# Newer Cisco Validated Design Guides Available

This guide is part of an older series of Cisco Validated Designs.

Cisco strives to update and enhance CVD guides on a regular basis. As we develop a new series of CVD guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in CVD guides, you should use guides that belong to the same series.

Open the latest version of this guide

Access the latest series of CVD Guides

Continue reading this archived version

# Hosted Cloud Connector Using Cisco UCS E-Series

## Technology Design Guide

December 2013

CISCO VALIDATED DESIGN

# Table of Contents

# Preface

Cisco Validated Designs (CVDs) provide the foundation for systems design based on common use cases or current engineering system priorities. They incorporate a broad set of technologies, features, and applications to address customer needs. Cisco engineers have comprehensively tested and documented each CVD in order to ensure faster, more reliable, and fully predictable deployment.

CVDs include two guide types that provide tested and validated design and deployment details:

- **Technology design guides** provide deployment details, information about validated products and software, and best practices for specific types of technology.
- **Solution design guides** integrate or reference existing CVDs, but also include product features and functionality across Cisco products and may include information about third-party integration.

Both CVD types provide a tested starting point for Cisco partners or customers to begin designing and deploying systems using their own setup and configuration.

## How to Read Commands

Many CVD guides tell you how to use a command-line interface (CLI) to configure network devices. This section describes the conventions used to specify commands that you must enter.

Commands to enter at a CLI appear as follows:

```
configure terminal
```

Commands that specify a value for a variable appear as follows:

```
ntp server 10.10.48.17
```

Commands with variables that you must define appear as follows:

```
class-map [highest class name]
```

Commands at a CLI or script prompt appear as follows:

```
Router# enable
```

Long commands that line wrap are underlined. Enter them as one command:

```
police rate 10000 pps burst 10000 packets conform-action set-discard-class-
transmit 48 exceed-action transmit
```

Noteworthy parts of system output or device configuration files appear highlighted, as follows:

```
interface Vlan64
  ip address 10.5.204.5 255.255.255.0
```

## Comments and Questions

If you would like to comment on a guide or ask questions, please use the feedback form.

For the most recent CVD guides, see the following site:

http://www.cisco.com/go/cvd/wan

# CVD Navigator

The CVD Navigator helps you determine the applicability of this guide by summarizing its key elements: the use cases, the scope or breadth of the technology covered, the proficiency or experience recommended, and CVDs related to this guide. This section is a quick reference only. For more details, see the Introduction.

## Use Cases

This guide addresses the following technology use cases:

- **Remote-Site Hosted Cloud Connector Applications**—This guide helps organizations deploy applications at remote-site locations and improve network performance by using local Internet access.

For more information, see the "Use Cases" section in this guide.

## Scope

This guide covers the following areas of technology and products:

- Design and configuration of Cisco UCS-E series module in the Cisco ISR-G2 router platform for use with VMware ESXi and Hosted Cloud Connector applications.

For more information, see the "Design Overview" section in this guide.

## Proficiency

This guide is for people with the following technical proficiencies—or equivalent experience:

- **CCNA Routing and Switching**—1 to 3 years installing, configuring, and maintaining routed and switched networks
- **VCP VMware**—At least 6 months installing, deploying, scaling, and managing VMware vSphere environments

## Related CVD Guides


Remote Site Using Local Internet Access Technology Design Guide

To view the related CVD guides, click the titles or visit the following site: http://www.cisco.com/go/cvd/wan

# Introduction

The *Hosted Cloud Connector Using Cisco UCS E-Series Technology Design Guide* enables an organization to access cloud-based services from their remote sites and provides the following benefits:

- Optimal routing from the remote site to the cloud service provider using local Internet access
- Flexible, on-demand deployment of applications on the existing remote-site routing platform
- Simple operational model for distributed service deployment

## Related Reading

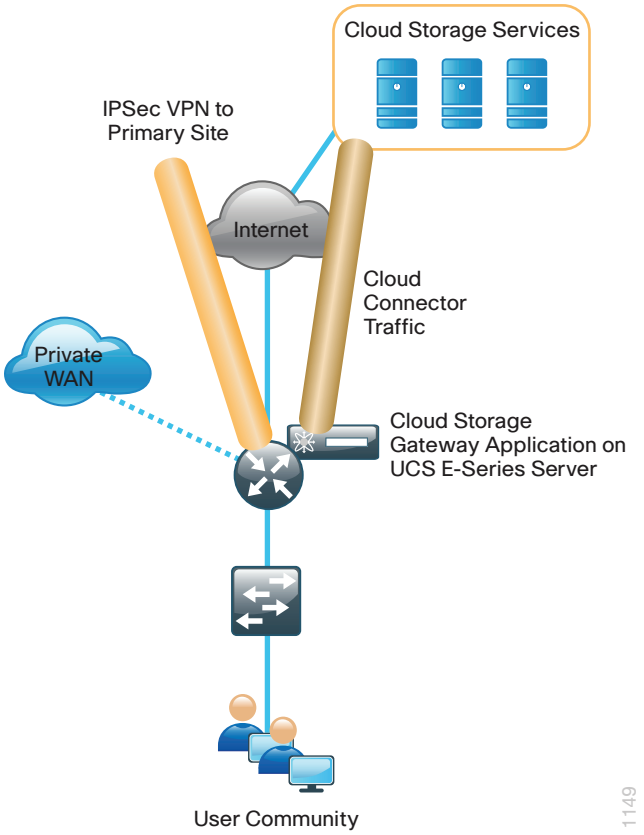
The Remote Site Using Local Internet Access Technology Design Guide provides guidance and configuration for deploying remote site WAN connectivity with Local Internet Access.

## Technology Use Cases

Organizations are quickly adopting cloud services to help enable new business models for greater flexibility at lower cost. Organizations are increasingly looking at the benefits of hosting cloud-based applications at the remote office and accessing the public cloud directly. These types of applications are called *cloud connectors* and can be hosted directly on the remote office router using an integrated Cisco Unified Computing System (UCS) server.

A cloud connector is a Cisco or third-party software component embedded in, hosted on, or integrated with enterprise routing platforms. You can use cloud connectors for a variety of applications, including storage, virtualization, document handling, security, collaboration, and provisioning.

*Figure 1 - Remote site hosted cloud connector on UCS E-Series Server*




When you deploy hosted cloud applications by using Cisco ISRG2 and UCS E-Series integrated server modules, you gain unique benefits such as unified support and serviceability, integrated security, and increased application visibility using Cisco AVC for an overall reduction in total cost of ownership (TCO).

### Use Case: Remote Site Hosted Cloud Connector Applications

This guide helps organizations deploy applications at remote-site locations and improve performance by using local Internet access and by reducing traffic transmitted over private WAN links to the primary site. The operational model is simplified by integrating the application within the existing Cisco Integrated Services Router (ISR) platform at the remote site without requiring additional standalone platforms.

This design guide enables the following network capabilities:

- Deployment of UCS E-Series Servers in ISRG2 routers
- Deployment of UCS-E specific VMware ESXi for Hosted Cloud Connector Applications
- Deployment of host cloud connector applications that communicate directly with a cloud service by using the local Internet connection

# Design Overview

Due to the adoption of cloud services and virtualized data centers, organizations are undergoing a tremendous transition. When deploying cloud connectors and a distributed cloud-services model for business continuity, increased productivity, and enhanced application performance, organizations are faced with several key challenges in network application security and visibility.

When organizations deploy Cisco Cloud Connector applications as part of an integrated platform using the Cisco ISRG2 and UCS E-Series Server module to leverage cloud services in the remote office, the organizations increase network performance by:

- Eliminating WAN backhaul
- Enabling service localization
- Reducing service and support costs

This is all possible while increasing security and visibility through advanced capabilities such as Cisco IOS Zone-Based Firewall (ZBFW) and Cisco Cloud Web Security (CWS), and Cisco AVC.

Cisco Cloud Connector applications deliver business-continuity solutions for voice, data retrieval, cloud storage, and security applications by leveraging local direct Internet access from the remote office location to the cloud-service provider. Additionally, this combined platform eliminates the need for additional remote office footprint and deployment concerns that often arise with multiple component solutions.

There are many Cisco Cloud Connectors available today, with more in development through the Cloud Connector ecosystem. The ecosystem is designed to foster third-party development of Cloud Connectors for hosted and scripted connectors.

Deploying hosted Cisco Cloud Connector applications today using a combined Cisco platform prepares an organization for additional benefits and integration of scripted Cloud Connectors. This is an integral part of the Cisco software-defined networking (SDN) strategy where the intelligence of the networking platforms can be accessed through the Cisco Open Network Environment Platform Kit (Cisco OnePK) application programming interface (API). The Cisco OnePK API allows modification of network behavior for a specific application.

## UCS E-Series Integrated Servers

The Cisco UCS E-Series Server is a converged computing solution, offering a bare metal OS, or virtualization-ready integrated networking platform.

Cisco UCS E-Series Server provides an integrated platform for Cisco and third-party cloud connector applications to run virtually “within the network” and is the basis for Cloud Connector Solutions. The hardware capabilities, ease of deployment and hypervisor support (VMware, Microsoft Hyper-V Server, Citrix XenServer) make UCS E-Series Server a viable platform for cloud services deployments.

*Figure 2 - UCS E-Series Server modules*

The Cisco UCS E-Series Server is offered in two form factors for the ISR-G2 2900 and 3900 series platforms with a fully integrated BMC controller (CIMC) like the UCS C-Series. Cisco SMARTnet Service for the ISRG2 router covers support for the UCS E-Series Server module. The UCS E-Series Servers are extremely efficient, using as much as 80% less power than a typical server resulting in a lower total cost of ownership (TCO).

*Table 1 - UCS E-Series Server module options*

| Component | UCS E140S | UCS E140D | UCS E160D | UCS E140DP | UCS E160DP |
|---|---|---|---|---|---|
| Router slot width | Single | Double | Double | Double | Double |
| CPU family | Zeon E3 | Zeon E5 | Zeon E5 | Zeon E5 | Zeon E5 |
| CPU cores | 4 | 4 | 6 | 4 | 6 |
| DDR3 memory slots | 2 | 3 | 3 | 3 | 3 |
| Max memory | 16G | 48G | 48G | 48G | 48G |
| Hard drive bays[1] | 2 | 3 | 3 | 3 | 3 |
| Internal 1GE ports | 2 | 2 | 2 | 2 | 2 |
| Built-in External 1GE ports | 1 | 2 | 2 | 2 | 2 |
| PCIe card support[2] | No | Yes | Yes | Included | Included |
| 10/100 management ports | 1 | 1 | 1 | 1 | 1 |
| RAID support | 0/1 | 0/1/5 | 0/1/5 | 0/1/5 | 0/1/5 |

1. Drive bays support 2.5 inch SAS, SSD, and SED drives.
2. There are two PCIe card options, a four-port 1GE module or a single port 10GE (SFP) with FCoE support.

## Cloud Storage Connectors

A *cloud storage connector* is locally hosted software that connects an organization via the Internet to cloud-based storage services. Cloud storage provides cost savings and business agility for organizations, while delivering easier ways to store, share, and protect enterprise data.

To enable distributed cloud storage, organizations must address several key challenges regarding security and overall network impact–specifically, the speed and latency in remote sites. By deploying storage cloud connector solutions using the solution presented in this guide, an organization can secure integration of an on-premises storage gateway and the cloud-based storage infrastructure with greatly reduced impact on WAN.

## Router Selection for Remote Sites

The actual WAN remote-site routing platforms remain unspecified because the specification is tied closely to the bandwidth required for a location and the potential requirement for the use of service module slots. One of the benefits of a modular design approach is that organizations have the ability to implement this solution with a variety of potential router choices.

There are many factors to consider in the selection of the WAN remote-site routers. Among those, and key to the initial deployment, is the ability to process the expected amount and type of traffic. You also need to make sure that you have enough interfaces, enough module slots, and a properly licensed Cisco IOS Software image that supports the set of features that is required by the topology. Cisco tested multiple integrated service router models, and the expected performance is shown in the following table.

*Table 2 - WAN remote site Cisco Integrated Services Router options*

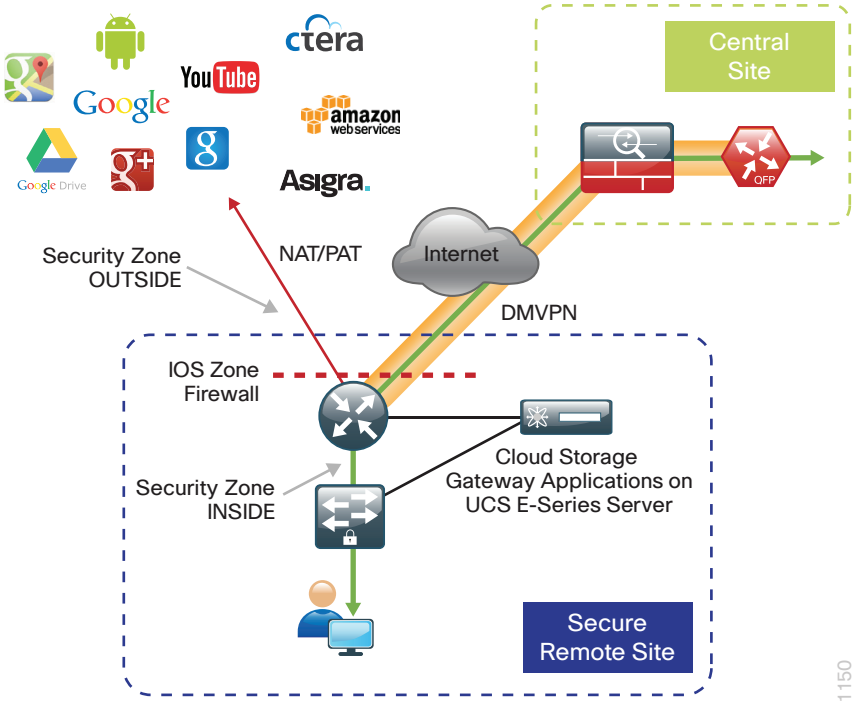
| Option | 2911 | 2921 | 2951 | 3925 | 3945 |
|---|---|---|---|---|---|
| Ethernet WAN with services[1] | 35 Mbps | 50 Mbps | 75 Mbps | 100 Mbps | 150 Mbps |
| On-board FE ports | 0 | 0 | 0 | 0 | 0 |
| On-board GE ports[2] | 3 | 3 | 3 | 3 | 3 |
| Service module slots | 1 | 1 | 2 | 2 | 4 |
| Redundant power supply option | No | No | No | Yes | Yes |
| Supported UCS E-Series Server module | UCS E140S | UCS E140S<br>UCS E140D | UCS E140S<br>UCS E140D | UCS E140S<br>UCS E140D<br>UCS E160D | UCS E140S<br>UCS E140D<br>UCS E160D |

1. The performance numbers are conservative numbers obtained when the router is passing Internet MIX (IMIX) traffic with heavy services configured and the CPU utilization is under 75 percent.
2. A single-router, dual-link remote-site requires four router interfaces when using a port-channel to connect to an access or distribution layer. Add the EHWIC-1GE-SFP-CU to the Cisco 2900 and 3900 Series Integrated Services Routers in order to provide the additional WAN-facing interface.

## Deploying Hosted Cloud Connectors on UCS E-Series Servers

Hosted cloud connector applications such as Amazon Web Services (AWS) storage gateway, Asigra, and CTERA, can be deployed at remote locations using an integrated UCS E-Series Server module.

*Figure 3 - Cisco secure remote site - cloud storage connector*




Cisco has chosen and validated several cloud storage solutions including the AWS storage gateway, Asigra Cloud Backup Connector, and the CTERA cloud storage solutions.

- The AWS storage gateway combined with the Cisco UCS E-Series Server platform is an easy to deploy secure and flexible cloud storage connector for small to large organizations.
- The Asigra offers the Asigra Cloud Backup Connector solution in partnership with Cisco. A Cisco 3900 and 2900 family of routers are pre-installed with Asigra Cloud Backup, providing organizations with a simple, cost effective, and ready to use data protection infrastructure while avoiding the need for separate IT investments for backup and recovery.
- CTERA's enterprise cloud storage solution combined with Cisco the ISRG2 and UCS E-Series Server platform enables the secure deployment of integrated cloud storage applications to remote offices locations.

**Reader Tip**

This guide assumes the remote-site router has been configured for local Internet access using the Remote Site Using Local Internet Access Technology Guide. This guide provides both local Internet routing and configuration guidelines for deploying security for local Internet configurations.

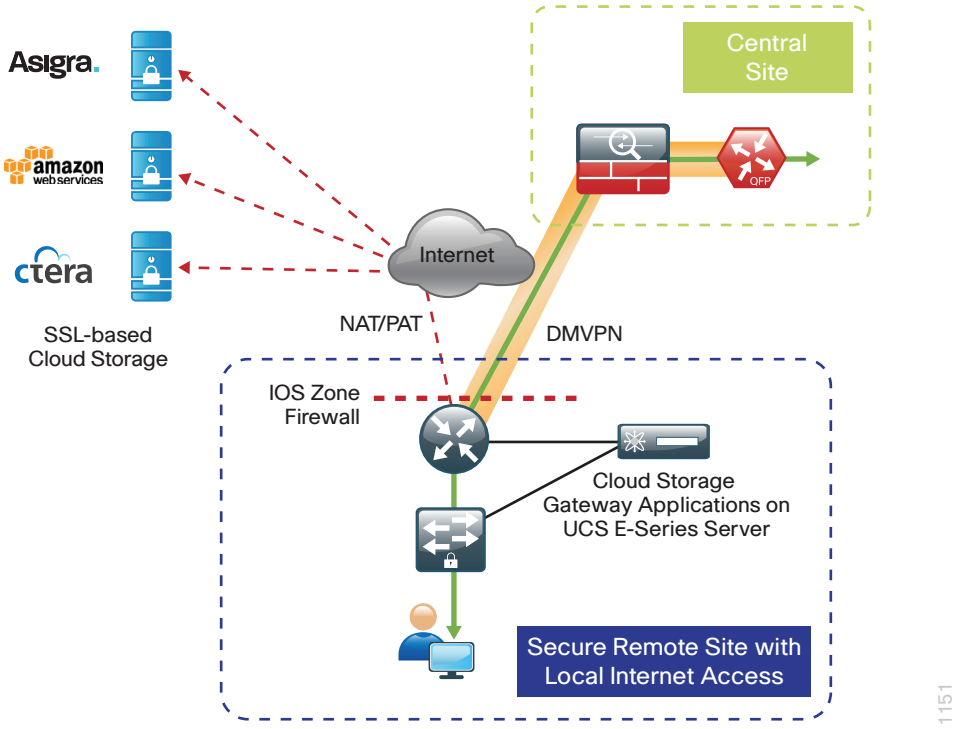
These applications allow remote-site locations to backup data directly to the cloud for disaster recovery (DR) and continuity of operations (COOP) requirements. Local Internet access provides increased performance for cloud-based applications as well as reduces bandwidth utilization on more expensive private WAN connections when compared to centralized Internet solutions.

*Table 3 - Cloud storage connector gateways*

| Gateway application | Software version | UCS E-Series Server ESXi versions |
|---|---|---|
| AWS | v145-VM | 5, 5.1.0 |
| Asigra | 12.2 | 5, 5.1.0 |
| CTERA | 3.2.47.3 | 5, 5.1.0 |

The UCS E-Series Server module can be deployed in Cisco 2900 and 3900 routers configured as part of remote site with local Internet designs taking advantage of the combined and integrated security features of the catalyst switching platform, UCS E-Series Server, and the ISRG2 router.

*Figure 4 - Hosted cloud storage applications*




## Tech Tip

UCS E-Series Server modules can be configured with SAS self-encrypting drives (SEDs). The contents of an SED are always encrypted. The encryption keys are also encrypted and protected in hardware that cannot be accessed by other parts of the system. Disk encryption is done in hardware on each drive without performance penalty. Disks are also not subject to attacks targeting other components of the server system.

For this capability use the E100S-HDSASED600G drive for the single-wide servers and E100D-HDSASED600G drives for the double-wide servers.

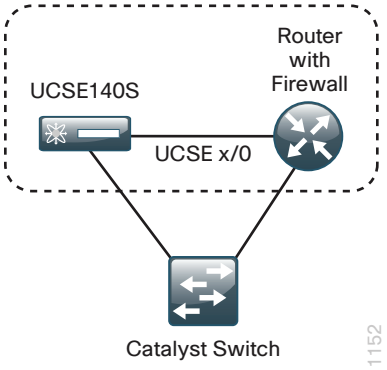
## Single Router Remote-Site Designs

In the single router VPN WAN design, you install a single or double-wide UCS E-Series Server module into the ISRG2 router.

> **Tech Tip**
>
> When resiliency is required the use of the double-wide modules is recommended in all designs. Double-wide modules provide greater application performance and resiliency options with RAID 5 and additional external interfaces.

The single-wide UCS E140S module can be deployed in designs where resiliency is not a critical factor and when router hardware is limited. In these designs, the external gigabit interface is connected to a single external switch.

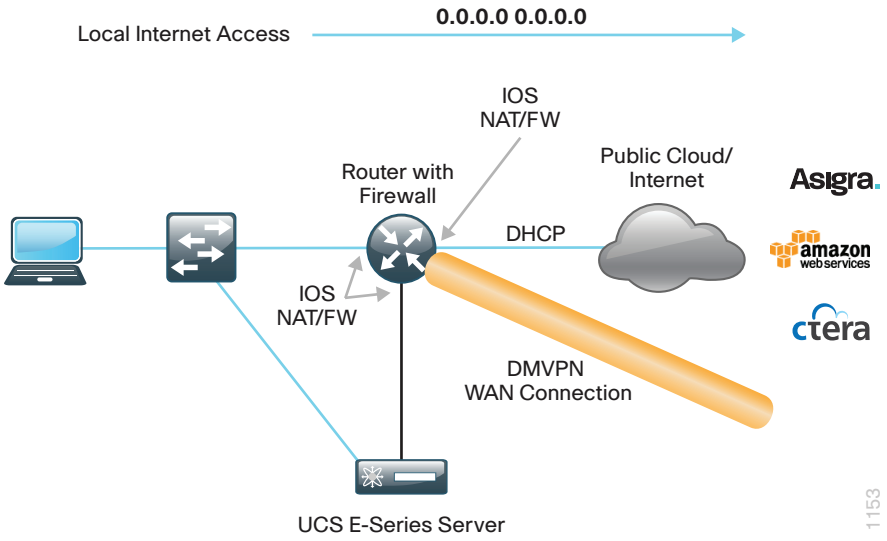
*Figure 5 - Cisco ISRG2 router with integrated UCS E-Series Server*




Hosted Cloud Connector applications access cloud services directly via split tunneling on the single outside Internet interface. Cloud applications communicate securely with cloud services using SSL-based communications.

You configure DMVPN for secure encrypted connectivity to internal network resources in a central location. In this configuration bandwidth is shared for internal and external communication. This design model has no redundancy for internal or external traffic.

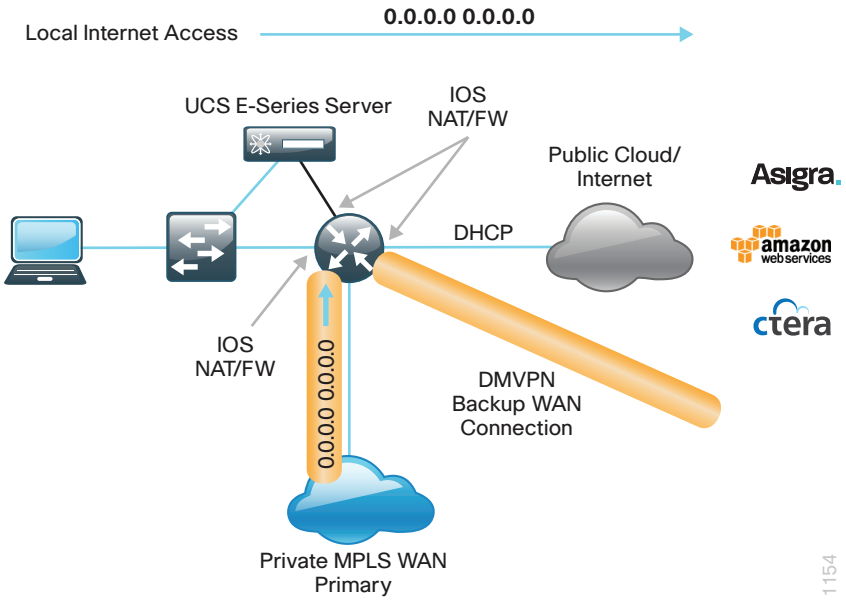
*Figure 6 - Single router VPN WAN - UCS E-Series Server*




In the single router MPLS Primary or L2 WAN primary with VPN WAN backup, you install a UCS E-Series Server module into the ISRG2 router. Hosted Cloud Connector applications access cloud services directly via split tunneling on the single outside Internet interface. Cloud applications communicate securely with cloud services using SSL-based communications.

You configure DMVPN as a backup path for secure encrypted connectivity to internal network resources in a central location. In this configuration, bandwidth is not shared for internal and external communication during normal operation. All internal traffic uses dedicated private WAN services and external communications for Internet browsing and cloud connector applications use the separate local Internet connection. During Internet failure situations, cloud services can be redirected to use central Internet access.

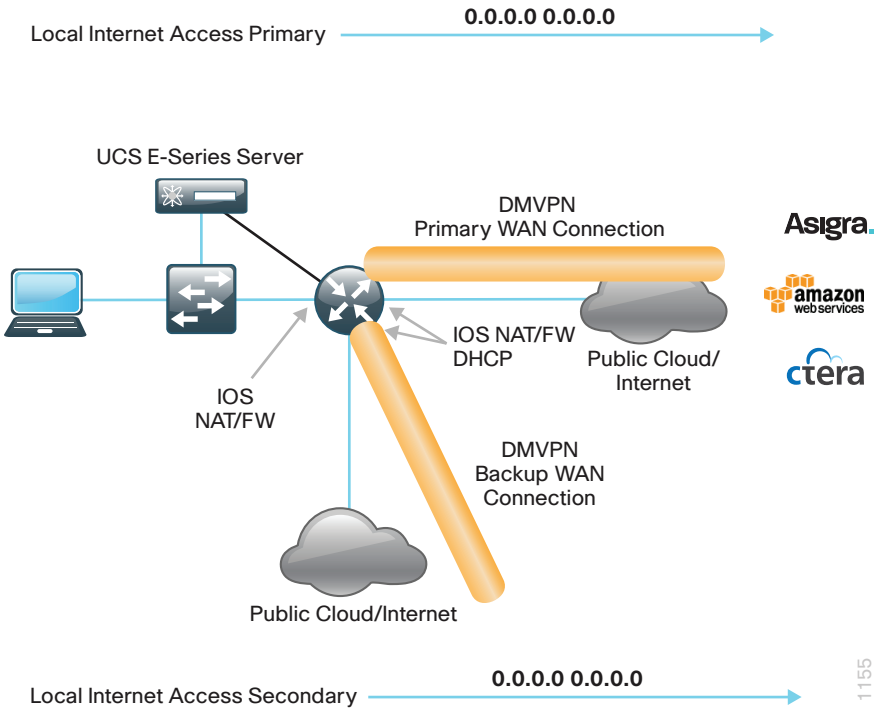
*Figure 7 - MPLS WAN & L2 WAN primary with VPN backup - UCS E-Series Server*



In the single router Dual VPN WAN configuration, hosted Cloud Connector applications access cloud services directly via split tunneling on the single outside Internet interface. Cloud applications communicate securely with cloud services using SSL-based communications.

You configure DMVPN for primary and backup paths for secure encrypted connectivity to internal network resources in a central location. In this configuration, bandwidth is not shared for internal and external communication during normal operation. All internal traffic uses the primary VPN WAN connection and external communications for Internet browsing and Cloud Connector applications use the secondary local Internet connection. During Internet failure situations, local Internet access is maintained.

*Figure 8 - VPN WAN primary with backup link - UCS E-Series Server*



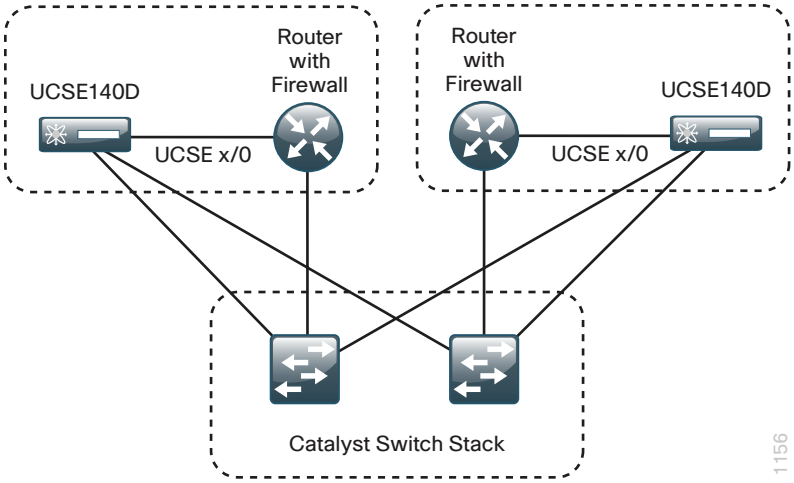

## Dual Router Remote-Site Designs

Where possible, in dual router deployments you should deploy the double-wide UCS E-Series Server such as the UCS E140D. The double-wide modules have two external Ethernet connections that can each be connected to different external switches to provide resilient connectivity for applications.

