Dell Power Edge M1000e Chassis Management Controller Version 4.5 - Single Sign-On and Kerberos Model

This technical brief highlights the working of Single Sign-On and Kerberos Authentication Model in CMC 4.5

Dell Engineering
January 2014

Author

Yogeshwar Bisht

A Dell Technical White Paper

Revisions

Date	Description
January 2014	Initial Release

THIS WHITE PAPER IS FOR INFORMATIONAL PURPOSES ONLY, AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND.

PRODUCT WARRANTIES APPLICABLE TO THE DELL PRODUCTS DESCRIBED IN THIS DOCUMENT MAY BE FOUND AT: http://www.dell.com/learn/us/en/19/terms-of-sale-commercial-and-public-sector Performance of network reference architectures discussed in this document may vary with differing deployment conditions, network loads, and the like. Third party products may be included in reference architectures for the convenience of the reader. Inclusion of such third party products does not necessarily constitute Dell's recommendation of those products. Please consult your Dell representative for additional information.

Trademarks used in this text:

Dell™, the Dell logo, Dell Boomi™, Dell Precision™ ,OptiPlex™, Latitude™, PowerEdge™, PowerVault™, PowerConnect™, OpenManage™, EqualLogic™, Compellent™, KACE™, FlexAddress™, Force10™ and Vostro™ are trademarks of Dell Inc. Other Dell trademarks may be used in this document. Cisco Nexus®, Cisco MDS®, Cisco NX-0S®, and other Cisco Catalyst® are registered trademarks of Cisco System Inc. EMC VNX®, and EMC Unisphere® are registered trademarks of EMC Corporation. Intel®, Pentium®, Xeon®, Core® and Celeron® are registered trademarks of Intel Corporation in the U.S. and other countries. AMD® is a registered trademark and AMD Opteron™, AMD Phenom™ and AMD Sempron™ are trademarks of Advanced Micro Devices, Inc. Microsoft®, Windows®, Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista® and Active Directory® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Red Hat® and Red Hat® Enterprise Linux® are registered trademarks of Red Hat, Inc. in the United States and/or other countries. Novell® and SUSE® are registered trademarks of Novell Inc. in the United States and other countries. Oracle® is a registered trademark of Oracle Corporation and/or its affiliates. Citrix®, Xen®, XenServer® and XenMotion® are either registered trademarks or

Table of contents

Revisions 2

Executive summary 5

Background 5

About Single Sign-On 5

1. Kerberos Model 6

2. Kerberos Workflow 7

3. Pre-requisites for Kerberos Authentication 10

Network Pre-requisites 10

CMC Pre-requisites 11

4. Configuring CMC for SSO 11

5. References 17

Executive summary

This document explains the following:

- Working of Single Sign-On(SSO) using Kerberos, a network authentication protocol
- Kerberos security mechanism
- Configuring the Dell Chassis Management Controller for SSO.

The Dell Chassis Management Controller uses Kerberos to support single-sign on and Active directory account credentials to log in.

Background

It all started in early 1990, when some organizations moved to a combination of some authentication protocols, commonly known as Enterprise SSO (ESSO). These protocols later developed to more advanced browser-based plugin, Web Access Management (WAM).

Some protocols like Kerberos contain SSO features. However, the emphasis was to integrate applications within the network perimeter only. Later, SSO was alligned to cloud based services also including Software as a Service (SaaS).

In 2012, SSO technologies were developed to accommodate enterprises of all sizes, This was mainly due to **Security Assertion Markup Language 2.0 (**SAML) protocol, which became an **Organization for the Advancement of Structured Information Standards (**OASIS) standard in 2005. The Simple Cloud Identity Management (SCIM) is the latest protocol available. This defines a simple, RESTful protocol for identity account management operations.

About Single Sign-On

Single sign-on is an authentication process that allows network users to access all authorized network resources without having to log in separately to each resource. Single sign-on allows the user to validate usernames and passwords against the corporate user database or other client application rather than having separate user names and passwords.

The idea of today's SSO is simple. The process authenticates the user for all the applications they have been given rights to. This eliminates further prompts when they switch applications during a particular session., There are various types of SSO. However, the preferred architecture is for a user to authenticate to a centrally managed system, and for applications to trust that central system for identity information about the user rather than re-authenticating.

1. Kerberos Model

Operating systems such as Windows (2000 and above), Windows server (2003 and above) use Kerberos as an authentication protocol, allowing users who signed into the domain to access Chassis Management Controller (CMC) auomatically. This means, users can access CMC without entering user name and password in a secure way.

Kerberos model is based on three pillars:

- **Key Distribution Center (KDC)**: A trusted third party and a domain service, which uses Active Directory to access user accounts. KDC basically provides two services.
  - **Authentication Service (AS)**: Issues Ticket Granting Ticket to access Ticket Granting Service.
  - **Ticket-Granting Service (TGS)**: Issues tickets for connection to computers in its domain.
- **Account Database**: Active directory is a source of account database that KDC uses to access user information.
- **Kerberos Policy**: It is defined at the domain and is implemented by the domain's KDC and is stored in Active Directory

