PowerEdge FX2 Chassis Management at Server

Dell Engineering and Technical Marketing

Chris Poblete, Rajeswari Ayyaswamy

March 2015

Table of contents

1 Chassis Management at Server Overview 4

2 How do you configure CMAS? 5

2.1 Configure CMAS in CMC 5

2.2 Configure CMAS in iDRAC 6

2.3 Configure Shared Component Update in iDRAC 8

3 What can you do with CMAS? 11

3.1 Configure CMC networking from server 11

3.2 Chassis sensor inventory and monitoring from iDRAC 13

3.3 CMC firmware update from iDRAC 16

3.4 CMC event proxy via iDRAC 17

3.5 CMC racadm command proxy via iDRAC 18

A Appendix 20

A.1 Glossary 20

A.2 Troubleshooting 20

A.3 Additional resources 21

1 Chassis Management at Server Overview

Chassis Management at Server, or CMAS, is the ability to manage and monitor the server and the chassis from the server's iDRAC. It breaks the tradition of one way chassis-server management where iDRAC manages only the server while CMC manages the chassis plus a limited server management such as power control. PowerEdge FX2 is unique because it allows shared infrastructure management in the server's iDRAC through CMAS.

How is CMAS useful?

a. CMAS is useful out of the box to configure CMC networking from a server during POST.
b. CMAS provides chassis sensor inventory and monitoring from the server's iDRAC.
c. CMAS allows CMC firmware update from the server's iDRAC.
d. CMAS allows CMC event proxy via the server's iDRAC.
e. CMAS allows CMC racadm command proxy via the server's iDRAC.

The following table shows the hardware and software requirements for CMAS feature.

Component	Requirement
Chassis	PowerEdge FX2 PowerEdge FX2s
Chassis Management Controller	CMC version 1.10 or later
Sleds	PowerEdge FM120 PowerEdge FC430 PowerEdge FC630 PowerEdge FC830
Management Controller	iDRAC7 version 1.57.57 or later iDRAC8 version 2.05.05 or later

2 How do you configure CMAS?

Chassis Management at Server feature requires enablement from two sides. The CMAS setting must be enabled both in CMC and in iDRAC for the feature to work. The default CMAS setting on both sides is Enabled. That means you are able to use the CMAS capabilities out of the box or when you reset configurations to default.

2.1 Configure CMAS in CMC

In CMC, Chassis Management at Server feature supports the following settings:

Mode	Description
None	Disables CMAS feature
Monitor	Enables read-only access to chassis shared infrastructure data from iDRAC
Manage and Monitor	Enables chassis shared infrastructure management from iDRAC (default value)

Note: To modify CMAS in CMC, the user must have the Login and Chassis Configuration privileges.

The settings can be configured using racadm or the CMC web UI.

Using racadm

Use the property *cfgRacTuneChassisMgmtAtServer* from group *cfgRacTuning*. This property is numeric. The numeric descriptions is as follows:

Value	Description
0	None
1	Monitor
2	Manage and Monitor (default value)

Example command to get the current value:

```
$ racadm getconfig -g cfgRacTuning -o cfgRacTuneChassisMgmtAtServer
```

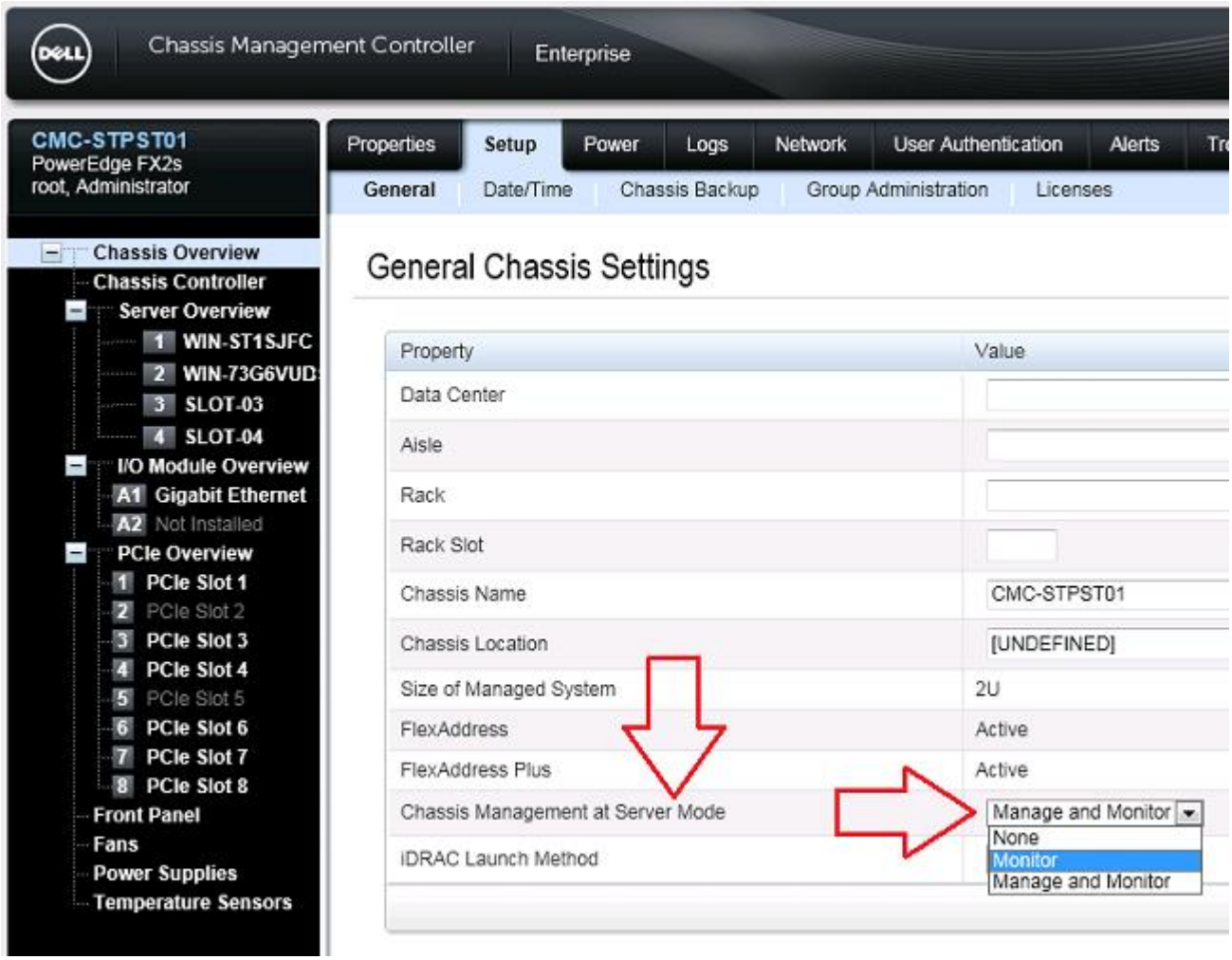
Example command to configure a new value (example Monitor):

```
$ racadm config -g cfgRacTuning -o cfgRacTuneChassisMgmtAtServer 1
```

