



Cisco C880 M4 Server with SAP HANA Tailored Datacenter Integration

Design and Deploy a SAP HANA Single-Node Solution Based on Standalone Cisco UCS C460 M4 Rack Servers with SLES for SAP 12 SP1

February 2017

Contents

Prerequisites	4
Architecture Overview	5
Recommended Network Layout	5
Disk and File System Layout	7
Configuration Overview: SAN Environment	8
Configuration Overview: NAS Environment	9
Physical Components of the Cisco C880 M4 Server	11
Cisco C880 M4 Server Configuration	13
Set Up the Cisco Integrated Management Controller	13
Connect to the Management Board	13
Set the Integrated Management Controller IP Address	14
Log in to the Web User Interface	15
Update the Firmware	16
Configure the System Intelligent Platform Management Interface	18
Configure BIOS Settings	21
C880M4 System Monitoring via SNMP	30
iSCSI Boot Configuration	36
Prepare for iSCSI Configuration	36
Configure iSCSI Boot	39
SAN Boot Configuration	56
Overview of Steps for Configuring the SAN Boot Environment	56
Notes on SAN Boot System Design	57
Notes on SAN Boot System Installation	57
Configure the SAN Boot Environment	58
Notes on SAN Boot System Operation	71
16-Gbps Fibre Channel Card Settings: UEFI Driver Version 6.11a5 or Later	72
Set UEFI Driver Version 6.11a5 or Later on the 16-Gbps Fibre Channel Card	72
Select the Method for Configuring the 16-Gbps Fibre Channel Card	73
Display the Device Manager	75
Start the HBA Setup Utility and Select the HBA	76
Acquire an HBA WWN	78
Initialize the HBA Settings	79
Enable the BIOS	80
Set the Link Speed and Topology	82
Set the Boot Device	87
Apply the Settings	96
Record the WWN Information of the Fibre Channel Port	98
16-Gbps Fibre Channel Card Settings: Traditional BIOS Driver Version 6.02x6 or Later	101
Configure the HBA Setup Utility	101
Enable the BIOS	103
Set the Link Speed and Topology	104
Set the Boot Device	110
Considerations for Linux Installation	118
Linux Server OS Installation	118
SAN Multipath Boot	118
Prepare for Linux Installation	118
Install the OS and Bundled Software	118
Install Emulex OneCommand Manager	119
Install the Multipath Driver	119
Restore the Multipath Connection	119
SLES 11 and 12 Installation: iSCSI	121

Post-Installation Configuration	123
Update the OS After the Installation.....	123
Verify the Driver Specification	123
Configure and Tune the OS	123
Bond Linux Ethernet Interfaces.....	124
VLAN Configuration	126
SSH Key Distribution	126
sysctl.conf	126
Network Time Protocol Configuration	128
SAP HANA Setup (Network File System).....	129
SAP HANA Setup (SAN)	130
mkfs.xfs.....	130
/etc/fstab	130
/etc/after.local.....	130
SAP HANA Installation	131
SAP Notes	131
Linux Notes	131
SAP Application Notes	132
Notes About Third-Party Software	132
SAP HANA Virtualization Notes	132
SAP HANA High Availability (Scale-Out Only)	133
Configure High Availability	133
Enable the SAP HANA Storage Connector API	134
Test the IPMI Connectivity	134
Autostart SAP HANA	135
SAP HANA Failover Test (Scale-Out Only).....	136
SAP HANA Server Network Configuration	138
SAP HANA Hardware Configuration Check Tool Preparation	142
OS Validation	142
Storage Test	142
Example (user = <SID>adm)	145
For More Information.....	146

Prerequisites

The Cisco® solution for SAP HANA requires basic to expert understanding of various aspects of IT infrastructure. Familiarity with the following configuration and installation skills will help you build and troubleshoot this solution:

- Skills essential for building this solution
 - Cisco Nexus® Family installation and configuration
 - Cisco Unified Computing System™ (Cisco UCS®) Family installation and configuration
 - NetApp installation and configuration (optional)
 - EMC installation and configuration (optional)
 - installation and configuration
 - SUSE Linux Enterprise Server for SAP Applications 11 and 12 installation and configuration
 - Red Hat Enterprise Linux (RHEL) Server for SAP HANA 6.7 installation and configuration
- Skills highly recommended for installing the solution at the customer site
 - SAP HANA installation and configuration
 - Cisco Transport Gateway installation and configuration
 - Cisco Smart Call Home configuration on Cisco Nexus and Cisco UCS platforms
- Optional skills
 - SAP Landscape Transportation (SLT) Replication Server installation and configuration
 - SAP Business Suite configuration (focus on remote functions calls [RFCs] and interfaces)
- Additional useful skills
 - Cisco Catalyst® Family configuration
 - Configuration of Cisco Nexus 2000 Series Fabric Extenders and Cisco Nexus 3000, 5000, 7000, and 9000 Series Switches
 - Configuration of a Fibre Channel SAN switch that is compatible with the Cisco C880 M4 Server (ideally, a Cisco MDS 9000 Family switch)

If you find any procedures that do not work as documented here, please collect as much information as you can and open a case at support.cisco.com:

Product: Cisco C880 M4 Server

Project: CSC.datacenter

Solution: HANA-Solution

Component: Documentation

Architecture Overview

The main requirements for a SAP HANA solution are defined by SAP. The hardware partner has only limited possibilities for altering the infrastructure design.

SAP has defined the following requirements:

- Intel® Xeon® processor E7-8880 v3 CPU
- 512 GB per CPU socket for analytics (768 GB for SAP S4/HANA)
- 10 Gigabit Ethernet redundant storage connectivity to network-attached storage (NAS)
- 8-Gbps (or greater) Fibre Channel redundant storage connectivity to SAN
- 10 Gigabit Ethernet redundant SAP HANA connectivity between SAP HANA nodes
- 1 and 10 Gigabit Ethernet redundant uplink
- SUSE Linux Enterprise Server for SAP applications 11 SP3, 4, and 12 (soon SP1 as well)
- RHEL Server for SAP HANA 6.7 (soon 7.0 as well)

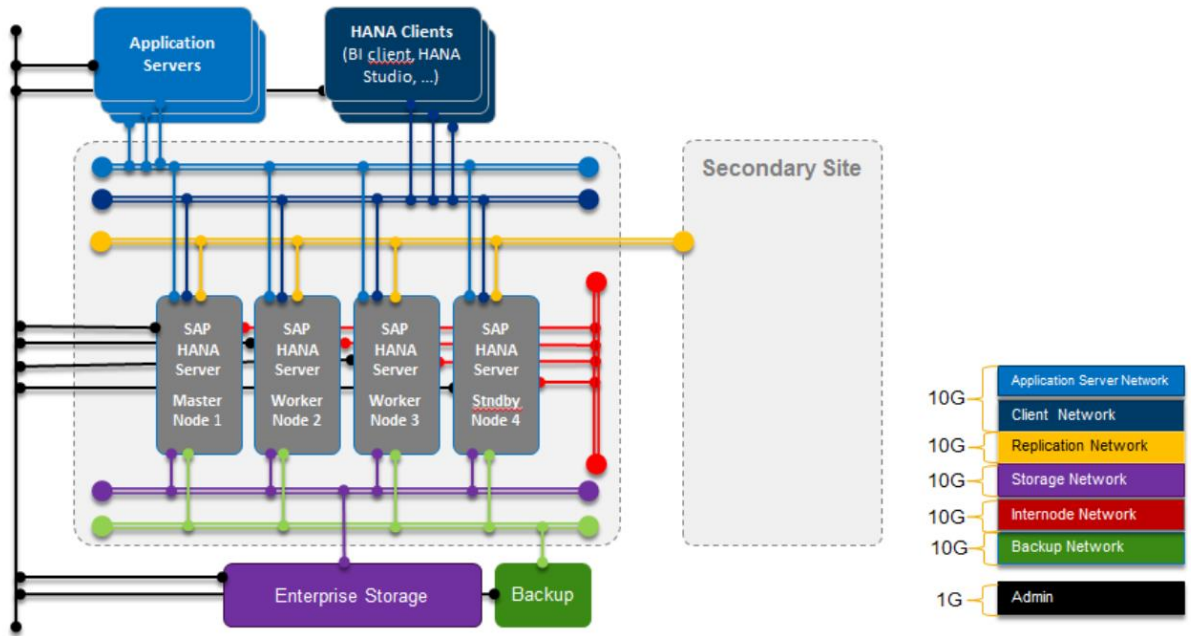
The architecture also includes the following components:

- Solution management components (optional)
 - Cisco 2911 Integrated Services Router (ISR; optional)
- Connectivity components (optional)
 - Cisco Nexus 2000 Series for Small Computer System Interface over IP (iSCSI) boot
 - Cisco Nexus 9000 Series for internal and external communication
 - Cisco MDS 9000 Family SAN connectivity
- Computing components
 - Cisco C880 M4 Server
 - 4 x 16-Gbps Fibre Channel
 - 8 x 10 Gigabit Ethernet
 - 4 x 1 Gigabit Ethernet
- Storage components
 - This document describes how to use existing customer storage to connect the Cisco C880 M4 to it.

Recommended Network Layout

Figure 1 shows a possible network configuration for an SAP Business Warehouse (BW) on SAP HANA system running on four hosts (one primary, two workers, and one standby) that are connected through an internode network (red). Two types of clients are attached: SAP BW application servers (light blue) and other SAP HANA clients (dark blue; for example, SAP HANA Studio). The data is persistently stored on enterprise storage (purple) and backed up to a separate storage location (green). To make this setup highly available, a standby host has been defined; moreover, the data is replicated to another data center using SAP HANA system replication (yellow). In addition, external administration tools can be used because a separate, low-bandwidth administrative network (black) is configured.

Figure 1. SAP HANA Network Layout



Source: SAP HANA TDI Network Guide ([SAP TDI Network Guide](#))

Disk and File System Layout

Rules from SAP and customer expectations determined the disk and file system layout. This layout must be implemented without any changes. Any change in the disk and file system layout will automatically invalidate certification, and SAP will deny any support. Neither local SAP consultants nor customers can change these rules. Please report any attempt to do so to the SAP HANA product management team.

```
/usr/sap/<SID>
```

Node-specific volume for storing local HANA information

```
/hana/shared/<SID>
```

Shared volume for storing the HANA executable files

```
/hana/data/<SID>/mnt00[001-999]
```

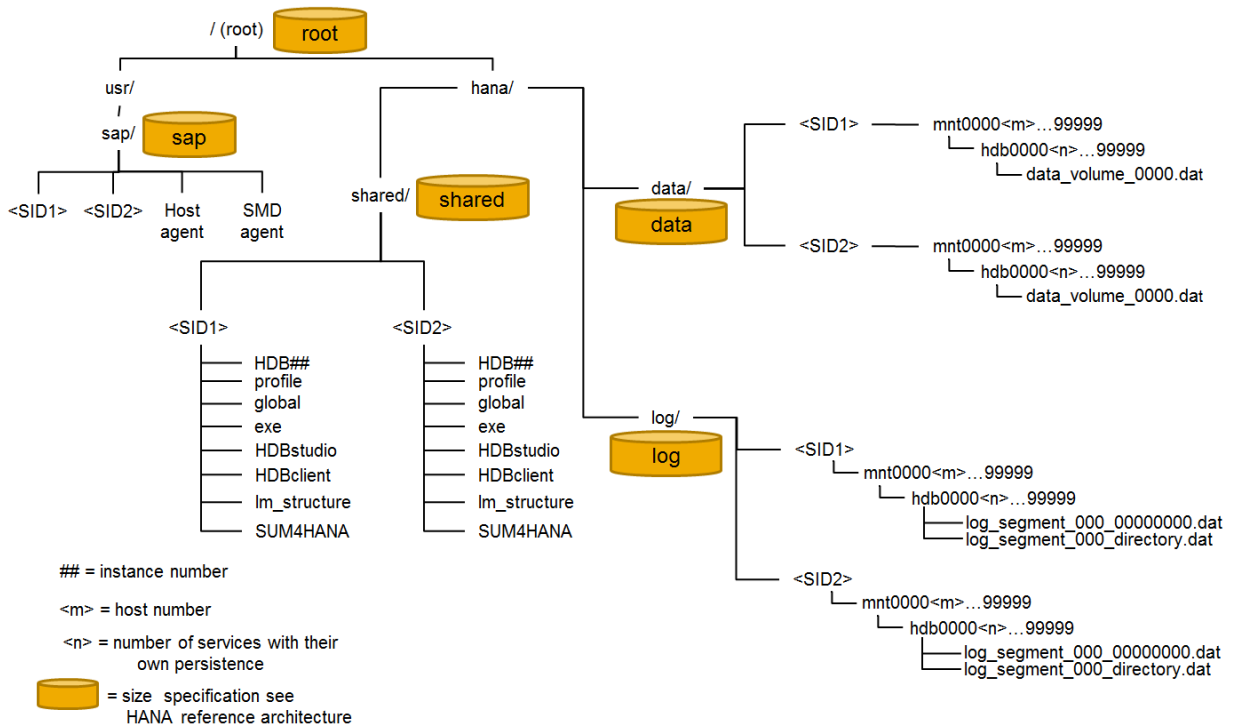
Data volumes

```
/hana/log/<SID>/mnt00[001-999]
```

Log volumes

Figure 2 shows the layout.

Figure 2. Disk and File System Layout

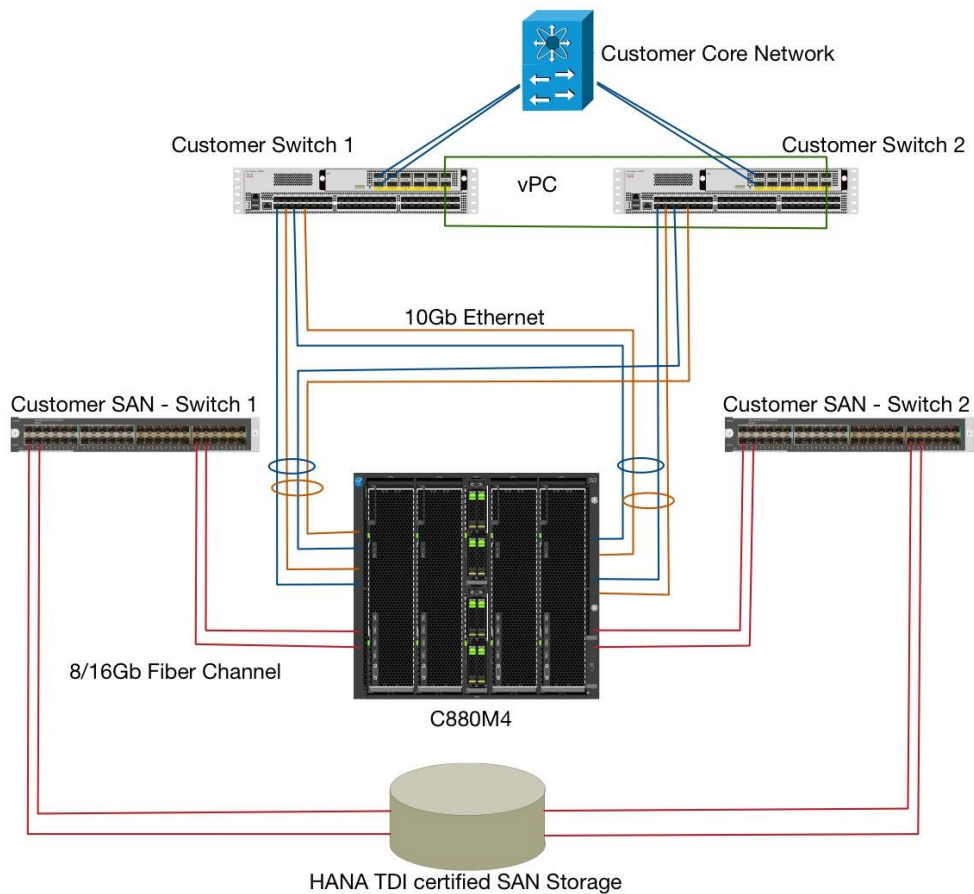


Configuration Overview: SAN Environment

Figure 3 shows how to connect the Cisco C880 M4 in a SAN environment. The base unit will be delivered with four 16-Gbps Fibre Channel interfaces, which can be used for OS SAN boot and for SAP HANA shared, data, and log volumes.

The network and SAN connectivity shown in this figure can be changed to meet customer requirements, but it must follow the SAP HANA Tailored Datacenter Integration (TDI) rules.

Figure 3. Sample SAN Configuration



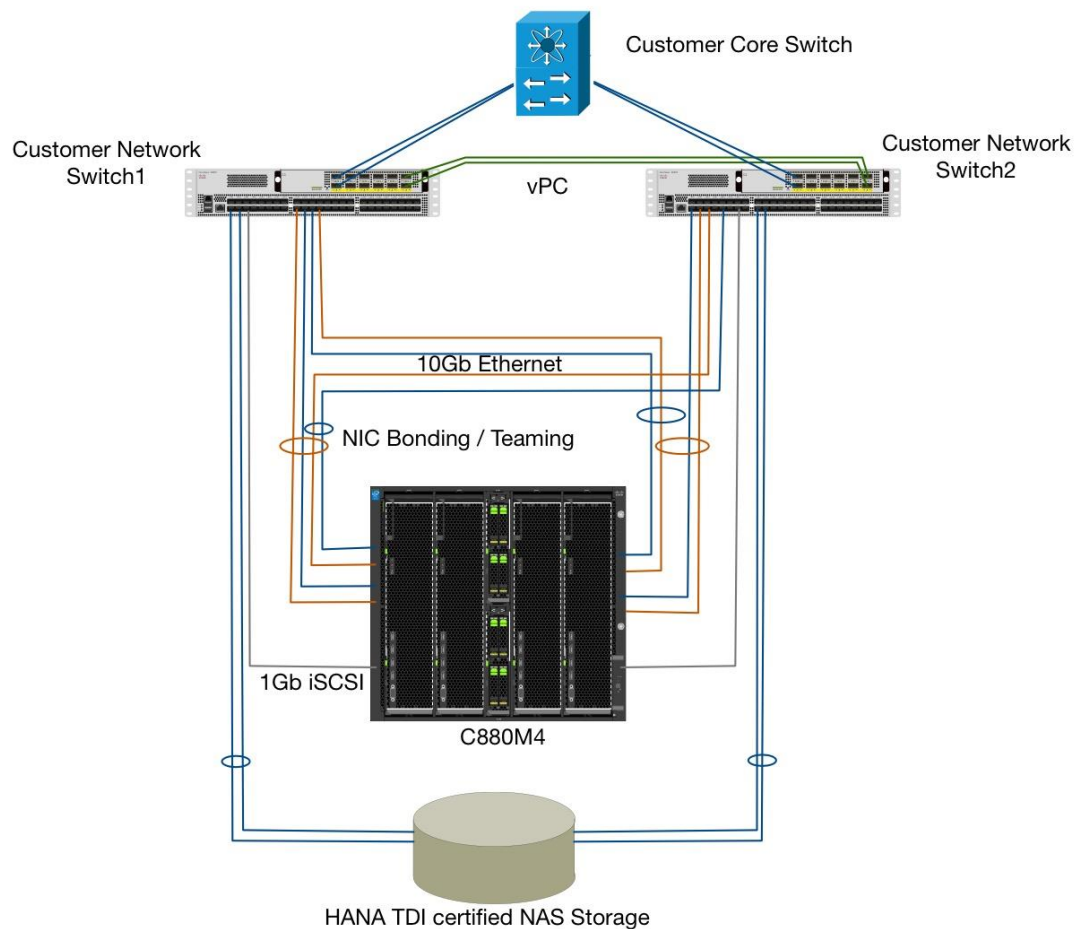
Configuration Overview: NAS Environment

Figure 4 shows how to connect the Cisco C880 M4 in an NAS environment. The base unit will be delivered with eight 10 Gigabit Ethernet interfaces, which can be used for SAP HANA shared, data, and log volumes.

The recommended approach is to use two of the four 1-Gbps Ethernet interfaces for iSCSI boot of the OS.

The network connectivity shown in this figure can be changed to meet customer requirements, but it must follow the SAP HANA TDI rules.

Figure 4. Sample NAS Configuration



SAP HANA TDI Versus SAP HANA Appliance

SAP HANA Tailored Datacenter Integration, or SAP HANA TDI, allows customers to use existing hardware and infrastructure components for their SAP HANA deployments.

Although SAP HANA TDI gives customers more flexibility, saving IT budget and existing investments, customers choosing this approach also have increased responsibility. With the SAP HANA TDI approach, only hardware is delivered. Finding a certified SAP HANA technician to install the SAP HANA software (including the Linux OS) is the customer's responsibility.

Customers choosing the SAP HANA TDI delivery model are also responsible for the OS provider's service contract and for end-solution validation, support, and security. Unlike the SAP HANA appliance approach, in which SAP and its hardware partners validate the solution and provide ongoing maintenance, with the TDI approach the customer is responsible for negotiating with all the OS and hardware partners to obtain individual agreements for solution maintenance and support.

Several tools and services are available for SAP HANA TDI customers to help with end-solution validation, go-live testing, and ongoing support:

- Hardware Configuration Check Tool for SAP HANA (documentation attached to SAP note 1943937) provides self-managed tests for customers to determine whether the hardware that they intend to use meets the minimum performance criteria required to run SAP HANA in a production environment.
- SAP provides go-live-checks and other support services for SAP HANA customers as part of the SAP support license (see SAP IT Planning for details).
- Cisco Advanced Service offers support to customers to set up an environment that meets all the SAP rules to successfully pass the Hardware Configuration Check Tool test and help ensure a successful project runtime environment.

Cisco Offering to Support SAP HANA TDI Customers

The Cisco Technical Assistance Center (TAC) offers a Cisco Solution Support (SSPT) contract through which the customer can purchase appliance-like support. Cisco SSPT for SAP HANA Infrastructure helps you resolve SAP HANA infrastructure problems faster by adding a solution-level perspective to your device-level service contracts. This service covers groups of Cisco UCS blade and rack server deployments as well as complementary Cisco and technology partner products.

For a detailed description, see <http://www.cisco.com/web/services/portfolio/solutions-support/documents/sspt-saphana-defintion.pdf>.

Also read Zora Caklovic's blog at <https://blogs.saphana.com/2015/02/18/sap-hana-tailored-data-center-integration-tdi-overview/>.

Physical Components of the Cisco C880 M4 Server

This section shows the components of the Cisco C880 M4.

Figure 5 shows the front of the Cisco C880 M4.

Figure 5. Cisco C880 M4: Front View of Connectors and System Boards

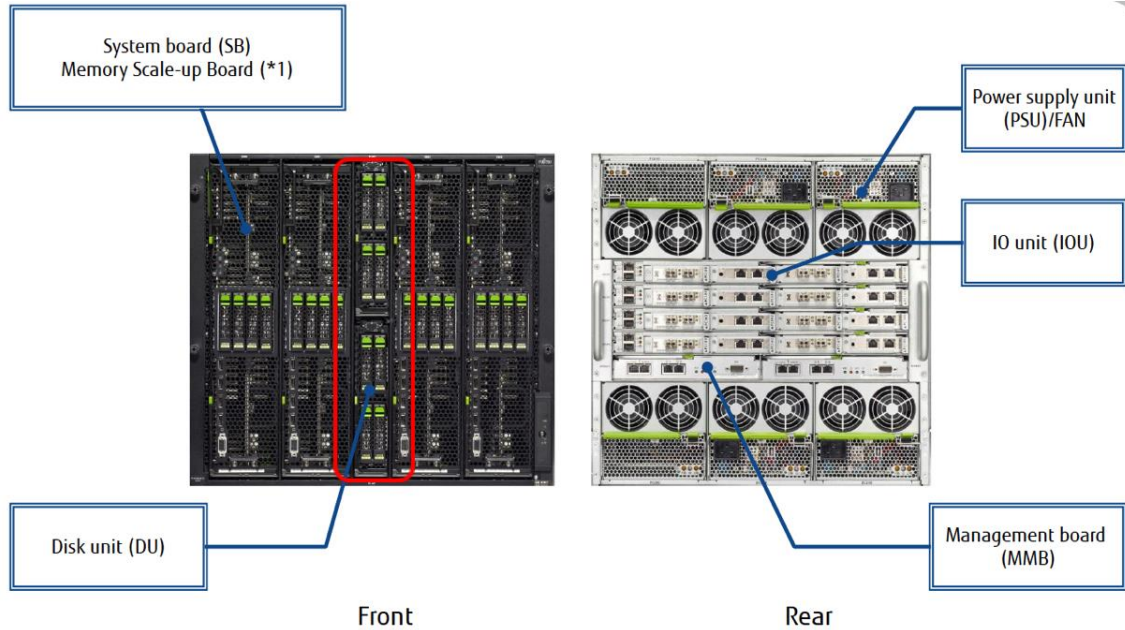


Figure 6 shows the rear of the Cisco C880 M4. Make sure that the power supply units (PSUs) and fans are placed in the slots as shown in this figure.

Figure 6. Cisco C880 M4: Rear View of Connectors

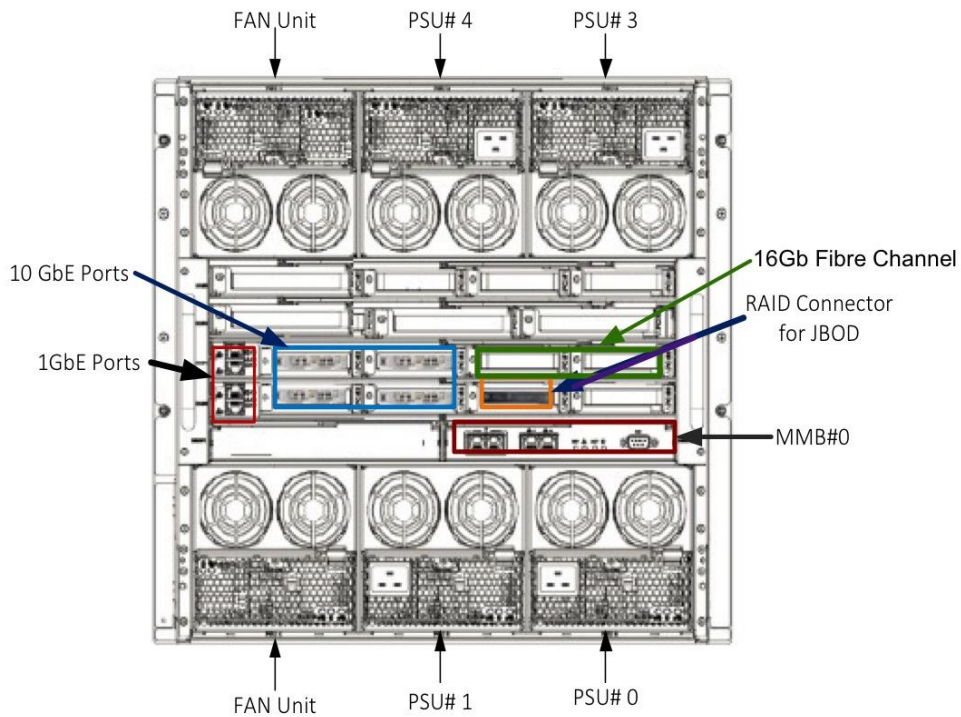
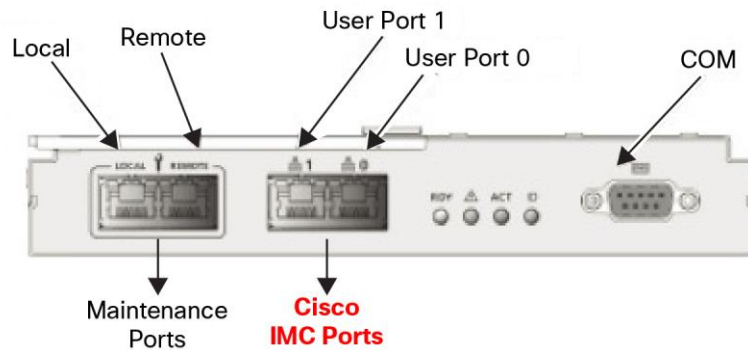


Figure 7 shows the management board (MMB) connectors on the Cisco C880 M4.

Figure 7. Cisco C880 M4: MMB 0 Connectors



Cisco C880 M4 Server Configuration

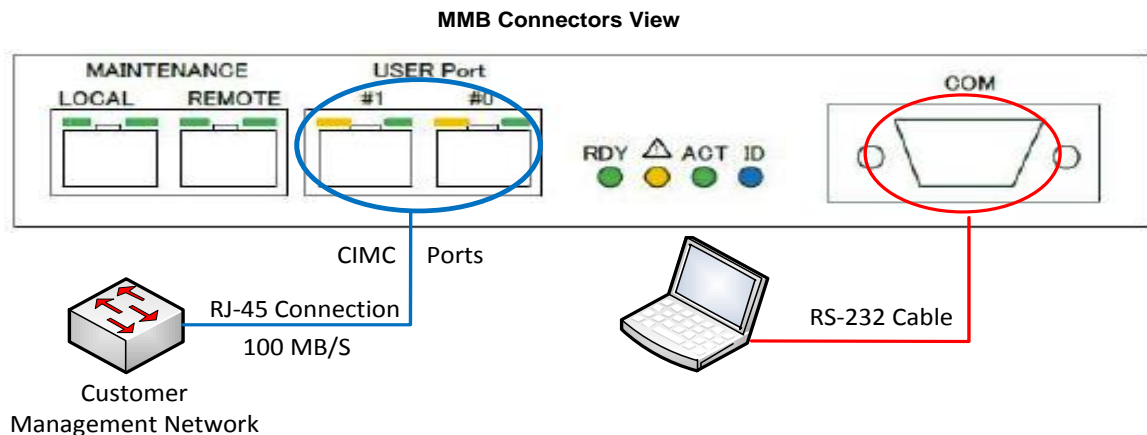
This section describes how to configure the Cisco C880 M4 Server.

Set Up the Cisco Integrated Management Controller

First you need to configure the onboard Cisco Integrated Management Controller (IMC).

1. Connect an RS-232 cable to the communications (COM) port.
2. Connect the user ports (IMC ports) to the customer management network and VLAN to access the IMC over your web browser (Figure 8). These two ports function as clustered ports.

Figure 8. Cisco C880 M4 MMB Connections



Note: After you power on the controller, wait for the ready (RDY) and active (ACT) LEDs to display a steady green light before performing the initial setup.

Connect to the Management Board

After you turn on the power, the MMB initialization process starts. During the initialization process, the MMB RDY LED flashes and the alarm LED of the unit in the front turns on.

After the initialization process is complete, the MMB RDY LED stops flashing and changes to a steady green light.

1. Verify that the COM port of the MMB is connected to the technician's system.
2. Set up the IP address for the IMC. Open a new serial connection using putty with the settings shown in Table 1.

Table 1. Cisco IMC Connection Settings

Item	Value
Baud rate	19200
Data bit	8
Parity bit	None
Stop bit	1
Flow control	None
Emulation	VT100

Note: The MMB initialization process takes about 6 minutes to complete.

After the serial connection is opened, you will see an initial message and login prompt on the terminal software screen. Enter the login name as **Administrator**. This is the preset default administrator user account name. After entering this user name, you are asked to change your password immediately.

3. Enter a new password. Then reenter the same password.

```
Cisco-1541432026 login: Administrator
You are required to change the password immediately (root enforced)
New password:
Retype New password:
Administrator >
```

Note: To see more commands and command syntax, enter the help command.

Set the Integrated Management Controller IP Address

Now set the IMC IP address.

1. Verify that the IMC ports are connected to the management network as shown in Figure 7.
2. After resetting the password as in the previous section, enter the commands shown here to set the IMC IP address and enable HTTP and Telnet access to it.

```
Administrator> set ip <ip address> <netmask>
Administrator> set gateway <ip address>
Administrator> set http enable
Administrator> set telnet enable
```

3. The default HTTP port is 8081. You can change this port if required by entering the following command:

```
Administrator> set http_port 80
```

Log in to the Web User Interface

Now log in to the web user interface. Table 2 shows settings.

Table 2. Settings to Log in to Web User Interface

Item	Value
URL	http://<Integrated Management controller IP>:8081
User name	Administrator
Password	Administrator's password

Figure 9 shows the login screen.

Figure 9. Cisco IMC Web User Interface Login Screen



Cisco C880 M4

Management Board Web UI Version 20.41



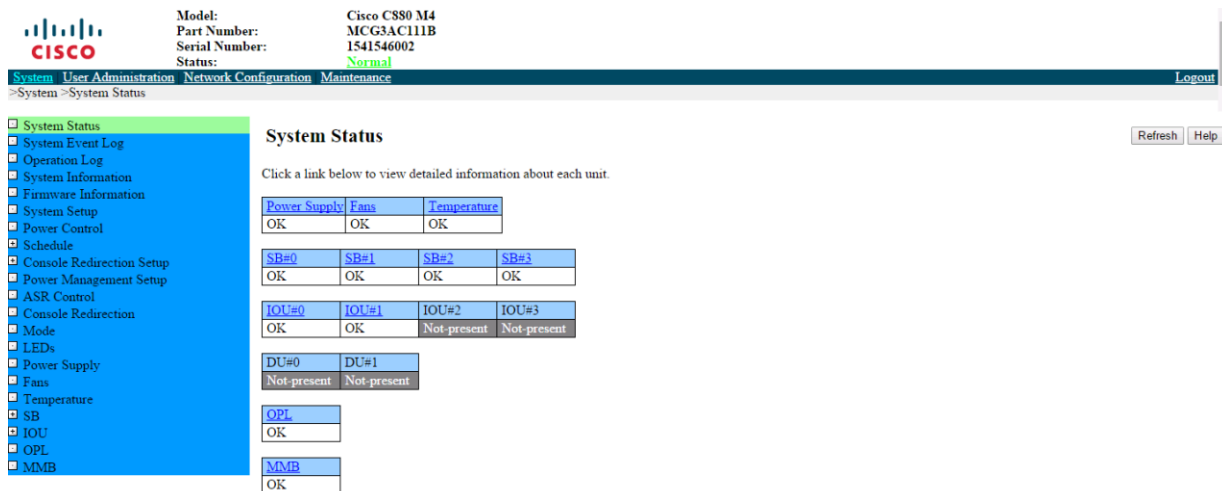
Username : Administrator
Password :

Login Cancel

* Username and password are case sensitive.

Figure 10 shows the system status and health screen that appears after you log in.

Figure 10. Cisco C880 M4 System Status and Health Page After Initial Login

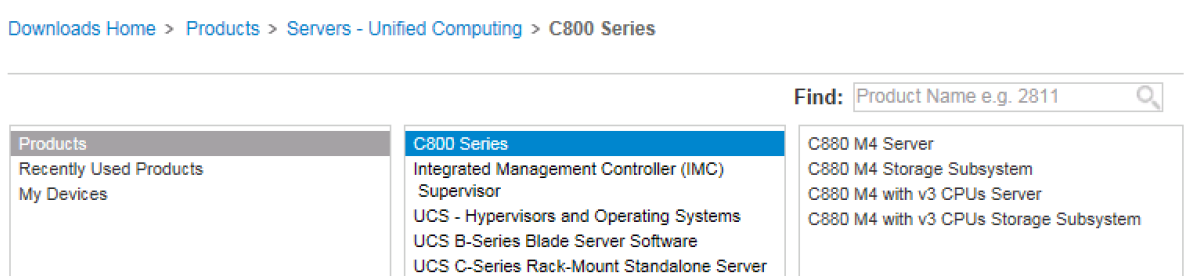


Update the Firmware

To update the server firmware, you first need to download the file.

1. Download the server firmware from <http://www.cisco.com/>. Choose Support > Products and select the Cisco C880 M4 Server (Figure 11).

Figure 11. Downloading Server Firmware



2. Choose the firmware according to the processor you are using:
 - Ivy-Bridge
 - Intel e7-88x0v2 firmware 1.0.x (x=4 in August 2016)
 - Haswell
 - Intel e7-88x0v3 firmware 1.2.x (x=4 in August 2016)
3. Unzip the downloaded C880M4-1.0.4.zip or C880M4-1.2.4.zip archive into a new directory on the system you use to start the MMB session.
4. Now perform the update. Log in to the system MMB through a web browser (Figure 12).

Figure 12. Logging in to the MMB



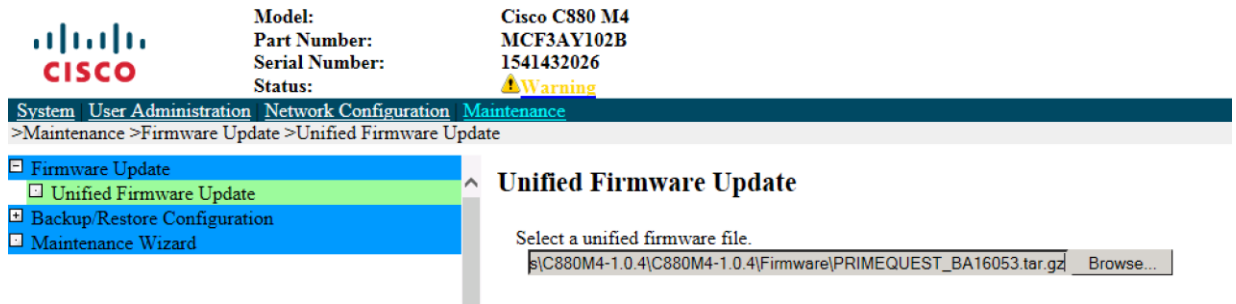
Username : Administrator

Password :

* Username and password are case sensitive.

5. Choose Maintenance > Firmware Update and browse to the firmware file (Figure 13).

Figure 13. Browsing to the Firmware File



6. Click Update.
7. Wait for the firmware version check window to appear (this process takes about 5 minutes).
8. Verify the firmware version. Then click OK

After about 1 minute, the progress bar appears. The time needed to update the firmware in a single MMB is about 70 minutes.

9. The web user interface session is disconnected during the firmware update process. For a single MMB configuration, log in to the web user interface again after about 5 minutes.

Configure the System Intelligent Platform Management Interface

By default, the Intelligent Platform Management Interface (IPMI) is not activated on the Cisco C880 M4 (Figure 14). If you want to use this function, you must enable it by configuring it at the command line interface (CLI).

Note: IPMI is not supported for the MMB IP address. Only the baseboard management controller (BMC) IP address can be used for the IPMI.

Figure 14.

The screenshot shows the Cisco C880 M4 configuration interface. At the top, the model is Cisco C880 M4, part number MCF3AY102B, and serial number 1541432026. A warning icon is present next to the status. The navigation menu includes System, User Administration, Network Configuration, and Maintenance. The current path is >Network Configuration >Network Interface >IPv4 Interface. The left sidebar shows a tree view with 'IPv4 Interface' selected. The main content area is titled 'IPv4 Interface' and contains a table for configuration. A note says 'Click the Apply button for all changes to take effect.' The table includes fields for IP Address, Hostname (CISCO-1541432026), Subnet Mask (255.255.255.0), Gateway address (172.23.1.1), and DNS (optional) settings (DNS, DNS Server 1, 2, 3, and Management LAN Dualization).

IPv4 Interface	
Click the Apply button for all changes to take effect.	
MMB IP Address	
IP Address	
Hostname	CISCO-1541432026
IP Address	172 . 23 . 1 . 100
Subnet Mask	255 . 255 . 255 . 0
Gateway address	172 . 23 . 1 . 1
DNS (optional)	
DNS	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
DNS Server 1
DNS Server 2
DNS Server 3
Management LAN	
Dualization	<input type="radio"/> Enable <input checked="" type="radio"/> Disable


You can check whether IPMI is enabled by entering the following command:

```
mgmtsrv01:/tftpboot # ipmitool -I lanplus -U admin -P admin -H 172.23.1.101
power status
Error: Unable to establish IPMI v2 / RMCP+ session
mgmtsrv01:/tftpboot #
```

To configure IPMI, follow these steps:

1. Set up the BMC IP address by configuring the console redirection IP address (Figure 15).

Figure 15. Configuring Console Redirection IP Address



Model: Cisco C880 M4
Part Number: MCF3AY102B
Serial Number: 1541432026
Status: ⚠ Warning

System
User Administration
Network Configuration
Maintenance

>System >Console Redirection Setup >IPv4 Console Redirection Setup

- [-] System Status
- [-] System Event Log
- [-] Operation Log
- [-] System Information
- [-] Firmware Information
- [-] System Setup
- [-] Power Control
- [+] Schedule
- [-] Console Redirection Setup
 - [-] IPv4 Console Redirection Setup
 - [-] IPv6 Console Redirection Setup
- [-] Power Management Setup
- [-] ASR Control
- [-] Console Redirection
- [-] Mode
- [-] LEDs
- [-] Power Supply
- [-] Fans
- [-] Temperature
- [+] SB
- [+] IOU
- [-] OPL
- [-] MMB

IPv4 Console Redirection Setup

Click the Apply Button to apply all changes.

IP Address	172 . 23 . 1 . 101
Subnet Mask	255 . 255 . 255 . 0
Video Redirection	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Virtual Media	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

2. Create the BMC user **admin** with password **admin**. The BMC user is disabled by default.

```

mgmtsrv01:/tftpboot # telnet 172.23.1.100
Telnet escape character is '\337'.
Trying 172.23.1.100...
Connected to 172.23.1.100.
login: Administrator
Password: ***
Last login: Tue Aug  2 12:00:37 from 172.25.1.6
Administrator > set bmc user admin admin admin quiet
Connection closed.
    
```

3. Test the function.

```
mgmtsrv01:/tftpboot # ipmitool -I lanplus -U admin -P admin -H 172.23.1.101
power status
Chassis Power is off
mgmtsrv01:/tftpboot # ipmitool -I lanplus -U admin -P admin -H 172.23.1.101
power on
Chassis Power Control: Up/On
mgmtsrv01:/tftpboot # ipmitool -I lanplus -U admin -P admin -H 172.23.1.101
power status
Chassis Power is on
mgmtsrv01:/tftpboot #
```

Configure Clustering with IPMI as Fencing Device

If you don't have a STONITH Block Devices (SBD) option to configure because of logging on shares Fibre Channel disks of a RHEL 6 installation, IPMI is also a valid option which can be configured.

The STONITH configuration with IPMI for SLES is shown here.

Note: The `server01-ipmi` and `server02-ipmi` parameters refer to the BMC IP address. Add those entries in the `/etc/hosts` file of both nodes.

