Getting Started with Implementing Cisco Unified Computing System (UCS) Training

Getting Started Implementing Cisco Unified Computing System (UCS) Training

In This Lesson:

- About your instructor
- Who should watch this course?
- What is Cisco UCS?
- What we will cover in the course

About Your Instructor – Jason Nash

- 18+ years of IT experience
- Implemented a number of Cisco UCS systems in production
- What I do
  - Data Center Solutions Principal for Varrow
  - Implemented a number of Cisco UCS systems in production
- Publications
  - Several technical study guides
- Speaking
  - VMworld several times
  - Many, many user groups and other events

Blog: http://www.jasonnash.com
Twitter: @TheJasonNash
LinkedIn: linkedin.com/in/jasonnash
Email: jason.nash@gmail.com
Getting Started Implementing Cisco Unified Computing System (UCS) Training

About Your Instructor – Jason Nash

- Education
  - BS in Internetworking Technology with a Minor in Security Administration
  - MS in Technology Systems with a concentration on Information Security
- Certifications
  - VCDX #49, CISSP, Cisco CCNP
  - Cisco Unified Computing Technology Support Specialist
  - Cisco Unified Computing Technology Design Specialist
- Other TrainSignal Training
  - VMware vSphere Security Design Training

Who Should Watch This Course?

- Anyone who wants to learn about Cisco UCS
  - Implementation
  - Architecture
- Anyone looking to implement, support, or manage Cisco UCS infrastructure for themselves or their clients
- Recommended experience
  - General server administration
  - General network administration
  - Storage administration is helpful, but not required
  - Exposure to VMware is beneficial

What is Cisco UCS?

- A true next-generation server platform
- The first disruptive server technology or product that I’ve seen in a long time
- A really great complementary hardware platform for virtualization
- The compute part of Cisco’s new virtualized data center strategy
- Foundation for your private cloud strategy
Getting Started Implementing Cisco Unified Computing System (UCS) Training

What We Will Cover in the Course

- How to setup the UCS Platform Emulator
- Review of Cisco’s data center strategy
- Components that make up Cisco UCS
- Physically installing and cabling the equipment
- Exploring the UCS Manager GUI and CLI
- How to configure LAN connectivity
- How to configure SAN connectivity
- Creating resource and identity pools

Getting Started Implementing Cisco Unified Computing System (UCS) Training

What We Will Cover in the Course

- All about Service Profiles that enable stateless computing
- Using Service Profile templates
- Regular management of UCS
- Permissions and user accounts within UCS Manager
- How to backup and restore the UCS configuration
- Configuring and managing high availability
- Cisco’s Nexus 1000v virtual switch
- VMware integration with UCS
- Tips for troubleshooting the UCS environment
- Preparing for the DCUCI exam
In This Lesson:

- An Overview of My Lab
- The Charlotte Lab
- The Greensboro Lab
- Cisco UCS Platform Emulator
- Using the UCS Platform Emulator

An Overview of My Lab

- Understandably, not everyone will have a hardware lab
- Will be using three different lab environments
  - Lab in Charlotte
  - Lab in Greensboro
  - Cisco's Platform Emulator
- Each one offers some different options and configurations
  - Lesson may require specific hardware
  - One lab may be in use by others
Implementing Cisco Unified Computing System (UCS) Training

Lab Setup and Platform Emulator Configuration

The Charlotte Lab
- Lab consists of
  - 6120 Fabric Interconnects
  - Two Chassis
  - Three Blades
  - Dual-socket
  - 24GB of RAM
  - Nexus 5010 Switches
  - MDS 9124
  - EMC CX3 SAN
- Most lesson labs on this gear

The Greensboro Lab
- Lab consists of
  - 6248 Fabric Interconnects
  - One Chassis
  - Two Blades
  - Dual-socket
  - 24GB of RAM
  - Catalyst 3750 Switches
  - MDS 9124
  - EMC NS-120 SAN
- Useful for showing new 6248UP interconnects

Cisco UCS Platform Emulator
- Cisco provides an EXCELLENT emulator for the UCS environment
  - UCSPE (UCS Platform Emulator)
- Runs the same UCS Manager code as the real gear
- Primary focus is for developers to test plugins and other add-ons
  - But makes for a great lab/test admin environment
  - Can even import a physical install's configuration
- Of course, there is no physical hardware
  - Gives you the management environment
  - Can't boot servers
- Current versions have a GUI for hardware configuration
Deploying the UCS Platform Emulator

- For this course I am using the 1.4 version of UCSPE
  - Cisco recently released the 2.0 version
- UCSPE is available from Cisco’s Developer site
- Can be run using
  - VMware Player
  - VMware Workstation
  - VMware Fusion
  - vSphere Server

Deploying the UCS Platform Emulator

- Once downloaded just unzip the archive
- Starting the emulator depends on what VMware hypervisor is used
- For VMware Player/Fusion/Workstation just use File – Open
  - Point to .VMX file
- vSphere environments require a few steps
  - Copy VM files to an accessible datastore
  - Import the VM using the VI Client
  - Confirm network settings
- Boot the VM and you will see Linux start
  - By default it will use DHCP to get an IP address
  - Once complete you can login to change network settings
  - Can also restart the emulator from text console

Using the Platform Emulator

- Just like a real UCS environment uses a Java client
  - Requires Java 1.6 JRE
  - Runs on most browsers
- Point your browser to the IP given in the text console
- May need to accept a SSL cert warning
- Default login is admin/admin
- Configuration options in the left frame
Lab – Using the Cisco UCS Platform Emulator

• In this lab we will
  – Deploy the UCSPE VM
  – Boot the VM and configure network settings
  – Show how to do virtual hardware configuration
  – Log in to UCS Manager

Lab Setup and Platform Emulator Configuration
Implementing Cisco Unified Computing System (UCS) Training

What We Covered

 An Overview of My Lab
 The Charlotte Lab
 The Greensboro Lab
 Cisco UCS Platform Emulator
 Using the UCS Platform Emulator
An Introduction to Cisco’s Unified Data Center

In This Lesson:

- Cisco’s Virtualized Data Center
- Understanding the Components
- Infrastructure Components – Nexus Switches
- A Quick Overview of FEX
- Virtual Infrastructure – Nexus 1000v
- Infrastructure Components – MDS Switches
- Cloud Provisioning and Automation

Cisco’s Virtualized Data Center

- Cisco has developed a line of products and technologies that extend virtualization throughout the data center
  - Not all virtualization is server consolidation!
- Cisco UCS is one component of that overall strategy
  - It’s the compute block
- It’s a good idea to understand how the pieces fit together
  - Also very important if you plan to sit the DCUCI exam
- The current approach is known as Data Center 3.0
  - Made up of layers and processes, not just products
An Introduction to Cisco’s Unified Data Center
Implementing Cisco Unified Computing System (UCS) Training

Understanding the Components

- It’s a good idea to understand the components of a modern data center
  - Currently undergoing a bit of a revolution
- 10Gb Ethernet has gone mainstream
  - Being driven by many new application requirements
- Virtualization is a catalyst for a lot of change
  - Consolidation
  - Automation
  - Cloud
- Need to understand the landscape if you plan to take the DCUCI exam

Infrastructure Components – Nexus Switches

- Many people are moving to 10Gb Ethernet for the data center
  - Some preparing for 40Gb and 100Gb!
- Cisco has several 10Gb switches
  - Nexus 5000 – First generation top-of-rack 10Gb
  - 5010 – 1U - 10 10Gb ports plus module
  - 5020 – 2U - 20 10Gb ports plus module
  - Module adds more 10Gb Ethernet or Fibre Channel
  - Support Fibre Channel over Ethernet (FCoE)
  - Layer 2 only
Infrastructure Components – Nexus Switches

- Nexus 5500 – Second generation top-of-rack 10Gb
  - 5548UP – 1U – 32 10Gb unified/universal ports plus module slot to add 16 more ports
  - 5596UP – 2U – 48 10Gb unified/universal ports plus 3 module slots to add up to 48 more ports
  - Optional Layer 3 capability
- Nexus 5500 switches are becoming popular for small core deployments
- Also used to add 10Gb to existing environments where larger switches are not needed

Infrastructure Components – Nexus Switches

- The large dense 10Gb core switches reside in the Nexus 7000 line
  - Nexus 7004 – Small 4-slot option
  - Nexus 7009 – A 9-slot switch that resembles the Catalyst 6500 in looks and size
  - Nexus 7010 – The original Nexus 7000 10-slot chassis
  - Nexus 7018 – The large 18-slot chassis
- Very fast, few expandable line
- In place upgrades to backplane switching speeds using fabric modules

Nexus 7000 Family

<table>
<thead>
<tr>
<th>Nexus 7000 and NX-OS</th>
<th>Nexus 7009</th>
<th>Nexus 7010</th>
<th>Nexus 7018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slots</td>
<td>7 I/O + 2 sup</td>
<td>8 I/O + 2 sup</td>
<td>16 I/O + 2 sup</td>
</tr>
<tr>
<td>Height</td>
<td>14 RU</td>
<td>21 RU</td>
<td>25 RU</td>
</tr>
<tr>
<td>BW / Slot Fab 1</td>
<td>N/A</td>
<td>230 Gig / slot</td>
<td>230 Gig / slot</td>
</tr>
<tr>
<td>BW / Slot Fab 2</td>
<td>550 Gig / Slot</td>
<td>550 Gig / slot</td>
<td>550 Gig / slot</td>
</tr>
</tbody>
</table>
Infrastructure Components – Nexus Switches

- For top-of-rack (ToR) connectivity there is the Nexus 2000 series
- These are Fabric Extenders (FEX), not true switches
  - Must be connected to a 5K or 7K
  - No local switching
- Range of models
  - 2148T – 48 1000Base-T and 4 10Gb interfaces
  - 2248TP – 24 1000Base-T and 2 10Gb interfaces
  - 2248TP – 48 1000Base-T and 4 10Gb interfaces
  - 2248TP – Same as 2248TP, but enhanced for higher workloads (larger buffers)
  - 2232PP – 32 1/10Gb and FCoE and 8 10Gb and FCoE
  - 2232TM 32 1/10GBase-T and optional module

A Quick Overview of FEX

- FEX, Fabric Extender, is a technology where a switching fabric is "extended" by using other devices, adapters, or software
  - The extended device is not a separate functional item
  - Requires connectivity back to a smart device
- There are several types of FEX
  - Switch FEX – An example is a Nexus 2K off of a 5548UP
  - Adapter FEX – Split a physical adapter in to multiple logical adapters
  - VM FEX – Extends adapter FEX in to a virtual machine
- Can be confusing and the terminology has evolved

Features:
- Adapter FEX split a physical NIC into multiple logical NICs
- VM-FEX extends Adapter FEX technology to virtual machine

Benefits:
- Single point of management
- Increased IO bandwidth utilization – less port-to-port cabling selections with adapter FEX
- Dynamic network & security policy mobility during VM migration with VM-FEX

Diagram thanks to Cisco
Virtual Infrastructure – Nexus 1000v

- Cisco has a Nexus switch that is virtual
  - Runs as part of the VMware environment
  - Announced support for Hyper-V
- Gives you Cisco/Nexus power and capability within the virtual environment
  - Network admins get visibility and control back
- Made up of two components:
  - VSM – Virtual Supervisor Module – Management/Control plane
  - VEM – Virtual Ethernet Module – Data plane

Virtualization Awareness at Scale

Diagram thanks to Cisco

Infrastructure Components – MDS Switches

- The MDS line is Cisco's Fibre Channel switches
  - Been around a long, long time
  - Reliable, standard
- Two major lines:
  - 9500 Series – Director class chassis switches
    - Examples: 9506, 9509
  - 9100 Series – Departmental switches, fixed configuration
    - Examples: 9124, 9134, 9148
- There is a 9222i switch that is often used for services
  - Fibre Channel replication
  - Encryption
  - Not normally seen as a standalone switch
Cloud Provisioning and Automation

- Over the last couple of years Cisco has made several key acquisitions in the cloud provisioning and automation space
  - Tidal Software
  - newScale
- newScale is now known as Cisco Cloud Portal
  - Services menu
  - Self-provisioning for private cloud
  - Manage lifecycle of services as well as chargeback
- Tidal is several products
  - Primarily used for automation and orchestration
  - Very cool and very powerful drag-and-drop interface
  - Great integration in to UCS

What We Covered

- Cisco’s Virtualized Data Center
- Understanding the Components
- Infrastructure Components – Nexus Switches
- A Quick Overview of FEX
- Virtual Infrastructure – Nexus 1000v
- Infrastructure Components – MDS Switches
- Cloud Provisioning and Automation
The Components of Cisco UCS B-Series

Implementing Cisco Unified Computing System (UCS) Training
Instructor: Jason Nash

In This Lesson:
- How is Cisco UCS different?
- Comparison of traditional blade enclosures to UCS
- Overview of the components that make up the UCS architecture
- Describe the Fabric Interconnects and their options
- Describe the Fabric Extenders
- Describe the UCS chassis
- Introduce each of the different blade models
- Compare the different mezzanine adapter options

How is Cisco UCS Different?
- UCS architecture is very different from other "legacy" blade systems
- Developed by itself as part of "Project California"
- Cisco modeled this after their long-life switch products, such as Catalyst 6500
Traditional Blade Enclosures

- Traditional blade enclosures are very complex...and expensive
- Usually see redundant switches in each chassis
- Along with redundant management modules
- Unified management requires an external management entity
- Think about uplinking all those switches for each new chassis install
  - Usually takes days or longer

That's a Lot of Infrastructure

- This is a logical diagram of a normal rack with traditional blade enclosures
- Each enclosure has 5 or 6 management points: plus the top-of-rack switches
- Lots of cabling
- Many IP addresses to manage

Blades....But Simpler.