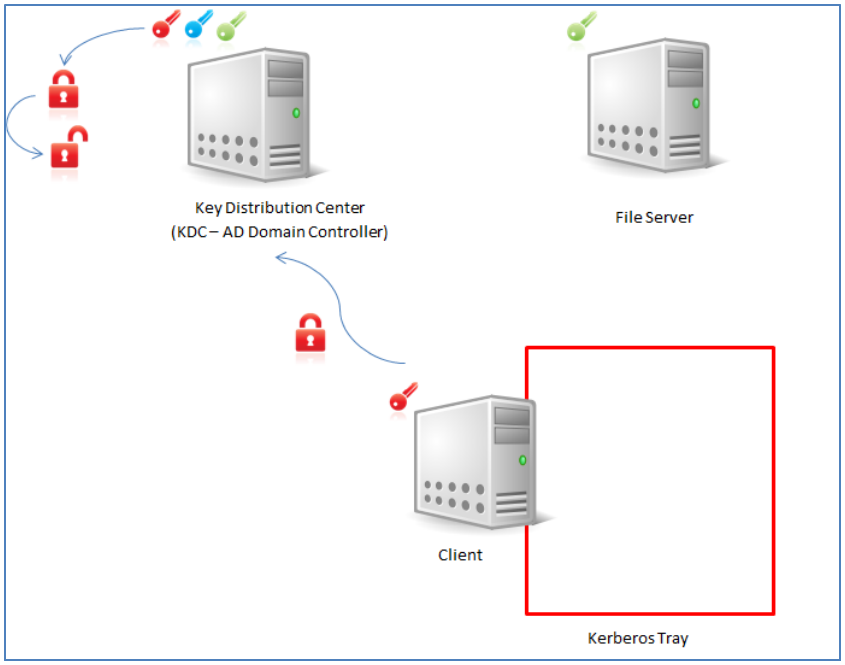
All traditional protocols, such as **Internet message access protocol** (IMAP), **Simple Mail Transfer Protocol** (SMTP), and so on, support Kerberos

Note: There is no communication between the Key Distribution Center (KDC) and server throughout the process.

2. Kerberos Workflow

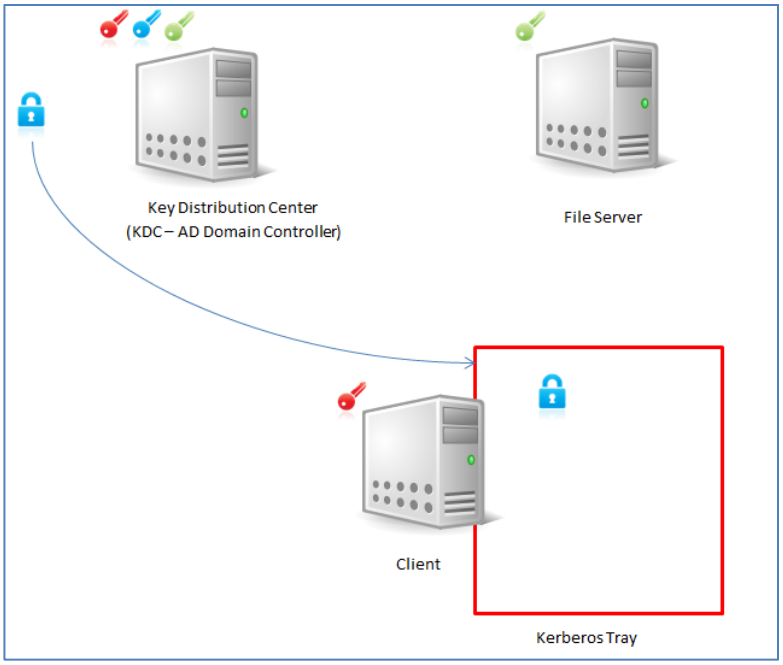
The following section describes how Kerberos functions.

1. Creating the Aunthenticator



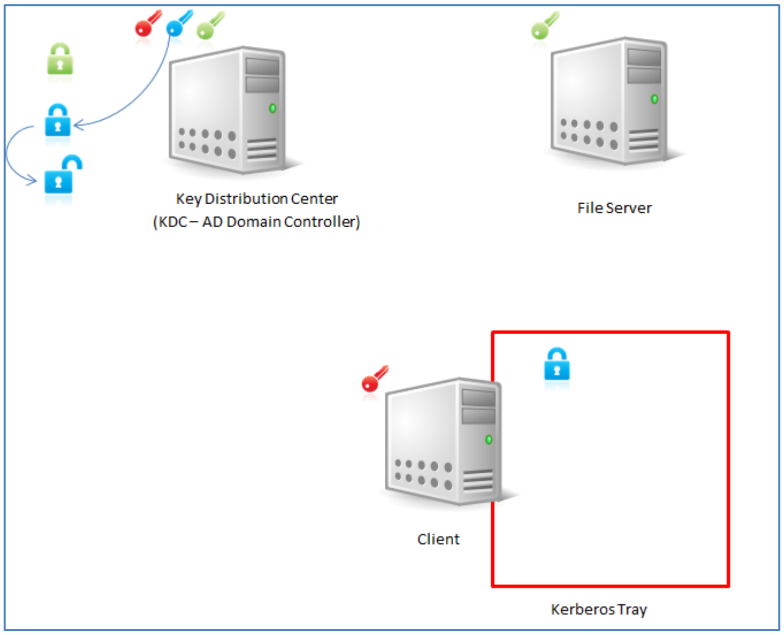
- The Client creates an authenticator (red lock), and a portion of which is not encrypted, for example the Username. This enables the domain controller to find out who is trying to authenticate. The other portion of the aunthenticator is encrypted using User's password (red key).
- KDC first searches for the user in its database. If it finds the user, then KDC opens the authenticator using the key, for example the password, which it holds for the user. In case KDC does not find the user, then it means the user is not authentic. After this authentication is done, the user need not enter the password again.

