



## Prepare Customer Site Servers

---

- [Prepare Customer Site Servers, on page 1](#)
- [Prepare Cisco UCS C-Series Customer Site Servers, on page 1](#)
- [Prepare Cisco UCS B-Series Customer Site Servers, on page 5](#)
- [NTP and Time Synchronization, on page 15](#)
- [Global Catalog Requirements, on page 18](#)

## Prepare Customer Site Servers

Perform all the procedures in this section on the Side A and the Side B servers.

## Prepare Cisco UCS C-Series Customer Site Servers

### Configure RAID for the C240 M3S TRC#1

For each array created using this procedure, use the following settings:

- Stripe size: 128KB
- Read Policy: Read Ahead Always
- Write Policy: Write Back with BBU

#### Procedure

---

- Step 1** Power on the UCS server, making sure that Quiet Boot is disabled in BIOS.
- Step 2** Press **Ctrl-H** during the initial startup sequence to enter the MegaRAID BIOS configuration utility.
- Step 3** Click **Start**.
- Step 4** Select **Configuration Wizard** on the left panel. Click **New Configuration**. Then click **Next**.
- Step 5** At the prompt to clear the configuration, click **Yes**.
- Step 6** Select **Manual Configuration**. Then click **Next**.
- Step 7** On the next screen, in the left panel, add the first eight drives to create Drive Group0 as follows:

- a) Select drives 1 - 8.
- b) Click **Add to Array**.
- c) Click **Accept DG**.

**Step 8** Add the remaining eight drives to create Drive Group1 as follows:

- a) On the left panel, select drives 9 - 16.
- b) Click **Add to Array**.
- c) Click **Accept DG**.
- d) Click **Next** to accept the Drive Group.

**Step 9** Add Drive Group0 to a span as follows:

- a) Select **Drive Group0**.
- b) Click **Add to Span**.
- c) Click **Next**.

**Step 10** Configure RAID for Drive Group0 as follows:

- a) For RAID Level, select **RAID 5**.
- b) For Stripe Size, select **128KB**.
- c) For Read Policy, select **read ahead = always**.
- d) For Write Policy, select **write back with bbu**.
- e) Click **Update Size** to finalize the RAID volume and to determine the size of the resulting volume. It resolves to 1.903TB
- f) Click **Accept** to accept the virtual drive definition, VD0.
- g) Click **Next**.
- h) Click **Back** to add the second RAID 5 array.

**Step 11** Click **Back** to add the second RAID 5 array as follows:

- a) Select **Drive Group1**.
- b) Click **Add to Span**.
- c) Click **Next**.

**Step 12** At the **RAID Selection** screen:

- a) For RAID Level, select **RAID 5**.
- b) For Stripe Size, select **128KB**.
- c) For Read Policy, select **read ahead = always**.
- d) For Write Policy, select **write back with bbu**.
- e) Click **Update Size**. The size resolves to 1.903TB.
- f) Click **Accept** to accept the virtual drive definition, VD1.

**Step 13** Click **Yes** at the BBU warning screen.

**Step 14** Click **Next** at the Virtual Live Definition screen to indicate that you have finished defining virtual drives.

**Step 15** Click **Accept** at the Configuration Preview screen to accept the RAID configuration.

**Step 16** Click **Yes** to save the configuration.

**Step 17** Click **Yes** to start drive configuration.

**Step 18** Click **Home** to exit the Wizard when both drives report their status as Optimal.

**Step 19** Click **Exit**.

After RAID configuration is complete on the drives, the system may try to initialize (format) the new RAID array. In this event, the current initialization progress can be seen from the **Web BIOS** screen. Wait for the

background initialization to complete before proceeding with any of the subsequent server configuration steps such as installing ESXi.

You can check background initialization progress on either the **Web BIOS Home** screen or **Virtual Drives** screen.