- Cisco removed almost all infrastructure from the chassis
- No switches, no IP addresses
- Everything handled by two top-of-rack management nodes (interconnects)
- No uplinking required when a new chassis is deployed
- Fewer parts means lower power consumption and far less management
An Overview of the UCS Components

- UCS Manager
  - Embedded - manages entire system
- UCS Fabric Interconnect
  - 20 Port, 40 Port, 48 Unified Port
- UCS Fabric Extender
  - Remote line card (40 Gbps or 80 Gbps)
- UCS Blade Server Chassis
  - Flexible bay configurations
- UCS Compute Options
  - Industry-standard architecture
- UCS Virtual Adapters
  - Choice of multiple adapters

The Components of Cisco UCS B-Series
Implementing Cisco Unified Computing System (UCS) Training

Fabric Interconnects – The 6100 Series

- Original fabric interconnects
  - Still offered, not obsoleted
- Two models available
  - 6120 – 20-port 1U – (8) 10Gb Licenses - One Module
    - 6140 – 40-port 2U – (16) 10Gb Licenses - Two Modules
- These handle all management
- Provide uplink connectivity to existing LAN and SAN environments
- Connect down to the chassis

6100 Interconnect Modules

- The 6100 interconnect takes one (6120) or two (6140) expansion module
- They are (from left to right)
  - 8-port 1/2/4-Gb Fibre Channel Module
  - 4-port Fibre Channel plus 4-port 10Gb Ethernet Module (Includes 10Gb port licenses)
  - 6-port 10Gb Ethernet Module
  - 6-port 1/2/4/8-Gb Fibre Channel Module
Implementing Cisco Unified Computing System (UCS) Training

The Components of Cisco UCS B-Series

Fabric Interconnects – The 6200 Series

- Second generation interconnect
  - Not replacing the 6100 series
- Currently only the 6248UP (Universal Port) is available
- Double the density of a 6120 in 1U
- Universal Port option allows any port to be used for network or storage
  - No specific Fibre Channel ports
- By default has 32 ports and goes up to 48 with an additional module

Fabric Extenders – 2100 Series

- Fabric Extenders (or FEX) get installed in the back of the chassis
- Two FEX in the chassis
- They uplink the chassis to the interconnect
  - Each FEX goes to a different interconnect
- Original model is the 2104XP
  - 4 ports of 10Gb Ethernet/FCoE (Fibre Channel over Ethernet)
  - Can wire 1, 2, or 4 ports on each FEX

Comparison of Interconnect Models

<table>
<thead>
<tr>
<th>Product Features</th>
<th>UCS 6140XP</th>
<th>UCS 6120XP</th>
<th>UCS 6248UP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rack Unit Weight</td>
<td>30 lbs</td>
<td>16.4 lbs</td>
<td>31 lbs</td>
</tr>
<tr>
<td>Rack Unit Depth</td>
<td>18U</td>
<td>14U</td>
<td>18U</td>
</tr>
<tr>
<td>10 Gigabit Ethernet Port Density</td>
<td>8</td>
<td>16</td>
<td>16</td>
</tr>
<tr>
<td>10 Gigabit Ethernet Port Density</td>
<td>32</td>
<td>64</td>
<td>48</td>
</tr>
<tr>
<td>Ports/Portability</td>
<td>2.2m</td>
<td>3.3m</td>
<td>3.3m</td>
</tr>
<tr>
<td>SF (UPLink)</td>
<td>10/100</td>
<td>10/100</td>
<td>10/100</td>
</tr>
<tr>
<td>SF (UPLink)</td>
<td>10/100</td>
<td>10/100</td>
<td>10/100</td>
</tr>
<tr>
<td>SF (UPLink)</td>
<td>10/100</td>
<td>10/100</td>
<td>10/100</td>
</tr>
<tr>
<td>SF (UPLink)</td>
<td>10/100</td>
<td>10/100</td>
<td>10/100</td>
</tr>
<tr>
<td>SF (UPLink)</td>
<td>10/100</td>
<td>10/100</td>
<td>10/100</td>
</tr>
</tbody>
</table>
Fabric Extenders – 2200 Series

- Second generation FEX
  - 2208XP – 8-ports of 10Gb
- Will work with 6100 or 6200 interconnects (but be aware of port usage on 6100s)
- Connect 1, 2, 4, or 8 cables from the FEX to the interconnect
- Can also port-channel multiple connections

The Chassis

- Simple chassis, no internal switches
- Holds up to 8 half-width blades or 4 full-width blades
  - Can mix and match
- Supports up to 4 power supplies for N+1 and Grid redundancy
- Total of 8 fan modules
- Two bays for 2100 or 2200 FEX in rear of chassis
Rear View of the UCS Infrastructure

20/40/48 x fabric/border ports
2 x cluster ports
1 x management port
2 x fabric extenders
4 or 8x 10GE SFP+ fabric ports

expansion module bay
(1 or 2)
2 x power entry
console port
8 x fan modules
dual redundant

2 x power entry

Graphic: Thanks to Cisco.com

The Components of Cisco UCS B-Series
Implementing Cisco Unified Computing System (UCS) Training

Compute Blades – B200M2
• Considered the "workhorse" blade
  • Very popular
  • Half-width form factor
• Has the following specs:
  • Dual-socket Intel 5600 CPUs
  • 12 DIMM slots for 192GB w/ 16GB DIMMs
  • Two SFF Hard Disks
  • Single Mezzanine Adapter

View of a Half-width Blade

Graphic: Thanks to Cisco.com
The Components of Cisco UCS B-Series
Implementing Cisco Unified Computing System (UCS) Training

**Compute Blades — B250M2**

- Considered the "VDI" blade
  - Extended memory support
  - Full-width form factor
- Has the following specs:
  - Dual-socket Intel 5600 CPUs
  - 48 DIMM slots for 384GB w/ 8GB DIMMs
  - Two SFF Hard Disks
  - Two Mezzanine Adapters

**View of a Full-width Blade**

- **Memory Slots**
- **Mezzanine Cards**
- **Drive Bays**
- **CPU Sockets**

Graphic: Thanks to Cisco.com

**Compute Blades — B230M2**

- Called the "Goldilocks" blade
  - Very powerful
  - Half-width form factor
- Has the following specs:
  - Dual-socket Intel E7-2800 CPUs
  - Up to 10 cores each so up to 20 cores!
  - 32 DIMM slots for 512GB w/ 16GB DIMMs
  - Two solid state drives
  - Single Mezzanine Adapter
The Components of Cisco UCS B-Series
Implementing Cisco Unified Computing System (UCS) Training

**Compute Blades – B440M2**
- Considered the “big” blade
  - Quad-socket
  - Full-width form factor
- Has the following specs:
  - Dual-socket Intel E7-4800 CPUs
  - 10 cores each so up to 40 cores!
  - 32 DIMM slots for 512GB w/ 16GB DIMMs
  - Four SFF Hard Disks
  - Two Mezzanine Adapters

**Compute Element Options**

<table>
<thead>
<tr>
<th>Blade</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>B200 M2</td>
<td>2 Socket Intel 5600, 2 SFF Disk, 12 DIMM</td>
</tr>
<tr>
<td>B250 M2</td>
<td>2 Socket Intel 5600, 2 SFF Disk, 48 DIMM</td>
</tr>
<tr>
<td>B320 M2</td>
<td>2 Socket Intel E7, 2 SSD Disk, 32 DIMM</td>
</tr>
<tr>
<td>B440 M2</td>
<td>4 Socket Intel E7, 4 SSD Disk, 32 DIMM</td>
</tr>
<tr>
<td>C200 M2</td>
<td>2 Socket Intel 5600, 4 Disks, 12 DIMM, 2 PCIe 1U</td>
</tr>
<tr>
<td>C210 M2</td>
<td>2 Socket Intel 5600, 16 Disks, 12 DIMM, 5 PCIe 2U</td>
</tr>
<tr>
<td>C240 M2</td>
<td>2 Socket Intel 5600, 8 Disks, 48 DIMM, 5 PCIe 2U</td>
</tr>
<tr>
<td>C260 M2</td>
<td>2 Socket Intel E7, 16 Disks, 32-64 DIMM, 7 PCIe 2U</td>
</tr>
<tr>
<td>C460 M2</td>
<td>4 Socket Intel E7, 12 Disks, 64 DIMM, 10 PCIe 4U</td>
</tr>
</tbody>
</table>

**Mezzanine Adapters – Input and Output!**
- Each blade can choose from a selection of mezzanine adapters for I/O
- Sometimes called I/O modules (terminology can get confusing)
- Full-width blades can have two mezzanine adapters
- Half-width blades can have one mezzanine adapter
- Not all adapters support Fibre Channel connectivity
- Need to also be aware of operating system support when selecting a mezzanine adapter
- Interoperability matrix for blades and adapters:
The Components of Cisco UCS B-Series
Implementing Cisco Unified Computing System (UCS) Training

- Offered in three variants
  - M72KR-E for Emulex chipset
  - M72KR-Q for QLogic chipset
  - M61KR-I for Intel chipset
- Comparable to a standard CNA (Converged Network Adapter) card
  - Supports 10Gb Ethernet and FCoE (Future for M61KR-I)
- No virtual interface configuration available (except SR-IOV)
- Pretty wide operating system support
- Previous generation called M71KR-E/Q
- Often used when the VIC (discussed in a minute) is not supported by an operating system

Mezzanine Adapters – M51KR-B
- Network adapter utilizing the Broadcom chipset
- Supports 10Gb Ethernet ONLY
  - No FCoE support in hardware
- No virtual interface configuration available
- Very wide operating system support
- Used when FCoE isn’t needed or for legacy operating system support is required

Mezzanine Adapters – M81KR (Palo)
- Called the VIC (Virtual Interface Card) or Palo (code name)
- Supports both 10Gb Ethernet and FCoE
- Physical ports can be divided into many virtual NICs (vNICs) or HBAs (vHBAs)
  - Up to a usable of about 56 each
- Limited operating system support (mostly modern/current operating systems)
- Very commonly used with VMware and current versions of Windows and Linux
Mezzanine Adapters – VIC1280
• Second generation VIC
• Has 8x10Gb port-channel to a single card
  – 80Gb per host!
• Supports both 10Gb Ethernet and FCoE
• Physical ports can be divided in to many virtual NICs (vNICs) or HBAs (vHBAs)
  – Up to a usable of about 116 VM interfaces with vSphere 5
• Limited operating system support (mostly modern/current operating systems)
• Very commonly used with VMware and current versions of Windows and Linux

An Overview of the UCS Architecture

Cisco UCS Logical View
Available Connectivity & Bandwidth Options

- 2x 1 Link
  - 20 Gbps per Chassis

- 2x 2 Link
  - 40 Gbps per Chassis

- 2x 4 Link
  - 80 Gbps per Chassis

- 2x 8 Links
  - 160 Gbps per Chassis

Common Questions About UCS

- Are the interconnects switches?
  - Yes and no. They do switch frames but in the default configuration they do not need to run spanning-tree.

- Are the interconnects connected?
  - Yes and no. They are connected for management clustering but do not actually pass data. If data needs to go from one fabric to the other, it must pass over the outside network.
Common Questions About UCS

- If the 2 fabric interconnects are a cluster is it an active/active or active/passive cluster?
  - Only the management plane acts as an active/passive cluster. LAN and SAN I/O are active on both fabric interconnects.

Common Questions About UCS

- If there are no switches in a chassis, does that impact performance?
  - No. The interconnects switch frames and do the intelligent processing. It’s not different than a blade in a traditional chassis sending frames to an internal switch. The few feet to the interconnect add no measurable latency.

What We Covered

- How is Cisco UCS different?
- Comparison of traditional blade enclosures to UCS
- Overview of the components that make up the UCS architecture
- Describe the Fabric Interconnects and their options
- Describe the Fabric Extenders
- Describe the UCS chassis
- Introduce each of the different blade models
- Compare the different mezzanine adapter options
Installing Cisco UCS Hardware

Implementing Cisco Unified Computing System (UCS) Training
Instructor: Jason Nash

In This Lesson:
- Starting the hardware installation
- Physical space in the rack
- Power capacity and plug types
- Power to the chassis
- Physically installing the equipment
- Cabling the interconnects, chassis, and infrastructure
- Necessary configuration information

• While several boxes full of UCS gear may look intimidating, it's not
  – Remember, UCS has far less infrastructure than others!
  – That's less to plug in
• The first concerns are physical implementation tasks
  – Confirm physical space in the rack
  – Make sure you have the right power cables (#1 implementation issue)
Implementing Cisco Unified Computing System (UCS) Training

Installing Cisco UCS Hardware

Physical Space in the Rack(s)

- Rack space requirements are as follows
  - 6120 Interconnect – 1U
  - 6140 Interconnect – 2U
  - 6248UP Interconnect – 1U
  - 5108 Chassis – 6U

- Remember that you will have two interconnects
- May be power limited on number of chassis before you run out of physical space
- May want to look at “deep” racks to give you more clearance
  - Some vendors have racks just for UCS that include all cabling and PDUs

Power Capacity and Plug Types

- Cisco has a power calculator for UCS
  - Have found it to be conservative (shows higher numbers)
- The number of power outlets can be a restriction
  - Interconnects require two each for redundancy (as shown below)
- Number of power cable types and options, please confirm that for your location and power type when ordering

Power to the Chassis

- Power to the chassis is often a concern as it requires a lot and you want to confirm the cable types, which can be similar and confusing
  - Confirm cable type when you order!
- Up to four power supplies can be installed
  - Each 2500W
- Two redundancy options
  - N+1 – Extra power supply to act as failover capacity should one fail
  - N+N (Grid) – Allows you to have one power feed go to one set of power supplies and a second feed go to the others so that an entire feed can fail
Installing Cisco UCS Hardware
Implementing Cisco Unified Computing System (UCS) Training

Now for the Heavy Lifting
• Once power capacity and capability are confirmed you are ready to rack all of the equipment
• Highly suggested to use a lift for the chassis as it can be VERY heavy
  – Remove fans and power supplies, if already installed
• Use included rack rail kits for installation
• Run power cables and plug in as needed
• Make sure power cables are actually redundant
  – Split across PDUs/feeds/UPS systems
• Install fans, power supplies, and FEX back in to the chassis once it is racked