2. Generating the Ticket Granting Ticket



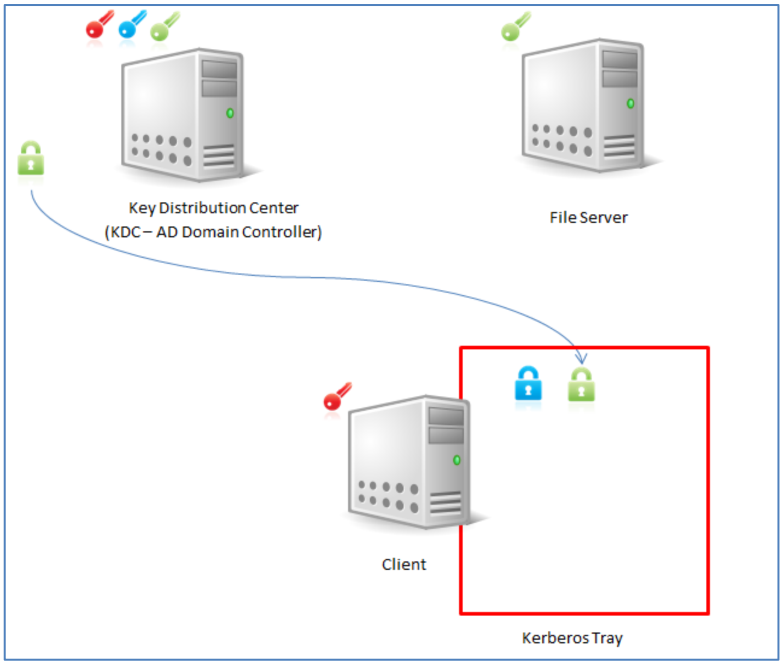
KDC generates an encrypted Ticket granting ticket (TGT). This TGT can be decrypted by KDC only. KDC sends the TGT to the Client where it is saved in the Kerberos tray (special area of memory in the Client that is not persistent).

3. Accessing File from Server



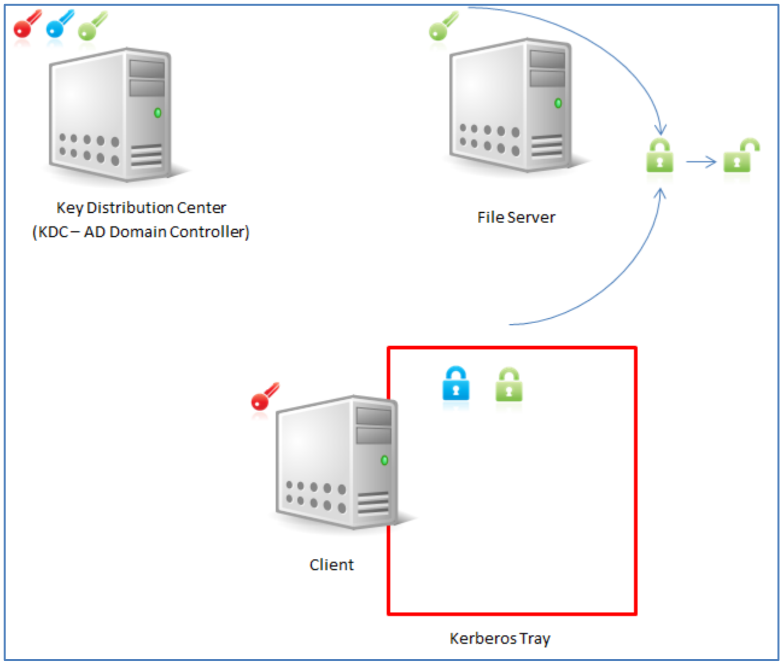
To access a file from file server, the Client needs a ticket for a file server. The Client sends the TGT, which is present in the Kerberos tray to KDC requesting a ticket for a file server.

4. Decrypting Ticket Granting Ticket on KDC



- After KDC receives the TGT from the client, it does not validate the user this time. KDC uses its key to decrypt the TGT. The key expires after 8 hours.
- KDC generates a ticket for file server. The file server is also in the same domain, hence KDC has its login password and it creates a ticket using login password as encryption key. This encrypted key is sent to the client which stores it in a Kerberos tray.

5. Decrypting Ticket Granting Ticket on the File Server



- ❖ Client sends a copy of the TGT to the file Server to gain access to the files. The Server holds a key to decrypt the ticket.
  Note: For each access request, the Client must send a fresh copy of the TGT to get access to the files. The Server does not maintain any TGT for the client in its memory.

3. Pre-requisites for Kerberos Authentication

Network Pre-requisites

- DNS server
- Microsoft Active Directory Server
- Kerberos Key Distribution Center (packaged with the Active Directory Server software)
- DHCP server
- The DNS server reverse zone must have an entry for the Active Directory server and CMC

CMC Pre-requisites

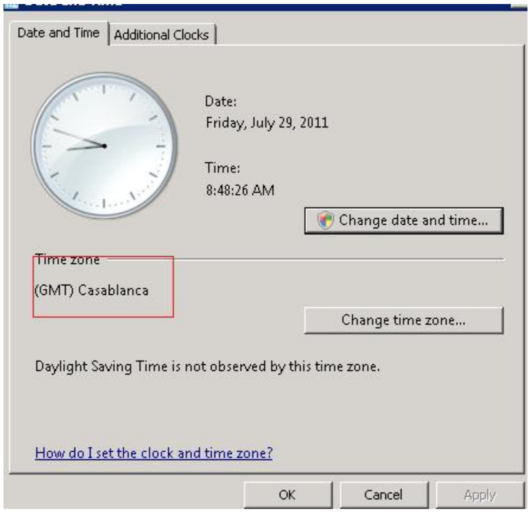
- The CMC must have firmware version 2.10 or later
- Each CMC user must have an Active Directory account
- The CMC must be a part of the Active Directory domain and Kerberos Realm

4. Configuring CMC for SSO

Configure CMC for the following SSO settings:

1. Date & Time Settings (system clock)

Set the same Date and Time for the AD Server and CMC. The permissible limit for variation is +1 or -1 minute.