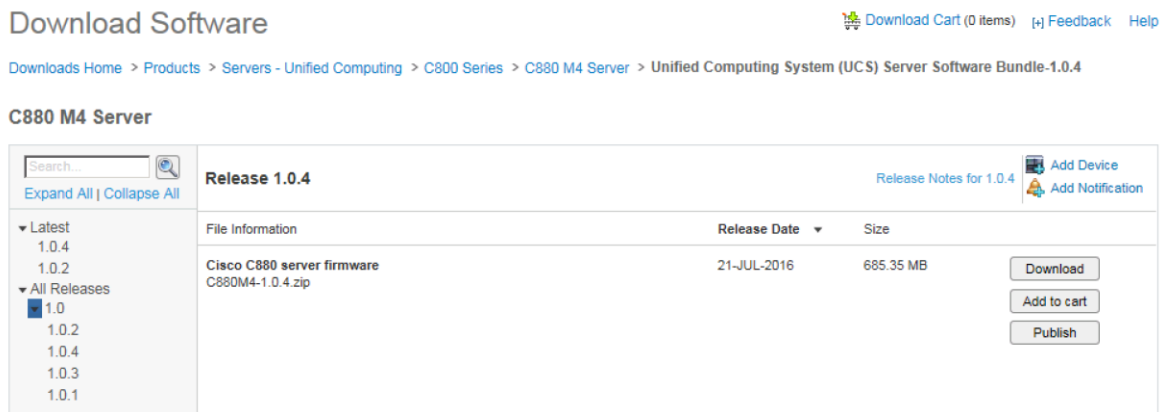
```
server01:~ # crm configure
crm(live)configure# primitive STONITH-Server01 stonith:external/ipmi op monitor
interval="0" timeout="60s" op monitor interval="300s" timeout="60s" on-
fail="restart" op start interval="0" timeout="60s" on-fail="restart" params
hostname="server01" ipaddr="server01-ipmi" userid="admin" passwd="admin"
interface="lanplus"
crm(live)configure# primitive STONITH-Server02 stonith:external/ipmi op monitor
interval="0" timeout="60s" op monitor interval="300s" timeout="60s" on-
fail="restart" op start interval="0" timeout="60s" on-fail="restart" params
hostname="server11" ipaddr="server02-ipmi" userid="admin" passwd="admin"
interface="lanplus"
crm(live)configure# location LOC_STONITH_Server01 STONITH-Server01 -inf:
server01
crm(live)configure# location LOC_STONITH_Server02 STONITH-Server02 -inf:
server02
```

Configure BIOS Settings

Before you configure BIOS settings, you should check for new system firmware.

1. To check for new system firmware, go to <http://www.cisco.com/>. Choose Support and search for the Cisco C880 M4 (Figure 16).

Figure 16. Checking for New Firmware

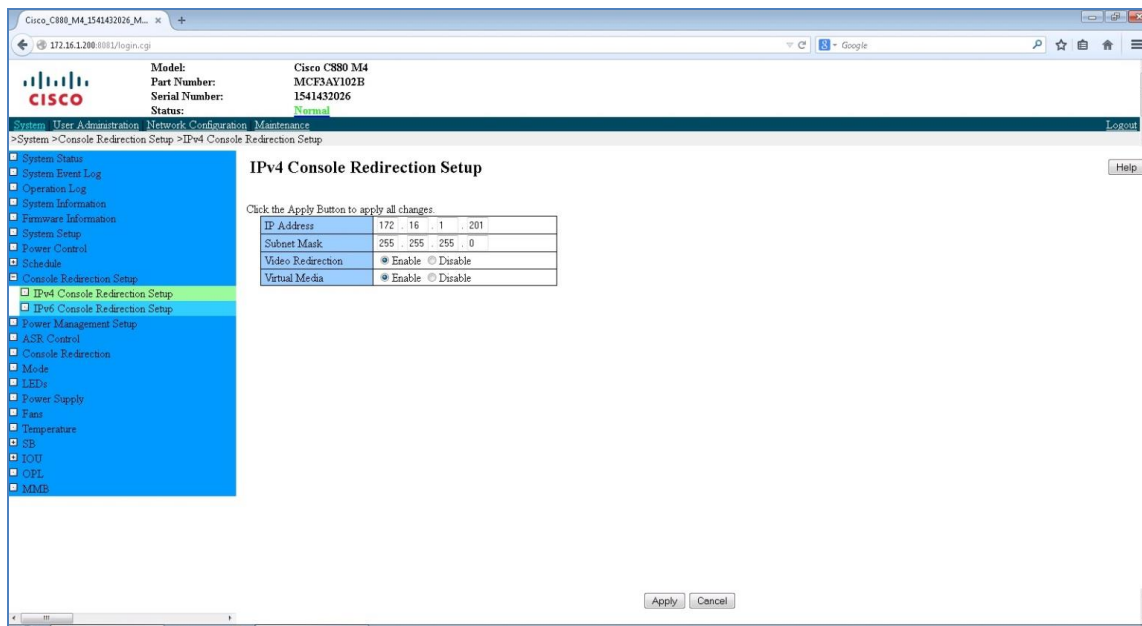


The screenshot shows the Cisco Download Software page for the C880 M4 Server. The page title is "Download Software" and it includes navigation links for "Downloads Home", "Products", "Servers - Unified Computing", "C800 Series", "C880 M4 Server", and "Unified Computing System (UCS) Server Software Bundle-1.0.4". The main content area is titled "C880 M4 Server" and features a search bar, "Expand All | Collapse All" links, and a "Release 1.0.4" section. The release information table is as follows:

File Information	Release Date	Size	
Cisco C880 server firmware C880M4-1.0.4.zip	21-JUL-2016	685.35 MB	<input type="button" value="Download"/> <input type="button" value="Add to cart"/> <input type="button" value="Publish"/>

2. Before you can set up the correct performance BIOS settings, you need to configure console redirection. Open a web browser and connect to the IMC web user interface as explained previously.
3. On the homepage, choose System > Console Redirection Setup > IPv4 Console Redirection Setup (Figure 17).

Figure 17. Cisco C880 M4 Console Redirection for Keyboard, Video, and Mouse (KVM)



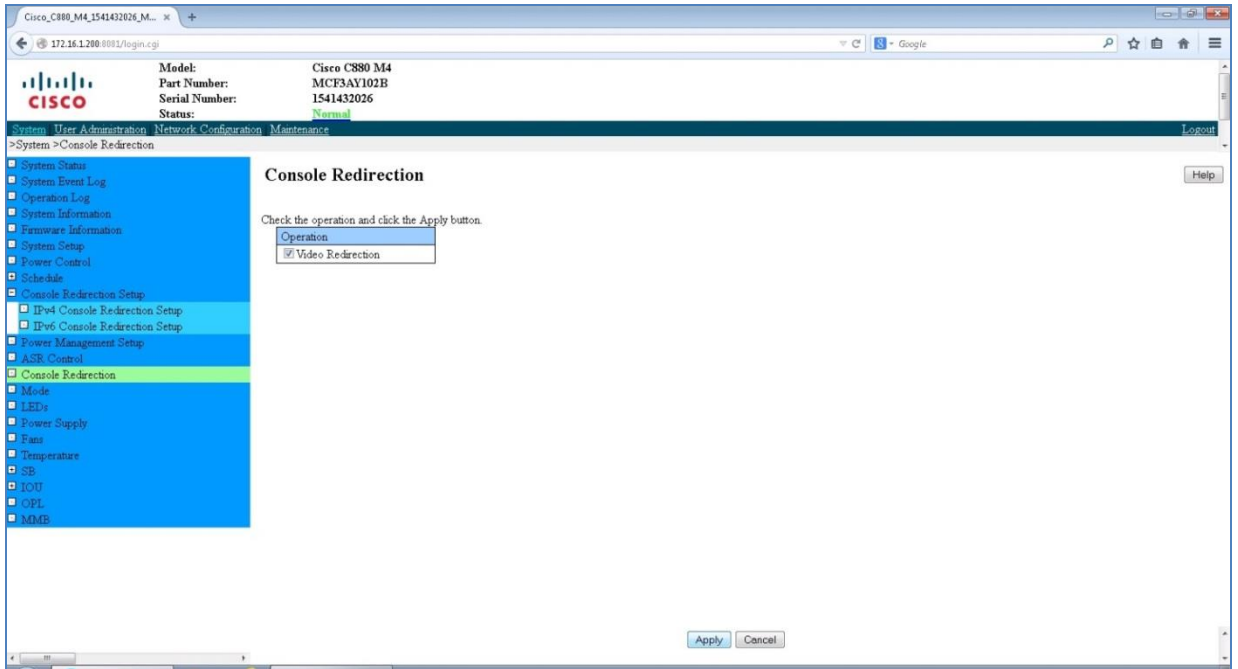
The screenshot shows the Cisco IMC web user interface for the IPv4 Console Redirection Setup. The page title is "IPv4 Console Redirection Setup" and it includes a "Help" button. The configuration table is as follows:

Click the Apply Button to apply all changes.	
IP Address	172 . 16 . 1 . 201
Subnet Mask	255 255 255 0
Video Redirection	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Virtual Media	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

4. Enter an IP address and select Enable for both the Video Redirection and Virtual Media options. Click Apply at the bottom of the page

5. In the menu on the left, select Console Redirection.
6. Select the Video Redirection check box and click the Apply button at the bottom of the page (Figure 18).

Figure 18. Selecting Video Redirection



7. Select Mode to configure the memory performance mode (Figure 19).

Figure 19. Selecting the Memory Mode

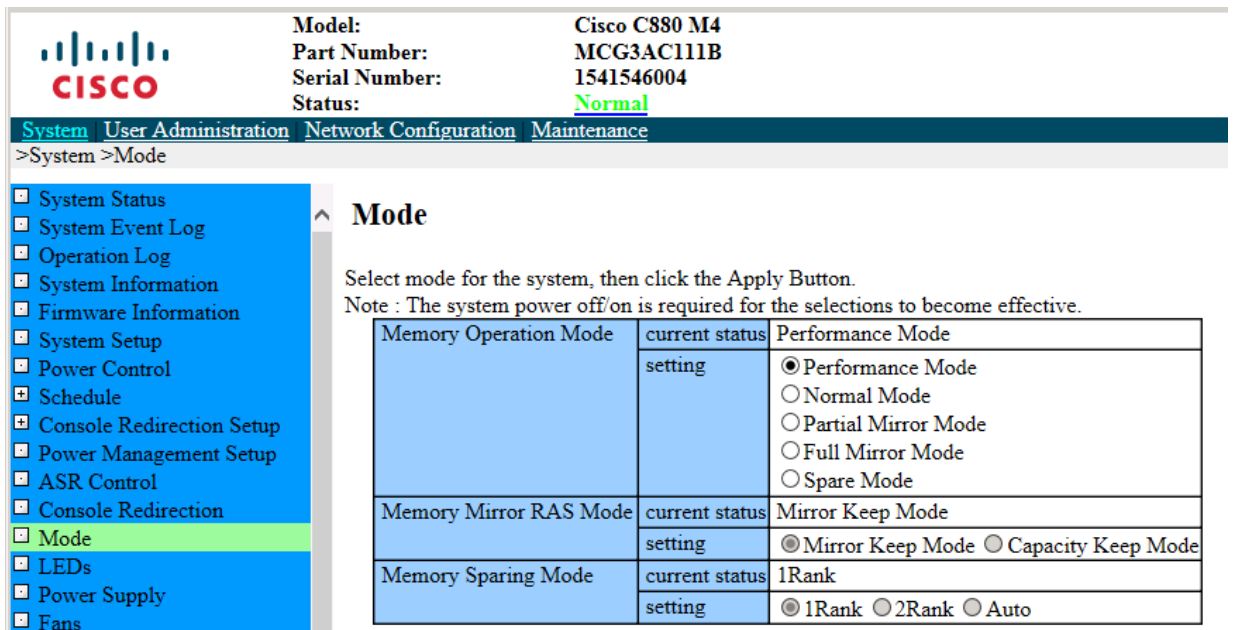


Figure 20. Cisco C880 M4: KVM Initial Screen

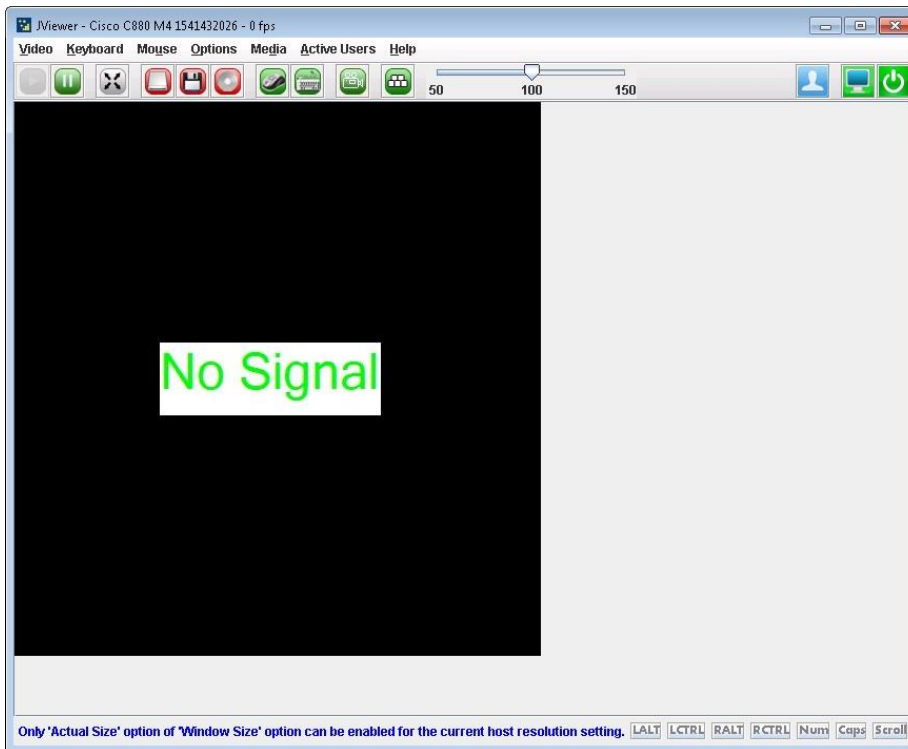


Figure 21. Cisco C880 M4: Selecting the Media Menu

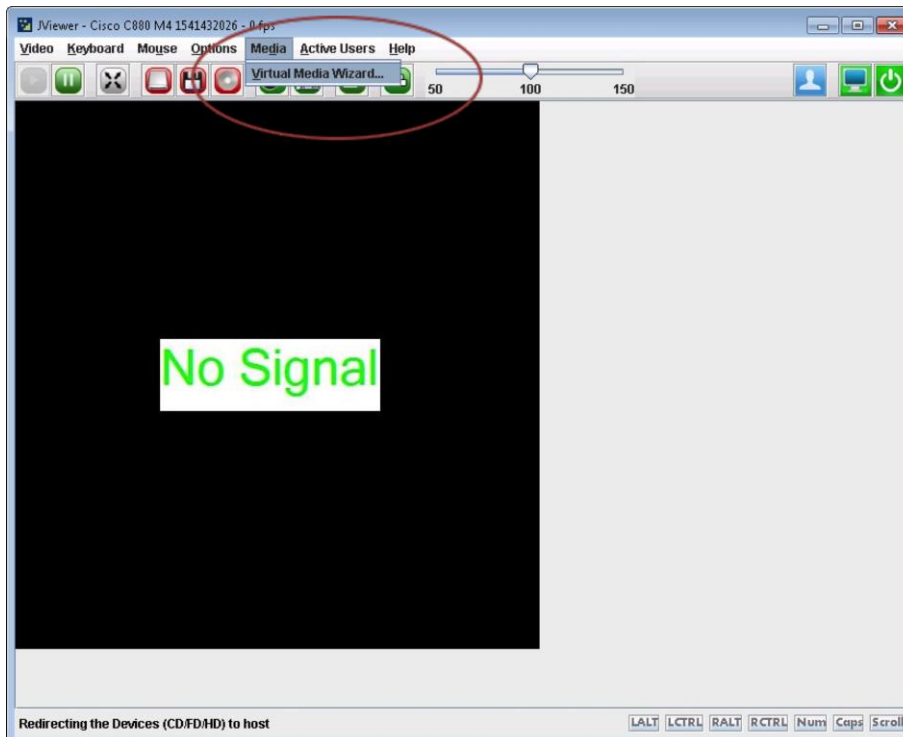
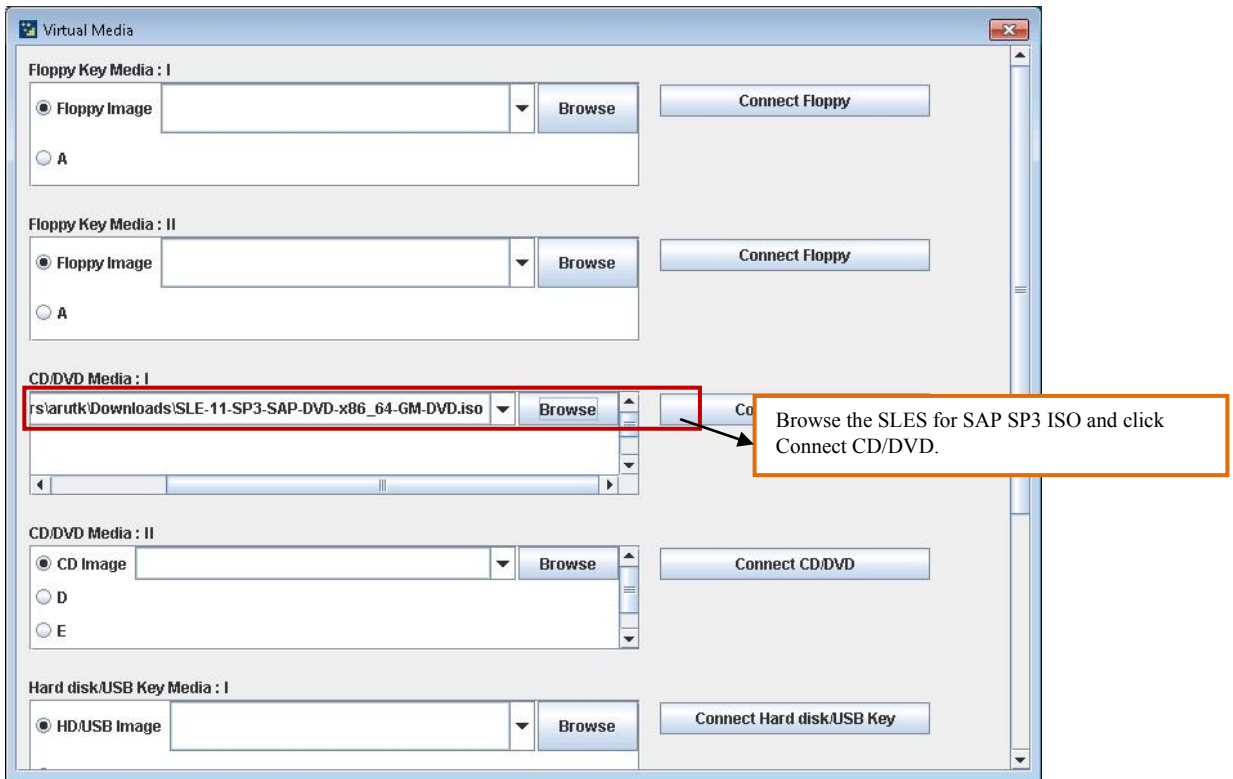
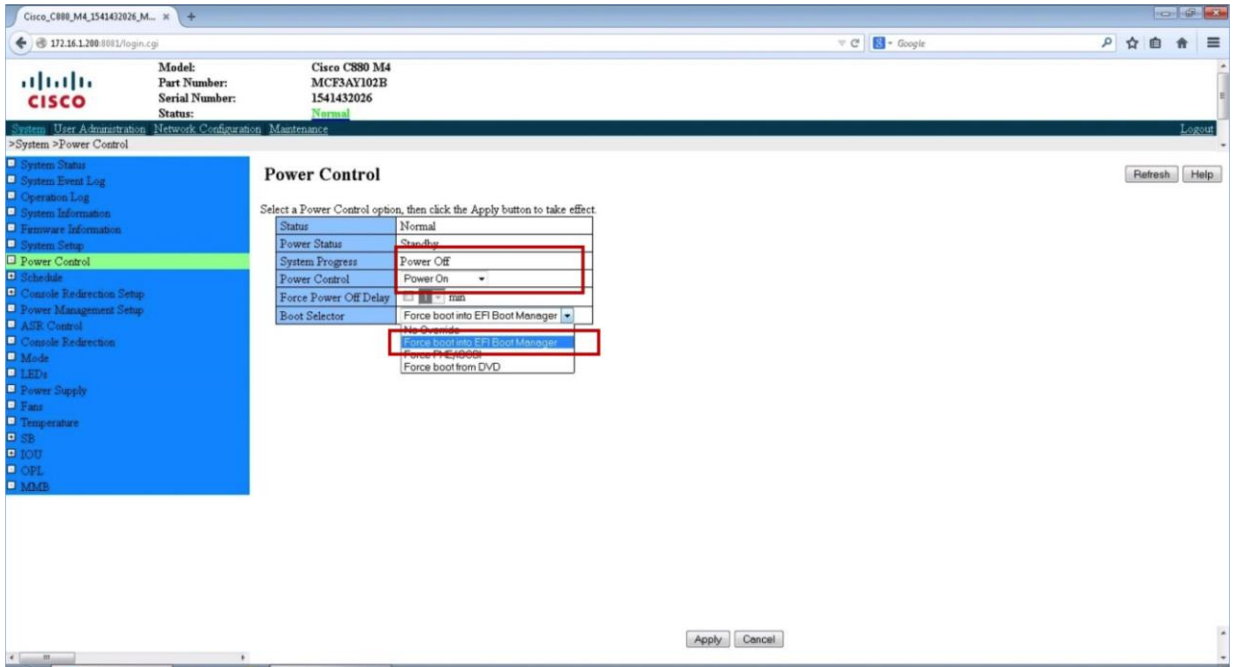


Figure 22. Cisco C880 M4: Selecting and Mounting the ISO Image



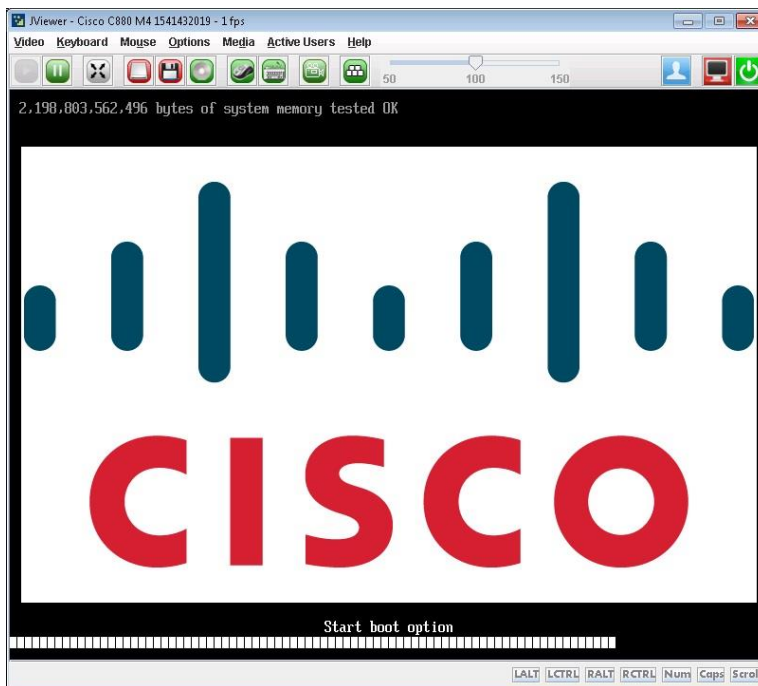
8. Select Power On and set the boot selector to Force Boot into EFI Boot Manager. Then click Apply at the bottom of the page (Figure 23).

Figure 23. Cisco C880 M4: Powering on the Server



The server boots (Figure 24).

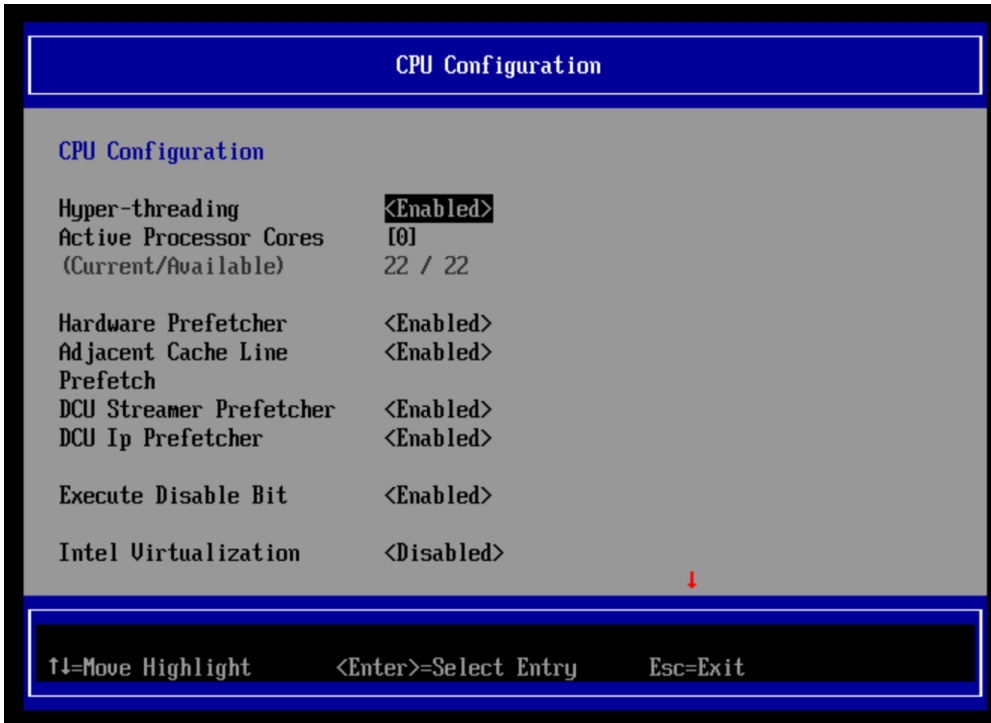
Figure 24. Booting the Server



9. After the servers boots, it displays the BIOS menu. Select CPU Configuration. Disable C-State.

10. Enable Uncore Frequency Override (Figure 25).

Figure 25. CPU Configuration (1)



11. Configure other settings as shown in Figures 26 and 27.

Figure 26. CPU Configuration (2)

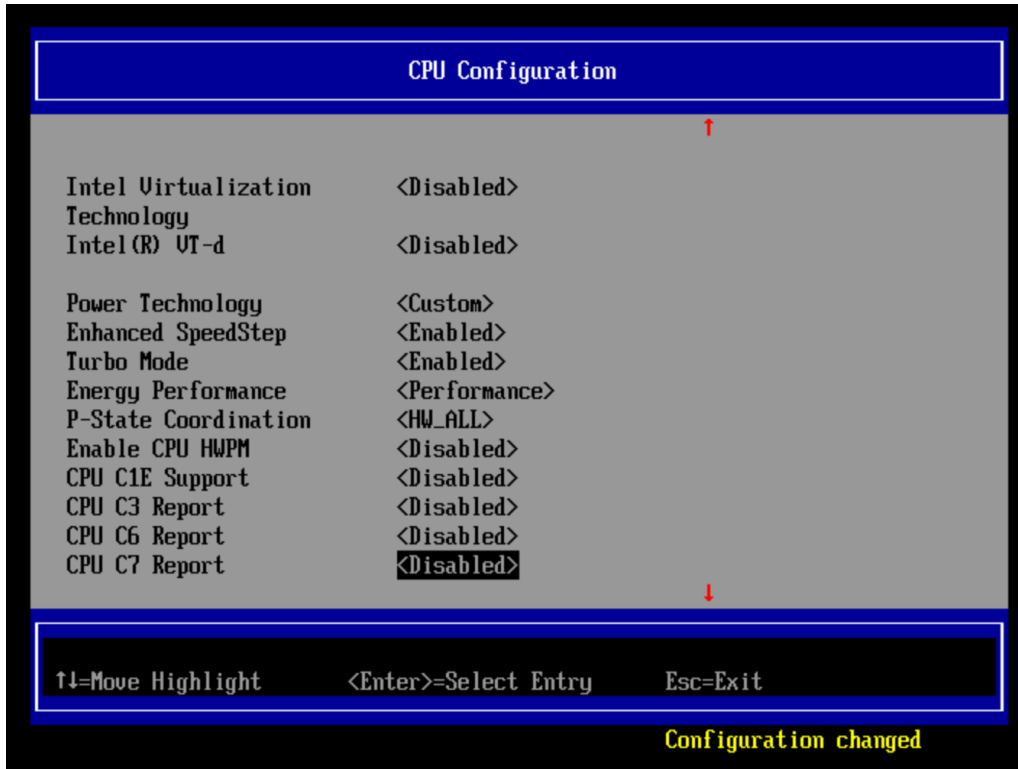
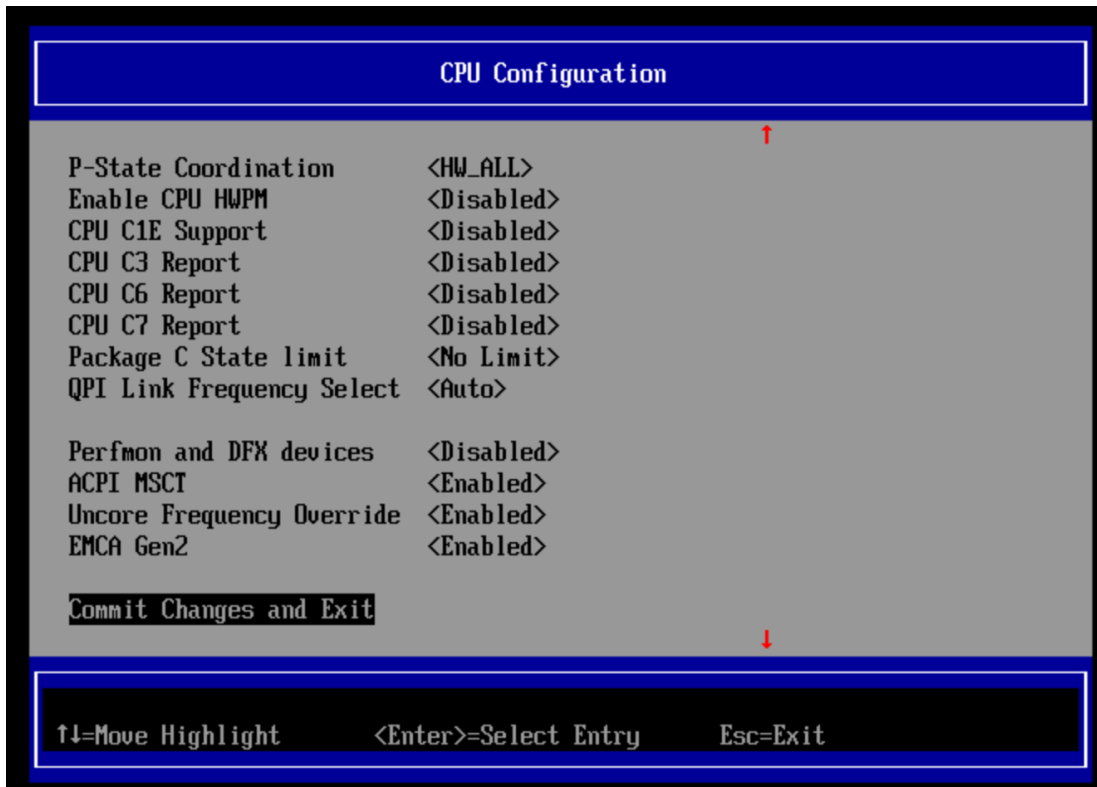
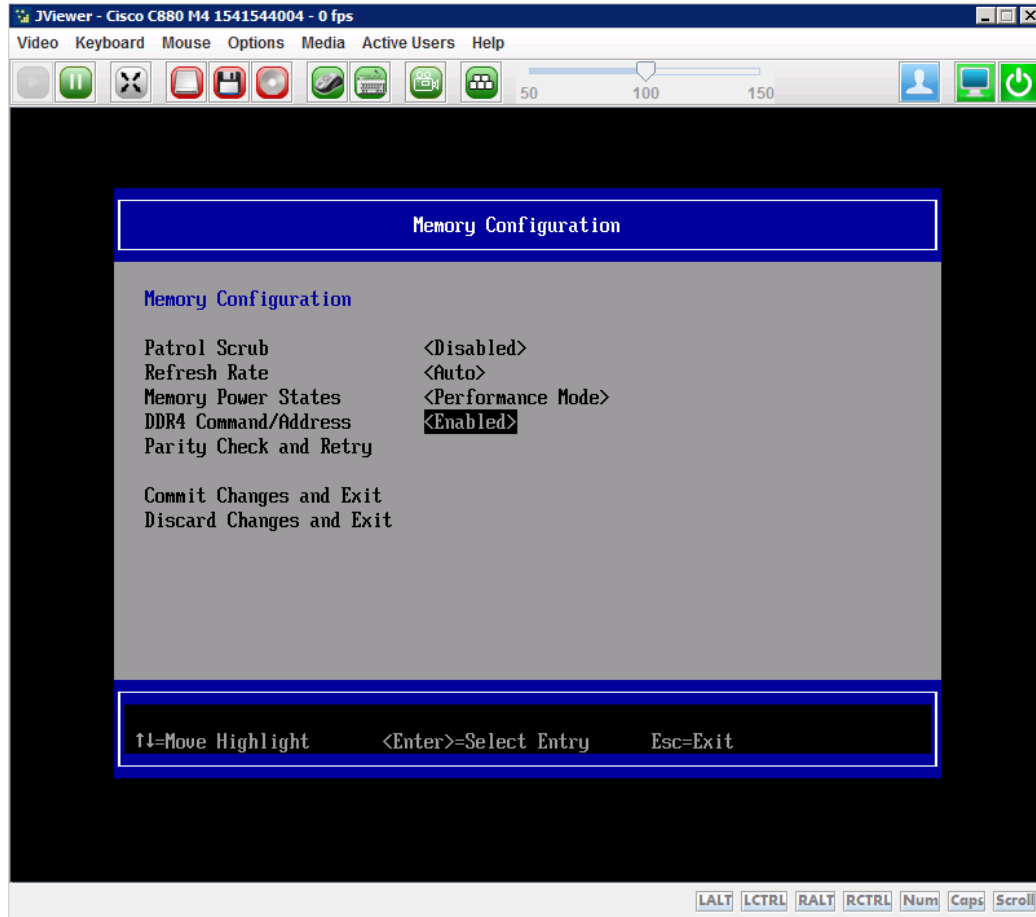


Figure 27. CPU Configuration (3)



12. Select the Commit Changes and Exit option and press Enter.
13. Press Esc to exit from the menu and return to the Main BIOS menu.
14. Select Memory Configuration (Figure 28).

Figure 28. Memory Configuration



15. Select the Commit Changes and Exit option and press Enter.
16. Press Esc to exit from the menu and return to the main BIOS menu.

C880M4 System Monitoring via SNMP

This example will show one of many options to monitor the system via SNMP. The next pictures will explain how the system gets prepared for SNMP monitoring and how the system can be integrated into Nagios/Check_MK.

First of all prepare the system to be able to respond on SNMP requests:

Log in on the MMB:



Cisco C880 M4 Management Board Web UI Version 20.57



Username :

Password :

* Username and password are case sensitive.

Figure 29. Navigate to Network Configuration → SNMP Configuration

The screenshot shows the Cisco configuration interface for the 'SNMP Community' page. At the top, the Cisco logo is on the left, and system details are on the right: Model: Cisco C880 M4, Part Number: MCF3AY102B, Serial Number: 1541432026, and Status: Warning. Below this is a breadcrumb trail: System > User Administration > Network Configuration > Maintenance > Network Configuration > SNMP Configuration > Community. A left-hand navigation menu lists various configuration sections, with 'SNMP Configuration' and 'Community' highlighted. The main content area is titled 'SNMP Community' and includes a note to click the 'Apply' button. Below this is a 'System Information' table with fields for System Name (CISCO-1541432026), System Location (Waldorf CISCO 4th), and System Contact (Ralf Klahr). A note states that the System Name can be configured in the System -> System Information page. At the bottom is a 'Community' table with columns for Community/User, IP Address/MASK, SNMP Version, Access, and Auth.

Community/User	IP Address/MASK	SNMP Version	Access	Auth
public	172.23.1.0/24	2	Read Only	noauth
public	172.25.1.0/24	2	Read Only	noauth
		1	Read Only	noauth
		1	Read Only	noauth

Set the SNMP community, the Network and the SNMP version.

Figure 30. Enable the SNMP Protocol under Network Configuration → Network Protocols

Model: Cisco C880 M4
Part Number: MCF3AY102B
Serial Number: 1541432026
Status: ⚠ Warning

System | User Administration | **Network Configuration** | Maintenance

>Network Configuration >Network Protocols

Network Protocols

Click the Apply Button to apply all changes.

Web (HTTP/HTTPS)

HTTP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
HTTP Port#[80,1024-65535]	80
HTTPS	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
HTTPS Port#[432,443,1024-65535]	432
Timeout (sec) [0,60-9999]	600

Telnet

Telnet	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Telnet Port#[23,1024-65535]	23
Timeout (sec) [0,60-9999]	600

SSH

SSH	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
SSH Port#[22,1024-65535]	22
Timeout (sec) [0,60-9999]	600


SNMP

SNMP Agent	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Agent Port#[161,1024-65535]	161
SNMP Trap	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Trap Port#[162,1024-65535]	162

Now the system is able to respond on SNMP requests:

```
mgmtsrv01:/var/spool/nagios # snmpwalk -v 2c -c public 172.23.1.100 |more
SNMPv2-MIB::sysDescr.0 = STRING: Cisco C880 M4 Management Board
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.9.1.31.1.1
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (740495) 2:03:24.95
SNMPv2-MIB::sysContact.0 = STRING: Ralf Klahr
SNMPv2-MIB::sysName.0 = STRING: CISCO-1541432026
SNMPv2-MIB::sysLocation.0 = STRING: Walldorf CISCO 4th.
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (5) 0:00:00.05
SNMPv2-MIB::sysORID.1 = OID: SNMP-MPD-MIB::snmpMPDMIBObjects.3.1.1
SNMPv2-MIB::sysORID.2 = OID: SNMP-USER-BASED-SM-MIB::usmMIBCompliance
SNMPv2-MIB::sysORID.3 = OID: SNMP-FRAMEWORK-MIB::snmpFrameworkMIBCompliance
SNMPv2-MIB::sysORID.4 = OID: SNMPv2-MIB::snmpMIB
```


Figure 31. Configure the SNMP trap destination where traps will be automatically send to.



Model: Cisco C880 M4
Part Number: MCF3AY102B
Serial Number: 1541432026
Status: ⚠Warning

System
User Administration
Network Configuration
Maintenance

>Network Configuration >SNMP Configuration >Trap

- Date/Time
- Network Interface
- Management LAN Port Configuration
- Network Protocols
- Refresh Rate
- SNMP Configuration
 - Community
 - Trap
 - SNMPv3 Configuration
- SSL
- SSH
- Remote Server Management
- Access Control
- Alarm E-Mail

SNMP Trap

Click the Apply Button to apply all changes.

Trap Destination

Community/User	IP Address	SNMP Version	Auth	Auth Type	Auth passphrase Priv passphrase
<input type="checkbox"/> public	172.25.1.6	2 ▾	[noauth ▾]	[MD5 ▾]	
<input type="checkbox"/>	::	1 ▾	[noauth ▾]	[MD5 ▾]	
<input type="checkbox"/>	::	1 ▾	[noauth ▾]	[MD5 ▾]	
<input type="checkbox"/>	::	1 ▾	[noauth ▾]	[MD5 ▾]	

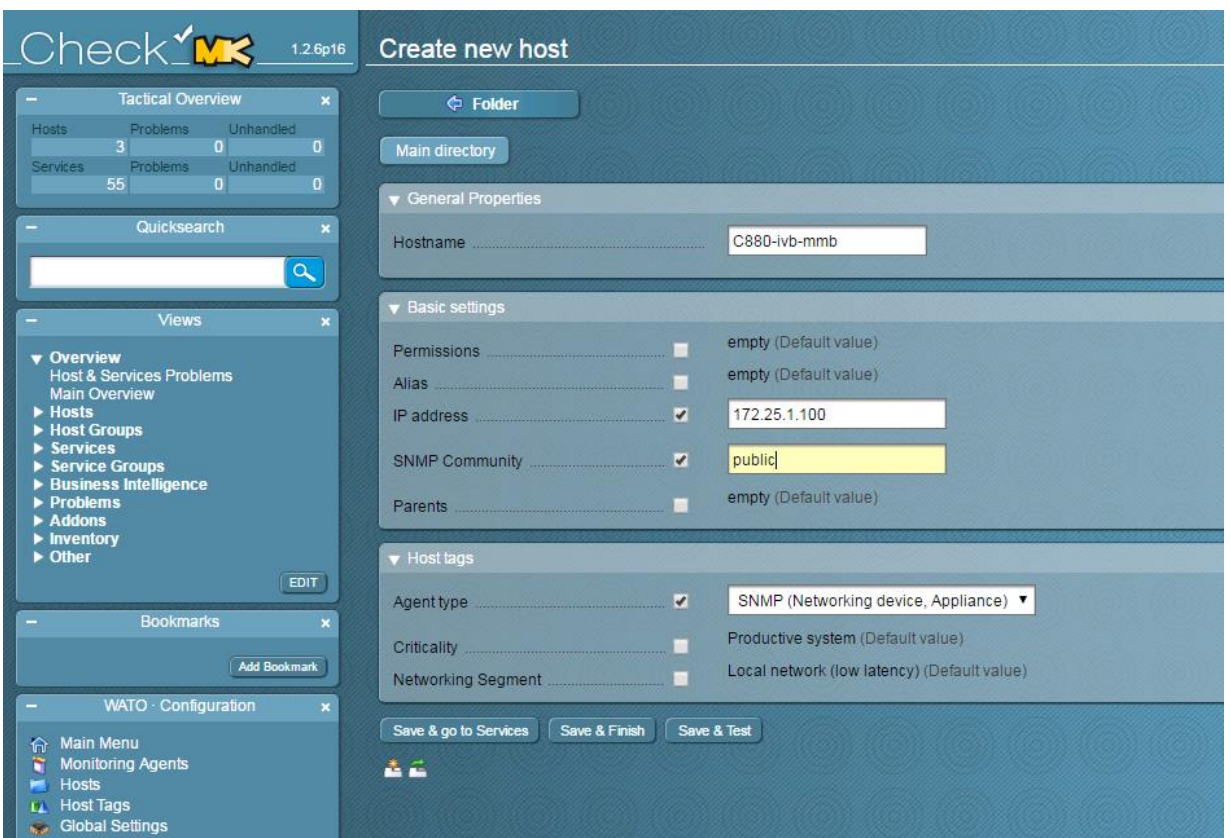
Now register the system in Check_MK (Nagios)

Select Hosts → New Host in Check_MK



Create a hostname for this system and fill in the IP address.

Figure 32. Once you select SNMP Appliance a new field with the SNMP Community string appears.



Save and go to Services.