Cabling - Interconnects
• Interconnects are the “hub” for cabling (excuse the networking pun)
• First step is to cable them for management clustering
• Make sure you connect as
  – L1 to L1
  – L2 to L2
• Do not cross the connections

Proper UCS Chassis Cabling
• There are a couple of rules when cabling a chassis to the interconnect
• For the 2104XP FEX you can cable 1, 2, or 4 cables to the interconnect (not 3)
• For the 2208XP FEX you can cable 1, 2, 4, or 8 cables to the interconnect
• Each FEX goes to its own interconnect
• DO NOT CROSS CONNECT!
• If you use the combo module in a 6100 interconnect do not plug a chassis in to those ports
Implementing Cisco Unified Computing System (UCS) Training

Installing Cisco UCS Hardware

Improper UCS Chassis Cabling

• Here is an example of improper configuration
• They have cross connected the FEX to the interconnects
• There are also 3 cables from one FEX to the interconnect
  – 1, 2, or 4 since this is a 2104XP FEX
• It’s easy to forget this since it’s common to cross connect network switches

Supported Cable Types

• Due to the reliance on 10Gb Ethernet there are some restrictions on the type of cables that can be used between the interconnects and the chassis (depends on FEX)
  • 2104XP FEX can use
    – SFP+ Copper (TwinAx) in 1M, 3M, and 5M lengths
    – SFP+ SR and MMF Fibre Cables
    – SFP+ LR and SMF Fibre Cables
  • 2208XP FEX can use
    – SFP+ Copper (TwinAx) in 1M, 3M, and 5M lengths
    – SFP+ Fabric Extender Transceiver (FET) Fibre (2208UP only)
    – SFP+ SR and MMF Fibre Cables
    – SFP+ LR and SMF Fibre Cables
• Try to use the Copper TwinAx if you can due to cost
  – <$200 for cable with transceivers
  – Fibre SR transceiver can be $700+ per end

Cabling to Existing Infrastructure

• Rest of cabling consists of connecting to existing infrastructure
• If you use Fibre Channel you will install the appropriate SFPs in the appropriate ports
  – For 6100 interconnects they go in the expansion module FC ports
  – For 6200 interconnects they can go in any port
• Connect to the existing network on any ports via supported cables and SFPs
  – Copper TwinAx
  – Fibre SFPs
Cabling Review
- The simple diagram below shows you a possible configuration
- Keep in mind that you can cable each chassis differently
  - High I/O chassis with a total of 8 connections
  - Low I/O chassis with a total of 2 or 4 connections
- Just make sure each FEX in a chassis is the same

Cabling Review

Site Planning
- Once the system is configured we can start basic configuration
- Before that, we need to gather some information including
  - System Name for the interconnects
    - Note that each interconnect will use the name plus append –A and –B to it to denote the different fabrics
  - Password for the admin account
  - Three static IP addresses
    - One for each interconnect
    - Third for the virtual IP used by the cluster
  - Subnet mask for the IPs
  - Default gateway
  - DNS server
  - Domain name for the system

Lab – A Tour of the UCS Equipment
- In this lab we will
  - Jump to one of my labs
  - Look at the actual equipment in the lab
  - Show you how to install all the sub-components
  - Show you how to connect all cabling
  - Provide examples of different cables and modules
  - Look at the components installed in a blade
What We Covered

- Starting the hardware installation
- Physical space in the rack
- Power capacity and plug types
- Power to the chassis
- Physically installing the equipment
- Cabling the interconnects, chassis, and infrastructure
- Necessary configuration information
In This Lesson:

- Introduction to UCS Manager
- Logging in to UCS Manager
- The main UCS Manager window
- Overview of the UCS Manager tabs
- UCS Manager Command-Line Interface

---

**Introduction to UCS Manager**

- Overall management point for a UCS environment is UCS Manager (UCSM)
- Web based system using Java
  - Requires Java 1.6 to be installed on the client
- No other fat client to install
- Simply point your browser to the cluster IP of the interconnects
- One very powerful characteristic of UCS is that it supports XML for configuration storage as well as provides a robust API
Exploring UCS Manager
Implementing Cisco Unified Computing System (UCS) Training

Logging in to UCS Manager

- When you login to UCSM a separate Java application will be launched
- Use your login credentials
  - By default you use the login of admin
- Problems here are usually related to Java version or installation

The Main UCS Manager Window

- The UCSM GUI is a tab-based interface
  - Tabs break out components/functions
- May look slightly different on different browsers and operating systems
- Left side is the main tree
- Right side shows context-based information

The UCSM Tabs - Equipment

- Equipment tab shows all physical components
  - Chassis
  - Interconnects
  - Fabric Extenders (for rack mount servers)
  - Rack mount servers
  - Sub-components of each
- Filter box lets you filter on certain components
- Easy way to see health of a component
  - Colored boxes denote problems or information
The UCSM Tabs - Servers

- Servers tab shows server related items
  - Service profiles
  - Service profile templates
  - All different policies
  - Server and UUID pools
  - Schedules
- Filter box lets you filter on certain components
- Easy way to see health of a component
  - Colored boxes denote problems or information

The UCSM Tabs - LAN

- LAN tab shows network related items
  - VLAN configuration
    - Global
    - Per-fabric
    - Uplink and appliance ports
    - Pin groups
    - Network policies
    - MAC pools
- Filter box lets you filter on certain components
- Easy way to see health of a component
  - Colored boxes denote problems or information

The UCSM Tabs - SAN

- SAN tab shows storage (Fibre Channel) related items
  - VSANs
    - Global
    - Per-fabric
    - Storage and adapter policies
    - WWNN and WWPN pools
- Filter box lets you filter on certain components
- Easy way to see health of a component
  - Colored boxes denote problems or information
Exploring UCS Manager
Implementing Cisco Unified Computing System (UCS) Training

The UCSM Tabs - VM
- VM tab shows VMware virtual machine related items
  - Port Profiles
  - vCenter servers
  - Virtual Machines
  - Underlying vNICs
- Filter box lets you filter on certain components
- Easy way to see health of a component
  - Colored boxes denote problems or information

The UCSM Tabs - Admin
- Admin tab shows administration related items
  - Faults, Events, and Audit logs
  - Syslog settings
  - Support information
  - Administrative settings
- Filter box lets you filter on certain components
- Easy way to see health of a component
  - Colored boxes denote problems or information

Lab – UCS Manager Demonstration
- In this lab we will
  - Explore UCS Manager
  - Highlight common functions and features
  - Look at the main tabs
  - Note where you can find common information
  - Give you a good idea of where to go when you have a question or need to make a change
Implementing Cisco Unified Computing System (UCS) Training

Exploring UCS Manager

UCS Manager – Command-Line Interface

• UCSM does offer a CLI for some functions
  – Not everything can be done via CLI
  – Really used for debugging and troubleshooting
• Allows for interaction to the underlying NX-OS operating system on the interconnects
• Normally drill down to a component or item by use of the scope command

Lab – UCSM Command-Line Interface

• In this lab we will
  – Explore the UCSM CLI
  – Show examples of common commands
    • ?
    • Show
    • Scope
    • Top/up
    • Where
    • Connect

What We Covered

✓ Introduction to UCS Manager
✓ Logging in to UCS Manager
✓ The main UCS Manager window
✓ Overview of the UCS Manager tabs
✓ UCS Manager Command-Line Interface
Initial Configuration of Cisco UCS

In This Lesson:
- Starting the initial configuration
- Connecting to the interconnects
- Using UCS Manager for the first time
- Configuring Chassis Discovery Policy
- Configuring Chassis Power Policy
- Configuring MAC Table Aging Policy
- Define DNS servers and local time zone

• You will need the information mentioned in the hardware installation lesson from the site survey
  - System Name for the interconnects
    - Note that each interconnect will use the name plus append -A and -B to it to denote the different fabrics
  - Password for the admin account
  - Three static IP addresses
    - One for each interconnect
    - Third for the virtual IP used by the cluster
  - Subnet mask for the IPs
  - Default gateway
  - DNS server
  - Domain name for the system
Connecting to the Interconnects

- The initial configuration of the interconnects is done via a serial cable
  - If you’ve setup a Cisco switch before this will be familiar
  - If your notebook doesn’t have a serial port there are USB/Serial adapters
- Connect the console cable that is included to your system and set your terminal application to the following:
  - 9600 Baud
  - 8 Data Bits
  - No Parity
  - 1 Stop Bit

Initial Configuration Walkthrough

- Now we will go to the lab and perform the initial configuration of the fabric interconnects
- Have the information we noted earlier handy
- For this demo I will be using HyperTerminal as my terminal client

Time for UCS Manager!

- The next step requires logging in to UCSM
  - Point your browser to the cluster IP you just configured
  - Download Java if required
- You will be configuring some basic options
  - Chassis Discovery Policy
  - Power Policy
  - MAC Address Table Aging
Chassis Discovery Policy

- The Chassis Discovery Policy is used when a new chassis is connected to the fabric interconnects.
- It defines the minimum number of uplinks from the chassis to the FIs:
  - Remember, you can do 1, 2, 4, or 8 (with newer I/O Modules).
- Select the lowest option you plan to use.

Power Policy

- The Power Policy specifies how the power supplies in each chassis will be configured.
- The options are:
  - Non-redundant – No power supply redundancy, not recommended.
  - N+1 – One power supply is used as a spare.
  - Grid – Used when there are two power sources and the power supplies are split.

MAC Address Table Aging Policy

- The MAC Address Table Aging Policy defines how long MAC addresses are known before being aged out.
- Highly suggested to leave this at default unless there is a specific reason to change.
- Older versions of UCSM did not let you specify the MAC table aging.
Finally, you want to set DNS and your local time zone.

- Done via the Admin tab
- Set redundant DNS servers for availability
- Set the correct time zone for log file and job scheduling accuracy

Now we will go to the lab and perform the initial configuration:

- Chassis discovery policy
- Power policy
- MAC table aging
- DNS servers
- Time zone

What We Covered

- Starting the initial configuration
- Connecting to the interconnects
- Using UCS Manager for the first time
- Configuring Chassis Discovery Policy
- Configuring Chassis Power Policy
- Configuring MAC Table Aging Policy
- Define DNS servers and local time zone
Configuring LAN Connectivity

Implementing Cisco Unified Computing System (UCS) Training
Instructor: Jason Nash

In This Lesson:

- Fabric interconnect switching modes
- Uplink switch configuration
- Using VLANs
- Configuring the upstream switch ports
- Using vNICS
- MAC address abstraction
- Using and configuring port-channels
- Configuring pin groups
- Network design considerations

Are the Fabric Interconnects Switches?

- Before we talk about connecting UCS to the rest of the network we need to talk about the Fabric Interconnects (FIs)
- Remember, the FIs are two top-of-rack devices that connect the UCS ecosystem to the rest of the world
  - Provide network switching
  - Provide Fibre Channel uplinks to storage
  - No switching done in the UCS chassis
- The FIs can operate in one of two modes:
  - EHM – Ethernet End Host Mode (the default)
  - ESM – Ethernet Switching Mode
Configuring LAN Connectivity
Implementing Cisco Unified Computing System (UCS) Training

Ethernet End Host Mode

- This is the default mode and should almost always be used

- FIs appear to the network as a host with a lot of MAC addresses
  - Not as a switch
  - Does not run the spanning-tree protocol (STP), (That's good!)
  - Far less network disruption or concern
  - All links are used due to no blocking by STP
  - Only learns server facing MAC addresses

- The two FIs are not connected to each other for data
  - Only the management cluster connections

- Reduces Control Plane load

The two FIs are not connected to each other for data
- Only the management cluster connections

- Network traffic going from one blade to another on the same VLAN and fabric is switched locally

- If the traffic is destined for outside the FI another VLAN or to a port on the other FI the traffic is sent out an uplink port

- Servers are pinned to one of those uplinks
  - Automatic or manual
  - Port or port-channel

- Traffic received by the FI for a server is forward on if the traffic arrives on the pinned uplink
  - Reverse Path Forwarding (RPF) check

- If traffic is received on a different uplink than the one pinned to the server it is dropped
  - Known as a déjà vu check

EHM Forwarding Rules

<table>
<thead>
<tr>
<th>Type of Traffic</th>
<th>From a Server</th>
<th>From the Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown Unicast</td>
<td>Flooded to servers and the pinned uplink</td>
<td>Dropped (no known server destination)</td>
</tr>
<tr>
<td>Known Unicast</td>
<td>Send to learned link</td>
<td>Send to learned server</td>
</tr>
<tr>
<td>Known Multicast</td>
<td>Depends on IGMP (Internet Group Management Protocol)</td>
<td>Depends on IGMP</td>
</tr>
<tr>
<td>Unknown Multicast</td>
<td>Flooded to the server links and the pinned uplink</td>
<td>Flooded to server links</td>
</tr>
<tr>
<td>Broadcast</td>
<td>Flooded to server links and uplinks</td>
<td>Flooded to server links</td>
</tr>
</tbody>
</table>
# Configuring LAN Connectivity

## EHM Learning Rules
- Unlike a true switch, the FIs do not learn MAC addresses from the network
  - They only learn the MAC addresses from servers
  - No need to know devices outside of UCS
- Learned MAC address do age out
  - Originally there was no MAC timeout
- Server MAC addresses can move between uplinks and interconnects during a failover
- Server MAC addresses can be statically configured

## Ethernet Switching Mode
- The other setting for the interconnects is Ethernet Switching Mode
- Makes the FIs operate as a standard switch
  - Introduces STP considerations
  - Uplinks will be blocked
- One big problem with this mode is that you cannot configure everything like you can a true switch
- Recommended to NOT use this unless absolutely necessary
  - Even then, reconsider your design
- Only time this makes sense is if it's a requirement to cross-connect fabric interconnects
- We will not cover this configuration!