Date:
Friday, July 29, 2011

Time:
8:48:26 AM

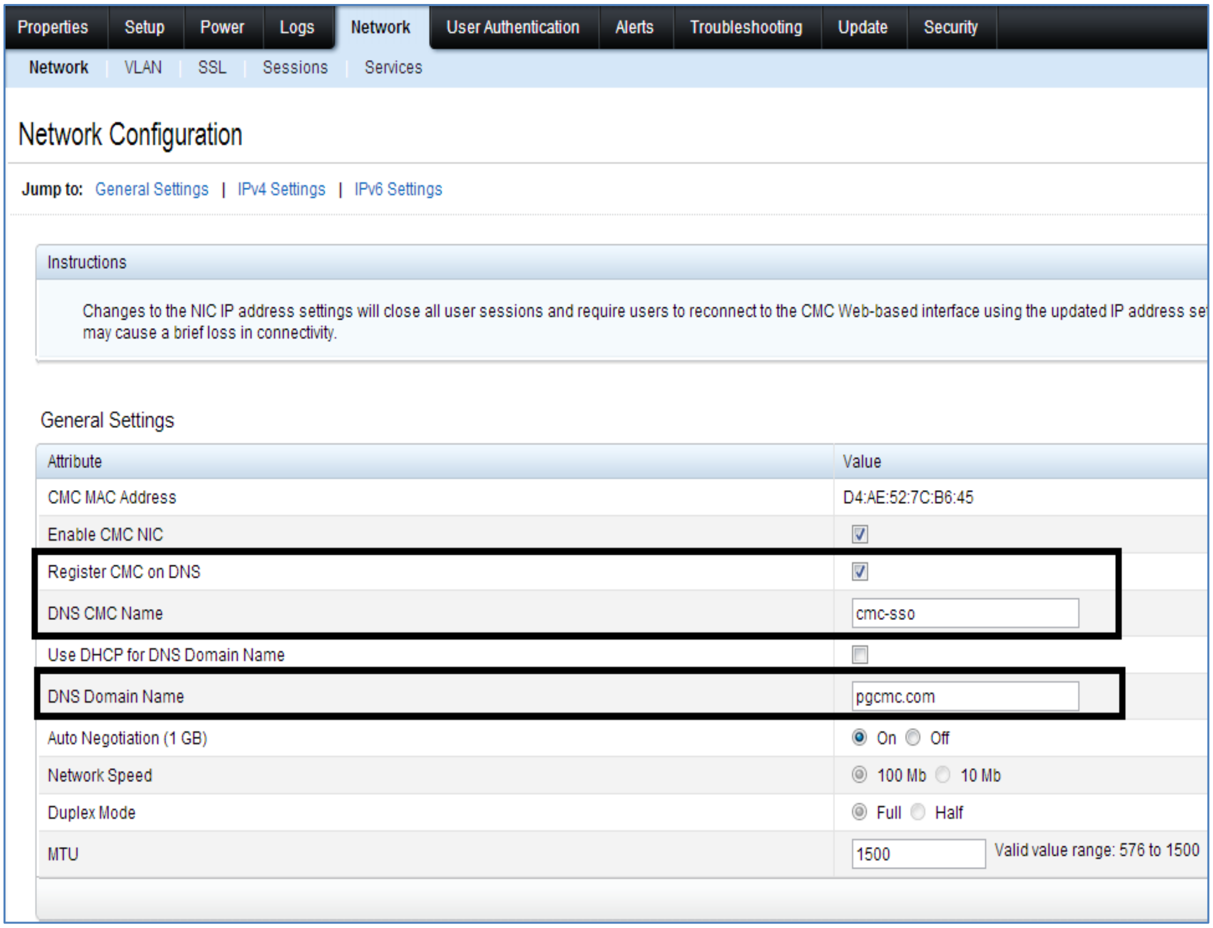
Time zone
(GMT) Casablanca

Daylight Saving Time is not observed by this time zone.

2. DNS Register Settings

Configure the DNS Register settings using the CMC Web interface:

a. In the CMC Web interface, from the system tree, click **Chassis Overview.**
b. Click **Network** → **Network.** The Network Configuration page is displayed.
c. In the **General Chassis Settings** section, select the **Register CMC on DNS** option.
d. Provide the **DNS CMC Name.**
e. Provide the **DNS Domain Name** of the server. For example, **pgcmc.com.**
f. In the IPV4 Settings section, provide the **Static Preferred DNS Server** and **Static Alternate DNS Server details.**



Network Configuration

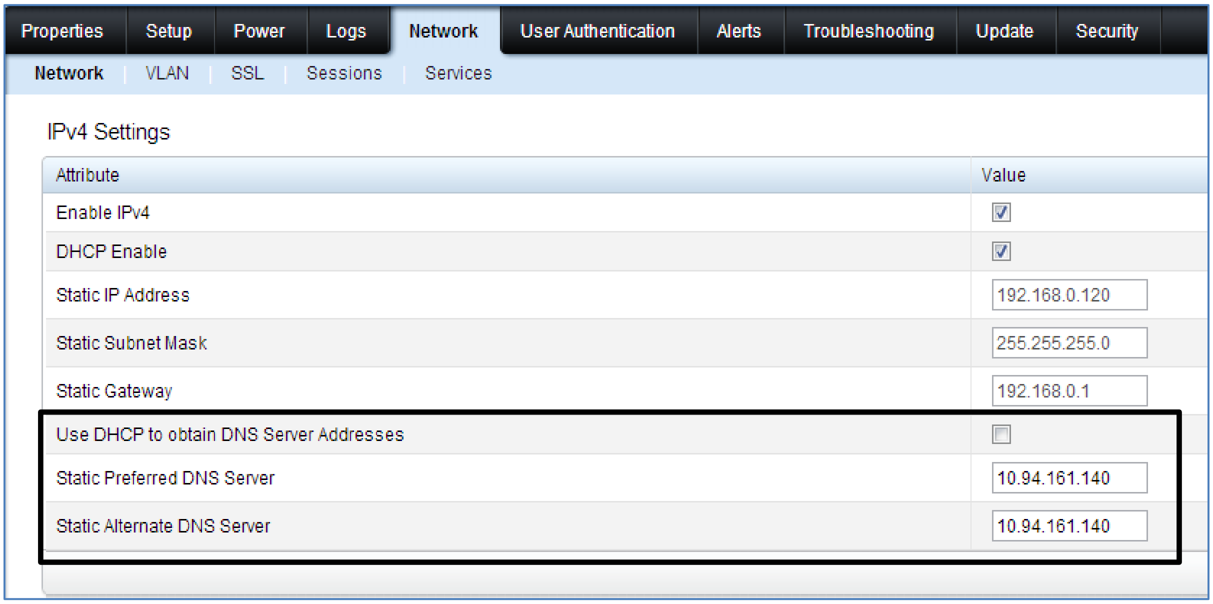
Jump to: General Settings | IPv4 Settings | IPv6 Settings

Instructions

Changes to the NIC IP address settings will close all user sessions and require users to reconnect to the CMC Web-based interface using the updated IP address se
may cause a brief loss in connectivity.