Using web UI

Login to CMC web UI and go to **Chassis Overview > Setup > General > General Chassis Settings** and look for the property *Chassis Management at Server Mode*.

Figure 1 – Configure CMAS in CMC



2.2 Configure CMAS in iDRAC

The CMAS configuration in iDRAC supports the following settings:

Mode	Description
Disabed	Disables CMAS feature for this iDRAC
Enabled	Allow chassis shared infrastructure management from this iDRAC

Note: To modify CMAS setting in iDRAC, the user must have the Server Control privilege. License required is base license.

The settings can be configured using racadm or the CMC web UI.

Using racadm

To configure CMAS, use the property *System.ChassisControl.ChassisManagementMonitoring*. The property may be set as numeric or as enumeration. Use the following table for reference:

Numeric Value	Enumeration Value
0	Disabled
1	Enabled (default value)

Example command to get the current value:

```
/admin1-> racadm get System.ChassisControl.ChassisManagementMonitoring
```

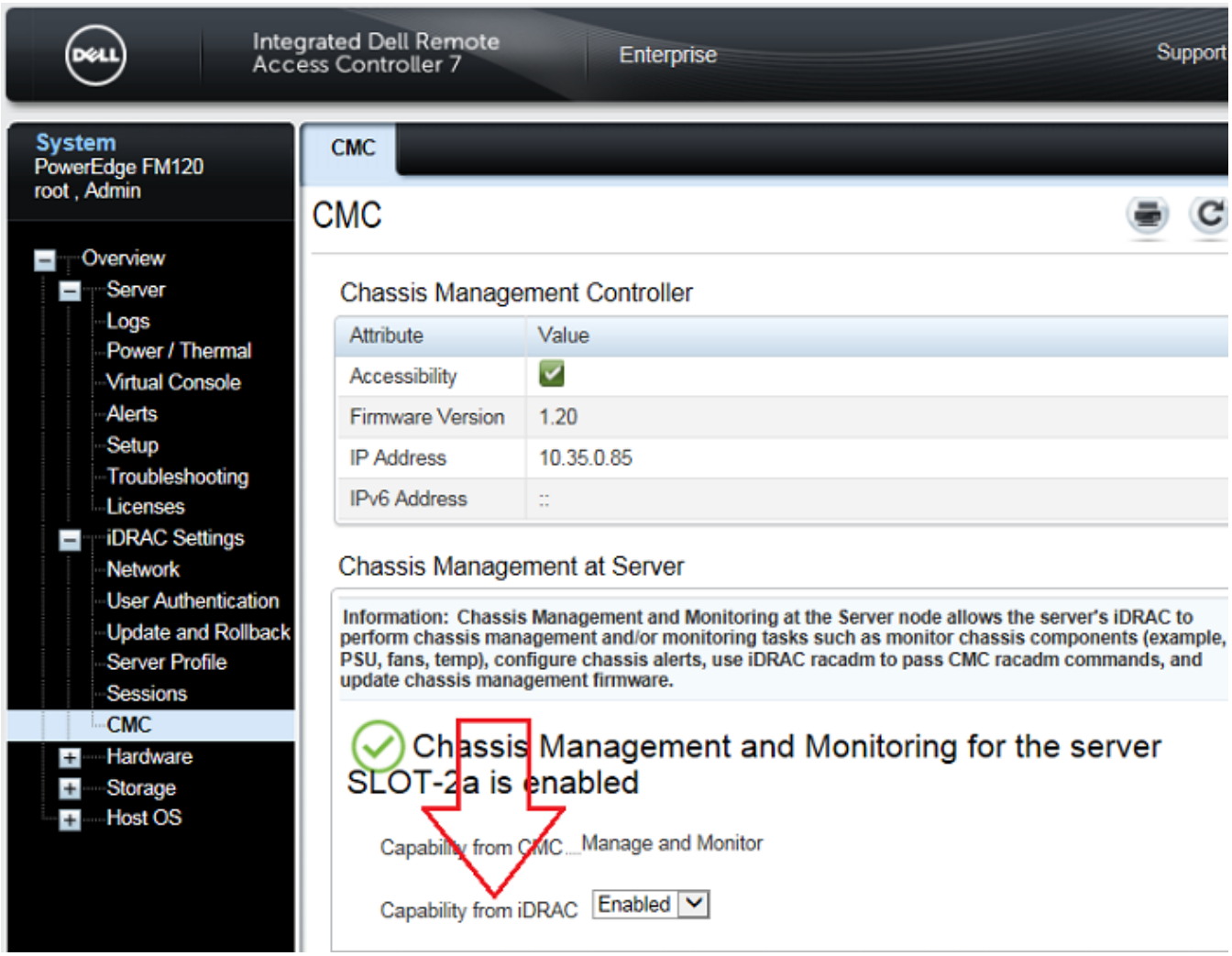
Example command to configure a new value (example Enabled):

```
/admin1-> racadm set System.ChassisControl.ChassisManagementMonitoring 1
```

