

Hosted Cloud Connector Using Cisco UCS E-Series

Technology Design Guide

August 2014 Series



Table of Contents

Preface	1
CVD Navigator	2
Use Cases	2
Scope	2
Proficiency.....	2
Introduction	3
Related Reading	3
Technology Use Cases	3
Use Case: Remote Site Hosted Cloud Connector Applications.....	4
Design Overview.....	4
UCS E-Series Integrated Servers	5
Cloud Storage Connectors	6
Deploying Hosted Cloud Applications	7
Router Selection for Remote Sites	7
Deploying Hosted Cloud Connectors on UCS E-Series Servers	8
Single Router Remote-Site Designs.....	10
Dual Router Remote-Site Designs	13
Installing and Configuring the UCS E-Series Server Module	16
Installing VMware ESXi on the UCS E-Series Server Module	28
Deploying Hosted Cloud Storage Applications on the UCS E-Series Server Module.....	61
Appendix A: Product List	65
Appendix B: Configurations	66
Remote Site 240	66
RS240-3945	66
Remote Site 242	76
RS242-2951-1	76
RS242-2951-2.....	83
Appendix C: Changes	93

Preface

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

CVDs include two guide types that provide tested design 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 existing CVDs but also include product features and functionality across Cisco products and sometimes 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.

CVD Foundation Series

This CVD Foundation guide is a part of the *August 2014 Series*. As Cisco develops a CVD Foundation series, the guides themselves are tested together, in the same network lab. This approach assures that the guides in a series are fully compatible with one another. Each series describes a lab-validated, complete system.

The CVD Foundation series incorporates wired and wireless LAN, WAN, data center, security, and network management technologies. Using the CVD Foundation simplifies system integration, allowing you to select solutions that solve an organization's problems—without worrying about the technical complexity.

To ensure the compatibility of designs in the CVD Foundation, you should use guides that belong to the same release. For the most recent CVD Foundation guides, please visit [the CVD Foundation web site](#).

Comments and Questions

If you would like to comment on a guide or ask questions, please use the [feedback form](#).

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.

The CVD Navigator helps you determine the applicability of this guide by summarizing its key elements: 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 CVD Foundation web site](#).

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

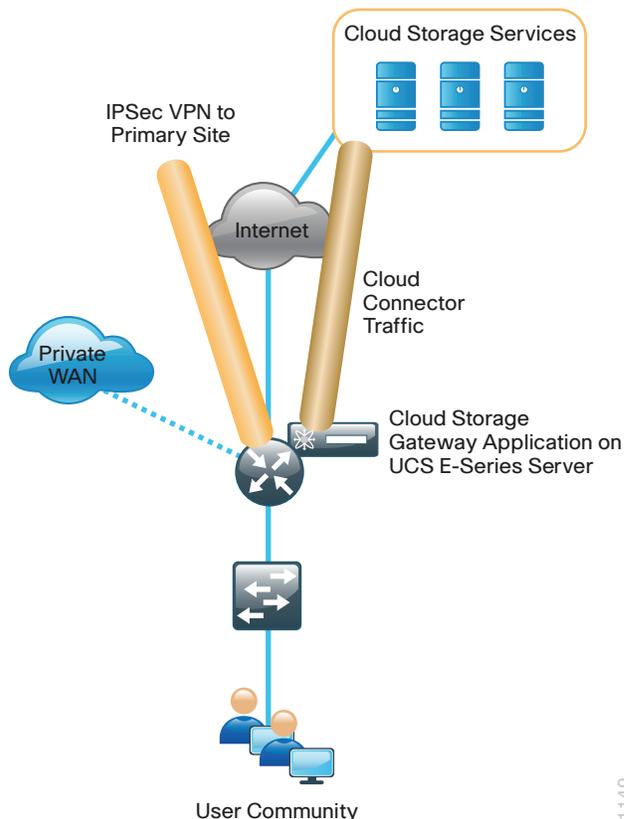
The [Remote Site Using Local Internet Access Technology Design Guide](#) provides guidance and configuration for deploying remote site WAN connectivity with Local Internet Access.

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



1149

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.

Deploying Hosted Cloud Applications

How to Read Commands

This guide uses the following conventions for commands that you enter at the command-line interface (CLI).