---

## Configure RAID for C240 M4SX

The disk array configuration for the C240 M4SX is already set up to match what is required for Packaged CCE. Verify the settings as follows.

### Procedure

---

Using Cisco Integrated Management Controller, check that the following settings are configured correctly:

- Virtual Drive Info: RAID 5 with 5 (Physical Disks) \* 4 (Virtual Drives/Datastores)
- Stripe Size: 128KB
- Write Policy: Write Back with BBU
- Read Policy: Read Ahead Always

For more information regarding RAID configuration for C240 M4SX in Configure RAID with GUI (UCS C-Series M4 Servers) section, see *Cisco Collaboration on Virtual Servers* Guide at: [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cucm/virtual/CHCS\\_BK\\_C7C7ED05\\_00\\_cisco-collaboration-on-virtual-servers/CHCS\\_BK\\_C7C7ED05\\_00\\_cisco-collaboration-on-virtual-servers\\_chapter\\_01.html#CUCM\\_TK\\_C2DC4F2D\\_00](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/virtual/CHCS_BK_C7C7ED05_00_cisco-collaboration-on-virtual-servers/CHCS_BK_C7C7ED05_00_cisco-collaboration-on-virtual-servers_chapter_01.html#CUCM_TK_C2DC4F2D_00).

---

## Configure RAID for C240 M5SX

The disk array configuration for the UCS C240 M5SX is already set up to match the requirements. Verify the settings as follows:

### Procedure

---

Using Cisco Integrated Management Controller, check that the following settings are configured correctly:

- Virtual Drive Info: RAID 5 with 6 (Physical Disks) \* 4 (Virtual Drives or Datastores)
- Stripe Size: 128KB
- Write Policy: Write Back with BBU
- Read Policy: Read Ahead Always

For more information regarding RAID configuration for C240 M5SX, see the *Installation and Configuration* section of the *Cisco Collaboration on Virtual Servers Guide* at:

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cucm/virtual/chcs\\_b\\_cisco-collaboration-on-virtual-servers.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/virtual/chcs_b_cisco-collaboration-on-virtual-servers.html)

---

## Install VMware vSphere ESXi

Packaged CCE uses standard VMware vSphere ESXi installation procedures. For installation procedures to install the supported version of vSphere ESXi that you are installing, see the VMware documentation at <https://www.vmware.com/support/pubs/>.

For Packaged CCE, you must install the ESXi on the first drive as the default boot drive for the server. Packaged CCE has no unique requirements.

### Add the Datastores to the Host Server

After installing vSphere ESXi, add the remaining datastores. Refer to the *vSphere Storage Guide* for the vSphere ESXi version in your deployment, available at <https://www.vmware.com/support/pubs/>.

Required datastores are dictated by the hardware platform used. Cisco UCS C-Series servers require a fixed and validated configuration.

### Add the Customer ESXi Host to the vCenter

Refer to the vCenter Server and Host Management documentation at <https://www.vmware.com/support/pubs/>

Customers without vCenter can install on management desktops to administer the Packaged CCE servers.

## Run the RAID Config Validator Utility

After you set up RAID configuration and add the datastores, run the RAID Config Validator utility to ensure that your datastore configuration is correct.

### Before you begin

To run the utility, Java 7 (any update) must be installed. Java 8 and later releases are not supported.

### Procedure

---

- Step 1** Download the Packaged CCE RAID Config Validator utility from the **Packaged CCE Download Software > Deployment Scripts** page at <https://software.cisco.com/download/type.html?mdfid=284360381&i=rm>. Extract the zip file locally.
- Step 2** Open the Windows command prompt and change to the directory where you downloaded the file.
- Step 3** Enter this command to run the tool: **java -jar PackagedCCERaidConfigValidator-<version>.jar <IP Address of the Side A ESXi host> <username> <password>**

For example:

```
C:\Users\Administrator\Desktop>java -jar PackagedCCERaidConfigValidator-11.0.jar xx.xx.xxx.xxx  
userName password
```

Messages appear on the monitor to show that the validation is starting. You then see an indication of a valid or invalid configuration.