General Settings

Attribute	Value
CMC MAC Address	D4:AE:52:7C:B6:45
Enable CMC NIC	☑
Register CMC on DNS	☑
DNS CMC Name	cmc-sso
Use DHCP for DNS Domain Name	□
DNS Domain Name	pgcmc.com
Auto Negotiation (1 GB)	● On ○ Off
Network Speed	● 100 Mb ○ 10 Mb
Duplex Mode	● Full ○ Half
MTU	1500 Valid value range: 576 to 1500



IPv4 Settings

Attribute	Value
Enable IPv4	☑
DHCP Enable	☑
Static IP Address	192.168.0.120
Static Subnet Mask	255.255.255.0
Static Gateway	192.168.0.1
Use DHCP to obtain DNS Server Addresses	□
Static Preferred DNS Server	10.94.161.140
Static Alternate DNS Server	10.94.161.140

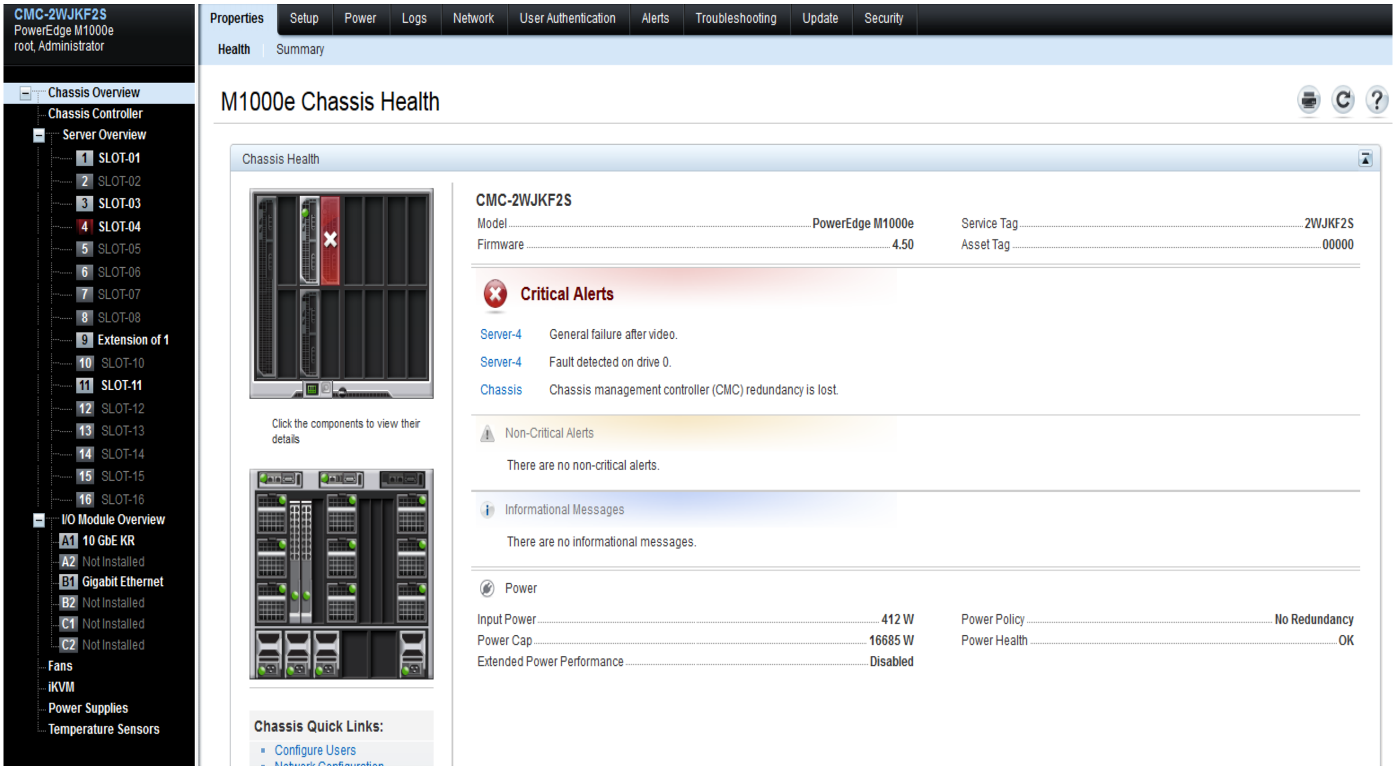
3. To select the schema

a. Click **Chassis Overview → User Authentication → Directory Services**. The **Directory Services** page is displayed.

b. Select **Microsoft Active Directory (Standard Schema)** for the type of Directory service.

c. In the Common Setting section, select **Enable Active Directory, Enable Single Sign-on and Certificate Validation Enabled** options**.**

d. In the **Root Domain Name** field, provide the Domain name registered in AD and IP of the Domain controller.



M1000e Chassis Health

CMC-2WJKF2S

Model PowerEdge M1000e
Firmware 4.50
Service Tag 2WJKF2S
Asset Tag 00000

Critical Alerts

Server-4 General failure after video.
Server-4 Fault detected on drive 0.
Chassis Chassis management controller (CMC) redundancy is lost.