Commands to enter at a CLI prompt:

```
configure terminal
```

Commands that specify a value for a variable:

```
ntp server 10.10.48.17
```

Commands with variables that you must define:

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

Commands at a CLI or script prompt:

```
Router# enable
```

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

```
police rate 10000 pps burst 10000  
packets conform-action
```

Noteworthy parts of system output (or of device configuration files) are highlighted:

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

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

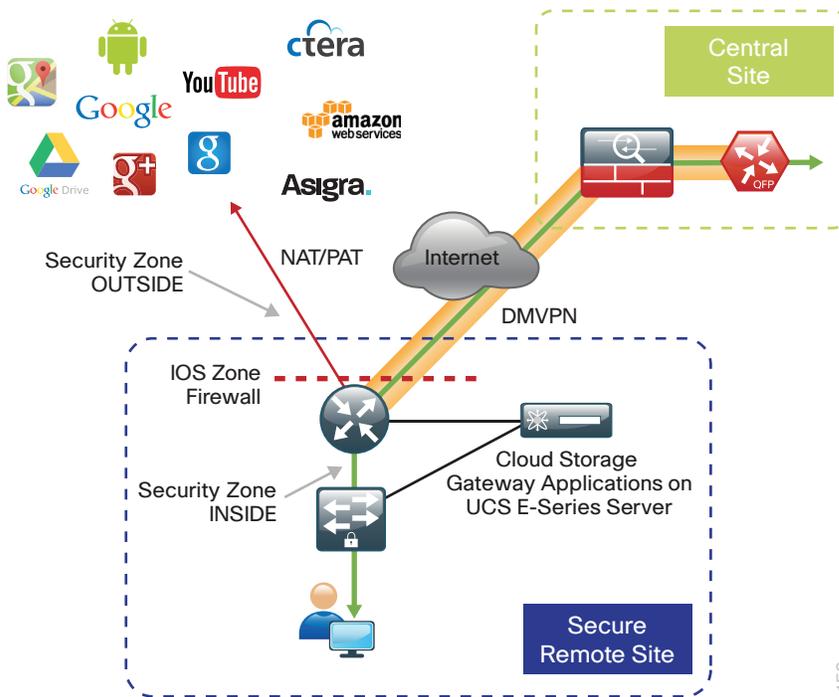
Option	2911	2921	2951	3925	3945
Ethernet WAN with services ¹	35 Mbps	50 Mbps	75 Mbps	100 Mbps	150 Mbps
On-board FE ports	0	0	0	0	0
On-board GE ports ²	3	3	3	3	3
Service module slots	1	1	2	2	4
Redundant power supply option	No	No	No	Yes	Yes
Supported UCS E-Series Server module	UCS E140S	UCS E140S UCS E140D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

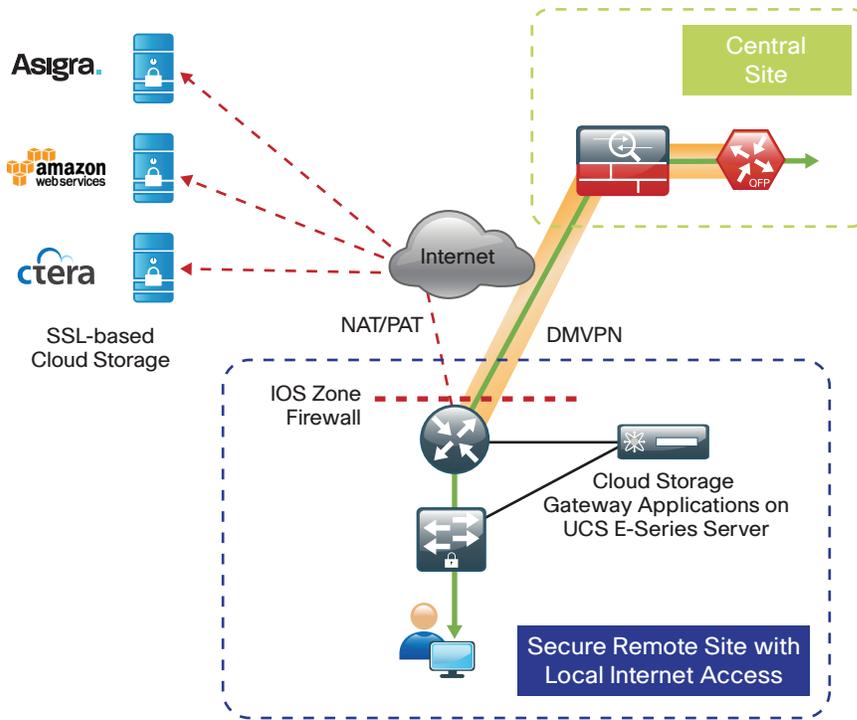
These applications allow remote-site locations to backup data directly to the cloud for disaster recovery (DR) and continuity of operations (COOP) requirements. Local Internet access provides increased performance for cloud-based applications as well as reduces bandwidth utilization on more expensive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



