



# **Cisco UCS blade server and switch configuration**

## **FlexPod**

NetApp  
June 03, 2021

This PDF was generated from [https://docs.netapp.com/us-en/flexpod/healthcare/ehr-meditech-deploy\\_cisco\\_ucs\\_blade\\_server\\_and\\_switch\\_configuration.html](https://docs.netapp.com/us-en/flexpod/healthcare/ehr-meditech-deploy_cisco_ucs_blade_server_and_switch_configuration.html) on October 13, 2021. Always check docs.netapp.com for the latest.

# Table of Contents

- Cisco UCS blade server and switch configuration . . . . . 1
  - Cisco Nexus switch configuration . . . . . 1
  - Cisco MDS 9132T configuration . . . . . 2
  - Cisco UCS configuration guidance . . . . . 4

# Cisco UCS blade server and switch configuration

The FlexPod for MEDITECH software is designed with fault tolerance at every level. There is no single point of failure in the system. For optimal performance, Cisco recommends the use of hot spare blade servers.

This document provides high-level guidance on the basic configuration of a FlexPod environment for MEDITECH software. In this section, we present high-level steps with some examples to prepare the Cisco UCS compute platform element of the FlexPod configuration. A prerequisite for this guidance is that the FlexPod configuration is racked, powered, and cabled per the instructions in the [FlexPod Datacenter with Fibre Channel Storage using VMware vSphere 6.5 Update 1, NetApp AFF A-series and Cisco UCS Manager 3.2 CVD](#).

## Cisco Nexus switch configuration

A fault-tolerant pair of Cisco Nexus 9300 Series Ethernet switches is deployed for the solution. You should cable these switches as described in the [Cabling Diagram](#) section. The Cisco Nexus configuration helps ensure that Ethernet traffic flows are optimized for the MEDITECH application.

1. After you have completed the initial setup and licensing, run the following commands to set global configuration parameters on both switches:

```
spanning-tree port type network default
spanning-tree port type edge bpduguard default
spanning-tree port type edge bpdufilter default
port-channel load-balance src-dst l4port
ntp server <global-ntp-server-ip> use-vrf management
ntp master 3
ip route 0.0.0.0/0 <ib-mgmt-vlan-gateway>
copy run start
```

2. Create the VLANs for the solution on each switch using the global configuration mode:

```
vlan <ib-mgmt-vlan-id>
name IB-MGMT-VLAN
vlan <native-vlan-id>
name Native-VLAN
vlan <vmotion-vlan-id>
name vMotion-VLAN
vlan <vm-traffic-vlan-id>
name VM-Traffic-VLAN
vlan <infra-nfs-vlan-id>
name Infra-NFS-VLAN
exit
copy run start
```

3. Create the Network Time Protocol (NTP) distribution interface, port channels, port channel parameters, and

port descriptions for troubleshooting per [FlexPod Datacenter with Fibre Channel Storage using VMware vSphere 6.5 Update 1, NetApp AFF A-series and Cisco UCS Manager 3.2 CVD](#).

## Cisco MDS 9132T configuration

The Cisco MDS 9100 Series FC switches provide redundant 32Gb FC connectivity between the NetApp AFF A200 or AFF A300 controllers and the Cisco UCS compute fabric. You should connect the cables as described in the [Cabling Diagram](#) section.

1. From the consoles on each MDS switch, run the following commands to enable the required features for the solution:

```
configure terminal
feature npiv
feature fport-channel-trunk
```

2. Configure individual ports, port channels, and descriptions as per the FlexPod Cisco MDS switch configuration section in [FlexPod Datacenter with FC Cisco Validated Design](#).
3. To create the necessary virtual SANs (VSANs) for the solution, complete the following steps while in global configuration mode:
  - a. For the Fabric-A MDS switch, run the following commands:

```
vsan database
vsan <vsan-a-id>
vsan <vsan-a-id> name Fabric-A
exit
zone smart-zoning enable vsan <vsan-a-id>
vsan database
vsan <vsan-a-id> interface fc1/1
vsan <vsan-a-id> interface fc1/2
vsan <vsan-a-id> interface port-channel110
vsan <vsan-a-id> interface port-channel112
```

The port channel numbers in the last two lines of the command were created when the individual ports, port channels, and descriptions were provisioned by using the reference document.