Non-Critical Alerts

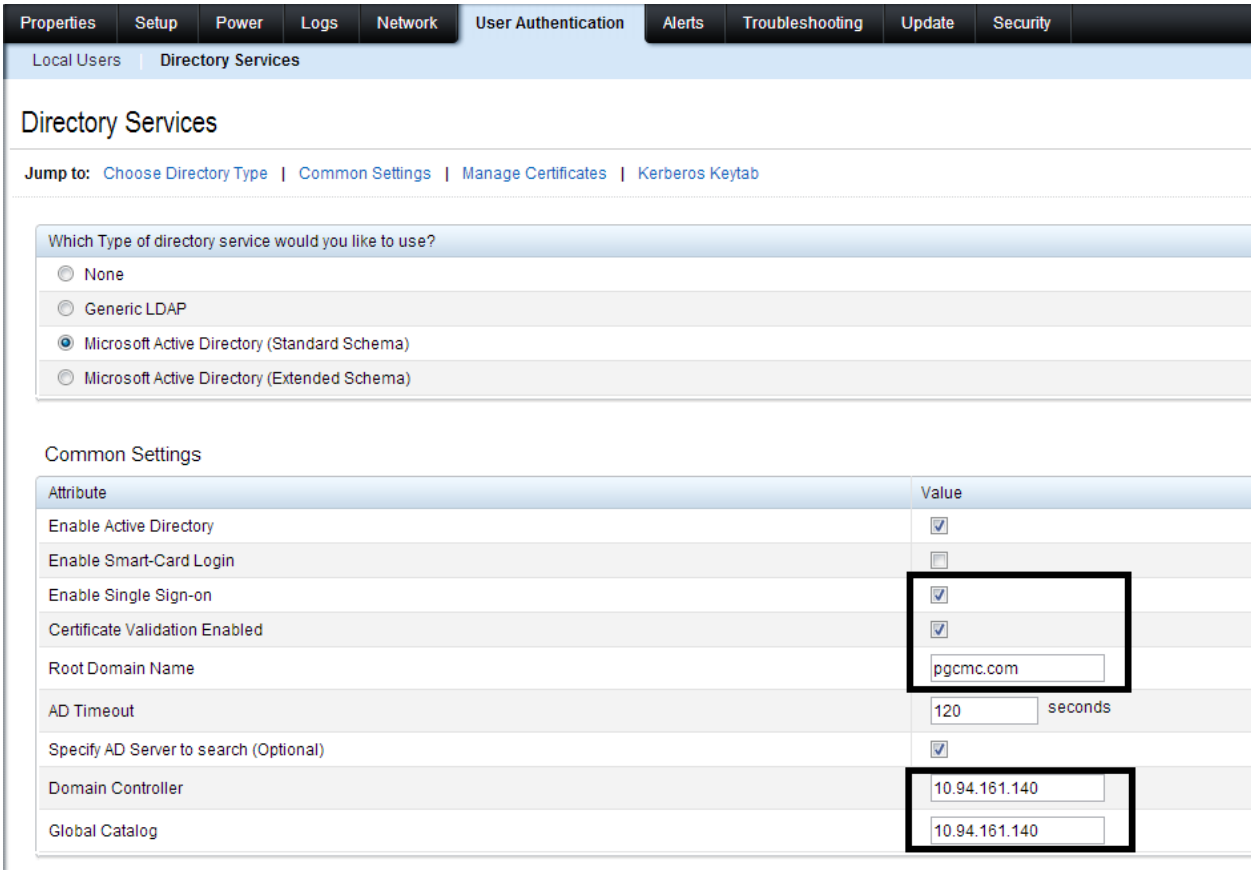
There are no non-critical alerts.

Informational Messages

There are no informational messages.

Power

Input Power 412 W
Power Cap 16685 W
Extended Power Performance Disabled
Power Policy No Redundancy
Power Health OK



Directory Services

Jump to: Choose Directory Type | Common Settings | Manage Certificates | Kerberos Keytab

Which Type of directory service would you like to use?

- ○ None
- ○ Generic LDAP
- ● Microsoft Active Directory (Standard Schema)
- ○ Microsoft Active Directory (Extended Schema)

Common Settings

Attribute	Value
Enable Active Directory	☑
Enable Smart-Card Login	□
Enable Single Sign-on	☑
Certificate Validation Enabled	☑
Root Domain Name	pgcmc.com
AD Timeout	120 seconds
Specify AD Server to search (Optional)	☑
Domain Controller	10.94.161.140
Global Catalog	10.94.161.140

4. Standard Schema Settings

To set the standard schema settings:

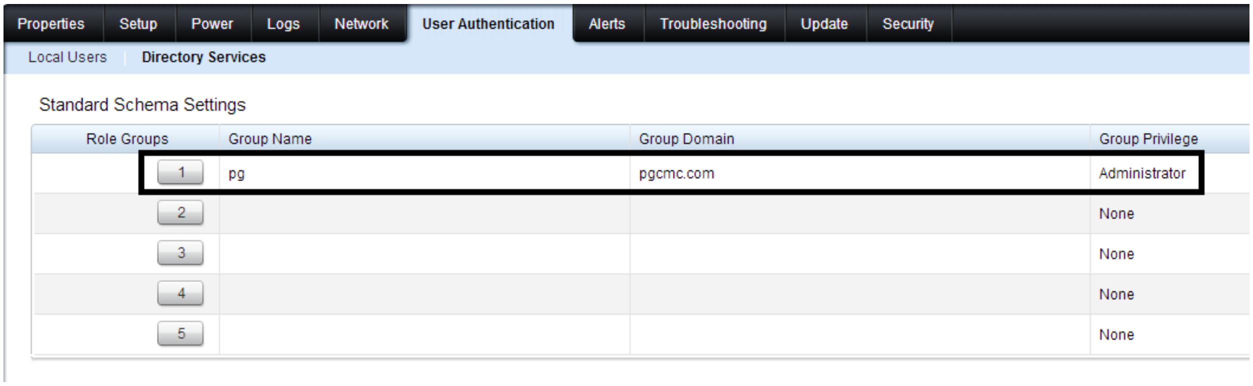
a. In the Standard Schema Settings section, create a group under the same Domain, for example pgcmc.com.

b. Click the numbered buttons under **Role Groups**, for example button 1.