Now the main system parameters are monitored with Check_mk and Nagios.

The screenshot shows the Check_MK web interface for host C880-ivb-mmb. On the left, there is a navigation menu with sections like Tactical Overview, Quicksearch, Views, and Bookmarks. The main area displays a table of services with columns for State, Service, Icons, Status detail, Age, Checked, and Perf-O-Meter. All services are in an 'OK' state.

State	Service	Icons	Status detail	Age	Checked	Perf-O-Meter
OK	Check_MK		OK - execution time 0.6 sec	119 min	24 sec	0.6 s
OK	Check_MK Discovery		OK - no unchecked services found	2 hrs	118 min	
OK	CPU utilization		OK - 21.0% utilization at 1 CPUs	119 min	24 sec	21 %
OK	Filesystem /mnt/fs0		OK - 46.7% used (64.68 of 138.56 MB), (levels at 80.00/90.00%), trend: 0.00 B / 24 hours	119 min	24 sec	46.68 %
OK	Filesystem /mnt/fs1		OK - 47.4% used (65.70 of 138.56 MB), (levels at 80.00/90.00%), trend: 0.00 B / 24 hours	119 min	24 sec	47.41 %
OK	Filesystem /mnt/hcp		OK - 17.8% used (292.68 MB of 1.61 GB), (levels at 80.00/90.00%), trend: 0.00 B / 24 hours	119 min	24 sec	17.79 %
OK	Interface 02		OK - [bond0] (up) MAC: 2c:d4:44:f0:96:00, 10 Mbit/s, in: 139.51 B/s, out: 322.57 B/s	119 min	24 sec	0.0% 0.0%
OK	Interface 03		OK - [eth0] (up) MAC: 2c:d4:44:f0:27:5f, 100 Mbit/s, in: 0.00 B/s, out: 0.00 B/s	119 min	24 sec	0.0% 0.0%
OK	Interface 06		OK - [eth3] (up) MAC: 2c:d4:44:f0:27:61, 100 Mbit/s, in: 7.13 B/s, out: 5.53 B/s	119 min	24 sec	0.0% 0.0%
OK	Interface 07		OK - [eth4] (up) MAC: 2c:d4:44:f0:27:60, 100 Mbit/s, in: 2.73 kB/s, out: 2.66 kB/s	119 min	24 sec	0.0% 0.0%
OK	Interface 08		OK - [eth5] (up) MAC: 2c:d4:44:f0:27:61, 100 Mbit/s, in: 7.13 B/s, out: 5.53 B/s	119 min	24 sec	0.0% 0.0%
OK	Memory used		OK - 0.05 GB used (0.05 GB RAM + 0.00 GB SWAP, this is 9.5% of 0.49 GB RAM)	119 min	23 sec	9%
OK	SNMP Info		OK - Cisco C880 M4 Management Board, CISCO-1541432026, Walldorf CISCO 4th., Ralf Klahr	119 min	23 sec	
OK	Uptime		OK - up since Tue Oct 18 10:50:44 2016 (0d 02:13:46)	119 min	23 sec	00d 02h 13m

View from Nagios:

The screenshot shows the Nagios web interface. The top navigation bar includes Home, Documentation, Current Status, Tactical Overview, Map, Services, Hosts, Host Groups, Service Groups, Problems, Reports, Availability, Trends, Alerts, Notifications, and System. The main content area displays 'Service Status Details For Host 'C880-ivb-mmb''. It includes a table of service status with columns for Host, Service, Status, Last Check, Duration, Attempt, and Status Information. All services are in an 'OK' state.

Host	Service	Status	Last Check	Duration	Attempt	Status Information
C880-ivb-mmb	CPU utilization	OK	10-18-2016 13:05:29	0d 2h 0m 58s	1/1	OK - 22.0% utilization at 1 CPUs
C880-ivb-mmb	Check_MK	OK	10-18-2016 13:05:29	0d 2h 0m 58s	1/1	OK - execution time 0.6 sec
C880-ivb-mmb	Check_MK Discovery	OK	10-18-2016 13:06:53	0d 2h 1m 44s	1/1	OK - no unchecked services found
C880-ivb-mmb	Filesystem /mnt/fs0	OK	10-18-2016 13:05:29	0d 2h 0m 58s	1/1	OK - 46.7% used (64.68 of 138.56 MB), (levels at 80.00/90.00%), trend: 0.00 B / 24 hours
C880-ivb-mmb	Filesystem /mnt/fs1	OK	10-18-2016 13:05:29	0d 2h 0m 58s	1/1	OK - 47.4% used (65.70 of 138.56 MB), (levels at 80.00/90.00%), trend: 0.00 B / 24 hours
C880-ivb-mmb	Filesystem /mnt/hcp	OK	10-18-2016 13:05:29	0d 2h 0m 58s	1/1	OK - 17.8% used (292.68 MB of 1.61 GB), (levels at 80.00/90.00%), trend: 0.00 B / 24 hours
C880-ivb-mmb	Interface 02	OK	10-18-2016 13:05:29	0d 2h 0m 58s	1/1	OK - [bond0] (up) MAC: 2c:d4:44:f0:96:00, 10 Mbit/s, in: 143.24 B/s, out: 326.64 B/s
C880-ivb-mmb	Interface 03	OK	10-18-2016 13:05:29	0d 2h 0m 58s	1/1	OK - [eth0] (up) MAC: 2c:d4:44:f0:27:5f, 100 Mbit/s, in: 0.00 B/s, out: 0.00 B/s
C880-ivb-mmb	Interface 06	OK	10-18-2016 13:05:29	0d 2h 0m 58s	1/1	OK - [eth3] (up) MAC: 2c:d4:44:f0:27:61, 100 Mbit/s, in: 143.24 B/s, out: 0.00 B/s
C880-ivb-mmb	Interface 07	OK	10-18-2016 13:05:29	0d 2h 0m 58s	1/1	OK - [eth4] (up) MAC: 2c:d4:44:f0:27:60, 100 Mbit/s, in: 2.92 kB/s, out: 2.84 kB/s
C880-ivb-mmb	Interface 08	OK	10-18-2016 13:05:29	0d 2h 0m 58s	1/1	OK - [eth5] (up) MAC: 2c:d4:44:f0:27:61, 100 Mbit/s, in: 12.19 B/s, out: 8.28 B/s
C880-ivb-mmb	Memory used	OK	10-18-2016 13:05:29	0d 2h 0m 58s	1/1	OK - 0.05 GB used (0.05 GB RAM + 0.00 GB SWAP, this is 9.5% of 0.49 GB RAM)
C880-ivb-mmb	SNMP Info	OK	10-18-2016 13:05:29	0d 2h 0m 58s	1/1	OK - Cisco C880 M4 Management Board, CISCO-1541432026, Walldorf CISCO 4th., Ralf Klahr
C880-ivb-mmb	Uptime	OK	10-18-2016 13:05:29	0d 2h 0m 58s	1/1	OK - up since Tue Oct 18 10:50:43 2016 (0d 02:14:46)

iSCSI Boot Configuration

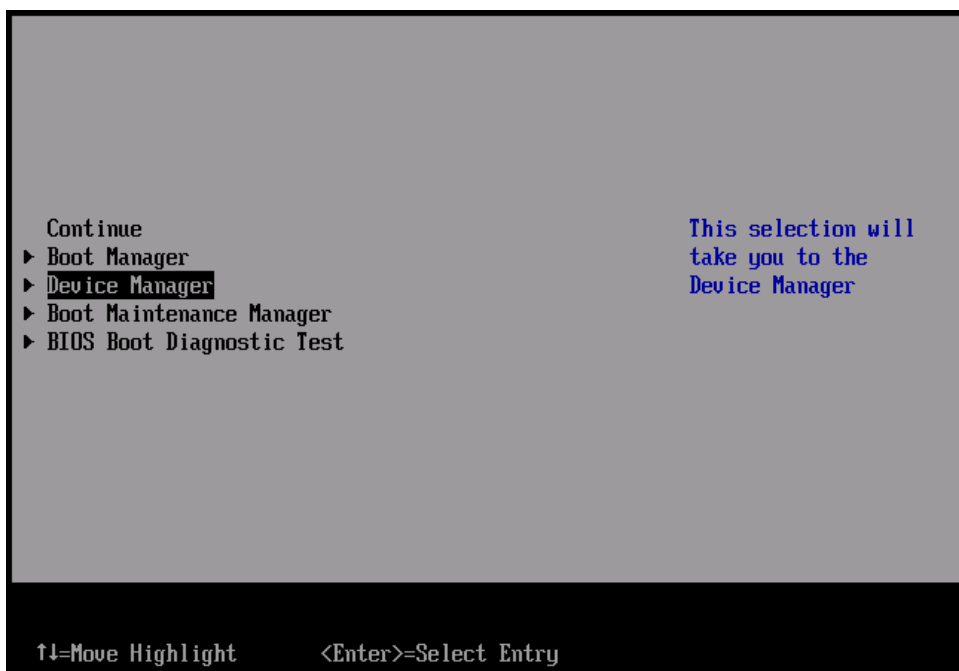
This section describes how to configure iSCSI boot.

Prepare for iSCSI Configuration

Perform the following steps before configuring iSCSI:

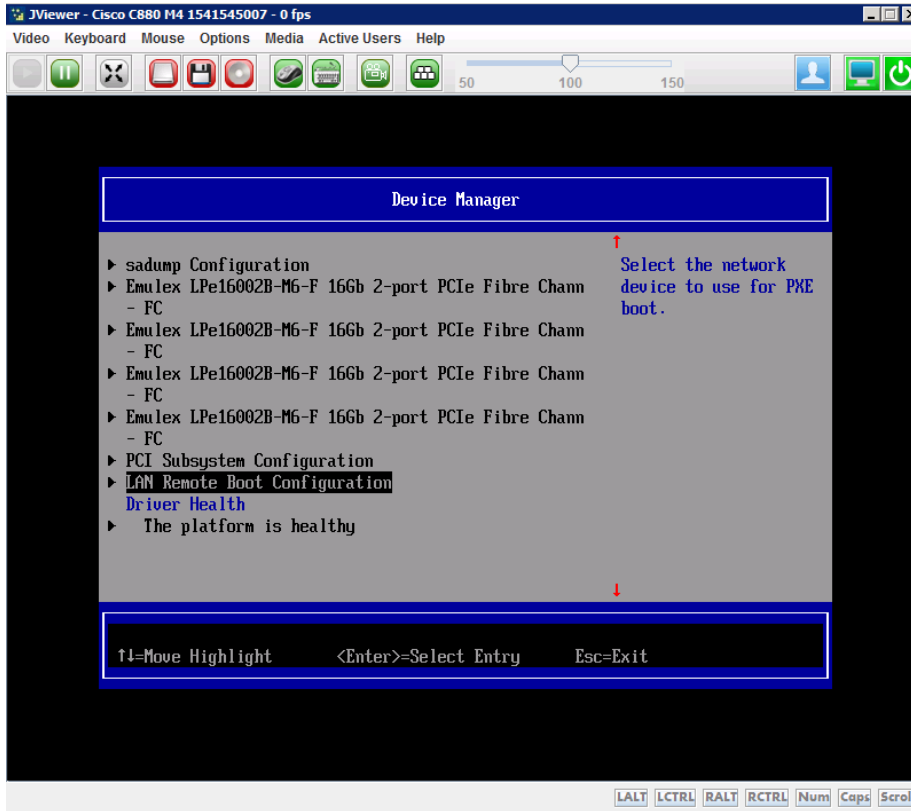
1. Start the system and from the Extensible Firmware Interface (EFI) Boot Manager, select Device Manager (Figure 33). This selection will start the Device Manager.

Figure 33. Starting the Device Manager



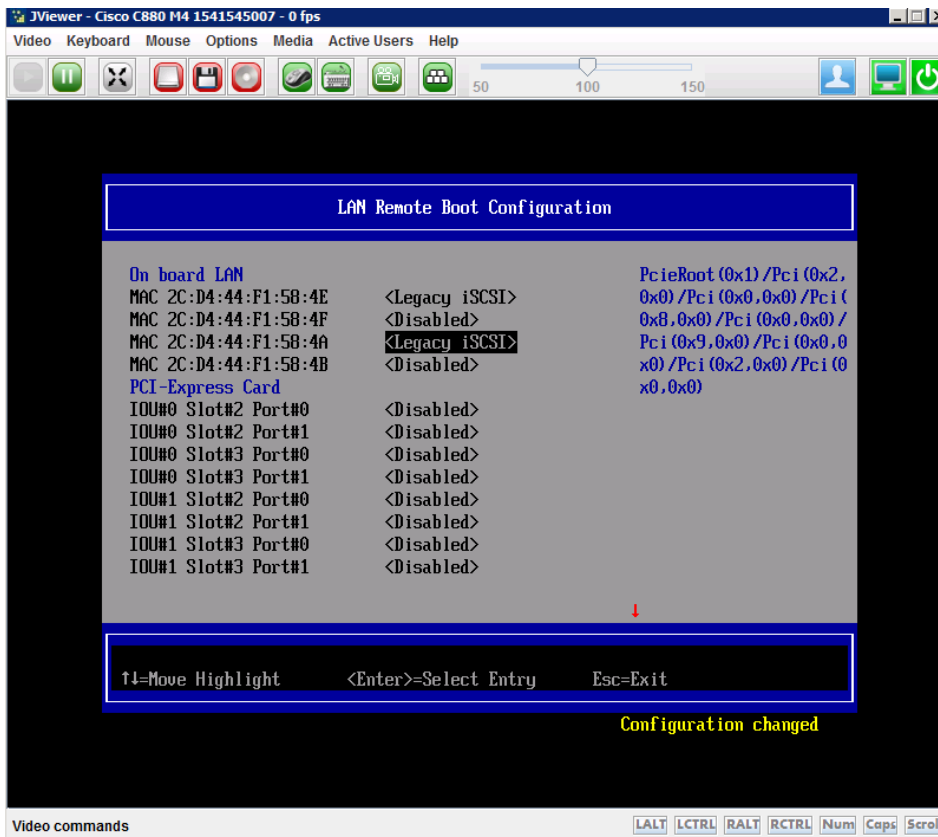
2. Select LAN Remote Boot Configuration (Figure 34).

Figure 34. Selecting LAN Remote Boot Configuration



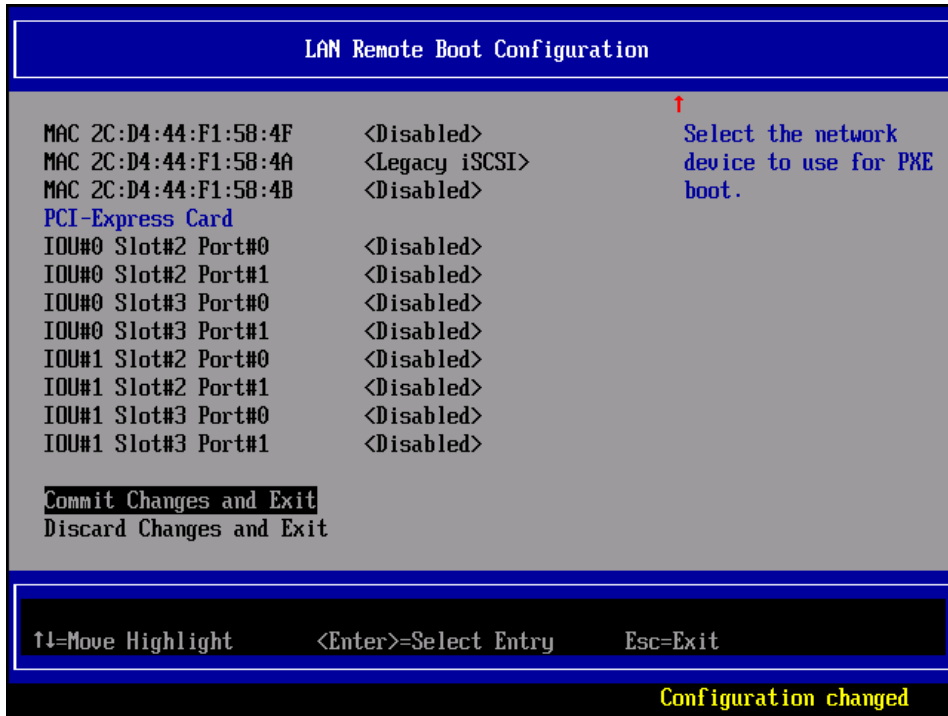
3. Enable the LAN controller BIOS (Figure 35).

Figure 35. Enabling the LAN Controller BIOS



4. Select Commit Changes and Exit (Figure 36).

Figure 36. Committing the Changes

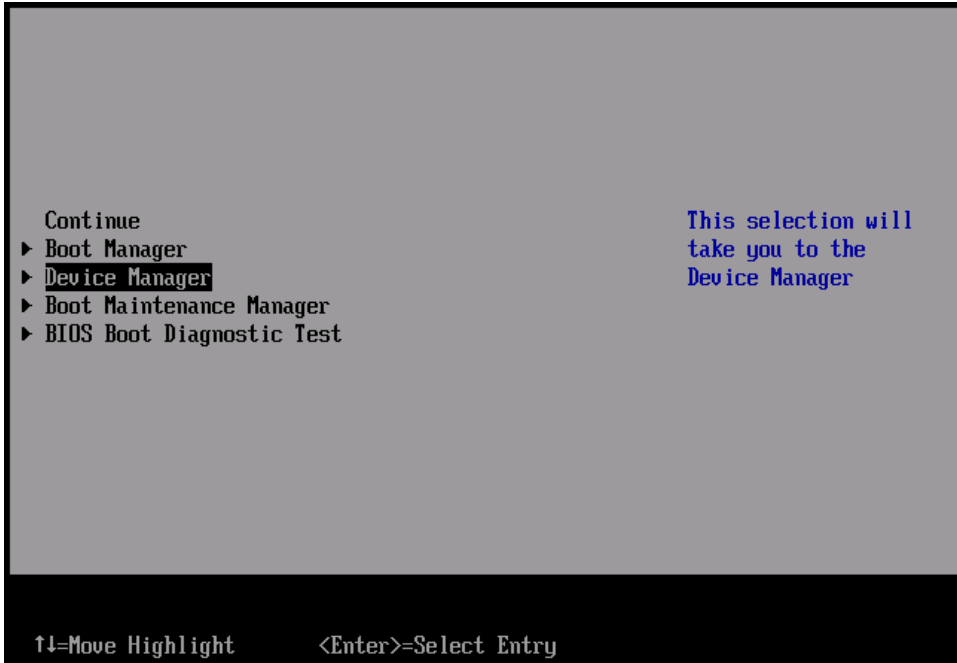


Configure iSCSI Boot

Now you are ready to configure iSCSI boot.

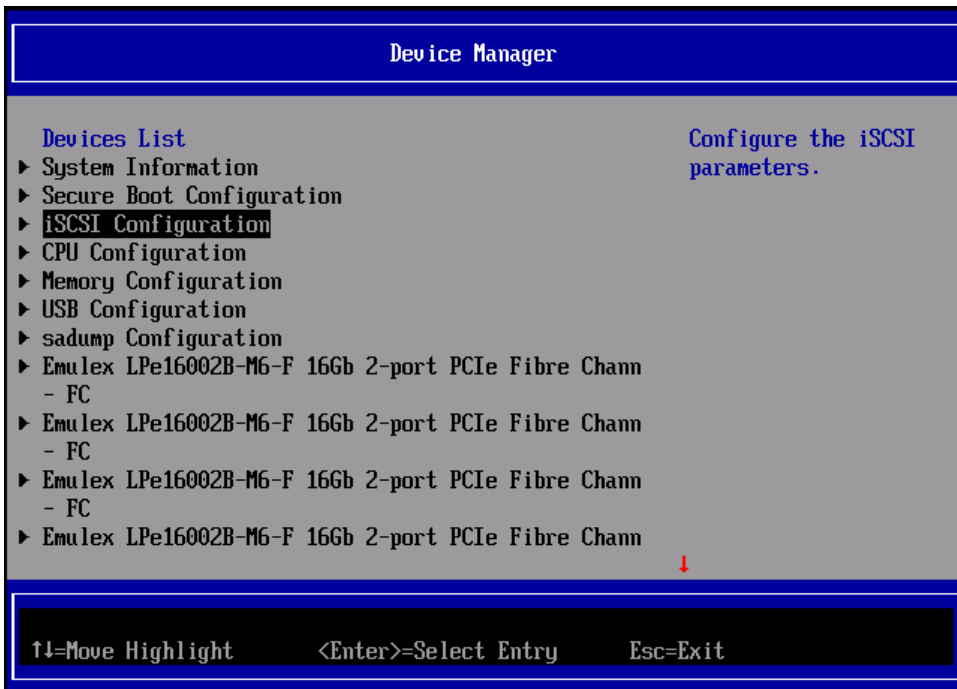
1. Reboot the system.
2. After the system has booted, restart the Device Manager (Figure 37).

Figure 37. Restarting Device Manager



3. Select iSCSI Configuration (Figure 38).

Figure 38. Selecting iSCSI Configuration



4. Define the iSCSI initiator name of the system (Figures 39 and 40).

Figure 39. Defining the iSCSI Initiator (1)

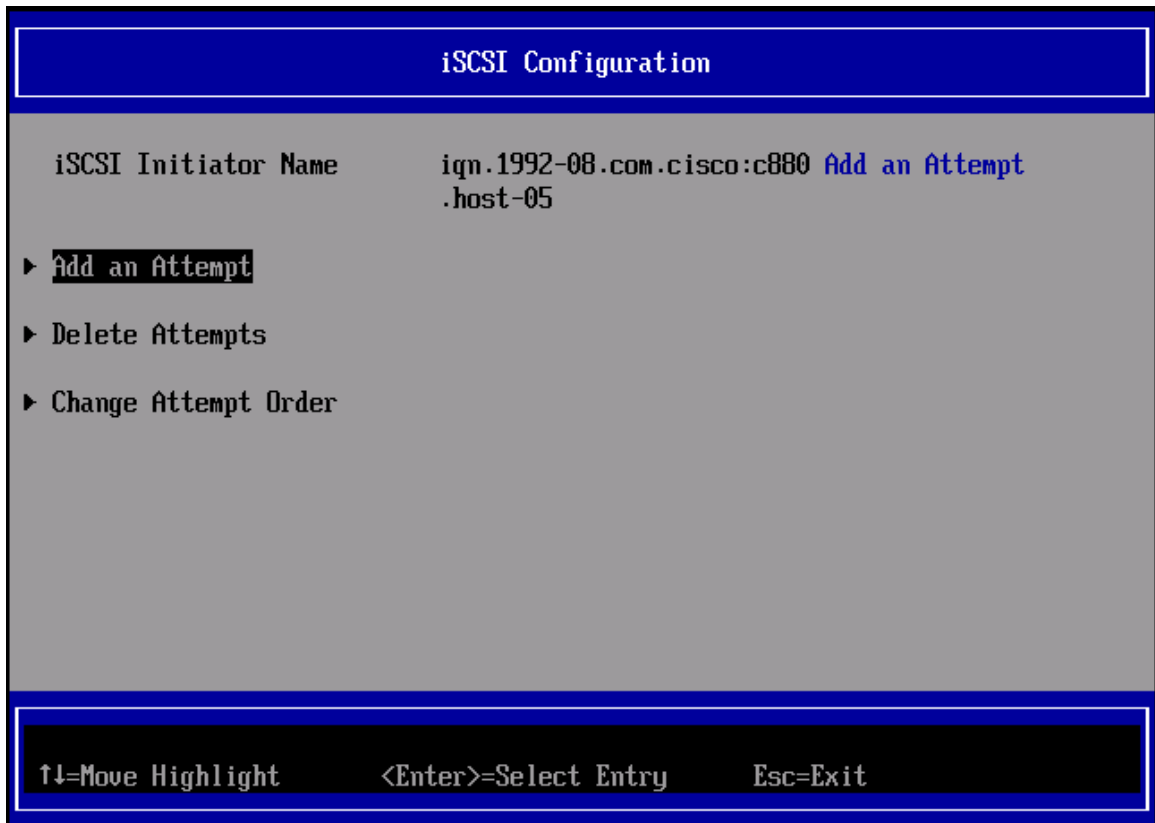
The image shows a terminal window titled "iSCSI Configuration". The main area is divided into a header and a content section. The header contains the title "iSCSI Configuration". The content section has a label "iSCSI Initiator Name" followed by a cursor. To the right of the cursor is a help text: "The worldwide unique name of iSCSI Initiator. Only IQN format is accepted." Below the label is a prompt "► Add an Attempt". A text input field is shown with the text "iqn.1992-08.com.cisco:c880.host-05" and a cursor at the end. Above the input field is the prompt "Please type in your data". At the bottom of the terminal window, there is a footer with the text "<Enter>=Complete Entry Esc=Exit Entry".

```
iSCSI Configuration

iSCSI Initiator Name      |
                          |
► Add an Attempt          | The worldwide unique
                          | name of iSCSI
                          | Initiator. Only IQN
                          | format is accepted.
                          |
Please type in your data
iqn.1992-08.com.cisco:c880.host-05_

<Enter>=Complete Entry  Esc=Exit Entry
```

Figure 40. Defining the iSCSI Initiator (2)



5. Configure the iSCSI adapter that you will use for the initial system boot (Figures 41 and 42).

Figure 41. Configuring the iSCSI Adapter (1)



Figure 42. Configuring the iSCSI Adapter (2)

Attempt Configuration		
iSCSI Attempt Name	1	Enter IP address in dotted-decimal notation.
iSCSI Mode	<Enabled>	
Internet Protocol	<IP4>	
Connection Retry Count	[16]	
Connection Establishing Timeout	[1000]	
ISID	2CD444F1584E	
Enable DHCP	[]	
Initiator IP Address	192.168.137.105	
Initiator Subnet Mask	255.255.255.0	

↓

↑↓=Move Highlight <Enter>=Select Entry Esc=Exit

Configuration changed

- Specify the iSCSI target (Figure 43).

Figure 43. Specifying the iSCSI Target

The screenshot shows a terminal window titled "Attempt Configuration". It contains several configuration fields and a text entry box. The fields are: "Internet Protocol" with value "<IP4>", "Connection Retry Count" with value "[16]", "Initiator IP Address" with value "192.168.137.105", "Initiator Subnet Mask" with value "255.255.255.0", and "Gateway" with value "192.168.137.1". The "Target Name" field is currently empty. A text entry box is open, showing the text "iqn.1992-08.com.netapp:c880.boot_". A red arrow points to the "Target Name" field, and another red arrow points to the text entry box. At the bottom, there is a prompt "<Enter>=Complete Entry Esc=Exit Entry" and a status message "Configuration changed" in yellow.

Attempt Configuration	
Internet Protocol	<IP4>
Connection Retry Count	[16]
Please type in your data	
iqn.1992-08.com.netapp:c880.boot_	
Initiator IP Address	192.168.137.105
Initiator Subnet Mask	255.255.255.0
Gateway	192.168.137.1
Target Name	

<Enter>=Complete Entry Esc=Exit Entry

Configuration changed

Figure 44.

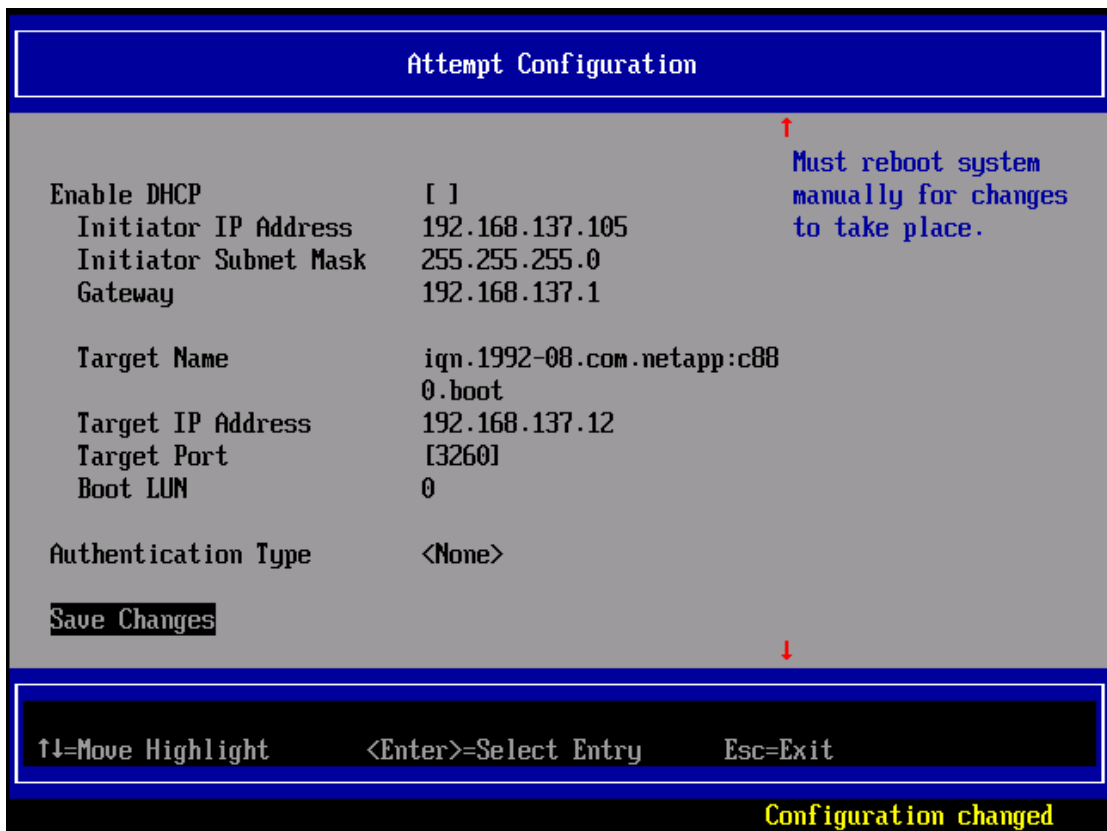


Figure 45.



Figure 46.

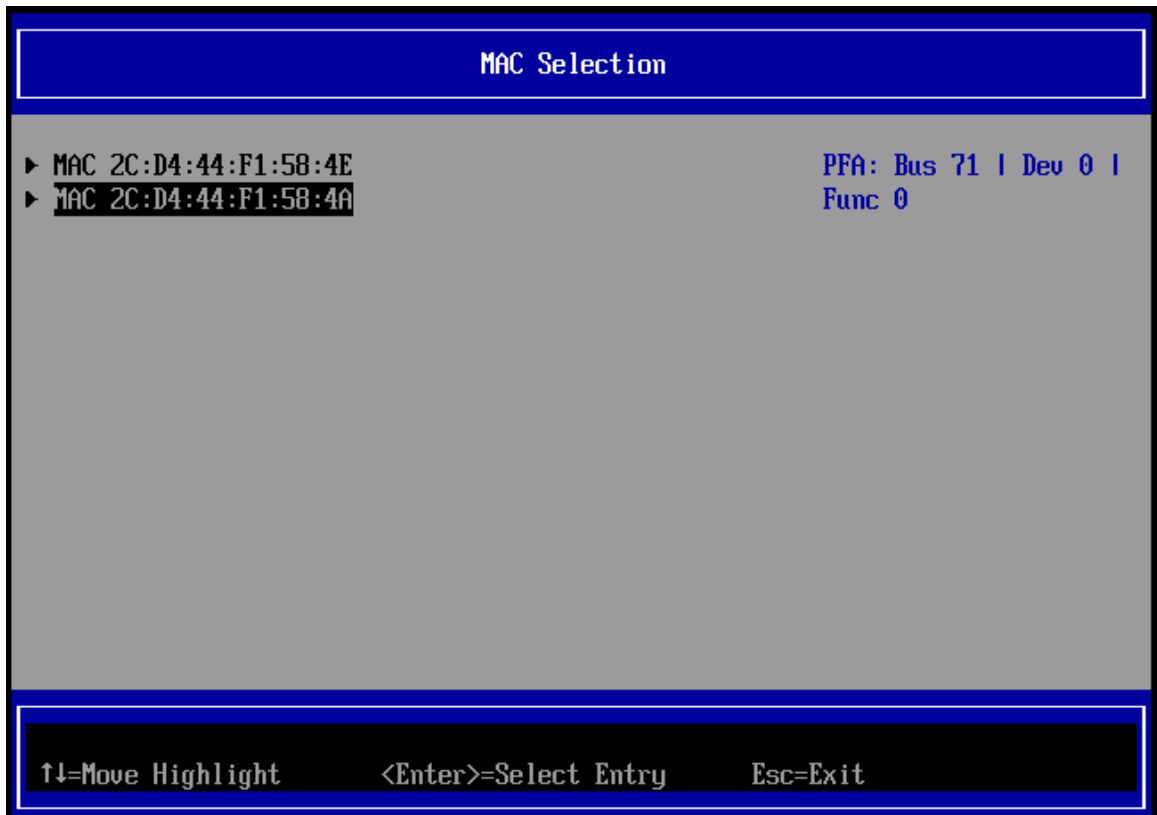


Figure 47.

Attempt Configuration		
iSCSI Attempt Name	2	Enter IP address in dotted-decimal notation.
iSCSI Mode	<Enabled>	
Internet Protocol	<IP4>	
Connection Retry Count	[16]	
Connection Establishing Timeout	[1000]	
ISID	2CD444F1584A	
Enable DHCP	[]	
Initiator IP Address	192.168.137.115	
Initiator Subnet Mask	255.255.255.0	

↓

↑↓=Move Highlight <Enter>=Select Entry Esc=Exit

Configuration changed

Figure 48.



Figure 49.

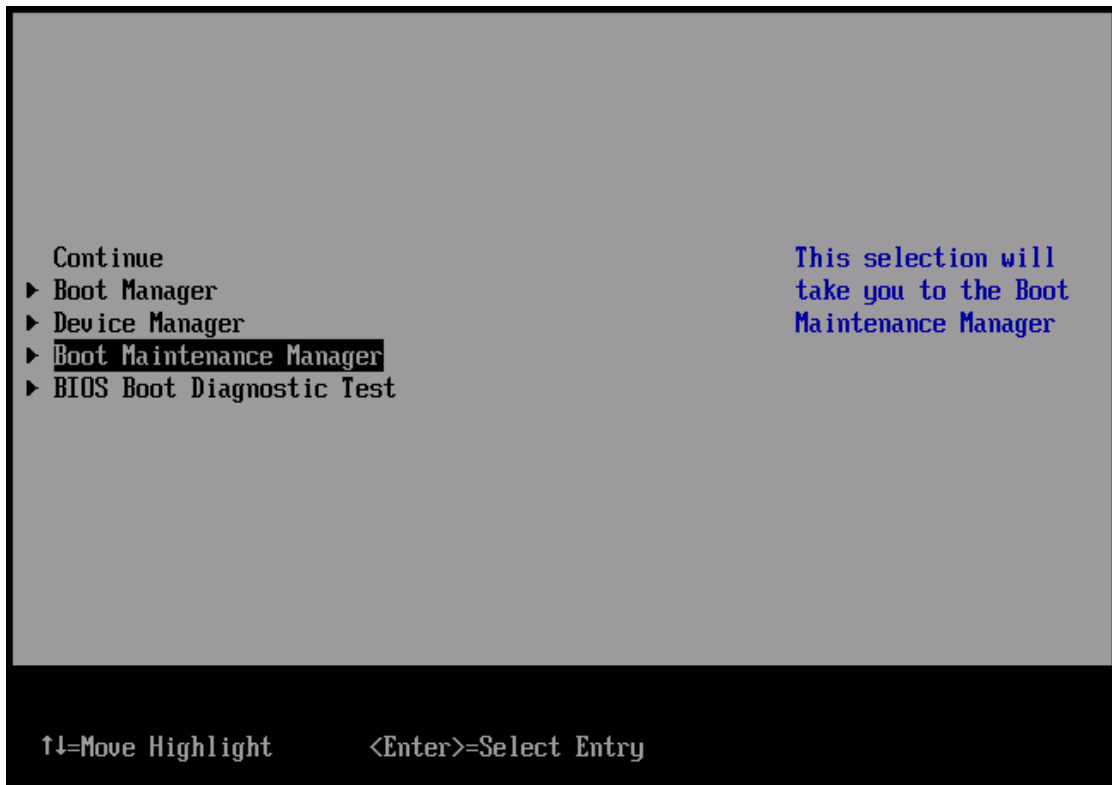


Figure 50.

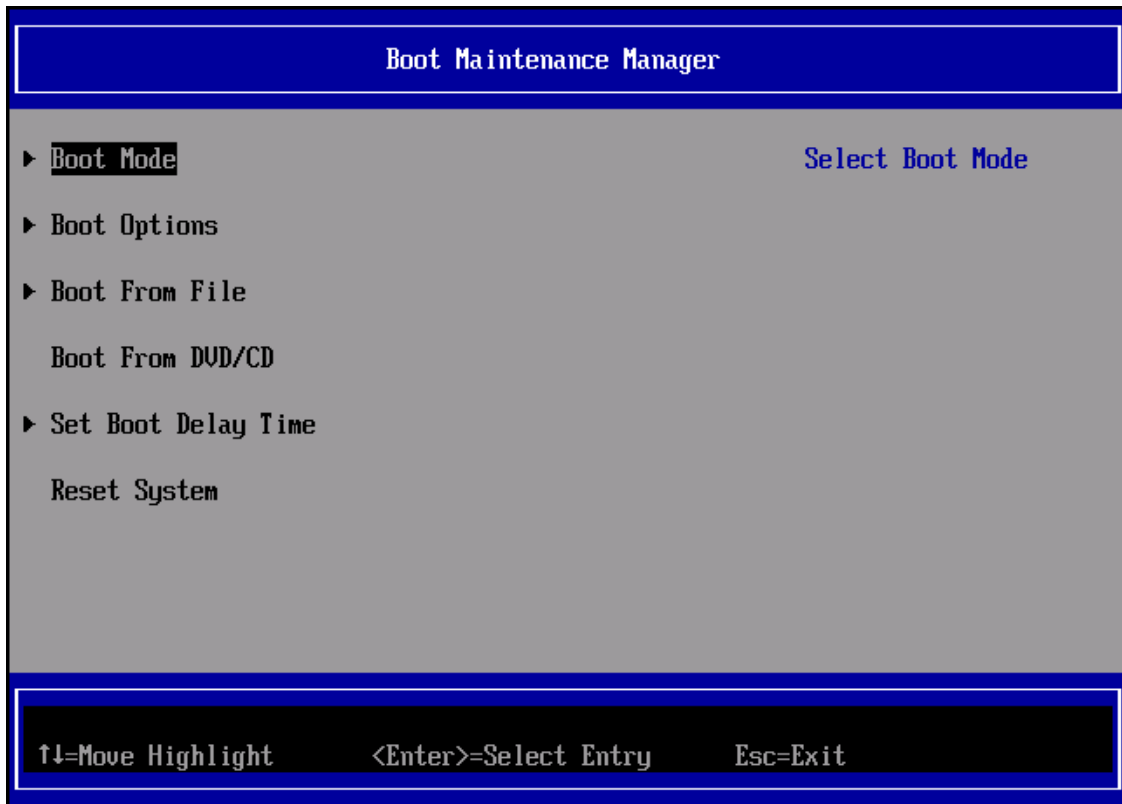
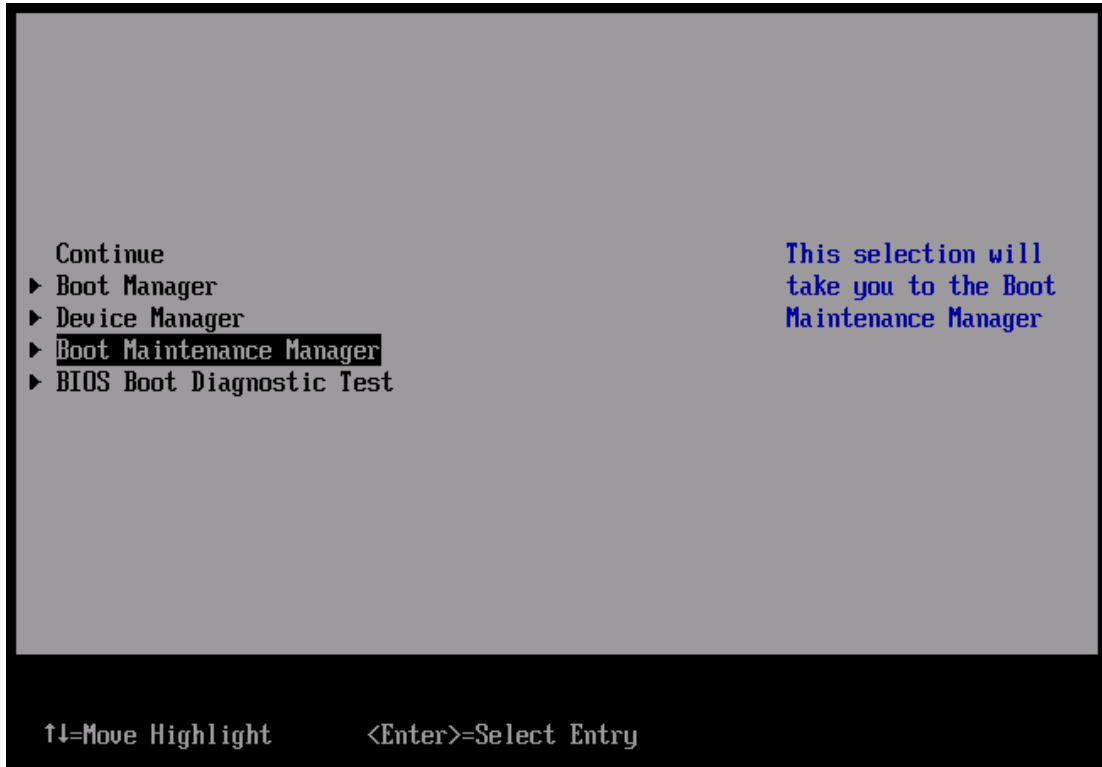


Figure 51.