i 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

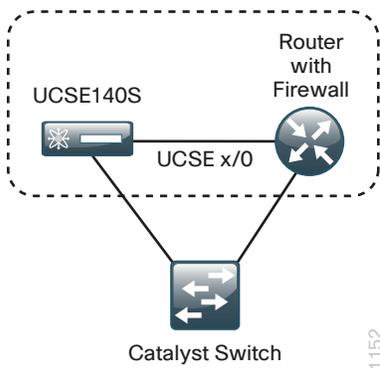
In the single router VPN WAN design, you install a single or double-wide UCS E-Series Server module into the ISRG2 router.

i 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.

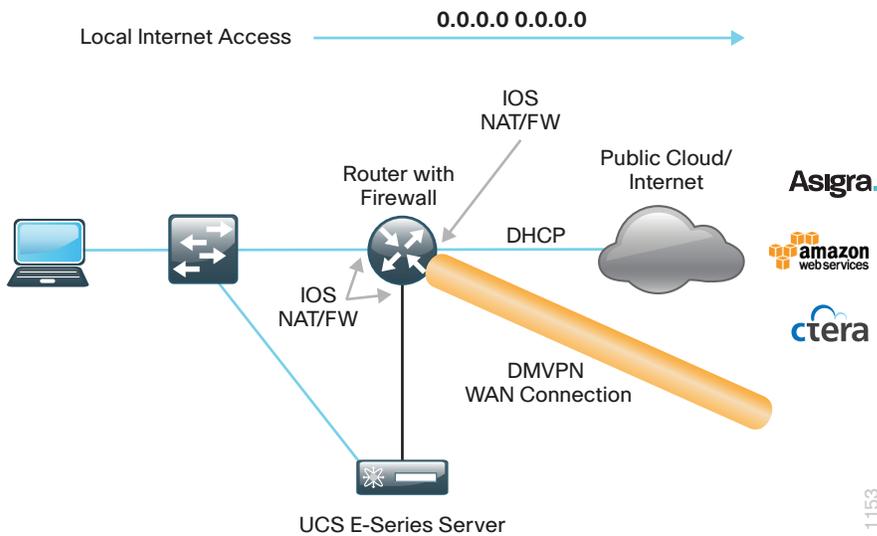
Figure 5 - Cisco ISRG2 router with integrated UCS E-Series Server



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.

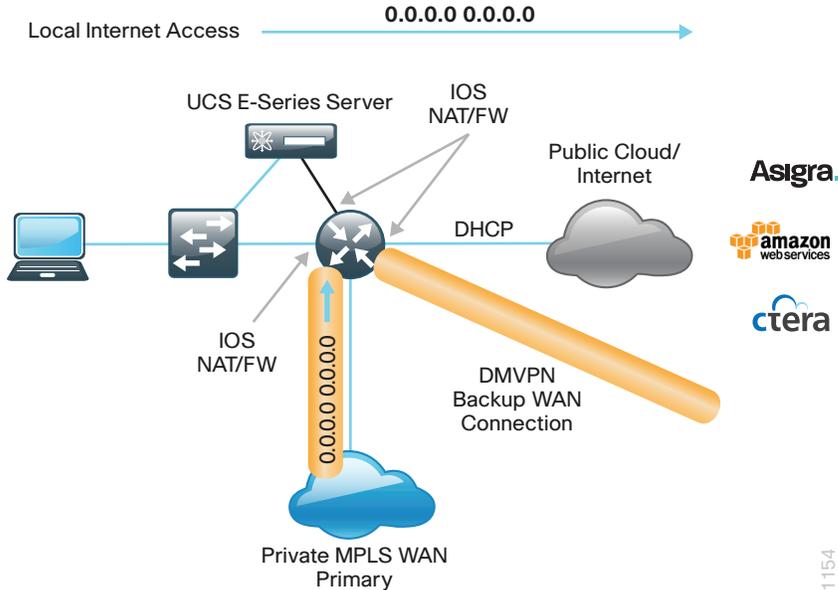
Figure 6 - Single router VPN WAN - UCS E-Series Server