**Tech Tip**

When resiliency is required, you should use double-wide modules in all designs. Double-wide modules provide greater application performance and resiliency options with RAID 5 and additional external interfaces.

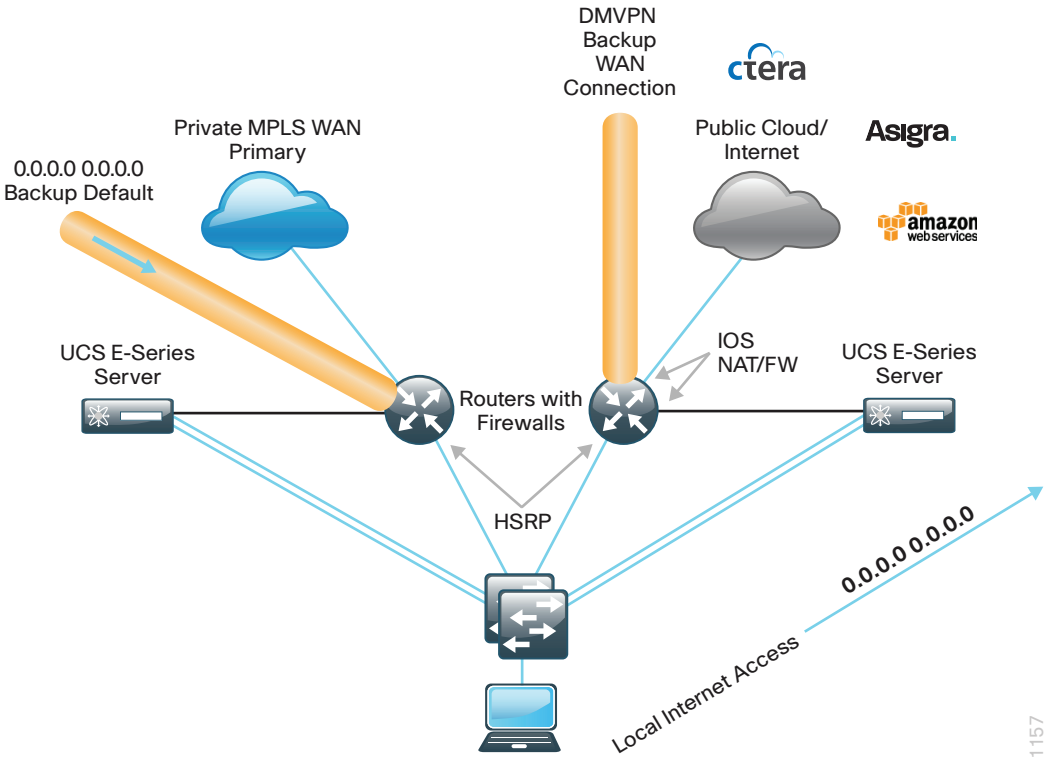
*Figure 9 - Cisco ISRG2 routers with integrated UCS E-Series Servers*




In dual router MPLS Primary or L2 WAN primary with VPN WAN backup, you install a UCS E-Series Server module into each ISRG2 router. Hosted Cloud Connector applications access cloud services directly via split tunneling on the single outside Internet interface. Cloud applications communicate securely with cloud services using SSL based communications.

You configure DMVPN as a backup path for secure encrypted connectivity to internal network resources in a central location. In this configuration bandwidth is not shared for internal and external communication during normal operation. All internal traffic uses dedicated private WAN services and external communications for Internet browsing and cloud connector applications use the separate local Internet connection. During Internet failure situations, cloud services can be redirected to use central Internet access.

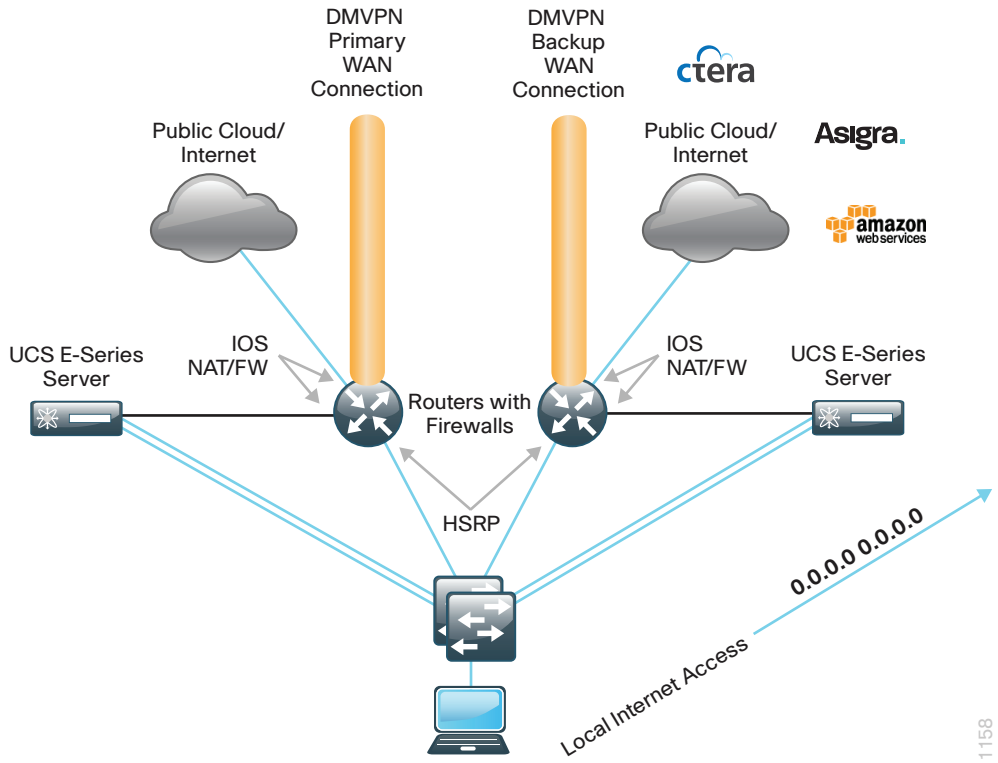
*Figure 10 - MPLS primary backup link and router - UCS E-Series Server*



In the dual router Dual VPN WAN, you install a UCS E-Series Server module into each ISRG2 router. Hosted Cloud Connector applications access cloud services directly via split tunneling on the single outside Internet interface. Cloud applications communicate securely with cloud services using SSL-based communications.

You configure DMVPN for primary and backup paths for secure encrypted connectivity to internal network resources in a central location. In this configuration bandwidth is not shared for internal and external communication during normal operation. All internal traffic uses the primary VPN WAN connection and external communications for Internet browsing and cloud connector applications use the secondary local Internet connection. During Internet failure situations, local Internet access is maintained.

*Figure 11 - VPN WAN backup link and router - UCS E-Series Server*




## Tech Tip

Although this task is not shown in this guide, you can configure multiple UCS E-Series Server modules for application scale and redundancy.

In single and dual router designs, you can install multiple UCS E-Series Server modules within a single router to meet specific organizational requirements. You can maintain some levels of application redundancy using VMware capabilities.

In these configurations, external storage solutions are probably required. For these and other types of requirements, consult your application and hypervisor technical representatives for configuration details.

PROCESS

## Installing and Configuring the UCS E-Series Server Module

1. Connect UCS E-Series Server to remote-site switch
2. Configure ISRG2 for CIMC access
3. Configure UCS E-Series Server using CIMC
4. Configure RAID using CIMC

In this process, you configure the remote site access switch, ISRG2 CLI for UCS E-Series Server Cisco Integrated Management Controller (CIMC) access, and prepare the integrated server hardware for applications.

### Reader Tip

To complete the full installation and configuration of a hosted cloud storage application on the Cisco UCS E-Series Server module, this process must be combined with the "Installing VMware ESXi on the UCS E-Series Server Module" and "Deploying Hosted Cloud Storage Applications on the UCS E-Series Server Module" processes in this guide.

### Configuration Checklist

The following table specifies the parameters, data, and universal design parameters that you need in order to set up and configure applications running on the Cisco UCS E-Series Server module. For your convenience, you can enter your values in the table and refer to it when configuring the UCS E-Series Server module. The values you enter will differ from those in this example, which are provided for demonstration purposes only.

*Table 4 - Cisco UCS E-Series Server module network parameters*

| Parameter | CVD values for an access-layer connection | CVD values for a distribution-layer connection | Site-specific values |
|---|---|---|---|
| In-band management network | 10.5.252.0/24 (existing data subnet) | 10.5.241.0/25 (new subnet for UCS E-Series Server management) | |
| UCS E-Series Server interface address | unnumbered gig0/2.64 | 10.5.241.1./25 | |
| CIMC interface address | 10.5.252.10/24 | 10.5.241.30/25 | |
| VMware ESXi interface address | 10.5.252.11/24 | 10.5.241.31/25 | |
| Switch interface number | 1/0/15, 2/0/15 | 1/0/15, 2/0/15 | |
| UCS E-Series Server default gateway | 10.5.252.3 | 10.5.241.1 | |
| UCS E-Series Server host name | RS242-UCS-E | RS240-UCS-E | |

## Procedure 1 Connect UCS E-Series Server to remote-site switch

Use this procedure to configure an access-layer switch for UCS E-Series Server connectivity. The access switch is the appropriate location to physically connect Cisco UCS E-Series Server modules at single-tier remote sites. Regardless of the switch type—single switch, switch stack, or modular—this type of connection must use a Layer 2 access interface. At distribution layer sites, the Cisco UCS E-Series Server module is physically connected to the distribution-layer switch.

This guide assumes that the Cisco UCS E-Series Server module has been installed into the remote-site router and that the LAN switch has already been configured. Only the procedures required to complete the connection of the switch to the UCS E-Series Server module are included. For more information about how to configure switches, see the Campus Wired LAN Technology Design Guide.

### Option 1: Single-wide UCS E-Series Server module

**Step 1:** Connect the Cisco UCS E-Series Server's external Ethernet interface to an Ethernet port on the remote site switch, and then return the switchport configuration to the default.

```
default interface GigabitEthernet1/0/15
```

**Step 2:** Define the switchport in the remote-site switch as an access port for the data VLAN, and then apply port-security and quality of service (QoS) configuration.

```
interface GigabitEthernet1/0/15
 description Link UCS-E 140S
 switchport access vlan 64
 switchport host
 ip arp inspection trust
 logging event link-status
 macro apply EgressQoS
 no shutdown
```

### Option 2: Double-wide UCS E-Series Server module

**Step 1:** Connect the Cisco UCS E-Series Server's external Ethernet interface to an Ethernet port on the remote site switch, and then return the switchport configuration to the default.

```
default interface GigabitEthernet1/0/15
default interface GigabitEthernet2/0/15
```

**Step 2:** Define the switchport in the remote-site switch as an access port for the data VLAN, and then apply port-security and QoS configuration.

```
interface GigabitEthernet1/0/15
 description Link UCS-E 140D interface gig 0/2
 switchport access vlan 64
 switchport host
 ip arp inspection trust
 logging event link-status
 macro apply EgressQoS
 no shutdown
```

```
interface GigabitEthernet2/0/15
 description Link UCS-E 140D interface gig 0/3
 switchport access vlan 64
 switchport host
 ip arp inspection trust
 logging event link-status
 macro apply EgressQoS
 no shutdown
```

**Tech Tip**

The single-wide UCS E-Series Server modules only have a single external Ethernet interface. The double-wide modules have two external Ethernet interfaces for VM traffic and should be connected to two external switches for redundancy.

## Procedure 2 Configure ISRG2 for CIMC access

**Tech Tip**

The UCS E-Series procedures in this guide assume that you are using an ISR G2 2900 series router or ISR G2 3900 series router. The ISR 4451-X router procedure, while similar, is not included in this guide.

The Cisco UCS E-Series Server module has two internal interfaces on the router. These interfaces are numbered depending on which slot the UCS E-Series Server module is installed. Interface ucse_/0 represents a routed PCIe interface and interface ucse_/1 represents the multi-gigabit fabric (MGF) interface. This procedure configures the PCIe interface, which is also referred to as the Console interface.

### Option 1: Layer 2 access switch

This is the recommended configuration for remote sites with an access layer only. Use this configuration if all UCS E-Series Server applications and CIMC access can reside on the remote site user Data VLAN and a dedicated server subnet or DMZ is not required.

Perform these steps to set up the CIMC interface.

**Step 1:** Determine the UCS E-Series Server interfaces.

```
RS242-2951-2#sh ip int brief

Interface      IP-Address      OK?   Method Status     Protocol
Ucse2/0          unassigned    YES   NVRAM   up          up
Ucse2/1          unassigned    YES   unset   up          up
```

**Tech Tip**

This example shows the Cisco UCS E-Series Server module installed in slot 2 of the router.

**Step 2:** Assign an IP address to the router's UCS E-Series Server interface. In this configuration you use **IP unnumbered** to share the IP address assigned to the internal data VLAN. This will be the gateway IP address for the Cisco UCS E-Series Server CIMC and hypervisor.

```
interface ucse2/0
 ip unnumbered GigabitEthernet 0/2.64
 no shutdown
```

**Step 3:** Assign an IP address and gateway to the CIMC.

```
interface ucse2/0
 imc ip address 10.5.252.10 255.255.255.0 default-gateway 10.5.252.3
```

**Tech Tip**

If you have configured Hot Standby Router Protocol (HSRP), do not use the HSRP virtual IP address. Use the real IP address assigned to the interface or subinterface.

```
Configure the CIMC LAN on Motherboard (LOM) for shared access.
interface ucse2/0
imc access-port shared-lom console
```

**Tech Tip**

Shared console access allows this interface to be used for CIMC access and network traffic. Dedicated mode allows only CIMC access.

**Step 4:** Configure a static host route for the CIMC host via the internal UCS E-Series Server interface.

```
ip route 10.5.252.10 255.255.255.255 ucse2/0
```

**Step 5:** Configure an additional static host route for the VMware ESXi host that will reside on the same subnet and share the UCS E-Series Server console for access.

```
ip route 10.5.252.11 255.255.255.255 ucse2/0
```

**Step 6:** If this is a dual router remote site, you must redistribute the static routes created in Step 4 and Step 5 into the LAN EIGRP process (Example: EIGRP-100). You use a route map with an access list to explicitly list which static routes are redistributed.

If static route redistribution has already been configured, then the route map may already exist and you can use it in a redistribute statement. In this case, add the new access list and the additional clause for the route map; otherwise, complete the entire step. The highlighted portion is optional.

```
ip access-list standard STATIC-ROUTE-LIST
 remark UCSE CIMC & ESXi host routes
 permit 10.5.252.10
 permit 10.5.252.11

route-map STATIC-IN permit 30
 match ip address STATIC-ROUTE-LIST
!
router eigrp 100
 redistribute static route-map STATIC-IN
```

Next, verify the CIMC configuration.

## Tech Tip

It is not always necessary to redistribute these static routes into the LAN EIGRP process.

```
ip route 10.5.252.10 255.255.255.255 ucse2/0
ip route 10.5.252.10 255.255.255.255 ucse2/0
```

This type of static route is known as a *pseudo-static* or *pseudo-connected* route because it meets two conditions:

1) the static route points directly to an interface and 2) the destination IP address is contained within an IP range that is referenced by an EIGRP network statement:

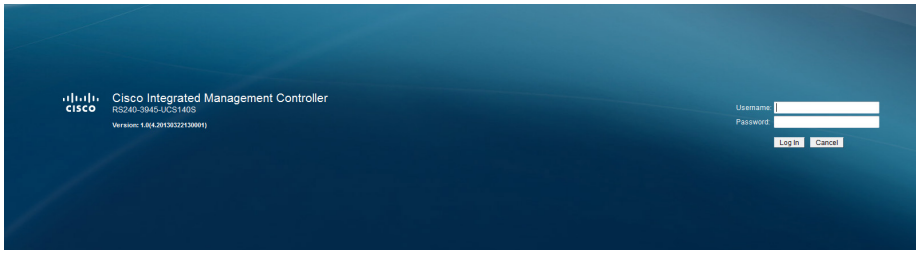
```
router eigrp 100 network 10.5.0.0 0.0.255.255
```

A pseudo-connected route is treated like a connected route and is automatically advertised within the EIGRP autonomous system as an EIGRP internal route (AD 90) and no redistribution is required.

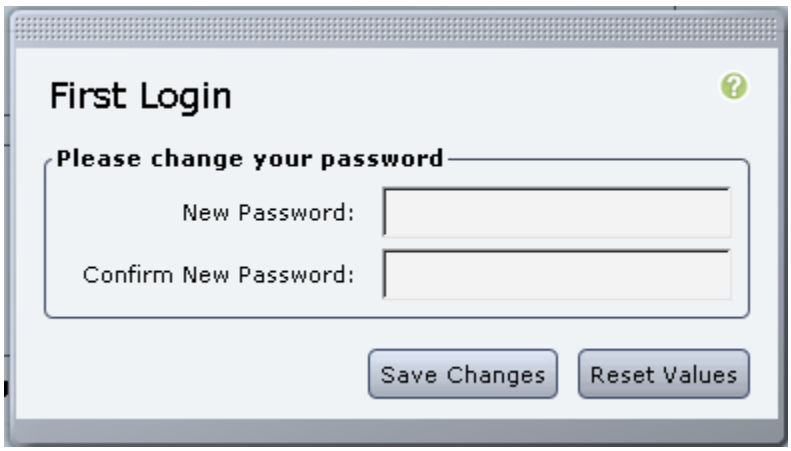
While the route will be automatically brought into the topology and treated similar to a connected route, EIGRP does not reclassify the route as a connected.

As with the example presented above, redistribution of static routes, and then applying configuration commands (such as route maps) to the redistribute routes would affect these routes.

**Step 7:** Open a browser window to the CIMC address (Example: https://10.5.252.10), enter the factory default username **admin** and factory default password **password**, and then click **Log In**.




**Step 8:** If this is the first time you log in to this device, you are prompted to change the password. Enter a new password (Example: c1sco123), and then click **Save Changes**.




## Option 2: Layer 3 distribution switch—dedicated UCS E-Series Server subnet

This is the recommended configuration for remote sites with a distribution layer.

This solution also provides flexibility for different application needs, such as the ability to contain certain applications in a local DMZ for each remote-site location.

When connecting to the distribution layer you must assign a dedicated subnet range for Cisco UCS E-Series Server management. The CIMC and ESXi interfaces are both assigned addresses in this range. The external UCS E-Series Server interfaces are connected to the LAN switches providing application access to internal facing VLANs and the Internet.

Perform these steps to set up the CIMC interface.

**Step 1:** Determine the UCS E-Series Server interfaces.

```
RS240-3945#sh ip int brief

Interface      IP-Address      OK?   Method Status    Protocol
ucse3/0          unassigned    YES   NVRAM   up          up
ucse3/1          unassigned    YES   unset   up          up
```

**Tech Tip**

This example shows the Cisco UCS E-Series Server module installed in slot 3 of the router.

**Step 2:** Assign an IP address to the router's UCS E-Series Server interface. In this configuration you explicitly assign an IP address on the newly assigned subnet range. This will be the gateway IP address for the Cisco UCS E-Series Server CIMC and hypervisor.

```
interface ucse3/0
 ip address 10.5.241.1 255.255.255.128
```

**Step 3:** Assign an IP address and gateway to the CIMC.

```
interface ucse3/0
 imc ip address 10.5.241.30 255.255.255.128 default-gateway 10.5.241.1
```

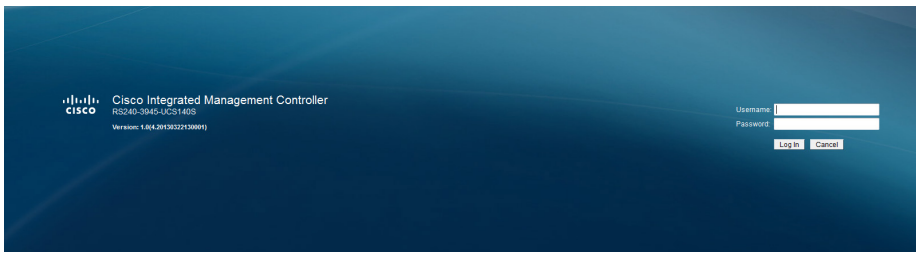
**Step 4:** Configure the CIMC LOM for shared access.

```
interface ucse3/0
 imc access-port shared-lom console
 no shutdown
```

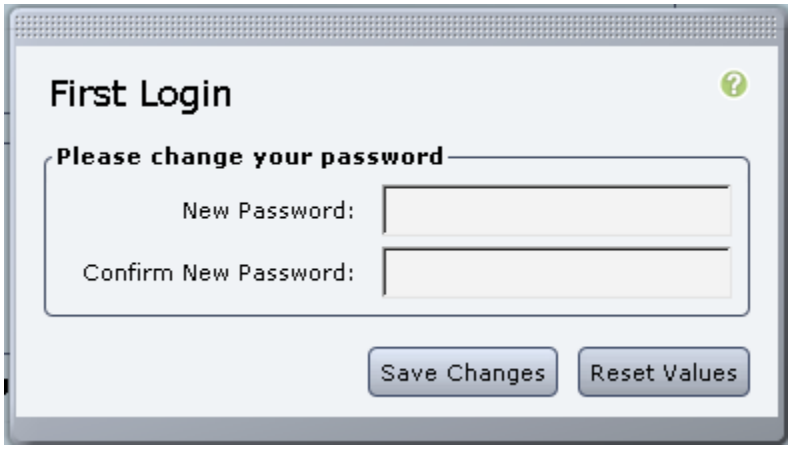
**Tech Tip**

Shared console access allows this interface to be used for CIMC access and network traffic. Dedicated mode allows only CIMC access.

**Step 5:** Open a browser window to the CIMC address (Example: https://10.5.241.30), enter the factory default username **admin** and factory default password **password**, and then click **Log In**.



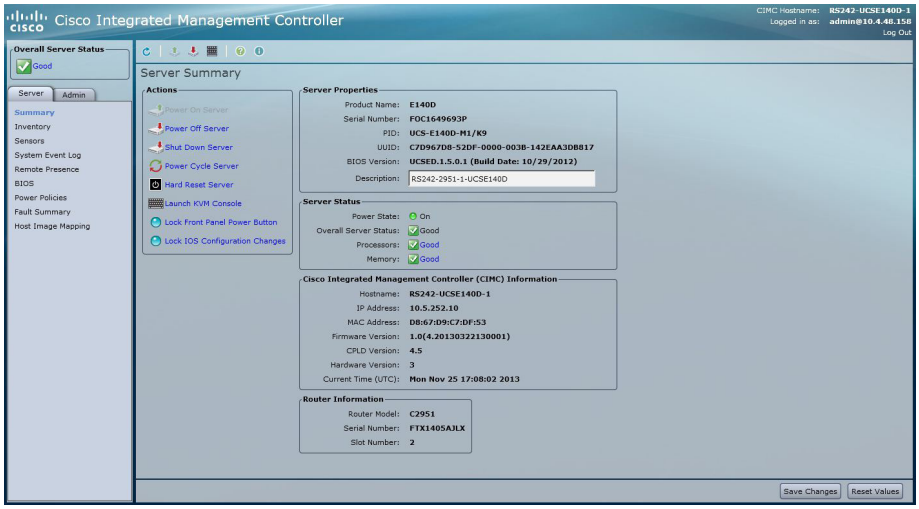
**Step 6:** If this is the first time you log in to this device, you are prompted to change the password. Enter a new password (Example: c1sco123), and then click **Save Changes**.




## Procedure 3 Configure UCS E-Series Server using CIMC

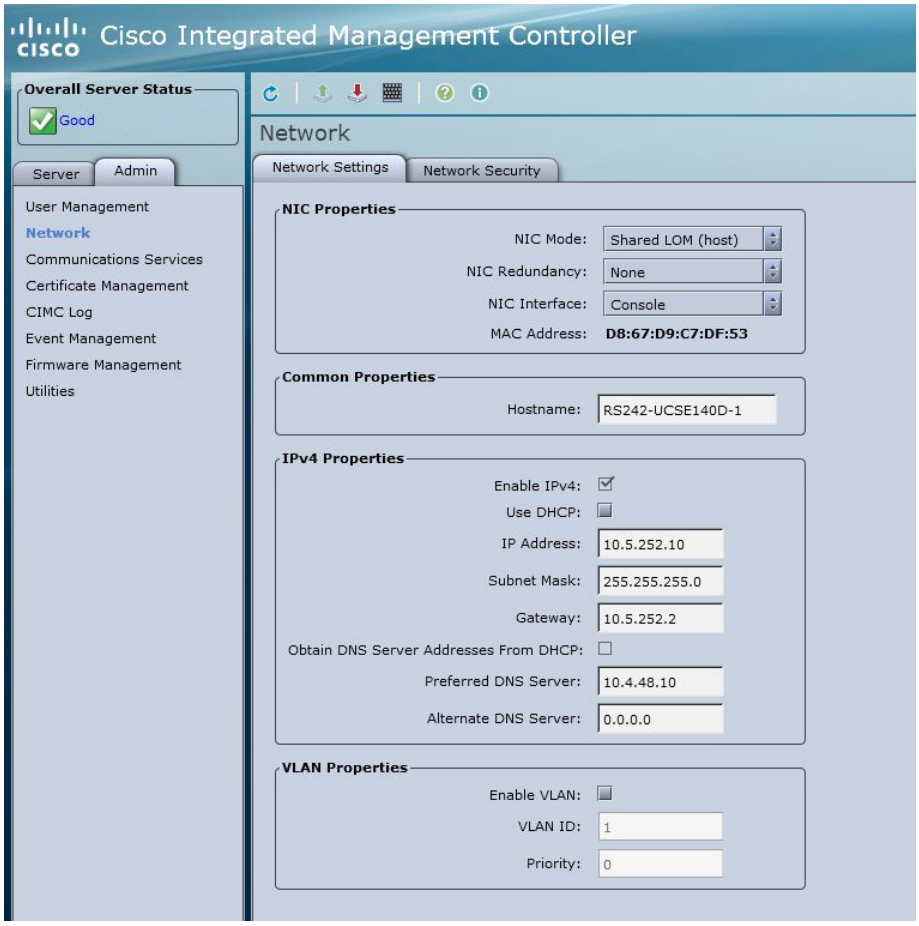
**Step 1:** On the Server Summary screen, verify the installed CPU and, if the memory and disk are correctly reported, that the correct versions of CIMC and BIOS are installed.

**Step 2:** Enter a description for this device (Example: RS242 UCS E-Series), and click then **Save Changes**.



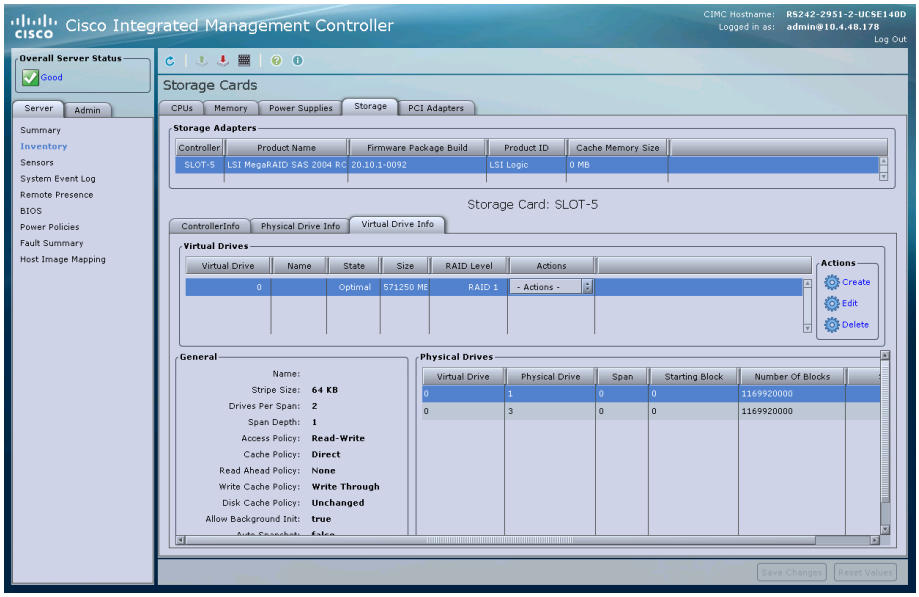

**Step 3:** Click the **Admin** tab, click **Network**, and then click the **Network Settings** tab.

**Step 4:** Configure a host name (Example: RS242-UCSE140D and the primary DNS server if necessary (Example: 10.4.48.10), click **Save Changes**, and then, on the warning dialog box, click **OK**.