A new page, **Configure Role Group 1** is displayed.

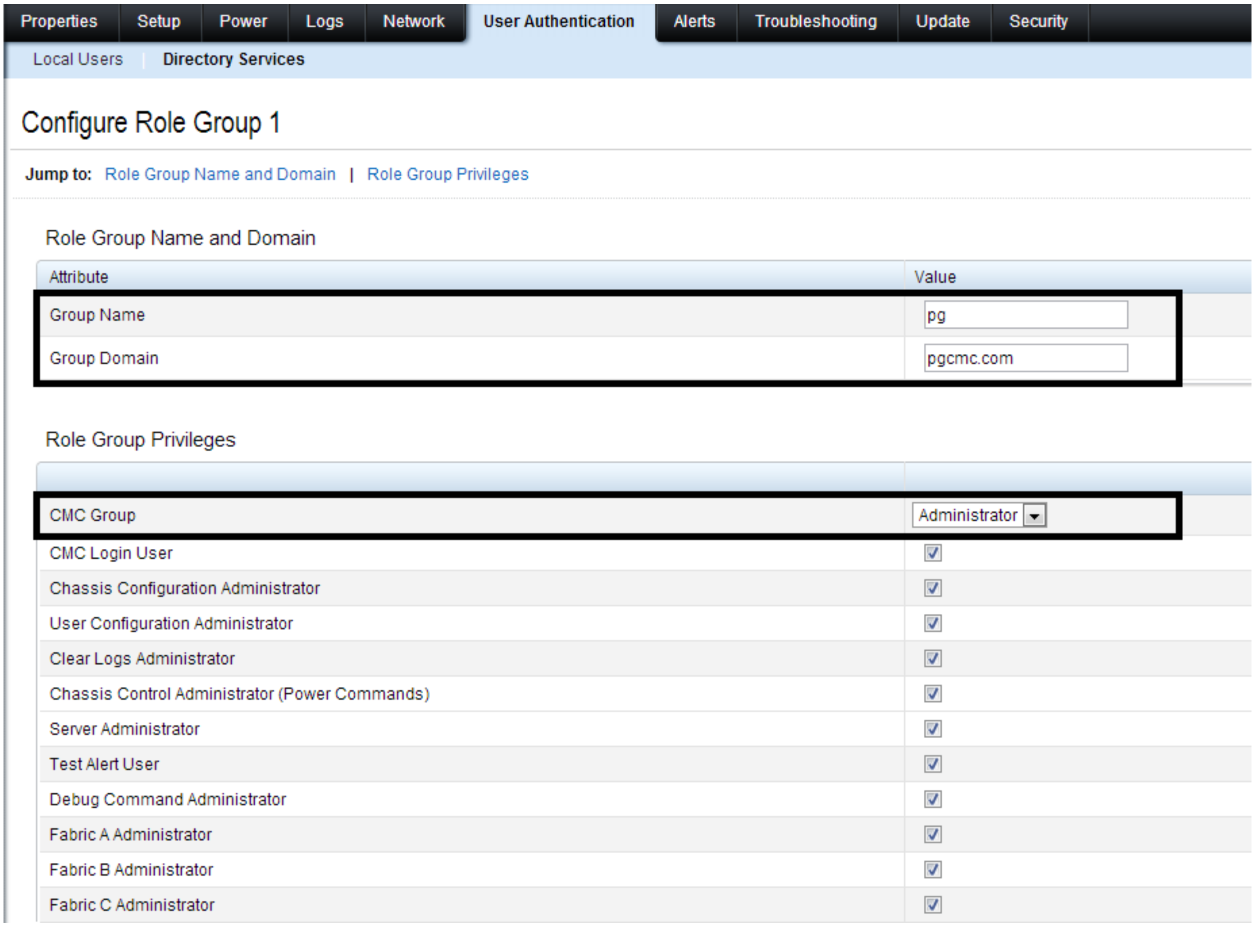
c. Provide the **Group Name** and **Group Domain**.

d. Under Role **Group Privileges**, select the required privilege.



Standard Schema Settings

Role Groups	Group Name	Group Domain	Group Privilege
1	pg	pgcmc.com	Administrator
2			None
3			None
4			None
5			None



Configure Role Group 1

Jump to: Role Group Name and Domain | Role Group Privileges

Role Group Name and Domain

Attribute	Value
Group Name	pg
Group Domain	pgcmc.com

Role Group Privileges

CMC Group	Administrator
CMC Login User	☑
Chassis Configuration Administrator	☑
User Configuration Administrator	☑
Clear Logs Administrator	☑
Chassis Control Administrator (Power Commands)	☑
Server Administrator	☑
Test Alert User	☑
Debug Command Administrator	☑
Fabric A Administrator	☑
Fabric B Administrator	☑
Fabric C Administrator	☑

5. Upload Kerberos keytab

a. Create a Kerberos keytab using ktpass:

```
For example,  ktpass –princ  HTTP/cmc-sso.pgcmc.com@PGCMC.COM -mapuser cmckerb -
crypto DES-CBC-MD5 -ptype KRB5_NT_PRINCIPAL -pass XXXX –out  c:\cmcssokerb
```

In this command

cmc-sso : DNS CMC Name (refer : Network -> Network -> General Settings)

pgcmc.com: DNS Domain Name (refer : Network -> Network -> General Settings)