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.

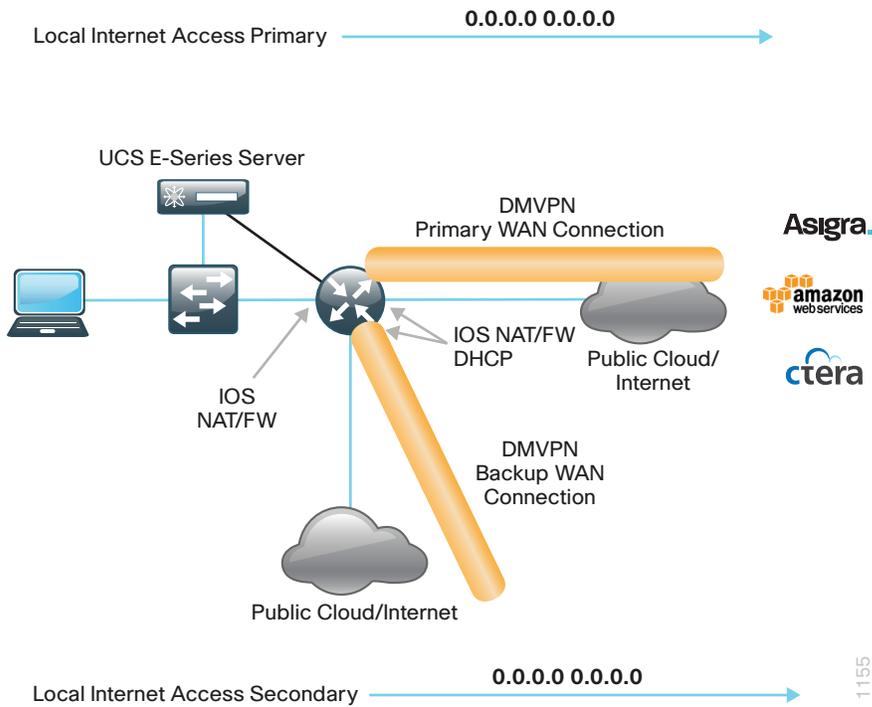
Figure 7 - MPLS WAN & L2 WAN primary with VPN backup - UCS E-Series Server



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



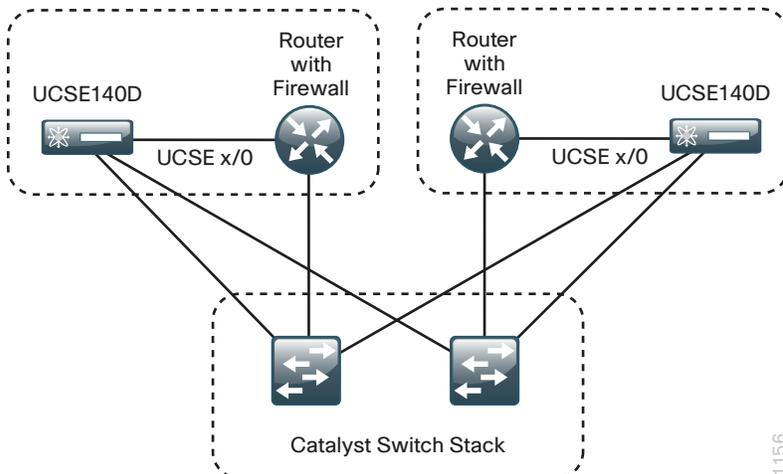
Dual Router Remote-Site Designs

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.