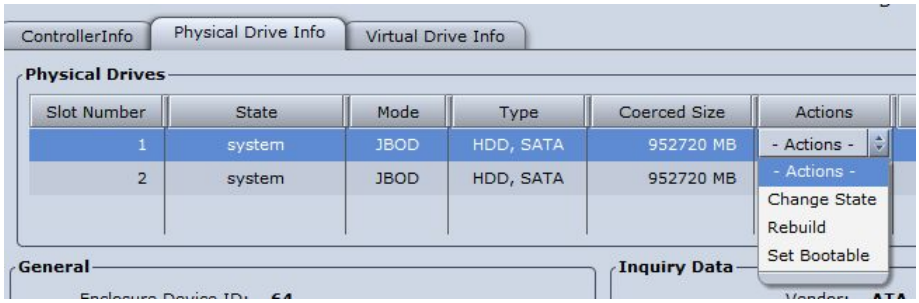
## Procedure 4 Configure RAID using CIMC

**Step 1:** Click the **Server** tab, click **Inventory**, and then click the **Storage** tab.




**Step 2:** Click the **Physical Drives Info** tab.

**Step 3:** For the drive in Slot Number 1, click **Actions**, and then choose **Change State**.




**Step 4:** If necessary, for the Physical Drive State, choose **UnconfiguredGood**, and then click **Confirm**.

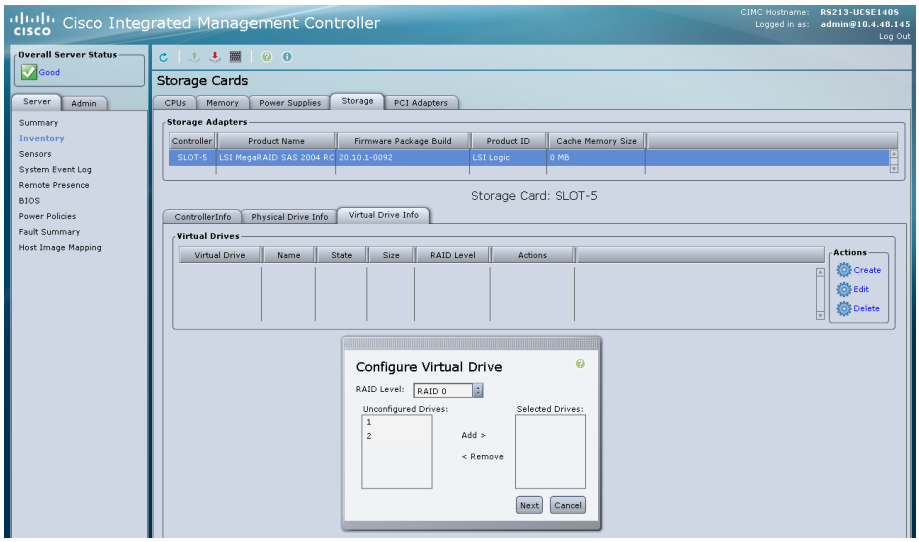

**Step 5:** If necessary, repeat Step 3 and Step 4 for the remaining drives.

**Step 6:** Click the **Virtual Drive Info** tab.

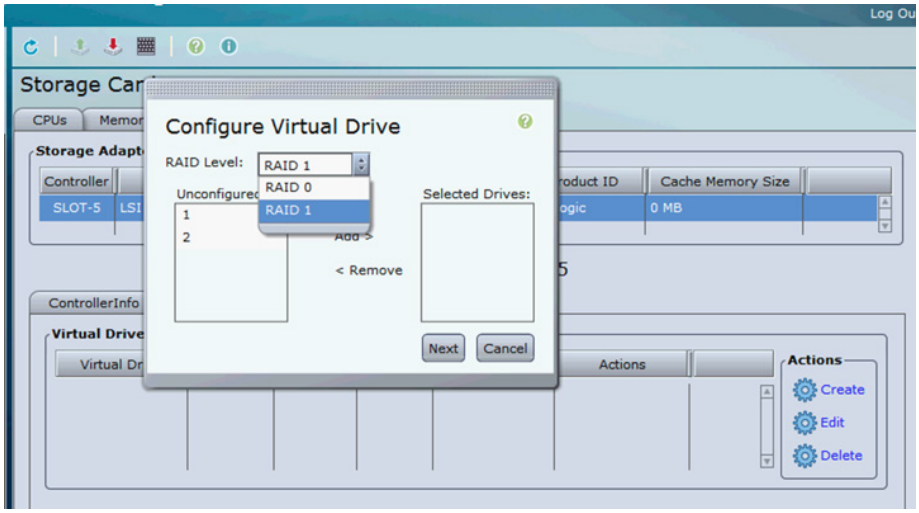
**Step 7:** In the **Actions** pane, choose **Create**.

### Tech Tip

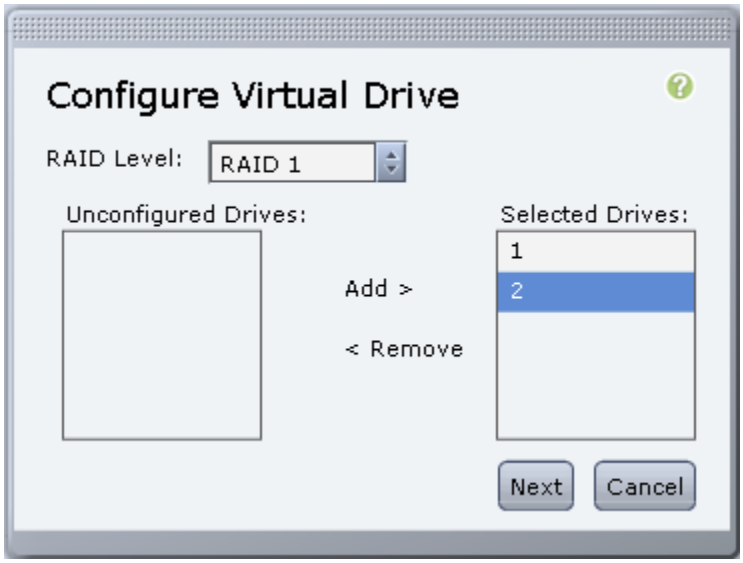
If you are configuring a Cisco UCS E-Series Server module with a single hard drive you can select RAID 0 and add the single drive to the list. It is best to use two drives when possible.



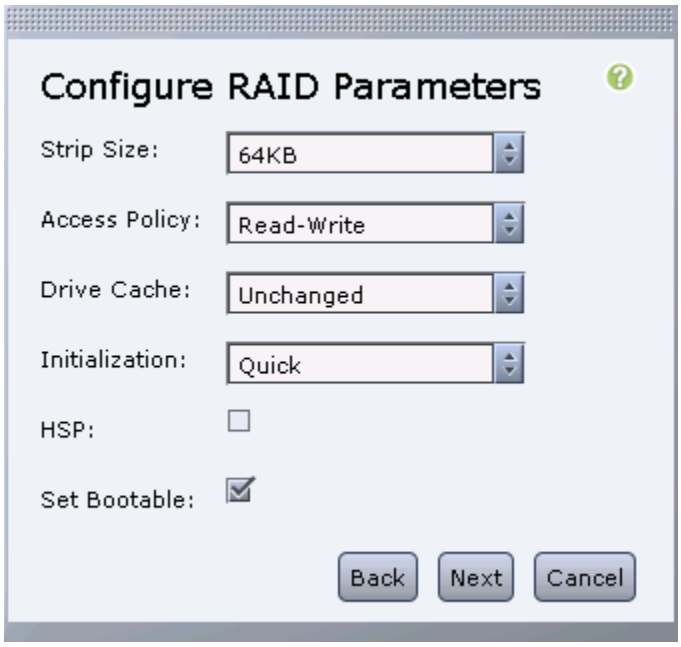

**Step 8:** In the Configure Virtual Drive dialog box, choose RAID Level **RAID 1** from the drop-down list. If your system only has a single drive, choose RAID Level **RAID 0** (this will be the only available option).



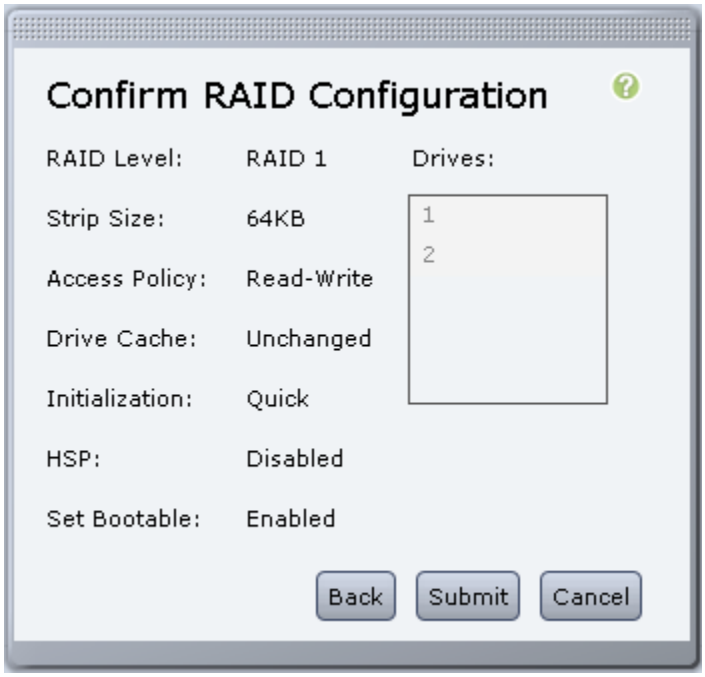
**Step 9:** Select the drives you want to include in the RAID configuration, move them from the **Unconfigured Drives** column to the **Selected Drives** column by clicking **Add**, and then, after you finish selecting all the drives click **Next**.



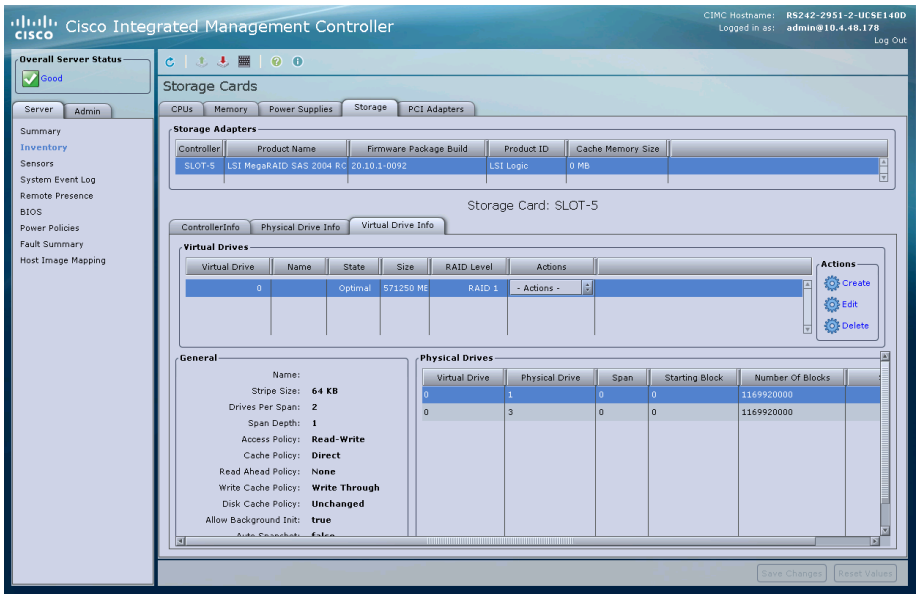

**Step 10:** In the Configure Raid Parameters dialog box, select **Set Bootable**, and then click **Next**.



**Step 11:** In the Confirm RAID Configuration dialog box, verify that the proper drives are listed, and then click **Submit**.




**Step 12:** Verify that the virtual and physical drives are properly assigned by clicking the **Server** tab, clicking **Inventory**, clicking the **Storage** tab, and then clicking the **Virtual Drive Info** tab.



PROCESS

## Installing VMware ESXi on the UCS E-Series Server Module

1. Download the VMware ESXi image specific to the UCS E-Series Server
2. Install VMware ESXi on the UCS E-Series Server
3. Configure VMware ESXi Host Settings
4. Add VMware ESXi host to vCenter
5. Add a datastore to ESXi hosts
6. Configure networking for ESXi host
7. Configure ESXi NIC teaming for resiliency

Use this process if your UCS E-Series Server module did not come with VMware ESXi pre-installed.

To avoid WAN utilization and possible congestion problems on your network, if possible you should install ESXi on the UCS E-Series Server modules before shipping them to remote locations.

### Tech Tip

If you are using VMware FL-SRE-V-HOST license (equivalent to VMware vSphere Hypervisor 5.X), make sure that the installed UCS E-Series Server RAM is 32GB or less. If the installed UCS E-Series Server RAM is more than 32GB, an error message appears and you cannot apply the license.

If you want to use 48GB RAM on the UCS E-Series Server, upgrade your license to FL-SRE-V-HOSTVC. You can verify the memory configuration prior to installing VMware ESXi by navigating to the **Server** tab, clicking **Inventory**, and then clicking the **Memory** tab.

### Procedure 1 Download the VMware ESXi image specific to the UCS E-Series Server

A custom version of VMware ESXi has been developed specifically for use on Cisco UCS E-Series Servers. Use the following steps to download the custom ISO image.

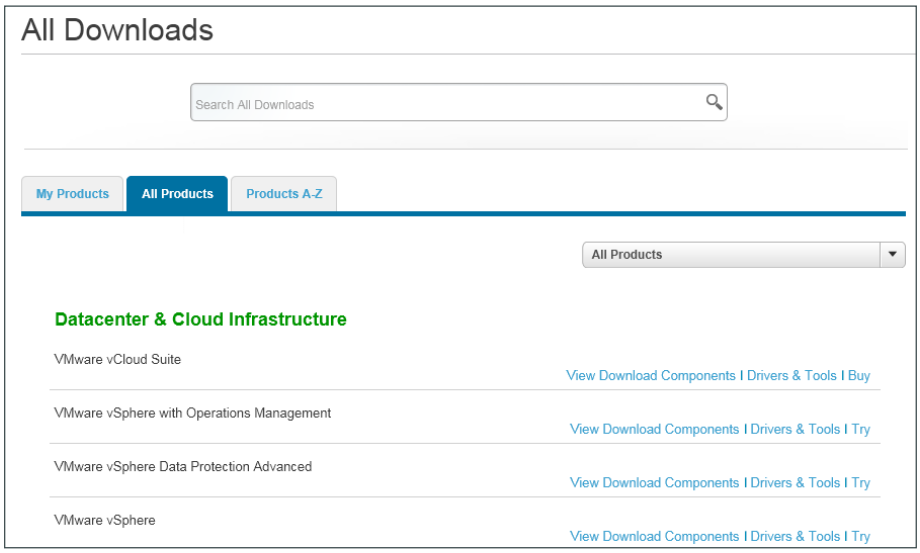
**Step 1:** Open a browser and navigate to the VMware login page:

https://my.vmware.com/web/vmware/login

**Step 2:** Enter your VMware credentials, and then click **Log In**. If you do not have an account with VMware, create an account by clicking **Register**.

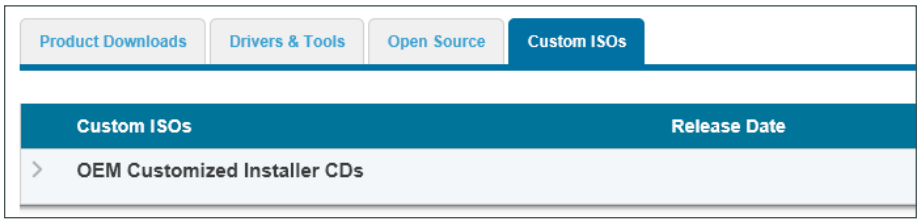
**Step 3:** Click **All Downloads**.

Step 4: Click the **All Products** tab and then click **View Download Components** for **VMware vSphere**.

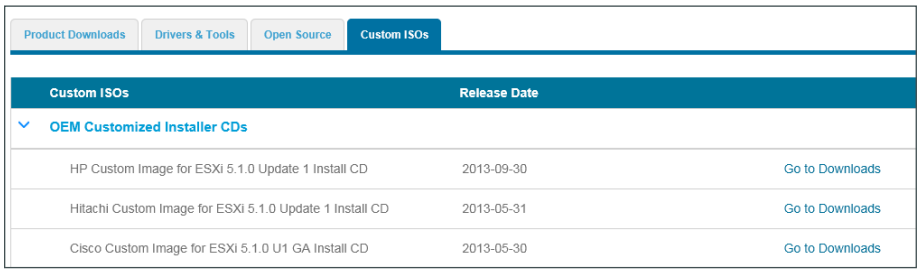



Step 5: Select version **5.1** in the **Select Version:** drop-down list.

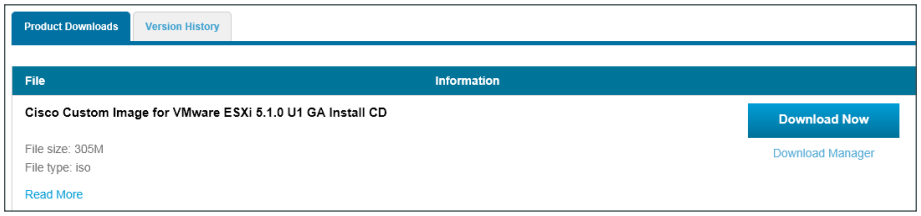

Step 6: Click the **Custom ISOs** tab, and then click the right arrow to expand the **OEM Customized Installer CDs**.




Step 7: For the **Cisco Custom Image for ESXi 5.1.0 U1 GA Install CD**, click **Go to Downloads**.



**Step 8:** To download the customized VMware vSphere Hypervisor image, click the **Product Downloads** tab, for the **File type: iso** version click **Download Now**.




## Procedure 2 Install VMware ESXi on the UCS E-Series Server

This procedure takes you through several important tasks: mounting the VMware ESXi ISO, setting the UCS E-Series Server Boot settings, and installing VMware ESXi onto the SD card of the UCS E-Series Server. It is important to keep both the CIMC and KVM console windows open throughout these steps.

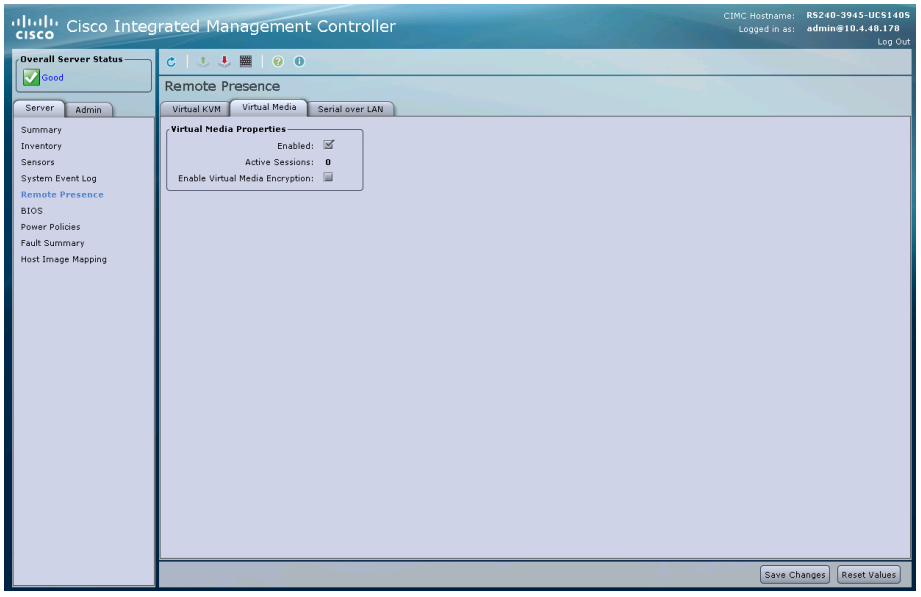
### Tech Tip

Installing the hypervisor onto the internal SD card of the ESXi server allows us to maintain separation and dedicate the internal RAID drives to the virtual machines loaded onto the server.

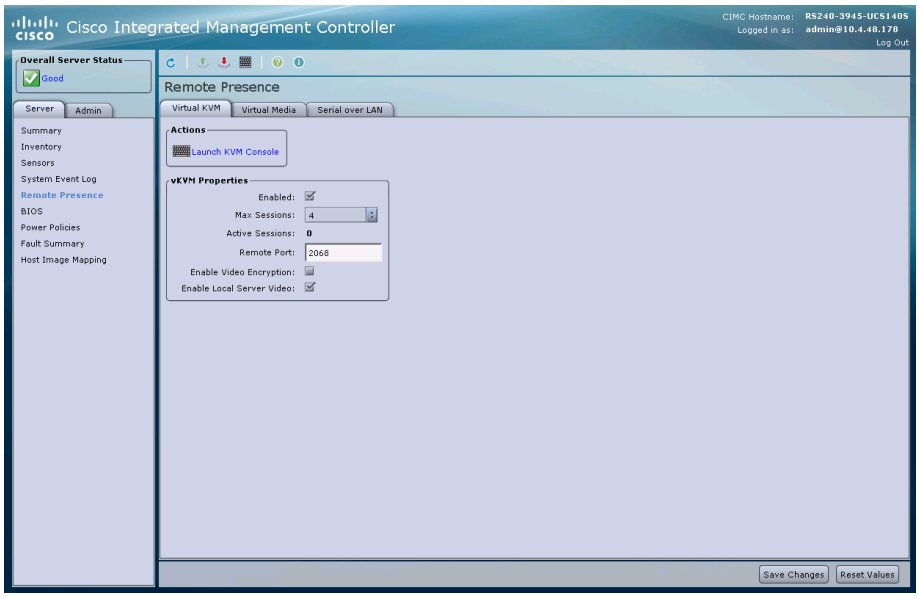
**Step 1:** Using your web browser, navigate to the CIMC address of the UCS E-Series Server module and log in (Examples: https://10.5.252.10 and admin/c1sco123).

**Step 2:** Accept any messages regarding untrusted certificates.

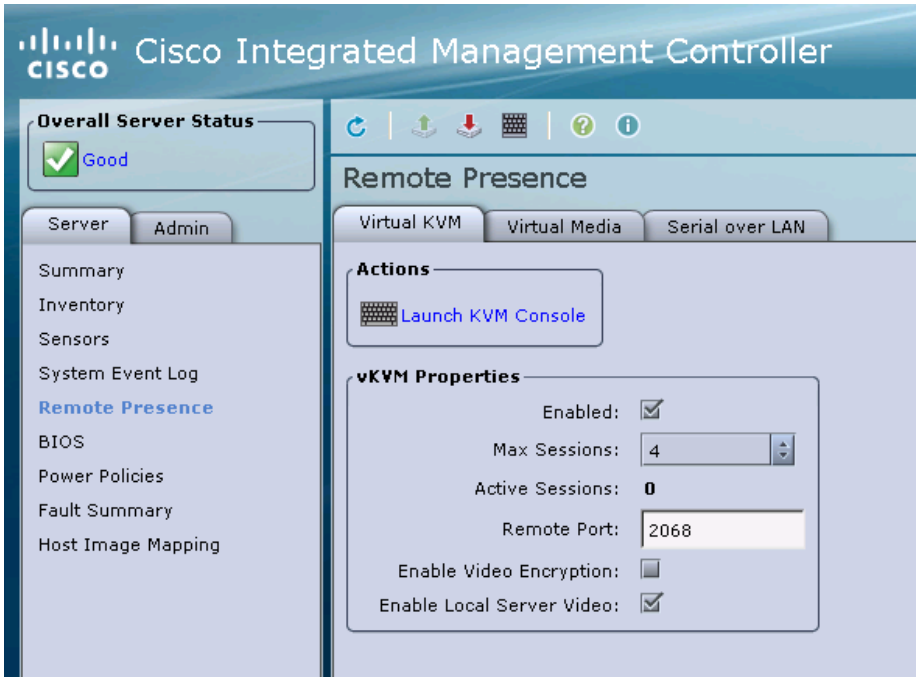
**Step 3:** In the **Server** tab, click **Remote Presence**, click the **Virtual Media** tab, and then ensure the **Enabled** check box is selected.



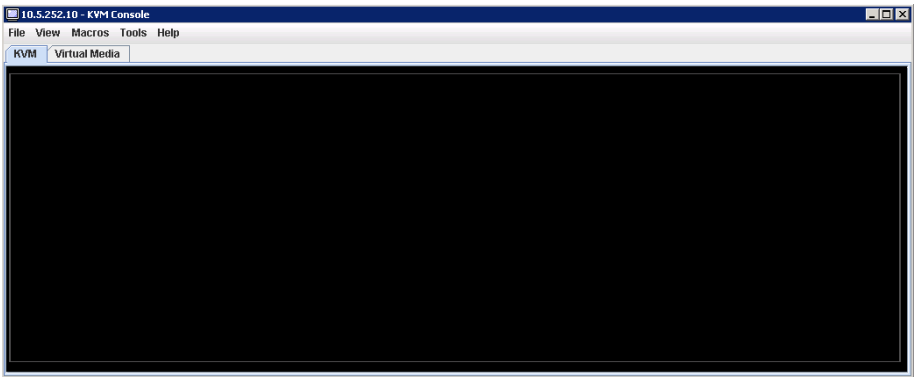
**Step 4:** Click the **Virtual KVM** tab, and then ensure the **Enabled** check box is selected.



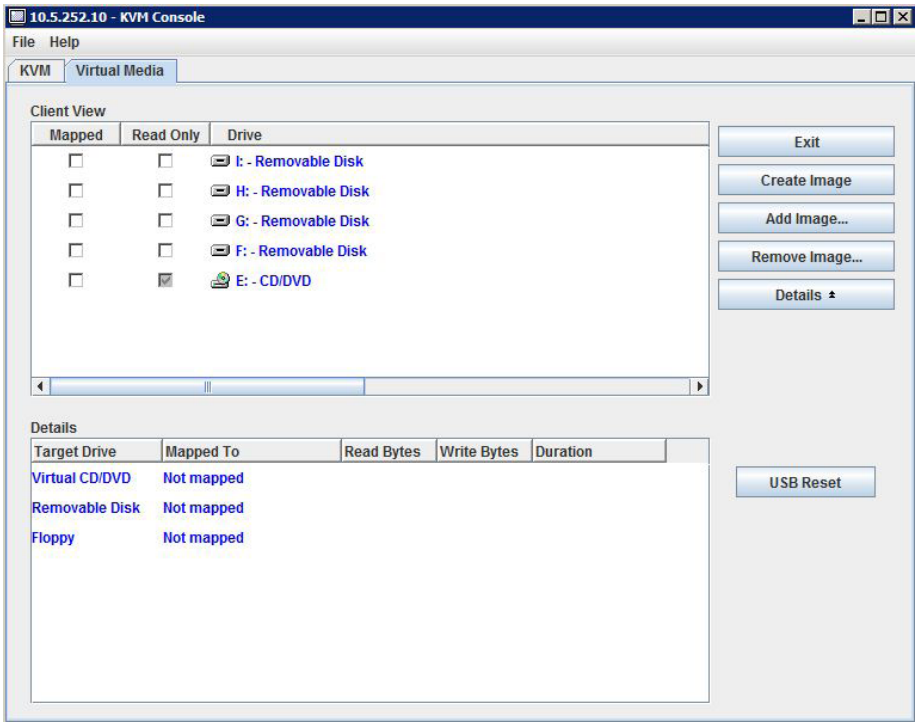

**Step 5:** On the **Virtual KVM** tab, under **Actions** click **Launch KVM Console**, and then accept any security warnings. The virtual KVM Console window opens.



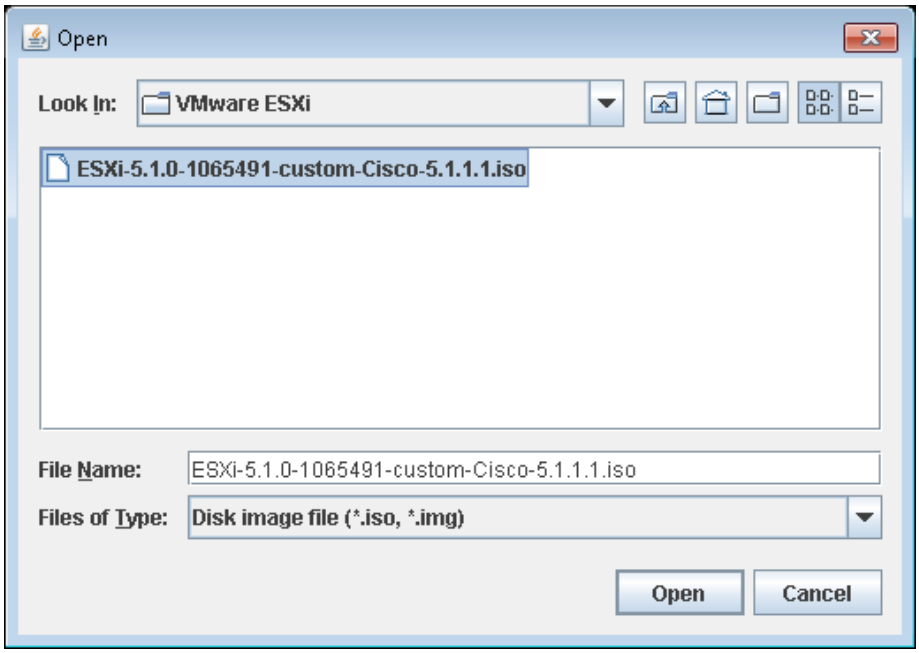
Step 6: In the KVM Console window, click the **Virtual Media** tab.