## Uplink Switch Configuration
- First step in connecting UCS to the rest of the network is to configure the existing switches
- To do this you normally perform the following tasks:
  - Configure interfaces to trunk mode
  - Configure spanning-tree portfast trunk
  - Specify VLANs to trunk
  - Create port-channels and add interfaces
    - Port channel must be LACP active mode
  - Uplinked switches must trunk VLANs to UCS
  - Cisco switches are NOT required
    - May need to use Pin Groups if connecting to separate Layer 2 domains (discussed later in this lesson)
      - For example, a physically separate DMZ and production
Using VLANs

- VLANs allow for "virtual" networks running over a single cable, switch, or other infrastructure
- UCS comes configured with VLAN1
- VLANs can be
  - Global – Same VLAN on both interconnects
  - Fabric Specific – VLAN may only exist on one fabric interconnect
- In almost all cases VLANs are global and exist on both fabrics
  - Else a fabric failure would cause a disruption if no application intelligence were used

---

Cisco Nexus 5000, 5500, and 7000 Configuration

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>show feature</td>
<td>Confirm LACP is available</td>
</tr>
<tr>
<td>config</td>
<td>Enter configuration mode</td>
</tr>
<tr>
<td>interface eth1/number</td>
<td>Select interface for configuration</td>
</tr>
<tr>
<td>description UCS Fabric Interconnect A</td>
<td>Good practice to give a port a description showing its purpose</td>
</tr>
<tr>
<td>Port 2/1 (Just an example)</td>
<td></td>
</tr>
<tr>
<td>channel-group port-channel-number</td>
<td>Add this port to the LACP port-channel</td>
</tr>
<tr>
<td>mode active</td>
<td></td>
</tr>
<tr>
<td>switchport mode trunk</td>
<td>Enable trunk mode</td>
</tr>
<tr>
<td>spanning-tree port type edge trunk</td>
<td>Tells STP this is an edge port</td>
</tr>
<tr>
<td>switchport trunk allowed vlan all (or give a list)</td>
<td>Specifies which VLANs to trunk</td>
</tr>
</tbody>
</table>

---

Cisco Nexus Port-Channel Configuration

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface port-channel port-channel/ number</td>
<td>Change configuration to the port-channel interface</td>
</tr>
<tr>
<td>description Port-Channel for UCS Fabric Interconnect A</td>
<td>Description showing purpose</td>
</tr>
<tr>
<td>switchport mode trunk</td>
<td>Enable trunk mode</td>
</tr>
<tr>
<td>spanning-tree port type edge trunk</td>
<td>Tells STP this is an edge port</td>
</tr>
<tr>
<td>switchport trunk allowed vlan all (or give a list)</td>
<td>Specifies which VLANs to trunk</td>
</tr>
</tbody>
</table>
Lab – Cisco Nexus NX-OS Configuration

- Configure ports for UCS connectivity
- Create a port-channel
- Add ports to the port-channel

**Cisco Catalyst IOS Configuration**

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>config terminal</td>
<td>Enter configuration mode</td>
</tr>
<tr>
<td>Interface te2/2/1</td>
<td>Select interface for configuration. This can vary depending on switch model, module type, port type, and speed.</td>
</tr>
<tr>
<td>description UCS Fabric Interconnect A Port 2/1 (Just an example)</td>
<td>Good practice to give a port a description showing its purpose</td>
</tr>
<tr>
<td>switchport</td>
<td>Specify this port as a Layer 2 switch port</td>
</tr>
</tbody>
</table>

**Cisco Catalyst IOS Configuration Continued**

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>switchport trunk encapsulation dot1q</td>
<td>Specifies the trunking protocol as 802.1q – NOTE: Some switches only support 802.1q</td>
</tr>
<tr>
<td>switchport mode trunk</td>
<td>Enable trunk mode</td>
</tr>
<tr>
<td>switchport trunk allowed vlan vlan-list</td>
<td>Specify which VLANs to trunk</td>
</tr>
<tr>
<td>spanning-tree portfast edge trunk</td>
<td>Tells STP this is an edge port</td>
</tr>
<tr>
<td>channel-group port-channel number mode active</td>
<td>Specifies the LACP port-channel number and specifies Active mode</td>
</tr>
</tbody>
</table>
Cisco Catalyst IOS Port-Channel Configuration

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface port-channel</td>
<td>Change configuration to the port-channel interface</td>
</tr>
<tr>
<td>description Port-Channel for</td>
<td>Description showing purpose</td>
</tr>
<tr>
<td>UCS Fabric Interconnect A</td>
<td></td>
</tr>
<tr>
<td>switchport</td>
<td>Specify this port as a Layer 2 switch port</td>
</tr>
<tr>
<td>switchport trunk encapsulation dot1q</td>
<td>Specifies the trunking protocol as 802.1q –</td>
</tr>
<tr>
<td></td>
<td>NOTE: Some switches only support 802.1q</td>
</tr>
<tr>
<td>switchport mode trunk</td>
<td>Enable trunk mode</td>
</tr>
<tr>
<td>switchport trunk allowed</td>
<td>Specify which VLANs to trunk</td>
</tr>
<tr>
<td>vlan all (or give a list)</td>
<td></td>
</tr>
<tr>
<td>spanning-tree portfast edge trunk</td>
<td>Tells STP this is an edge port –</td>
</tr>
<tr>
<td></td>
<td>NOTE: On some switches this may be spanning-tree portfast trunk</td>
</tr>
</tbody>
</table>

Lab – Cisco IOS Configuration

• Configure ports for UCS connectivity
• Create a port-channel
• Add ports to the port-channel

Using vNICs

• We covered the different mezzanine cards in an earlier lesson
  – The M81KR and VIC1280 allow for virtual interfaces
  – Other adapters only allow one interface per port
• When creating vNICs you need to decide:
  – If you want multiple vNICs (if supported)
  – Which fabric do they belong to and is failover allowed?
  – Any other special features, such as integration with VMware
• Your cabling configuration can affect the number of vNICs you are allowed to configure
vNIC Failover

- Some mezzanine cards allow for hardware failover
  - Intel 10Gb Ethernet cards do not
  - Broadcom do not
  - M72KR-Q/E do not
- Should the I/O Module or all uplinks to the interconnect fail the port on the mezzanine can flip to the other I/O module
  - Do not need any sort of teaming driver on the blade operating system
- Now supported for VMware hosts as well
  - Earlier versions of UCSM did not
- Can enable or disable on a per vNIC basis

vNIC Limitations

- The number of vNICs you can configure on a virtual interface card depends on the number of I/O modules and cables
- The M81KR (Palo) supports up to 128 virtual devices
  - Each one is referred to as a "VNtag"
  - Some VNtags are used up for internal functions
- The limits apply to both vNICs and vHBAs
- Very common to use these to segment network traffic
  - Example: With VMware to split vMotion, FT, Management, NFS, etc

vNIC Limitation Tables

<table>
<thead>
<tr>
<th>No Of IOM Links</th>
<th>6124/6140: &quot;Discrete mode&quot;</th>
<th>6248: &quot;Discrete mode&quot;</th>
<th>6248: &quot;Port-channel mode&quot;</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>13</td>
<td>60</td>
<td>60</td>
</tr>
<tr>
<td>2</td>
<td>28</td>
<td>116</td>
<td>116</td>
</tr>
<tr>
<td>4</td>
<td>58</td>
<td>116</td>
<td>116</td>
</tr>
<tr>
<td>8</td>
<td>116</td>
<td>116</td>
<td>116</td>
</tr>
</tbody>
</table>

Applies with two interconnects, if only one is used cut in half
vNICs and VLANs

• How are they related?
  – Consider each vNIC to be a physical network adapter or HBA
  – The installed OS will treat them as such
• Even vHBAs actually use a VLAN to support Fibre Channel over Ethernet (FCoE)
  – Will discuss more in a later lesson
• A vNIC can have one or more VLANs assigned to it for traffic
  – Can be a single untagged (native) VLAN
  – Multiple tagged VLANs

MAC Address Abstraction

• Cisco UCS uses the concept of Service Profiles for hardware abstraction
• Instead of hardware MAC addresses it can use virtual MAC addresses from an administrative pool
  – Will create that pool in a later lesson
  – Highly advised to use a virtual MAC, not the real one
• This allows for abstraction and portability of the vNIC
• Also allows for failover between fabrics

Configuring Port-Channels

• When connecting the interconnects to the network core you have options:
  – Individual links
  – Combining links into port-channels
• Port-channels offer several advantages
  – Faster failover should a link or links fail
  – Less disruption to the network
  – Appear as a single border interface so you get better pinning performance (usually)
• Port-channels with UCS require 802.3ad LACP for negotiation
Lab — Configuring LAN Connectivity

• Enable network ports on the interconnects
• Create port-channels
• Create global VLAN(s)
• Create local VLAN(s)
• Confirm EHM mode of the interconnect

Using Pin Groups

• Normally, UCS will balance servers across uplink ports
• What if you want to specify that servers use specific ports?
• Pin Groups allow you to define which uplink server ports use
• Without pin groups UCS will pick an uplink to use
  – Often what is implemented
• Let's walkthrough the configuration

Lab — Create Pin Group

• In this lab we will
  – Create a LAN pin group
Network Considerations

- UCS provides very flexible network configuration, but there are things to keep in mind.
- Try to limit inter-fabric communication as it must traverse the outside network, unless using Switch mode.
- Be aware of how you deploy your vNICs and their use with the installed operating system.
- Don’t let the OS load-balance across vNICs in both fabrics.
  - Important when defining VMware port-groups.
  - Will discuss in more detail in a later lesson.
- Dis-jointed networks really require UCSM 2.0 for proper configuration.
  - Separate networks, like a DMZ.

Network Considerations Continued

- If inter-fabric traffic is making you consider Switch mode, reconsider the design.
- Finally, remember that traffic comes in to a server via its pinned uplink so make sure of your upstream configuration.
  - Should traffic source from an upstream switch that is peered to the one of the pinned uplink, consider changing the uplink.
  - Don’t cause unnecessary traversing of traffic.
- Be aware of network oversubscription.
  - Oversubscription is normal in networking.
  - Be aware of how much ingress/egress traffic you have with UCS.
  - Size uplinks appropriately.

What We Covered

- Fabric interconnect switching modes.
- Uplink switch configuration.
- Using VLANs.
- Configuring the upstream switch ports.
- Using vNICs.
- MAC address abstraction.
- Using and configuring port-channels.
- Configuring pin groups.
- Network design considerations.
In This Lesson:

- Cisco UCS and storage connectivity
- Benefits of iSCSI and Fibre Channel with UCS
- A primer on Fibre Channel
- How UCS integrates with the Fibre Channel fabric
- Connecting SAN Ports
- Virtual Storage Area Networks (VSANs)
- Fibre Channel over Ethernet (FCoE)
- Virtual Host Bus Adapters
- Other storage ports

Cisco UCS and Storage Connectivity

- You can use just about any storage you want with UCS
  - Local
  - Fibre Channel (FC)
  - iSCSI
  - NFS
- Only type that really requires configuration is FC
  - Boot from iSCSI is the only other time
- Much like networking, all connectivity for FC storage is done by the Fabric Interconnects

- You can use just about any storage you want with UCS
- Only type that really requires configuration is FC
- Much like networking, all connectivity for FC storage is done by the Fabric Interconnects
Benefits of iSCSI and Fibre Channel with UCS

- UCS uses the concept of Service Profiles
  - Allows for flexibility and mobility
- Maximum benefit gained when you boot from SAN
  - Local disk is more restrictive
  - Can not boot from NFS
- Boot from Fibre Channel has been around a long time
  - Boot from iSCSI is now supported in UCSM 2.0
- Your boot storage does not mean you can only use that
  - Boot vSphere from FC but use NFS for datastores

A Primer on Fibre Channel

- Popular, mature storage technology that operates at 1, 2, 4, and 8Gb speeds
- Provides block level access to storage, usually a storage array
- Servers that connect to FC storage normally use Host Bus Adapters (HBAs)
  - Connect using fibre optic cables
- Modern FC fabrics (networks) use switches and are similar to switched Ethernet networks
  - Small "workgroup" switches
  - Large "director" switches

A Primer on Fibre Channel – Addressing

- Servers are usually known as "initiators"
- Storage is usually known as "targets"
- To allow the two to communicate perform a process known as "zoning"
  - Zone one or more initiators to one or more targets
- Addressing on FC fabrics is similar to MAC address with Ethernet
  - WWNN (World Wide Node Name) – A device or HBA address
    - Example 20:00:00:00:00:12:12:12
  - WWPN (World Wide Port Name) – An address for a specific port
    - A dual-port HBA would have a single WWNN and two WWPNs
- The WWNN/WWPN is hardcoded to the HBA according to a manufacturer-based system, like a MAC address
By default, devices on an FC fabric are not allowed to communicate.

Zoning is the process of allowing communication.

You zone initiators to targets using WWNN/WWPNs.

The exact process depends on the make and model of your FC switches.

Cisco MDS can use CLI or Fabric Manager GUI.

Details outside the scope, but important to understand.

Will demo in a lab later in this lesson.

A Primer on Fibre Channel – Port Types

- **N_Ports** – Node ports, a port on an end node (server or array)
- **E_Ports** – Expansion ports, usually connect switches
- **F_Ports** – Fabric ports, ports on a switch that connect to N_Ports

There are some other ports, but those are the ones you see most often.

