2.3.4              1.8.8.5     2 u   46   64   37    0.585   10.659   8.258

ind assid status  conf reach auth condition  last_event cnt
===========================================================
  1  4891  f63a   yes   yes   ok   sys.peer    sys_peer  3
```

Note If you want to change NTP type from unauthenticated to authenticated or vice versa, you can change it using following commands:

a. Run the **cmxos ntp clear** command to clear current NTP settings.

b. Run the **cmxos ntp type** command to select appropriate type.

Configuring Unauthenticated NTP Server

To add unauthenticated NTP server, follow these steps:

Procedure

Step 1 Connect to CMX command line either from a console, or from a VMWare vSphere console.

Step 2 To delete all the NTP configurations, run the **cmxos ntp clear** command.

Step 3 To configure unauthenticated NTP server, run the **cmxos ntp type** command, followed by the IP addresses of the NTP server.

Step 4 (Optional) To verify the status of the NTP server configuration, run the **cmxos ntp status** command.

Updating Auntenticated NTP Server Parameters

To update configured authenticated NTP server parameters, follow the steps:

Procedure

Step 1 To change the local password and set a new password, run the **cmxos ntp auth password** command.

1. If you want to change the local password, execute cmxos ntp auth password command and set the new password

```
[cmxadmin@cmx]# cmxos ntp auth password
Enter local password:
Repeat for confirmation:
Password changed and host key/cert file generated successfully.
[cmxadmin@cmx-vmdev282 ~]$
```

Step 2 To add/delete NTP server details, run the **cmxos ntp auth servers** command.

```
[cmxadmin@cmx]# cmxos ntp auth servers

Server 1 is already configured with IP 1.2.3.4

Do you want to (1) Edit (2) Delete (3) Skip ? [1]: 3
Enter hostname / IP for NTP Server #2 (blank to skip) []: 1.2.3.5
Please enter complete path of exported IFF (encrypted) key file: /tmp/iffkey2
Checking if server 1.2.3.5 is reachable ...
OK
Key file successfully saved as ntpkey_iffkey_ntpserver2.3747444855
NTP Server added successfully

NTP Service restarted successfully
```

Note If you need to restart NTP service, run the **cmxos ntp restart** command. It will restart NTP daemon. Run **cmxos ntp status** command to check the NTP status. You can add **--verbose** option to the command if you want detailed output.

```
[cmxadmin@cmx]# cmxos ntp restart
NTP Service restarted successfully
```

Troubleshooting Cisco CMX Server Shutdown Problems

The Cisco CMX server shuts down all the services when disk space usage reaches 85 percent. If you encounter this issue, create additional disk space on your Cisco CMX server by deleting unnecessary files, if any, from the server. Run the cmxos clean find/normal command to find unnecessary files and delete it to free some disk space.

After you have sufficient space, you can choose to restart your Cisco CMX server by running the **cmxctl start –a** command, if required.

Performing Periodic Maintenance for Cisco CMX

We recommend that you schedule a maintenance window every two months to perform Cisco CMX software restart (system, application services). This periodic maintenance can be performed on both HA and standalone setups. It will take up to 5 mins and help Cisco CMX to reclaim system resources yielding better performance. From the operations perspective this would result in scheduled downtime of approximately 30 mins per year.

Note To clean up long queues and long running processes, we recommend that you schedule a full restart of Cisco CMX once a month during a low activity time, such as late at night or early in the morning. The restart takes approximately 5 minutes to complete.

To restart Cisco CMX, follow the steps

Procedure

Step 1 To shut down a Cisco CMX service, run the following command:

cmxctl stop -a

Step 2 To kill services, run the following command:

cmxos kill

Step 3 To restart agent, run the following command:

cmxctl agent restart

Step 4 To restart a Cisco CMX service, run the following command:

cmxctl start

Step 5 To start Cisco CMX API server, run the following command:

cmxos apiserver start