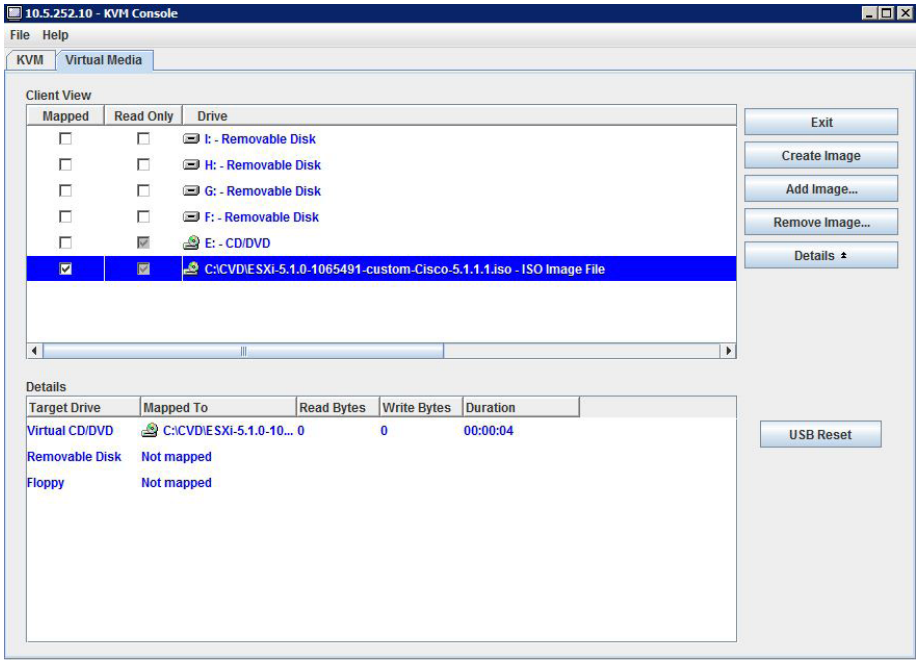

Step 7: In the KVM Console window, click **Add Image**.



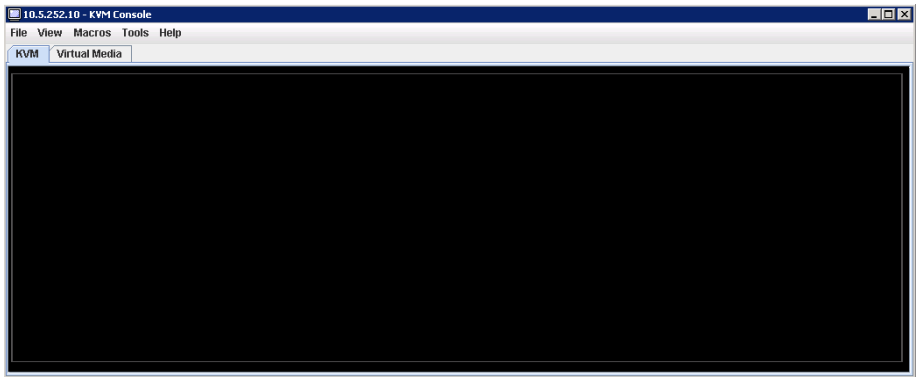
**Step 8:** Browse to the VMware ESXi ISO image, and then click **Open**.



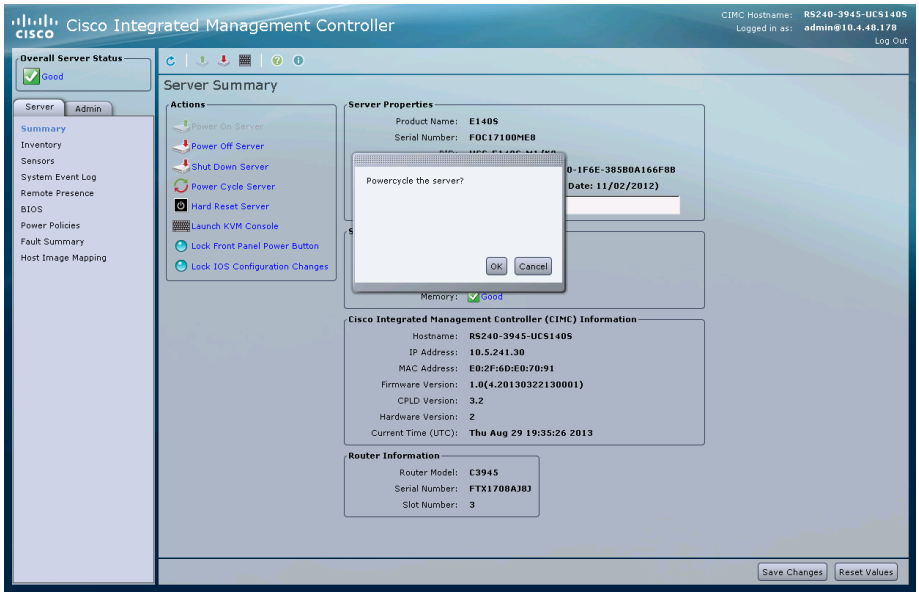

**Step 9:** For the newly added image, select **Mapped**. This maps the ISO file and completes the mount.



**Step 10:** Return to the KVM Console window by clicking the **KVM** tab. You can monitor the status of the server by using this console window. Keep this window open and visible.

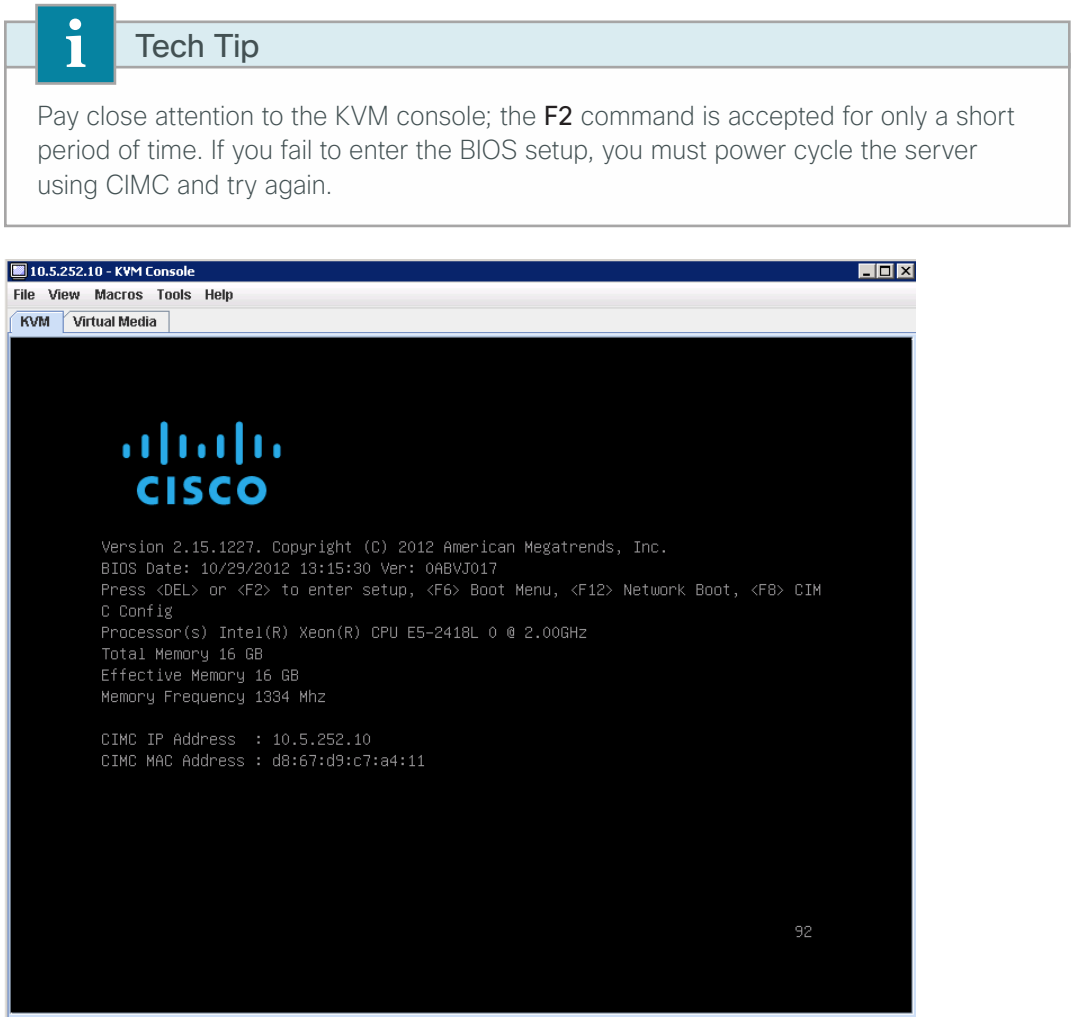



**Step 11:** In the CIMC, click the **Server** tab, click **Summary**, reboot the server by clicking **Power Cycle Server**, and then click **OK** in the warning dialog box. The console screen turns blank and green for a moment during this process.

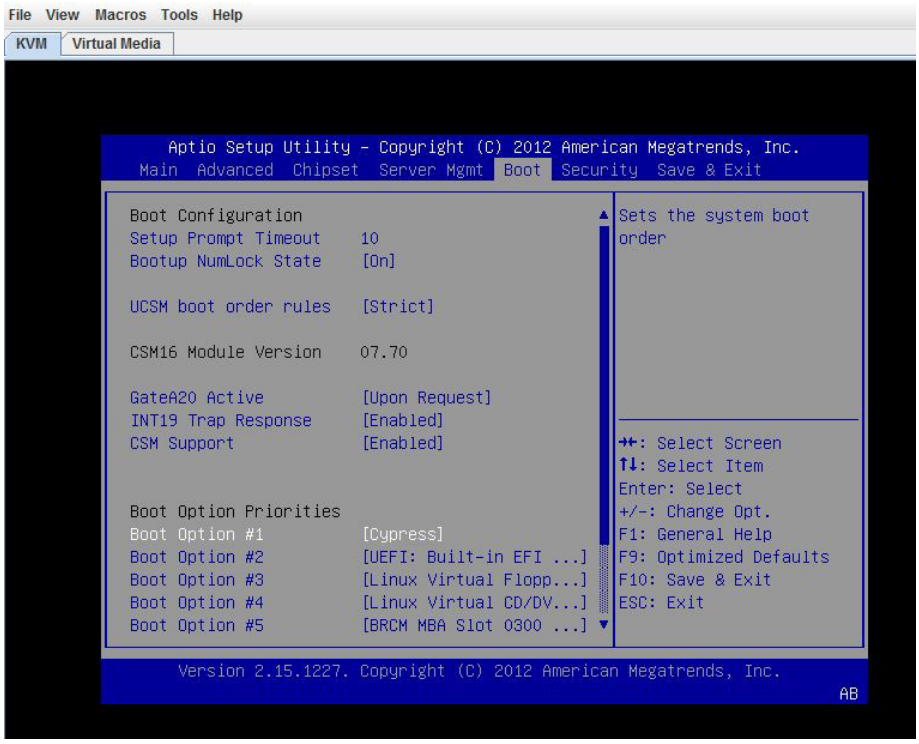



**Step 12:** Monitor the KVM Console window as the server boots, and, when prompted, enter the BIOS setup by pressing **F2**.

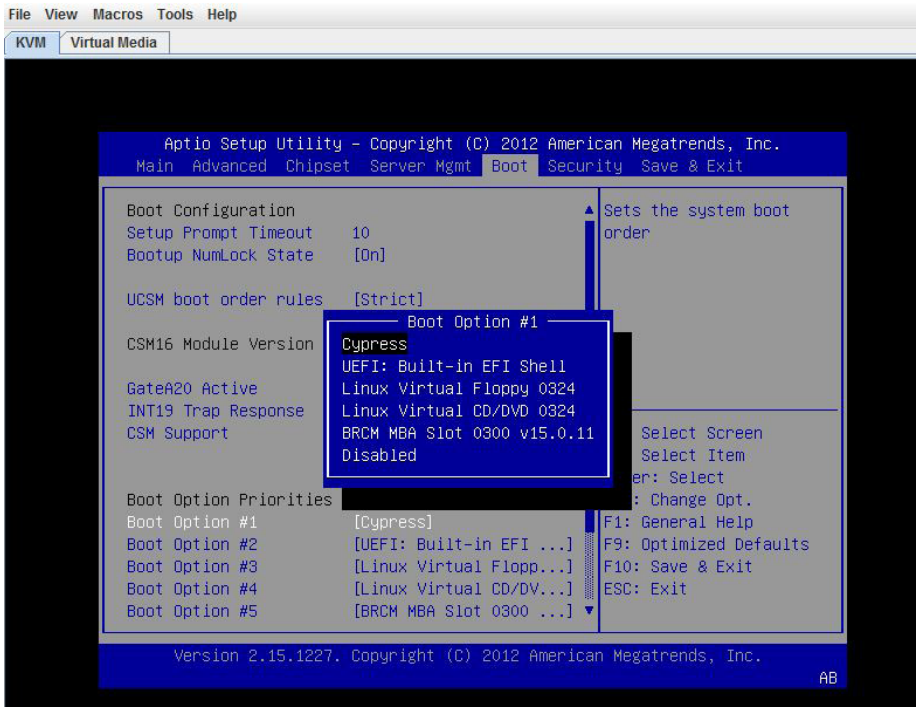
**Step 13:** When prompted, enter the password (Example: c1sco123). If this is the first time entering the BIOS, you are prompted to set a BIOS password (Example: c1sco123).



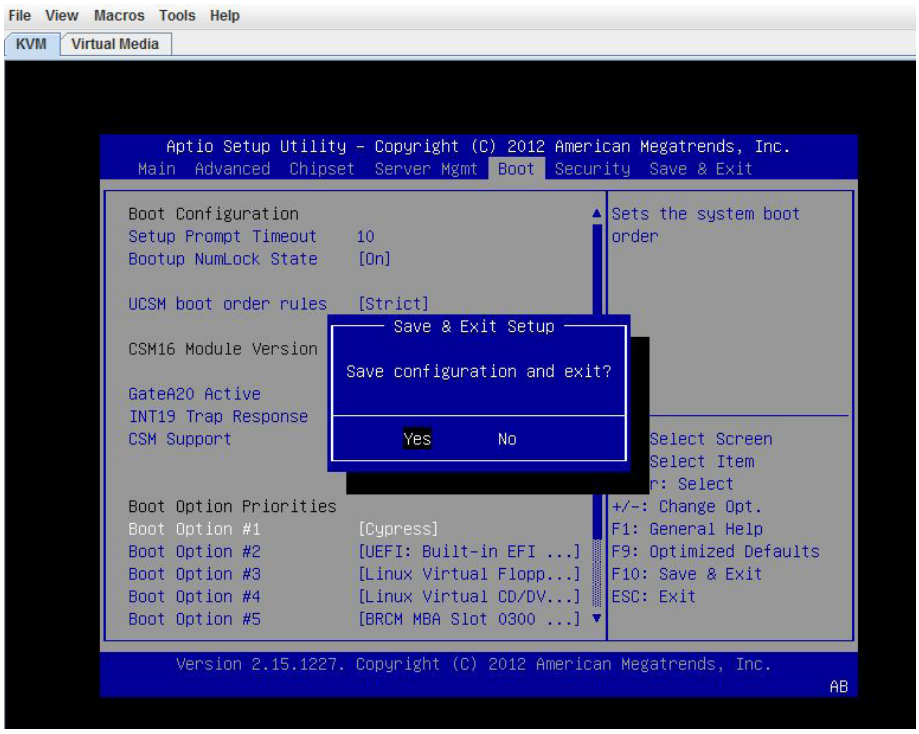
**Step 14:** Using the arrows on your keyboard, navigate to the **Boot** tab, highlight **Boot Option #1**, and then press **Enter**.




**Step 15:** In the Boot Option #1 dialog box, choose **Cypress**, and then press **Enter**.

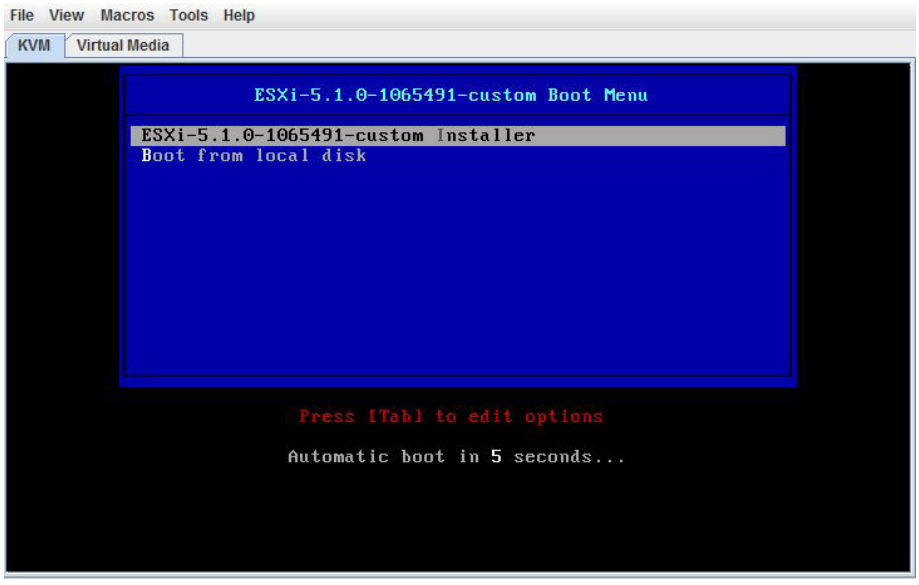


**Step 16:** Press **F10**. In the save and exit dialog box, choose **Yes,** and then press **Enter**. This saves the BIOS settings and exits BIOS. The system reboots.

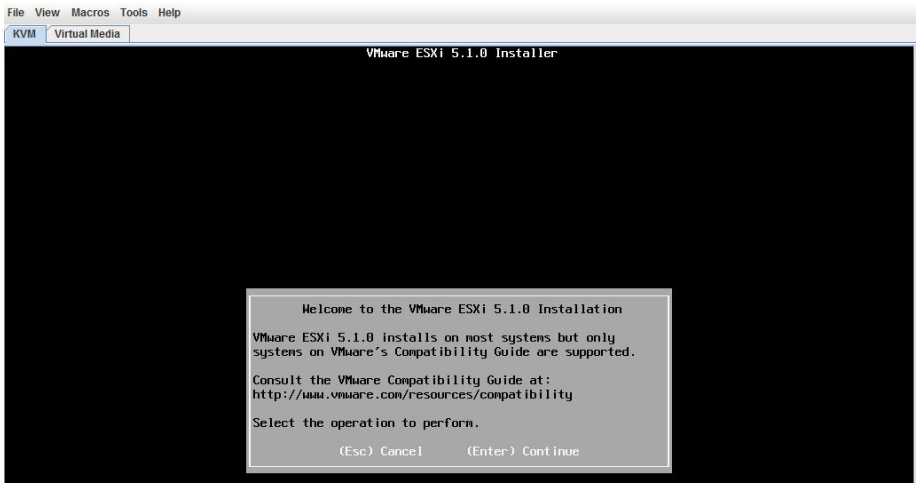



**Step 17:** In the virtual KVM window, click the **KVM** tab, and then monitor the KVM Console window as the server boots. The server loads the ESXi Installer from the mapped ISO image.

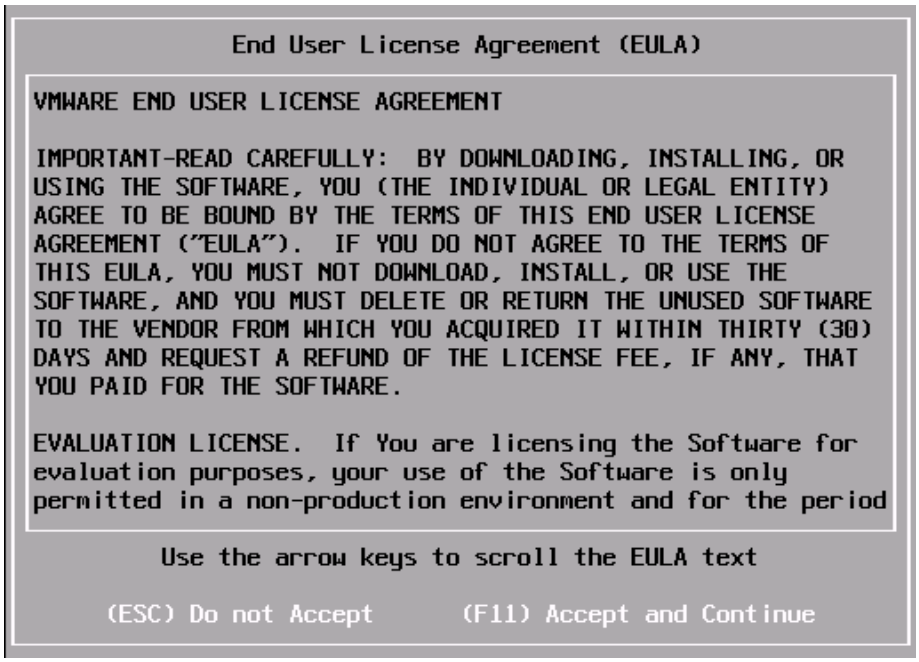
**Step 18:** When the VMware VMvisor Boot Menu appears, select **ESXi Installer**



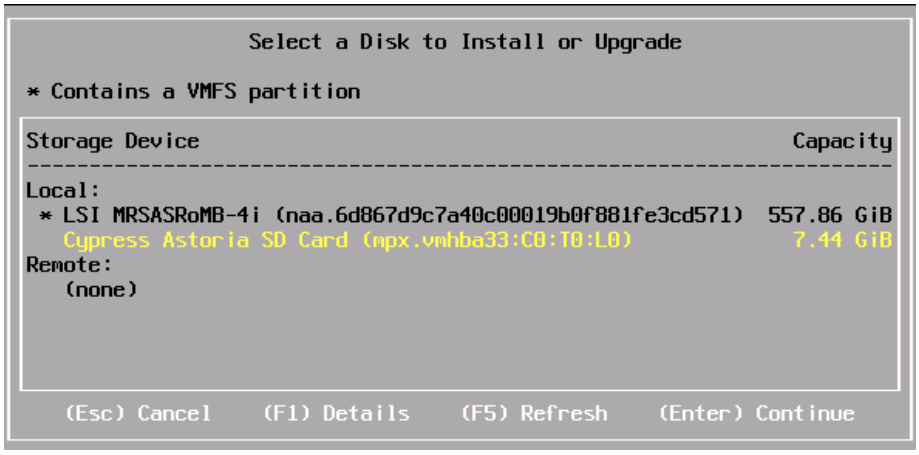
**Step 19:** In the Welcome dialog box, choose **Enter**. The installation of ESXi begins.




**Step 20:** Accept the End User License Agreement (EULA) by pressing **F11.**

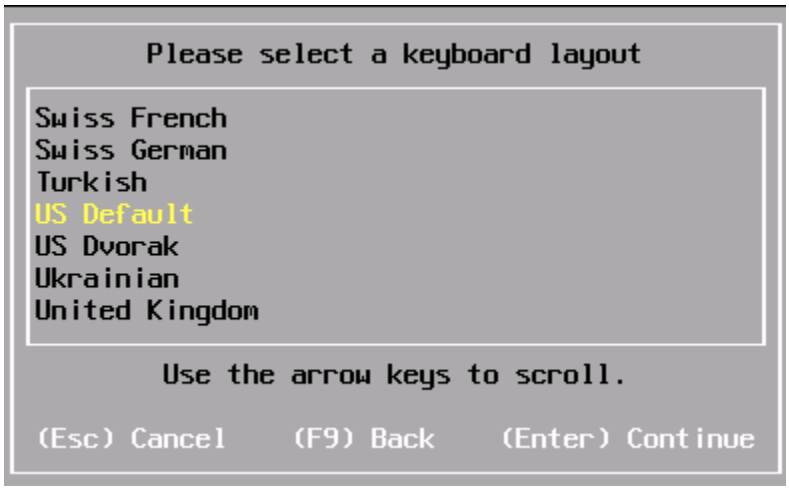


**Step 21:** Using the down arrow, choose the SD card as the local storage device, press **Enter** (Example: Cypress Astoria SD Card), and then when prompted to confirm disk selection, press **Enter**.



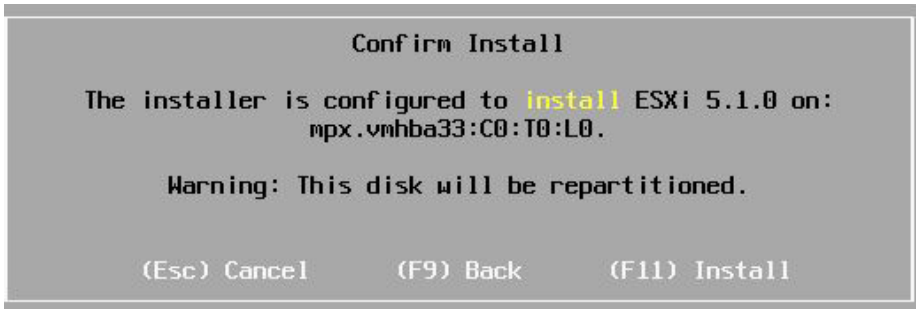


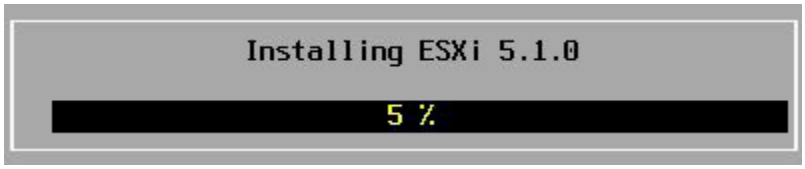
**Step 22:** For the keyboard layout, choose **US Default**, and then press **Enter**.



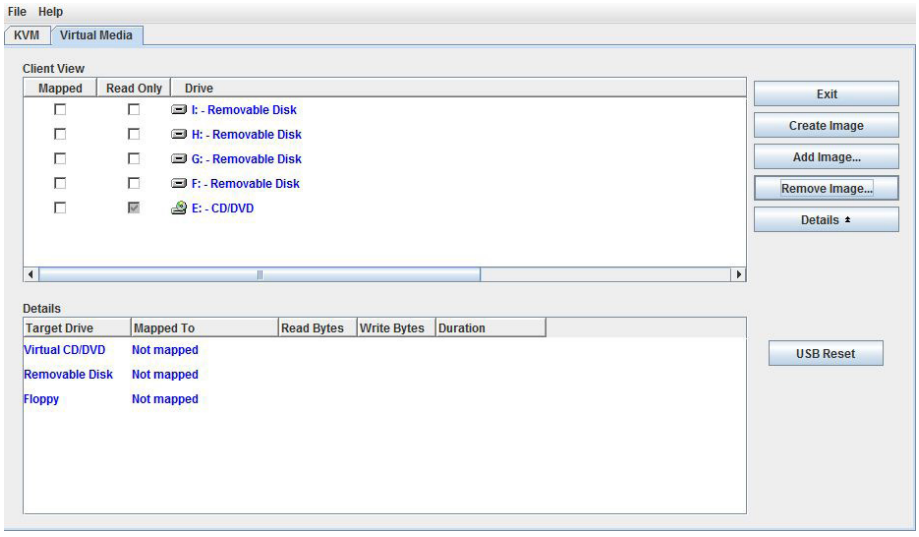
**Step 23:** Set the root password, and then press **Enter** (Example: c1sco123).


**Step 24:** The system scans for resources, which may take a few moments. Press **F11**. A status bar shows the progress of the ESXi installation.