Using web UI

Login to iDRAC web UI and go to **Overview > iDRAC Settings > CMC > Chassis Management at Server** and look for the *Capability from iDRAC.*

Figure 2 – Configure CMAS in iDRAC



2.3 Configure Shared Component Update in iDRAC

Shared Component Update is a feature that allows users to update CMC firmware from iDRAC through the Chassis Management at Server feature. Shared Component Update in iDRAC supports the following settings:

Mode	Description
Disabled	Disables shared component update from iDRAC
Enabled	Allow CMC firmware update through host OS and Lifecycle Controller from iDRAC. Prerequisite: Property *System.ChassisControl.ChassisManagementMonitoring* must be Enabled first.

Note: To modify Shared Component Update setting in iDRAC, the user must have the Server Control privilege. License required is base license.

Requires

- iDRAC firmware version 2.10.10 or later

The settings can be configured using racadm or the CMC web UI.

Using racadm

To configure Shared Component Update, use the property *iDRAC.Update.EnableSharedCompUpdate*. The property may be set as numeric or as enumeration. Use the following table for reference:

Numeric Value	Enumeration Value
0	Disabled (default value)
1	Enabled

Example command to get the current value:

```
/admin1-> racadm get iDRAC.Update.EnableSharedCompUpdate
```

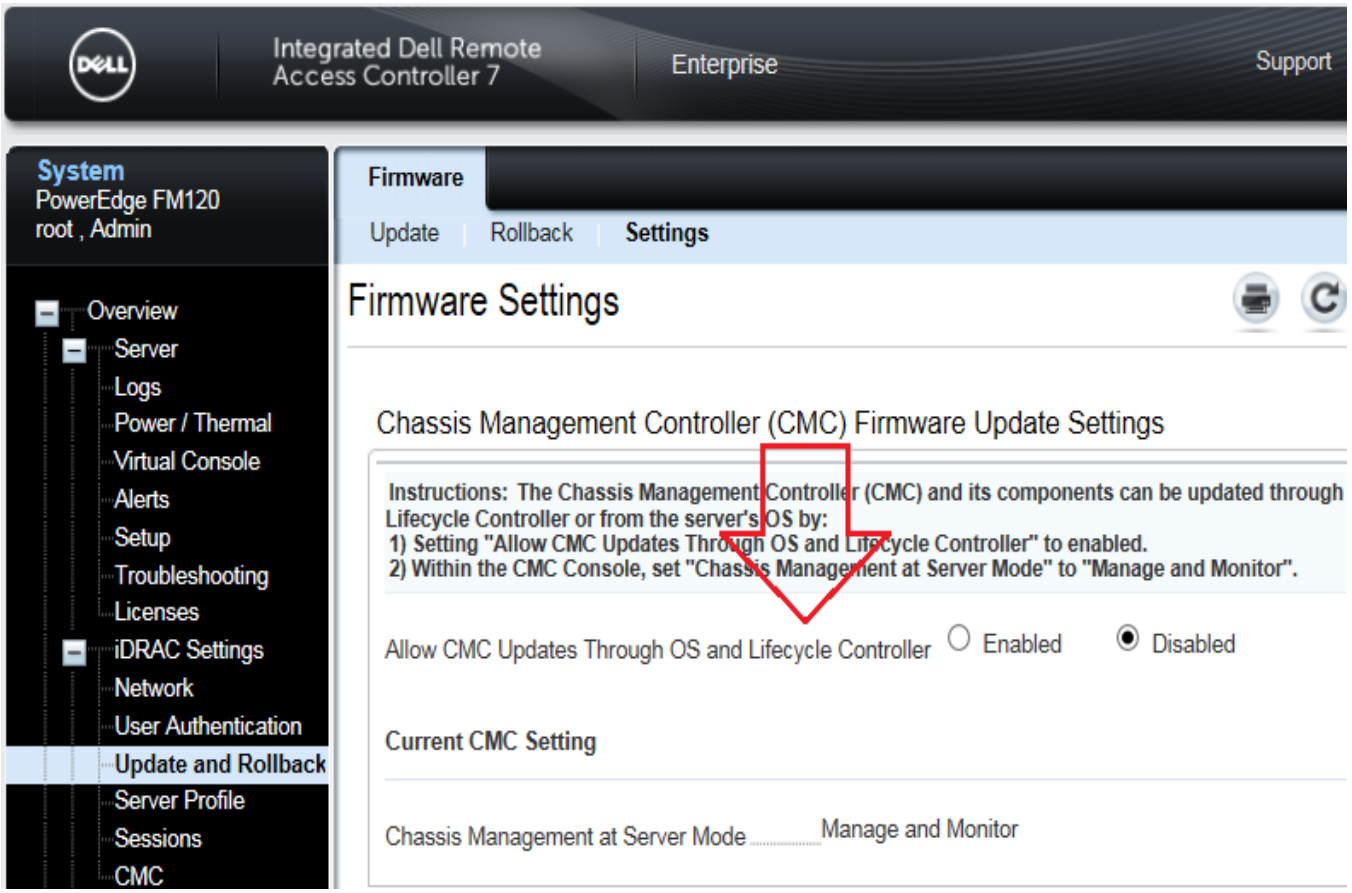
Example command to configure a new value (example Enabled):

```
/admin1-> racadm set iDRAC.Update.EnableSharedCompUpdate 1
```

Using web UI

Login to iDRAC web UI and go to **Overview > iDRAC Settings > Update and Rollback > Firmware > Settings > CMC Firmware Updating Settings** and look for the *Allow CMC Updates through OS and Lifecycle Controller.*

Figure 3 – Configure shared component update in iDRAC



3 What can you do with CMAS?

3.1 Configure CMC networking from server

Out of the box, PowerEdge FX2 CMC network configuration is set to static IP address. Once a network cable is connected to the CMC port 1, you can access the CMC using the static IP address 192.168.0.120. This is also the default IP address which is set when you reset CMC configuration to default settings.