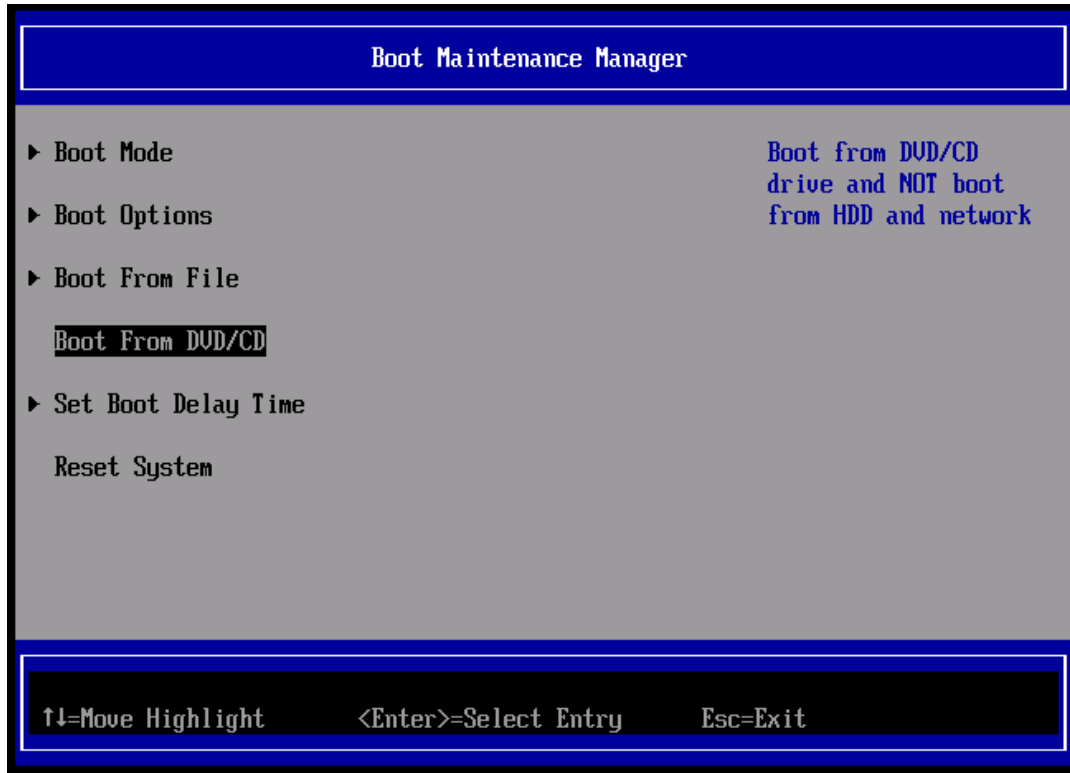
7. Reboot the system and select Boot Maintenance Manager (Figure 52).

Figure 52. Selecting Boot Maintenance Manager



8. Boot the system (Figure 53).

Figure 53. Booting the System



SAN Boot Configuration

This section describes the procedure for installing the SAN boot environment and provides design notes.

Only field engineers should perform the tasks described in this section for this solution, including the options provided by Cisco. Customers must not perform these tasks under any circumstances:

- Newly install or move equipment
- Remove the front, rear, and side covers
- Install or remove built-in options
- Connect or disconnect external interface cables
- Perform maintenance (including repair and periodic diagnosis and maintenance operations)

Overview of Steps for Configuring the SAN Boot Environment

This section describes the flow for configuring the SAN boot environment for the Cisco C880 M4 Server. Follow these steps to configure the SAN boot environment.

Note the following:

- Use a single-path configuration (connection with only one Fibre Channel cable) until the installation of the OS and the multipath driver is complete.
 - After installing the OS and multipath driver, connect the Fibre Channel cable to restore the original state. Then power on the partition of the Cisco C880 M4 again.
 - Register the logical unit number (LUN) that is the destination of the OS installation in all the host bus adapters (HBAs) to be used to start the system.
 - Before turning on the power to the partition of the Cisco C880 M4, confirm that the SAN storage in which the OS will be stored and the Fibre Channel switch are completely ready.
1. Design the SAN boot environment:
 - a. Create a diagram for Fibre Channel cabling between the SAN storage unit and the Cisco C880 M4 in which the SAN boot environment is to be configured. Also create a zone design drawing.
 - b. Design the RAID (LUN_R) settings and partition (LUN) for the SAN storage that stores the target OS for SAN boot.
 2. Configure the settings for the Cisco C880 M4:
 - a. Change the Unified EFI (UEFI) setting of the Cisco C880 M4 Server and the HBA UEFI and extended BIOS settings of the Fibre Channel card.
 - b. Record the World Wide Name (WWN) for each Fibre Channel port. Also record the World Wide Node Name (WWNN) as required.
 3. Configure the settings for the SAN environment:
 - a. Following the Fibre Channel cabling diagram created in step 1, install the SAN storage and Fibre Channel switch and connect them with cables.
 - b. Based on the RAID setting, partition design, and zone information configured in step 1 and on the WWN information recorded in step 2, configure the settings for the SAN storage and Fibre Channel switches.
 - c. In the configuration of the HBA UEFI and extended BIOS of the Fibre Channel card included in the Cisco C880 M4 Server, search for the WWN of the connection destination SAN storage and set it.

4. Install the OS and bundled software:
 1. Use the Synchronous Versatile Input Module (SVIM) to install the OS and bundled software.
 2. Install the multipath driver as required.
 3. Following the Fibre Channel cabling diagram created in step 1, connect the Cisco C880 M4 to the SAN storage and Fibre Channel Fibre Channel switch.
 4. Register the boot disk (the LUN that is the destination of the OS installation) in all the HBAs to be used to start the system.
 5. Register the LUN at the dump output destination on the Fibre Channel card when you configure it for sadump to dump device SAN storage.
6. Configure the SAN boot environment:
 - a. Specify the priority of the boot devices with the UEFI or traditional BIOS of the Cisco C880 M4.

Notes on SAN Boot System Design

Note the following points when designing the SAN boot system:

- Some software may require high performance for Fibre Channel traffic. Be sure to measure Fibre Channel performance on a test system before installing software.
- For SAN storage, the boot disk assigned for each server must be configured so that it can be accessed exclusively by that server. You accomplish this by zoning or masking LUNs or by combining them. (In a SAN boot environment, boot disk LUNs must be configured so that servers and storage have a one-to-one correspondence.)
- Only a single pass is effective for dump output of sadump. Therefore, Even if a pass is cut during dump output, other passes don't become effective. Without continuing, the dump output is failed.
- Only a port on the Fibre Channel card used for an OS start makes the boot setting effective. When boot setting in a port on the Fibre Channel card which isn't used for an OS start (data pass) becomes effective, OS doesn't sometimes start.

Notes on SAN Boot System Installation

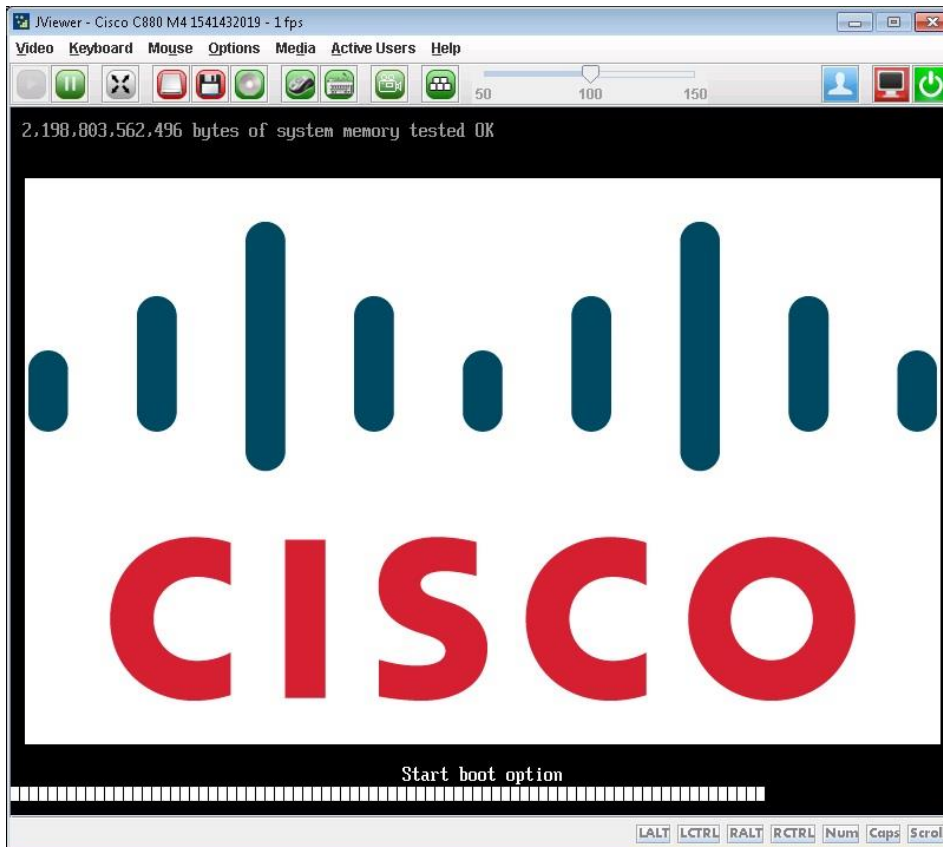
Only the boot disk must be visible during installation of the OS. Disconnect all disks other than the installation destination disk. For a multipath configuration, change to a single-path configuration (only one Fibre Channel cable connected). Also, the settings on the SAN storage side must be configured so that only the boot disk is visible.

Configure the SAN Boot Environment

After the OS is installed, when the system is installed on the UEFI BIOS, you should set the boot path in the boot options.

1. Start the system (Figure 54).

Figure 54. Starting the System



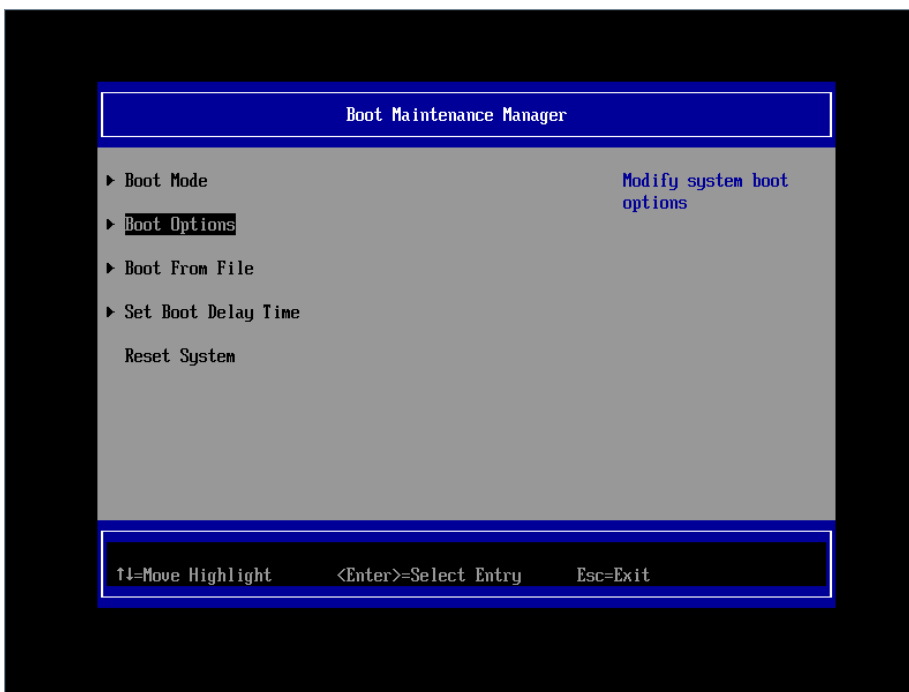
2. When the Cisco logo appears, press any key except the Enter key to display the Boot Manager main page.
3. Select Boot Maintenance Manager (Figure 55).

Figure 55. Selecting Boot Maintenance Manager



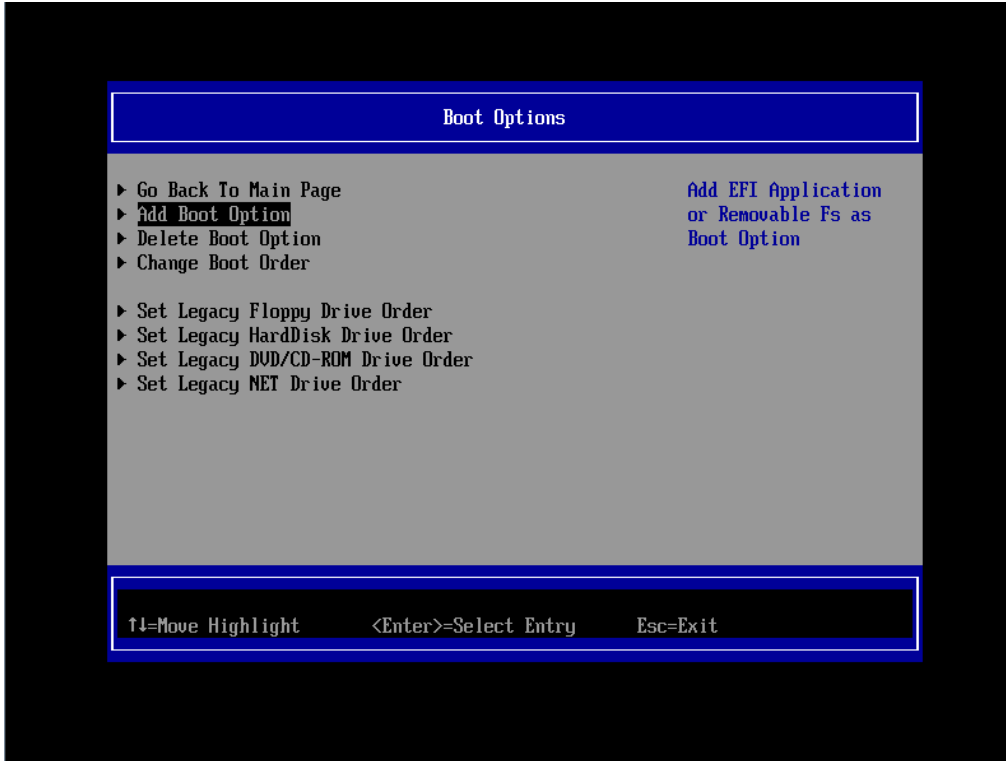
4. On the Boot Maintenance Manager screen, select Boot Options (Figure 56).

Figure 56. Selecting Boot Options



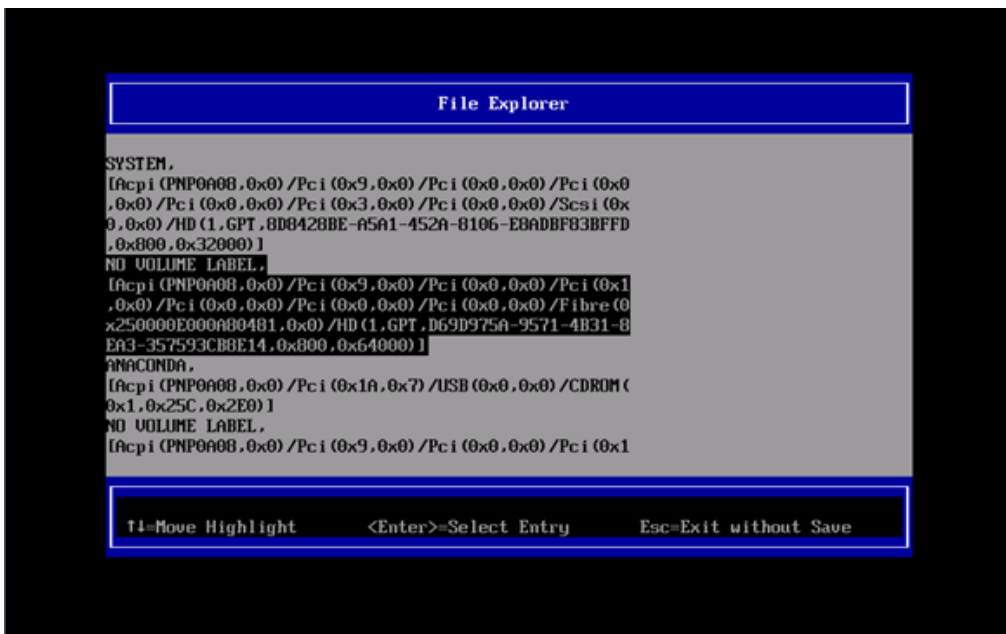
5. On the Boot Options screen, select Add Boot Option (Figure 57).

Figure 57. Selecting Add Boot Option



6. On the File Explorer screen, select Fiber Disk Volume (Main). For .../Fiber (connected to WWN, connected to LUN), select Volume(Main); see Figure 58.

Figure 58.



7. Select the boot file and press Esc several times. The selection hierarchy and the file differ depending on the OS. For example, for an RHEL server, select <EFI> and then <redhat> and then grub.efi (Figures 59, 60, and 61).

Figure 59. Selecting the Boot File (1)



Figure 60. Selecting the Boot File (2)

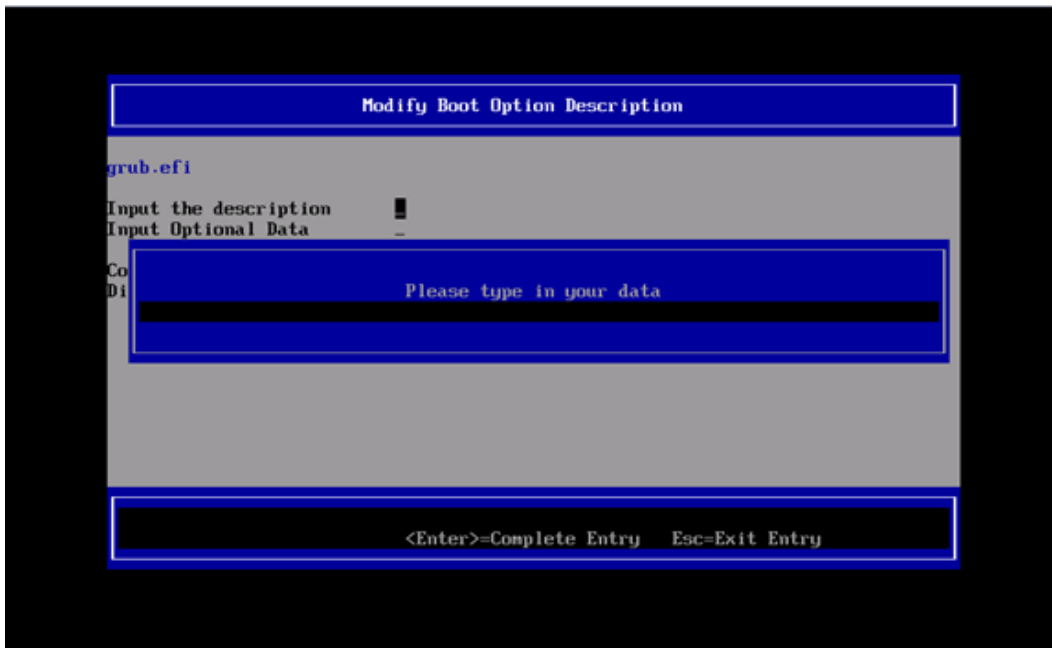


Figure 61. Selecting the Boot File (3)



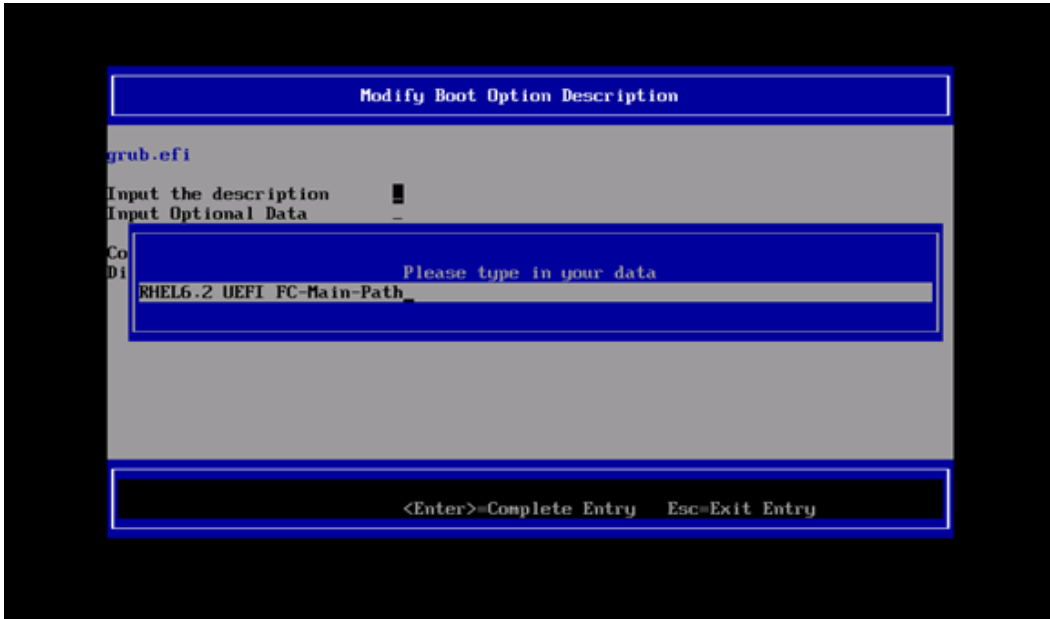
8. On the Modify Boot Option Description screen, select "Input the description" and then press the Enter key (Figure 62).

Figure 62. Getting Ready to Enter a Description



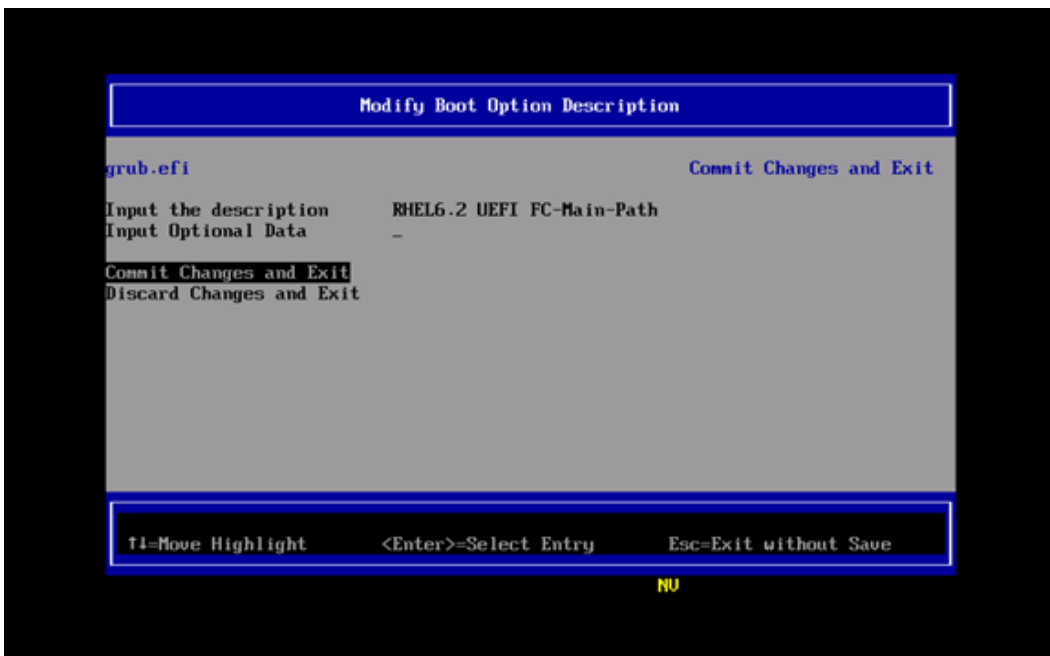
9. On the "Please type in your data" screen, enter <<Boot Option Name (Main)>> (Figure 63). The boot option name should contain five or more characters.

Figure 63. Entering the Main Boot Option Name



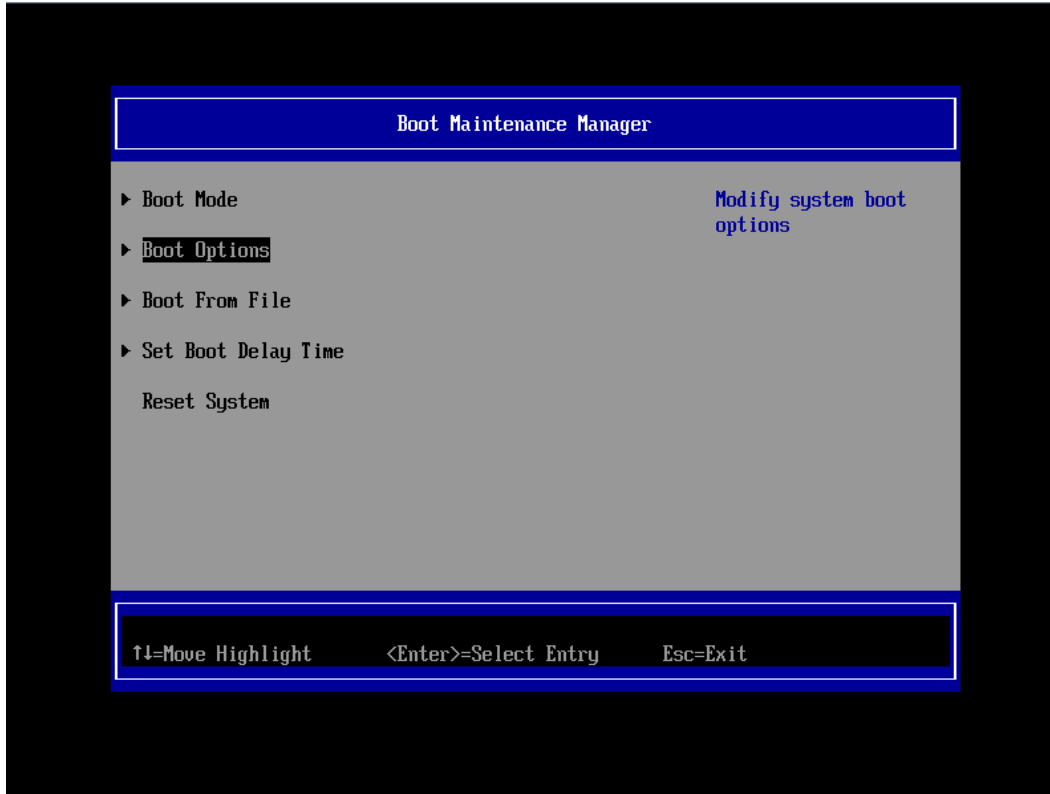
10. On the Modify Boot Option Description screen, select Commit Changes and Exit and then press the Enter key (Figure 64).

Figure 64. Saving the Changes



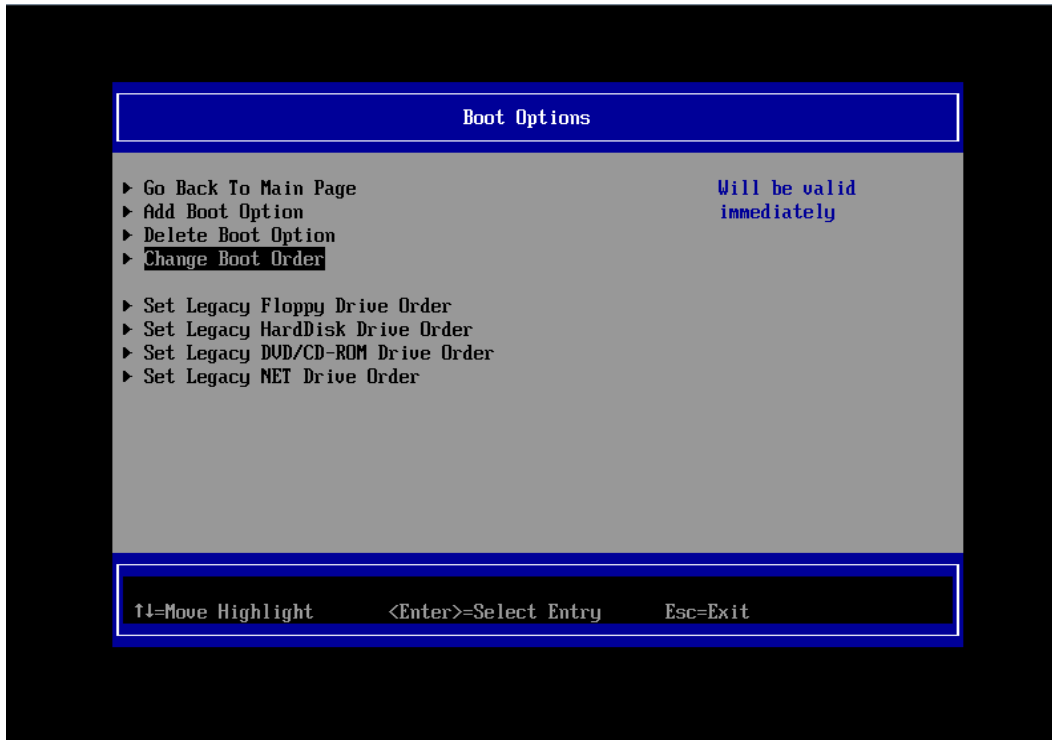
11. Repeat steps 6 through 10 to set up Boot Option (Sub).
12. On the Boot Maintenance Manager screen, select Boot Options (Figure 65).

Figure 65. Selecting Boot Options



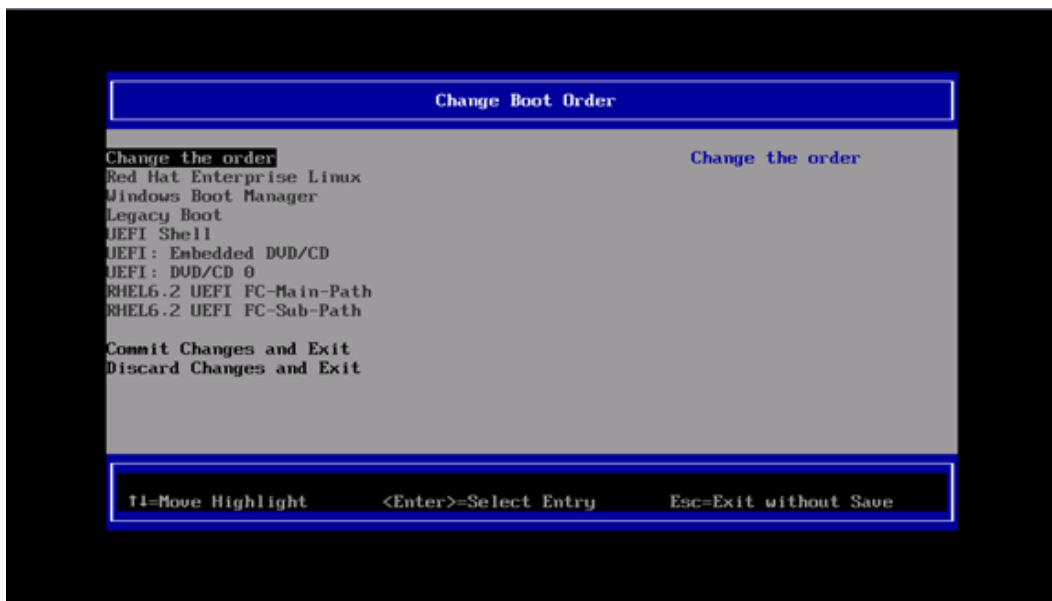
13. On the Boot Options screen, select Change Boot Order (Figure 66).

Figure 66. Selecting Change Boot Order



14. On the Change Boot Order screen, select "Change the order" (Figure 67).

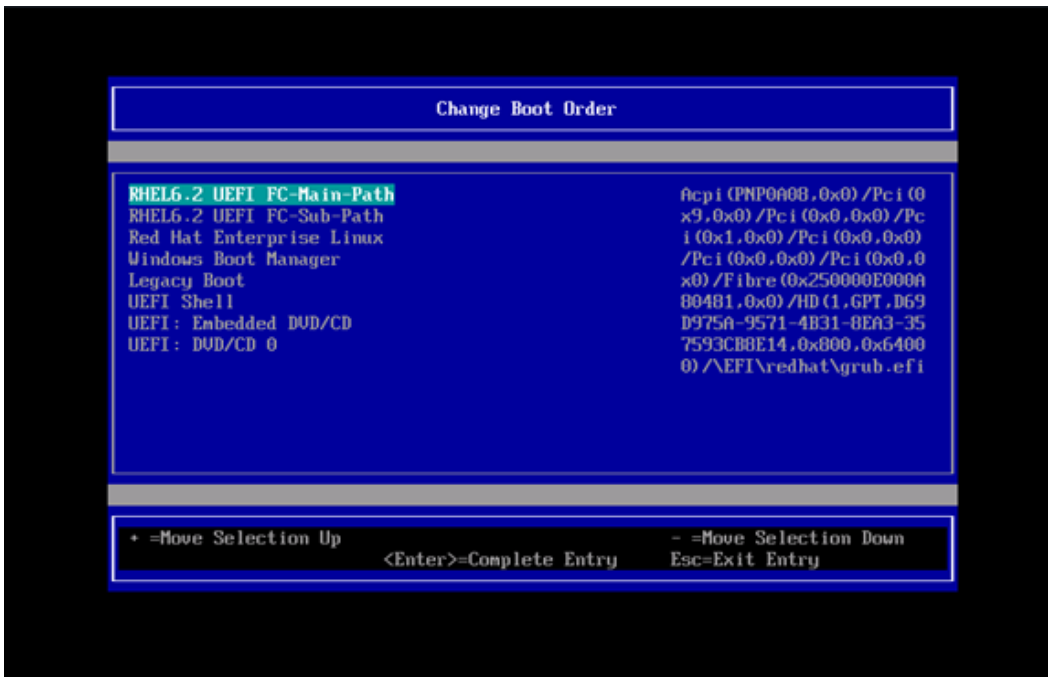
Figure 67. Changing the Boot Order



15. On the Change Boot Order screen, press the + key or the - key and set the boot priority as follows (Figure 68):
- Move <<Boot Option Name (Main)>> to the top.

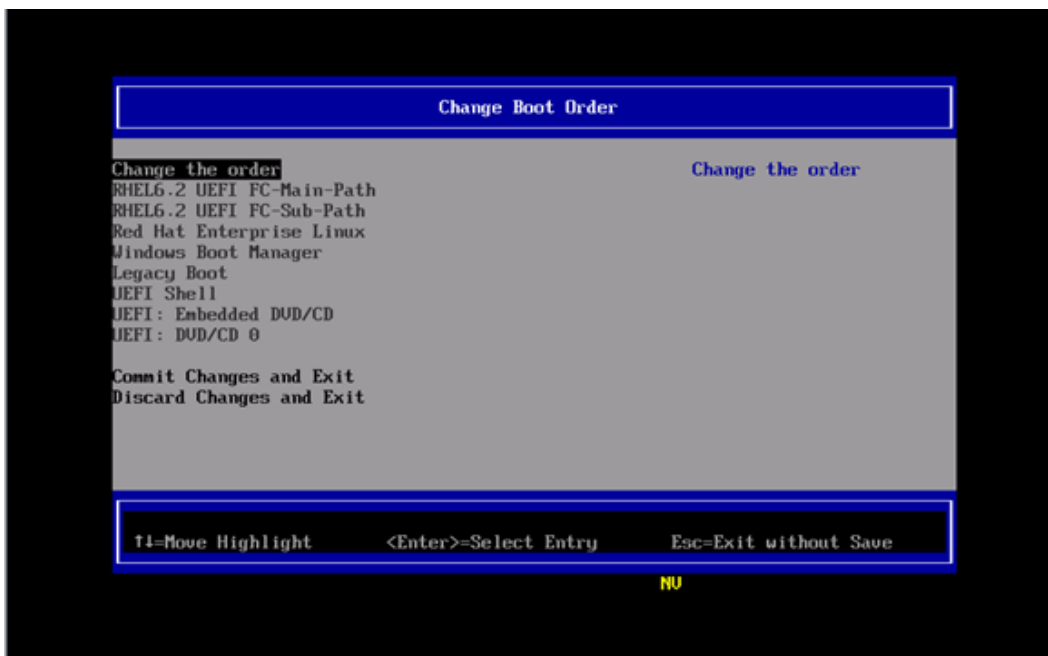
- b. Move <<Boot Option Name (Main)>> so that it is second from the top.

Figure 68. Setting the Boot Priority



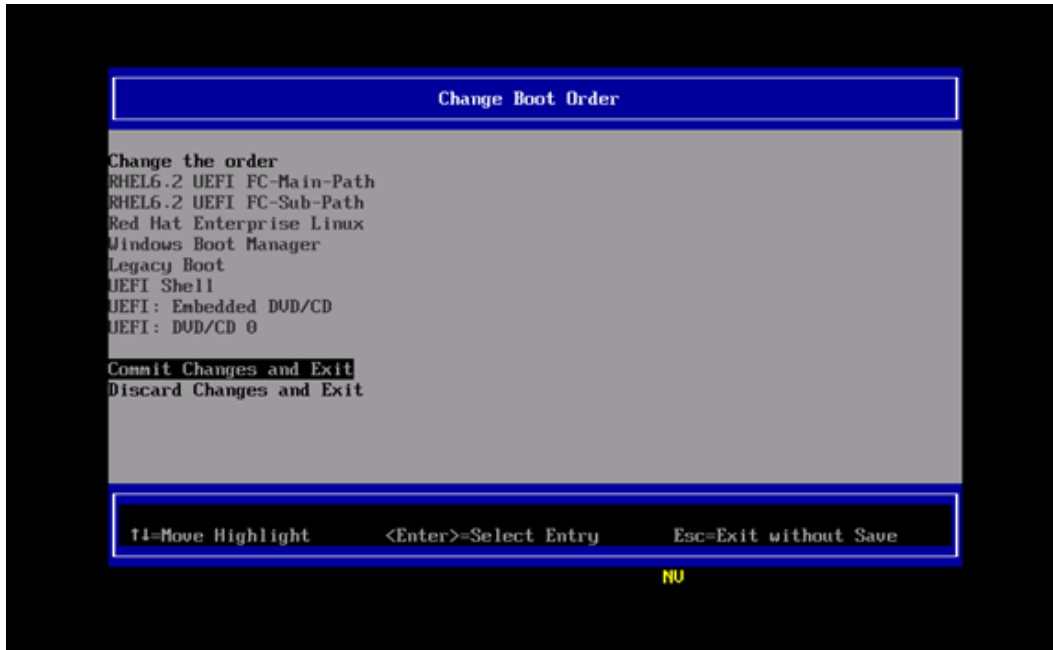
- 16. After modifying the boot priority, press the Enter key (Figure 69).

Figure 69.



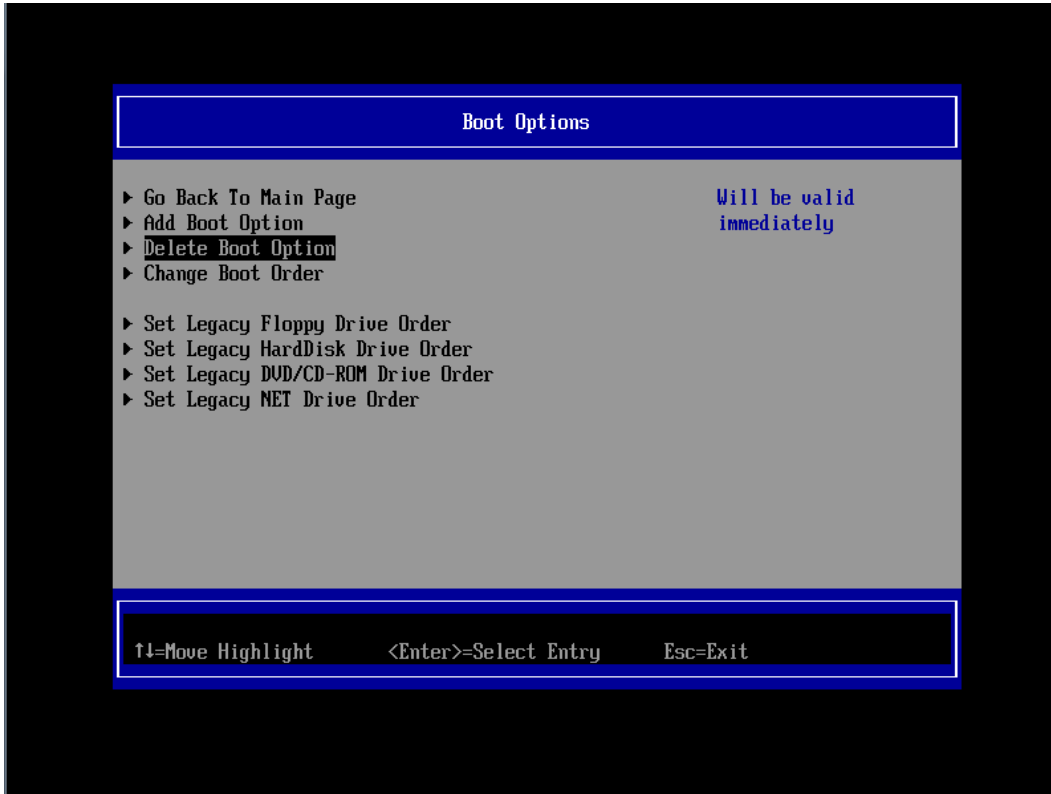
- 17. On the Change Boot Order screen, select Commit Changes and Exit and then press the Enter key (Figure 70).

Figure 70. Saving the Changes



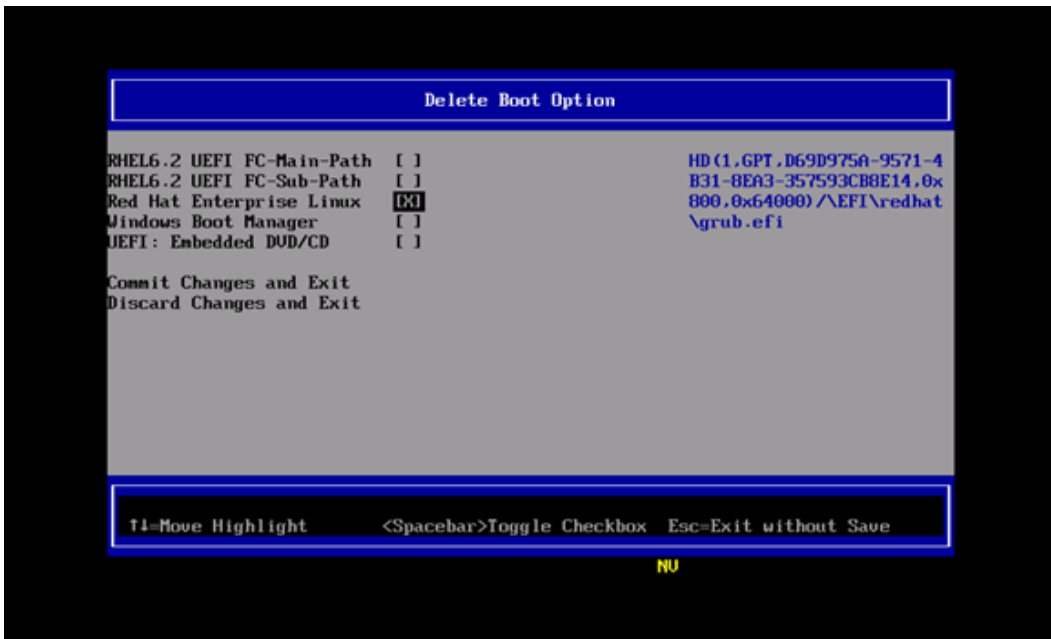
18. On the Boot Maintenance Manager screen, select Boot Options.
19. On the Boot Options screen, select Delete Boot Option (Figure 71).

Figure 71. Selecting Delete Boot Option



20. On the Delete Boot Options screen, select the ID boot option, which is set when you install the OS (Figure 72). Press the Enter key to delete it (the ID boot option is shown as an entry named HD(...)).