A Primer on Fibre Channel – Port Types

N_Port Virtualization

- By default, Cisco UCS uses a technology known as N_Port ID Virtualization (NPIV)
- NPIV allows a single N_Port to have many initiators behind it
- Requires a switch operating in NPIV mode
- Interconnects use N_Port Virtualization (NPV)
  - Can be confusing
  - Must enable NPV on the core FC switch, not NPV
- Simply put, this lets the interconnects appear as a FC host with a lot of WWPNs
  - Similar to EHV mode for networking
Fibre Channel Switching Mode

- In later versions of UCSM the FIs have two modes
  - FC End-Host Mode
  - FC Switching Mode
- End-host is the default
  - Uses NPIV
  - Appears as a host with many WWPNs
- Switching mode operates as a limited functionality switch
  - Not recommended
  - Scalability issues
  - Only for very small deployments

Fibre Channel Port-Channels and Trunking

- Similar to Ethernet port-channels
  - Bind multiple links together
  - Allows for better load distribution
- Trunking also similar to Ethernet trunks
  - Allows for multiple VSANs over links
  - When enabled all VSANs can traverse all links
- Both were introduced in UCSM 1.4

Connecting SAN Ports

- As with networks you specify storage uplink ports
- Which ports you can use depends on the interconnect
  - 6100 Series – Ports on the Fibre Channel module with an SFP
  - 6200 Series – Any port with a Fibre Channel SFP installed
    - Must configure the "slider"
- Within UCSM you enable the port for storage connectivity
  - If trunking is used all ports carry all VSANs
- Add the port to a port-channel, if desired
- Physically connect FI A to FC Fabric A and FI B to FC Fabric B
Pinning and Load Balancing of FC
• Similar to pinning for data, vHBA ports are pinned to FC uplinks
  • An uplink can be
    – A single uplink connect
    – A port-channel
  • Suggested to use port-channels if you can
    – Faster failover should a link fail
    – Better load distribution
  • Pinning is done automatically by default
    – Can be overridden with pin groups
  • If uplinks carry only specific VSANs then vHBA ports are tied to those that carry the same VSAN

What are VSANs?
• VSANs (Virtual Storage Area Networks) are similar to VLANs
  – Virtual storage networks
  – Supported by Cisco MDS
  – Not supported on non-Cisco switches
• Can be configured globally or on specific fabrics
• All Cisco MDS defaults to VSAN 1
  – Common to see that used
• Non-Cisco switches will use VSAN 1 on both fabrics

Fibre Channel over Ethernet (FCoE)
• Simply put, FCoE is Fibre Channel encapsulated in Ethernet
  – Used between the interconnects and the chassis
  – Can be used external as well
• Guaranteed to be lossless
  – QoS and other features
• Happens behind the scenes
  – Blades only see Fibre Channel
  – No special configuration
  – Standard operating system tools
Fibre Channel over Ethernet VLANs

- Each VSAN has a corresponding Ethernet VLAN
  - Used to carry FCoE traffic
- These must not conflict with other VLANs
  - Cannot have VLAN 10 for data and FCoE
- Suggested to dedicate a range of VLANs to FCoE
  - Usually a mapping to the VSAN number

About Virtual HBAs

- Virtual HBAs provide Fibre Channel access to the blades
- Some mezzanine cards offer additional functionality
  - M81KR and VIC1280 provide virtual HBAs
  - CNA cards provide fixed configuration HBAs
  - 10Gb data cards offer no FC capability
- There is no hardware-based failover of HBAs
  - Just like legacy FC
  - Use the operating systems multipathing capability or a 3rd party tool such as PowerPath
- vHBAs are tied to a VSAN membership
  - A single vHBA can only be tied to a single VSAN

vHBA Limitation Tables

<table>
<thead>
<tr>
<th>No Of</th>
<th>6120/6140:</th>
<th>6248:</th>
<th>6248:</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOM Links</td>
<td>&quot;Discrete mode&quot;</td>
<td>&quot;Port-channel mode&quot;</td>
<td>&quot;Port-channel mode&quot;</td>
</tr>
<tr>
<td>1</td>
<td>13</td>
<td>60</td>
<td>60</td>
</tr>
<tr>
<td>2</td>
<td>28</td>
<td>116</td>
<td>116</td>
</tr>
<tr>
<td>4</td>
<td>58</td>
<td>116</td>
<td>116</td>
</tr>
<tr>
<td>8</td>
<td>116</td>
<td>116</td>
<td>116</td>
</tr>
</tbody>
</table>

Applies with two interconnects, if only one is used cut in half
Lab – Configuring SAN Connectivity

- Confirm End-Host Mode
- Create VSANs
- Assign FCoE VLAN
- Enable Fibre Channel uplink ports
- Create Fibre Channel port-channels
- Show VSAN trunking configuration
- Assign ports to the port-channel
- Show an example of zoning

Other Storage Ports

- In UCSM 1.4 Cisco added three new port types
  - Appliance – Direct connected NFS/iSCSI
  - FC Storage Port – Direct connected FC storage
  - FCoE Storage Port – Direct Connected FCoE storage
- Appliance port simply allows for direct Ethernet connectivity of a NAS storage array
- FC Storage Port is for direct connected FC arrays
  - But the FIs do not perform fabric services such as zoning
  - Scaling limitations, requires other FC switch
- FCoE Storage Port – Similar to the FC Storage Port but for direct connected FCoE arrays

What We Covered

- Cisco UCS and storage connectivity
- Benefits of iSCSI and Fibre Channel with UCS
- A primer on Fibre Channel
- How UCS integrates with the Fibre Channel fabric
- Virtual Host Bus Adapters
- Virtual Storage Area Networks (VSANs)
- Fibre Channel over Ethernet (FCoE)
- Connecting SAN ports
Creating Pools

What are pools?

- Cisco UCS uses a concept of Service Profiles
  - Abstracts hardware information
  - Allows for dynamic provisioning
- Instead of using hardware addresses/settings/configurations we use identity pools
  - Allow for administrative assignments of those things
  - Configured based on purpose/location/OS
  - Removes reliance on hardware settings
- Also resource pools for server deployment
  - Automate provisioning
  - Allows for easy selection of blades based on criteria

Types of pools:
- Management IP Address Pool
- UUID Pools
- MAC Address Pools
- WWNN Pools
- WWPN Pools
- Server Pools
- Server Pool Membership
Types of Pools

- We will be talking about
  - Management IP Address Pool
  - UUID Pools
  - MAC Address Pools
  - WWNN Pools
  - WWPN Pools
  - Server Pools
  - Server Pool Membership
- The key to most of these is standardization
  - Create a standard and stick with it
  - Make it meaningful and extensible

Management IP Address Pool

- Pool of IP addresses are used to access a server via the CIMC (Cisco Integrated Management Controller)
  - KVM console
  - Serial over LAN
  - IPMI
- Possible to set these statically
  - Assigned to a server
  - Assigned to a service profile
  - Easier to use a pool (most common)
- The assigned addresses must be routable
  - Connect through the mgmt0 interfaces on the FIs

Lab — Create Management IP Pool

- In this lab we will
  - Create a Management IP Pool
  - Assign a static IP to a server
UUID Pools

- Universally Unique Identifier (UUID) is like a serial number
  - Usually embedded in BIOS
  - Sometimes used for licensing or identification
- Represented by 32 hex digits separated by 5 hyphens in 8-4-4-12 notation
  - Example: 550e2711-b29c-a716-525b1-556d45500000
- Created in Servers -> Pools -> UUID Suffix Pools
- The Prefix is set and should not be changed as it is unique to that install of UCS
  - Suffix is settable

Suggested UUID Pool Format

- While we will talk about formats for other pools, there is no real suggested format for UUIDs
- May want to create a "domain ID" for this install
  - Will be used in other pools
  - Differentiates installations of UCS

Lab – UUID Pool Creation

- In this lab we will
  - Create a UUID suffix pool
MAC Address Pools

- Each vNIC needs a unique MAC Address
  - Can use the hardcoded address
  - For mobility use a MAC pool
- MAC addresses are 48-bit addresses
  - Hex separated by colons
  - Example: 00:25:B5:2C:4D:B2
  - 00:25:B5 is an OUI (Organizationally Unique Identifier)
- Created in LAN -> Pools – MAC Pools
- As of 1.4.1x you can assign the entire 48-bit address
  - Previously 00:25:B5 could not be changed
  - Suggested you do **not** change

Suggested MAC Address Pool Format

- Can use the MAC address to denote information
  - Cluster number
  - Physical location
  - Operating system
- Suggestion below
  - GH denotes cluster/location number
  - IJ could be OS or Fabric, or both...or neither
  - KL is a sequential set of hex numbers for allocation

<table>
<thead>
<tr>
<th>Suggestion</th>
<th>User Defined</th>
</tr>
</thead>
<tbody>
<tr>
<td>OUI</td>
<td>Extension ID</td>
</tr>
<tr>
<td>AB CD EF</td>
<td>GH IJ KL</td>
</tr>
<tr>
<td>00 25 B5</td>
<td>Domain ID</td>
</tr>
</tbody>
</table>

Lab – MAC Address Pool Creation

- In this lab we will
  - Create a MAC address pool
Creating Pools
Implementing Cisco Unified Computing System (UCS) Training

**WWNN Pools**

• WWNN (World Wide Node Names) are unique addresses for fibre channel nodes
  
  • Formatted as 64-bit addresses separated by colons
    
    • Example: 20:0A:00:25:B5:00:00:EF
  
  • 00:25:B5 is Cisco's OUI but can be overridden
  
  • Two common formats
    
    – NAA=2 – Address starts with 20 (as above)
    – NAA=5 – Address starts with 50 (normally reserved for storage arrays)
  
  • Created in SAN -> Pools -> WWNN Pools

**Suggested WWNN Pool Formats**

• There is a lot of flexibility in the WWNN format
  
  – Can define almost the entire address
  – Suggested to leave the Cisco OUI
  – You do not often zone with WWNNs
  
  • Examples:
    
    – 20:11:00:25:B5:XX:XX:XX – The use of 11 in second field denotes this is a WWNN
    – 20:Domain_ID:00:25:B5:XX:XX:XX – Use second field for cluster/location ID
    – 20:Domain_ID:00:25:B5:OS_ID:XX:XX – Use the sixth field to identify the operating system used

**WWPN Pools**

• WWPN (World Wide Port Names) are unique addresses for fibre channel ports on a node
  
  – Nodes will usually have multiple WWPNs
  
  • Formatted as 64-bit addresses separated by colons
    
    • Example: 20:0A:00:25:B5:00:00:EF
  
  • 00:25:B5 is Cisco's OUI but can be overridden
  
  • Unlike the WWNN the 0 in the first field is not hardcoded
  
  • Created in SAN -> Pools -> WWPN Pools
**Suggested WWPN Pool Formats**

- There is a lot of flexibility in the WWPN format
  - Can define almost the entire address
  - Suggested to leave the Cisco OUI
  - You often zone with WWPNs
- Examples:
  - `21:Domain_ID:00:25:B5:XX:XX:XX` – Use the second number in the first field to denote fabric (1=A and 2=B)
  - `21:Domain_ID:00:25:B5:XX:XX:XX` – Use second field for cluster/location ID
  - `22:Domain_ID:00:25:B5:OS_ID:XX:XX` – Use the sixth field to identify the operating system used

**Lab — WWNN and WWPN Pool Creation**

- In this lab we will
  - Create a WWNN pool
  - Create a WWPN pool

**Server Pools**

- Server pools, as the name suggests, are pools of servers
- Used to simplify provisioning
- When you deploy a Service Profile you can deploy it to
  - A physical blade
  - A server pool
- If you deploy to a pool it grabs a blade from the pool
- A blade can exist in multiple pools
  - Once it is assigned a profile it is removed from both
**Server Pool Membership**

- Servers can be assigned to pools two ways
  - Manually by an administrator
  - Automatically by a pool policy
- Automated membership is based on criteria
  - Create an empty pool
  - Select the pool qualification criteria
  - Create a pool policy
  - Associates the criteria policy with the pool
- Blades are placed in pool at time of discovery
  - If you want to apply it to existing blades you must first re-acknowledge them

**Lab – Server Pool Creation**

- In this lab we will
  - Create a server pool
  - Create server pool policy qualification
  - Create a server pool policy
  - Re-acknowledge existing blades

**What We Covered**

- What are pools?
- Types of pools
- Management IP Address Pool
- UUID Pools
- MAC Address Pools
- WWNN Pools
- WWPN Pools
- Server Pools
- Server Pool Membership
Creating and Managing Service Profiles

In This Lesson:

- What really makes a server a server?
- Bringing it all together with Service Profiles
- Creating Service Profiles
- Service Profile templates

What Really Makes a Server a Server?

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Presentation_ID 21

Not All Server Vendors Include Management Components as a standard package
Implementing Cisco Unified Computing System (UCS) Training

Creating and Managing Service Profiles

Bringing it Together with Service Profiles
• The key to the stateless nature of server provisioning on UCS is the Service Profile
  • A Service Profile is the server, not the hardware blade
    – Required for provisioning
    – Can derive many identifiers from pools, not hardware
  • A single Service Profile is associated to a single blade at a time
    – Can be disassociated and reassociated to another
    – Even to a different model blade (not blade specific)

Contents of Service Profiles
• NIC MACs
• HBA WWNs
• Server UUID
• VLANs
• VLAN Tagging
• FC Fabrics
• FC Boot Parameters
• Number of vNICs
• vNIC Transmit Speed
• Boot order
• PXE settings
• IPMI Settings
• Number of vHBAs
• QoS
• Call Home
• Template Association
• Org & Sub Org Assoc.
• Server Pool Association
• Statistic Thresholds
• BIOS scrub actions
• Disk scrub actions
• BIOS firmware
• Adapter firmware
• BMC firmware
• RAID settings
• Advanced NIC settings
• Serial over LAN settings

The Two Opt-in Models
• There are two “opt-in” models that you will sometimes hear discussed with UCS
  – Good terms for the DCUCI exam
• Basic Opt-in – This is similar to traditional blade servers in that hardware defaults and identifiers are used, not pools
  – You can move profiles with this but those items WILL change
  – HIGHLY recommended not to use this model
• Logical Server Opt-in – Uses pools for identifiers and other information
  – You can move profiles with the identifiers intact
  – This is the model you should almost always use
Creating Service Profiles

- Creating a Service Profile is easy
  - UCSM provides a wizard that walks you through it
- Along the way you can make manual decisions or refer to many different policies or templates
  - vNIC Template
  - vHBA Template
  - Local Disk Policy
  - Boot Policy
  - Etc.
- If you do not have a policy you can "step out" of the wizard to create one
- Make sure you have your pools configured before starting

Service Profile Templates

- Not very efficient to manually create a new profile for each blade
  - Especially if they are the same configuration
- Service Profile templates allow you to easily spawn new profiles
- Process to create them is very similar to a single profile
- Two types of templates
  - Initial – If you modify the template the changes do not get passed to those profiles created from the template
  - Updating – If you make a change to the template that change gets pushed down to the profiles created from the template
- Should create a Maintenance Policy so that blades do not reboot on a change without notice

Lab – Creating a Service Profile

- In this lab we will
  - Use the wizard to create a Service Profile
  - Create the necessary policies
  - Explain the purpose and function of the policies
  - Associate a profile with a blade
  - Move the profile to another blade
Implementing Cisco Unified Computing System (UCS) Training

Creating and Managing Service Profiles

Installing an Operating System
• A Service Profile does not really do anything to install an operating system on the blade
• You can use on to specify boot from SAN, iSCSI, or network
  – Network via PXE
• You can also use virtual media access via KVM to boot a disc image
• A tool that we use for scripted installations is the Ultimate Deployment Appliance (UDA)
  – http://www.ultimatedeployment.org/
• If using or installing vSphere 5 look at the Auto Deployment feature

Lab – KVM Access
• In this lab we will
  – Access the KVM on a blade
  – Show the interface for accessing the KVM
  – Look at how to use virtual media for OS installation

What We Covered
- What really makes a server a server?
- Bringing it all together with Service Profiles
- Creating Service Profiles
- Service Profile templates
In This Lesson:

- What do I mean by routine management?
- Startup and shutdown of the interconnects
- Controlling component Power
- Status and locator LEDs
- Event, Fault, and Audit logs
- Checking status via the CLI
- Configuring Call Home
- Upgrading UCS firmware
- License Management

Routine Management of Cisco UCS

What Do I Mean By Routine Management?