PowerEdge FX2 chassis does not have an LCD panel like its predecessors PowerEdge M1000e and VRTX. So how is this done in FX2?

Requires

- Manage and Monitor mode in CMC

Either out of the box or after resetting configuration of CMC and iDRAC, the steps to configure CMC networking from a server are:

1. Attach a monitor and keyboard in the KVM "right" panel of the chassis. Alternatively, you can use remote console redirection via iDRAC.
2. Choose a server in any slot and use the KVM select button located in the Control "left" panel of the chassis to cycle the selection of KVM to the server.
3. Power on the server using the sled power button.
4. Press F2 to go to System Setup.
5. Get current IP address of CMC.
   a) Once in System Setup, select:
      iDRAC Settings > System Summary
   b) Scroll down the page to the bottom to see *Chassis Management Controller* section.
   c) Snapshot below shows you what you see in this page.
6. Configure network settings of CMC.
   a) Once in System Setup, select:
      iDRAC Settings > CMC Settings > CMC Network
   b) Snapshots below shows you what you can configure in the Network page.

Snapshots

Figure 4 – CMC current settings in System Setup

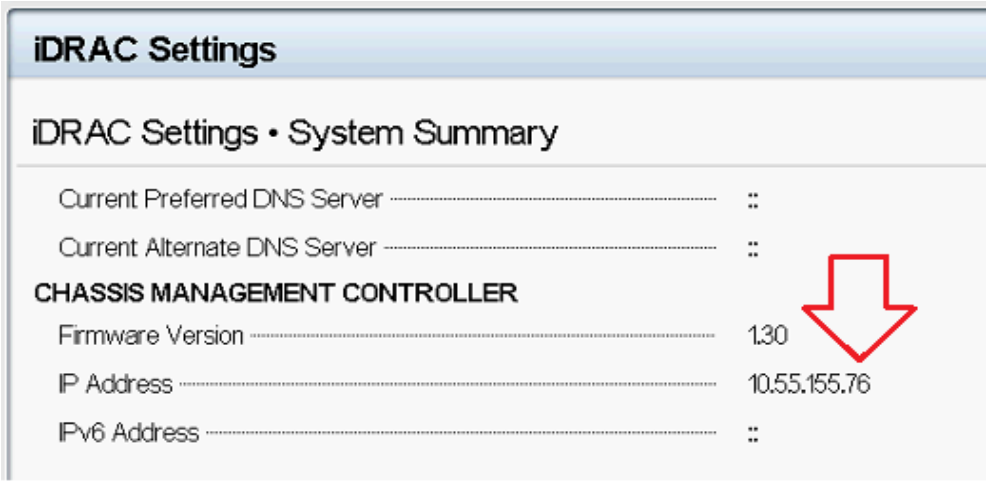


Figure 5 – CMC network settings (part 1 of 3)

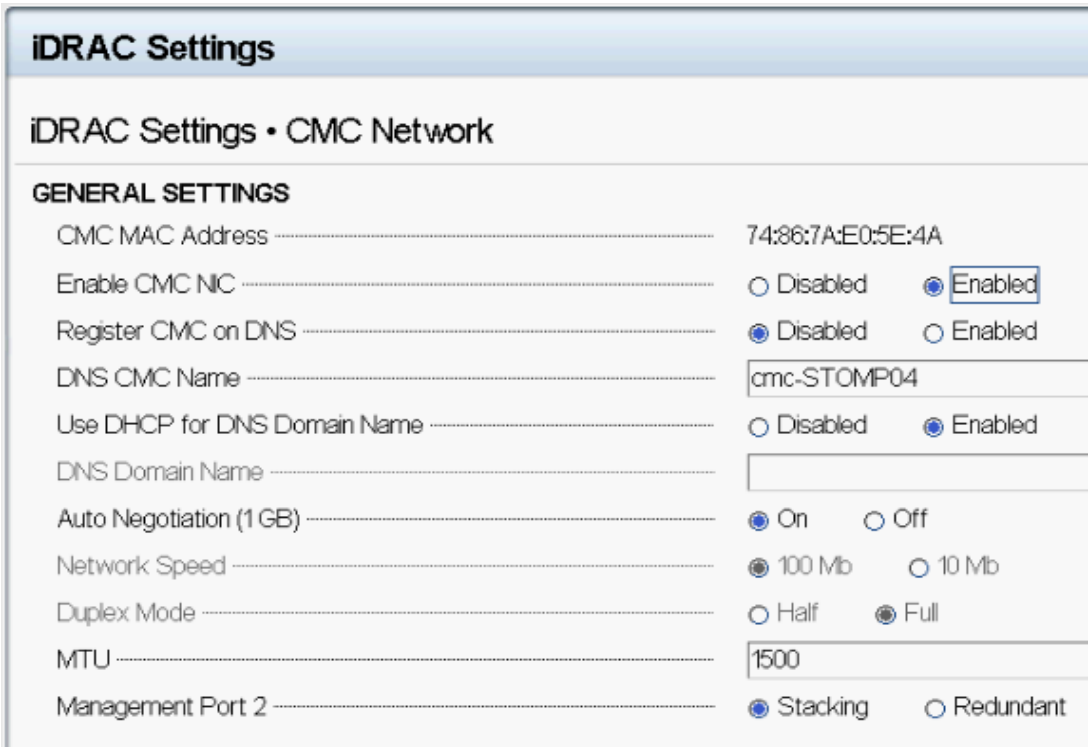
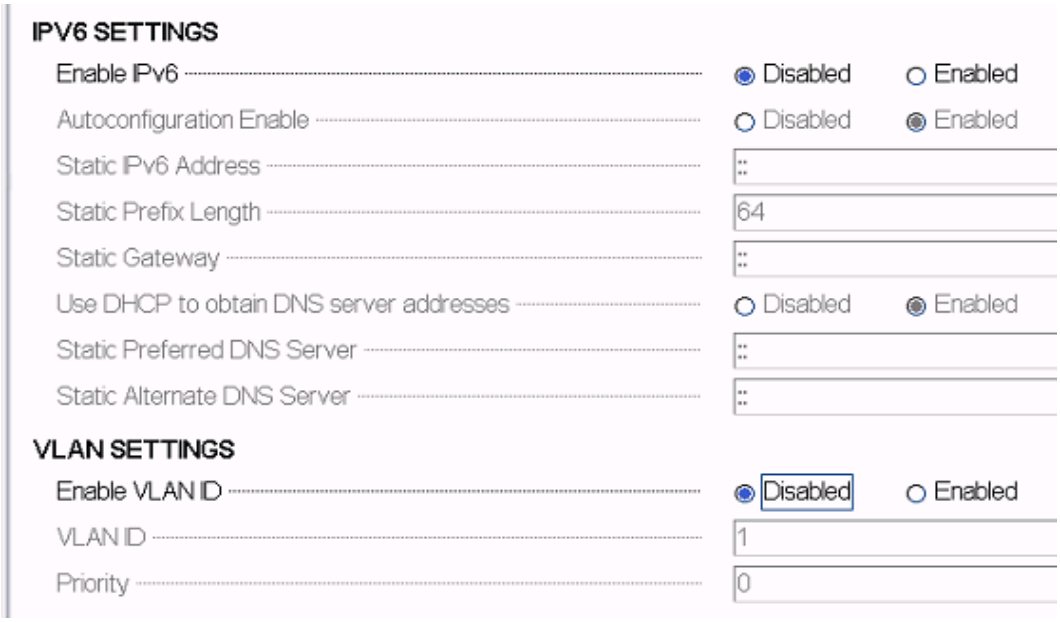