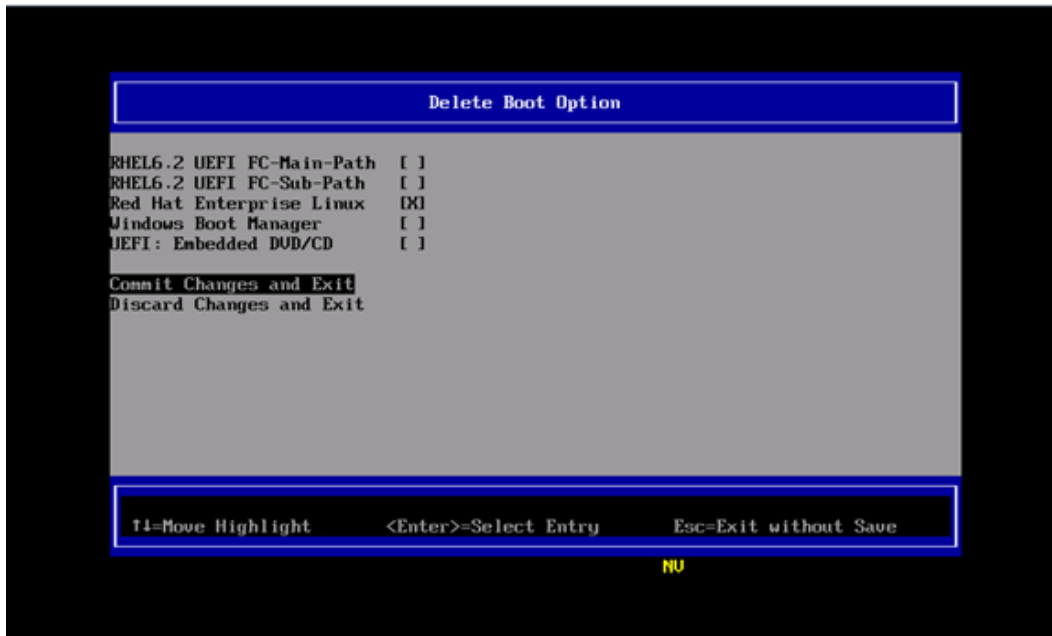
Figure 72. Deleting the ID Boot Option



NU

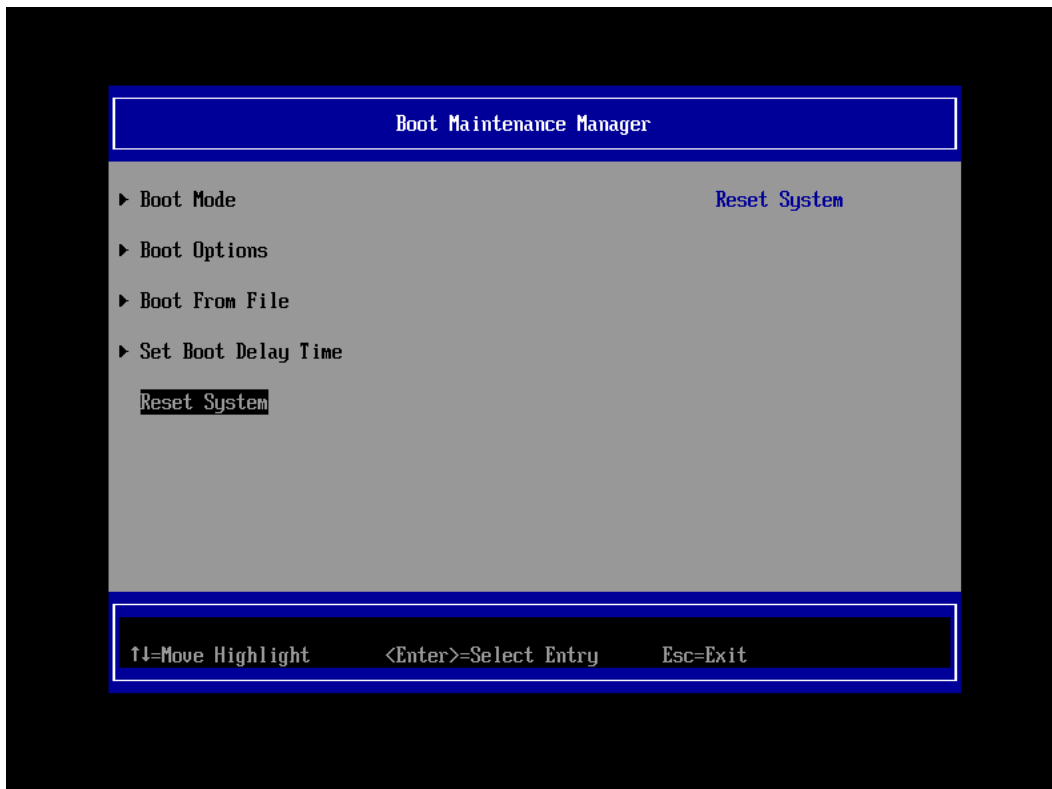
21. On the Delete Boot Option screen, select Commit Changes and Exit (Figure 73).

Figure 73. Saving the Changes



22. On the Boot Maintenance Manager screen, select Reset System (Figure 74). Then reboot the system.

Figure 74. Selecting Reset System



23. If you made the configuration changes listed here, initialize the settings on the Fibre Channel card after introducing the system. The Fibre Channel card configurations are reset. When the resetting is complete, reboot system.

- When a sadump dump device is registered with a Fibre Channel card
- When SAN storage and settings in the Fibre Channel switch were changed (LUN mapping was changed)
- When host affinity, port zoning, etc. were changed
- When the OS that starts by configuration change is changed
- When you register the device to the Fibre Channel card to add the LUN device

For more information about initialization of the Fibre Channel card, refer to the section “Initialization of the Fibre Channel Card.”

For information about resetting the Fibre Channel card, see the following sections in this document:

- “Settings on the 8-Gbps Fibre Channel Card”
- “16-Gbps Fibre Channel Card Settings”

Notes on SAN Boot System Operation

Note the following points when operating the SAN boot system:

- Be sure to confirm that the SAN storage and Fibre Channel switch are both in the Ready state.
- Use the MMB web user interface to set the time period until the partition is powered on.
- When the partition is started, the boot disk may not be found. In this case, reset the partition from the UEFI.
- Record the dates and times of server switching (Fibre Channel card replacement and moves) on separate media. Prepare this media to protect against the possibility that a faulty part of the hardware can no longer be located after event log primary analysis, a hardware failure, or the occurrence of some other problem.
- When the Fibre Channel card has been replaced with a maintenance part, the HBA UEFI or traditional BIOS must be reset. Also, the SAN storage unit must be reset.
- In the SAN boot environment, an OS boot may fail depending on the quality of the Fibre Channel transmission path. In such a case, use the Fibre Channel switch and SAN storage unit to check the alarm or system status and identify the faulty part. Then in the Power Control window of the MMB web user interface, select Reset to restart the system.
- In a Linux environment, a SAN boot in a multipath configuration can be performed. To start in Rescue mode and automatically mount the SAN disk in such a case, enable only one Fibre Channel port in advance of startup. If the multipath configuration is left as is, the system may fail to start normally. Even if you do not use automatic mounting, you should enable only one Fibre Channel port in advance of startup in Rescue mode to prevent operational errors. For details, see the section “Notes on SAN Boot System Installation.”

16-Gbps Fibre Channel Card Settings: UEFI Driver Version 6.11a5 or Later

This section describes the settings on the 16-Gbps Fibre Channel card in the Cisco C880 M4 Server. With these settings, the system starts from a LUN of the SAN storage unit in the Fibre Channel SAN boot environment.

Set UEFI Driver Version 6.11a5 or Later on the 16-Gbps Fibre Channel Card

This section describes the procedure for setting UEFI Driver Version 6.11a5 or later.

To start the system from a LUN of the SAN storage unit in the SAN boot environment, the process described here is required for all HBAs to be used to start the system. Running this process registers in the HBA the SAN storage unit LUN from which the system is to be started.

The figures in this section use UEFI Driver Version 6.11a5. All screenshots in the figures are examples only, and contents may vary depending on the system configuration, etc.

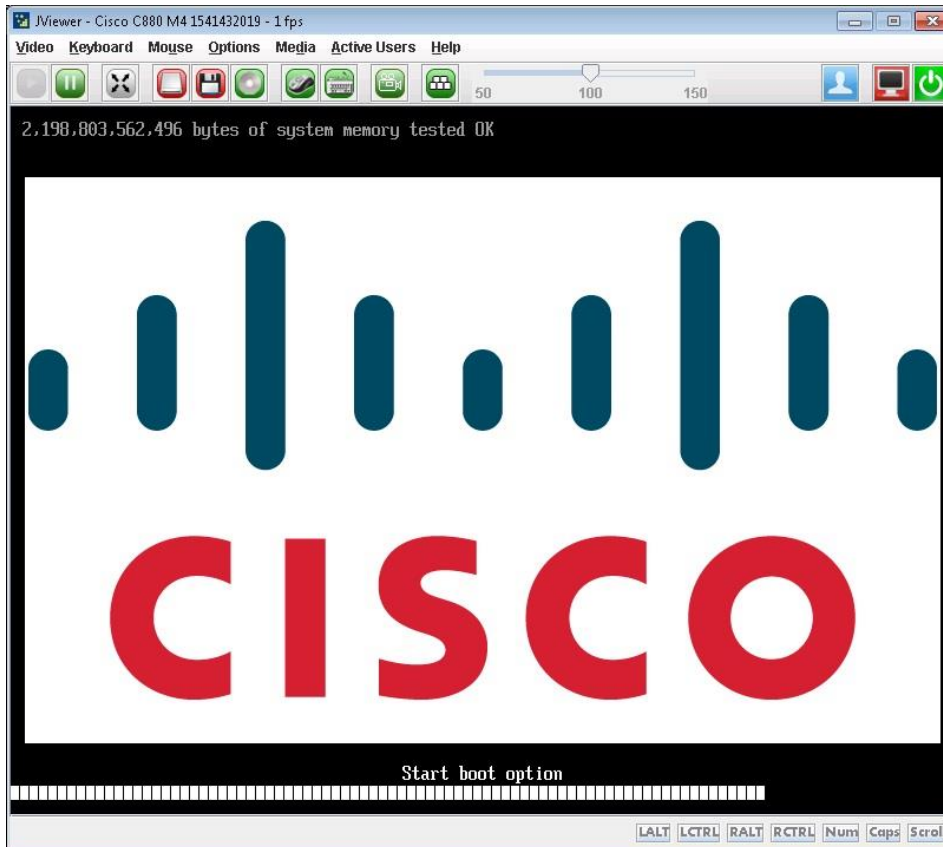
Note the following:

- To add sadump as the dump device for the SAN, you must set the LUN by selecting Add Boot Device in the UEFI driver utility.
- You must set the Fibre Channel card on each port.

When a setting is added or changed, the partition must be rebooted. Perform the operations here after rebooting the relevant partition.

1. Reboot the system.
2. When the Cisco logo appears, press any key except the Enter key (Figure 75).

Figure 75.



If you don't perform this step, the dump device is not added.

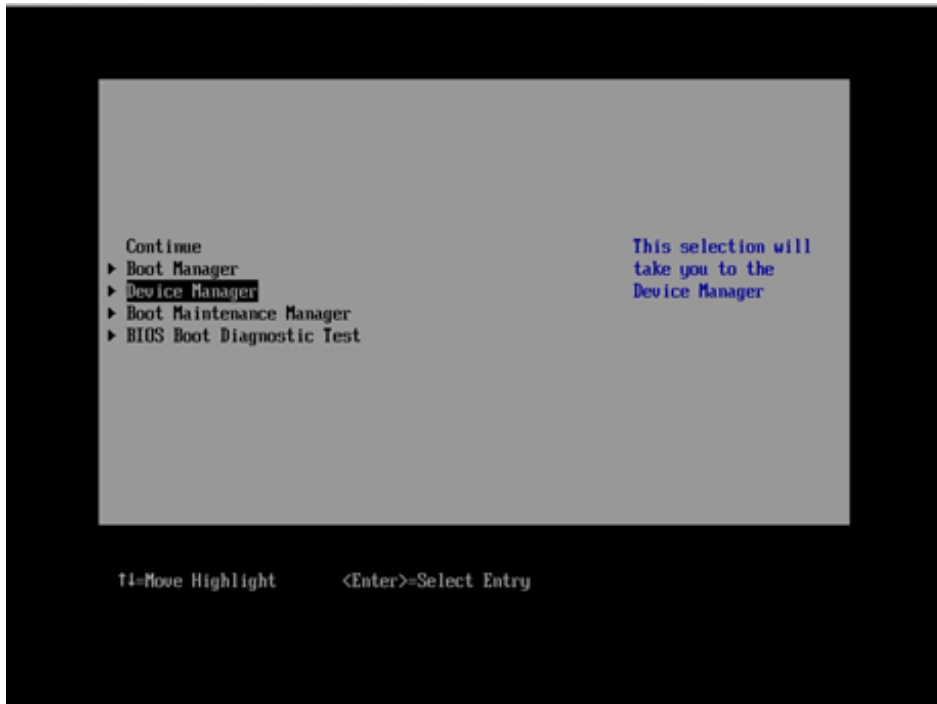
Note that you cannot mix different 16-Gbps Fibre Channel card firmware versions in a single server. You also cannot mix different boot BIOS driver versions in a single partition. If you have different versions of the 16-Gbps Fibre Channel card firmware or UEFI driver, install the same version of the firmware driver in the server and partition.

Select the Method for Configuring the 16-Gbps Fibre Channel Card

Check the UEFI driver version from the Device Manager screen of the Boot Manager main page.

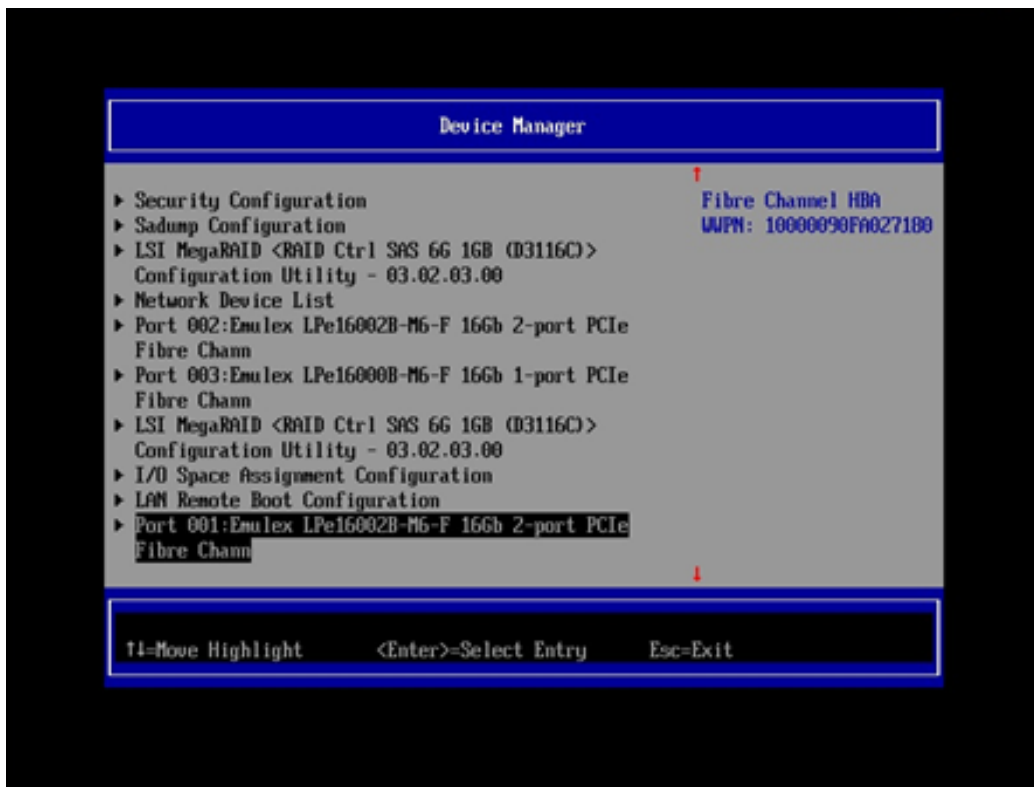
1. From the Boot Selector screen in the Power Control window of the MMB, select "Force boot into EFI Boot Manager." Then turn on the power. Start the UEFI shell.
2. The Boot Manager main page appears. Select Device Manager and then press the Enter key (Figure 76).

Figure 76. Selecting Device Manager



The Device Manager screen appears (Figure 77).

Figure 77. Device Manager Screen



Note the following points when using UEFI Driver Version 6.11a5 or later to set a SAN boot configuration on the 16-Gbps Fibre Channel card. Refer to Display Adapter Info on the Port 001:Emulex LPe16002B-M6-F 16Gb 2-port PCIe Fiber Chann screen to check the UEFI driver version.

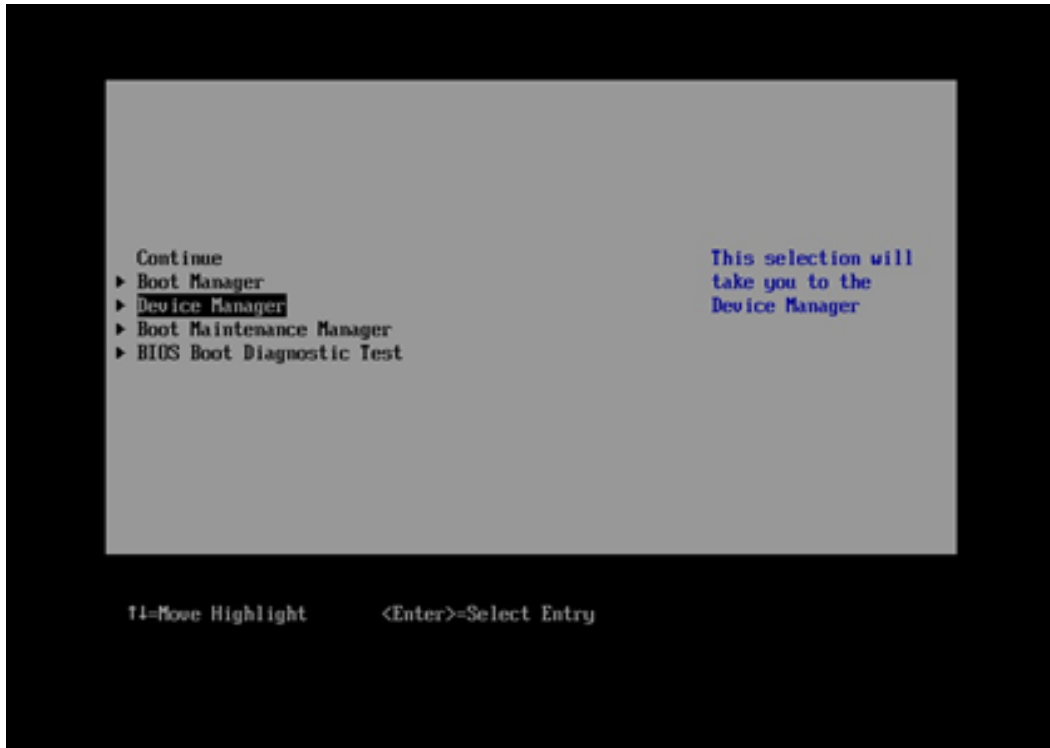
- Before deleting a registered boot entry with the Delete Boot Device process, be sure to change the BIOS setting (Set Boot from SAN) to Disable.
- Running the Delete Boot Device process with Enable as the BIOS setting (Set Boot from SAN) may sometimes render the Emulex Configuration Utility inoperable. In such a case, in the Power Control window of the MMB web user interface, select Reset to restart the system. Then reenter the settings for the 16-Gbps Fibre Channel card.

Display the Device Manager

Display the Device Manager screen.

1. Select Device Manager (Figure 78).

Figure 78. Selecting Device Manager



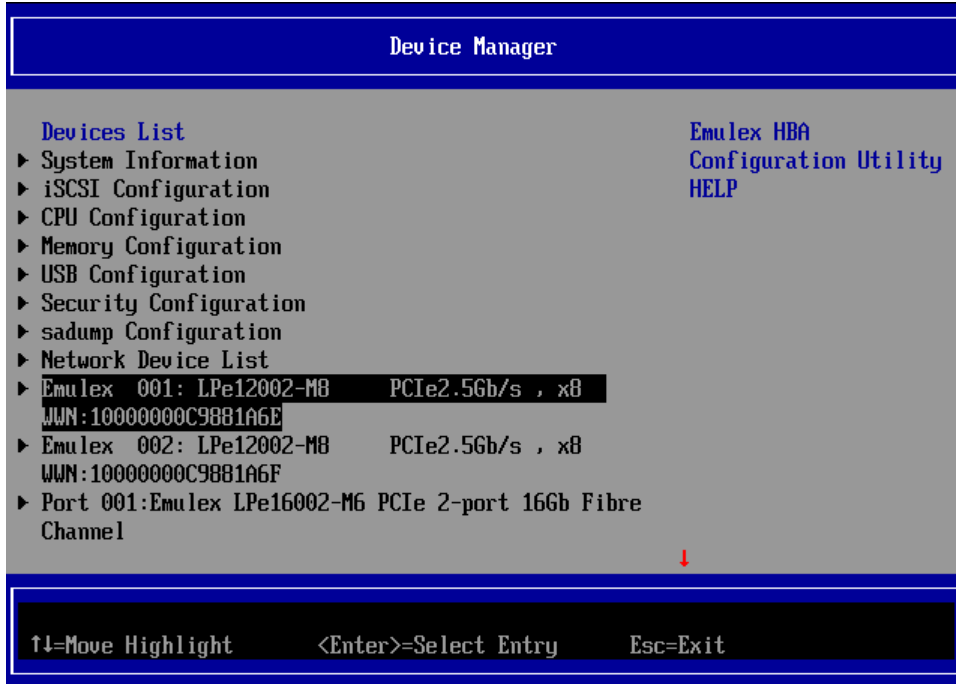
2. Press the Enter key. The Device Manager screen appears.

Start the HBA Setup Utility and Select the HBA

Now set up the HBA. The Device Manager screen displays the list of HBAs to be set.

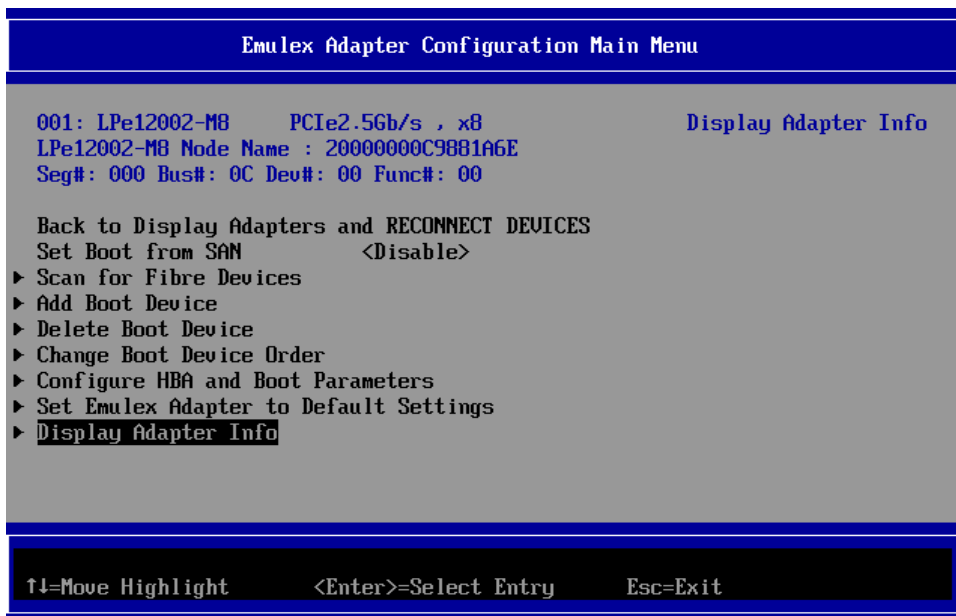
1. Select Port 001:Emulex LPe16002B-M6-F 16Gb 2-port PCIe Fiber Chann. (Figure 79). In the example here, port 0 of the LPE16002B-M6-F dual-port Fibre Channel card is selected.

Figure 79. Selecting the HBA



2. Press Enter. The Emulex Adapter Configuration Main Menu screen is displayed (Figure 80).

Figure 80. Emulex Adapter Configuration Main Menu Screen

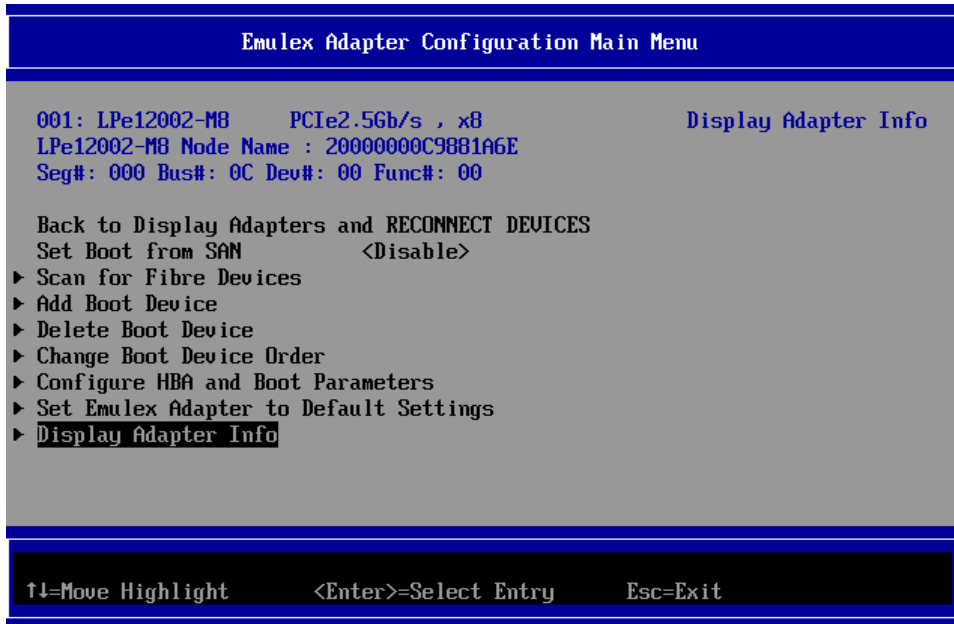


Acquire an HBA WWN

Confirm the WWN of the HBA for which setup is currently being performed.

1. Select Display Adapter Info (Figure 81). The WWN of the HBA is displayed as the node name.

Figure 81. Selecting Display Adapter Info



2. Check the information. The MMB web user interface displays the slot containing the mounted HBA as the PCI-Express Slots item whose Seg, Bus, and Dev values match the Seg#, Bus#, and Dev# values on the Emulex Adapter Configuration Main Menu screen.

Note that the I/O Unit (IOU) and PCI_Box screens of the System menu display the PCI-Express Slots items. The Emulex Fibre Channel EFI-Bios Utility screen uses hexadecimal notation for the displayed values, and the MMB web user interface uses decimal notation (Table 3).

Table 3. MMB Web User Interface Display

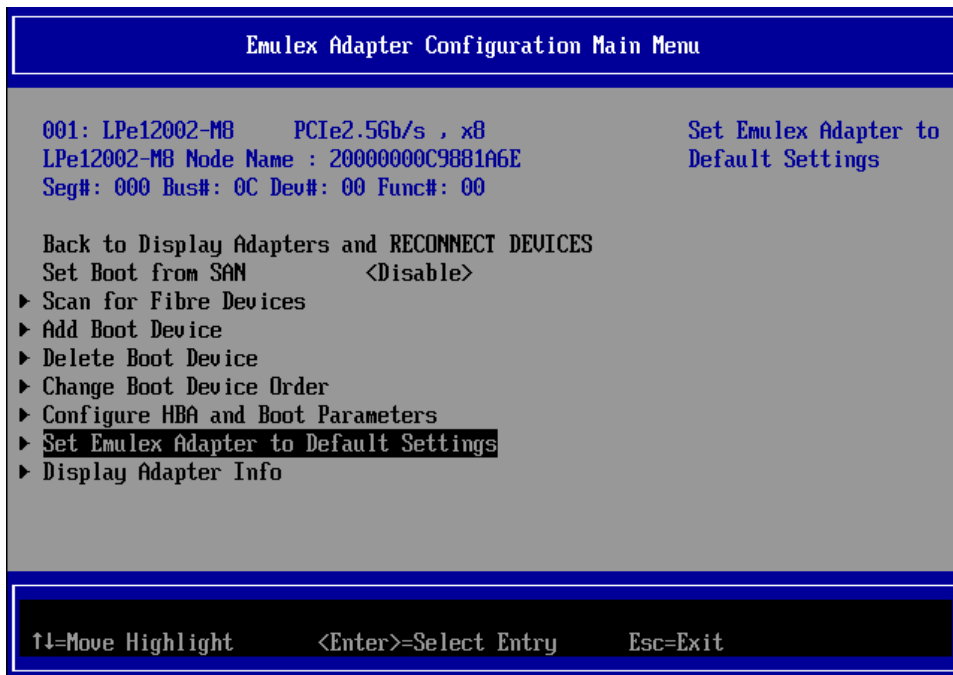
PCI Express (PCIe) Slots					
PCI Slot Number	Power Status	Slot Status	Link Width	Seg/Bus/Dev	PCIe Card Information
					Firmware Version
0	Standby	Not present			
1	On	OK	x8	0/13/0	-
2	On	OK	x8	0/14/0	-
3	Standby	Not present			

Initialize the HBA Settings

An HBA that has just been shipped from the factory has initialized settings and does not require the steps listed here. Perform these steps to restore the default adapter settings.

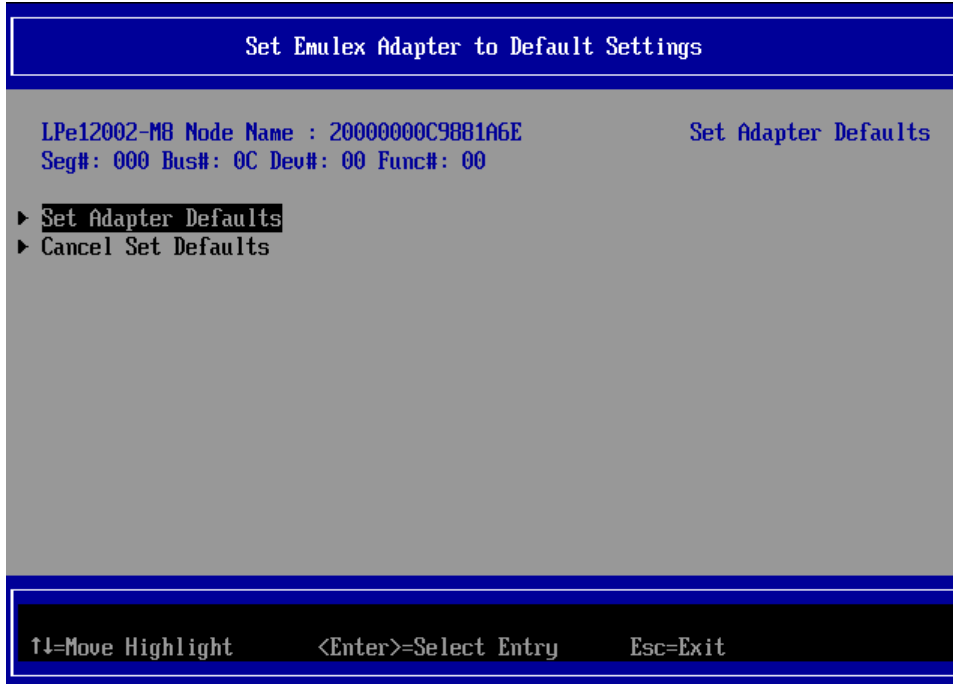
1. Select Set Emulex Adapter to Default Settings and then press the Enter key (Figure 82).

Figure 82. Selecting Set Emulex Adapter to Default Settings



2. The Set Emulex Adapter to Default Settings screen appears. Select Set Adapter Defaults and then press the Enter key (Figure 83).

Figure 83. Selecting Set Adapter Defaults



After the initialization is complete, you are returned to the Adapter Selection screen.

Enable the BIOS

Enable the HBA BIOS so that the HBA can recognize the LUNs of the SAN storage unit and so that the system can be started from one of them.

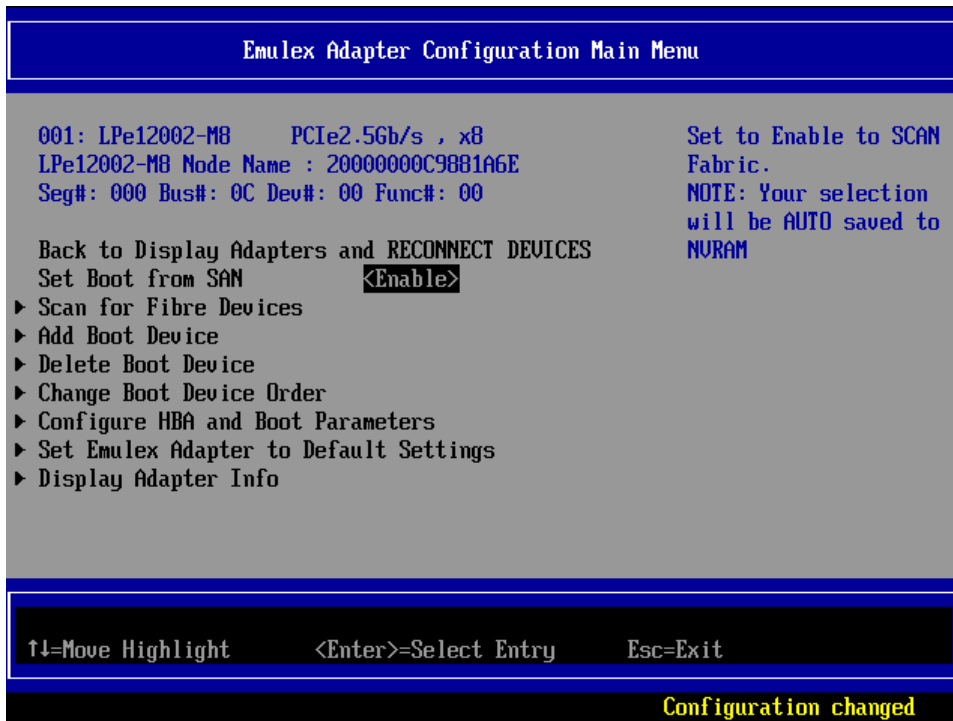
1. On the Emulex Adapter Configuration Main Menu screen, select Set Boot from SAN <Disable>.
2. The screen for selecting Disable or Enable appears. Select Enable and then press the Enter key (Figure 84).

Figure 84. Enabling the Adapter



3. Confirm that Set Boot from SAN < Enable > is displayed (Figure 85).

Figure 85. Confirming That Set Boot from SAN Is Enabled



Set the Link Speed and Topology

This section describes how to configure the speed and topology settings.

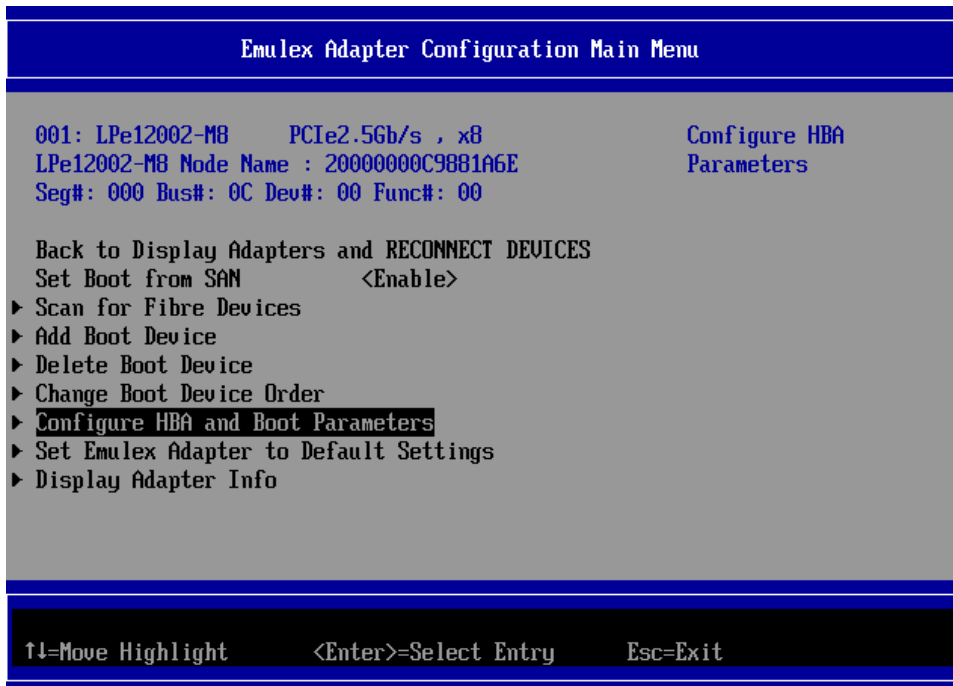
Note: When you connect a 16-Gbps Fibre Channel card to storage that supports 16 Gbps, you have to connect using a Fibre Channel switch. In this case, a conventional Fibre Channel Arbitrated Loop (FCAL) connection is not supported. If you use a 16-Gbps Fibre Channel card with the link speed slowed to 4 or 8 Gbps, you can use a FCAL connection.

Set a Static Topology

On the Emulex Adapter Configuration Main Menu screen, configure the settings that correspond to the connection pattern (fabric connection or FCAL connection).

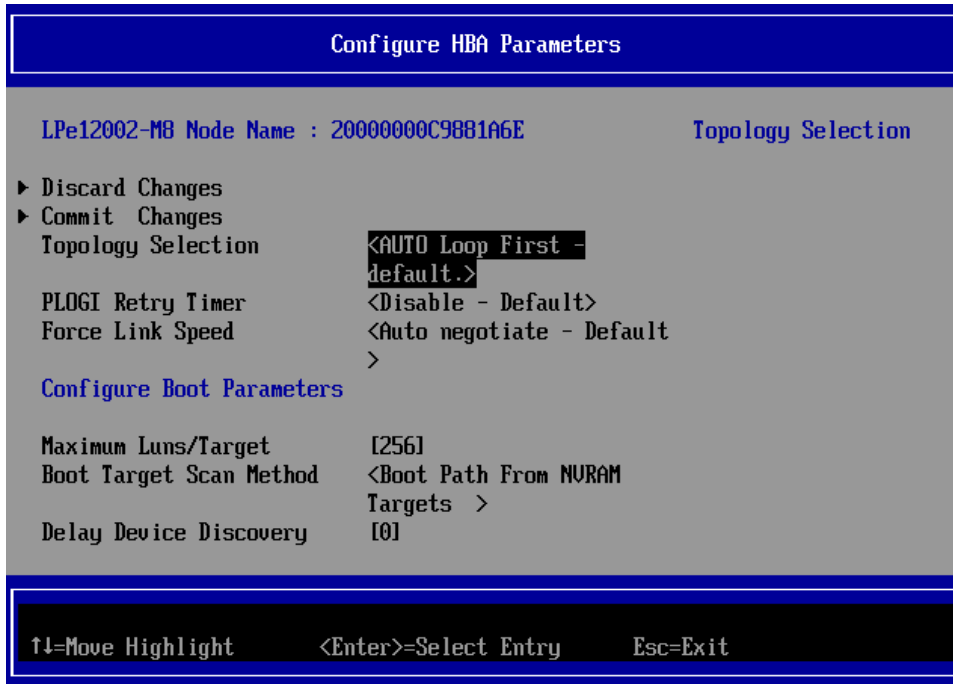
1. Select Configure HBA and Boot Parameters and then press the Enter key (Figure 86).

Figure 86. Selecting Configure HBA and Boot Parameters



2. For Topology Selection, select <AUTO Loop First – default.> and then press the Enter key (Figure 87).

Figure 87. Selecting the Topology



3. Select the connection method and then press the Enter key. Change the setting from the default setting of <AUTO Loop First – default.> as follows:
 - For a fabric connection, select the Point to Point option (Figures 88 and 89).
 - For a FCAL connection, select the FCAL option (for 4- and 8-Gbps connections only).

Figure 88. Setting a Fabric Connection



Figure 89. Point-to-Point Topology Displayed



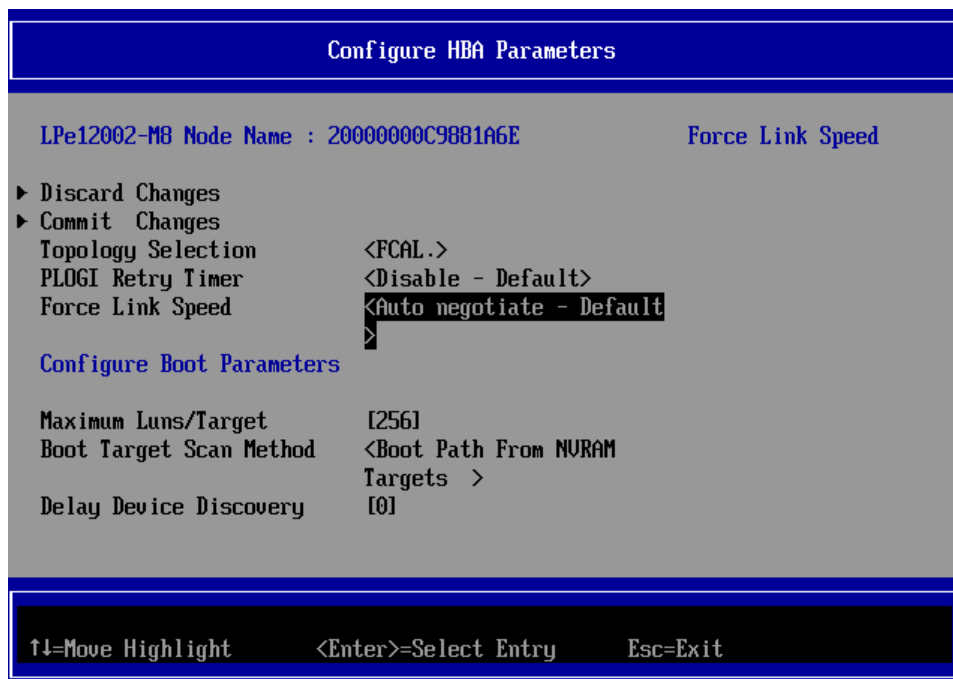
Set a Static Link Speed

With an EFI BIOS, configure the following settings that correspond to the connection link speed (4, 8, or 16 Gbps).

Note: Do not set Auto negotiate - Default. First, set the fixed link speed. Otherwise, the connected device will not be recognized.