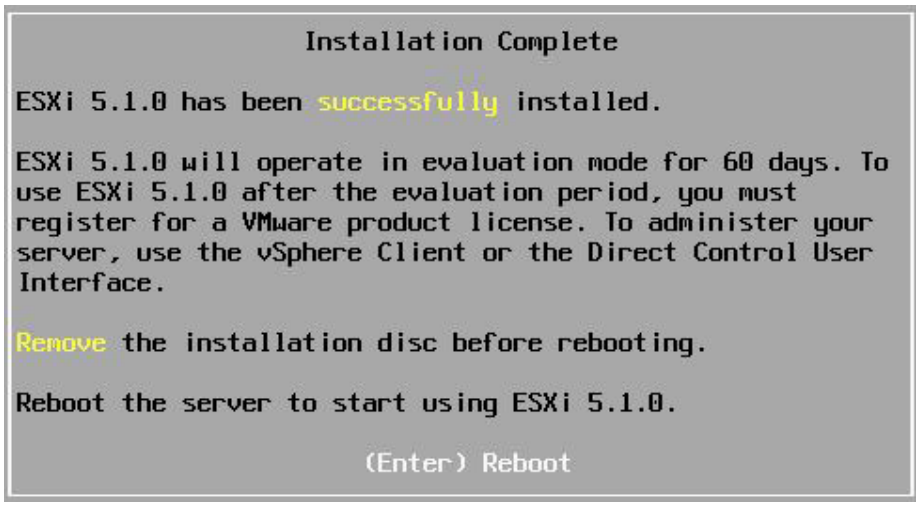



**Step 25:** After a successful installation of ESXi, in the **KVM Console** window, click the **Virtual Media** tab, click **Remove Image**, and agree to the warning. This unmounts the image.

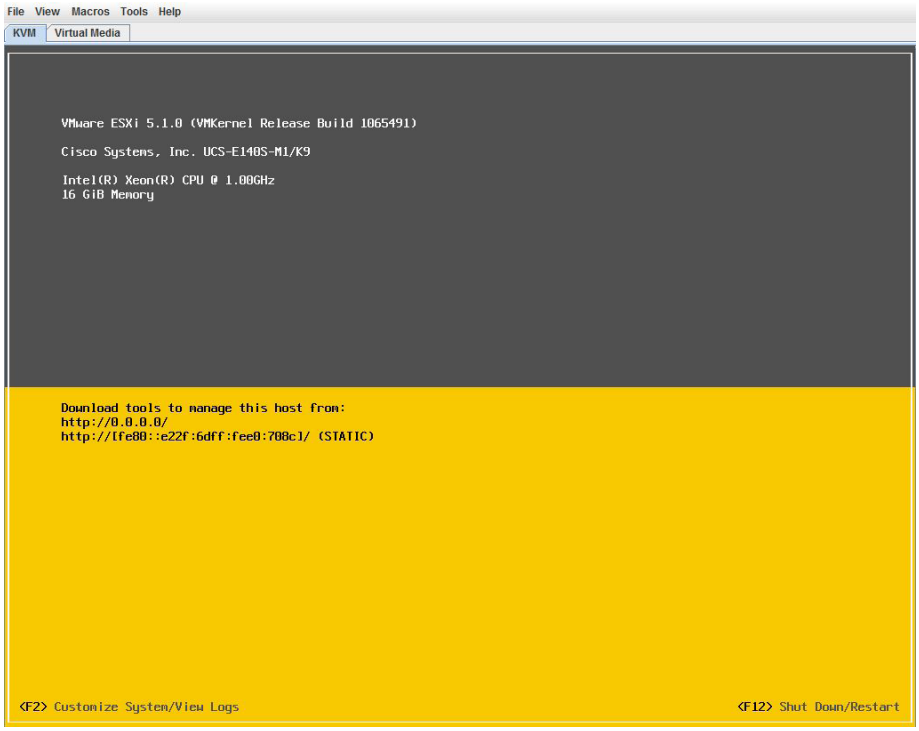


**Step 26:** On the **KVM** tab, press **Enter**. The system restarts, loading the ESXi image installed on the SD drive.

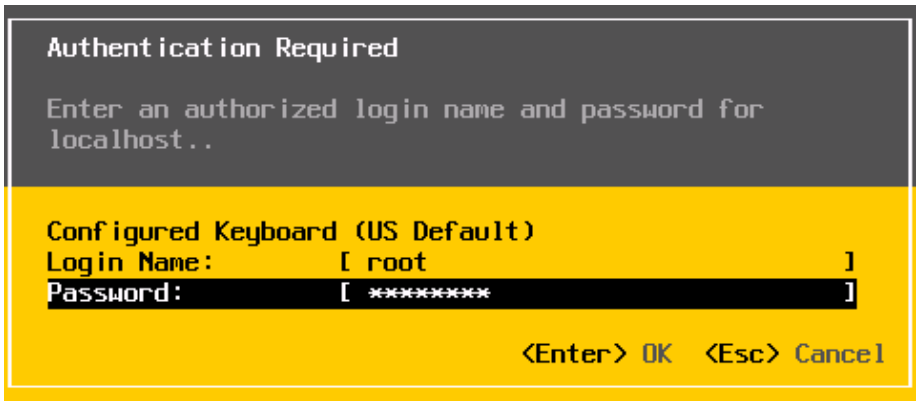



## Procedure 3 Configure VMware ESXi Host Settings

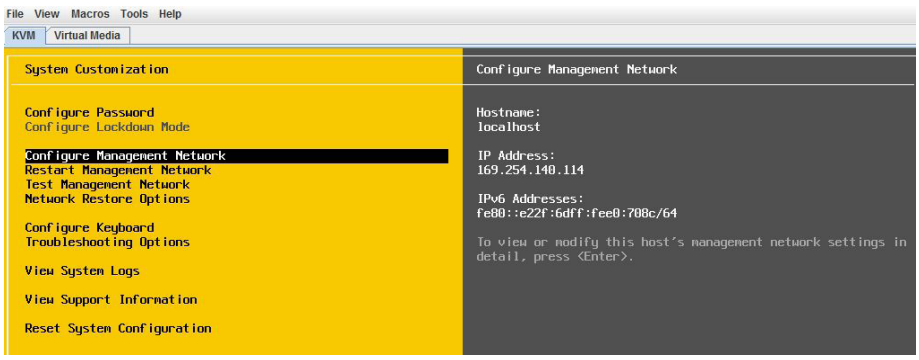
**Step 1:** In the **ESXi home screen window**, press **F2**. This enables you to customize the system after ESXi is finished booting.



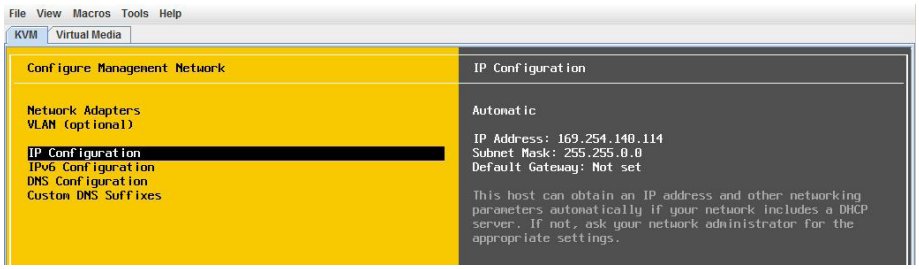
**Step 2:** Log in using the credentials you set during installation (Example: root/c1sco123).




**Step 3:** Using the down arrow key, highlight to the **Configure Management Network** option, and then press **Enter**.

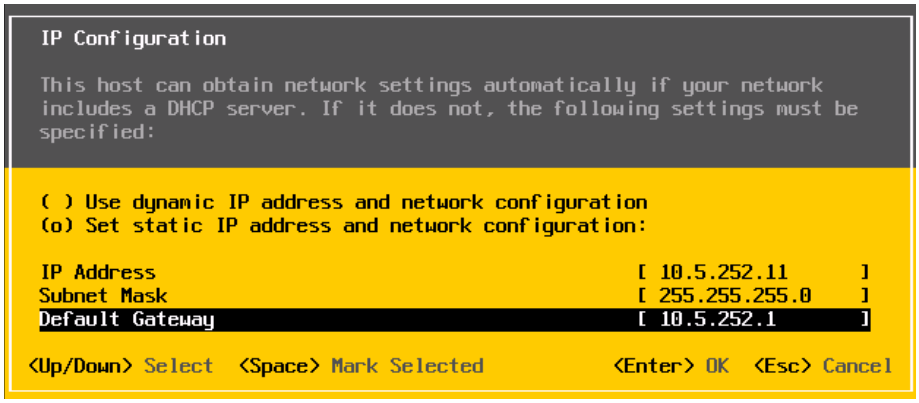



**Step 4:** Choose **IP Configuration**, and then press **Enter**.

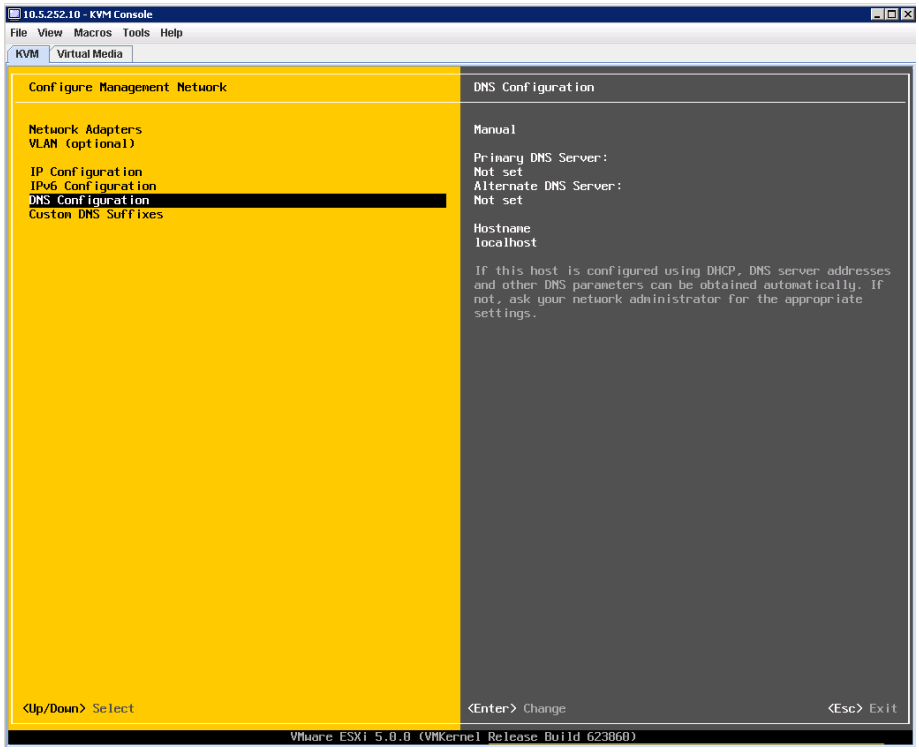



**Step 5:** Highlight **Set static IP address and network configuration**, and select it by pressing the space bar.

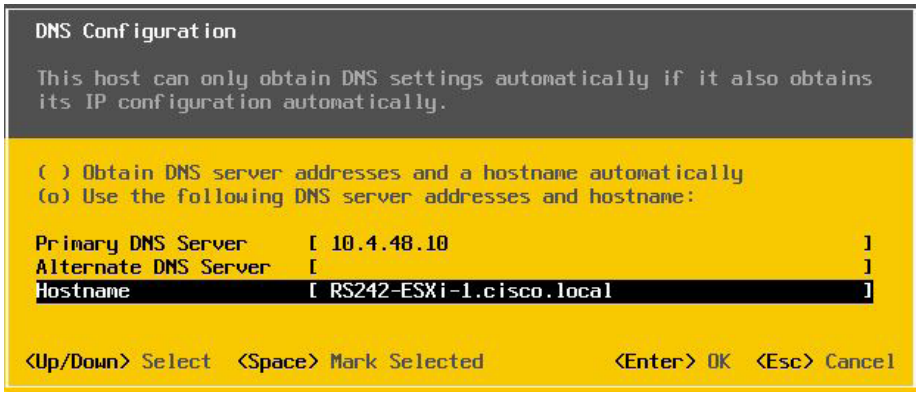
**Step 6:** Using the down arrow, enter the assigned values from Table 2 (Example:10.5.252.11, 255.255.255.0, 10.5.252.1) for **IP address**, **subnet mask**, and **default gateway**, and then press **Enter**.




**Step 7:** Use the down arrow, select **DNS Configuration**, and then press **Enter**.

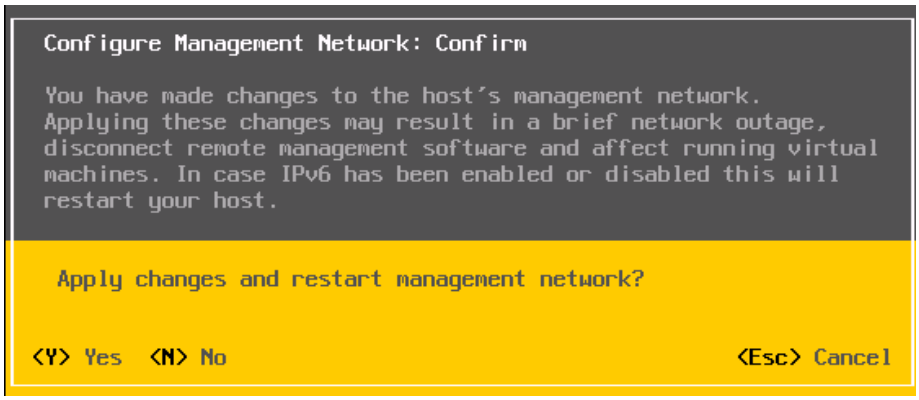


**Step 8:** Configure the primary DNS server and host name (Example: 10.4.48.10 and RS242-ESXi-1.cisco.local, and then press **Enter**.




**Step 9:** On the Configure Management Network screen, exit by pressing **ESC**.

**Step 10:** In the confirmation dialog box, confirm that you want to apply changes and restart by pressing **Y**.



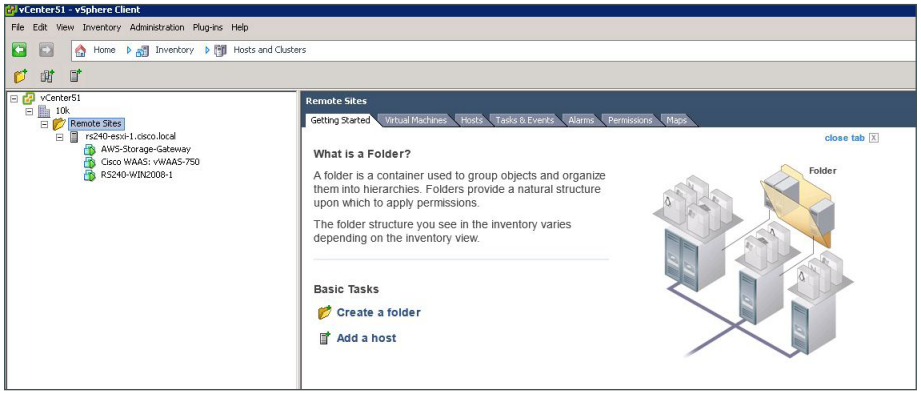

## Procedure 4 Add VMware ESXi host to vCenter

**Step 1:** From the VMware vSphere client, select the folder location where you want to add the ESXi host (Example: Remote Sites).

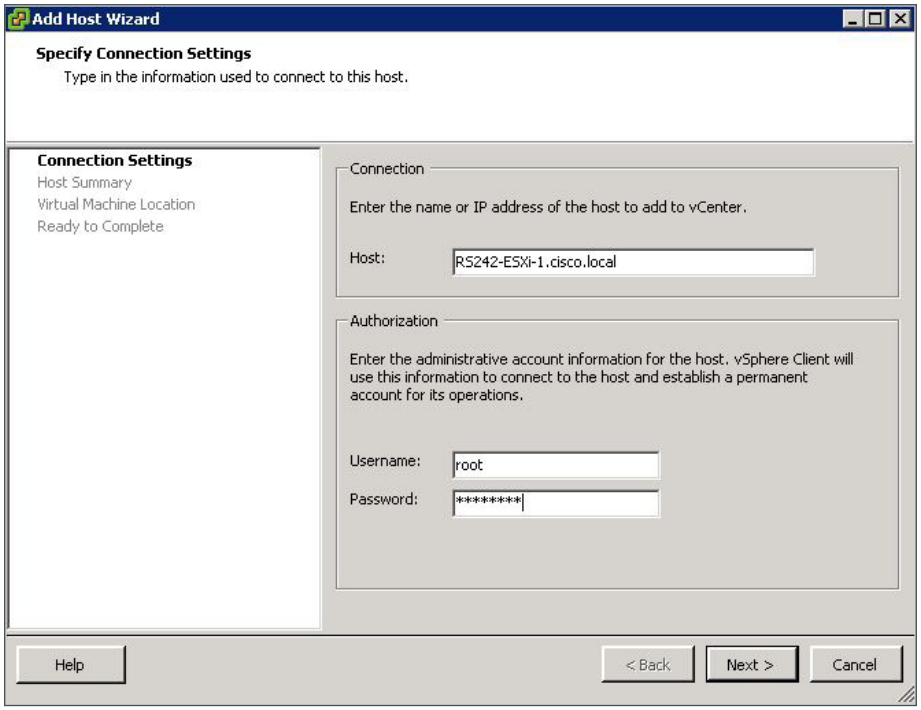
**Step 2:** On the **Getting Started** tab, under **Basic Tasks**, click **Add a host**.

## Tech Tip

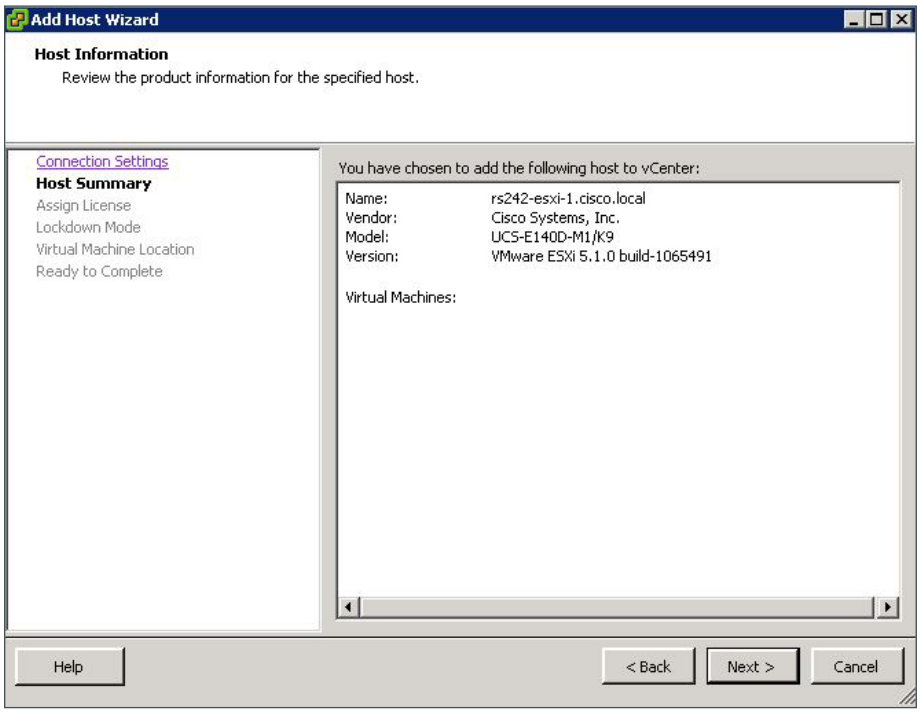
You must have the ESXi host name and IP address configured in your DNS database if you want to be able to reference it by name in the vCenter. Add a new DNS entry if required.



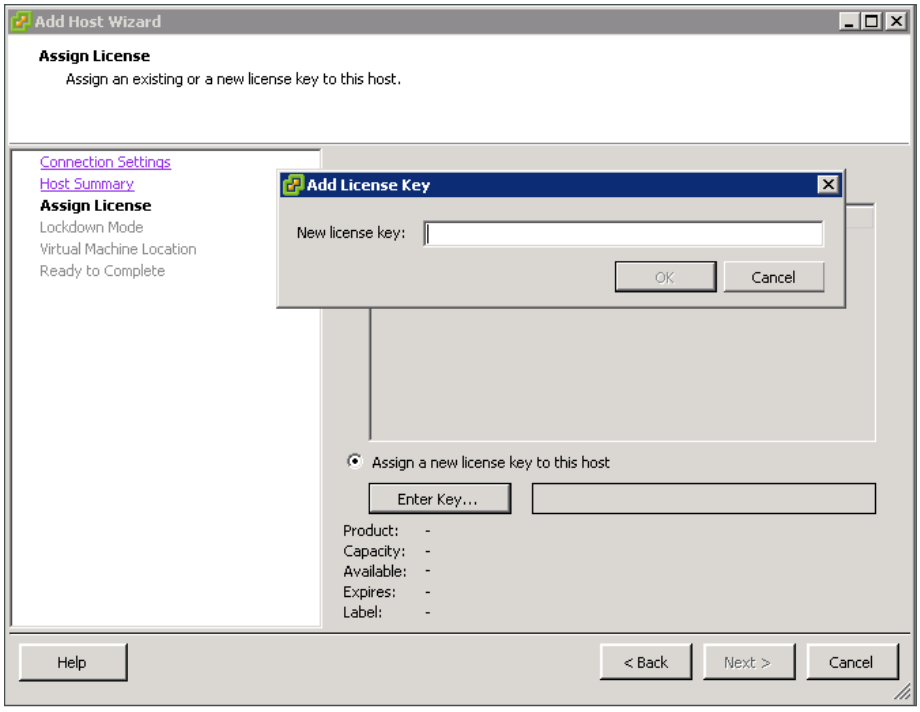

**Step 3:** In the Connection Settings pane, enter the host name of the ESXi host and the username and password (Example: root / c1sco123), and then click **Next**. If necessary, accept the Security Alert by clicking **Yes**.



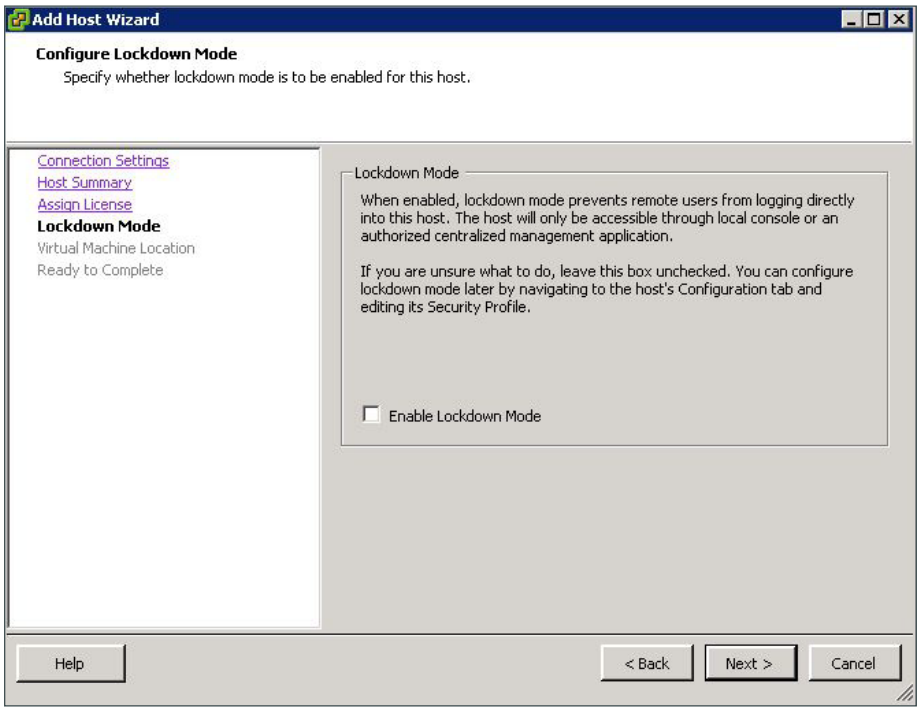
**Step 4:** In the Host Summary pane, verify the details of the ESXi host you want to add, and then click **Next**.



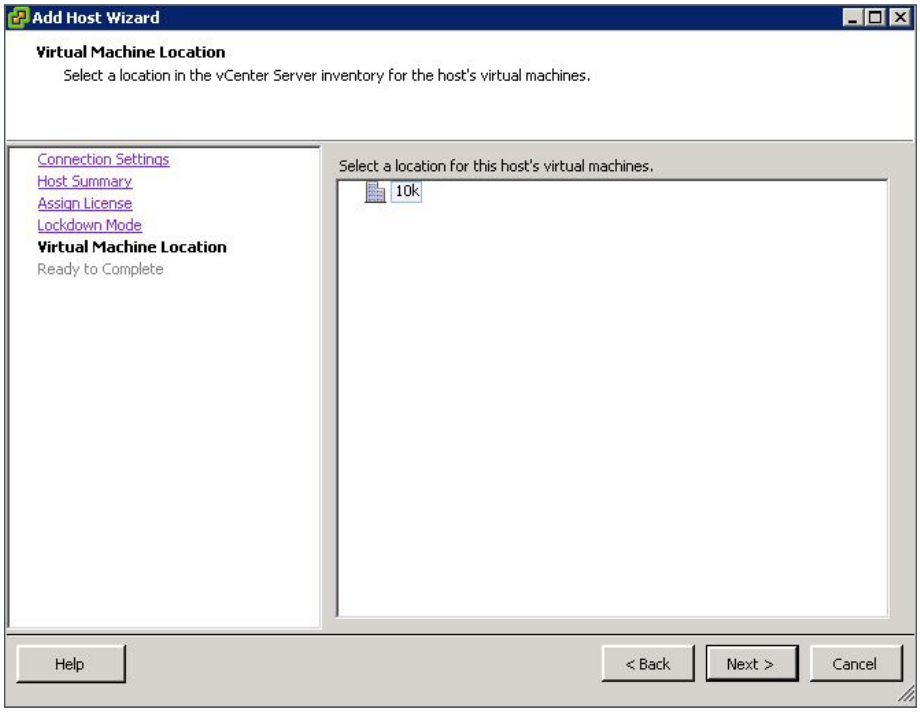

**Step 5:** In the **Assign License** window, click in the circle to assign the appropriate VMware license key or add a new license key and then click **Next**.



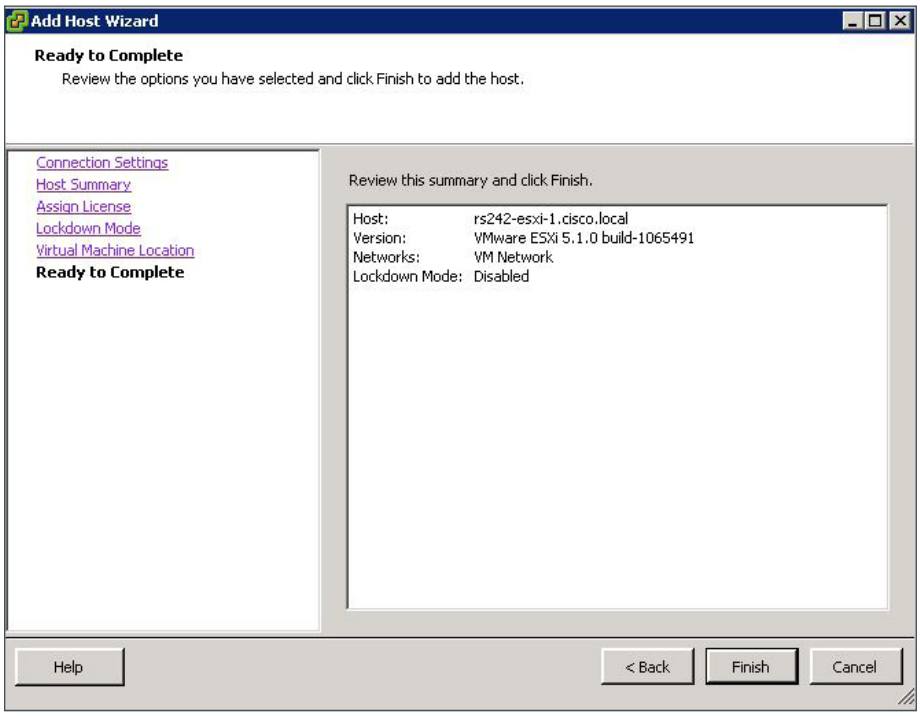
Step 6: In the Lockdown Mode pane, verify that **Enable Lockdown Mode** is cleared, and then click **Next**.