Figure 6 – CMC network settings (part 2 of 3)

Figure 7 – CMC network settings (part 3 of 3)



3.2 Chassis sensor inventory and monitoring from iDRAC

The following chassis sensor information is shared for iDRAC through CMAS:

a. Chassis fans
b. Chassis power supply
c. Chassis ambient temperature

The above sensor information is available to all interfaces where sensors such as CPU are reported.

a. iDRAC web UI
b. Lifecycle Controller (F10)
c. iDRAC racadm
d. WSMAN (CIM_View, CIM_Sensor)

e. IPMI sensors
f. iDRAC SNMP

Snapshots

Figure 8 – Chassis fans and power supplies in iDRAC web UI

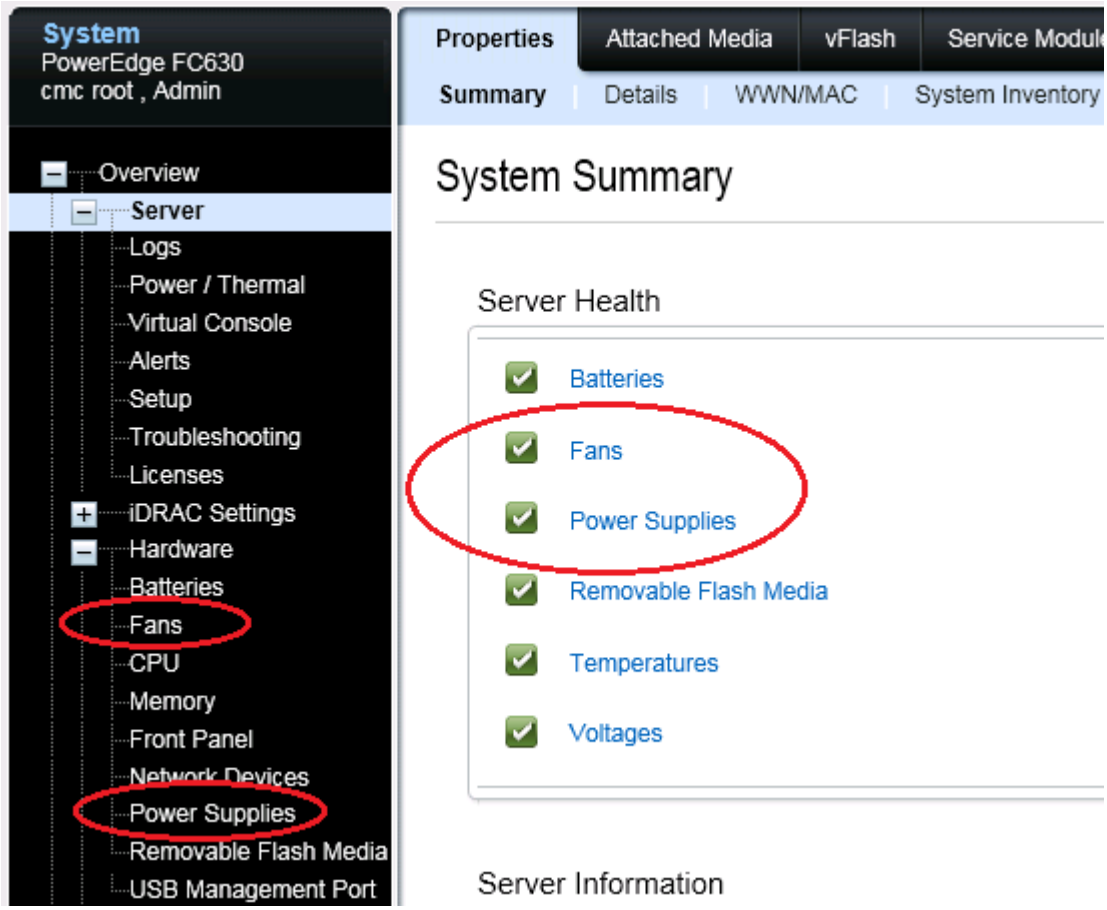


Figure 9 – Chassis fans and power supplies in Hardware Inventory under iDRAC web UI.