- Step 4** If your configuration is valid, repeat step 2. Enter the IP address of the Side B server instead of the Side A server.

---

### What to do next

If the utility reports an invalid configuration, you must recreate the RAID configuration. To do this, reset the RAID configuration, re-install ESXi, and then re-run the RAID Config Validator utility to re-validate the configuration.

RAID configuration errors include:

- Non-supported server found or used.
- Incorrect number of datastores found.
- Incorrect sizes set for the datastores.

## Prepare Cisco UCS B-Series Customer Site Servers

Before you complete the configuration steps in this section, the customer site UCS B-Series must be installed, configured, and operational.

For additional information and guidance on UCS B-Series installation and configuration, refer to the UCS B-Series documentation (<https://www.cisco.com/c/en/us/products/servers-unified-computing/product-listing.html>) or your Cisco Data Center Unified Computing Authorized Technology Provider.

This section includes only specific configuration requirements for Packaged CCE deployments on the UCS B-Series platform. Customers may have varying design and configuration needs due to their data center requirements and infrastructure. However, all configurations must meet the Packaged CCE requirements for high availability. For example, the design must not create the potential for a single point of failure, which can adversely impact the operation of Cisco call processing applications.

UCS B-Series may have a variable number of LUNs on the SAN provisioned to meet Packaged CCE IOPS requirements.

See the *Virtualization for Cisco Packaged CCE* at [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/uc\\_system/virtualization/pcce\\_virt\\_index.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/virtualization/pcce_virt_index.html) for IOPs requirements.



---

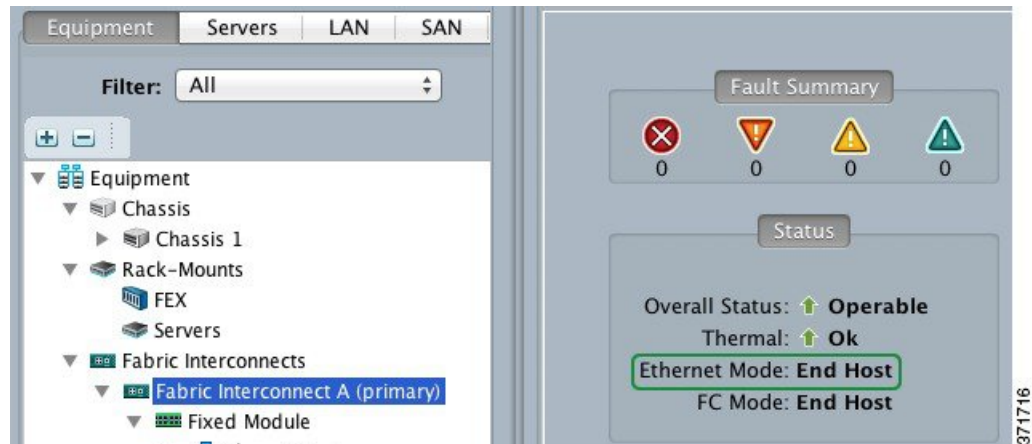
**Note** All UCS hardware configuration examples in this section use the Cisco UCS Manager GUI. You can also use the UCS Manager CLI or API.

---

# Fabric Interconnect Requirements

## Ethernet Mode

The Fabric Interconnects' Ethernet Mode must be set to End Host.



## Ethernet Uplinks

Cisco UCS Fabric Interconnect Ethernet uplinks (Uplink Ports) for Packaged CCE are required to be 10G, with each Fabric Interconnect cross-connected to two common-L2 data center switches. The uplinks can be in a single-link, Port-Channel (EtherChannel), vPC or VSS (MEC) uplink topology.

If any Port-Channel uplink are used, corresponding Port-Channel must be created in UCS Manager, where the ID of the Port-Channel matches that on the data center switch.