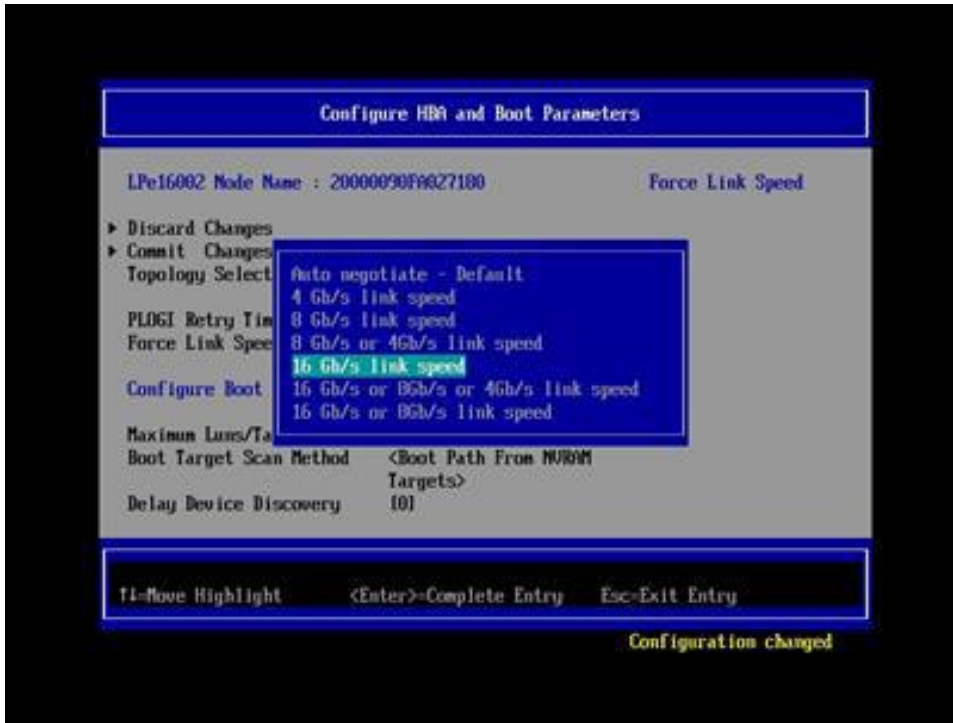
1. Select Force Link Speed <Auto negotiate – Default> and then press the Enter key (Figure 90).

Figure 90. Static Link Speed Setting (1)



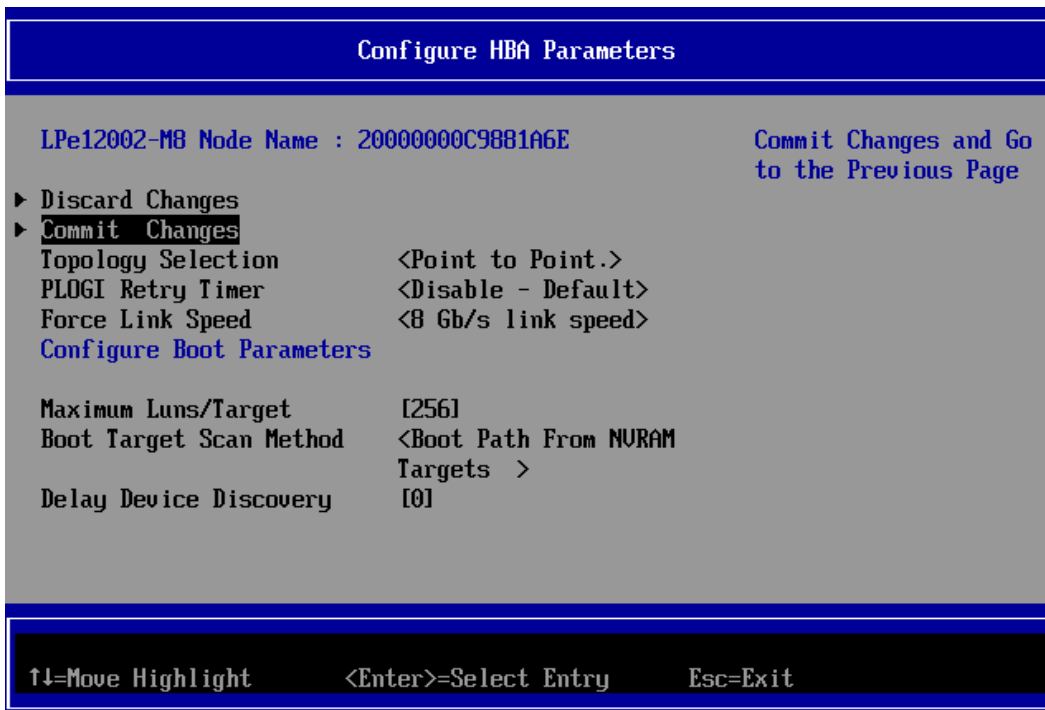
2. Select the link speed that corresponds to the connection environment (connected Fibre Channel switch or SAN storage unit) and then press the Enter key (Figure 91).

Figure 91. Static Link Speed Setting (2)



3. Confirm that the specified link speed is displayed for [Force Link Speed (Figure 92).

Figure 92. Topology and Link Speed Change Confirmation (1)



4. Commit the changes. After the completion of the Commit Changes process, you are returned to the Port 001:Emulex LPe16002B-M6-F16Gb 2-port PCIe Fiber Chann screen (Figure 93).

Figure 93. Topology and Link Speed Change Confirmation (2)



Note that after you change the Topology Selection or Force Link Speed settings and then select Discard Changes, if you are returned to the screen for changing settings, the changes to the 16-Gbps Fibre Channel card settings have been discarded. However, you may still see the changed settings displayed by the utility. In this case, select the 16-Gbps Fibre Channel card again from the menu as described earlier in the section “Start the HBA Setup Utility and Select the HBA” before proceeding.

Set the Boot Device

Now set the boot device.

1. On the Port 001:Emulex LPe16002B-M6-F 16Gb 2-port PCIe Fiber Chann screen, select Scan for Fiber Devices and then press the Enter key (Figure 94).

Figure 94. Boot Device Settings (1)



During the search process, "Please Wait" is displayed.

2. Press the Esc key or select Go to Configuration Main Menu to return the previous page. Then press the Enter key (Figure 95).

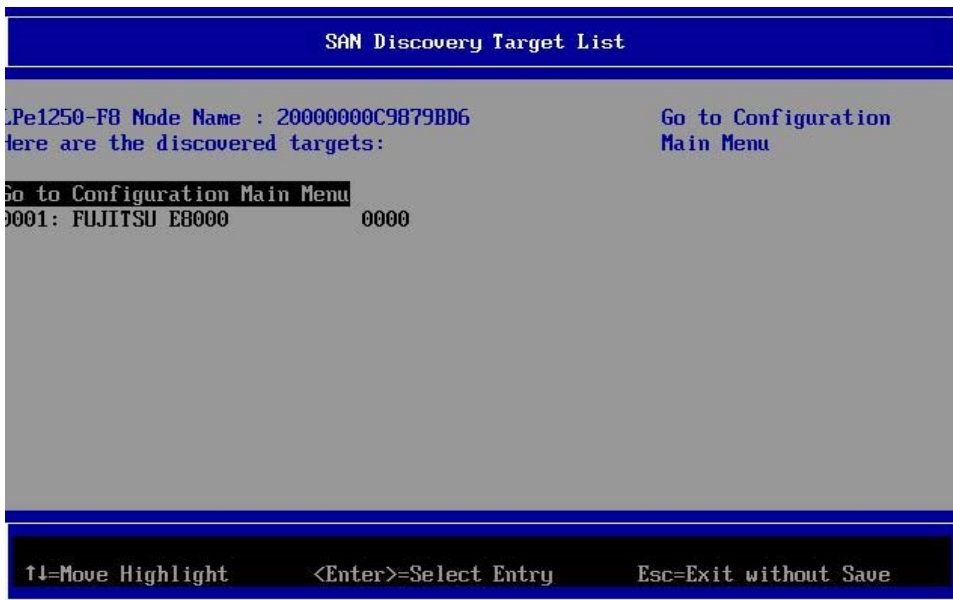
Figure 95. Boot Device Settings (2)



Note: If the expected Fibre Channel device is not displayed, the SAN storage or physical connection setting of the Fibre Channel switch may be incorrect. Confirm these settings again.

3. On the Configuration Main Menu screen, press the Enter key (Figure 96).

Figure 96. Boot Device Settings (3)



- The Emulex Adapter Configuration Main Menu screen appears. Select Add Boot Device and then press the Enter key (Figure 97).

Figure 97. Boot Device Settings (4)



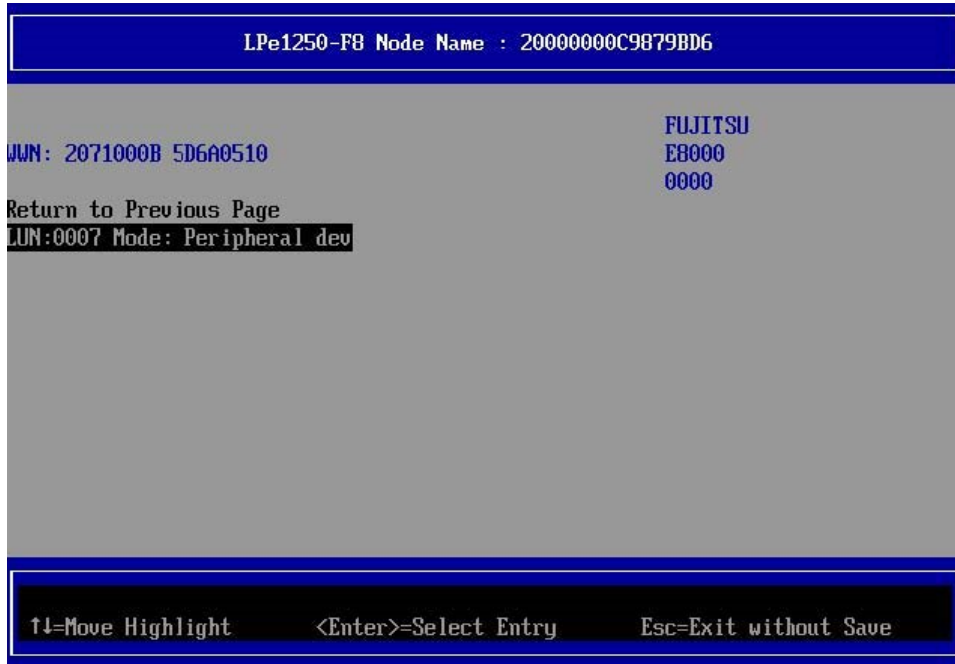
- The SAN Discovery Target List screen displays the targets found in the search by the Scan for Fiber Devices option. Select the Fibre Channel device that specifies the boot device and then press the Enter key (Figure 98).

Figure 98. Boot Device Settings (5)



- The LUN connected to the selected target is displayed. Select the LUN from which the system is to be started. Then press the Enter key. A confirmation screen appears (Figure 99).

Figure 99. Boot Device Settings (6)



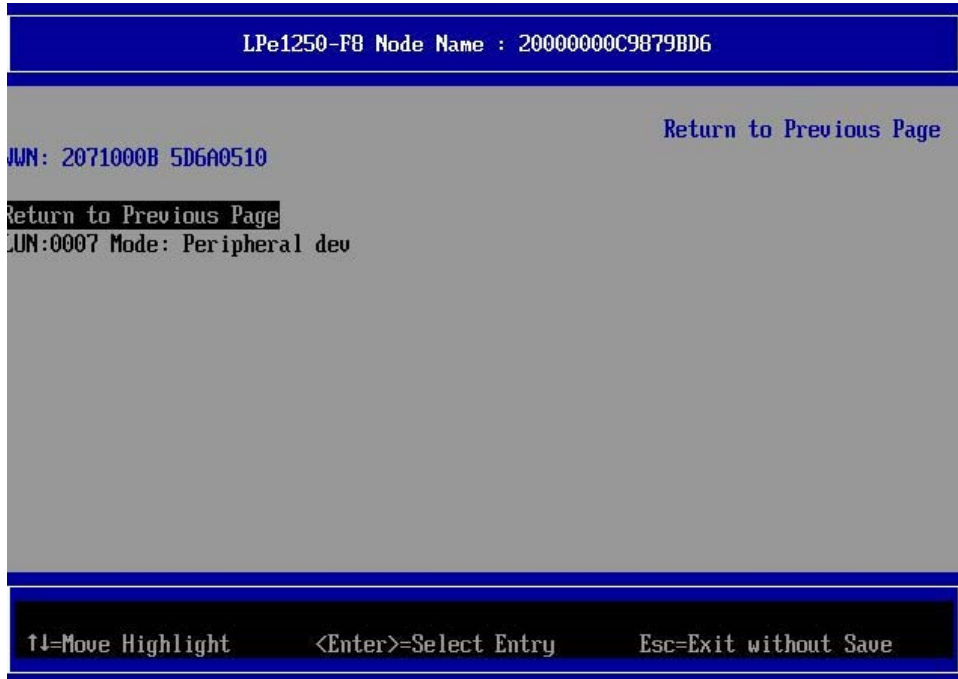
- Select Commit Changes and then press the Enter key (Figure 100).

Figure 100. Boot Device Settings (7)



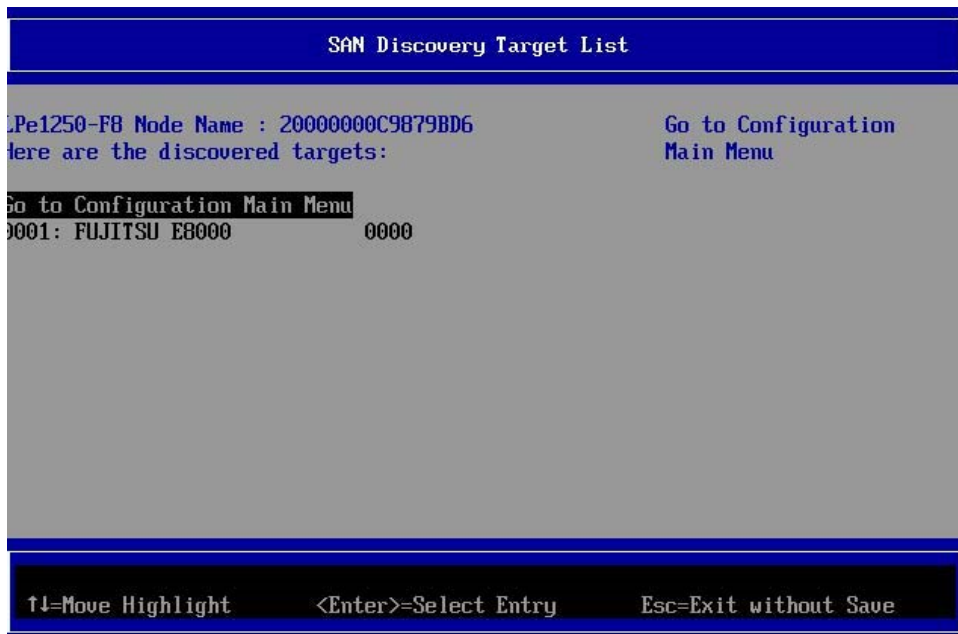
8. Select Return to Previous Page and then press the Enter key to return to the next higher menu level (Figure 101).

Figure 101. Boot Device Settings (8)



9. Select Go to Configuration Main Menu and then press the Enter key to return to the next higher menu level (Figure 102).

Figure 102. Boot Device Settings (9)



10. To register the sadump dump device, repeat step 3. If you do not want to register the dump device, proceed to step 11.
11. On the Emulex Adapter Configuration Main Menu screen, select Delete Boot Device and then press the Enter key (Figure 103). Here, confirm only the registration status of the boot device that was set with Commit Changes.

Figure 103. Boot Device Settings (10)



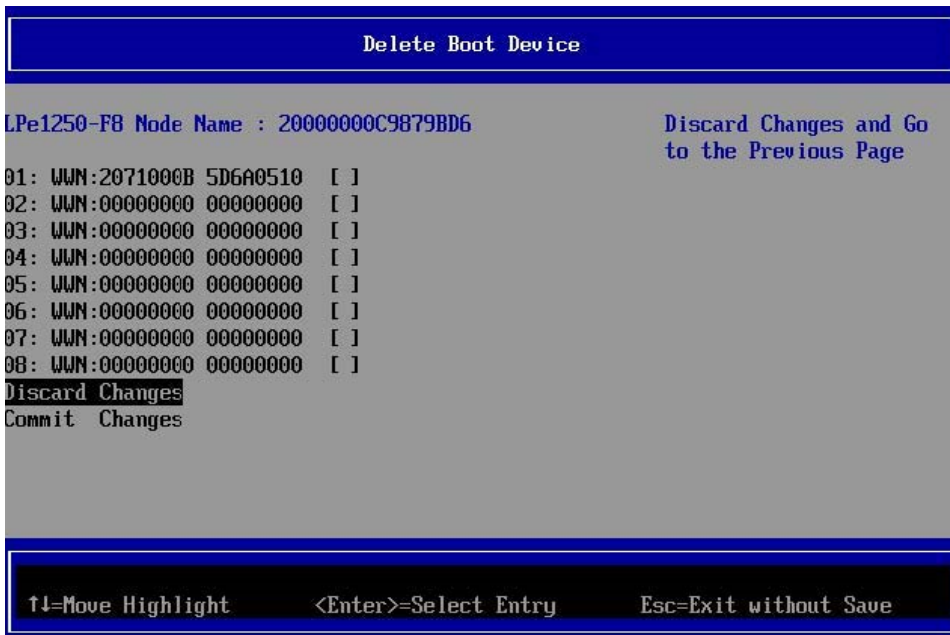
12. Confirm the registration of the boot device that was set with Commit Changes. In the following example, LUN 0007 is confirmed as connected to the target WWN: 207100B 5D6A0510 (Figure 104).

Figure 104. Boot Device Settings (11)



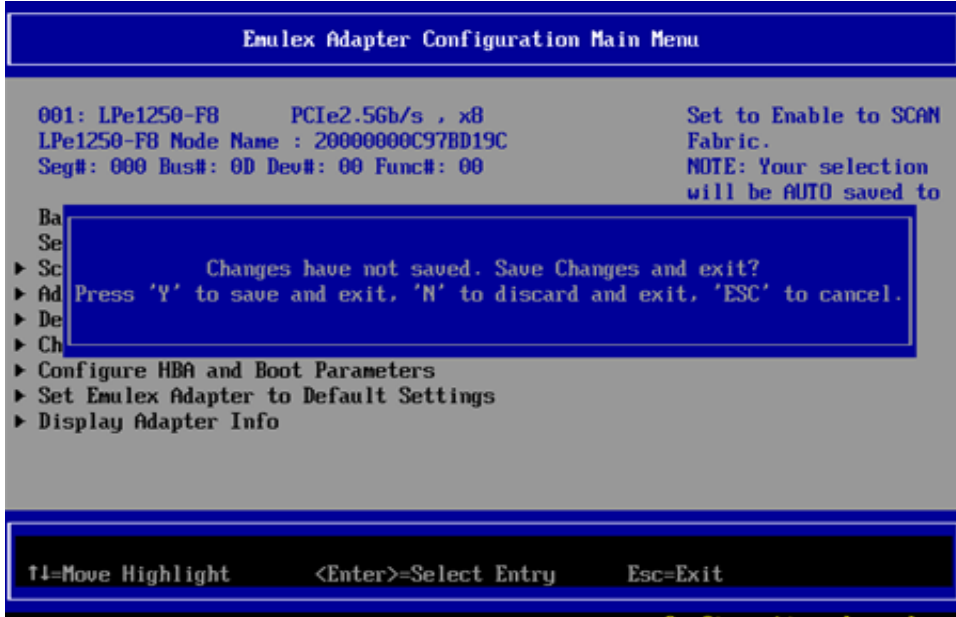
13. Select Discard Changes and then press the Enter key to return to the next higher menu level (Figure 105).

Figure 105. Boot Device Settings (12)



14. Press the Esc key and then press the Y key to return to the next higher menu level (Figure 106).

Figure 106. Boot Device Settings (13)



Important: Do not select Back to Display Adapters and RECONNECT DEVICES to return to the next higher menu level (Figure 107). If you do, your system will hang. If your system hangs and does not operate for three minutes and more, reset the system and restart the configuration process.

Figure 107. Boot Device Settings (14)



15. For a multipath configuration, configure the settings described in the sections from “Start the HBA Setup Utility and Select the HBA” to “Set Link Speed and Topology” for all the HBAs connected to the SAN storage unit LUN from which the system is started. Also, after installing the OS and multipath driver, perform the operation described in “Set Boot Device for All the HBAs Used to Start the System.”
16. After configuring all the settings, select Exit Emulex HBA Configuration Utility and then press the Enter key to return to the Device Manager menu.

Note: If following message appears after you complete the operations, press the N key or the Esc key:

Changes have not saved. Save Changes and exit?
 Press 'Y' save and exit, 'N' to discard and exit, 'ESC' to cancel.

You need not perform another operation here because the Commit Changes or Discard Changes operation from the menu completes the task of changing or discarding settings.

Select the relevant item from the Delete Boot Device or Change Boot Device Order menu. Then select Commit Changes or Discard Changes. Then return to the Delete Boot Device or Change Boot Device Order menu.

Apply the Settings

Restart the system to apply the changes in the settings. To restart the system, use the following procedure or select Reset from the Power Control window of the MMB web user interface.

1. Press the Esc key to go to the Boot Manager main page (Figure 108).

Figure 108. Restarting the System (1)



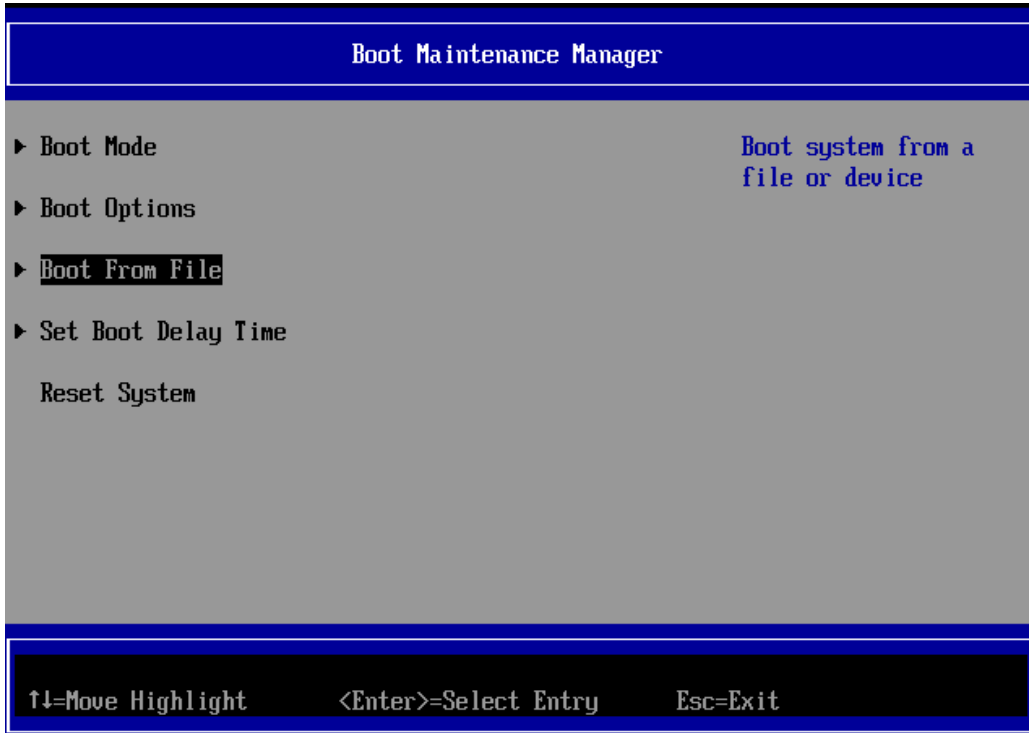
2. Select Boot Maintenance Manager and then press the Enter key to go to the Boot Maintenance Manager screen (Figure 109).

Figure 109. Restarting the System (2)



3. Select Reset System and then press the Enter key. The system is restarted (Figure 110).

Figure 110. Restarting the System (3)



4. While the Cisco logo is displayed, press any key except Enter.

Record the WWN Information of the Fibre Channel Port

Using the design diagram for the SAN boot environment, refer to the WWN address information assigned to the Fibre Channel port of the 16-Gbps Fibre Channel card of each server.

Confirm the WWN with Port Name in the Adapter Selection menu. The menu appears after the Emulex Configuration Utility restarts (Figure 111).

Figure 111. Device Manager Menu



Note: If you are updating the 16-Gbps Fibre Channel card firmware (for example, the boot BIOS), check the WWN after the firmware update. To clearly identify the mounting location of the 8-Gbps Fibre Channel card, record the host name (the name that identifies the Cisco C880 M4 Server), mounted card, mounting slot location, BUS number, and DEV number. For the BUS number and slot number, check the BUS number and slot number of the target HBA from the IOU menu and PCI_Box menu of the MMB web user interface. The BUS number is the middle of the three numbers delimited by slashes in the Seg/Bus/Dev item.

The example in Table 4 shows how the WWNs are recorded.

Table 4. WWN Recording Example

Host Name (to Identify Server)	Mounted Card (Type)	PCI	Fibre Channel Port
		BUS-DEV	WWN
Server 1	MC-0JFC21	0x - 00	10 00 00 00 C9**
		0x - 00	10 00 00 00 C9**
Server 2	MC-0JFC21	0x - 00	10 00 00 00 C9**
		0x - 00	10 00 00 00 C9**
•	•	•	•
•	•	•	•
•	•	•	•
•	•	•	•

Note:

- Always keep the WWN information up-to-date, and share and manage it together with the SAN boot system administrator and maintenance personnel.
- If the WWN information is wrong, connection to the SAN storage is disabled, and you will experience problems such as being unable to start the operating system.
- When an 8-Gbps Fibre Channel card is moved or hardware is replaced for maintenance purposes, the WWN may be changed.

16-Gbps Fibre Channel Card Settings: Traditional BIOS Driver Version 6.02x6 or Later

This section describes the procedure for setting traditional BIOS Driver Version 6.02x6 or later.

Configure the HBA Setup Utility

Start by configuring the HBA Setup Utility.

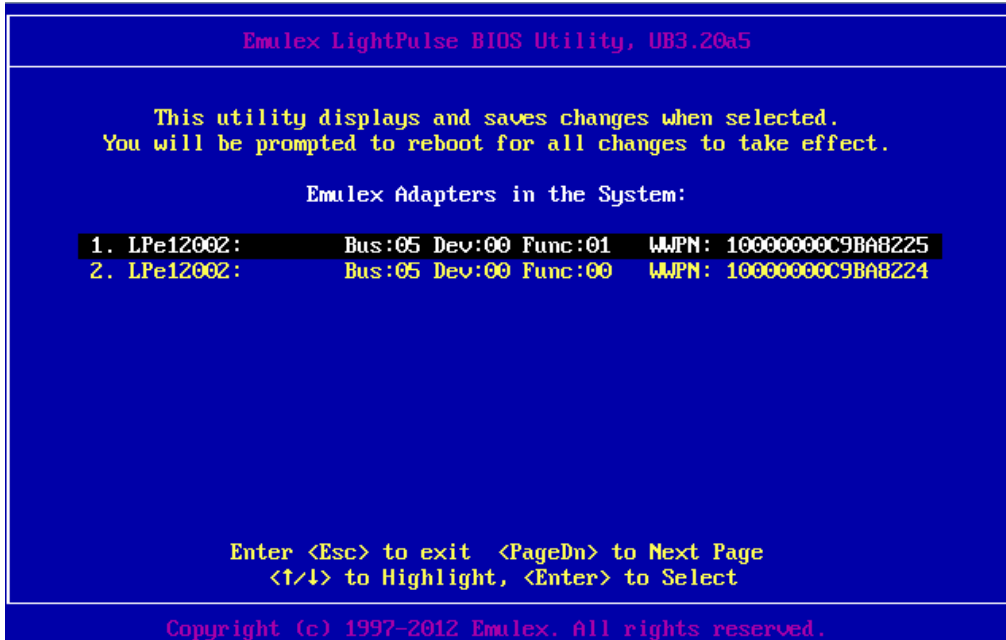
1. Start the system, and when the screen shown in Figure 108 appears, press Alt+E or Ctrl+E.

Figure 112. Starting Traditional BIOS Setup

A screenshot of a BIOS utility screen for an Emulex LightPulse FC x86 BIOS. The text is displayed in a monospaced font on a black background. The text reads: "Emulex LightPulse FC x86 BIOS, Version 6.02x6", "Copyright (c) 1997-2013 Emulex. All rights reserved.", "Press <Alt E> or <Ctrl E> to enter Emulex BIOS configuration utility. Press <s> to skip Emulex BIOS", "Emulex BIOS is Disabled on Adapter 01", "Installing Emulex BIOS", and "Bringing the Link up, Please wait...".

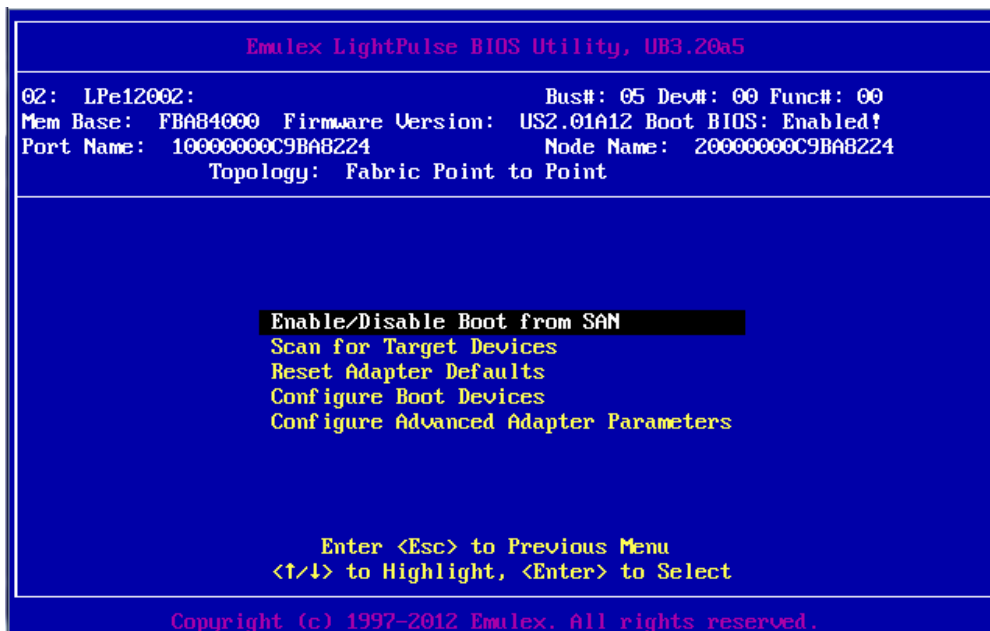
2. Start the Emulex LightPulse BIOS Utility. Fibre Channel ports of the Fibre Channel card appear on the HBA list screen. Select a Fibre Channel port to set up and press the Enter key (Figure 113).

Figure 113. Emulex LightPulse BIOS Utility (1)



The menu for the Fibre Channel port you selected in the previous screen appears. The memory address (Mem Base), firmware version, World Wide Port Name (WWPN), World Wide Node Name (WWNN), and topology for the Fibre Channel port also are listed (Figure 114).

Figure 114. Emulex LightPulse BIOS Utility (2)

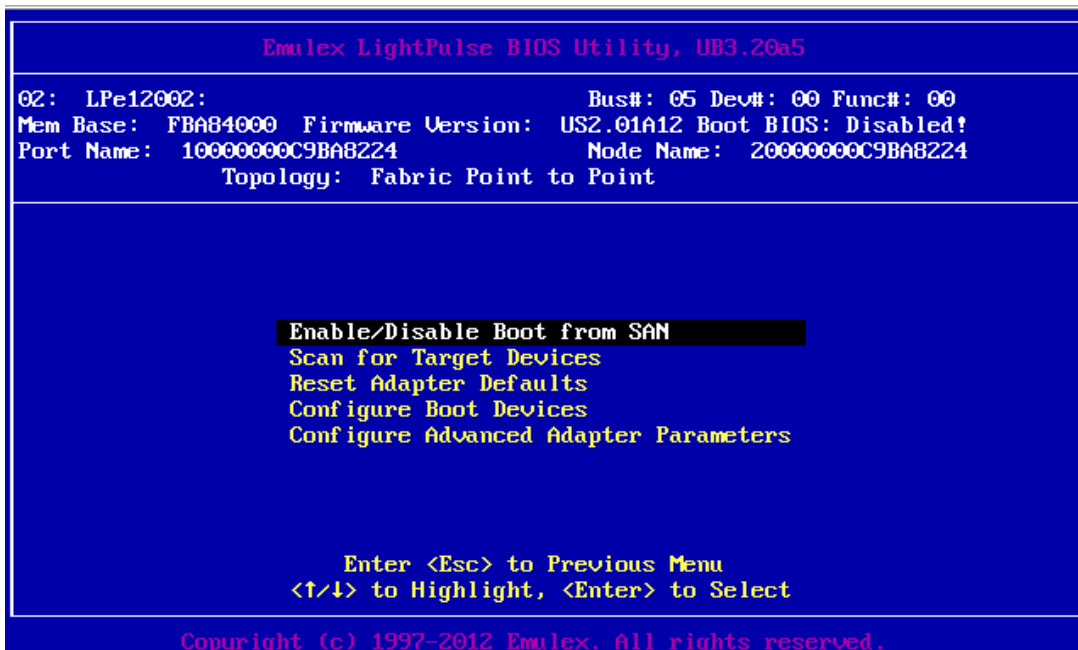


Enable the BIOS

Enable the HBA BIOS so that the HBA can recognize the LUNs of the SAN storage unit and so that the system can be started from one of them.

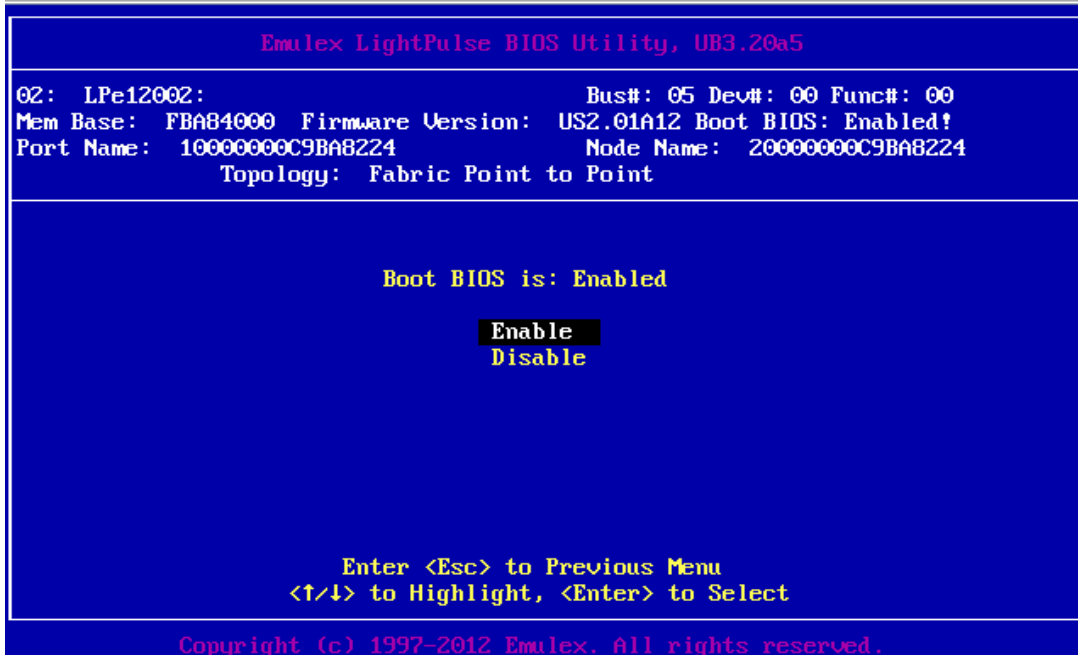
1. On the Port 001:Emulex LPe16002B-M6-F 16Gb 2-port PCIe Fiber Chann screen, select Set Boot from SAN <Disable>.
2. The screen for selecting <Disable> or <Enable> appears. Select <Enable> and then press the Enter key.
3. Select Enable/Disable Boot from SAN and then press the Enter key (Figure 115).

Figure 115. Enable/Disable Boot from SAN Setup Screen (1)



4. Select Enable for the boot BIOS and then press the Enter key (Figure 116).

Figure 116. Enable/Disable Boot from SAN Setup Screen (2)



Note: Confirm that the boot BIOS is enabled.

Set the Link Speed and Topology

This section describes how to set the speed and topology.

Set the Topology

Follow these steps to set the topology:

1. In the main menu, select Configure Advanced Adapter Parameters and then press the Enter key (Figure 117).

Figure 117. Topology Selection Settings (1)

```
Emulex LightPulse BIOS Utility, UB3.20a5
02: LPe12002: Bus#: 05 Dev#: 00 Func#: 00
Mem Base: FB84000 Firmware Version: US2.01A12 Boot BIOS: Enabled!
Port Name: 10000000C9BA8224 Node Name: 20000000C9BA8224
Topology: Auto Topology: Loop First (Default)

Enable/Disable Boot from SAN
Scan for Target Devices
Reset Adapter Defaults
Configure Boot Devices
Configure Advanced Adapter Parameters

Enter <Esc> to Previous Menu
<↑/↓> to Highlight, <Enter> to Select

Copyright (c) 1997-2012 Emulex. All rights reserved.
```

2. Select Topology Selection and then press the Enter key (Figure 118).

Figure 118. Topology Selection Settings (2)

```
Emulex LightPulse BIOS Utility, UB3.20a5
02: LPe12002: Bus#: 05 Dev#: 00 Func#: 00
Mem Base: FB84000 Firmware Version: US2.01A12 Boot BIOS: Enabled!
Port Name: 10000000C9BA8224 Node Name: 20000000C9BA8224
Topology: Auto Topology: Loop First (Default)

Change Default ALPA of this Adapter
Change PLOGI Retry Timer
Topology Selection
Enable or Disable Spinup Delay
Auto Scan Setting
Enable or Disable EDD 3.0
Enable or Disable Start Unit Command
Enable or Disable Environment Variable
Enable or Disable Auto Boot Sector
Link Speed Selection

Enter <Esc> to Previous Menu
<↑/↓> to Highlight, <Enter> to Select

Copyright (c) 1997-2012 Emulex. All rights reserved.
```

- When you connect a 16-Gbps Fibre Channel card to storage that supports 16 Gbps, you have to connect through a Fibre Channel switch. Note that conventional FCAL connection is not supported in this case. Confirm the SAN connection configuration and select the appropriate setting. Then press the Enter key. Change the setting from Auto Topology: Loop First (Default) by referring to the connection settings in Figure 119.

Figure 119. Fabric Point to Point Setting Screen

```
Emulex LightPulse BIOS Utility, UB3.20a5
QZ: LPe12002: Bus#: 05 Dev#: 00 Func#: 00
Mem Base: FBAB4000 Firmware Version: US2.01A12 Boot BIOS: Enabled!
Port Name: 10000000C9BA8224 Node Name: 20000000C9BA8224
Topology: Auto Topology: Loop First (Default)

Topology: Auto Topology: Loop First (Default)
Auto Topology: Loop First (Default)
Auto Topology: Point to Point First
FC-AL
Fabric Point to Point

Enter <Esc> to Previous Menu
<↑/↓> to Highlight, <Enter> to Select

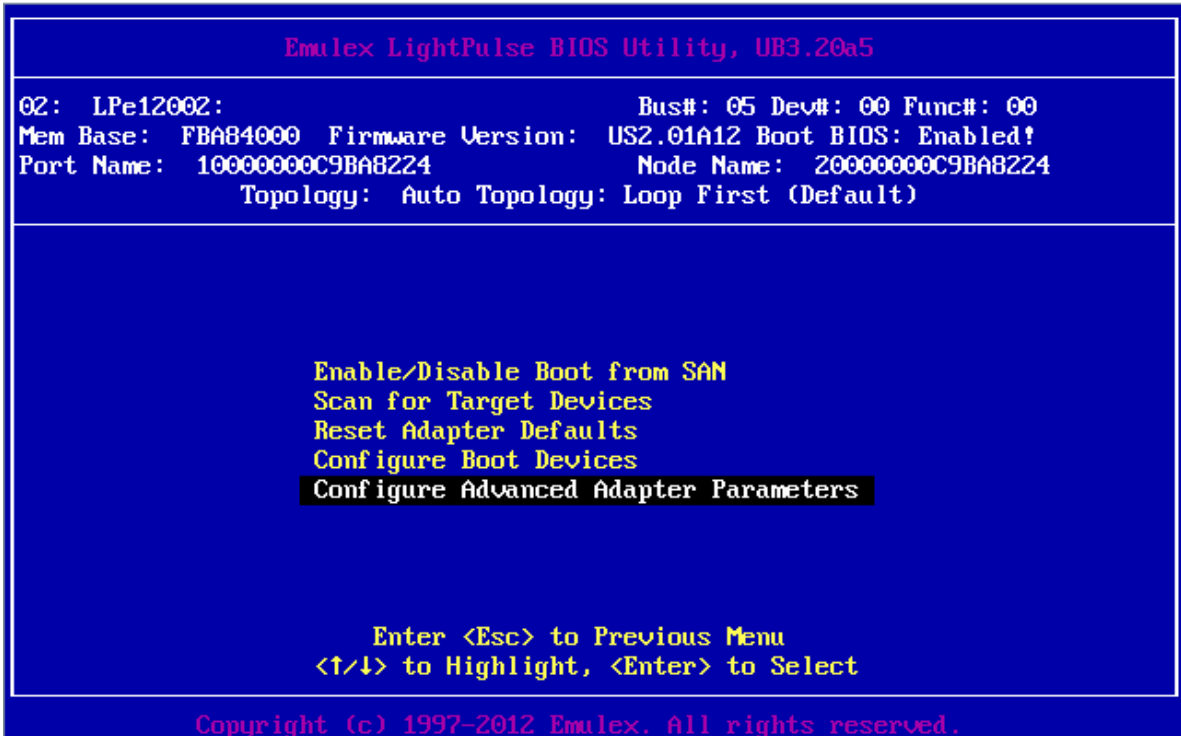
Copyright (c) 1997-2012 Emulex. All rights reserved.
```

Set the Link Speed

Configure the setting that corresponds to the connection link speed (2, 4, or 8 Gbps). Do not set Auto Select (Default).