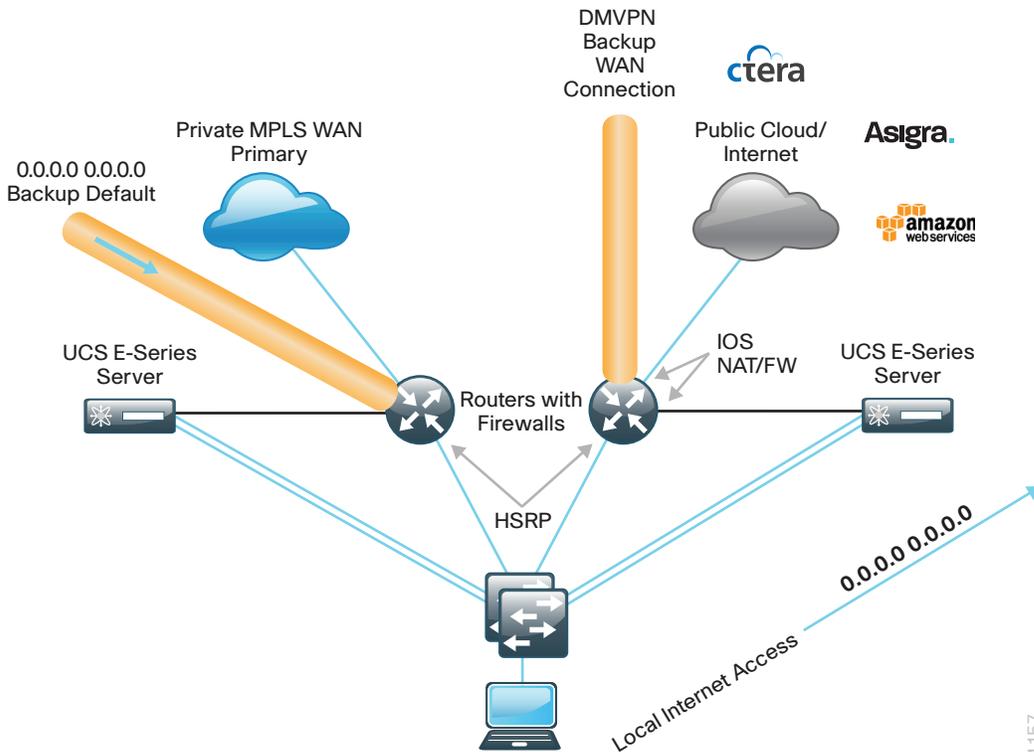
Figure 9 - Cisco ISRG2 routers with integrated UCS E-Series Servers



In dual router MPLS Primary or L2 WAN primary with VPN WAN backup, you install a UCS E-Series Server module into each ISR2G2 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.

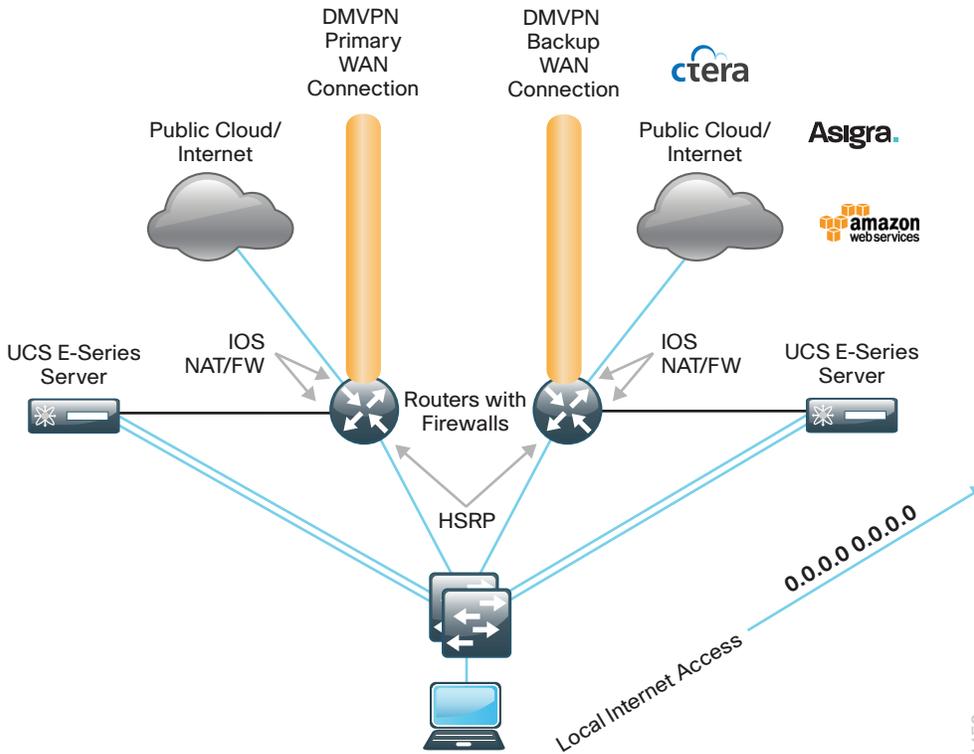
Figure 10 - MPLS primary backup link and router - UCS E-Series Server