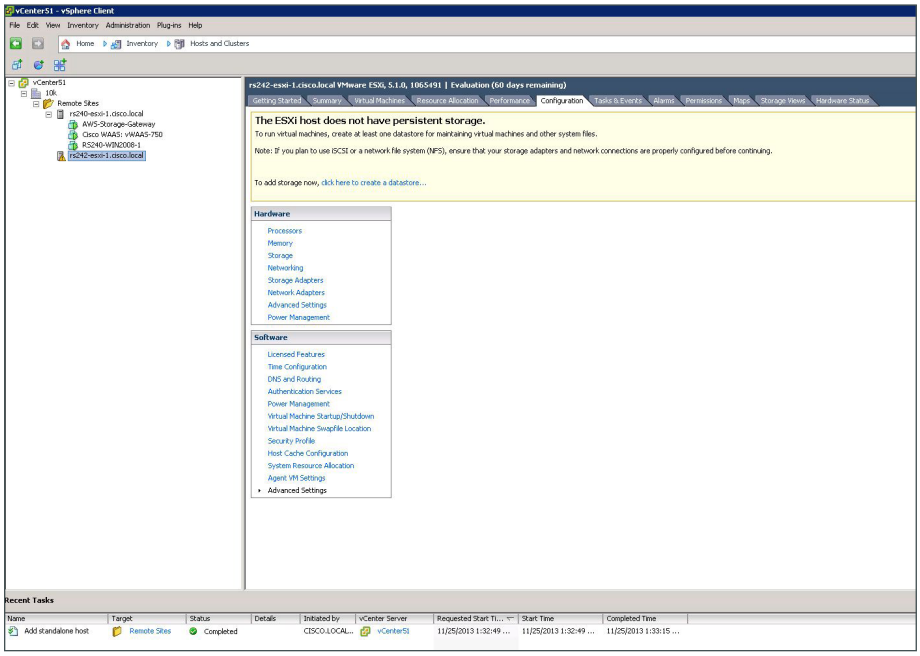

Step 7: In the Virtual Machine Location pane, select the proper location for the new EXSi host, and then click **Next**.



**Step 8:** In the Ready to Complete summary pane, verify the information, and then click **Finish**.




**Step 9:** Select the new ESXi host, click the **Summary** tab and then verify that the information is correct.



## Procedure 5 Add a datastore to ESXi hosts

In this procedure, you add storage for the virtual machines and other system files to use. The storage is a disk drive physically located on the server.

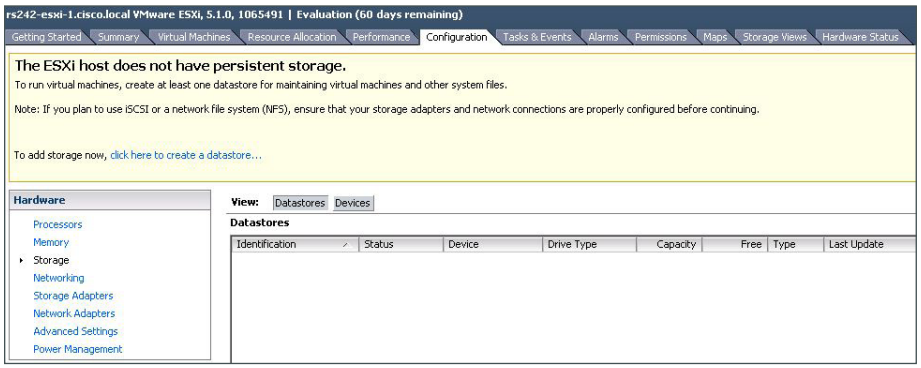
### Tech Tip

If you are installing the vSphere client on a server with USB storage for ESXi, you may receive a warning “System logging not Configured on host <hostname>”, which means that you do not have a location to store log files for ESXi on this host. In this case, you can store log files on a syslog server. More information can be found at: http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2003322

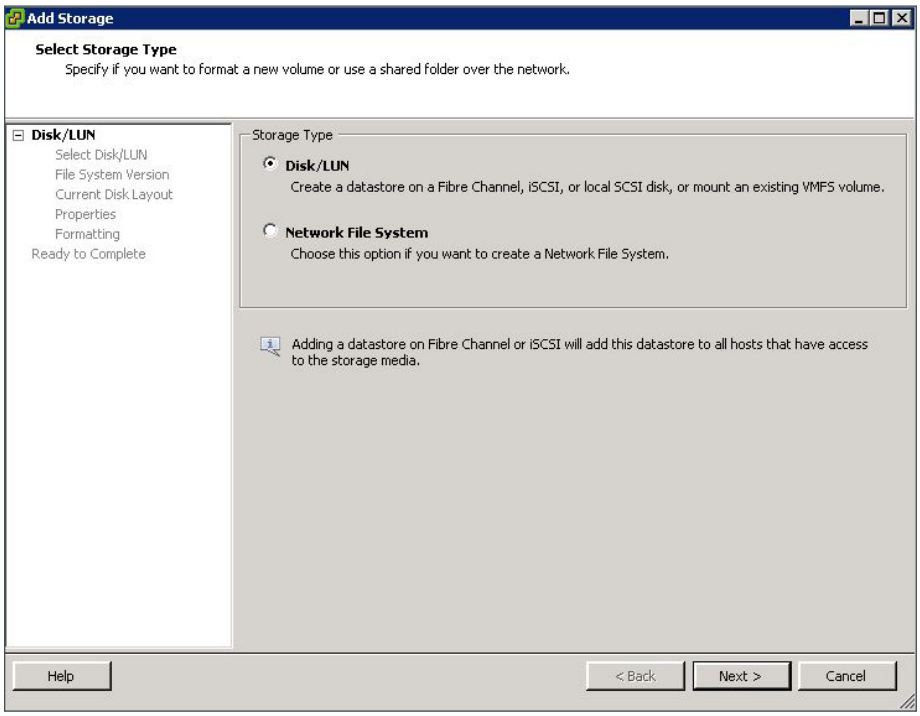
**Step 1:** Using vSphere Client, log in to the ESXi host.

**Step 2:** On the Configuration tab, in the Hardware pane, click **Storage**.

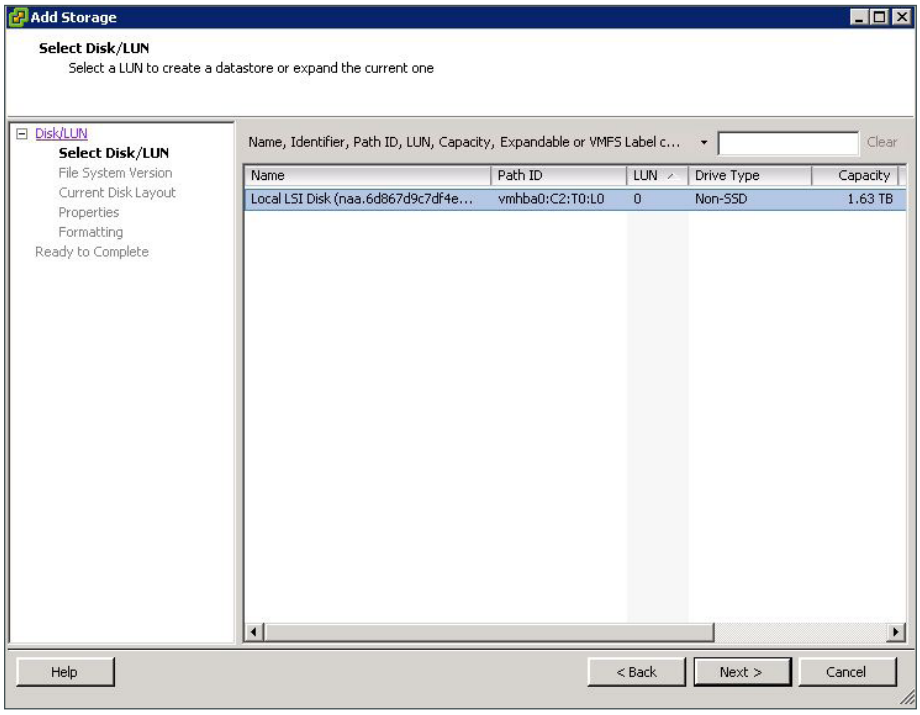
**Step 3:** If your ESXi host does not have a provisioned virtual machine file system (VMFS), in main window, in the “The VMware ESX Server does not have persistent storage” message, click **Click here to create a datastore**.



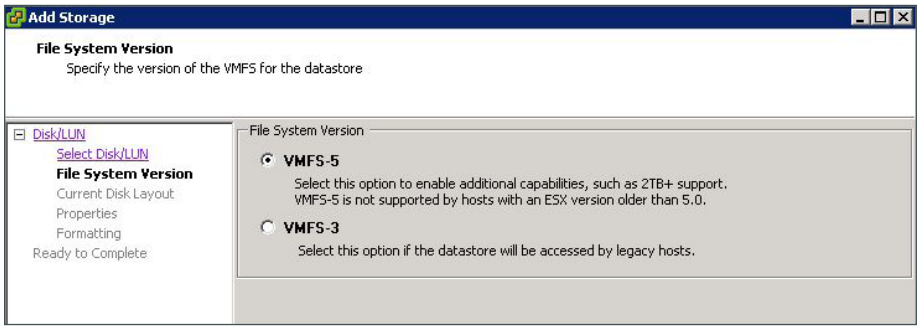
**Step 4:** In the Add Storage wizard, select **Disk/LUN**, and then click **Next**.



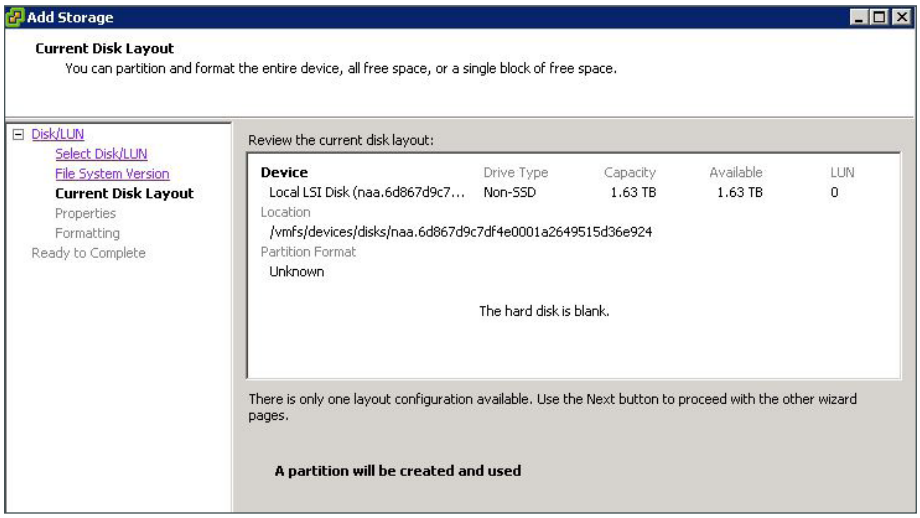

**Step 5:** On the Select Disk/LUN page, select the local disk and then click **Next**.



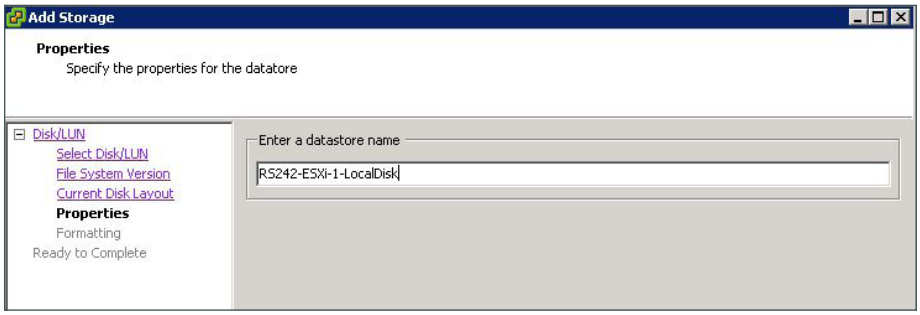
**Step 6:** On the File System Version page, select **VMFS-5** or **VMFS-3**. Hosts running ESXi 4.x will not be able to access VMFS-5 datastores. Unlike VMFS-3, VMFS-5 uses standard 1 MB file system block size with support of 2 TB+ virtual disks.



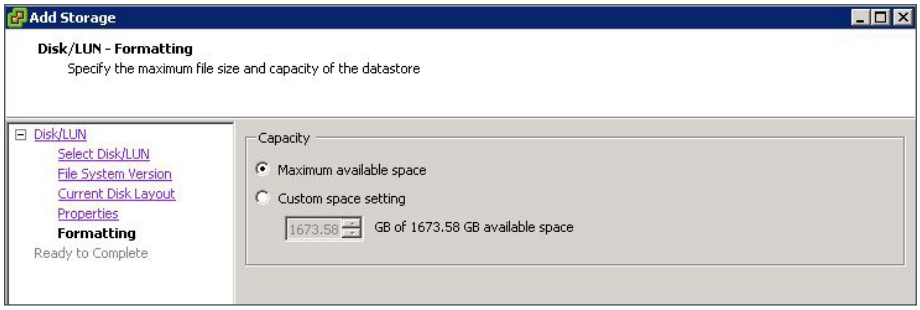

**Step 7:** Review the disk capacity and partition information, and then click **Next**.




**Step 8:** Enter a datastore name, and then click **Next**.

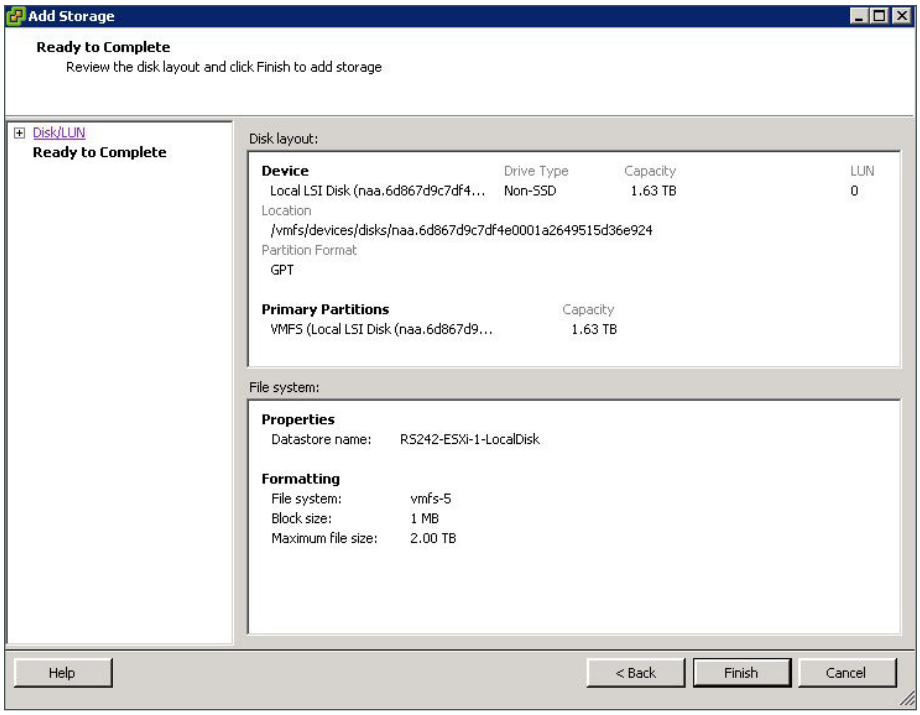


**Step 9:** On the Disk/LUN Formatting page, accept the defaults by clicking **Next**. This formats the maximum available space in the disk.




**Step 10:** Click **Finish**.

The Add Storage wizard is completed.



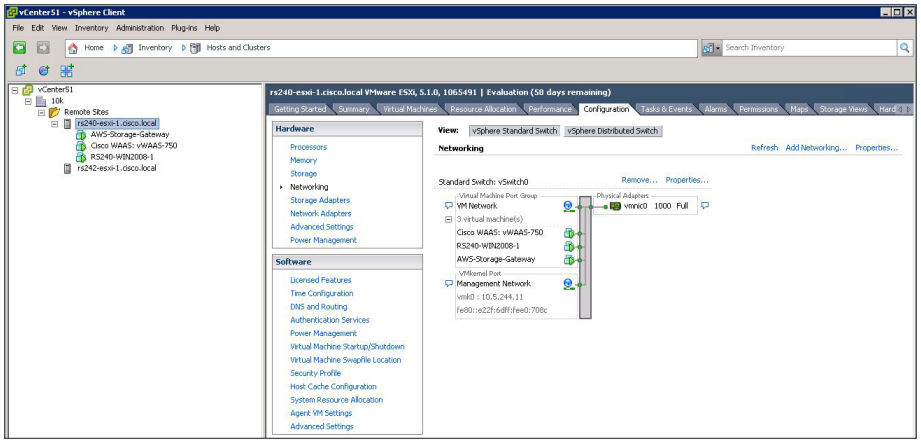
## Procedure 6 Configure networking for ESXi host

Use this procedure to configure UCS E-Series Server with a single network interface card (NIC). This procedure uses the values in the following table to map the correct network interfaces to the vSwitch.

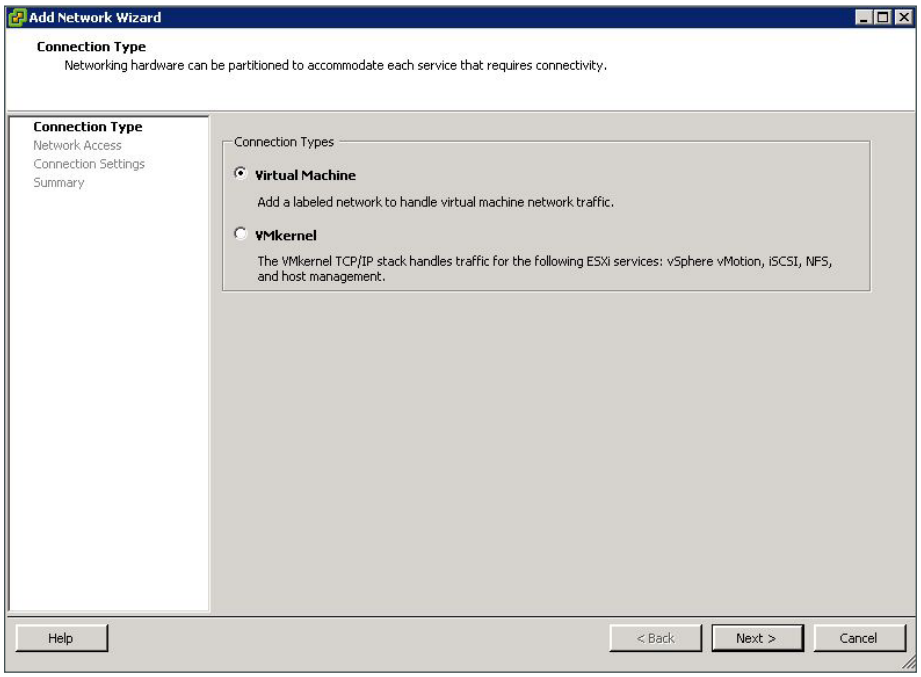
*Table 5 - Cisco UCS E-Series Server interface assignments*

| Interface usage | UCS E140S (single-wide) | UCS E140D (double-wide) |
|---|---|---|
| Console/internal | vmnic0 | vmnic0 |
| Internal MGF | vmnic1 | vmnic1 |
| External (1) | vmnic2 | vmnic2 |
| External (2) | | vmnic3 |
| vSwitch port group network label | ESXi-external | ESXi-external-dual |

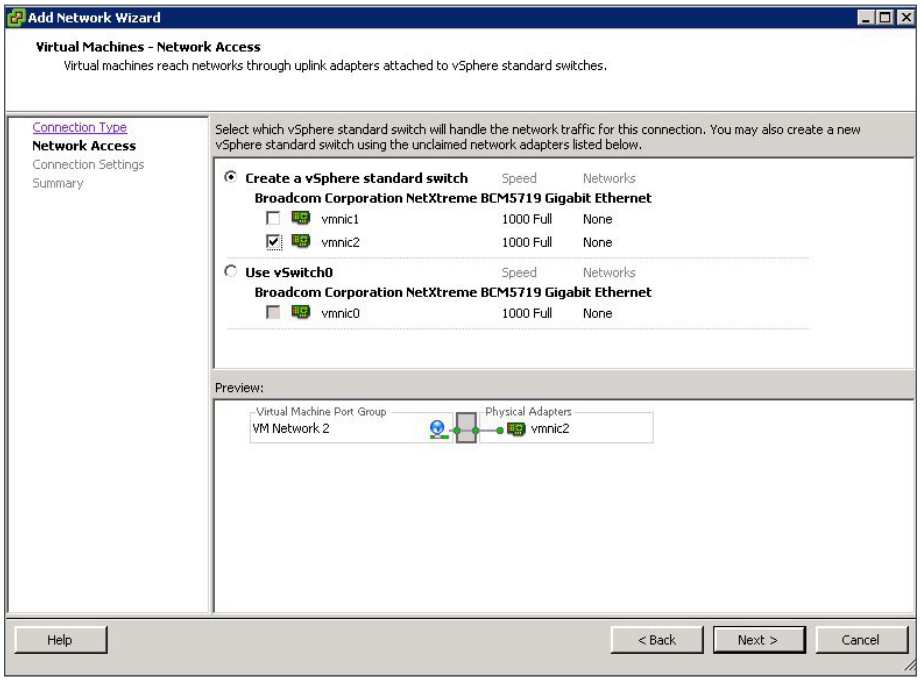
**Step 1:** Click the **Configuration** tab, click **Networking**, and then click **Add Networking**.



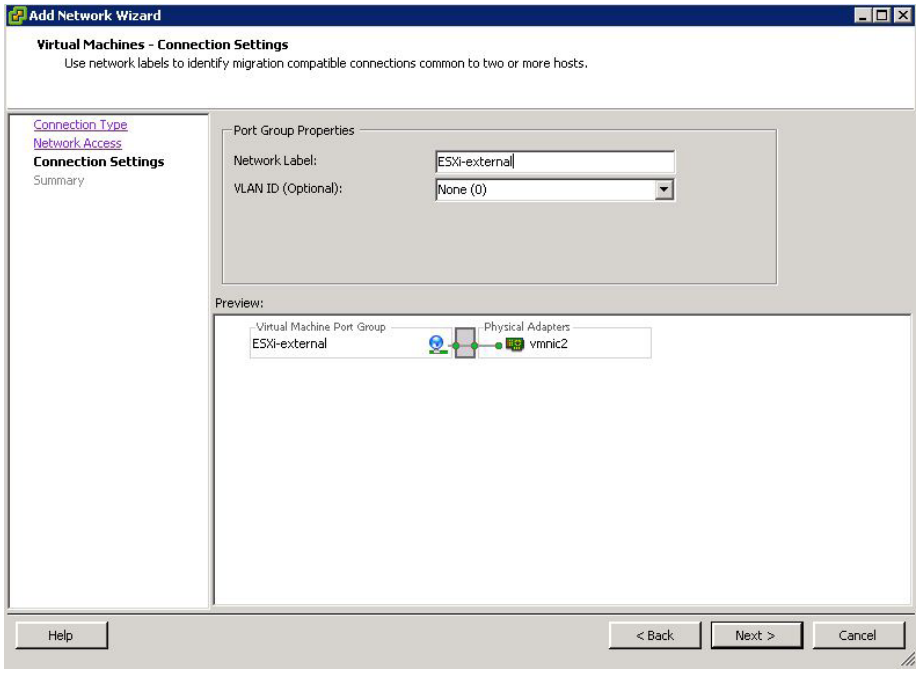
**Step 2:** In the **Connection Type** dialog box, select **Virtual Machine**, and then click **Next**.



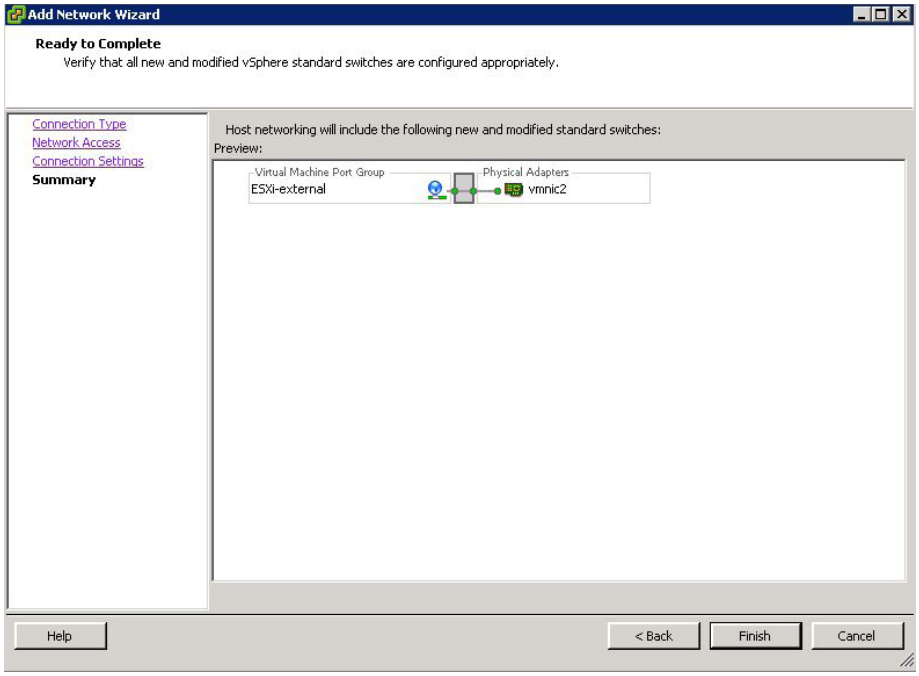

**Step 3:** Select the external NIC card, **vmnic2**, to be used for this vSwitch, and then click **Next**. This example uses a single interface.



**Step 4:** In the Port Group Properties pane, edit the Network Label (Example from Table 5: ESXi-external), set the VLAN ID to **None (0)**, and then click **Next**.




**Step 5:** Review the final host networking configuration, and then click **Finish**.



## Procedure 7 Configure ESXi NIC teaming for resiliency

### (Optional)

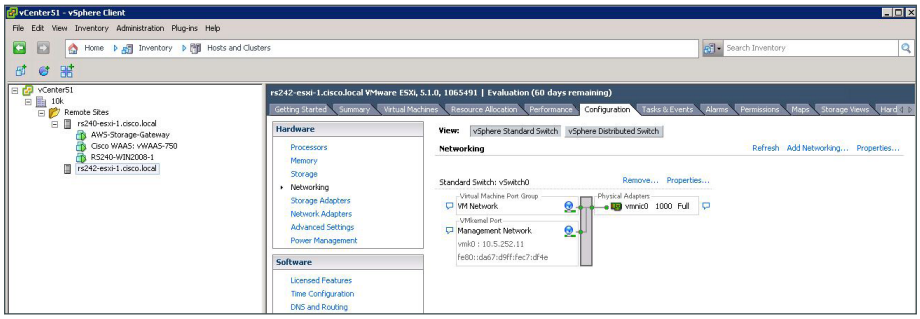
This procedure is only required if you have two external NICs connecting to external switches for resiliency. This example uses the default ESXi NIC teaming configurations for redundancy.

This procedure uses the values in the following table to map the correct network interfaces to the vSwitch.