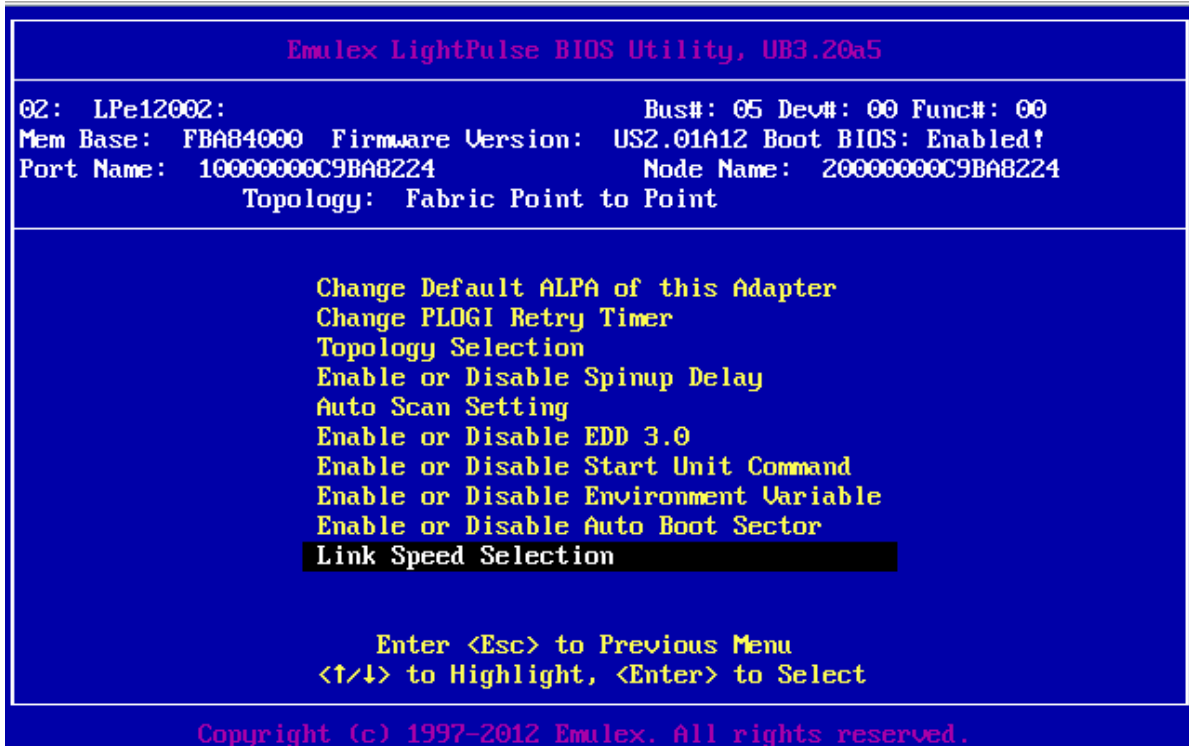
- In the main menu, select Configure Advance Adapter Parameters and press the Enter key (Figure 120).

Figure 120. Configure Advanced Adapter Parameters Screen



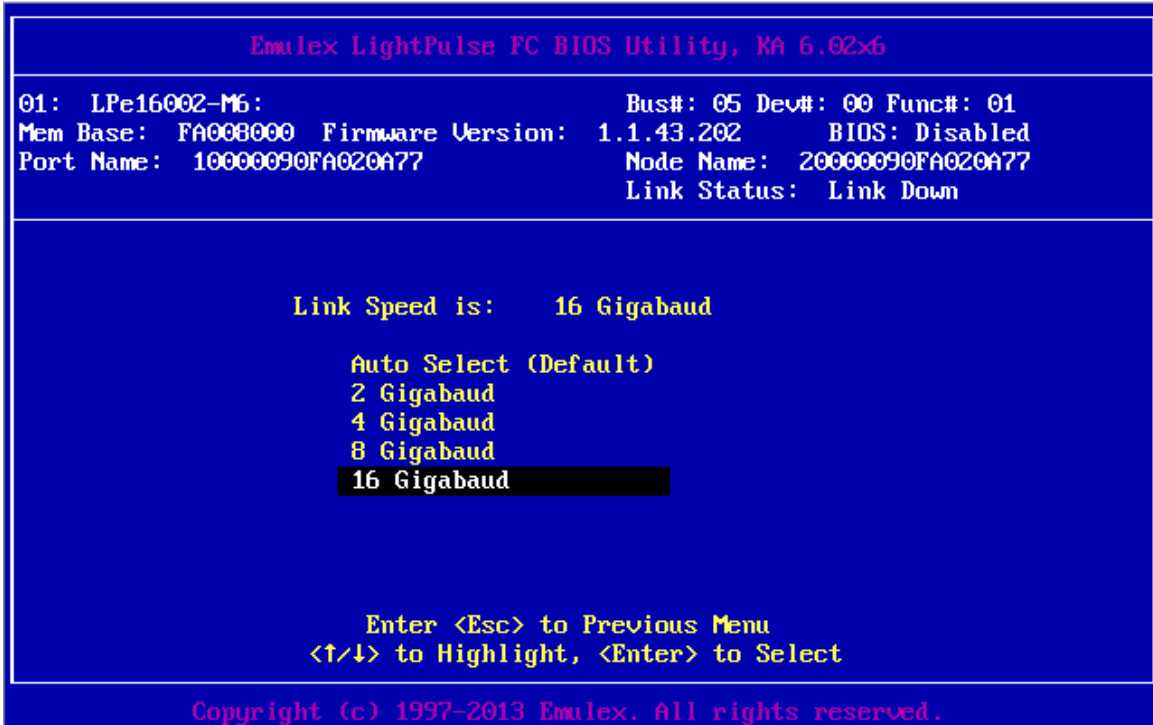
2. On the next screen, select Link Speed Selection and then press Enter key (Figure 121).

Figure 121. Link Speed Selection Settings Screen (1)



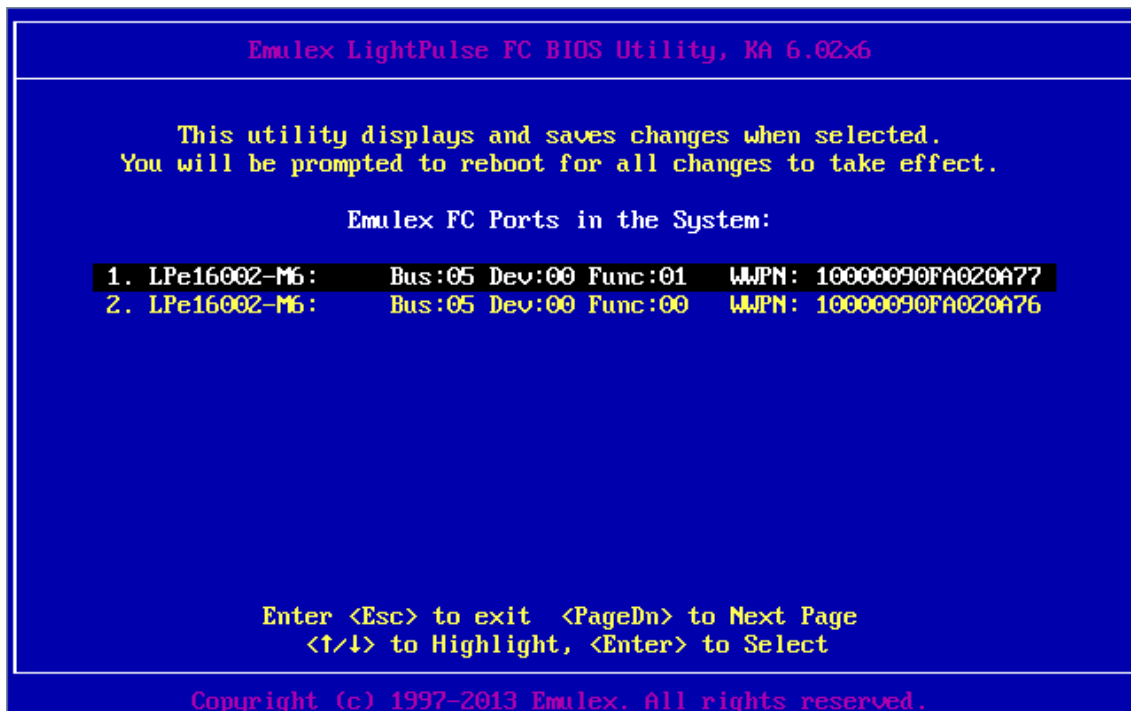
3. Select the link speed that corresponds to the connection environment (connected Fibre Channel switch or SAN storage unit) and then press the Enter key (Figure 122).

Figure 122. Link Speed Selection Settings Screen (2)



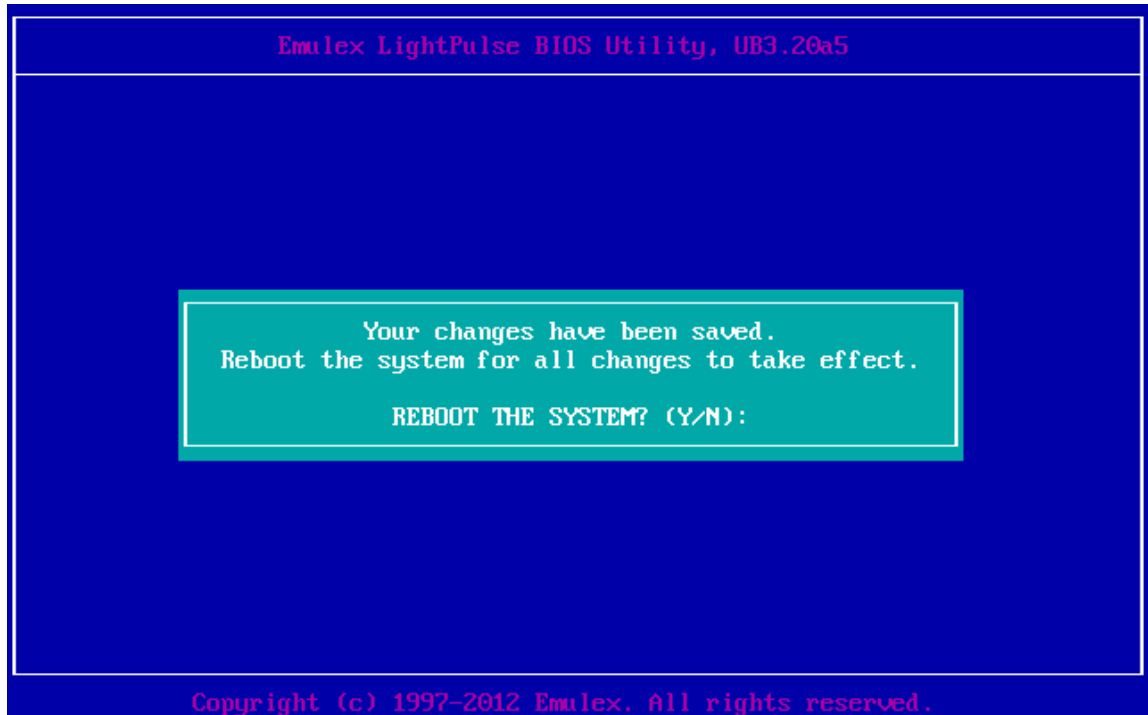
4. Press the Esc key three times to return to the LightPulse BIOS Utility (Figure 123).

Figure 123. Emulex LightPulse BIOS Utility Screen



5. Press the Esc key again. Press Y to reboot the system and save your changes (Figure 124).

Figure 124. Saving Emulex LightPulse BIOS Settings

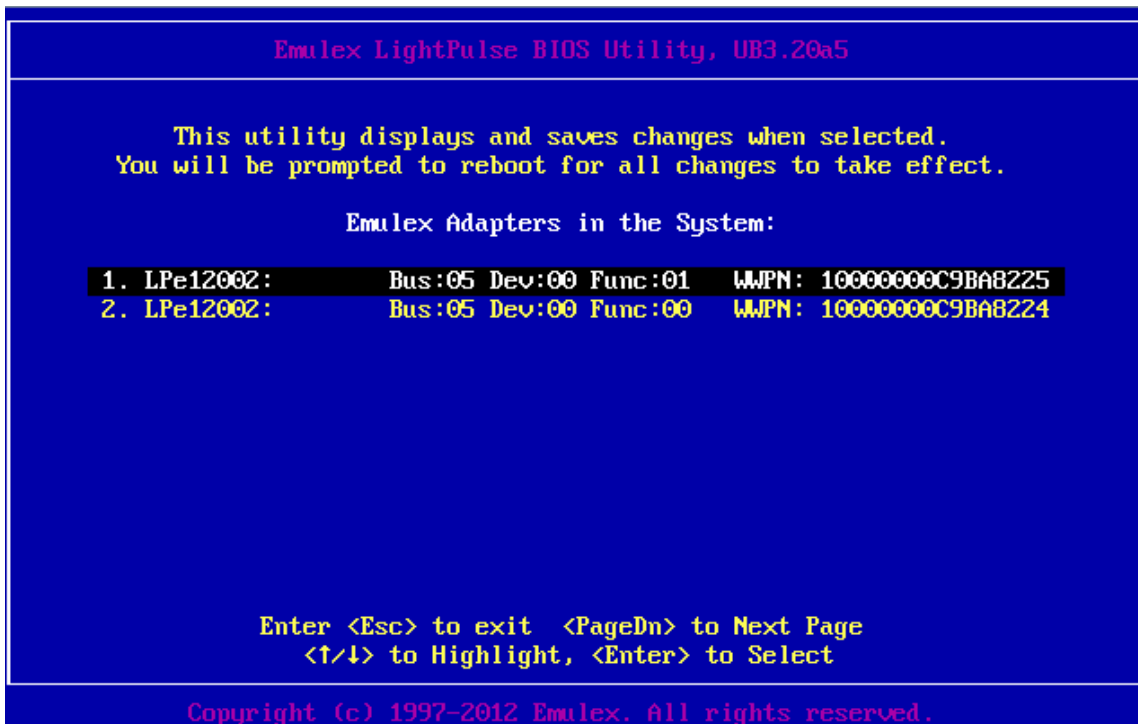


Set the Boot Device

Now set the boot device. Note that the settings for the 8-Gbps (12002) and the 16-Gbps (16002) devices are identical.

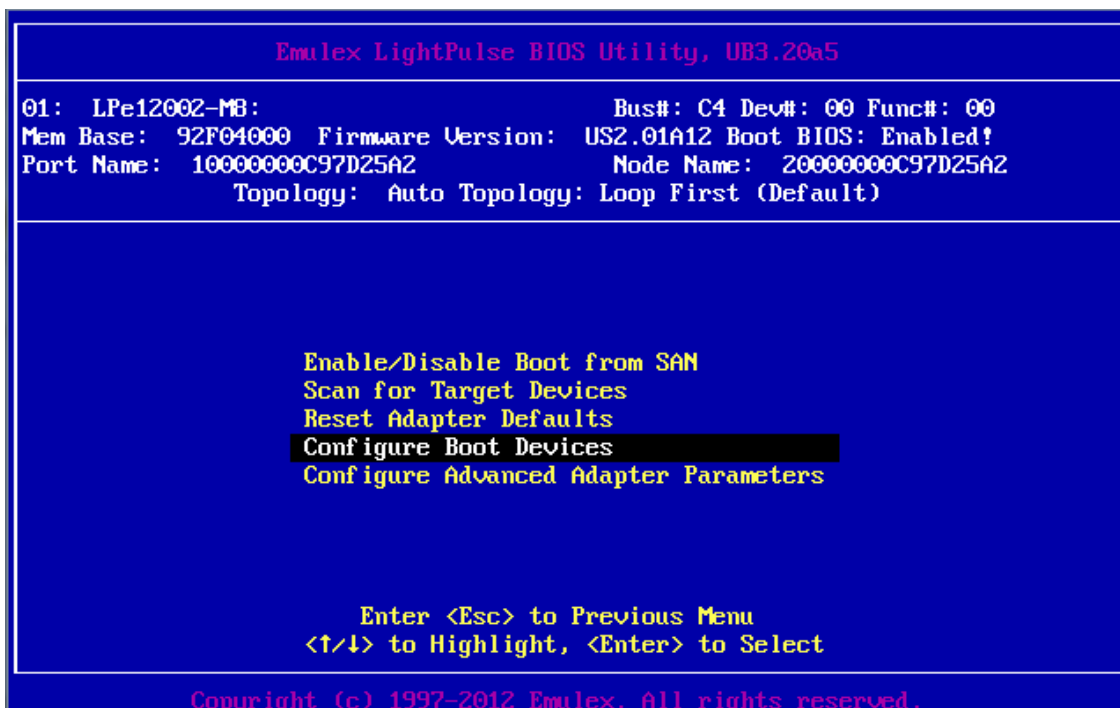
1. Select a connected boot device from the Fibre Channel port and then press the Enter key (Figure 125).

Figure 125. BIOS Device Settings (1)



2. In the main menu, select Configure Boot Devices and then press the Enter key (Figure 126).

Figure 126. BIOS Device Settings (2)



3. Select Primary Boot and then press the Enter key (Figure 127).

Figure 127. BIOS Device Settings (3)

```
Emulex LightPulse BIOS Utility, UB3.20a5

02: LPe12002:                               Bus#: 05 Dev#: 00 Func#: 00
Mem Base: FBAB4000 Firmware Version: US2.01A12 Boot BIOS: Enabled!
Port Name: 10000000C9BA8224                 Node Name: 20000000C9BA8224
Topology: Auto Topology: Loop First (Default)

List of Saved Boot Devices:

1. Unused  DID:000000 WWPN:00000000 00000000 LUN:00 Primary Boot
2. Unused  DID:000000 WWPN:00000000 00000000 LUN:00
3. Unused  DID:000000 WWPN:00000000 00000000 LUN:00
4. Unused  DID:000000 WWPN:00000000 00000000 LUN:00
5. Unused  DID:000000 WWPN:00000000 00000000 LUN:00
6. Unused  DID:000000 WWPN:00000000 00000000 LUN:00
7. Unused  DID:000000 WWPN:00000000 00000000 LUN:00
8. Unused  DID:000000 WWPN:00000000 00000000 LUN:00

<↑/↓> to Highlight, <Enter> to Select

Copyright (c) 1997-2012 Emulex. All rights reserved.
```

4. Select the boot device: in this case, FUJITSU ETERNUS_DXL, and then press the Enter key (Figure 128).

Figure 128. BIOS Device Settings (4)

```
Emulex LightPulse BIOS Utility, UB3.20a5
-----
01: LPe12002-MB:                Bus#: C4 Dev#: 00 Func#: 00
Mem Base: 92F04000 Firmware Version: US2.01A12 Boot BIOS: Enabled!
Port Name: 10000000C97D25A2      Node Name: 20000000C97D25A2
Topology: Auto Topology: Loop First (Default)
-----

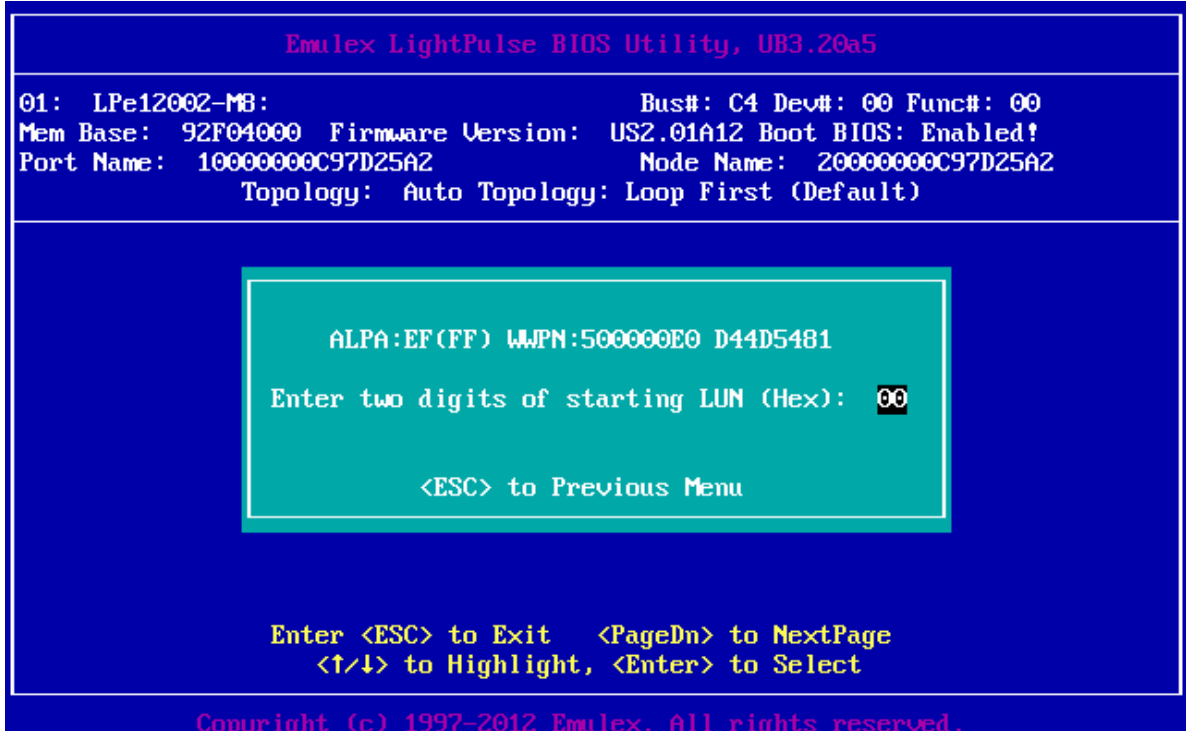
00. Clear selected boot entry!!
01. ALPA:EF(FF) WWPN:500000E0 D44D5481 LUN:00 FUJITSU ETERNUS_DXL 0000

Enter <ESC> to Exit <PageDn> to NextPage
<1/↓> to Highlight, <Enter> to Select

Copyright (c) 1997-2012 Emulex. All rights reserved.
```

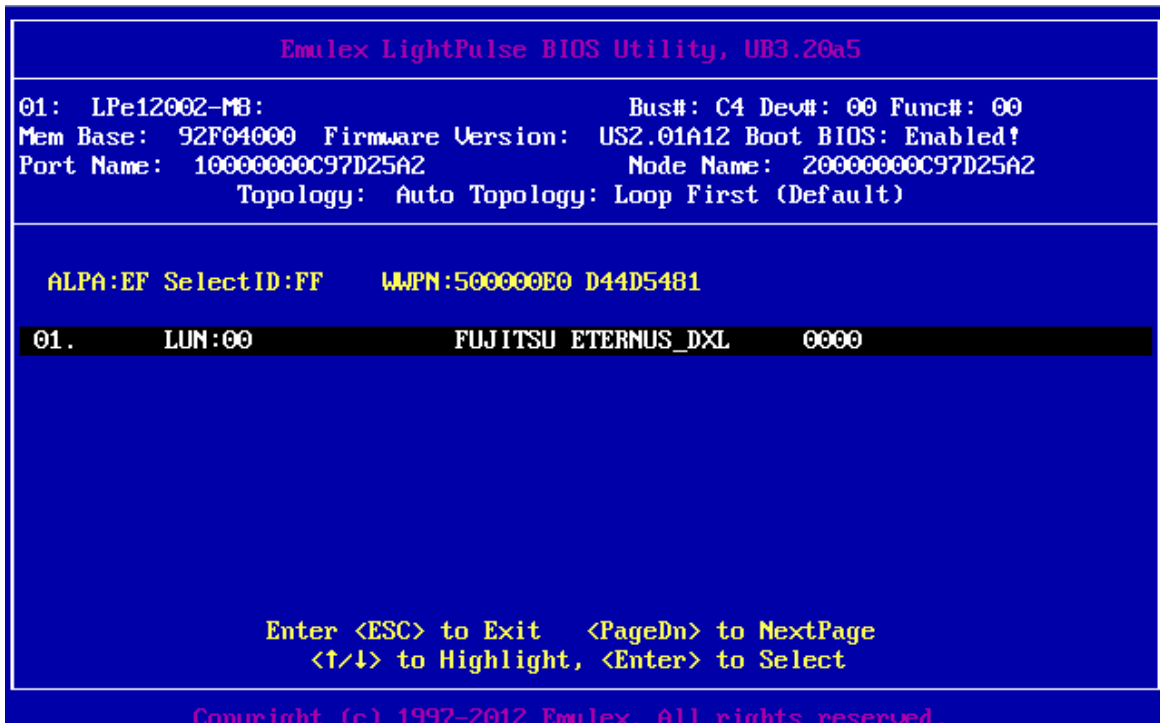
5. The device information is displayed. Press the Enter key (Figure 129).

Figure 129. BIOS Device Settings (5)



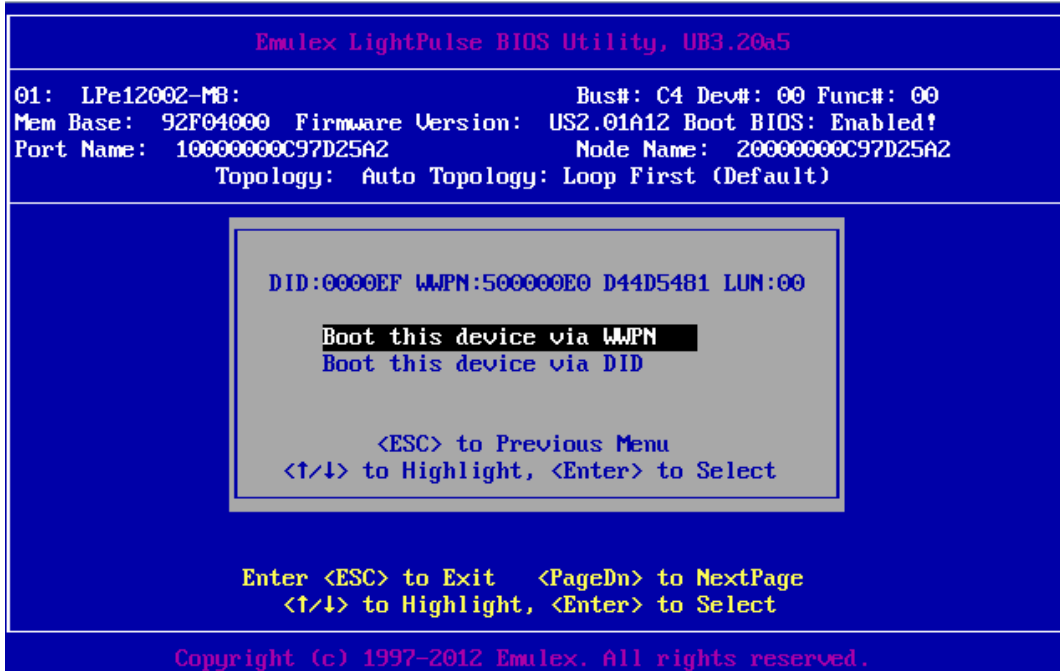
6. Select the device that is registered (Figure 130).

Figure 130. BIOS Device Settings (6)



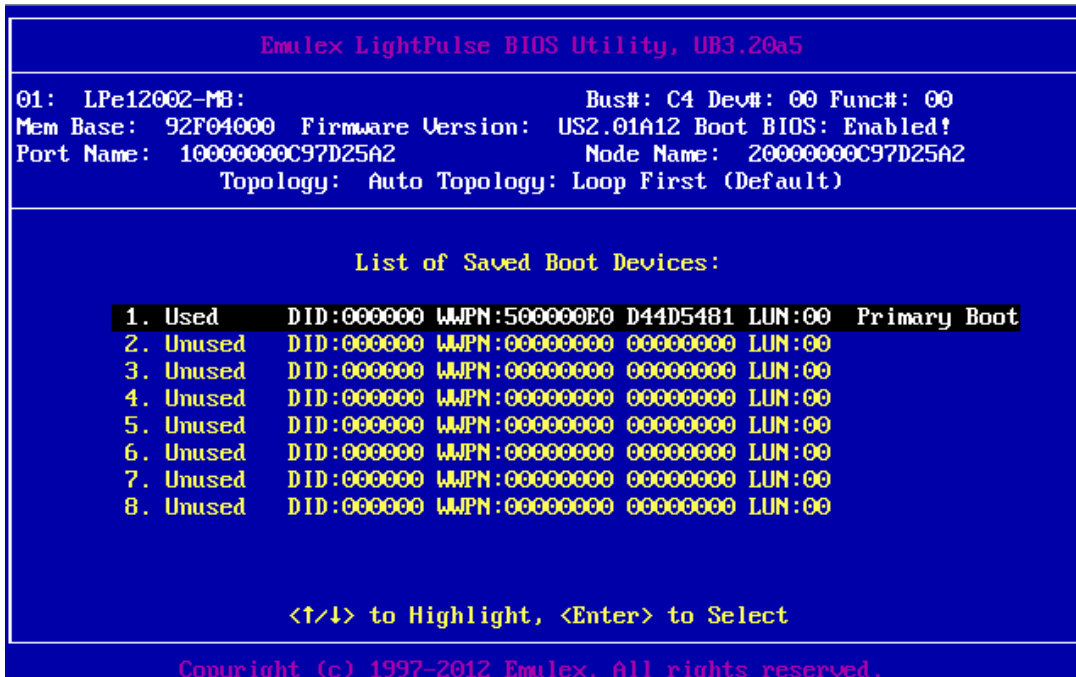
7. Select "Boot this device via WWPN" and then press the Enter key (Figure 131).

Figure 131. BIOS Device Settings (7)



The boot device is added (Figure 132).

Figure 132. BIOS Device Settings (8)



- Press the Enter key. From the main menu, select Scan for Target Devices and then press the Enter key (Figure 133).

Figure 133. BIOS Device Settings (9)

```
Emulex LightPulse BIOS Utility, UB3.20a5

01: LPe12002-MB:          Bus#: C4 Dev#: 00 Func#: 00
Mem Base: 92F04000 Firmware Version: US2.01A12 Boot BIOS: Enabled!
Port Name: 10000000C97D25A2 Node Name: 20000000C97D25A2
Topology: Auto Topology: Loop First (Default)

Enable/Disable Boot from SAN
Scan for Target Devices
Reset Adapter Defaults
Configure Boot Devices
Configure Advanced Adapter Parameters

Enter <Esc> to Previous Menu
<↑/↓> to Highlight, <Enter> to Select

Copyright (c) 1997-2012 Emulex. All rights reserved.
```

The search results for the boot device are displayed (Figure 134).

Figure 134. BIOS Device Settings (10)

```
Emulex LightPulse BIOS Utility, UB3.20a5

01: LPe12002-MB:          Bus#: C4 Dev#: 00 Func#: 00
Mem Base: 92F04000 Firmware Version: US2.01A12 Boot BIOS: Enabled!
Port Name: 10000000C97D25A2 Node Name: 20000000C97D25A2
Topology: Auto Topology: Loop First (Default)

Devices Present on This Adapter:

01. ALPA:EF(CF) WWPN:500000E0 D44D5481 LUN:00 FUJITSU ETERNUS_DXL 0000

Enter <Esc> to Previous Menu

Copyright (c) 1997-2012 Emulex. All rights reserved.
```

- Press the Esc key to return to the main menu (Figure 135).

Figure 135. BIOS Device Settings (11)

```
Emulex LightPulse BIOS Utility, UB3.20a5
01: LPe12002-M8: Bus#: C4 Dev#: 00 Func#: 00
Mem Base: 92F04000 Firmware Version: US2.01A12 Boot BIOS: Enabled!
Port Name: 10000000C97D25A2 Node Name: 20000000C97D25A2
Topology: Auto Topology: Loop First (Default)

Enable/Disable Boot from SAN
Scan for Target Devices
Reset Adapter Defaults
Configure Boot Devices
Configure Advanced Adapter Parameters

Enter <Esc> to Previous Menu
<↑/↓> to Highlight, <Enter> to Select

Copyright (c) 1997-2012 Emulex. All rights reserved.
```

Note: If the expected Fibre Channel device is not displayed, the SAN storage or physical connection settings of the Fibre Channel switch may be incorrect. Confirm these settings again.

10. Press the Esc key. The message to save the setting is displayed. Then return to the Device Manager.
11. For a multipath configuration, configure the settings described earlier in the sections from “Start the HBA Setup Utility” to “Set the Link Speed and Topology” for all the HBAs connected to the SAN storage unit LUN from which the system is started. Also, after installing the OS and multipath driver, perform the operation described in the section “Set the Boot Device” for all the HBAs used to start the system.
12. After all the settings are configured, select Exit Emulex HBA Configuration Utility and then press the Enter key to return to the Device Manager menu.

Considerations for Linux Installation

This section describes how to install Red Hat Enterprise Linux on the Cisco C880 M4 Server.

Linux Server OS Installation

Refer to OS installation manual for information about installing the Linux OS.

SAN Multipath Boot

You must verify that the OS you are installing supports multipath boot. Not every OS supports SAN and iSCSI multipath boot. Ask your OS vendor before you make any decisions about the system.

Prepare for Linux Installation

Prepare for the Linux installation in advance.

For a multipath configuration, disconnect the secondary cable connected to the server. Specifically, use a single-path configuration (connection with only one Fibre Channel cable) until you complete the installation of the OS and multipath driver.

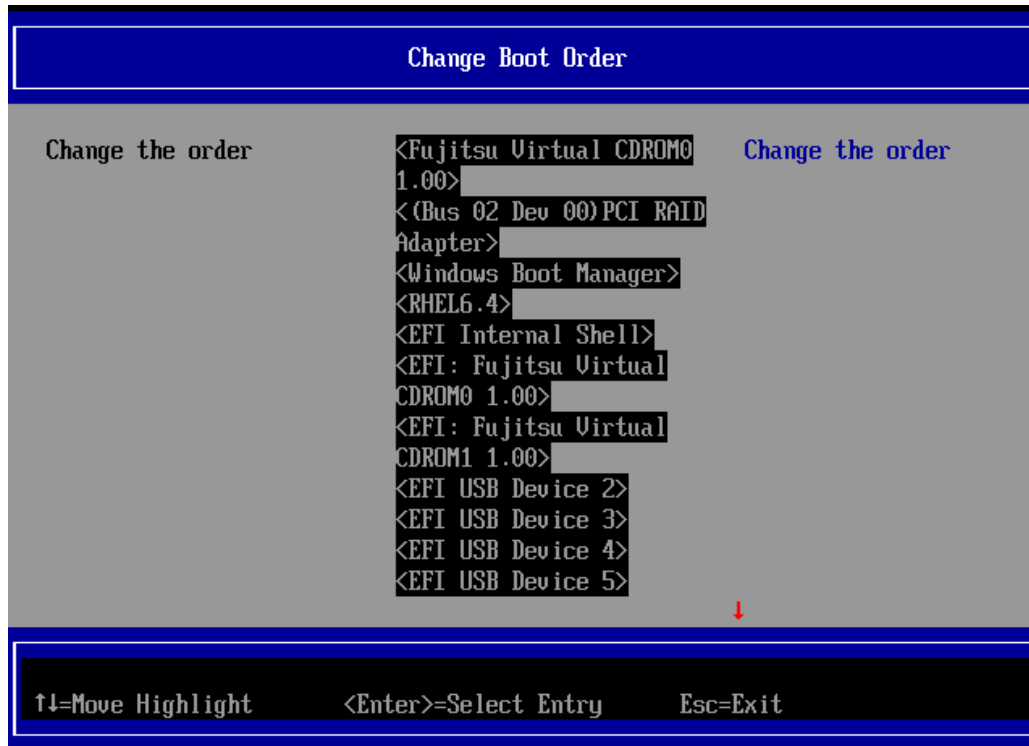
If the server is in a multipath connection state, the OS cannot be installed correctly. Manually disconnect the secondary Fibre Channel path before you begin the installation (disconnect the secondary cable of each server).

Install the OS and Bundled Software

If the OS supports UEFI mode, you can install it in this mode using the following procedure to change the boot order:

1. After powering on the partition, press any key other than the Enter key while the Cisco logo is displayed to display the Boot Manager main page.
2. On the Boot Manager main page, select the following items from the menu in the following order:
 - a. Boot Maintenance Manager
 - b. Boot Options
 - c. Change Boot Order
 - d. "Change the order"
3. Specify the order as follows for the highest-priority device to boot from remote storage (Figure 136):
 - For device installed in UEFI BIOS mode: UEFI: Fujitsu Virtual CDROM0 1.00
 - For device installed in traditional BIOS mode: Fujitsu Virtual CDROM0 1.00

Figure 136. Change Boot Order Menu for Cisco C880 M4



4. Specify Commit Changes and Exit.
5. Specify Reset System to reboot the partition.

Install Emulex OneCommand Manager

Now install Emulex OneCommand Manager (OCManager).

1. If you install OCManager, you will need to install the Linux libnl package. Use the Fibre Channel card driver utility and install OCManager. OCManager includes the libnl package.
2. Copy the binary files on the Cisco C880 M4 Server's optional directory.
3. For information about how to install OCManager, refer to the installation procedure for the original equipment manufacturer (OEM) driver.

Note: One end of the Fibre Channel cable is still off the connector at this point.

Install the Multipath Driver

Install the multipath driver. For the installation procedure, refer to the manual for the multipath driver that you are using.

Restore the Multipath Connection

Recover the multipath connection.

The OS is shut down, the cable of the Fibre Channel passing cut according to procedure 1 is reconnected after the power supply of the partition is cut, and the OS is started. After it shuts down after the start by the multipath is confirmed, internal hard-disk drive (HDD) into is added when internal HDD into is used.

Confirm the multipath status with the following process:

1. Configure the UEFI driver on the HBA. (Refer to the sections “8-Gbps Fibre Channel Card” and “16-Gbps Fibre Channel Card” for more information.)
2. From the Boot Manager main page, select Boot Maintenance Manager > Boot Options > Set Legacy HardDisk Drive Order.
3. Review the screen (Figure 137). If multiple HDDs are not listed, you need to recover the multipath connection.

Figure 137. Set Legacy HardDisk Drive Order Menu (Multipath)



4. After confirming the existence of multiple HDDs, reboot OS.

SLES 11 and 12 Installation: iSCSI

After the system has been prepared for iSCSI or SAN boot, you can install the OS.

1. Boot the system (Figures 138 and 139).

Figure 138. Booting the System (1)

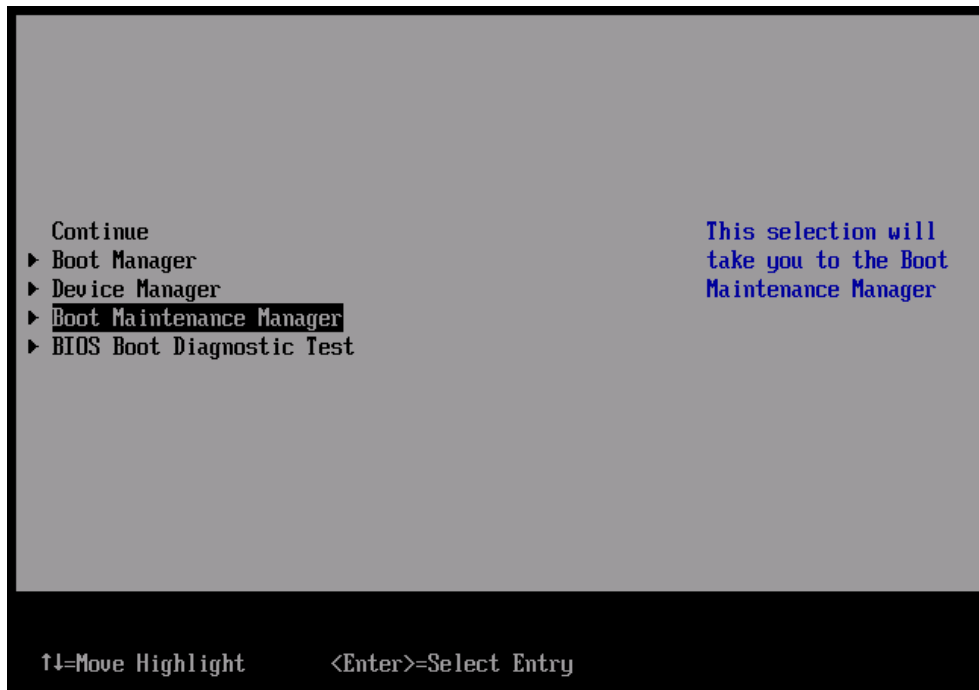
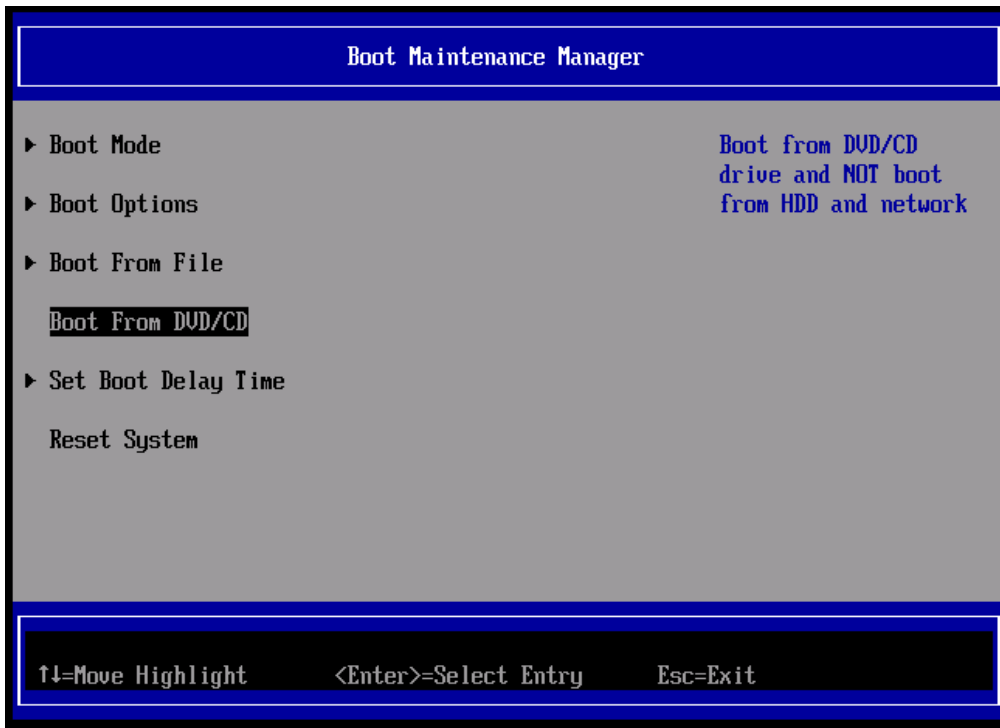
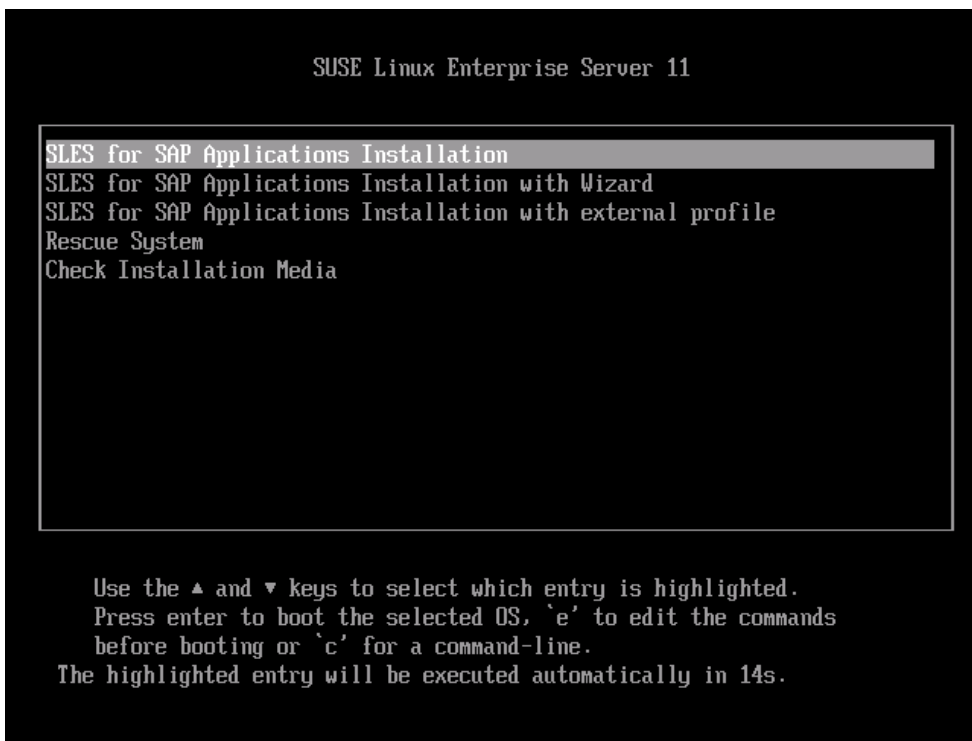


Figure 139. Booting the System (2)



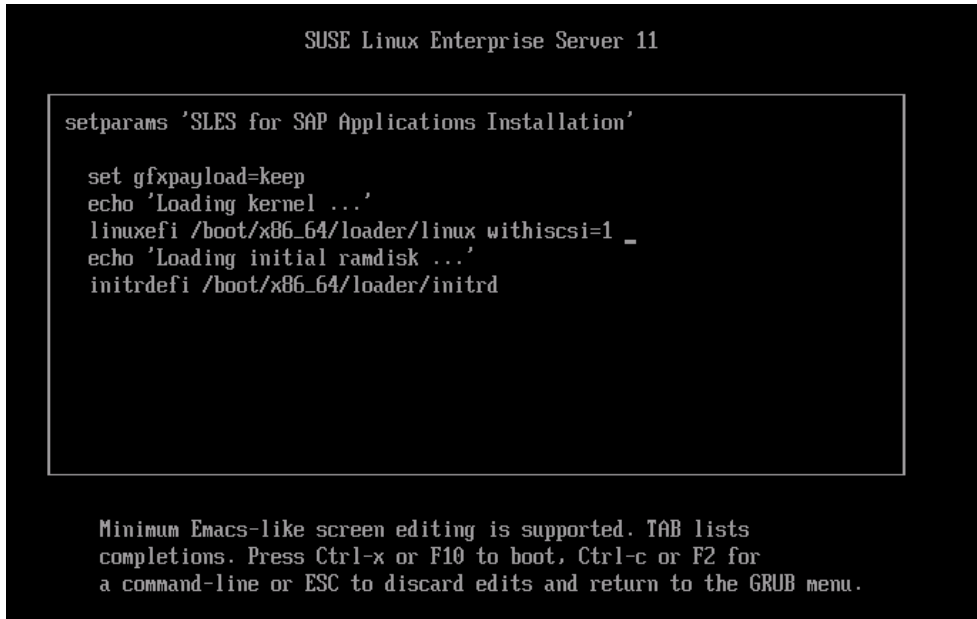
2. After the Cisco C880 M4 reboots, the installation option for SLES appears. Select it (Figure 140)

Figure 140. Installing SLES



3. If the boot method is iSCSI, select “e” to enable the iSCSI boot environment for SLES (Figure 141).

Figure 141. Enabling the iSCSI Boot Environment



```
SUSE Linux Enterprise Server 11

setparams 'SLES for SAP Applications Installation'

set gfxpayload=keep
echo 'Loading kernel ...'
linuxefi /boot/x86_64/loader/linux withiscsi=1
echo 'Loading initial ramdisk ...'
initrdefi /boot/x86_64/loader/initrd

Minimum Emacs-like screen editing is supported. TAB lists
completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for
a command-line or ESC to discard edits and return to the GRUB menu.
```

Post-Installation Configuration

This section presents procedures you should follow after you install the OS.