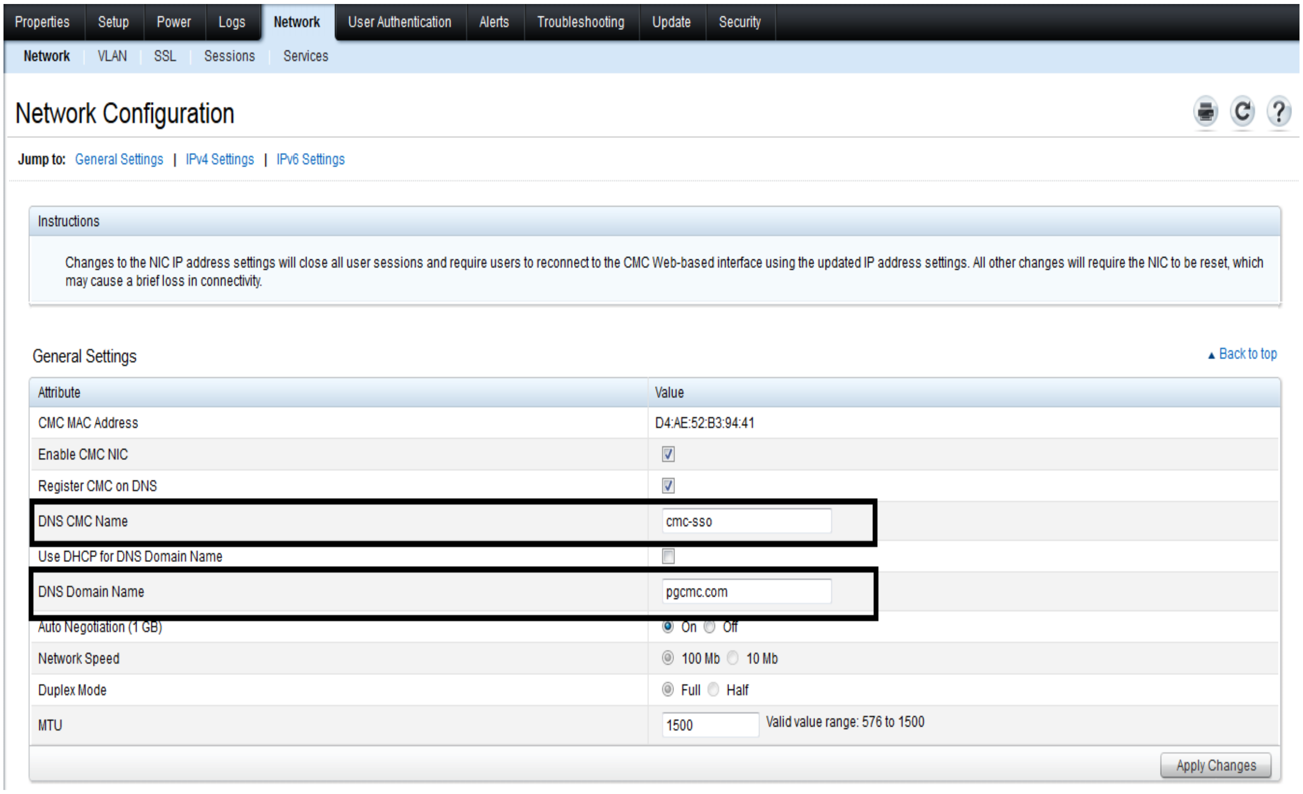
The Ktpass utility creates Kerberos keytab files that are used by UNIX Kerberos-based systems to define KDC hosts and user/service mappings.

The syntax for the command is:

```
ktpass /out filename /princ username [/mapuser] [/in filename] [/crpyto type]
[/ptype type] [/keyno keynum] [/?]
```

Switch usage:

- /out filename - Specifies the name of the keytable file to be generated.
- /princ principal_name - The principal name.
- /pass password - Password to use for this principal name.
- /mapuser username - Map the name of a Kerberos principal to a local account.
- /mapOp [add|set] - Defines how the mapping attribute is set. The default is to add.
- /DesOnly - Set the account for DES-only encryption.
- /in filename - The name of an existing keytab file to be used as the basis for the new keytab file.
- /crypto [DES-CBC-CRC|DES-CBC-MD5] - Specify the encryption type to use (DES-CBC-CRC is the default).
- /ptype ptype - Sets the principal type:
  KRB5_NT_PRINCIPAL: The name of the principal or for users
  KRB5_NT_SRV_INST: User service instance
  KRB5_NT_SRV_HST: Host service instance
- /kvno number - The key version number (the default is 1).
- /? - Shows the usage screen.



Network Configuration

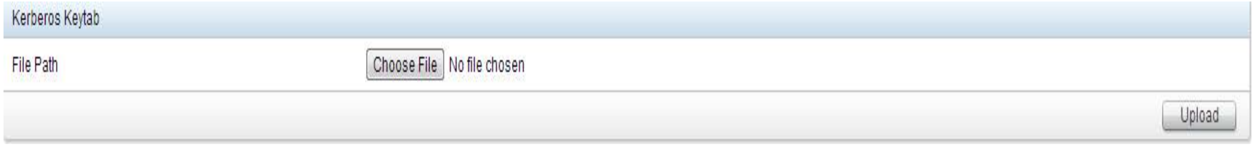
Instructions

Changes to the NIC IP address settings will close all user sessions and require users to reconnect to the CMC Web-based interface using the updated IP address settings. All other changes will require the NIC to be reset, which may cause a brief loss in connectivity.

General Settings

Attribute	Value
CMC MAC Address	D4:AE:52:B3:94:41
Enable CMC NIC	☑
Register CMC on DNS	☑
DNS CMC Name	cmc-sso
Use DHCP for DNS Domain Name	□
DNS Domain Name	pgcmc.com
Auto Negotiation (1 GB)	● On ○ Off
Network Speed	● 100 Mb ○ 10 Mb
Duplex Mode	● Full ○ Half
MTU	1500 Valid value range: 576 to 1500

b. Under **Kerberos Keytab** section, click **Choose File** to select the file and click **Upload**.



Kerberos Keytab

File Path No file chosen

5. References

For browser settings related information on Dell Chassis Management Controller version 4.5, see *Dell Chassis Management Controller Version 4.5 User's Guide* on Dell.com.
For additional info on CMC, see Chassis Management Controllers on Dell.com.

Also to know about Active Directory interaction with Chassis Management Controller please see the whitepaper The Theory and Operation of the Dell Chassis Management Controller (CMC) with Microsoft Active Directory.