If Port-Channel uplinks to data center switches are used, the UCS B Series Fabric Interconnects support only Link Aggregation Control Protocol (LACP). Ensure that the data center switch and Port-Channels are configured for, and support, LACP. This requirement also applies to vPC and VSS Port-Channels.

## FC Mode

Both End Host and Switching modes are supported. End Host is the default for FC and FCoE NPIV with a supported FC Switch. Switching mode requires FC Zoning to be configured in the Fabric Interconnects. Refer to UCS Fabric Interconnect documentation for more information on these modes and use cases, and to specific SAN switch and SAN controllers vendor documentation as necessary. UCS Fabric Interconnect documentation is available at <https://www.cisco.com/c/en/us/products/servers-unified-computing/ucs-6200-series-fabric-interconnects/index.html>.

## FC Storage Port and FCoE Uplinks

Packaged CCE supports all FC and FCoE connected SAN topologies as supported by the UCS Fabric Interconnects, provided that all storage redundancy, latency, IO and bandwidth requirements are met.



**Note** If direct-attach SAN is used, qualified direct-attach FC and FCoE storage vendors are currently limited to EMC, Hitachi Data Systems, and NetApp. Please refer to the latest Cisco UCS hardware compatibility list for the most current qualified vendors and models, at [https://www.cisco.com/en/US/products/ps10477/prod\\_technical\\_reference\\_list.html](https://www.cisco.com/en/US/products/ps10477/prod_technical_reference_list.html).

### QoS System Class and QoS Policy

Unified CM and CCE applications set L3 QoS DSCP (AF/CS), which is not handled by the Fabric Interconnects; Fabric Interconnects are not L3 aware. Packaged CCE does not require specific QoS System Class or QoS Policy settings for VMware vSwitches.

## Cisco UCS B-Series Blade Requirements

Cisco UCS Manager uses Pools, Policies and Templates which are collected in a Service Profiles Template and applied to a blade as a Service Profile.

Packaged CCE does not have any specific requirements for the blade Service Profile or Service Profile Templates, other than the vNIC and vHBA requirements to conforming to network VLAN and FC/FCoE VSAN requirements (see [vNIC Requirements, on page 7](#) and [vHBA Requirements, on page 8](#)).

For consistent and verifiable configuration and conformance of server configurations, use vNIC, vHBA and Service Profile Templates.

For more detail on UCS blade configuration and service profiles and templates, refer to the appropriate Cisco UCS Manager documentation.

## vNIC Requirements

Packaged CCE requires that you configure a minimum of two vNIC Ethernet interfaces on the UCS B-series blade. You must assign each of these two interfaces to alternate Fabric Interconnects for redundancy.

Name	MAC Address	Desired Order	Actual Order	Fabric ID	Desired Placement
vNIC eth0	00:25:B5:00:10:DF	1	1	A	Any
vNIC eth1	00:25:B5:00:10:FF	2	2	B	Any

Do **not** enable Fabric Failover for any Packaged CCE host vNIC interfaces.

Name: eth0  
 Description:   
 Owner: Local  
 Fabric ID:  Fabric A  Fabric B  Enable Failover

The VMware VMKernel and Management interface is allowed to share the same vNICs with Packaged CCE.

This table is an example of collapsed vNIC interfaces for all VLANs:

vNIC	VLANS	Fabric	Notes
eth0	PCCE Visible (Active) PCCE Private (Standby) VMware Kernel & Management (Active) Default VLAN (Active) Other Management (Active)	A	Active and Standby are denoted to show the reference design for traffic flow through these vNICs as aligned to Fabric Interconnects as controlled in the VMware layer. See the UCS B Series Networking section for more details.
eth1	PCCE Visible (Standby) PCCE Private (Active) VMware Kernel & Management (Standby) Default VLAN (Standby) Other Management (Standby)	B	



**Note** Networks other than the Packaged CCE Visible and Private networks are not required to be set to Active/Standby, as shown in the table. They can be set to Active/Active (no override), or assigned as needed to distribute load evenly across the infrastructure.