- Hardware startup and shutdown
  - Shutting down and rebooting the fabric interconnects
  - Booting, rebooting, and shutting down the blade servers
- Logging and Call Home
  - Reviewing changes in the environment
  - Configuring the Call Home feature should service be required
  - Event, fault, and logging configuration
**Startup and Shutdown of the Interconnects**

- Starting up the interconnects is very easy
  - Just plug in the power!
- Rebooting an interconnect requires access to the CLI
  - `connect local-mgmt
  - reboot`

**Controlling Blade Server Power**

- Remember, you don’t manage a blade directly
  - You manage the service profile associated
- Power On/Off is handled via the service profile
- If no profile is associated, you cannot boot/shutdown the blade

**Blade Hardware Reset**

- Like many servers a B-series blade has a hard reset and power button on the front
- Power button is routed through the BMC (baseboard management controller)
  - BMC is the local management on the blade
  - Holding power for <4 secs will perform a soft reset
  - Holding power for >4 secs will perform a hard reset
  - Power button can be disabled with a BIOS policy if desired
I/O Module Hardware Reset

• The slide title is a little misleading
  – There is no hardware reset on an I/O module
• They are powered on and off with the chassis itself
  – Cannot be manually reset

Status and Locator LEDs

• Following devices have status and power LEDs
  – Fabric Interconnects – Status lights on the front and back
  – Blades – Server power light on the front
  – I/O Module – Port-activity and status lights
• Following devices have locator LEDs
  – Blades
  – Chassis
• The locator LEDs are activated from UCSM and let you confirm hardware location

Configuring Logging

• Very little to configure for logging
  – By default everything is monitored and logged
  – Can be exported to CSV for reporting
• Few settings you may consider
  – Flapping interval – Prevents a fault from recurring in rapid succession
  – Clear Action – When you clear a fault, do you want it to be retained or deleted immediately
  – TFTP Core Exporter – If an error causes a core dump you can have that sent to a TFTP server automatically
**Event, Fault, and Audit Logs**

- Several different types of monitoring
  - Events – Log changes to physical or logical devices
  - Faults – Shows faults for any object
  - Auditing – Keeps track of any administrative change to the system

**SNMP and Remote Monitoring**

- Several settings in Communication Management -> Communication Services
  - SNMP
  - HTTP/HTTPS
  - Telnet
  - CIM XML
- SNMP v3 is supported
  - Same MIBs as the Nexus series of switches (5000 or 5500)

**Checking Status Via CLI**

- Can pull some information about the environment using the CLI
- Can gather from the following:
  - Underlying Nexus operating system
  - Baseboard Management Controllers (BMC) – The out-of-band management on each blade
  - Chassis Management Controller (CMC) – Lives on the FEX and performs monitoring of the chassis
  - I/O Adapters on blades
- Output can be filtering and redirected to a file
Commands for Checking Status

- Here are some common useful commands
  - `show tech-support ucsm brief` – Good overview of overall system version and status
  - `show tech-support ucsm detail` – Generates a LOT of data and is stored in a compressed file that can be transferred off the interconnect
  - `show tech-support chassis` – Gathers information from the chassis, blades, FEX, I/O modules, and BMC
    - Can be filtered for detail

Setting Threshold Policies

- Threshold policies let you generate alerts based on thresholds that you set
- Examples include
  - All sorts of Ethernet port stats
  - Fibre Channel port stats
  - vNIC port stats
- Created via a wizard

Configuring the Call Home Feature

- The Call Home feature uses SMTP to send an email to notify administrators or support of a problem
  - TAC may know of a problem before you!
- Type of data sent is configurable
  - Pre-configured and custom profiles
  - CiscoTAC-1 – Used by Cisco TAC for data gathering
  - full_txt – Includes full XML data
  - short_txt – Shorter plain text data
- Will need configuration information
  - CCO ID
  - Contact information
  - SMTP server
Lab – Demo of Logging Capabilities

- In this lab we will
  - Configure logging settings
  - Show the Events log
  - Show the Audit Log
  - Show the Faults Log
  - Show SNMP configuration
  - Check status via CLI
  - Create a threshold policy
  - Configure Call Home

Upgrading Component Firmware

- One key feature of UCS is the ease of upgrading firmware
- Numerous components to upgrade
  - Interconnect
  - CMC
  - BMC
  - Mezzanine adapters
  - BIOS
  - Onboard RAID (LSI)
- Can be done via UCSM GUI or CLI

Upgrading Component Firmware

- Software updates are downloaded from cisco.com using your CCO login
- Each component can store two images
  - Active image that is running
  - Backup image as a fallback (or for upgrade staging)
- Types of images
  - Kernel – Underlying operating system
  - System – Version/name of the image currently booted
  - Backup – Version/name not currently booted or running
  - Startup – Version/name that will be booted the next time the component is restarted
Implementing Cisco Unified Computing System (UCS) Training

Routine Management of Cisco UCS

Downloading Firmware to UCS
- You can get new firmware to the UCS system using several protocols
  - FTP
  - TFTP
  - SCP
  - SFTP
- Required parameters will vary depending on the one chosen
- Normally you download the full firmware "blob" that includes all firmware for all components
- Cisco now offering individual upgrades, if needed
  - Useful if a new blade generation is released

Lab – Upgrade UCS Firmware
- In this lab we will push a new firmware blob to the UCS system
- Stage components for upgrade
- Activate the new version
- Using the fully redundant nature of UCS the demo will show this without a disruption to the environment

What We Covered
- What do I mean by routine management?
- Startup and shutdown of the interconnects
- Controlling component Power
- Status and locator LEDs
- Event, Fault, and Audit logs
- Checking status via the CLI
- Configuring Call Home
- Upgrading UCS firmware
- License Management
Managing Permissions in UCS Manager

In This Lesson:
- Organizational Structure in UCSM
- Organizational Inheritance
- What is Role Based Access Control?
- Understanding Roles and Privileges
- Using Locales
- Centralized Authentication
- Combining for Multi-tenancy

Organizational Structure in UCSM

- Can define a management structure within UCSM
- For management only, not for server operation
- Useful for multi-tenant implementations of UCS
Using the Organizational Structure

- By default, the only structure created is the root organization.
- You can create sub-organizations under the root organization (org).
- Under an org, you can create Service Profiles, pools, policies, etc.
- If no org is selected, the object will be created in the root org.
- There is no way to move an object from one org to another.

Organizational Inheritance

- Some objects can be inherited through the org structure:
  - For example, when creating a Service Profile at a low level org, you can use identity pools in higher orgs.
  - Identity pools work in a similar fashion:
    - MAC, WWN, WWPN, UUID
  - As do many service policies:
    - vNIC, Firmware, Disk, IPMI, etc.
  - Allows for standard configuration for some options across an organization.

Inheritance
Implementing Cisco Unified Computing System (UCS) Training

Managing Permissions in UCS Manager

Compute Blade Ownership

- Blades are not owned by any org
- They can exist in one or more orgs and server pools
- Therefore they can be associated with Service Profiles that exist in any org

What is Role Based Access Control?

- Role Based Access Control (RBAC) lets you assign permissions to a role
- Then you put people in that role
- For example, a role of Storage Admin may have access to change the SAN configuration
- You then assign the Storage Admin role to specific users
- Much more manageable than doing permissions per-user

Understanding Roles and Privileges

- Important to understand the difference
- Roles are made up of a collection of privileges
  - A user can be assigned to one or more roles, not a 1:1 relationship
  - If assigned to multiple roles the privileges are combined
- Privileges are single rights or capabilities
  - A role will have one or more privileges assigned to it
  - The idea being you simplify management by creating roles that are made up of privileges and then assign a user or users to that role
  - Later you can add other users to the same role easily
Combining Organizations and RBAC

- The two are really not directly related
  - Can be considered complementary
- Can use orgs without RBAC
  - Just use the admin user
  - Just use orgs for management
- Can use RBAC without orgs
  - All access granted at the root org

The Predefined Roles

- Cisco UCS contains several roles that are already defined
  - **Server Admin** – Server Equipment in UCSM – allows for management of physical blades, Service Profiles, maintenance, and other related items
  - **Network Admin** – Network in UCSM – allows for configuration of network connections including VLANs, uplinks, trunks, and other items related to external connectivity
  - **Storage Admin** – Storage in UCSM – allows for configuration of storage connectivity including VSANs, uplinks, and other Fibre Channel features
  - **Operations** – Operations in UCSM – allows for monitoring of faults, events, and Call Home configuration

Lab – Predefined Roles

- In this lab we will
  - Look at the pre-defined roles
  - Show which privileges they are assigned
Locales
- Locales are a collection of orgs and are used to help assign roles for management
  - The orgs do not have to be related (parent/child)
- You assign a locale to a user
- Useful so that you can assign privileges to many orgs with one role
- Required to use external authentication

Lab – Users and Locales
- In this lab we will
  - Create a new user
  - Assign them one or more roles
  - Create a new locale
  - Assign a locale to the user

Centralized Authentication
- In most datacenters there is a central authentication method
- Cisco supports several authentication systems
  - RADIUS
  - TACACS+
  - LDAP
- Useful for centralized account management and auditing
- When using central authentication UCS will pass credentials
  1. User logs in to UCS
  2. UCS passes credentials to the authentication server
  3. Authentication server passes or declines the login request
  4. UCS grants access to the user
Configuring the Authentication Server

- When using some authentication methods you must make a change to the server schema
- Must add a Cisco-specific attribute to the user’s account
  - LDAP – CiscoAVPair
  - RADIUS & TACACS+ – cisco-av-pair
- How to do this will depend on the exact authentication server implementation that you use

Lab – External Authentication Configuration

- In this lab we will
  - Look at the configuration options for external configuration

Combining for Multi-tenancy

- Now let’s put it all together
- Organizational Structure
  - Management hierarchy for UCSM
  - No real affect on the operation of blades
- Locales
  - Used to group orgs to ease administration and management
  - Must be used for external authentication
- RBAC
  - Ease management configuration
  - Used to delegate privileges to users
  - Only manages access within UCSM, not to blades or their operating systems
What We Covered
- Organizational Structure in UCSM
- Organizational Inheritance
- What is Role Based Access Control?
- Understanding Roles and Privileges
- Using Locales
- Centralized Authentication
- Combining for Multi-tenancy
Configuring Backup and Restore for Cisco UCS

In This Lesson:
- Backing Up UCS Configurations
- About the Full-State Backup
- About the System Configuration
- About the Logical Configuration
- About the All Configuration
- Creating Backup Jobs
- Importing UCS Configuration Backups

- Obviously, it's a good idea to backup the UCS configuration
- It's possible to have both interconnects fail
  - Bad luck
  - Site disaster
- There are several types of backups
  - Full-state backup
  - System configuration
  - Logical configuration
  - All configuration
- Some backups are in XML and can be edited and reused
  - Templates for other installs
About the Full-State Backup

- Binary file that includes a snapshot of the entire system
  - Not stored in XML
  - Not possible to edit and import
- This is "the" way to fully backup the UCS environment
- Used to do a full system recovery
  - To the same FIs
  - To new FIs

About the System Configuration Backup

- Includes all system configuration settings
  - Stored in XML
  - Useful for editing and import
- Includes primarily AAA information
  - Roles
  - Access
  - TACACS/LDAP/RADIUS
- Known as config-system in UCS
- You cannot use this for a system restore

About the Logical Configuration Backup

- Includes all logical configuration settings
  - Stored in XML
  - Useful for editing and import
- Includes many items such as
  - Service profiles
  - VLANs
  - VSSAs
  - Pools
  - Policies
- Known as config-logical in UCS
- You cannot use this for a system restore
About the All Configuration Backup

- Includes all system and logical configuration
  - Stored in XML
  - Useful for editing and import
- Known in UCS as config-all
- Combination of backups from config-logical and config-system
- You cannot use this for a system restore

Creating Backup Jobs

- Backup jobs are created within the UCSM GUI or CLI
- Jobs must be run manually
  - Still no way to schedule jobs
- Options to select when creating a job include:
  - Admin State – Enabled or disabled
  - Type – Full, All, System, Logical
  - Protocol – FTP, TFTP, SCP, SFTP
  - Hostname – Destination for backup
  - Remote File – Name of the backup file
  - User – User for login to remote system
  - Password – The user’s password
- Can watch status in the FSM (Finite State Machine)

Lab – Creating UCS Backup Jobs

- In this lab we will
  - Create backup jobs in the UCSM GUI
  - Create backup jobs in the UCSM CLI
Importing UCS Backups