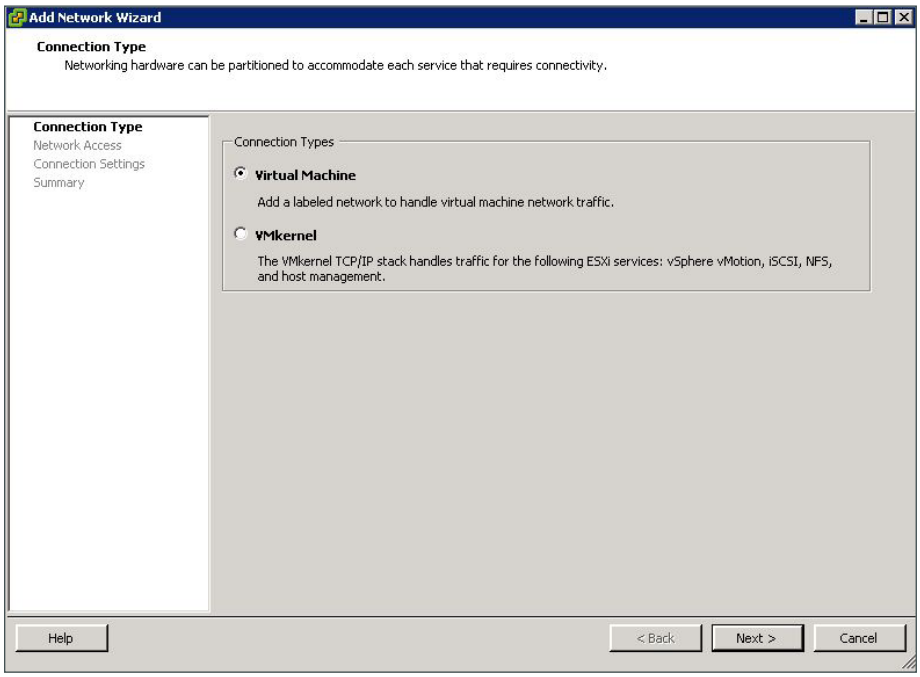
*Table 6 - Cisco UCS E-Series Server interface assignments*

| Interface usage | UCS E140S (single-wide) | UCS E140D (double-wide) |
|---|---|---|
| Console/internal | vmnic0 | vmnic0 |
| Internal MGF | vmnic1 | vmnic1 |
| External (1) | vmnic2 | vmnic2 |
| External (2) | | vmnic3 |
| vSwitch port group network label | ESXi-external | ESXi-external-dual |

**Step 1:** Click the **Configuration** tab, and then click **Networking**, and then click **Add Networking**.



**Step 2:** In the **Connection Type** dialog box, select **Virtual Machine**, and then click **Next**.

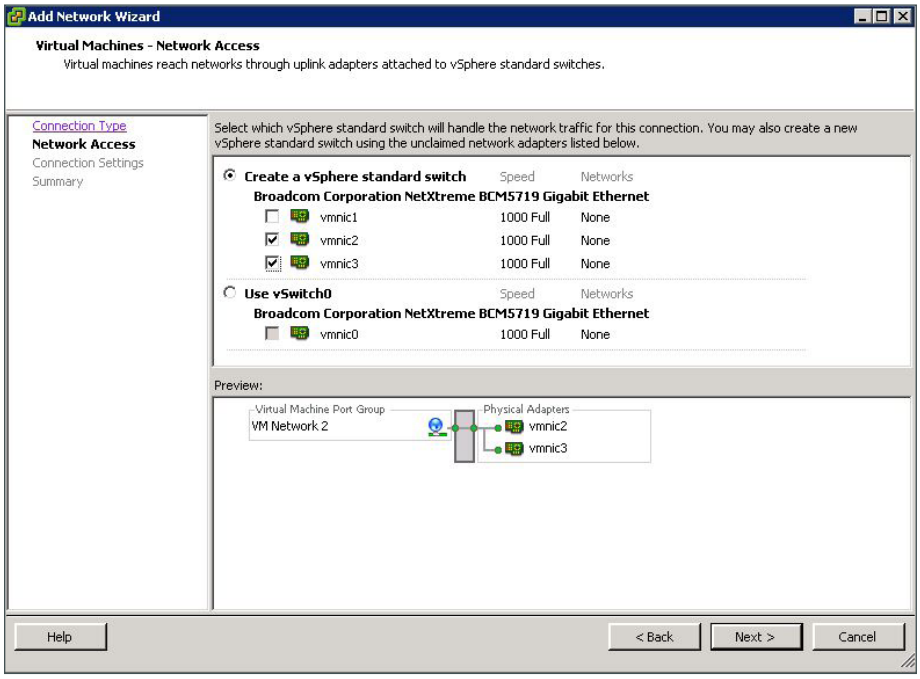


**Step 3:** Select the external NIC cards, **vmnic2** and **vmnic3**, to be used for this vSwitch, and then click **Next**.

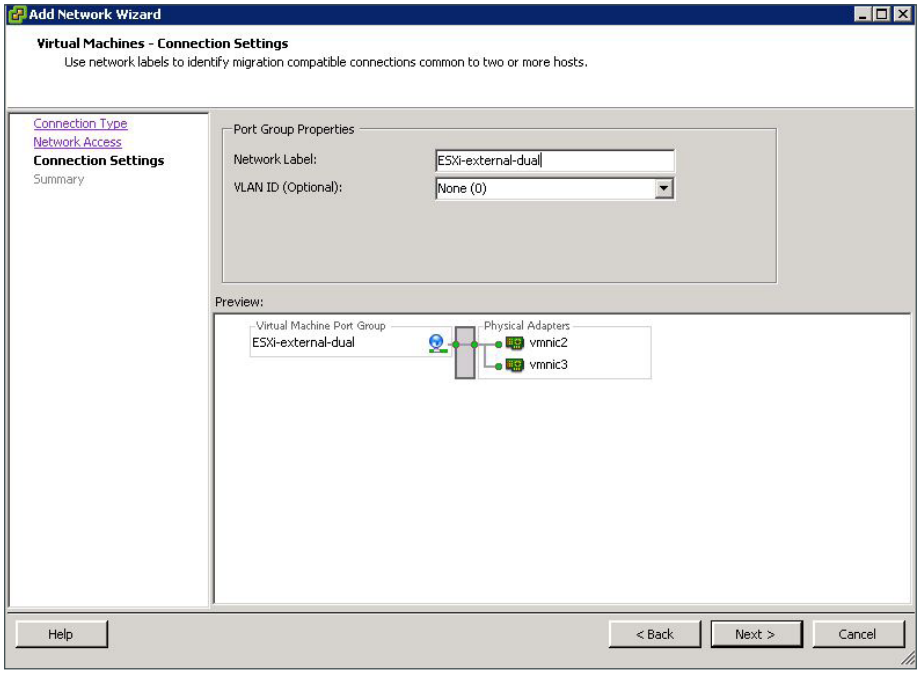
## Tech Tip

The single-wide UCS E-Series Server modules only have a single external Ethernet interface. The double-wide modules have two external Ethernet interfaces for VM traffic and can be connected to two external switches for redundancy.

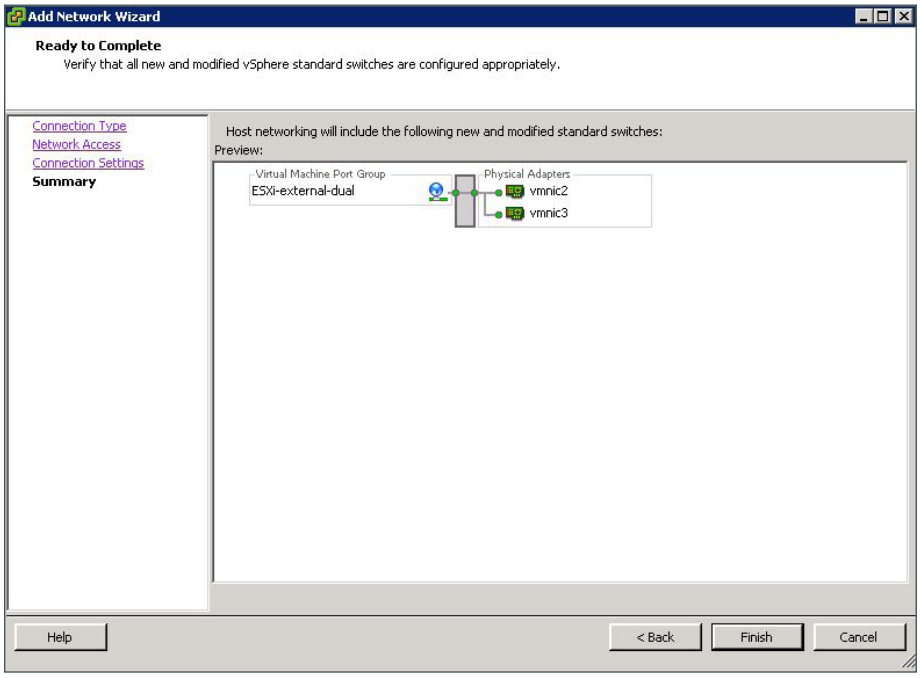
When selecting **vmnic2** and **vmnic3** for dual NIC configurations ESXi automatically configures failover for these interfaces and balances traffic based on port.



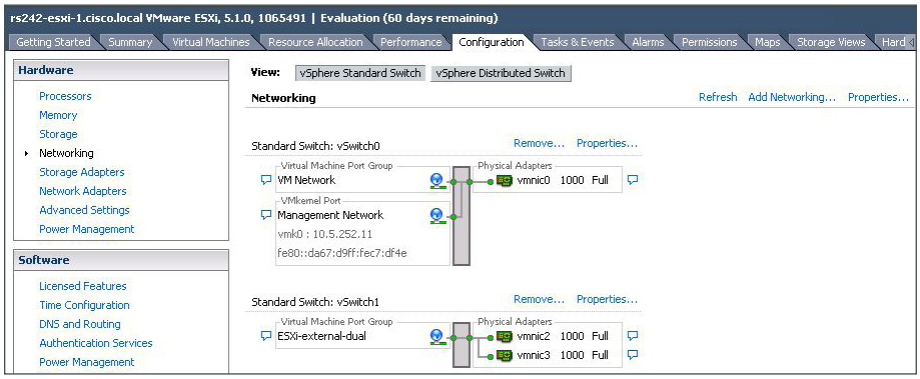
**Step 4:** In the Port Group Properties pane, edit the Network Label (Example from Table 6: ESXi-external-dual), set the VLAN ID to **None (0)**, and then click **Next**.




**Step 5:** Review the final host networking configuration, and then click **Finish**.



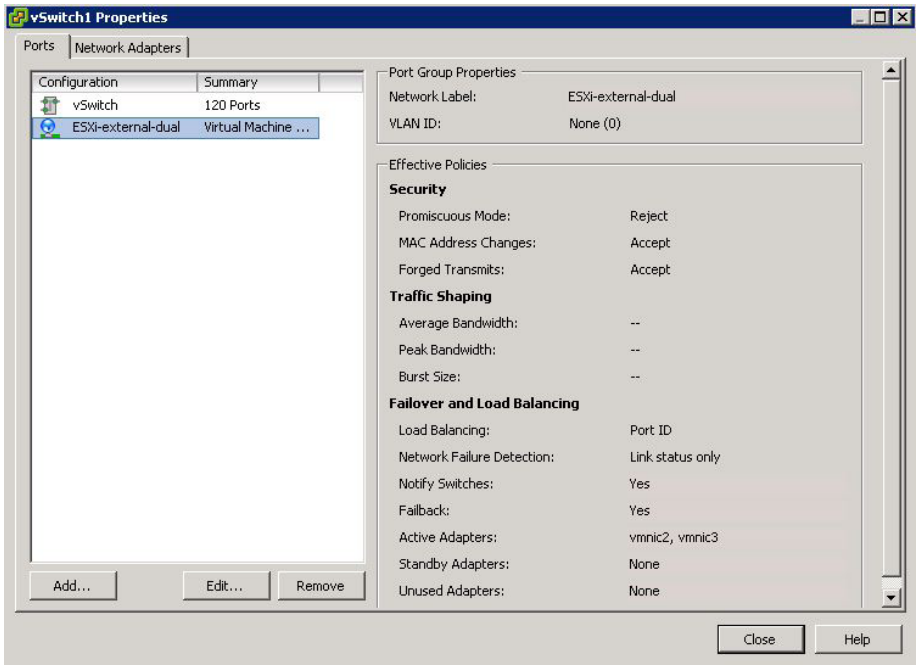
**Step 6:** View properties by clicking **Properties** for the newly created vSwitch (Example: vSwitch1).



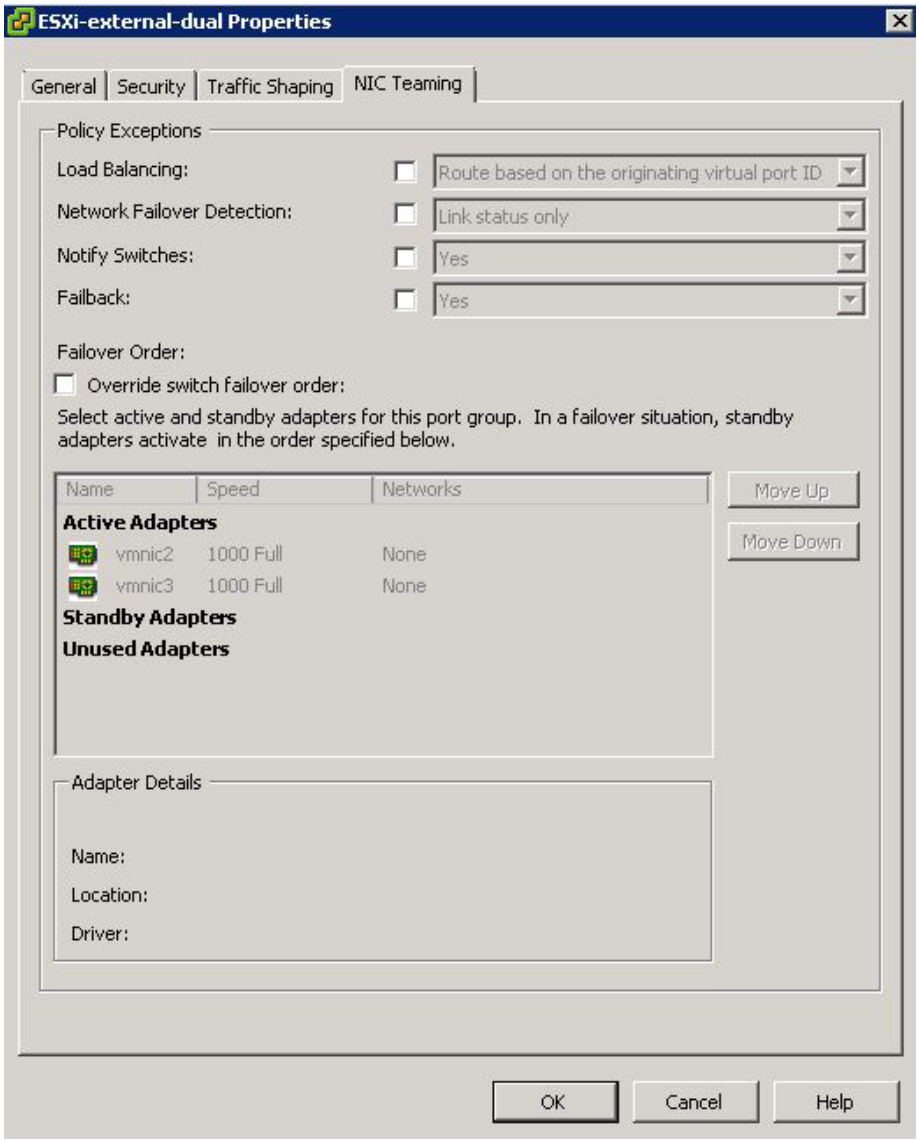

**Step 7:** In the vSwitch Properties pane, select the Port Group (Example: ESXi-external-dual), and click **Edit**.

## Tech Tip

By using the default VMware settings, this NIC redundancy configuration provides failover for link or switch failure for applications installed on a Cisco UCS E-Series Server double-wide module such as the UCS E140D.



**Step 8:** In the Port Group Properties pane, view the Failover and Load Balancing details by clicking the **NIC Teaming** tab. The configuration options dialog box appears.



PROCESS

# Deploying Hosted Cloud Storage Applications on the UCS E-Series Server Module

1. Deploy OVA for hosted cloud connector applications

To avoid WAN congestion and possible installation issues, download or copy the installation Open Virtual Appliance (OVA) files to a local host at the remote location and perform the install from a remote host at that location.

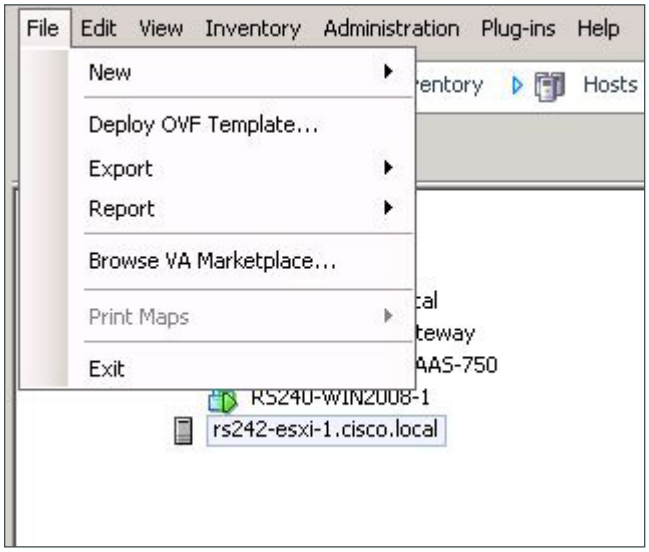
Most Cloud Connector applications are available as OVA and are designed to be installed into a virtual environment. The OVA is an industry standard format with prepackaged disk, memory, CPU, NICs, and other virtual-machine-related configuration parameters.

## Procedure 1 Deploy OVA for hosted cloud connector applications

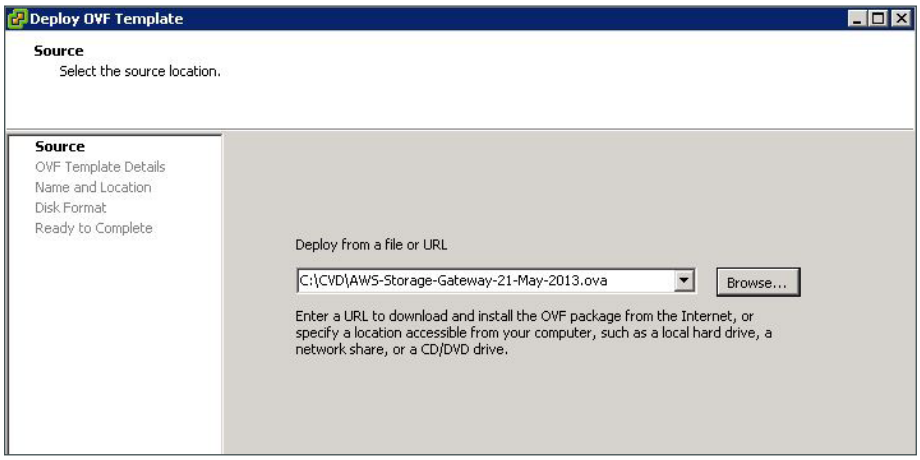
This procedure shows how to install an OVA using VMware vCenter.

**Step 1:** From vCenter, click the ESXi host that you plan to use to run your virtual machine (Example: rs242-esxi-1.cisco.local).

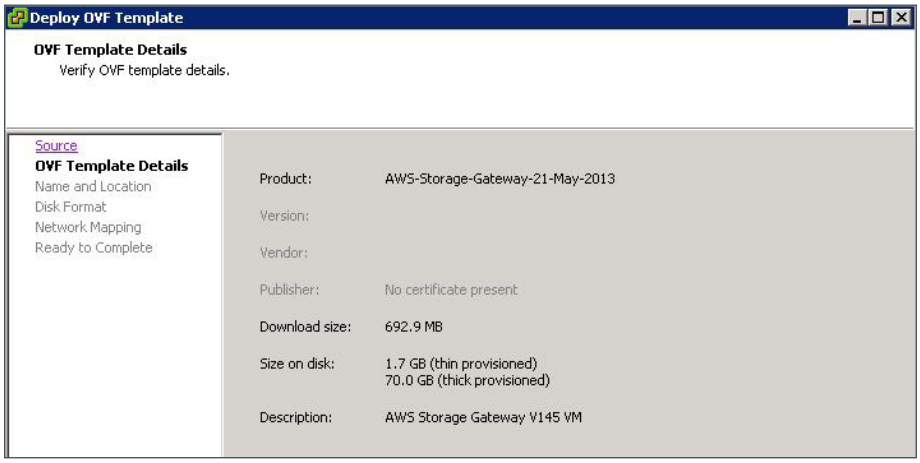
**Step 2:** From the **File** menu, click **Deploy OVF template**.



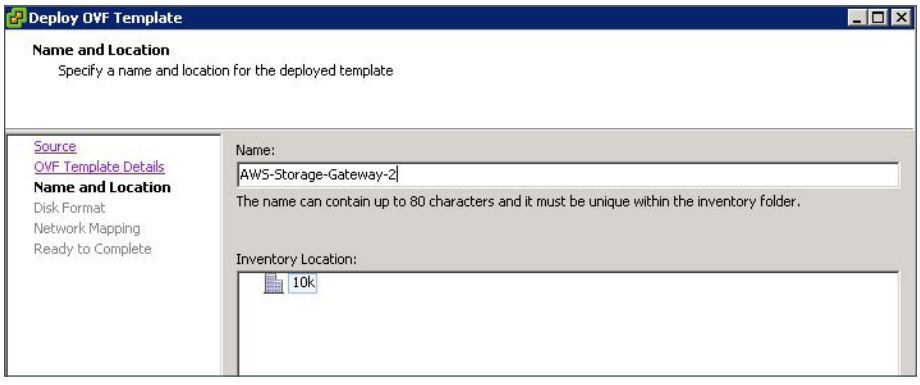
Step 3: Browse to the local OVA file to install, and then click **Next**.



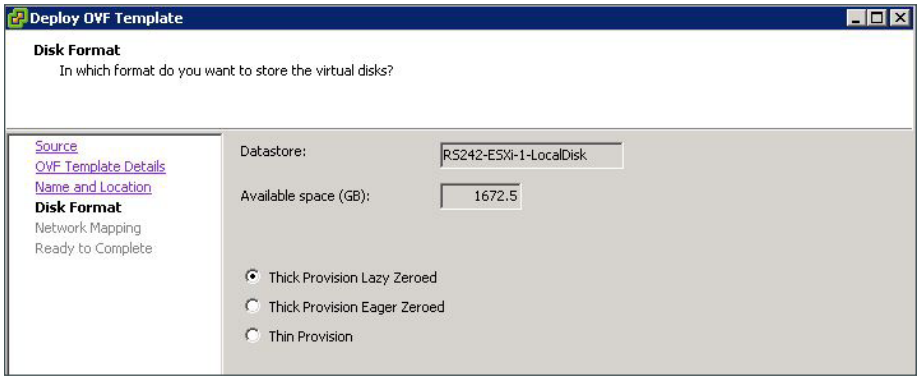

Step 4: Review the template details and then click **Next**.



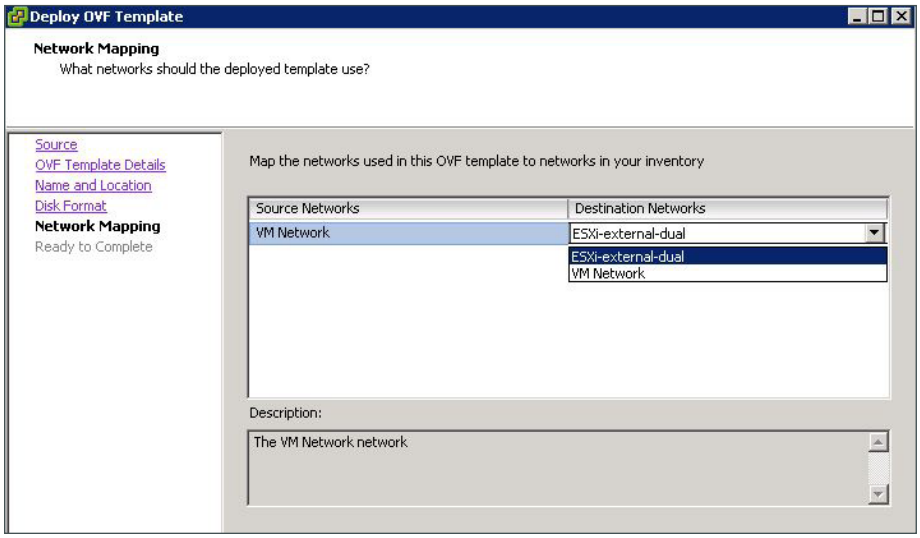

Step 5: Enter a name for the OVA (Example: AWS-Storage-Gateway-2), select the proper location, and then click **Next**.



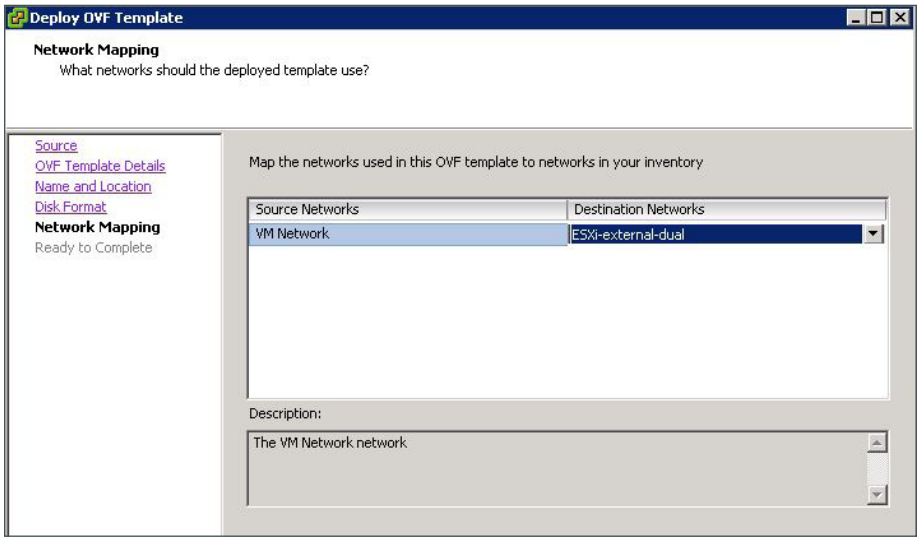
**Step 6:** Verify the data store and the provisioning according to the recommendations of the application vendor. To accept the recommended Disk Format Settings, click **Next**.



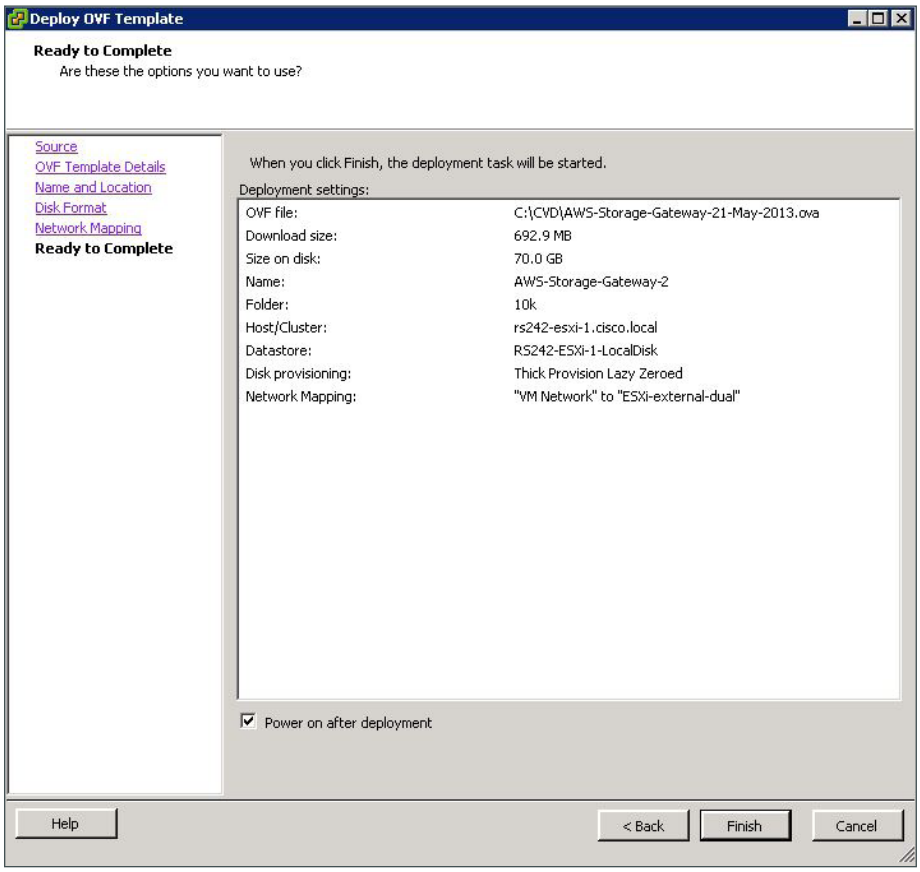

**Step 7:** Click the current setting for Destination Networks. All destination network choices are displayed.



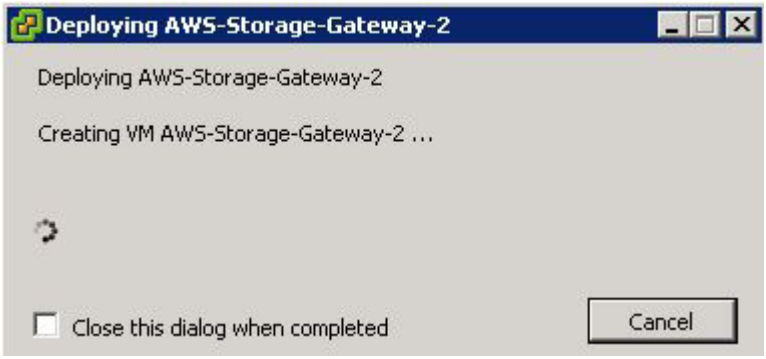

**Step 8:** Select the destination network by choosing the ESXi networking profile created in Procedure 10, Step 4 (Example: ESXi-external-dual), and then click **Next**.