## vHBA Requirements

You must configure a minimum of two vHBA FC interfaces on the UCS B-series blade. You must assign each of these two interfaces to alternate Fabric Interconnects for redundancy.

Name	WWPN	Desired Order	Actual Order	Fabric ID	Desired Placement
vHBA fc1	20:00:00:25:B5:00:10:DF	4	4	B	Any
vHBA fc0	20:00:00:25:B5:00:10:EF	3	3	A	Any

These FC vHBAs can be used for either FC or FCoE connected SAN. Use a different VSAN for each Fabric Interconnect (A/B) path to the SAN, but common VSAN is also supported.

Common (as depicted) or separate vHBA interfaces may be used for Packaged CCE datastores and ESXi Boot from SAN storage path.



## Packaged CCE UCS B-Series Fabric Interconnects Validation Tool

This tool performs checks on currently deployed UCS B-Series Fabric Interconnect clusters to determine compliance with Packaged CCE requirements. If Packaged CCE will be deployed on two separate UCS B Series Fabric Interconnect clusters, run the tool for each cluster.



**Note** To run this tool, the Java version applicable to the version of the tool you are using must be installed.

Java 7 (any update) or Java 8 (any update) must be installed.

In addition to running this tool, see *Virtualization for Cisco Packaged CCE* at [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/uc\\_system/virtualization/pcce\\_virt\\_index.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/virtualization/pcce_virt_index.html) and the *Solution Design Guide for Cisco Packaged Contact Center Enterprise* at <https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-technical-reference-list.html> to ensure full compliance.

To begin, [download](#) this file:

```
UCSValidatorTool-<version>.zip
```

Where <version> indicates the version of the tool you intend to install.

Once downloaded, follow these instructions to run the tool:

1. Unzip the UCSValidatorTool zip file to create a UCSValidatorTool directory.
2. Change to the UCSValidatorTool directory.
3. Run "java -jar UCSValidatorTool.jar".

The tool requests the following information:

- Company name (Required to generate the PDF filename using Company Name)
- IP Address of UCS Manager
- HTTPS (yes/no)
- Port (defaults to 80 for HTTP/443 for HTTPS)
- Username: Read-only credentials to UCS Manager
- Password

The following shows an example of the prompts.

```
Welcome to the Unified Computing System Verification Utility (version 11.6.1.0).
This tool will validate the UCS Fabric Interconnects for Packaged CCE requirements.
Enter company name: Cisco Systems Inc.
Enter UCS Manager cluster IP address: <ip-address-of-UCS-manager>
Use HTTPS? Yes/No: > (n[o]=80; y[es]=443)y
Port: [443]<port-number>
Enter UCS Manager access information with read privilege:
Username: <your-username>
Password: ****
Processing .....
```

After the validation process is complete, a summary of the pass/fail test results is displayed on the console, and output as both a log file (results/ucsValidation.log) and as a PDF file (Company-Name-date.pdf).

The following table provides a detailed explanation of each tool validation rule check run against the UCS B-Series Fabric Interconnects.

**Table 1: Requirement Validation Rules**

Category	Type	Requirements
Fabric Interconnect	Count	Two matching Fabric Interconnects (HA)
	Ethernet Mode	Mode must be End Host
	UCS Manager	Version 2.2(1) or later. A higher version than this may be required depending on the version of ESXi that you installed. Use the UCS Hardware and Software Compatibility tool to help you select the appropriate version. The tool can be found here: <a href="https://ucsheltool.cloudapps.cisco.com/public/">https://ucsheltool.cloudapps.cisco.com/public/</a>