In the dual router Dual VPN WAN, you install a UCS E-Series Server module into each ISR2G2 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



1158

i 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.

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 by 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
  load-interval 30
  no shutdown
  macro apply EgressQoS
```

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
  load-interval 30
  no shutdown
```

```

macro apply EgressQoS

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
load-interval 30
no shutdown
macro apply EgressQoS

```



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

```
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

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: On Internet-facing routers that provide local Internet services, add the UCS-E Series interface to the inside security zone.

```
interface ucse2/0
  zone-member security INSIDE
```

Reader Tip

For more information on Zone Based firewall, see the [Remote Site Using Local Internet Access Technology Design Guide](#).

Step 5: 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 6: 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 7: If this is a dual router remote site, you must redistribute the static routes created in Step 4 and Step 6 into the LAN EIGRP process (AS 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 LAN
  address-family ipv4 unicast autonomous-system 100
  topology base
  redistribute static route-map STATIC-IN
  exit-af-topology
  exit-address-family
```

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 LAN
  address-family ipv4 unicast autonomous-system 100
  network 10.5.0.0 0.0.255.255
  exit-address-family
```

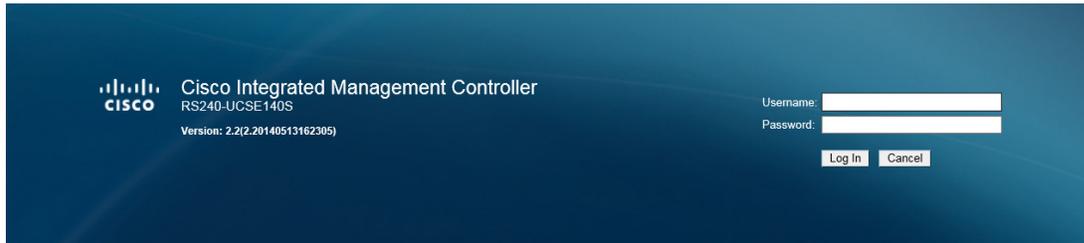
A pseudo-connected route is treated like a connected route and is automatically advertised within the EIGRP autonomous system as an EIGRP internal route (AD 90) and no redistribution is required.

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.

Next, verify the CIMC configuration.

Step 8: 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 9: 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. The following example shows the Cisco UCS E-Series Server module installed in slot 3 of the router.

```
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

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: On Internet-facing routers that provide local Internet services, add the UCS-E Series interface to the inside security zone.

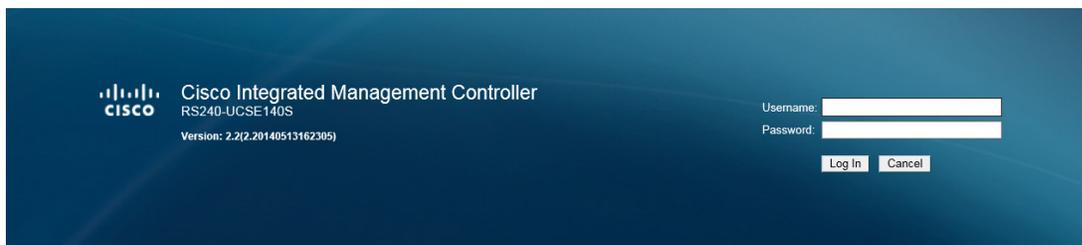
```
interface ucse3/0
 zone-member security INSIDE
```



Reader Tip

For more information on Zone Based firewall, see the [Remote Site Using Local Internet Access Technology Design Guide](#).