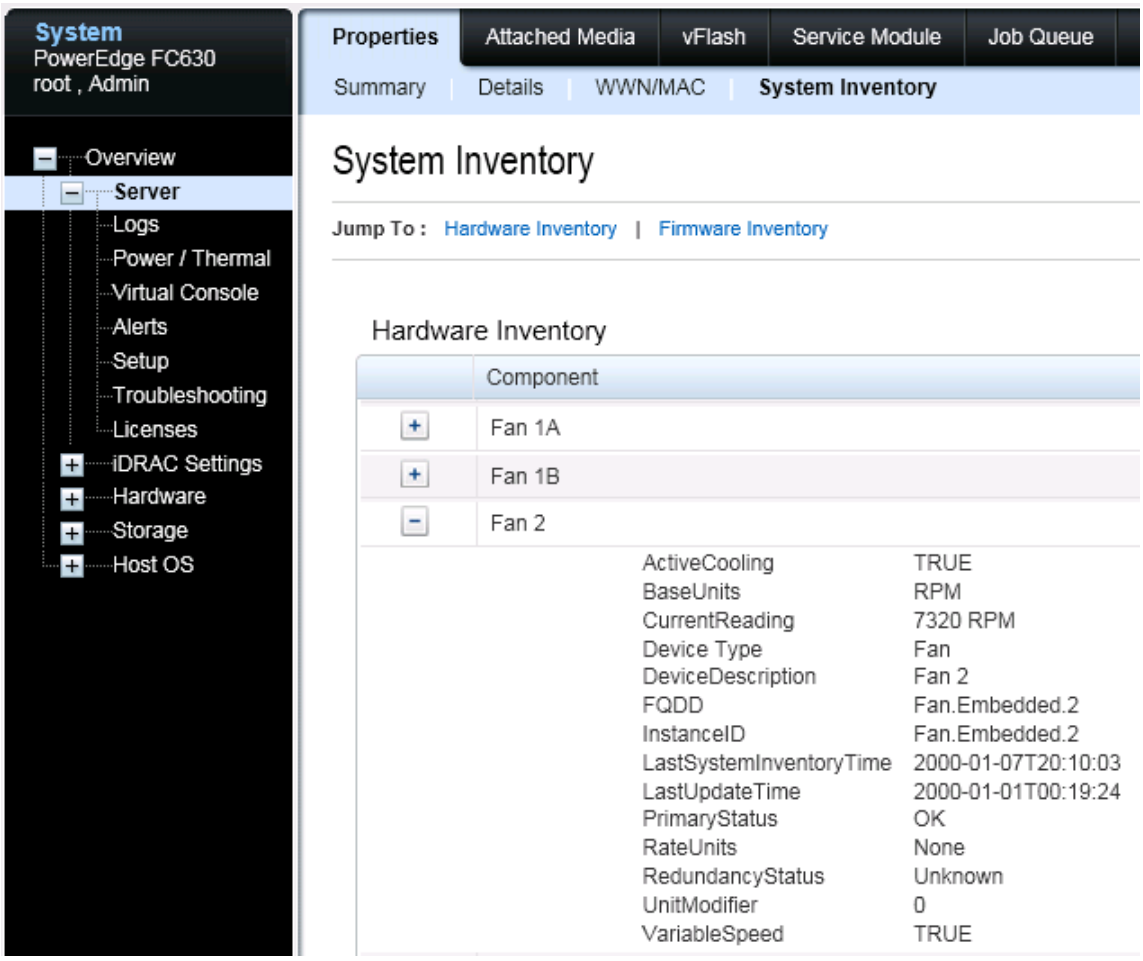
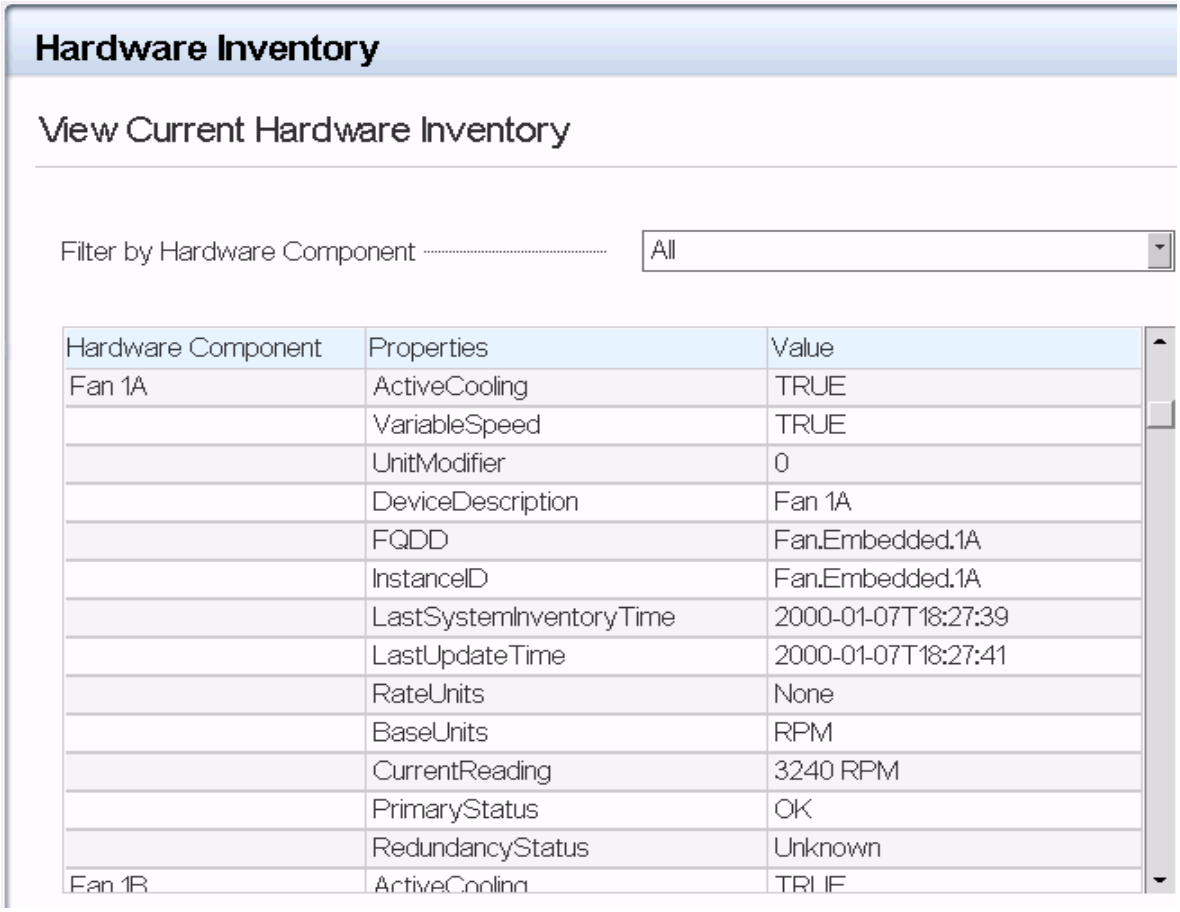