- b. For the Fabric-B MDS switch, run the following commands:

```

vsan database
vsan <vsan-b-id>
vsan <vsan-b-id> name Fabric-B
exit
zone smart-zoning enable vsan <vsan-b-id>
vsan database
vsan <vsan-b-id> interface fc1/1
vsan <vsan-b-id> interface fc1/2
vsan <vsan-b-id> interface port-channel111
vsan <vsan-b-id> interface port-channel113

```

The port channel numbers in the last two lines of the command were created when the individual ports, port channels, and descriptions were provisioned by using the reference document.

4. For each FC switch, create device alias names that make the identification of each device intuitive for ongoing operations by using the details in the reference document.
5. Finally, create the FC zones by using the device alias names that were created in step 4 for each MDS switch as follows:
  - a. For the Fabric-A MDS switch, run the following commands:

```

configure terminal
zone name VM-Host-Infra-01-A vsan <vsan-a-id>
member device-alias VM-Host-Infra-01-A init
member device-alias Infra-SVM-fcp_lif01a target
member device-alias Infra-SVM-fcp_lif02a target
exit
zone name VM-Host-Infra-02-A vsan <vsan-a-id>
member device-alias VM-Host-Infra-02-A init
member device-alias Infra-SVM-fcp_lif01a target
member device-alias Infra-SVM-fcp_lif02a target
exit
zoneset name Fabric-A vsan <vsan-a-id>
member VM-Host-Infra-01-A
member VM-Host-Infra-02-A
exit
zoneset activate name Fabric-A vsan <vsan-a-id>
exit
show zoneset active vsan <vsan-a-id>

```

- b. For the Fabric-B MDS switch, run the following commands:

```
configure terminal
zone name VM-Host-Infra-01-B vsan <vsan-b-id>
member device-alias VM-Host-Infra-01-B init
member device-alias Infra-SVM-fcp_lif01b target
member device-alias Infra-SVM-fcp_lif02b target
exit
zone name VM-Host-Infra-02-B vsan <vsan-b-id>
member device-alias VM-Host-Infra-02-B init
member device-alias Infra-SVM-fcp_lif01b target
member device-alias Infra-SVM-fcp_lif02b target
exit
zoneset name Fabric-B vsan <vsan-b-id>
member VM-Host-Infra-01-B
member VM-Host-Infra-02-B
exit
zoneset activate name Fabric-B vsan <vsan-b-id>
exit
show zoneset active vsan <vsan-b-id>
```