Category	Type	Requirements
	Ethernet Uplinks	

Category	Type	Requirements
		<p>The Fabric Interconnect rule:</p> <p>Checks all Ethernet uplinks for one set that passes the following requirement validation rules.</p> <ul style="list-style-type: none"> <li>• Uplink Ethernet interface speed must be 10, 20, or 40 Gbps</li> <li>• For Uplink Eth Interfaces: <ul style="list-style-type: none"> <li>• Two or more (even, by two's) per Fabric Interconnect with common VLAN(s) (for grouping of ports across Fabric Interconnects - differentiate grouping if disjoint-L2)</li> <li>• Four or more (even, by four's) per Fabric Interconnect pair grouped by common VLAN(s)</li> </ul> </li> <li>• For Port Channels: <ul style="list-style-type: none"> <li>• One or more Port Channels per Fabric Interconnect</li> <li>• Two or more Port Channels (even by two's) per Fabric Interconnect pair matched by common VLAN(s) <ul style="list-style-type: none"> <li>• Two or more member Ethernet ports (even, by two's) per Port Channel</li> <li>• VLAN matched Port Channel pairs must have 4 or more (even, by four's) member Ethernet interfaces in total</li> </ul> </li> </ul> </li> </ul> <p>Caveats:</p> <ul style="list-style-type: none"> <li>• Even though Packaged CCE does not support splitting the Public and Private VLANs over disjoint-L2 uplinks, this tool examines each disjoint-L2 uplink set and provides pass/fail results. If any one set of uplinks is found to meet the requirements, the rule will pass even if others fail. In this case (as the tool is pre-deployment), if an uplink set that failed the rule is intended for Packaged CCE VLANs, it must be corrected to meet requirements for support.</li> <li>• The tool does not connect to or inspect the upstream data center switches to confirm the following requirements: <ul style="list-style-type: none"> <li>• Fabric Interconnect pair cross-connected to upstream data center switch pair</li> <li>• Data center switch pair Ethernet interface ports properly configured for standard, EtherChannel,</li> </ul> </li> </ul>

Category	Type	Requirements
		<p>vPC, or VSS uplink designs</p> <ul style="list-style-type: none"> <li>Data center switch pair Ethernet interface ports properly configured for Virtual Switch VLAN Tagging (802.1q)</li> </ul>
IO Model (Fabric Extender)	Count	<p>The IO Model (Fabric Extender) rule:</p> <ul style="list-style-type: none"> <li>Checks for two matching IO Modules on each blade chassis (minimum one required).</li> </ul> <p>Caveats:</p> <ul style="list-style-type: none"> <li>This rule does not validate whether or not the two IO Modules are correctly connected to different Fabrics Interconnects (one to A and the other to B). However, the tool and output PDF does include the connection information for each IO Module (as shown in the following example).</li> </ul> <pre> Rule: IO Module count and models should match design. Result: Pass Details: --- Supported Chassis Configuration --- Chassis 1 PID N20-C6508 Serial FOX1721GCRG IO Module 1 PID UCS-IOM-2208XP Fabric ID A IO Module 2 PID UCS-IOM-2208XP Fabric ID B                     </pre> <ul style="list-style-type: none"> <li>This rule does not validate that each IO Module has a minimum of two ports connected to its paired Fabric Interconnect as required.</li> </ul>