• Creating an import job is very similar to a backup job
• Select if you want to "merge" or "replace" data
  – Replace – Erase existing configuration and replace it with the imported configuration
  – Merge – Attempts to create objects that exist in the backup set but not in the current configuration
• The Full-state import requires you to erase the FI config and import
  – Command-line operation only
  – Very destructive
• Other backups can be imported at initial configuration or after UCSM is running

Lab – Importing a UCS Backup Configuration

• In this lab we will
  – Import logical configuration backups via UCSM GUI
  – Import logical configuration backups via UCSM CLI
  – Show how to start an import of the full-state backup at initial configuration

What We Covered

✓ Backing Up UCS Configurations
✓ About the Full-State Backup
✓ About the System Configuration
✓ About the Logical Configuration
✓ About the All Configuration
✓ Creating Backup Jobs
✓ Importing UCS Configuration Backups
Configuring High Availability of Cisco UCS

Implemtening Cisco Unified Computing System (UCS) Training
Instructor: Jason Nash

In This Lesson:

- Cisco UCS and High Availability
- High Availability Connections
- High Availability Clustering
- High-Availability Terms
- High Availability Data
- Fabric Interconnect Elections
- Uh Oh! Split Brain!
- Managing High Availability

Cisco UCS and High Availability

- By now you're probably aware that UCS is very highly available
  - Redundant (almost) everything
- This lesson will walk through managing all of the high availability connections, features, and options
High Availability Connections

As discussed earlier, interconnects are connected to each other via Ethernet cables for clustering:

- L1 to L1, L2 to L2
- One or more connections from each chassis to each interconnect
  - 1, 2, 4, or 8 connections from each FEX

High Availability Clustering

- Each interconnect is a separate entity
  - Both run NX-OS and UCSM
  - One is active for UCSM at a time
  - Both are active for I/O
- Management port on each FI connected to the same Layer 2 management network
- Each FI has its own management IP
  - Plus a third shared cluster IP
- Remember that each FEX in a chassis goes to a SINGLE interconnect

High-Availability Terms

- Terms are important to understanding some concepts
  - Very important if taking the DCUCI exam
- Node – A node is one of the fabric interconnects
  - Primary Node – The active FI for UCSM clustering
  - Subordinate Node – The non-active FI for UCSM clustering
- Group – Both nodes (interconnects) make up a group
- Again, UCSM clustering is active/passive
  - I/O connectivity is both nodes active
High Availability Data
• Each fabric interconnect has its own NVRAM (Non-Volatile Random Access Memory) that it uses to store data
  – When both FIs are functioning the data can be replicated between them over the cluster links
  – Goes for configuration data as well as other things such as firmware images
• Each Chassis Management Controller (CMC) stores information in NVRAM about the chassis
  – Serial EEPROM (SEEPROM)
  – Chassis Number
  – Each node (FI) can see this information

Fabric Interconnect Elections
• One of the interconnects is designated the leader
• This does not change unless there is a major disruption
  – In fact, an FI can actually crash/reboot and still maintain leadership
  – The idea is to reduce disruption of the cluster
• Normally a new leader is not elected unless
  – Current leader crashes
  – An administrative change forces it
• Usually you do nothing for this process
  – It’s automatic and inconsequential who is cluster leader
  – Does not affect I/O

Configuring Node High Availability
• Remember during initial install when you told setup that you were creating a cluster?
  – That’s it!
• No other configuration is required if configured properly
  – If HA is not functional, check cross-connect cables
  – L1 to L1, L2 to L2
Uh Oh! Split Brain!

- Split brain occurs when both interconnects think they are active
- What might cause this?
  - FIs cannot communicate over Layer 2 or Layer 3
    - Known as a "partition in space"
    - Given the direct connection this is very rare
    - One FI may have a newer configuration that was not replicated to the other
    - Other FI may have been down at the time
    - Known as a "partition in time"
- To resolve this the interconnects use the SEEPROM in the chassis

Resolving Split Brain

- Both causes of split brain are resolved in a similar fashion using the SEEPROM in a chassis
- For a "partition in space" they use a "quorum race" where they each try to write as fast as possible
  - The one that writes first wins
  - The other aborts and backs out of the cluster
  - Can rejoin later when communication is restored
- For a "partition in time" the primary node writes a version number to the SEEPROM
  - If the primary node is down and the subordinate tries to create the cluster it first compares its version to that of the SEEPROM
  - If it is the same or newer the cluster is started

Managing High Availability

- Occasionally you may want to flip the status of the nodes
- Two types of promotions/demotions
  - Switchover – Issued by the administrator and makes the subordinate node primary, and the primary subordinate
    - Sometimes called a synchronous request
  - Failover – Caused by UCSM and promotes the subordinate to primary
    - Sometimes called an asynchronous request
  - Can force switchover and monitor HA status using CLI commands
Lab – Managing High Availability

• In this lab we will
  – Check cluster status
  – Change the primary node (ask nicely)
  – Force a primary node change (force the issue)

What We Covered

 Cisco UCS and High Availability
 High Availability Connections
 High Availability Clustering
 High-Availability Terms
 High Availability Data
 Fabric Interconnect Elections
 Uh Oh! Split Brain!
 Managing High Availability
Virtual Networking and Cisco UCS

In This Lesson:

- Warning! Virtualization ahead!
- What does one have to do with the other?
- Overview of the Cisco Nexus 1000v
- Architecture and components of the Nexus 1000v
- What are pass through switching and VM-FEX?
- Let's talk about vSphere Networking
- Dive in to VM-FEX

Warning! Virtualization Ahead!

- This lesson is heavy on virtualization terms and ideas, specifically VMware
- If you are not familiar with VMware you may struggle to understand all of the concepts presented
- If you plan to take the DCUCI exam you need to understand these as they are tested pretty heavily
What Does One Have to Do With the Other?

- The UCS system has some integration with VMware and other hypervisors
  - Pass Through Switching (PTS)
  - VM-FEX
- Cisco has a virtual switch for VMware and Hyper-V
  - Called the Nexus 1000v
  - No real integration between it and UCS but must be understood

Overview of the Cisco Nexus 1000v

- The Cisco distributed virtual switch extends the vSphere Distributed Switch (vDS) and adds many key features
  - Security policies
  - More robust security
    - DHCP Snooping
    - Dynamic ARP Inspection
    - IP Source Guard
  - Quality of Service
  - Network and application monitoring
  - Get the network back to being owned and managed by the network team

Overview of the Cisco Nexus 1000v

- Comes at a cost
  - Additional per-socket licensing
  - More complex with additional components
    - Not integrated in to vCenter like the dvSwitch
    - Requires Cisco knowledge for support and management
    - It is managed and configured via CLI just like a physical Cisco switch
  - More configuration options can cause misconfiguration
    - More complex configuration with many more options and settings
Components of the Cisco Nexus 1000v

- **Virtual Supervisor Module (VSM)**
  - GUI interface to the Nexus 1000v
  - Leverages VSM CLI
  - Controls multiple VEMs as a single network device

- **Virtual Ethernet Module (VEM)**
  - Replaces VMware's virtual switch
  - Enables advanced switching capability on the hypervisor
  - Provides each VM with dedicated "switch ports"

Key Points About the Nexus 1000v

- The VSM is the control plane
  - Provides management functions
  - Not in the data path so data flows if the VSMs are down
  - Can be run as virtual appliances or as a physical appliance (Nexus 1010) rack mount server

- The VEM is the data plane
  - Makes switching and forwarding decisions
  - VEM installed on each vSphere host

- No real integration between UCS and the 1000v switch
  - Managed and controlled outside of UCSM

Let’s Talk About vSphere Networking

- Normally vSphere sees the physical NICs installed in a server and you assign them as vSwitch uplinks
- Local traffic is switched inside the vSwitch, external traffic sent to the physical switch
- Load is on the vSphere server and on the network admin to trunk all of these connections
What are Pass Through Switching and VM-FEX?

- Remember our discussion earlier on FEX?
  - Extending a fabric to another switch or device
  - FEX in a UCS chassis are really part of the interconnects
- With VM-FEX you can control NICs assigned to a vSphere host from UCSM
  - Allows for switching to be done in the physical interconnect
  - Offloads that from the vSphere host
  - Requires the Cisco VIC adapter (M81KR or VIC1280)
  - Also requires vSphere Enterprise Plus and the vSphere Distributed Switch to be deployed

Quick Diagram Showing VM-FEX

- Shows VM-FEX and Pass Through Switching
- Pass Through Switching uses the VMDirectPath function of vSphere to directly give a VM access to a network interface
  - Bypasses the hypervisor for increased performance

Integrating UCS and vSphere

- For this configuration to work there must be integration between UCS and the VMware environment
- UCS Manager talks to vCenter and pushes Port Groups and other configuration information
  - Port Groups are setup as port-profiles in UCSM
  - They denote things such as VLAN, port security, and rate limiting
- As VMs are vMotioned around those changes are sent back to UCSM so that the interconnects are aware and can update
  - Allows for vMotion of VMs even with VMDirectPath enabled
The Two Modes of VM-FEX

- The first mode is called Emulated mode
  - VMs do not have direct access to the virtual hardware presented by the VIC
  - vSphere emulates an NIC (vmxnet3 for example) to replicate the hardware that it virtualized for the guest OS
- The second mode is called VMDirectPath or Pass-Through Switching (PTS)
  - The VM has direct access to the virtual hardware presented by the VIC
  - Every NIC in a guest VM is 1:1 mapped to a dynamic Ethernet interface on the VIC
  - Highest performance mode
  - Supports vMotion with vSphere 5

Requirements for VM-FEX

- For VM-FEX to be configured and function it has some specific requirements
- Hypervisor must be VMware vSphere or RedHat KVM
  - Hyper-V support is coming
- Must be vSphere Enterprise Plus licensing
  - Must be using the vOS
- Blade servers must use either the M81KR or VIC1280 adapters
- Each vSphere host must have the Cisco VEM component
  - Same as used with the Nexus 1000v
- To deploy you create Dynamic vNIC Connection Policies in UCSM for Service Profiles

Configuring UCSM and vCenter for VM-FEX is a multistep process

- UCSM does provide a very useful wizard
- Still requires importing an extension key in to vCenter
- All steps performed by the wizard can be done manually
- Will need to create vNIC policy and update Service Profiles
Lab – Using VM-FEX

• In this lab we will
  – Overview of VM-Fex
  – Look at UCS configuration
  – Show integration

What We Covered

 Warning! Virtualization Ahead!
 What Does One Have to Do With the Other?
 Overview of the Cisco Nexus 1000v
 Architecture and Components of the Nexus 1000v
 What is Pass Through Switching and VM-FEX?
 Let’s Talk About vSphere Networking
 Dive in to VM-FEX
Troubleshooting Cisco UCS

In This Lesson:
- What are the common areas of problems?
- General troubleshooting
- All about faults
- What are core files?
- Gathering tech support files
- Troubleshooting different functions
- Powering down the environment
- Other resources

What are the Common Areas of Problems?
- The UCS architecture is very straightforward
- Not a lot of moving parts that can cause problems
  - Bonus of minimal infrastructure
- Dynamic nature of Service Profiles can help
  - If you think a blade is bad just move the profile to another
- Still find occasional firmware bugs
- Java client can be problematic
  - Most always it’s the JRE
General Troubleshooting

- First, know where to look for information
  - **Faults** – Created when there is a problem or a threshold has been reached
  - **Events** – Created whenever something happens and stays there
    - Does not get cleared like a fault
  - **Audit Log** – Events created that show user activity
    - Also not cleared
  - **System Event Log (SEL)** – Resides in the CIMC (Cisco Integrated Management Controller) on a blade
    - Stores information from BIOS
    - Limited in size, around 40KB
  - **Syslog** – If you configure Syslog don’t forget to check that log

Fault Severity Levels

- Faults have a specified severity level and can actually change severity, depending on what happens
  - **Critical** – Bad. Most likely disruptive and requires immediate attention.
  - **Major** – Still bad. Most likely something is severely degraded and causing an impact.
  - **Minor** – Should not be causing a disruption but should be corrected so it does not escalate.
  - **Warning** – Potentially impactful problem. Usually something you should investigate.
  - **Condition** – Informational message.
  - **Info** – Another, lower severity, informational message.

Varying Fault States

- Along with severity faults also have different states and these can cause some confusion
  - **Cleared** – The condition has been resolved and the fault or problem is now cleared
  - **Flapping** – If a fault happens, gets cleared, then happens again within a set interval (the flapping interval) it will be marked as flapping
  - **Soaking** – Similar to flapping, the fault was triggered and then cleared in a short period of time
  - Lifecycle is normally that a fault occurs, is resolved, cleared after a time, and eventually deleted
Different Types of Faults

• There are a number of different specific types of faults that denote what or where the problem has occurred
  – FSM – Task within the FSM has failed
  – Equipment – Physical equipment failure
  – Server – A server task has failed, such as a problem associating a service profile to a blade
  – Configuration – UCSM cannot successfully perform a configuration change
  – Environment – Power, thermal, or other environmental management issue
  – Connectivity – There is a connectivity problem, usually with an adapter or other module
  – Network – Network problem such as a link has gone down
  – Operational – Operational problem such as a log being full

What Are Core Files?