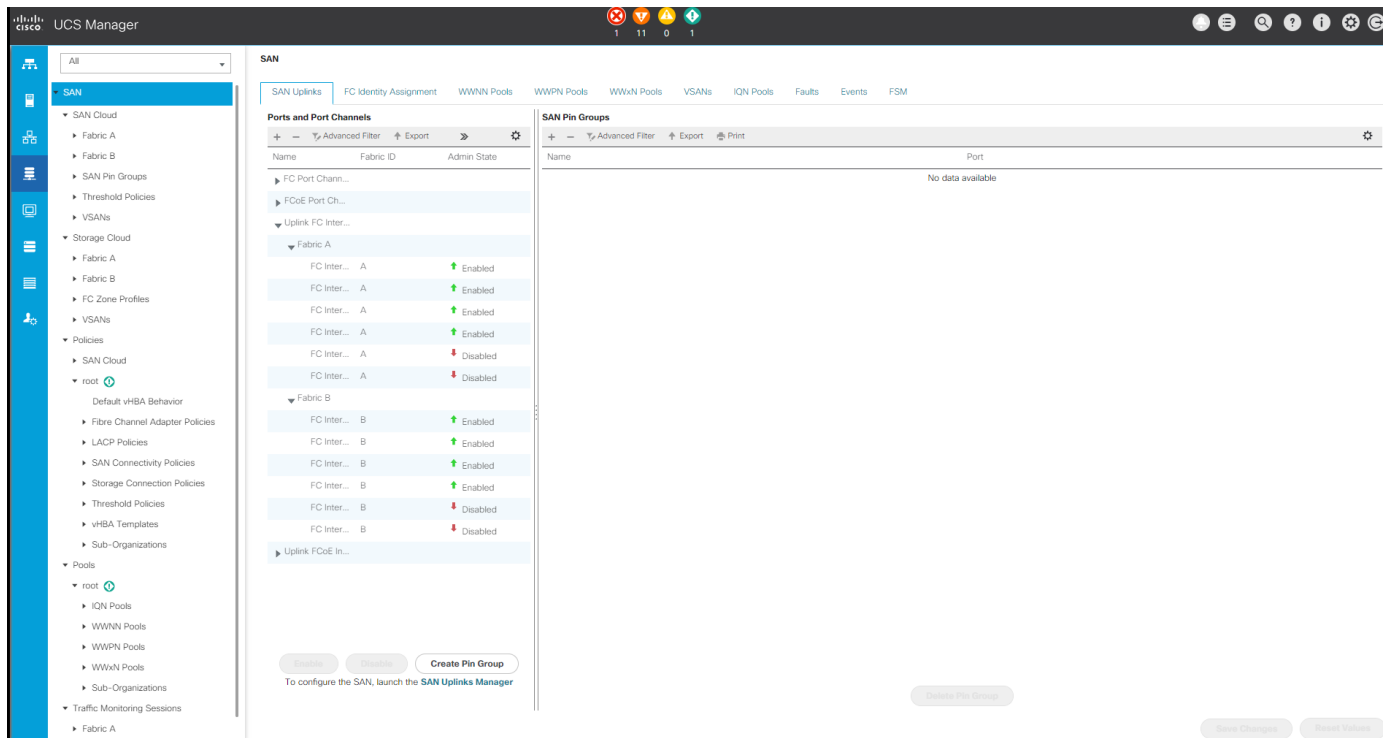
## Cisco UCS configuration guidance

Cisco UCS enables you as a MEDITECH customer to leverage your subject-matter experts in network, storage, and compute to create policies and templates that tailor the environment to your specific needs. After they are created, these policies and templates can be combined into service profiles that deliver consistent, repeatable, reliable, and fast deployments of Cisco blade and rack servers.

Cisco UCS provides three methods for managing a Cisco UCS system, called a domain:

- Cisco UCS Manager HTML5 GUI
- Cisco UCS CLI
- Cisco UCS Central for multidomain environments

The following figure shows a sample screenshot of the SAN node in Cisco UCS Manager.



In larger deployments, independent Cisco UCS domains can be built for more fault tolerance at the major MEDITECH functional component level.

In highly fault- tolerant designs with two or more data centers, Cisco UCS Central plays a key role in setting global policy and global service profiles for consistency between hosts throughout the enterprise.

To set up the Cisco UCS compute platform, complete the following procedures. Perform these procedures after the Cisco UCS B200 M5 Blade Servers are installed in the Cisco UCS 5108 AC blade chassis. Also, you must complete the cabling requirements as described in the [Cabling Diagram](#) section.

1. Upgrade the Cisco UCS Manager firmware to version 3.2(2f) or later.
2. Configure the reporting, Cisco call home features, and NTP settings for the domain.
3. Configure the server and uplink ports on each Fabric Interconnect.
4. Edit the chassis discovery policy.
5. Create the address pools for out- of- band management, universal unique identifiers (UUIDs), MAC address, servers, worldwide node name (WWNN), and worldwide port name (WWPN).
6. Create the Ethernet and FC uplink port channels and VSANs.
7. Create policies for SAN connectivity, network control, server pool qualification, power control, server BIOS, and default maintenance.
8. Create vNIC and vHBA templates.
9. Create vMedia and FC boot policies.
10. Create service profile templates and service profiles for each MEDITECH platform element.
11. Associate the service profiles with the appropriate blade servers.

For the detailed steps to configure each key element of the Cisco UCS service profiles for FlexPod, see the [FlexPod Datacenter with Fibre Channel Storage using VMware vSphere 6.5 Update 1, NetApp AFF A-series and Cisco UCS Manager 3.2 CVD](#) document.

Next: ESXi Configuration Best Practices.



## Copyright Information

Copyright © 2021 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

## Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.