Category	Type	Requirements
SAN Hardware and Transport	Type and Data Rate	<p>The SAN Hardware and Transport rule:</p> <p>Checks all FC uplink types for one set of FC uplinks that pass the following requirement validation rules.</p> <ul style="list-style-type: none"> <li>• FC port speed must be 2, 4, or 8 Gbps</li> <li>• FCoE port speed must be 10, 20, or 40 Gbps</li> <li>• For FC ports: <ul style="list-style-type: none"> <li>• One or more per Fabric Interconnect</li> </ul> </li> <li>• For FCoE ports: <ul style="list-style-type: none"> <li>• Two or more (even, by two's) per Fabric Interconnect</li> </ul> </li> <li>• Number of FC and/or FCoE port channels must match on Fabric Interconnect pair (must be symmetrical) <ul style="list-style-type: none"> <li>• Two or more FC member ports per Fabric Interconnect</li> <li>• Two or more FCoE member ports (even, by two's) per Fabric Interconnect</li> </ul> </li> </ul> <p>Caveats:</p> <ul style="list-style-type: none"> <li>• This rule does not match FC or FCoE port counts between Fabric Interconnects (though this may be required for a given SAN design).</li> <li>• It does not validate any specific Cisco UCS and SAN switch and SAN controller supported designs.</li> <li>• It does not inspect FC or FCoE VSAN memberships for uplink grouping.</li> <li>• It does not inspect the FC Mode to validate uplinks for internal versus external NPV/NPIV designs.</li> </ul>

The following table provides a detailed explanation of the UCS B-Series requirements not validated by this tool.

Table 2: Requirements Not Validated by the Tool

Category	Requirement
UCS Blade Server	<p>UCS blade specification must match one of the following:</p> <ul style="list-style-type: none"> <li>• B200 M3 TRC#1: <a href="https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/collaboration-virtualization-hardware.html">https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/collaboration-virtualization-hardware.html</a></li> <li>• B200 M4 TRC#1: <a href="https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/collaboration-virtualization-hardware.html">https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/collaboration-virtualization-hardware.html</a></li> </ul> <p>Note: B200 M4 TRC#1 is supported for Release 11.0(1) and later only.</p> <p>Storage and Ethernet interface requirements:</p> <ul style="list-style-type: none"> <li>• Two vHBAs, alternately pinned to Fabric A and B</li> <li>• Two vNICs, alternately pinned to Fabric A and B</li> <li>• No Fabric Failover enabled on vNICs</li> </ul>
UCS SAN HCL	<p>The following SAN components (as applicable) must be on the UCS HCL for the version of UCS Manager firmware used:</p> <ul style="list-style-type: none"> <li>• FC SAN switch</li> <li>• SAN controller</li> </ul>
SAN LUN	<p>SAN LUNs must:</p> <ul style="list-style-type: none"> <li>• Meet the IOPS requirements</li> <li>• Meet the storage latency requirement</li> </ul>
VMware vSphere ESXi	<p>The tool does not connect to or check any vSphere ESXi specific requirements.</p>

For more UCS HCL resources, see:

- <https://www.vmware.com/resources/compatibility/search.php>
- <https://www.cisco.com/c/en/us/support/servers-unified-computing/unified-computing-system/products-technical-reference-list.html>

## NTP and Time Synchronization

Packaged CCE requires that all parts of the solution have the same time. While time drift occurs naturally, it is critical to configure NTP to keep solution components synchronized.

To prevent time drifts on Live Data reports, the NTP settings on the Rogger VMs, the PG VMs, the AW VMs, and on the Cisco Unified Intelligence Center Publisher and Subscriber VMs must be synchronized.

For Cisco UCS B-series servers, you also must set the time zone and NTP Time Server using the UCS Manager. See [Set Time Zone and NTP Time Server for Cisco UCS B-Series Servers](#), on page 17 for more information.

**Important**

Microsoft periodically releases cumulative time zone updates. These updates include worldwide changes to time zone names, bias (the amount of time in minutes that a time zone is offset from Coordinated Universal Time (UTC)), and observance of daylight saving time. These patches update the information in the Windows registry. When these updates are available, apply them to all virtual machines in the deployment that are running a Microsoft Windows operating system.

**Windows Active Directory Domain**

The Windows Active Directory Primary Domain Controller (PDC) emulator master for the forest in which the Packaged CCE domain resides (whether same, parent, or peer) must be properly configured to use an external time source. This external time source should be a trusted and reliable NTP provider, and if already configured for the customer's forest, must be used (and useable) as same source for all other applications as detailed in this section for the Packaged CCE solution.