Figure 10 – Chassis fans and power supplies in Hardware Inventory under Lifecycle Controller (F10) page.



3.3 CMC firmware update from iDRAC

Using CMAS feature and with additional configuration in iDRAC, the CMC firmware can be updated from the Sled through all supported update interfaces.

a. Supported host OS (refer to iDRAC User's Guide for the list)
b. Web UI
c. racadm
d. WSMAN
e. Lifecycle Controller

Requires

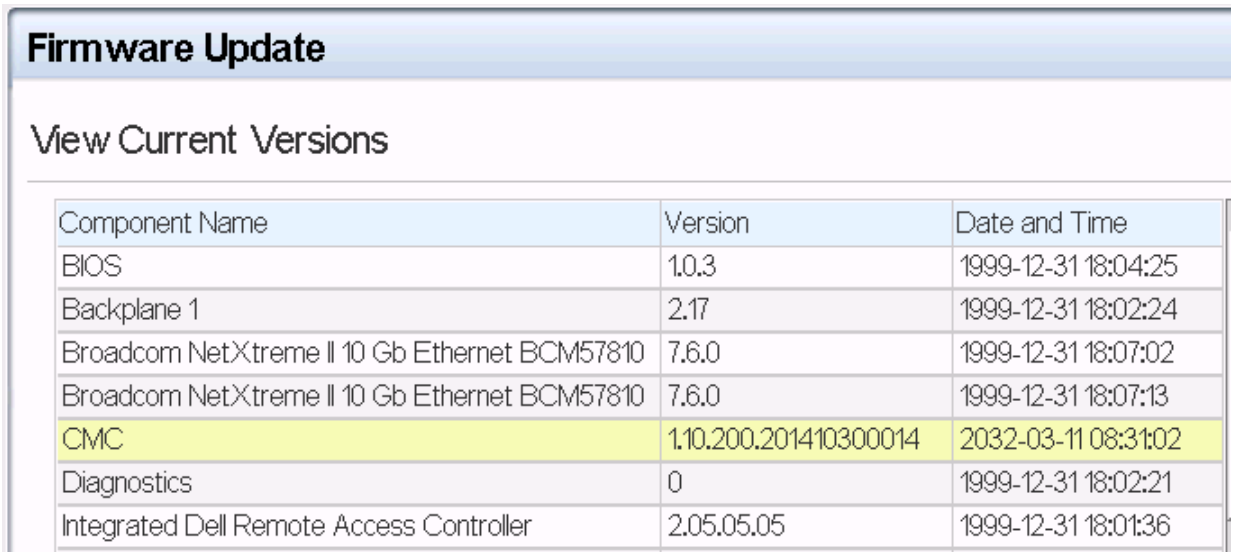
- iDRAC firmware version 2.05.05 or later
- Manage and Monitor mode in CMC
- Shared Component Update enabled in iDRAC

When Shared Component Update is enabled in iDRAC, the CMC firmware component is added to the Firmware Inventory list.

Similar to other component when updating through iDRAC or Lifecycle Controller, provide the EXE update file of the CMC update package. You can get this from the PowerEdge FX2 driver download from support.dell.com.

Snapshots

Figure 11 – CMC firmware in the Firmware inventory list under Lifecycle Controller



3.4 CMC event proxy via iDRAC

Using CMAS capability, all CMC events logged to the chassis log can be sent from CMC to iDRAC. With the proxy feature, CMC events can be monitored via iDRAC alert mechanism without placing CMC on the network.

Requires

- CMC firmware version 1.20 or later
- iDRAC firmware version 2.10.10 or later

When CMAS is enabled, CMC events are forwarded to iDRAC and logged to the iDRAC's Lifecycle Log. For each event originating from CMC and given the matching category, type and severity, an alert from iDRAC and an alert from CMC can be sent if both have alerts configured and enabled. Configure the alerts on both sides properly to prevent duplicates.

Example

CMC event: *Clear system event log (SEL)*

This event corresponds to the alert filter described in the table below when looking at the web UI.