• If a component in the UCS system fails it may create a core file
• Core files contain a lot of information
  – Memory dump from time of crash
  – Useful for a snapshot of the error condition
• Can configure UCSM to TFTP those off when created
  – Use the Core File Exporter function
• Can view core files from UCSM and the CLI
  – Really only usable by Cisco TAC
  – Not human readable

Tech Support Files

• Often when working on a problem Cisco TAC will request a "tech support" bundle
  – Contains a lot of information on the UCS configuration
  – Easy way to gather almost everything they would need
• Can create these for UCSM, chassis, FEX, and/or rack server
• Can be created via the UCSM GUI or CLI
  – Prior to UCSM 1.4(1) you could only do this via CLI
Lab – Create Tech Support File

- In this lab we will
  - Create the tech support file from UCSM
  - Create the tech support file from the CLI

Troubleshooting KVM Issues

- There are several things that can cause remote KVM to not work
- Check the Management IP pool used by KVM
  - Must be on same VLAN as mgmt0 on the interconnects
  - Must be in the same routable IP range too
- Confirm the cables and connections to each interconnect
  - KVM access goes through the mgmt0 port
    - Experienced this when some KVMs worked, some didn't
- If there are multiple KVM sessions open, close some
- Have been browser and OS issues with virtual media in KVM
  - Try a Windows system with Internet Explorer

Troubleshooting Boot from SAN

- This one is common
  - Often the first time many have done boot from SAN
- No magic bullet, just confirm configuration
  - Target WWN correct?
  - Boot LUN created and in the same storage group as the host?
  - Is your zoning correct?
  - Is your boot policy set for boot from SAN?
    - Suggested that all boot LUNs appear to the host as LUN 0.
    - Is the host registered on the array?
- Different arrays may also require other configuration
Troubleshooting Server Blades

• If a blade acts odd consider moving the service profile to another and see if the problem follows
  – Easy way to narrow down to configuration or hardware
• Check the blade status LEDs
  – Hard disks have status LEDs on the front
  – Blade status LED will notify you of problems
    • Solid for minor error
    • Blinking for major error
• Common for misconfigured memory to cause a problem
  – Confirm the memory configuration and placement
• There is a dongle available for direct blade access and troubleshooting

The Ethanalyzer

• Fabric Interconnects have an integrated Ethanalyzer tool for viewing management and data traffic
  – Uses Wireshark
• Must be connected to the underlying NX-OS to use
• Can capture different types of traffic
  – inbound-hi – FCoE, FC, LACP, STP and DCBX
  – inbound-low – ICMP, CDP, TCP/UDP/IP/ARP for management
  – Mgmt – Management interface
• Save captures to a file for later analysis with Wireshark
  • Example:
  – LabFI-A(nxos)# ethanalyzer local interface inbound-low
    write volatile:///sample-capture

Powering Down the UCS Environment

• During planned maintenance you may need to take the entire environment down
  – UPS maintenance
  – Move the infrastructure to a new rack
• Very simple process with a few steps
  1. Create a configuration backup
    – Move it off the interconnect to a safe place
  2. Gracefully power down all operating systems and blades
    – When powered down the power LED on the blade shows amber instead of green
  3. Unplug the chassis power
  4. Unplug the subordinate FI and then the primary
Other Information Resources

- Cisco has a good troubleshooting guide
  - From general problems to very specific
- Great Twitter list of UCS resources (including me!) by Steve Chambers
  - https://twitter.com/stevie_chambers/#/ciscoucs
- Updated list of many resources by Steve Chambers
  - https://supportforums.cisco.com/docs/DOC-8594
- Cisco Community including a very active forum

Suggested Continual Reading

- The Unified Computing Blog by Dave Alexander
  - http://www.unifiedcomputingblog.com/
- Sean McGee, Cisco DC Architect (GREAT information)
  - http://www.mseanmcgee.com/
- Michael Heil, Large UCS Customer
  - http://healthitguy.wordpress.com/
- Jeremy Waldrop, a Varrow brother and our DC Practice Lead
  - https://jeremywaldrop.wordpress.com/
- Define the Cloud blog by Joe Onisick
  - http://www.definethecloud.net/

What We Covered

- What Are the Common Areas of Problems?
- General Troubleshooting
- All About Faults
- What Are Core Files?
- Gathering Tech Support Files
- Troubleshooting Different Functions
- Powering Down the Environment
- Other Resources
Implementing Cisco UCS Start to Finish

In This Lesson:
- Before you order
- When the gear arrives
- Cabling configuration
- Starting the configuration process
- Basic configuration in UCSM
- Administration/Monitoring configuration
- Storage configuration
- Network configuration
- Service profiles

Before You Order
- Size the environment for your needs
  - Choose the right size Fabric Interconnects
  - Look and compare blades
- CPUs and memory combinations
- Confirm the power requirements of the configuration
  - Make sure correct power cables are ordered
- Check space in the rack(s) for initial install as well as future growth
- Good idea to go ahead and plan out schemes for identity pools
  - Keep in mind your environment might grow
Before You Order

- Verify distance to other switches and confirm proper SFPs get ordered
- Have your vendor or Cisco look for any product holds or delays
- Do you have 10Gb in your network now?
  - Will you add it?
- Make sure you have the modules and SFPs for the other end
- Do a port count on the Fabric Interconnects so you can confirm licensing
  - All ports licensed
  - Interconnects include some licensing

When the Gear Arrives

- Compare what you received with your order
  - Check packing list
  - Locate all small parts, like SFPs
- If you did not order cables with the UCS equipment make sure those are acquired
  - CAT6 cables for mgmt0 and L1/L2
  - Fibre cables for Fibre Channel or 10GBase-SR/LR SFPs
- Rack the gear
  - Use team work
  - Use a lift for the chassis
- Install modules as needed
  - Power supplies, fans, FI modules, blades

Cabling Configuration

- Refer back to the live lab video if needed
- Connect Fabric Interconnects to management network via mgmt0 interfaces
- Cross connect the cluster links L1 -> L1, L2 -> L2
- Connect I/O modules in chassis to the Fabric Interconnects
  - Again, do not cross connect the I/O modules to both FIs
  - 1, 2, 4, or 8 connections only
- If applicable, connect FC cables from each Interconnect to a single FC fabric
- Connect each Interconnect to uplevel switches
  - Cross connect these, if possible
Starting the Configuration Process

- Have 3 IP addresses and the associated network information ready
- Connect to the first FI with a serial cable
- Perform initial cluster configuration
  - Choose a cluster name, remember it will append -A and -B to the name
- When done, boot the second FI and have it join the new cluster
- Confirm you can ping both mgmt0 IP addresses as well as the shared cluster IP
- Make sure you can log in to the cluster IP and see UCSM

Basic Configuration in UCSM

- Set the basic policies
  - Chassis Discovery Policy
  - Minimum number of uplinks
  - Power Policy
    - Power supply redundancy mode for the chassis
  - Configure server uplinks
    - Ports that go to the I/O modules
  - Suggested to go ahead and update the firmware to the latest
  - Configure configuration backup jobs

Administration/Monitoring Configuration

- Configure external authentication, if used
  - Don’t forget the schema addition
- Create any custom roles you plan to use
- Create any org structure and locales that may be needed
- Create the Management IP Pool
  - Remember, must be on same subnet and VLAN as mgmt0 interfaces
- Configure basic functions
  - DNS server
  - NTP/Timezone
  - Call Home
  - Add any additional licenses
Storage Configuration

- What storage protocol do you plan to use?
- If using FC make sure to
  - Get proper SFPs for both ends
  - Enable NPIV mode on your FC switches
  - Create your WWNN and WWPN pools
- Connect cables to your FC switches
- Enable storage uplink ports in UCSM
  - Confirm connectivity
  - Suggest you use port-channels, if you can
    - Requires Cisco MDS
- Configure pinning groups, if you plan to use them
- Feel free to pre-zone using your WWPN pools

Network Configuration

- Confirm modules and SFPs in the uplink switches that you plan to use
- Configure the ports as directed in the lesson
  - VLAN trunking
  - Spanning-tree edge port configuration
- Create all needed VLANs in UCSM
- Connect cables between FIs and switches
  - Suggest you use port-channels
- Configure pinning groups, if planning to use them
- Create your MAC address pool(s)

Service Profiles

- Create your policies and UUID pool(s) now or during Service Profile creation
  - BIOS and Firmware policies
  - vNIC and vHBA templates
  - Any server pools (if used)
  - Local Disk policies
  - Maintenance Policy (user ack.)
- Create your Service Profile Templates for any standard build
  - Then deploy your Service Profiles as needed
What We Covered

- Before you order
- When the gear arrives
- Cabling configuration
- Starting the configuration process
- Basic Configuration in UCSM
- Administration/Monitoring configuration
- Storage configuration
- Network configuration
- Service profiles
Preparing for the DCUCI Cisco Data Center Unified Computing Systems Implementation Exam

In This Lesson:
- A word about the exam
- An overview of the exam
- Candidate Profile
- Some cautions about the exam
- The Cisco Data Center Unified Computing Support Specialist Certification
- Recertification
- Before and after the exam

First, a Word About the Exam
- At the time of the creation of this course the current exam is 642-983
  - Valid until May 7, 2012
- There is a revision to the exam (642-994) announced
  - Available on February 7, 2012
- Blueprints for the exams are very similar
- While this course was designed to help you deploy, use, and support UCS we also tried to make sure it covered the items in the blueprints as well
An Overview of the Exam

- This exam is about deploying, using, and supporting Cisco UCS
  - LAN connectivity
  - SAN connectivity
  - Creation of pools and profiles
  - Troubleshooting
- It also heavily covers other components in the Cisco data center strategy
  - MDS
  - Nexus 5K/7K
  - Nexus 1000v
- This course plus any hands-on work, even with the UCSPE, should prepare you

Candidate Profile

- Audience profile:
  - The person taking this exam should be a well-rounded UCS administrator including SAN connectivity, LAN connectivity, deploying operating systems on blades with Service Profiles, and integrating with VMware vSphere
  - A few things that concern people are the external integrations such as Fibre Channel and VMware
  - May not be using those in your environment
- Information in this course should more than cover you for those pieces if you are light in experience

Some Cautions About the Exam

- My purpose is not to scare you, but prepare you
- One concern I have about the exam is there is no indication of which version of UCS Manager they are testing you on
  - Things change over time
  - Features and limitations change as versions are released
- Cisco sometimes uses terms in training material and exams that are not used in product documentation
  - Have tried to use the terms here where appropriate
Cisco Data Center Unified Computing Support Specialist

• Taking the DCUCI exam by itself does not gain you any certification.
  – It is a component of the DC Unified Computing Support Specialist certification.
• The Cisco Data Center Unified Computing Support Specialist is designed to test a learner’s knowledge of the fundamentals of the Cisco Unified Computing System and their ability to implement a virtualized Data Center environment.
  – Key word being “virtualized”

There are several components to the certification:

• Step 1: Cisco Pre-requisites
  – ICSNS (Data Center Storage Networking Support Specialist) and DCNIS (Data Center Networking Infrastructure Support Specialist)
  OR
  – “Fast start option”: Choose this option if you wish to bypass the first choice by completing your Cisco CCNA certification and passing the DCUCI Qualifier Exam (642-979)
• Step 2: Earn your VMware Certified Professional (VCP) certification
• Step 3: Pass the DCUCI exam

Like most Cisco specialist exams the Cisco Data Center Unified Computing Support Specialist must be renewed every two years.

Two options for renewal:
  – Retake all exams required for the exam
  OR
  – Pass a current CCIE or CCDE written exam
Study Recommendations

• To prepare for the DCUCI exam I suggest
  – Watch and study this video series
  – Take full advantage of the Cisco UCS Platform Emulator
  – If you have access to physical hardware use that as well
    • If you work for a partner contact your Cisco account manager
      for access to remote labs
  – If you want or need more detailed information refer to the UCS
    documentation on Cisco’s site

• Do NOT use brain dumps or actual exam questions to “study”

Preparing for the Exam

• Go ahead and schedule your exam
  – At least for me, having a date on the calendar provides a lot of
    motivation
  – Otherwise I’ll just keep postponing it and days become weeks
• Steadily study, don’t try to cram the night before
• Have what you need when you arrive at the testing center
  – Two forms of ID of which one must have a photo
  – Picture will be taken
• Get there early just in case there is a problem
• When you take the exam you are given a sheet to write on
  – Not really needed for this exam
  – Some people like to note how many confident answers they have

After the Exam

• If you pass the exam and are working toward the larger
  certification you will need to link your information to that of
  VMware to confirm your VCP certification
  – This can take days or in my original case, weeks
• If for some reason you do not pass (and it happens to
  everyone) you must wait 5 calendar days
  – Starts on the day after your exam
And That’s It!

Good Luck!
Next Steps

Implementing Cisco Unified Computing System (UCS) Training
Instructor: Jason Nash

You Are Here
Now you’ve added Cisco UCS to your list of infrastructure proficiencies

Where you go from here depends on what interests you more:
- VMware or Hyper-V?
- Storage?
- Networking?
- Application deployment?

Cisco Virtualized Data Center

Other technologies that combine well with UCS:
- Nexus switching
- MDS Fibre Channel storage
- Virtualization
- Other storage technologies

Great need for converged skillsets as organizations start to embrace cloud and other streamlined infrastructure

Combination of skills needed for deployment, management, and troubleshooting these environments
Next Step Supporting Resources

1. Cisco Data Center Blog
   http://blogs.cisco.com/category/datacenter/

2. Twitter can be a great resource!
   • Suggested hashtags: #CiscoUCS #Nexus #1000v #vSphere

3. Great content at Cisco Live
   • Not just for the networking crowd!

4. Check the resources I gave you in the troubleshooting lesson
   • Several great blogs for staying up to date on new UCS features

5. Several good UCS books out as well

6. Ways to learn about storage
   • http://nixapedia.com/category/vapps/

Literal Next Steps

Once you determine the path you believe is best for you, you might consider if there are certifications that will help to validate your experience.

You will certainly need training to embrace new subjects and TrainSignal has an immense library of training to choose from.

You will need to keep moving forward... in much the same way technology never stands still.
   • Cisco UCS is evolving very quickly
   • Datacenter technologies are racing along

We Value Your Opinion

There are so many ways to reach us!
   • Call us at 1-888-229-5055 (worldwide: 1-847-776-8800)
   • Email us at feedback@trainsignal.com
   • Post on our forums at http://forums.trainsignal.com/

Join the TrainSignal Conversation
   http://www.trainsignal.com/blog
   http://www.facebook.com/trainsignal
   http://twitter.com/trainsignal
   http://www.trainsignal.com
   http://www.youtube.com/trainsignalinc
   http://www.youtube.com/trainsignaloffice