See the following references for properly configuring Windows Active Directory Domain for NTP external time source:

- [How to configure an authoritative time server in Windows Server.](#)



**Note** Do not use the "Fix it for me" function in this article.

- AD DS: [The PDC emulator master in this forest should be configured to correctly synchronize time from a valid time source.](#)

Microsoft Windows Server Domains do not automatically recover or fail over the authoritative internal time source for the domain when the PDC emulator master server is lost, due to hardware failure or otherwise. This article, [Time Service Configuration on the DC with PDC Emulator FSMO Role](#), helps describe how you must additionally configure the new target server to be the authoritative internal time source for the domain. It also covers manual intervention to recover and seize or reassign the PDC Flexible Single-Master Operations (FSMO) role to another domain controller.

**Windows Components in the Domain**

Windows hosts in the domain are automatically configured to synch their time with a PDC emulator, whether by the PDC emulator master with authoritative internal time source or chained from same in the domain forest hierarchy.

**Windows Components Not in the Domain**

Use the following steps to set NTP time source for a Windows Server that is not joined to a domain:

1. Log in as a user with administrative privileges.
2. In the Command Prompt window, type the following line and press ENTER: `w32tm /config /manualpeerlist:PEERS /syncfromflags:MANUAL`



**Note** Replace peers with a comma-separated list of NTP servers.



3. Restart the w32time service: `net stop w32time && net start w32time.`
4. Synch w32time service with peers: `w32tm /resync.`
5. Use the following Service Control command to ensure proper start of the w32time service on any reboot of the server: `sc triggerinfo w32time start/networkon stop/networkoff.`

### Cisco Integrated Service Routers

Cisco IOS Voice Gateways must be configured to use the same NTP source for the solution in order to provide accurate time for logging and debugging. See [Basic System Management Configuration Guide, Cisco IOS Release 15M&T: Setting Time and Calendar Services](#).

### VOS Components

Components such as Unified Intelligence Center, Finesse, Social Miner , and Unified Communications Manager must point to the same NTP servers as the domain authoritative internal time source.

### CLI commands for NTP Servers

While NTP servers are typically specified at install time, here a few commands you can use from the platform cli of the above listed components, to list, add and remove ntp servers. From the platform CLI:

- To list existing ntp servers: `utils ntp servers list`
- To add an additional ntp server: `utils ntp server add <host or ip address to add>`
- To delete an existing ntp server: `utils ntp server delete (row number of the item to delete).` Press **Enter**.

### ESXi Hosts

All Packaged CCE ESXi hosts (including those for optional components), must point to the same NTP server(s) used by the Windows domain PDC emulator master as the their external time source.

For details on configuring NTP on ESXi hosts, see the VMware documentation at <https://www.vmware.com/support/pubs/>.

## Set Time Zone and NTP Time Server for Cisco UCS B-Series Servers

Set the time zone and NTP Time server for UCS B-series server in the UCS Manager.

### Procedure

- 
- Step 1** From the **Admin** tab in UCS Manager, select **Stats Mangement > Time Zone Management**.
  - Step 2** Select the **Time Zone** from the down-down menu.
  - Step 3** Click **Add NTP Time Server**.
  - Step 4** Enter the IP address of the NTP Time Server, and click **OK**.
  - Step 5** Click **Save**.
-

# Global Catalog Requirements

Packaged CCE uses the Global Catalog for Active Directory Lookup. All domains in the AD Forest in which the Packaged CCE Hosts reside must publish the Global Catalog for that domain. This includes all domains with which your solution interacts, for example, Authentication, user lookup, and group lookup.

In a multi-domain forest, a Global Catalog is required at each AD site. Global Catalog is a central repository of domain information in an AD forest. A significant performance degradations and failure occur without local or Global Catalog. It is important for every AD query to search each domain in the forest. The multi-site deployments are required to query across WAN links.



---

**Note** This does not imply cross-forest operation. Cross-forest operation is not supported.

---