Filter	In CMC	In iDRAC

Category	System Health	System Health
Event/Alert	Sys Event Log	Sys Event Log
Severity	Informational	Informational

Alert targets are configured independently in CMC and iDRAC. For example, CMC could be configured to send an email alert for this event, while iDRAC could be configured to send SNMP trap for this event.

How do I limit PSU/fan alerts to come from a single server?

There are two ways to accomplish this. One way is to enable CMAS on the server you want as your source and then disable CMAS on the other servers using the information in Section 2.2 on how to Configure CMAS in iDRAC, In this scenario, only one iDRAC in the chassis has access to components shared by CMAS feature but it guarantees that any alerts associated with shared components will come from only one iDRAC. Note that if you remove the sled containing this iDRAC, you lose access to CMAS features.

The other way is to leave CMAS enabled in all iDRAC in the chassis but disable all alerts associated to PSU and fans in each of the iDRAC except from the iDRAC that you want as your source. But PSU and fans are not the only source of events that come from CMC. There are other CMC events such as "clear System Event Log (SEL)" that have similar events in iDRAC. There is no option to disable a particular event originating from either CMC or iDRAC.

Choose one of the two ways described above that best fits your needs.

3.5 CMC racadm command proxy via iDRAC

Using CMAS capability, iDRAC racadm proxy feature can redirect CMC racadm commands to CMC via iDRAC. With the proxy feature, CMC configuration and inventory can be accomplished without placing CMC on the network.

Requires

- Racadm tool version 8.1 or later
- CMC firmware version 1.20 or later
- iDRAC firmware version 2.10.10 or later

The proxy feature works with local and remote racadm only. Local racadm is racadm that is run from the host OS and targets the host iDRAC. Remote racadm is racadm that is run from any host OS and targets a remote (requires IP address) iDRAC. It does not work with firmware racadm, one that runs via ssh to iDRAC or CMC.

The CMC racadm commands that you can run with the proxy feature depends on the CMAS setting. If the setting is disabled, then the proxy commands will not work. If the setting is Monitor only, then you can only send monitoring CMC commands. If the setting is Manage and Monitor, then you can send monitoring and configuration CMC commands.

Note: The "--proxy" option must be the last item in the command line.

Example command to get CMC sensor information using local racadm:

```
# racadm getsensorinfo --proxy
```

Example command to get CMC sensor information using remote racadm:

```
# racadm -r 192.168.1.150 -u root -p XXX getsensorinfo --proxy
```

Example command to set the power redundancy policy of the chassis using local racadm:

```
# racadm config -g cfgChassisPower -o cfgChassisRedundancyPolicy 1 --proxy
```

Example command to set the configuration mode of the storage sled in slot 4 to single-split host using remote racadm:

```
# racadm -r 192.168.1.150 -u root -p XXX config -g cfgStorageModule -m
storage-4 -o cfgStorageModuleStorageMode 2 --proxy
```

If the minimum software requirement is not met, the proxy option has no effect on the racadm command. In other words, the command is processed by iDRAC.

If CMC is not connected to the network, the import, export and file operation commands that require access to network shares such as TFTP will not work.

The credential provided to the racadm tool must be the iDRAC credential. The privileges associated with the iDRAC credential is mapped to CMC privilege when forwarding the command to CMC. For example, if a CMC command requires Chassis Control Administrator and Server Administrator privileges, then the user running the racadm proxy request need to have the System Control privilege.

The mapping of privileges are as follows:

iDRAC privilege	Maps to CMC privilege
Login	CMC Login User
Configure	Chassis Configuration Administrator
Configure User	User Configuration Administrator
Logs	Clear Logs Administrator
System Control	Chassis Control Administrator
System Control	Server Administrator
System Operations	Test Alert User
Debug	Debug Command Administrator
System Control	Fabric Administrator

A Appendix

A.1 Glossary

Term	Description
CMAS	Chassis management at server – the feature that allows chassis management from iDRAC.
CMC	Chassis management controller – out-of-band systems management of PowerEdge chassis.
iDRAC	Integrated Dell remote accesss controller – out-of-band systems management of PowerEdge server.
IPMI	Intelligent platform management interface – standard specification for management and monitoring of computer systems.
racadm	Command line tool for iDRAC and CMC.
sled	A container that is inserted into a modular server chassis. A compute sled contains a server, also called a blade.
WSMAN	Web services for management – standard specification for management and monitoring of computer systems. See http://www.dmtf.org/standards/wsman

A.2 Troubleshooting

Symptom	Recommendation
You see the error in iDRAC: "*RAC0709: Unable to retrieve the fan information. Power on the server. If the server is already powered on, wait for a few minutes and refresh the page...*"	In addition to what is already suggested in the message, check if the Chassis Management at Server setting is configured in CMC and in iDRAC (See Section 2).
You see the error while updating CMC firmware in the host OS: "*The shared components could not be updated through operating system because CMC and/or iDRAC is not configured to enable this behavior...*"	Check if the Chassis Management at Server setting is configured in CMC and in iDRAC (See Section 2).

A.3 Additional resources

Support.dell.com is focused on meeting your needs with proven services and support.

DellTechCenter.com is an IT Community where you can connect with Dell Customers and Dell employees for the purpose of sharing knowledge, best practices, and information about Dell products and installations.

Referenced or recommended Dell publications:

- Learn more about PowerEdge FX2 chassis and its components
  See Manuals and Documentation for your PowerEdge FX2/FX2s
- Get an overview of the Dell Systems Management offerings
  Dell OpenManage Systems Management Overview Guide at dell.com/openmanagemanuals
- Learn more about Systems Management solution for managing the PowerEdge chassis
  Chassis Management Controller at dell.com/esmmanual
- Learn more about Systems Management solution for managing the PowerEdge servers
  Remote Access Controller at dell.com/esmmanual
- Know about the RACADM subcommands and supported RACADM interfaces
  RACADM Command Line Reference Guide for iDRAC and CMC at dell.com/esmmanual