Update the OS After the Installation

You should register your SUSE and Red Hat installation and update the OS completely to be sure that you are using the latest available software release.

Note: SAP will release a SAP HANA OS release matrix soon. Not all available OS releases are supported for all SAP HANA releases.

Verify the Driver Specification

The only driver that is dependent on the system is the Emulex Fibre Channel driver. This driver must match the installed firmware on the Emulex controller. Explicitly check which driver must be used for the installed firmware of the Emulex controller.

All other components use the standard Linux native driver and can be updated during the OS update.

If you have any questions, open a support call with the Cisco TAC.

Configure and Tune the OS

Configure and tune the OS for all nodes installed to run SAP HANA.

SUSE

Change the host name to the customer-specific host name:

```
linux:~ # vi /etc/HOSTNAME
server01.wdf.sap.corp
```

SUSE

Set the run level to 3 to disable the x-environment:

```
linux:~ # vi /etc/inittab
# The default runlevel is defined here
id:3:initdefault:
```

SUSE

Disable unnecessary services:

```
linux:~ # chkconfig alsasound off
linux:~ # chkconfig cups off
linux:~ # chkconfig boot.kdump off
linux:~ # chkconfig boot.md off
linux:~ # chkconfig boot.lvm off
linux:~ # chkconfig lvm_wait_merge_snapshot off
linux:~ # chkconfig postfix off
linux:~ # chkconfig smartd off
linux:~ # chkconfig smb off
linux:~ # chkconfig smbfs off
linux:~ # chkconfig splash off
linux:~ # chkconfig splash_early off
linux:~ # chkconfig xdm off
linux:~ # chkconfig ntp on
```

Bond Linux Ethernet Interfaces

You usually must have a redundant network environment for a successful and stable system configuration. Only active-standby configurations are recommended for this configuration.

Example

```
/etc/sysconfig/network #
```

ifcfg-eth0

```
BOOTPROTO='none'  
MTU='9000'  
NAME='vNIC'  
REMOTE_IPADDR=''  
STARTMODE='off'  
UNIQUE='rBUF.GtN+arZDK79'  
USERCONTROL='no'  
_nm_name='bus-pci-0000:00:0c.0'
```

ifcfg-eth1

```
BOOTPROTO='none'  
MTU='9000'  
NAME='vNIC'  
REMOTE_IPADDR=''  
STARTMODE='off'  
UNIQUE='rBUF.FgrwMRwr45'  
USERCONTROL='no'  
_nm_name='bus-pci-0000:00:0d.0'
```

ifcfg-bond0

```
BOOTPROTO='static'  
BROADCAST='172.16.32.255'  
IPADDR='172.16.32.10'  
MTU='9000'  
NETMASK='255.255.255.0'  
NETWORK='172.16.32.0'  
REMOTE_IPADDR=''  
STARTMODE='onboot'  
BONDING_MASTER="yes"  
BONDING_MODULE_OPTS="mode=1 miimon=100"  
BONDING_SLAVE0='bus-pci-0000:00:0c.0'  
BONDING_SLAVE1='bus-pci-0000:00:0d.0'
```

VLAN Configuration

Use the following configuration:

```
/etc/sysconfig/network # cat ifcfg-vlan410
BOOTPROTO='static'
ETHERDEVICE='bond0'
IPADDR='172.20.253.180/26'
STARTMODE='onboot'
USERCONTROL='no'
VLAN=yes
```

SSH Key Distribution

Use the following configuration:

```
mgmtsrv01:~/ .ssh # ssh-copy-id -i id_rsa.pub server01
Password:*****
mgmtsrv02:~/ .ssh # ssh-copy-id -i id_rsa.pub server01
Password:*****
mgmtsrv01: # ssh server01
Last login: Mon Jan  9 15:00:57 2012 from mgmtsrv02.cisco-hana.corp
server01:~ #
```

sysctl.conf

Use the following configuration:

```
# Controls IP packet forwarding
net.ipv4.ip_forward = 0
# Do not accept source routing
net.ipv4.conf.default.accept_source_route = 0
# Controls the use of TCP syncookies
net.ipv4.tcp_syncookies = 1
fs.inotify.max_user_watches = 65536
kernel.shmmax = 9223372036854775807
kernel.sem = 1250 256000 100 8192
kernel.shmall = 1152921504606846720
kernel.shmmni = 524288
# SAP HANA Database
# Next line modified for SAP HANA Database on 2016.01.04_06.52.38
vm.max_map_count=588100000
fs.file-max = 20000000
fs.aio-max-nr = 196608
vm.memory_failure_early_kill = 1
#
net.core.rmem_max = 16777216
```

```
net.core.wmem_max = 16777216
net.core.rmem_default = 262144
net.core.wmem_default = 262144
#
net.core.optmem_max = 16777216
net.core.netdev_max_backlog = 300000
net.ipv4.tcp_slow_start_after_idle = 0
net.ipv4.conf.default.promote_secondaries = 1
net.ipv4.conf.all.promote_secondaries = 1
net.ipv4.icmp_echo_ignore_broadcasts = 1
net.ipv4.conf.default.accept_source_route = 0
net.ipv4.tcp_rmem = 65536 16777216 16777216
net.ipv4.tcp_wmem = 65536 16777216 16777216
#
net.ipv4.conf.default.accept_source_route = 0
net.ipv4.tcp_syncookies = 0
net.ipv4.tcp_dsack = 0
#
net.ipv4.tcp_no_metrics_save = 1
net.ipv4.tcp_moderate_rcvbuf = 1
net.ipv4.tcp_window_scaling = 1
net.ipv4.tcp_timestamps = 1
net.ipv4.tcp_sack = 1
sunrpc.tcp_slot_table_entries = 128
# Linux SAP swappiness recommendation
vm.swappiness=10
# Next line added for SAP HANA Database on 2015.09.16_02.09.34
net.ipv4.ip_local_port_range=40000 65300
```

Network Time Protocol Configuration

All SAP HANA systems (including storage systems) must have identical time settings. Therefore, you must set up the Network Time Protocol (NTP) as described here.

To configure the management station, you must specify <CUSTOMER_NTP_Server>:

```
mgmtsrv01:~ # vi /etc/ntp.conf
...
..
##
server <CUSTOMER_NTP_Server> # Generall Time Server
server 127.0.0.1 # Timeserver for the Appliance
fudge 127.127.1.0 stratum 10 # LCL is unsynchronized
...
.
mgmtsrv01:~ # ntpq -p
      remote           refid      st t when poll reach  delay  offset  jitter
=====
*timehost3.wdf.s .PPS.          1 u  61  64  377   0.954  -1.137  4.382
  localhost       .STEP.         16 l   -  64    0   0.000   0.000  0.000
mgmtsrv02:~ #
```

Configure all application nodes as follows:

```
server01:~ # ntpq -p
      remote           refid      st t when poll reach  delay  offset  jitter
=====
*mgmtsrv01m      10.17.120.30   2 u  14  64   3   0.280  -1.087  0.863
+mgmtsrv02m      10.17.122.27   2 u  13  64   3   0.311  -1.254  0.914
server01:~ #
```


SAP HANA Setup (Network File System)

You need to define the volumes on the NAS system. The recommended approach is to split the data and log volumes between the two storage systems. Refer to NetApp TR-4290 for detailed storage information.

Figure 142. Volume Layout

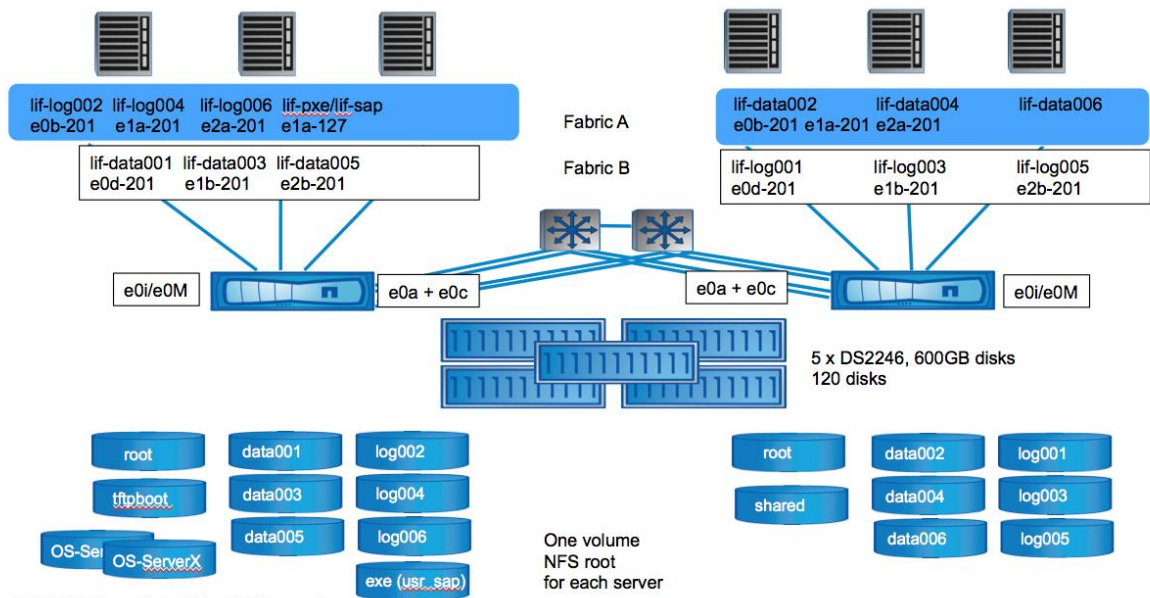


Figure 143 shows the volume layout for the NetApp FAS8040.

SAP HANA Setup (SAN)

After the SAN LUNs have been created and the SAN zoning has been configured correctly, you need to be able to see all the LUNs on the system. Create the file systems on the visible LUNs.

Note that for SAN multipathing, only the default Linux Multipath I/O (MPIO) driver is supported for multipathing in the SAN environment. Any other driver, such as EMC PowerPath, must be supported by the specific driver.

mkfs.xfs

```
mkfs.xfs -f -b size=4096 /dev/sapdatavg/datavol
mkfs.xfs -f -b size=4096 /dev/sapdatavg/logvol
mkfs.xfs -f -b size=4096 /dev/ sapdatavg /sapmnt
```

/etc/fstab

```
<DEVICE>/data-lun /hana/data      xfs
nobarrier,noatime,nodiratime,logbufs=8,logbsize=256k,async 1 2
<DEVICE>/log-lun /hana/log        xfs
nobarrier,noatime,nodiratime,logbufs=8,logbsize=256k,async 1 2
<DEVICE>/shared-lun /hana/shared      xfs defaults 1 2
```

/etc/after.local

```
#!/bin/bash
# (c) Cisco Systems Inc. 2014
# - after.local
#
# Performance Settings
# SAP Note 1824819
echo "Setting the CPU Speed to PERFORMANCE for SAP HANA"
/usr/bin/cpupower frequency-set -g performance 2>&1
# Disable THP on the system
echo never > /sys/kernel/mm/transparent_hugepage/enabled
. /etc/rc.status
# IO scheduler
echo deadline > /sys/block/<DEVICE>/queue/scheduler
#
echo 4096 > /sys/block/<DEVICE>/queue/nr_requests
#
echo 4096 > /sys/block/<DEVICE>/queue/read_ahead_kb
```

SAP HANA Installation

Use the official SAP documentation, which describes the installation process with and without the SAP unified installer.

For the SAP HANA installation documentation, see http://help.sap.com/hana_appliance.

All other SAP installation and administration documentation is available at <http://service.sap.com/instguides>.

SAP Notes

Read the following SAP Notes before you start the installation process. These SAP Notes contain the latest information about the installation, as well as corrections to the installation documentation. Make sure that you have the most up-to-date version of each SAP Note, which you can find at the SAP Service Marketplace at <https://service.sap.com/notes>.

SAP HANA IMDB Notes

- SAP Note 1730999: Configuration changes in SAP HANA appliance
- SAP Note 1514966: SAP HANA 1.0: Sizing SAP In-Memory Database
- SAP Note 1780950: Connection problems due to host name resolution
- SAP Note 1780950: SAP HANA SPS06: Network setup for external communication
- SAP Note 1743225: SAP HANA: Potential failure of connections with scale-out nodes
- SAP Note 1755396: Released disaster-tolerant solutions for SAP HANA with disk replication
- SAP Note 1890444: SAP HANA system slow due to CPU power save mode

Linux Notes

- SAP Note 1824819: SAP HANA database: Recommended OS settings for SLES 11 and SLES 4 SAP SP2
- SAP Note 1731000: Unrecommended configuration changes
- SAP Note 1557506: Linux paging improvements
- SAP Note 1310037: SUSE Linux Enterprise Server 11 installation notes
- SAP Note 1726839: SAP HANA Database: Potential crash when using XFS file system
- SAP Note 1740136: SAP HANA: Wrong mount option may lead to corrupt persistency
- SAP Note 1829651: Time-zone settings in SAP HANA scale-out landscapes

SAP Application Notes

- SAP Note 1658845: SAP HANA database hardware check
- SAP Note 1637145: SAP BW on SAP HANA: Sizing SAP In-Memory Database
- SAP Note 1661202: Support for multiple applications on SAP HANA
- SAP Note 1681092: Support for multiple SAP HANA databases on one SAP HANA (Multi-SID)
- SAP Note 1577128: Supported clients for SAP HANA 1.0
- SAP Note 1808450: Homogenous system landscape for SAP HANA BW

Notes About Third-Party Software

- SAP Note 1730928: Using external software in a SAP HANA appliance
- SAP Note 1730929: Using external tools in an SAP HANA appliance
- SAP Note 1730930: Using antivirus software in an SAP HANA appliance
- SAP Note 1730932: Using backup tools with Backint for SAP HANA

SAP HANA Virtualization Notes

- SAP Note 1788665: SAP HANA running on VMware vSphere virtual machines
- SAP Note 1788665 (update September 10, 2013): Note now mentions SAP HANA TDI tool

SAP HANA High Availability (Scale-Out Only)

Since SAP HANA Revision 35, the `ha_provider` Python class supports the STONITH function (STONITH = Shoot The Other Node In The Head). With this Python class, you can reboot the failing node to prevent a split brain situation and thus inconsistency in the database. Because NFSv3 is used, you must implement the STONITH function to prevent the database corruption because of double-mounted file systems. If the database fails over to another node, the failed node will be rebooted from the primary name server. This feature eliminates the risk of double-mounted file systems.

Configure High Availability

The management node contains the two configuration files located in the `C880_HA_Scripts.tar` package.

Copy both files to `/hana/shared/HA` and adapt the user settings.

At the Cisco C880 M4 console, prepare the script to match the configured IPMI user name and password. The default settings are `ipmi-user sapadm` and `ipmi-user-password cisco`.

```
linux:/ # mkdir /hana/shared/HA
linux:/ # cd /hana/shared/HA
linux:/ # tar -xvf /tmp/C880_HA_Scripts.tar
linux:/ # chown -R anaadm:sapsys /hana/shared/HA
linux:/ # ls -l /hana/shared/HA
-rwxr-xr-x 1 root root 1225 Jul  3 14:25 ucs_ha_class.py
-rwxr-xr-x 1 root root 2058 Jul 28 18:50 ucs_ipmi_reset.sh
mgmtsrv06:/opt/Cisco/scripts # vi ucs_ipmi_reset.sh
cishana01:/hana/shared/HA # cat ucs_ipmi_reset.sh
#!/bin/bash
# Cisco Systems Inc.
# SAP HANA High Availability
# Version c880.01
# changelog: 30/12/2015: Changed for C880
if [ -z $1 ]
then
    echo "please add the hostname to reset to the command line"
    exit 1
fi
# Trim the domain name off of the hostname
host=`echo "$1" | awk -F'.' '{print $1}'`
PASSWD=cisco
USER=sapadm
```

Enable the SAP HANA Storage Connector API

The SAP Storage Connector API provides a way to call a user procedure whenever the SAP HANA name server triggers a node failover. The API requires the files mentioned here.

Run the procedure on the primary name server.

To activate the procedure in the event of a node failover, edit the global.ini file in <HANA installdirectory>/<SID>/global/hdb/custom/config/ and add the following entry:

```
[Storage]
ha_provider = ucs_ha_class
ha_provider_path = /hana/shared/HA
```

```
server01: # cd /hana/shared/<SID>/global/hdb/custom/config
server01:/hana/shared/ANA/global/hdb/custom/config # ls -l
-rw-r----- 1 anaadm sapsys  90 Feb 15 11:22 global.ini
-rw-rw-r-- 1 anaadm sapsys 9560 Feb 15 11:23 hdbconfiguration_1
drwxr-x--- 3 anaadm sapsys 4096 Feb 15 11:22 lexicon
-rw-r--r-- 1 anaadm sapsys  128 Feb 15 12:34 nameserver.ini
server01:/hana/shared/ANA/global/hdb/custom/config #
server01:/hana/shared/ANA/global/hdb/custom/config # vi global.ini
[persistence]
basepath_datavolumes=/hana/data/ANA
basepath_logvolumes=/hana/log/ANA
[storage]
ha_provider = ucs_ha_class
ha_provider_path = /hana/shared/HA
```

To activate the change, restart the SAP HANA database.

Test the IPMI Connectivity

Test the IPMI connectivity on all nodes. Note that 02 means power up, and 00 means power down.

```
mgmtsrv01:/ # ipmitool -I lanplus -H server01-ipmi -U sapadm -P cisco -t 0x24
raw 0x30 0x71 0x00
02 08 00 01 02 03 80 81 82 83
mgmtsrv01:/ #
```

Make sure that all nodes respond to the **ipmitool** command.

Make sure that all MMB IP addresses are in the /etc/host file of the appliance.

```
mgmtsrv01:/opt/Cisco/scripts # grep ipmi /etc/hosts
192.168.76.28  server03-ipmi  server03-ipmi
192.168.76.29  server01-ipmi  server01-ipmi
192.168.76.37  server04-ipmi  server04-ipmi
192.168.76.38  server02-ipmi  server02-ipmi
mgmtsrv01:/opt/Cisco/scripts #
```

The Python class will be called from the primary name server of the SAP HANA database. Therefore, the Python class must be mentioned in the global.ini file.

Autostart SAP HANA

If you prefer to have the SAP HANA system started automatically after a reset, you can enable the **autostart** function in the instance profile of SAP HANA. You will need to configure this function in all instance profiles.

```
server01:/hana/shared/ANA/profile # vi ANA_HDB00_server01
...
..
Autostart = 1
...
..
```

SAP HANA Failover Test (Scale-Out Only)

It is very important to test the node failover before you release the system to the customer.

If a SAP HANA node is reset by the primary name server, a log entry is written in the `/var/log/messages` file of the primary name server.

```
Aug 26 17:24:54 server01 logger: STONITH HANA Node:server05
Aug 26 17:24:55 server01 logger: anaadm Resetting the HANA Node server05
because of an Nameserver reset command
Aug 26 17:25:58 server01 logger: anaadm HANA Node server05 switched from ON to
OFF
Aug 26 17:27:00 server01 logger: anaadm HANA Node server05 switched from OFF
to ON
Aug 26 17:27:01 server01 logger: anaadm Release NFS locks of HANA Node
server05 done, system is booting
```

Make sure that all nodes respond to the `ipmitool` command.

Make sure that all management IP addresses are in the `/etc/host` file of the appliance.

```
mgmtsrv01:/opt/Cisco/scripts # grep ipmi /etc/hosts
192.168.76.28 server03-ipmi server03-ipmi
192.168.76.29 server01-ipmi server01-ipmi
192.168.76.37 server04-ipmi server04-ipmi
192.168.76.38 server02-ipmi server02-ipmi
mgmtsrv01:/opt/Cisco/scripts #
```

If the SAP HANA primary name server is “killing” one of the nodes, a status message is written in the `/var/log/messages` file of the primary name server. The output looks like the following text. The default response of the STONITH process is to reboot the node.

```
cishana01:/hana/shared # grep logger /var/log/messages
Aug 17 02:52:13 cishana01 logger: STONITH HANA Node:cishana02
Aug 17 02:52:13 cishana01 logger: anaadm Resetting the HANA Node cishana02
because of an Nameserver reset command
Aug 17 02:52:27 cishana01 logger: anaadm HANA Node cishana02 switched from ON
to OFF
Aug 17 02:52:35 cishana01 logger: anaadm HANA Node cishana02 switched from OFF
to ON
Aug 17 02:52:35 cishana01 logger: anaadm Release NFS locks of HANA Node
cishana02 done, system is booting
cishana01:/hana/shared #
```


From the SAP HANA Studio, failover will look like Figures 143 through 146.

Figure 143. Normal Operation

Host	Active	Host Status	Fail...	Name Server R...	Name Serv...	Index Server Ro...	Index Server ...	Failover Gro...	Failover Group (Actual)	Storage Partition
server01	YES	OK		MASTER 1	MASTER	WORKER	MASTER	default	default	1
server02	YES	OK		SLAVE	SLAVE	WORKER	SLAVE	default	default	2
server03	YES	OK		SLAVE	SLAVE	WORKER	SLAVE	default	default	3
server04	YES	OK		MASTER 2	SLAVE	WORKER	SLAVE	default	default	7
server05	YES	OK		SLAVE	SLAVE	WORKER	SLAVE	default	default	5
server06	YES	OK		MASTER 3	SLAVE	WORKER	SLAVE	default	default	6
server07	YES	OK		SLAVE	SLAVE	WORKER	SLAVE	default	default	4
server08	YES	OK		SLAVE	SLAVE	WORKER	SLAVE	default	default	8
server09	YES	OK		SLAVE	SLAVE	WORKER	SLAVE	default	default	9
server10	YES	OK		SLAVE	SLAVE	WORKER	SLAVE	default	default	10
server11	YES	OK		SLAVE	SLAVE	WORKER	SLAVE	default	default	11
server12	YES	IGNORE		SLAVE	SLAVE	STANDBY	STANDBY	default	default	-

Figure 144. Failover Detected

Host	Active	Host Status	Failover Status	Name Server Role (Configured)	Name Server Role (Actual)	Index Server Role (Configured)	Index Server Role (Actual)	Failover
server01	YES	OK		MASTER 1	MASTER	WORKER	MASTER	default
server02	YES	OK		SLAVE	SLAVE	WORKER	SLAVE	default
server03	YES	OK		SLAVE	SLAVE	WORKER	SLAVE	default
server04	YES	OK		MASTER 2	SLAVE	WORKER	SLAVE	default
server05	NO	WARNING	STARTED	SLAVE	SLAVE	WORKER	SLAVE	default
server06	YES	OK		MASTER 3	SLAVE	WORKER	SLAVE	default
server07	YES	OK		SLAVE	SLAVE	WORKER	SLAVE	default
server08	YES	OK		SLAVE	SLAVE	WORKER	SLAVE	default
server09	YES	OK		SLAVE	SLAVE	WORKER	SLAVE	default
server10	YES	OK		SLAVE	SLAVE	WORKER	SLAVE	default
server11	YES	OK		SLAVE	SLAVE	WORKER	SLAVE	default
server12	YES	IGNORE		SLAVE	SLAVE	STANDBY	STANDBY	default

Figure 145. Failover Initiated

Host	Active	Host Status	Failover Status	Name Server Role (Configured)	Name Server Role (Actual)	Index Server Role (Configured)	Index Server Role (Actual)
server01	YES	OK		MASTER 1	MASTER	WORKER	MASTER
server02	YES	OK		SLAVE	SLAVE	WORKER	SLAVE
server03	YES	OK		SLAVE	SLAVE	WORKER	SLAVE
server04	YES	OK		MASTER 2	SLAVE	WORKER	SLAVE
server05	NO	WARNING	FAILOVER TO SERVER12	SLAVE	SLAVE	WORKER	STANDBY
server06	YES	OK		MASTER 3	SLAVE	WORKER	SLAVE
server07	YES	OK		SLAVE	SLAVE	WORKER	SLAVE
server08	YES	OK		SLAVE	SLAVE	WORKER	SLAVE
server09	YES	OK		SLAVE	SLAVE	WORKER	SLAVE
server10	YES	OK		SLAVE	SLAVE	WORKER	SLAVE
server11	YES	OK		SLAVE	SLAVE	WORKER	SLAVE
server12	STARTING	WARNING		SLAVE	SLAVE	STANDBY	SLAVE

Figure 146. Failover Complete

The screenshot shows the SAP HANA System Administration console for 'ANA (SYSTEM)' at IP 192.168.76.101. The 'Hosts' tab is selected, displaying a table with columns for Host, Active status, Host Status, Failover Status, Name Server Role (Configured), Name Server Role (Actual), Index Server Role (Configured), Index Server Role (Actual), and Failover Group. The table lists 12 servers (server01 to server12) with their respective roles and statuses. Server05 is the only one with a 'NO' active status and 'INFO' host status.

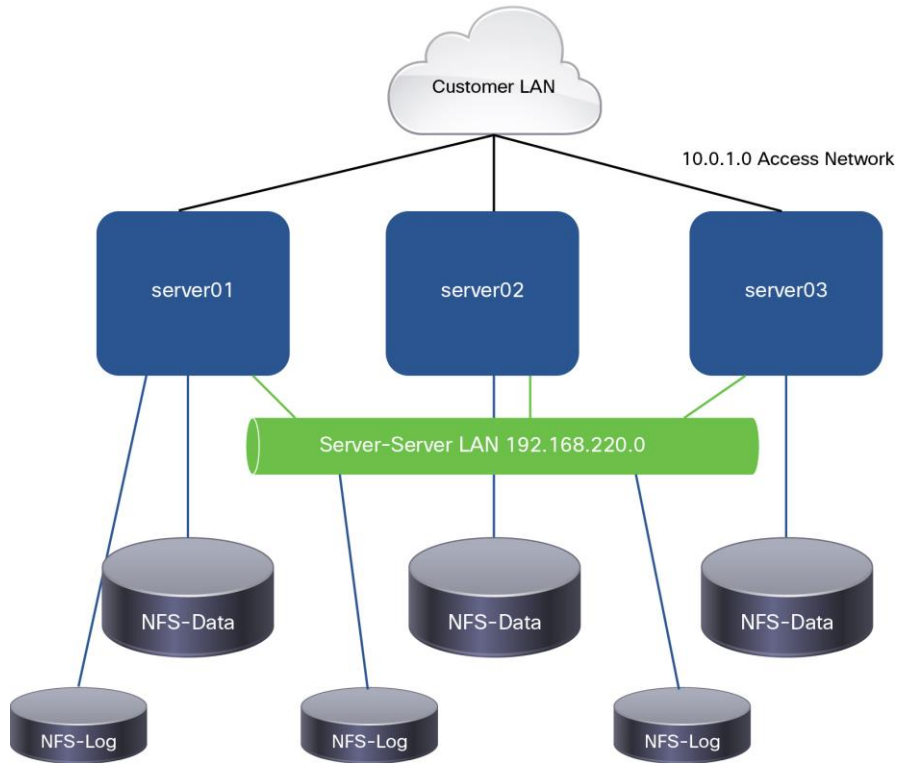
Host	Active	Host Status	Failover Status	Name Server Role (Configured)	Name Server Role (Actual)	Index Server Role (Configured)	Index Server Role (Actual)	Failover G
server01	YES	OK		MASTER 1	MASTER	WORKER	MASTER	default
server02	YES	OK		SLAVE	SLAVE	WORKER	SLAVE	default
server03	YES	OK		SLAVE	SLAVE	WORKER	SLAVE	default
server04	YES	OK		MASTER 2	SLAVE	WORKER	SLAVE	default
server05	NO	INFO		SLAVE	SLAVE	WORKER	STANDBY	default
server06	YES	OK		MASTER 3	SLAVE	WORKER	SLAVE	default
server07	YES	OK		SLAVE	SLAVE	WORKER	SLAVE	default
server08	YES	OK		SLAVE	SLAVE	WORKER	SLAVE	default
server09	YES	OK		SLAVE	SLAVE	WORKER	SLAVE	default
server10	YES	OK		SLAVE	SLAVE	WORKER	SLAVE	default
server11	YES	OK		SLAVE	SLAVE	WORKER	SLAVE	default
server12	YES	INFO		SLAVE	SLAVE	STANDBY	SLAVE	default

SAP HANA Server Network Configuration

The default communication path among the SAP HANA nodes uses the access network (in this example, VLAN 301), which has an MTU value of 1500. To optimize the internode traffic, the MTU value needs to be 9000, which is already set in the storage VLAN (in this example, VLAN 220). Hence, you need to change the traffic to the access VLAN as shown here (Figure 147).

As part of setting up a distributed system, you need to configure the network parameters. Make sure that you do this before you add hosts because one server needs to be available so that you can connect to the SAP HANA Studio. For more information, refer to the SAP HANA administration guide.

Figure 147.



```

server01:/> sapcontrol -nr 42 -function StopSystem HDB
server01:/> netstat -ia
Kernel Interface table
  Iface      MTU Met    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-
OVR Flg
eth0      1500 0   335051   0   94   0   192786   0   0
0 BMRU
eth1        1500  0     160      0     0     0     15      0     0
0 BMRU
eth2        9000  0     91       0     0     0     12      0     0
0 BMRU
eth3        9000  0     87       0     0     0     11      0     0
0 BMRU
eth4        9000  0  1181301   0     0     0  3183694   0     0
0 BMRU
eth5        9000  0  35809384  0     0     0  48992286  0     0
0 BMRU
eth6        1500  0     85       0     0     0     11      0     0
0 BMRU
eth7        9000  0     700      0     0     0     735     0     0
0 BMRU
eth8        9000  0     86       0     0     0     11      0     0
0 BMRU
lo          16436 0     308      0     0     0     308     0     0
0 LRU
[root@server01 ~]#

linux1:~ #

```

Before the change, all internal SAP HANA traffic goes over the access LAN (eth2).

```
server01:/> vi /hana/shared/ANA/global/hdb/custom/config/global.ini
[communication]
listeninterface = .internal
#listeninterface = .global
#listeninterface = .local
#listeninterface = 192.168.220.0/24
[internal_hostname_resolution]
192.168.220.101 = server01
192.168.220.102 = server02
192.168.220.103 = server03
192.168.220.104 = server04
server01:/ > sapcontrol -nr 42 -function StartSystem HDB
04.10.2013 12:14:01
StartSystem
OK
server01:/ > hdbnsutil -reconfig -hostnameResolution=internal
```

For more information, see:

- http://help.sap.com/saphelp_hanaplatform/helpdata/en/32/c22f81e8c14268a4e5de01cd033e8f/content.htm
- http://help.sap.com/saphelp_hanaplatform/helpdata/en/0c/6738ab85c64da1aed0fa91c25ed47c/content.htm

```
linux1:/ > sapcontrol -nr 42 -function GetSystemInstanceList
04.10.2013 12:20:21
GetSystemInstanceList
OK
hostname, instanceNr, httpPort, httpsPort, startPriority, features, dispstatus
linux2, 42, 54213, 0, 0.3, HDB, GREEN
linux4, 42, 54213, 0, 0.3, HDB, GREEN
linux1, 42, 54213, 0, 0.3, HDB, GREEN
linux3, 42, 54213, 0, 0.3, HDB, GREEN
linux1:/ > exit
linux1:~ # netstat -ia
Kernel Interface table
Iface MTU Met RX-OK RX-ERR RX-DRP RX-OVR TX-OK TX-ERR TX-DRP
eth0 9000 0 20242 0 0 0 20171 0 0
eth1 1500 0 505653 0 0 0 1902027 0 0
eth2 1500 03158299 0 3 0 41251411 0 0
eth3 1500 0 0 0 0 0 0 0 0
linux1:~ #
```

After the change, all internal SAP HANA traffic goes over the server LAN (eth7).

SAP HANA Hardware Configuration Check Tool Preparation

To prepare the necessary parameter files, you need to know the specific storage settings for the NetApp FAS8040 with cluster data ONTAP to archive the KPIs.

You should download the latest SAP HANA Hardware Configuration Check Tool (HWCCT) from the SAP marketplace.

After parsing the test, persist the settings in the database.

These files show the necessary test parameters.

OS Validation

```
{
  "report_id": "ntap_evalos",
  "use_hdb": false,
  "blades": [
    "cishana01"
  ],
  "tests": [
    {
      "package": "LandscapeTest",
      "test_timeout": 0,
      "id": 1,
      "config": {},
      "class": "EvalOs"
    }
  ]
}
```

Storage Test

Note: The values presented for the data and log tests (async...) + (max_pa...) are storage specific and must be checked and validated by the SAP HANA TDI storage vendor.

```

{
  "report_id": "netapp_8_nodes",
  "use_hdb": false,
  "blades": [
    "cishana01"
  ],
  "tests": [
    {
      "id": 1,
      "package": "FilesystemTest",
      "test_timeout": 0,
      "config": { "mount": {
        "cishana01": ["/hana/log/ANA/mnt00001/"]
      },
        "parameter": { "max_parallel_io_requests": "128",
          "async_read_submit": "on",
          "async_write_submit_active": "on",
          "max_parallel_io_requests" = "128",
          "async_write_submit_blocks": "all" },
        "duration": "long"
      },
      "class": "LogVolumeIO"
    },
    {
      "id": 2,
      "package": "FilesystemTest",
      "test_timeout": 0,
      "config": { "mount": {
        "cishana01": ["/hana/data/ANA/mnt00001/"]
      },
        "para",
          "async_read_submit": "on",
          "async_write_submit_active": "on",
          "max_parallel_io_requests" = "128",
          "async_write_submit_blocks": "all" },
        "duration": "long"
      },
      "class": "DataVolumeIO"
    }
  ]
}

```

Configure the settings to persist in the database (SAP Note <http://service.sap.com/sap/support/notes/1930979>).
 Make sure that the database is running.

```
cishana01:/usr/sap/ANA/HDB00> sapcontrol -nr 00 -function GetSystemInstanceList
03.09.2015 20:58:44
GetSystemInstanceList
OK
hostname, instanceNr, httpPort, httpsPort, startPriority, features, dispstatus
cishana01, 0, 50013, 50014, 0.3, HDB, GREEN
```

Because **hdbparam** must be run on every data file, you first must collect all the data files.

```
cishana01:/usr/sap/ANA/HDB00> ls -lR /hana/data/ANA/
/hana/data/ANA/:
drwxr-x--- 5 anaadm sapsys 4096 Aug 28 01:33 mnt00001
/hana/data/ANA/mnt00001/hdb00001:
-rw-rw-r-- 1 anaadm sapsys 342114304 Sep  3 18:41 datavolume_0000.dat
/hana/data/ANA/mnt00001/hdb00002:
-rw-r--r-- 1 anaadm sapsys 3473588224 Sep  3 18:42 datavolume_0000.dat
/hana/data/ANA/mnt00001/hdb00003:
-rw-r--r-- 1 anaadm sapsys 341671936 Sep  3 18:42 datavolume_0000.dat
```

Run these commands for all four parameters:

```
max_parallel_io_requests = 128
async_read_submit = on
async_write_submit_active = on
async_write_submit_blocks = all
```


Example (user = <SID>adm)

```
cishana01:/usr/sap/ANA/HDB00> hdbparam --paramset
fileio"[/hana/data/ANA/mnt00001/hdb00001/]".max_parallel_io_requests=128
Following servers available:
  1: host [cishana01] port 030001      NameServer      ActiveYes; pid 30859
  2: host [cishana01] port 030002      Preprocessor     ActiveYes; pid 30987
...
..
.
cishana01:/usr/sap/ANA/HDB00> hdbparam --paramset
fileio"[/hana/data/ANA/mnt00001/hdb00001/]".async_read_submit=on
Following servers available:
  1: host [cishana01] port 030001      NameServer      ActiveYes; pid 30859
  2: host [cishana01] port 030002      Preprocessor     ActiveYes; pid 30987
...
..
.
cishana01:/usr/sap/ANA/HDB00> hdbparam --paramset
fileio"[/hana/data/ANA/mnt00001/hdb00001/]".async_write_submit_active=on
Following servers available:
  1: host [cishana01] port 030001      NameServer      ActiveYes; pid 30859
  2: host [cishana01] port 030002      Preprocessor     ActiveYes; pid 30987
...
..
.
cishana01:/usr/sap/ANA/HDB00> hdbparam --paramset
fileio"[/hana/data/ANA/mnt00001/hdb00001/]".async_write_submit_blocks=all
Following servers available:
  1: host [cishana01] port 030001      NameServer      ActiveYes; pid 30859
  2: host [cishana01] port 030002      Preprocessor     ActiveYes; pid 30987
...
..
.
```

Continue this process for every SAP HANA data file.

For More Information

- SAP HANA end-user documentation: <http://help.sap.com/hana/>
- SLES deployment guide:
https://www.suse.com/documentation/sles11/pdfdoc/book_sle_deployment/book_sle_deployment.pdf
- SLES administration guide:
https://www.suse.com/documentation/sles11/pdfdoc/book_sle_admin/book_sle_admin.pdf
- Cisco UCS 6248UP 48-Port Fabric Interconnect hardware installation guide:
http://www.cisco.com/en/US/docs/unified_computing/ucs/hw/6200/install/6200_HIG.pdf
- Cisco UCS 5108 Blade Server Chassis hardware installation guide:
http://www.cisco.com/en/US/docs/unified_computing/ucs/hw/chassis/install/5108_HIG.pdf
- Cisco UCS B440 M2 Blade Server installation notes:
http://www.cisco.com/en/US/docs/unified_computing/ucs/hw/chassis/install/quadblade.pdf
- Cisco Nexus 5000 Series Switches hardware installation guide:
http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/hw/installation/guide/n5k_hig.pdf
- Cisco Nexus 2000 Series Fabric Extenders hardware installation guides:
http://www.cisco.com/en/US/docs/switches/datacenter/nexus2000/hw/installation/guide/N2KFEX_HIG.pdf
<http://www.cisco.com/en/US/docs/switches/datacenter/nexus2000/hw/installation/guide/overview.pdf>
- Cisco 2911 Integrated Services Router:
http://www.cisco.com/en/US/docs/routers/access/2900/hardware/installation/guide/2900_3900_HIG.pdf
- Cisco UCS C220 M3 Rack Server hardware installation guide:
http://www.cisco.com/en/US/docs/unified_computing/ucs/c/hw/C220/install/C220.pdf
- Cisco R Series Rack PDU installation guide:
http://www.cisco.com/en/US/docs/unified_computing/ucs/hw/rack_power/installation/guide/Rack-PDU.pdf



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax 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: www.cisco.com/go/trademarks. 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. (1110R)