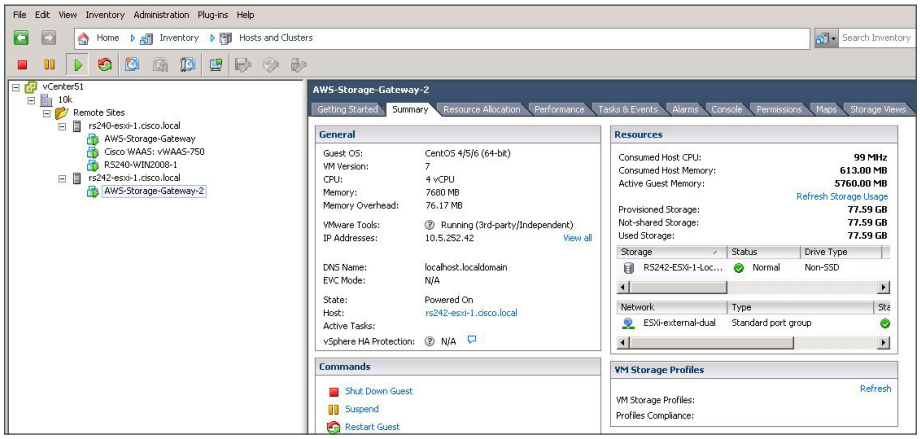
Step 9: Review the OVA summary information, select **Power on after deployment**, and then click **Finish**.




Step 10: Monitor the deployment.




**Step 11:** After the OVA is installed, highlight the installed OVA, and then, on the **Summary** tab, verify its status.




**Step 12:** Finish configuring the Cloud Connector application according to the guidelines provided by the third-party vendor.

# Appendix A: Product List

## WAN Remote Site

| Functional Area | Product Description | Part Numbers | Software |
|---|---|---|---|
| Modular WAN Remote-site Router | Cisco 3945 Voice Sec. Bundle, PVDM3-64, UC and SEC License PAK | C3945-VSEC/K9 | 15.2(4)M4 securityk9 license datak9 license |
| | Cisco 3925 Voice Sec. Bundle, PVDM3-64, UC and SEC License PAK | C3925-VSEC/K9 | |
| | Data Paper PAK for Cisco 3900 series | SL-39-DATA-K9 | |
| | Cisco 2951 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK | C2951-VSEC/K9 | |
| | Cisco 2921 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK | C2921-VSEC/K9 | |
| | Cisco 2911 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK | C2911-VSEC/K9 | |
| | Data Paper PAK for Cisco 2900 series | SL-29-DATA-K9 | |
| | 1941 WAAS Express only Bundle | C1941-WAASX-SEC/K9 | |
| | Data Paper PAK for Cisco 1900 series | SL-19-DATA-K9 | |
| Virtual Servers | Cisco UCS E-Series Double-Wide Server Blades, Intel Xeon E5-2400 Six Core processor, 8GB RAM, 2 SD cards, PCIe card | UCS-E160DP-M1/K9 | – |
| | Cisco UCS E-Series Double-Wide Server Blades, Intel Xeon E5-2400 Six Core processor, 8GB RAM, 2 SD cards | UCS-E160D-M1/K9 | |
| | Cisco UCS E-Series Double-Wide Server Blades, Intel Xeon E5-2400 Quad Core processor, 8GB RAM, 2 SD cards, PCIe card | UCS-E140DP-M1/K9 | |
| | Cisco UCS E-Series Double-Wide Server Blades, Intel Xeon E5-2400 Quad Core processor, 8GB RAM, 2 SD cards | UCS-E140D-M1/K9 | |
| | Cisco UCS E-Series Single-Wide Server Blades, Intel Xeon E3 Quad Core processor, 8GB RAM, 2 SD cards | UCS-E140S-M1/K9 | |
| VMWare | VMware vSphere | ESXi | 5.1.0 U1 |

# Appendix B: Configurations

This appendix shows the validated router configurations for each of the remote sites and solutions presented in this guide, which deploys Cisco UCS E-Series servers for Hosted Cloud Connector applications at remote sites with local Internet access.

## Remote Site 240

This site uses a single router MPLS WAN primary with VPN WAN backup.

### RS240-3945

```
version 15.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname RS240-3945
!
boot-start-marker
boot system flash0:c3900-universalk9-mz.SPA.152-4.M4.bin
boot-end-marker
!
!
enable secret 4 /DtCCr53Q4B18jSIm1UEqu7cNVZTOhxTZyUnZdsSrsw
!
aaa new-model
!
!
aaa group server tacacs+ TACACS-SERVERS
 server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization console
aaa authorization exec default group TACACS-SERVERS local
!
aaa session-id common
clock timezone PST -8 0
clock summer-time PDT recurring
!
!
ip cef
```

```
!
ip domain name cisco.local
ip multicast-routing
ip inspect log drop-pkt
no ipv6 cef
!
parameter-map type inspect global
 log dropped-packets enable
 max-incomplete low 18000
 max-incomplete high 20000
 spoofed-acker off

multilink bundle-name authenticated
!
!
username admin password 7 121A540411045D5679
!
redundancy
!
ip ssh source-interface Loopback0
ip ssh version 2
!
track 60 ip sla 110 reachability
!
track 61 ip sla 111 reachability
!
track 62 list boolean or
 object 60
 object 61
!
class-map type inspect match-any INSIDE-TO-OUTSIDE-CLASS
 match protocol ftp
 match protocol tcp
 match protocol udp
 match protocol icmp
class-map type inspect match-any INSPECT-ACL-OUT-CLASS
 match access-group name ACL-RTR-OUT
class-map type inspect match-any PASS-ACL-IN-CLASS
 match access-group name ESP-IN
 match access-group name DHCP-IN
class-map type inspect match-any PASS-ACL-OUT-CLASS
 match access-group name ESP-OUT
 match access-group name DHCP-OUT
class-map type inspect match-any INSPECT-ACL-IN-CLASS
 match access-group name ACL-RTR-IN
!
policy-map type inspect ACL-OUT-POLICY
```

```
 class type inspect INSPECT-ACL-OUT-CLASS
  inspect
 class type inspect PASS-ACL-OUT-CLASS
  pass
 class class-default
  drop
policy-map type inspect INSIDE-TO-OUTSIDE-POLICY
 class type inspect INSIDE-TO-OUTSIDE-CLASS
  inspect
 class class-default
  drop
policy-map type inspect ACL-IN-POLICY
 class type inspect INSPECT-ACL-IN-CLASS
  inspect
 class type inspect PASS-ACL-IN-CLASS
  pass
 class class-default
  drop
!
zone security INSIDE
zone security OUTSIDE
zone-pair security IN_OUT source INSIDE destination OUTSIDE
 service-policy type inspect INSIDE-TO-OUTSIDE-POLICY
zone-pair security TO-ROUTER source OUTSIDE destination self
 service-policy type inspect ACL-IN-POLICY
zone-pair security FROM-ROUTER source self destination OUTSIDE
 service-policy type inspect ACL-OUT-POLICY
!
crypto keyring GLOBAL-KEYRING
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
!
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 2
crypto isakmp keepalive 30 5
crypto isakmp profile ISAKMP-INET-PUBLIC
   keyring GLOBAL-KEYRING
   match identity address 0.0.0.0
!
crypto ipsec security-association replay window-size 1024
!
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256 esp-sha-hmac
 mode transport
!
crypto ipsec profile DMVPN-PROFILE1
 set transform-set AES256/SHA/TRANSPORT
```

```
 set isakmp-profile ISAKMP-INET-PUBLIC
!
!
interface Loopback0
 ip address 10.255.251.240 255.255.255.255
 ip pim sparse-mode
!
interface Tunnel10
 bandwidth 10000
 ip address 10.4.34.240 255.255.254.0
 no ip redirects
 ip mtu 1400
 ip hello-interval eigrp 200 20
 ip hold-time eigrp 200 60
 ip pim dr-priority 0
 ip pim nbma-mode
 ip pim sparse-mode
 ip nhrp authentication cisco123
 ip nhrp map multicast 172.16.130.1
 ip nhrp map 10.4.34.1 172.16.130.1
 ip nhrp network-id 101
 ip nhrp holdtime 600
 ip nhrp nhs 10.4.34.1
 ip nhrp registration no-unique
 ip nhrp shortcut
 ip nhrp redirect
 zone-member security INSIDE
 ip summary-address eigrp 200 10.5.240.0 255.255.248.0
 ip tcp adjust-mss 1360
 tunnel source GigabitEthernet0/1
 tunnel mode gre multipoint
 tunnel route-via GigabitEthernet0/1 mandatory
 tunnel protection ipsec profile DMVPN-PROFILE1
!
interface Port-channel1
 no ip address
!
interface Port-channel1.64
 encapsulation dot1Q 64
 ip address 10.5.244.1 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim sparse-mode
 ip nat inside
 ip virtual-reassembly in
 zone-member security INSIDE
!
interface Port-channel1.69
```

```
 encapsulation dot1Q 69
 ip address 10.5.245.1 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim sparse-mode
 ip nat inside
 zone-member security INSIDE
!
interface GigabitEthernet0/0
 description MPLS-A (remote-as 65401 - 192.168.3.50)
 bandwidth 10000
 ip address 192.168.3.49 255.255.255.252
 zone-member security INSIDE
 duplex auto
 speed auto
 no cdp enable
!
interface GigabitEthernet0/1
 ip dhcp client default-router distance 10
 ip dhcp client route track 62
 ip address dhcp
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip nat outside
 ip virtual-reassembly in
 zone-member security OUTSIDE
 duplex auto
 speed auto
 no lldp transmit
 no lldp receive
 no cdp enable
 no mop enabled
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 channel-group 1
!
interface ucse3/0
 ip unnumbered Port-channel1.64
 ip nat inside
 zone-member security INSIDE
 imc ip address 10.5.244.10 255.255.255.0 default-gateway 10.5.244.1
 imc access-port shared-lom console
!
!
```

```
router eigrp 200
 distribute-list route-map BLOCK-DEFAULT in
 network 10.4.34.0 0.0.1.255
 network 10.5.0.0 0.0.255.255
 network 10.255.0.0 0.0.255.255
 passive-interface default
 no passive-interface Tunnel10
 eigrp router-id 10.255.251.240
 eigrp stub connected summary redistributed
!
router bgp 65511
 bgp router-id 10.255.251.240
 bgp log-neighbor-changes
 network 10.5.244.0 mask 255.255.255.0
 network 10.5.245.0 mask 255.255.255.0
 network 10.255.251.240 mask 255.255.255.255
 network 192.168.3.48 mask 255.255.255.252
 aggregate-address 10.5.240.0 255.255.248.0 summary-only
 neighbor 192.168.3.50 remote-as 65401
!
ip local policy route-map PBR-SLA-SET-NEXT-HOP
ip forward-protocol nd
!
no ip http server
ip http authentication aaa
ip http secure-server
!
ip pim autorp listener
ip pim register-source Loopback0
ip nat inside source list NAT interface GigabitEthernet0/1 overload
ip route 10.0.0.0 255.0.0.0 Null0 254
ip route 10.5.244.10 255.255.255.255 ucse3/0
ip route 10.5.244.11 255.255.255.255 ucse3/0
ip route 172.16.130.1 255.255.255.255 GigabitEthernet0/1 dhcp
ip tacacs source-interface Loopback0
!
ip access-list standard NAT
 permit 10.5.240.0 0.0.7.255
ip access-list standard NO-DEFAULT
 deny   0.0.0.0
 permit any
!
ip access-list extended ACL-RTR-IN
 permit udp any any eq non500-isakmp
 permit udp any any eq isakmp
 permit icmp any any echo
 permit icmp any any echo-reply
```

```
 permit icmp any any ttl-exceeded
 permit icmp any any port-unreachable
 permit udp any any gt 1023 ttl eq 1
ip access-list extended ACL-RTR-OUT
 permit udp any any eq non500-isakmp
 permit udp any any eq isakmp
 permit icmp any any
ip access-list extended DHCP-IN
 permit udp any eq bootps any eq bootpc
ip access-list extended DHCP-OUT
 permit udp any eq bootpc any eq bootps
ip access-list extended ESP-IN
 permit esp any any
ip access-list extended ESP-OUT
 permit esp any any
ip access-list extended SLA-SET-NEXT-HOP
 permit icmp any host 172.18.1.253
 permit icmp any host 172.18.1.254
!
ip sla auto discovery
ip sla 110
 icmp-echo 172.18.1.253 source-interface GigabitEthernet0/1
 threshold 1000
 frequency 15
ip sla schedule 110 life forever start-time now
ip sla 111
 icmp-echo 172.18.1.254 source-interface GigabitEthernet0/1
 threshold 1000
 frequency 15
ip sla schedule 111 life forever start-time now
!
nls resp-timeout 1
cpd cr-id 1
route-map PBR-SLA-SET-NEXT-HOP permit 10
 match ip address SLA-SET-NEXT-HOP
 set ip next-hop dynamic dhcp
!
route-map BLOCK-DEFAULT permit 10
 match ip address NO-DEFAULT
!
!
snmp-server community cisco RO
snmp-server community cisco123 RW
snmp-server trap-source Loopback0
snmp-server enable traps entity-sensor threshold
tacacs server TACACS-SERVER-1
 address ipv4 10.4.48.15
```

```
 key 7 00371605165E1F2D0A38
!
!
!
control-plane
!
line con 0
 logging synchronous
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line 195
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
 speed 9600
 flowcontrol software
line vty 0 4
 transport preferred none
 transport input ssh
line vty 5 15
 transport preferred none
 transport input ssh
!
scheduler allocate 20000 1000
ntp source Loopback0
ntp update-calendar
ntp server 10.4.48.17
!
end
```

# Remote Site 242

This site uses a dual-router design with MPLS primary and VPN WAN backup. Cisco UCS E-Series servers are deployed in each of the remote-site routers.

## RS242-2951-1

```
version 15.2
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname RS242-2951-1
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 /DtCCr53Q4B18jSIm1UEqu7cNVZTOhxTZyUnZdsSrsw
!
aaa new-model
!
!
aaa group server tacacs+ TACACS-SERVERS
 server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization console
aaa authorization exec default group TACACS-SERVERS local
!
aaa session-id common
clock timezone PST -8 0
clock summer-time PDT recurring
!
ip cef
!
!
ip domain name cisco.local
ip multicast-routing
no ipv6 cef
!
multilink bundle-name authenticated
!
!
username admin password 7 06055E324F41584B56
!
redundancy
!
```

```
ip ssh source-interface Loopback0
ip ssh version 2
!
track 50 ip sla 100 reachability
!
!
interface Loopback0
 ip address 10.255.252.242 255.255.255.255
 ip pim sparse-mode
!
interface Port-channel1
 no ip address
!
interface Port-channel1.64
 encapsulation dot1Q 64
 ip address 10.5.252.2 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim dr-priority 110
 ip pim sparse-mode
 standby version 2
 standby 1 ip 10.5.252.1
 standby 1 priority 110
 standby 1 preempt
 standby 1 authentication md5 key-string 7 094F1F1A1A0A464058
 standby 1 track 50 decrement 10
!
interface Port-channel1.69
 encapsulation dot1Q 69
 ip address 10.5.253.2 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim sparse-mode
!
interface Port-channel1.99
 encapsulation dot1Q 99
 ip address 10.5.248.9 255.255.255.252
 ip pim sparse-mode
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 bandwidth 10000
 ip address 192.168.4.49 255.255.255.252
 duplex auto
 speed auto
 no cdp enable
```

```
!
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 channel-group 1
!
interface ucse2/0
 ip unnumbered Port-channel1.64
 imc ip address 10.5.252.10 255.255.255.0 default-gateway 10.5.252.2
 imc access-port shared-lom console
!
interface ucse2/1
 no ip address
!
!
router eigrp 100
 default-metric 100000 100 255 1 1500
 network 10.5.0.0 0.0.255.255
 network 10.255.0.0 0.0.255.255
 redistribute eigrp 200
 redistribute bgp 65511
 redistribute static route-map STATIC-IN
 passive-interface default
 no passive-interface Port-channel1.99
 eigrp router-id 10.255.252.242
!
router bgp 65511
 bgp router-id 10.255.252.242
 bgp log-neighbor-changes
 network 10.5.252.0 mask 255.255.255.0
 network 10.5.253.0 mask 255.255.255.0
 network 10.255.252.242 mask 255.255.255.255
 network 192.168.4.48 mask 255.255.255.252
 aggregate-address 10.5.248.0 255.255.248.0 summary-only
 neighbor 192.168.4.50 remote-as 65402
 distance 254 192.168.4.50 0.0.0.0 DEFAULT-IN
!
ip forward-protocol nd
!
no ip http server
ip http authentication aaa
ip http secure-server
!
ip pim autorp listener
ip pim register-source Loopback0
```

```
ip route 10.5.252.10 255.255.255.255 ucse2/0
ip route 10.5.252.11 255.255.255.255 ucse2/0
ip tacacs source-interface Loopback0
!
ip access-list standard DEFAULT-IN
 permit 0.0.0.0
ip access-list standard STATIC-ROUTE-LIST
 permit 10.5.252.11
 remark UCSE CIMC & ESXi host routes
 permit 10.5.252.10
!
ip sla auto discovery
ip sla 100
 icmp-echo 192.168.4.50 source-interface GigabitEthernet0/0
 threshold 1000
 frequency 15
ip sla schedule 100 life forever start-time now
!
route-map STATIC-IN permit 20
 match ip address STATIC-ROUTE-LIST
!
!
snmp-server community cisco RO
snmp-server community cisco123 RW
snmp-server trap-source Loopback0
snmp-server enable traps entity-sensor threshold
tacacs server TACACS-SERVER-1
 address ipv4 10.4.48.15
 key 7 04680E051D2458650C00
!
!
!
control-plane
!
!
!
line con 0
 logging synchronous
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line 131
```

```
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
 speed 9600
 flowcontrol software
line vty 0 4
 transport preferred none
 transport input ssh
line vty 5 15
 transport preferred none
 transport input ssh
!
scheduler allocate 20000 1000
ntp source Loopback0
ntp update-calendar
ntp server 10.4.48.17
!
end
```

### RS242-2951-2

```
version 15.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname RS242-2951-2
!
boot-start-marker
boot-end-marker
!
!
enable secret 5 $1$CAeB$6KAR8cjlqzLRQMhbpzSqe.
!
aaa new-model
!
!
aaa group server tacacs+ TACACS-SERVERS
 server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
```

```
aaa authorization console
aaa authorization exec default group TACACS-SERVERS local
!
!
aaa session-id common
clock timezone PST -8 0
clock summer-time PDT recurring
!
ip cef
!
!
ip domain name cisco.local
ip multicast-routing
ip inspect log drop-pkt
no ipv6 cef
!
parameter-map type inspect global
 log dropped-packets enable
 max-incomplete low 18000
 max-incomplete high 20000
 spoofed-acker off
!
multilink bundle-name authenticated
!
!
username admin password 7 094F1F1A1A0A464058
!
redundancy
!
ip ssh source-interface Loopback0
ip ssh version 2
!
track 60 ip sla 110 reachability
!
track 61 ip sla 111 reachability
!
track 62 list boolean or
 object 60
 object 61
!
class-map match-any DATA
 match dscp af21
class-map type inspect match-any INSIDE-TO-OUTSIDE-CLASS
 match protocol ftp
 match protocol tcp
 match protocol udp
 match protocol icmp
```

```
class-map match-any INTERACTIVE-VIDEO
 match dscp cs4  af41
class-map type inspect match-any INSPECT-ACL-OUT-CLASS
 match access-group name ACL-RTR-OUT
class-map match-any CRITICAL-DATA
 match dscp cs3  af31
class-map type inspect match-any PASS-ACL-IN-CLASS
 match access-group name ESP-IN
 match access-group name DHCP-IN
class-map match-any VOICE
 match dscp ef
class-map match-any SCAVENGER
 match dscp cs1  af11
class-map type inspect match-any PASS-ACL-OUT-CLASS
 match access-group name ESP-OUT
 match access-group name DHCP-OUT
class-map match-any NETWORK-CRITICAL
 match dscp cs2  cs6
 match access-group name ISAKMP
class-map type inspect match-any INSPECT-ACL-IN-CLASS
 match access-group name ACL-RTR-IN
!
policy-map WAN
 class VOICE
  priority percent 10
 class INTERACTIVE-VIDEO
  priority percent 23
 class CRITICAL-DATA
  bandwidth percent 15
  random-detect dscp-based
 class DATA
  bandwidth percent 19
  random-detect dscp-based
 class SCAVENGER
  bandwidth percent 5
 class NETWORK-CRITICAL
  bandwidth percent 3
 class class-default
  bandwidth percent 25
  random-detect
policy-map type inspect ACL-OUT-POLICY
 class type inspect INSPECT-ACL-OUT-CLASS
  inspect
 class type inspect PASS-ACL-OUT-CLASS
  pass
 class class-default
  drop
```

```
policy-map type inspect INSIDE-TO-OUTSIDE-POLICY
 class type inspect INSIDE-TO-OUTSIDE-CLASS
  inspect
 class class-default
  drop
policy-map WAN-INTERFACE-G0/0
 class class-default
  shape average 20000000
   service-policy WAN
policy-map type inspect ACL-IN-POLICY
 class type inspect INSPECT-ACL-IN-CLASS
  inspect
 class type inspect PASS-ACL-IN-CLASS
  pass
 class class-default
  drop
!
zone security INSIDE
zone security OUTSIDE
zone-pair security IN_OUT source INSIDE destination OUTSIDE
 service-policy type inspect INSIDE-TO-OUTSIDE-POLICY
zone-pair security TO-ROUTER source OUTSIDE destination self
 service-policy type inspect ACL-IN-POLICY
zone-pair security FROM-ROUTER source self destination OUTSIDE
 service-policy type inspect ACL-OUT-POLICY
!
crypto keyring GLOBAL-KEYRING
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
!
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 2
crypto isakmp keepalive 30 5
crypto isakmp profile ISAKMP-INET-PUBLIC
   keyring GLOBAL-KEYRING
   match identity address 0.0.0.0
!
crypto ipsec security-association replay window-size 1024
!
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256 esp-sha-hmac
 mode transport
!
crypto ipsec profile DMVPN-PROFILE2
 set transform-set AES256/SHA/TRANSPORT
 set isakmp-profile ISAKMP-INET-PUBLIC
!
```

```
!
interface Loopback0
 ip address 10.255.253.242 255.255.255.255
 ip pim sparse-mode
!
interface Tunnel10
 bandwidth 10000
 ip address 10.4.34.242 255.255.254.0
 no ip redirects
 ip mtu 1400
 ip hello-interval eigrp 201 20
 ip hold-time eigrp 201 60
 ip pim dr-priority 0
 ip pim nbma-mode
 ip pim sparse-mode
 ip nhrp authentication cisco123
 ip nhrp map 10.4.34.1 172.16.130.1
 ip nhrp map multicast 172.16.130.1
 ip nhrp network-id 101
 ip nhrp holdtime 600
 ip nhrp nhs 10.4.34.1
 ip nhrp registration no-unique
 ip nhrp shortcut
 ip nhrp redirect
 zone-member security INSIDE
 ip summary-address eigrp 200 10.5.248.0 255.255.248.0
 ip tcp adjust-mss 1360
 tunnel source GigabitEthernet0/0
 tunnel mode gre multipoint
 tunnel route-via GigabitEthernet0/0 mandatory
 tunnel protection ipsec profile DMVPN-PROFILE2
!
interface Port-channel1
 no ip address
!
interface Port-channel1.64
 encapsulation dot1Q 64
 ip address 10.5.252.3 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim dr-priority 105
 ip pim sparse-mode
 ip nat inside
 ip virtual-reassembly in
 zone-member security INSIDE
 standby version 2
 standby 1 ip 10.5.252.1
 standby 1 priority 105
```

```
 standby 1 preempt
 standby 1 authentication md5 key-string 7 104D580A061843595F
!
interface Port-channel1.99
 encapsulation dot1Q 99
 ip address 10.5.248.10 255.255.255.252
 ip pim sparse-mode
 ip nat inside
 ip virtual-reassembly in
 zone-member security INSIDE
!
interface GigabitEthernet0/0
 ip dhcp client default-router distance 10
 ip dhcp client route track 62
 ip address dhcp
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip nat outside
 ip virtual-reassembly in
 zone-member security OUTSIDE
 duplex auto
 speed auto
 no lldp transmit
 no lldp receive
 no cdp enable
 no mop enabled
 service-policy output WAN-INTERFACE-G0/0
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 channel-group 1
!
interface ucse2/0
 ip unnumbered Port-channel1.64
 ip nat inside
 zone-member security INSIDE
 imc ip address 10.5.252.12 255.255.255.0 default-gateway 10.5.252.3
 imc access-port shared-lom console
!
interface ucse2/1
no ip address
!
!
router eigrp 200
```

```
 distribute-list route-map BLOCK-DEFAULT in
 network 10.4.34.0 0.0.1.255
 network 10.5.0.0 0.0.255.255
 network 10.255.0.0 0.0.255.255
 passive-interface default
 no passive-interface Tunnel10
 eigrp router-id 10.255.253.242
 redistribute eigrp 100 route-map LOOPBACK-ONLY
 eigrp stub connected summary redistributed
!
!
router eigrp 100
 network 10.5.0.0 0.0.255.255
 network 10.255.0.0 0.0.255.255
 redistribute eigrp 200
 redistribute static route-map STATIC-IN
 passive-interface default
 no passive-interface Port-channel1.99
!
!
ip local policy route-map PBR-SLA-SET-NEXT-HOP
ip forward-protocol nd
!
no ip http server
ip http authentication aaa
ip http secure-server
!
ip pim autorp listener
ip pim register-source Loopback0
ip nat inside source list NAT interface GigabitEthernet0/0 overload
ip route 10.0.0.0 255.0.0.0 Null0 254
ip route 10.5.252.12 255.255.255.255 ucse2/0
ip route 10.5.252.13 255.255.255.255 ucse2/0
ip route 172.16.130.1 255.255.255.255 GigabitEthernet0/0 dhcp
ip tacacs source-interface Loopback0
!
ip access-list standard DHCP-DEFAULT
 remark DHCP default route
 permit 0.0.0.0
ip access-list standard NAT
 permit 10.5.248.0 0.0.7.255
ip access-list standard NO-DEFAULT
 deny   0.0.0.0
 permit any
ip access-list standard R1-LOOPBACK
 permit 10.255.252.242
ip access-list standard STATIC-ROUTE-LIST
```

```
 remark UCSE CIMC & ESXi host routes
 permit 10.5.252.13
 permit 10.5.252.12
!
ip access-list extended ACL-RTR-IN
 permit udp any any eq non500-isakmp
 permit udp any any eq isakmp
 permit icmp any any echo
 permit icmp any any echo-reply
 permit icmp any any ttl-exceeded
 permit icmp any any port-unreachable
 permit udp any any gt 1023 ttl eq 1
ip access-list extended ACL-RTR-OUT
 permit udp any any eq non500-isakmp
 permit udp any any eq isakmp
 permit icmp any any
ip access-list extended DHCP-IN
 permit udp any eq bootps any eq bootpc
ip access-list extended DHCP-OUT
 permit udp any eq bootpc any eq bootps
ip access-list extended ESP-IN
 permit esp any any
ip access-list extended ESP-OUT
 permit esp any any
ip access-list extended ISAKMP
 permit udp any eq isakmp any eq isakmp
ip access-list extended SLA-SET-NEXT-HOP
 permit icmp any host 172.18.1.253
 permit icmp any host 172.18.1.254
!
ip sla auto discovery
ip sla 110
 icmp-echo 172.18.1.253 source-interface GigabitEthernet0/0
 threshold 1000
 frequency 15
ip sla schedule 110 life forever start-time now
ip sla 111
 icmp-echo 172.18.1.254 source-interface GigabitEthernet0/0
 threshold 1000
 frequency 15
ip sla schedule 111 life forever start-time now
!
nls resp-timeout 1
cpd cr-id 1
route-map PBR-SLA-SET-NEXT-HOP permit 10
 match ip address SLA-SET-NEXT-HOP
 set ip next-hop dynamic dhcp
```

```
!
route-map LOCAL-DEFAULT permit 10
 match ip address DHCP-DEFAULT
!
!
route-map LOOPBACK-ONLY permit 10
 match ip address R1-LOOPBACK
!
route-map BLOCK-DEFAULT permit 10
 match ip address NO-DEFAULT
!
route-map STATIC-IN permit 20
 match ip address STATIC-ROUTE-LIST
!
!
snmp-server community cisco RO
snmp-server community cisco123 RW
snmp-server trap-source Loopback0
snmp-server enable traps entity-sensor threshold
tacacs server TACACS-SERVER-1
 address ipv4 10.4.48.15
 key 7 073C244F5C0C0D2E120B
!
!
!
control-plane
!
!
line con 0
 logging synchronous
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line 131
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
 speed 9600
 flowcontrol software
line vty 0 4
```

```
 transport preferred none
 transport input ssh
line vty 5 15
 transport preferred none
 transport input ssh
!
scheduler allocate 20000 1000
ntp source Loopback0
ntp server 10.4.48.17
!
end
```

## Feedback

Please use the feedback form to send comments and suggestions about this guide.


**Americas Headquarters**
Cisco Systems, Inc.
San Jose, CA

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

**Europe Headquarters**
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.





B-0000175-1 12/13