Step 6: 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 7: 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**.

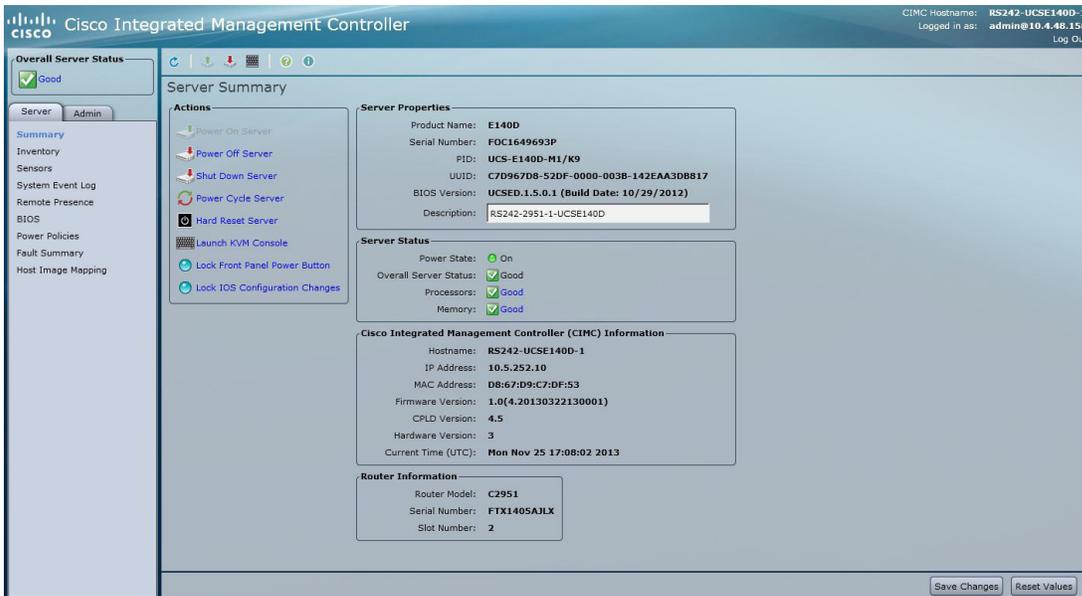


The image shows a web interface titled "First Login" with a green question mark icon. Below the title, it says "Please change your password". There are two input fields: "New Password:" and "Confirm New Password:". At the bottom, there are two buttons: "Save Changes" and "Reset Values".

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**.



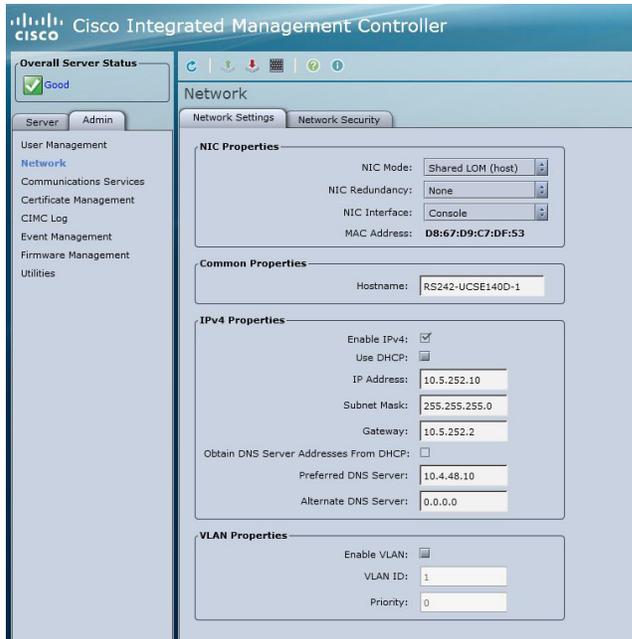
The image shows the Cisco Integrated Management Controller (CIMC) interface. The top bar displays "Cisco Integrated Management Controller" and "CIMC Hostname: RS242-UCSE1400-1". The main content area is titled "Server Summary" and is divided into several sections:

- Overall Server Status:** Shows a green checkmark and "Good".
- Actions:** Includes buttons for Power On Server, Power Off Server, Shut Down Server, Power Cycle Server, Hard Reset Server, Launch KVM Console, Lock Front Panel Power Button, and Lock IOS Configuration Changes.
- Server Properties:**
 - Product Name: E140D
 - Serial Number: FOC1649693P
 - PID: UCS-E140D-M1/K9
 - UUID: C7D967D8-52DF-0000-0038-142EAA3D8817
 - BIOS Version: UCSED.1.5.0.1 (Build Date: 10/29/2012)
 - Description: RS242-2951-1-UCSE140D
- Server Status:**
 - Power State: On
 - Overall Server Status: Good
 - Processors: Good
 - Memory: Good
- Cisco Integrated Management Controller (CIMC) Information:**
 - Hostname: RS242-UCSE1400-1
 - IP Address: 10.5.252.10
 - MAC Address: D8:67:D9:C7:DF:53
 - Firmware Version: 1.0(4.20130322130001)
 - CPLD Version: 4.5
 - Hardware Version: 3
 - Current Time (UTC): Mon Nov 25 17:08:02 2013
- Router Information:**
 - Router Model: C2951
 - Serial Number: FTX1405AJLX
 - Slot Number: 2

At the bottom right, there are "Save Changes" and "Reset Values" buttons.

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 by using CIMC

Verify whether or not your UCS E-Series already has a virtual drive with RAID configured. If a virtual drive exists, you may skip Step 2 through Step 11.

Step 1: Click on the **Server** tab, select **RAID**.

Figure 12 - UCS E-Series with an existing virtual drive

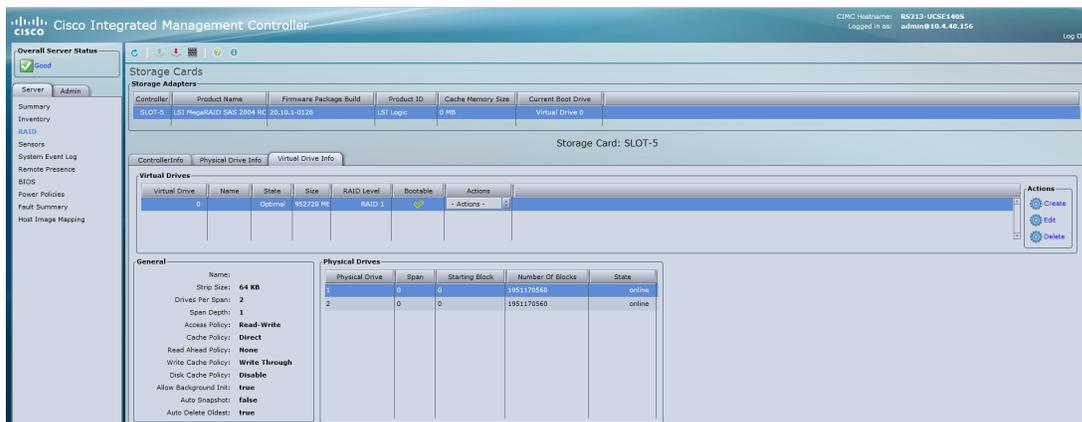
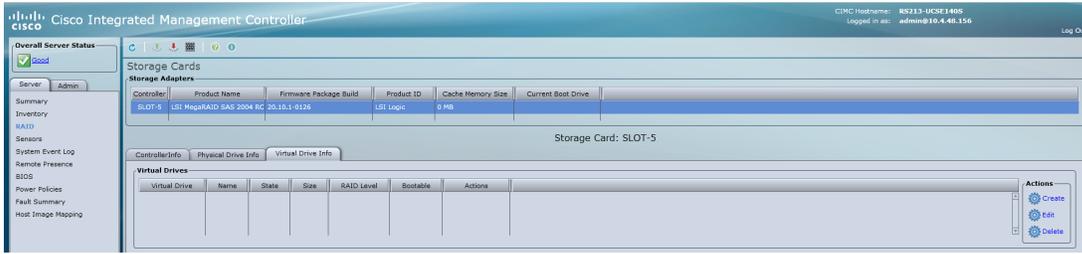
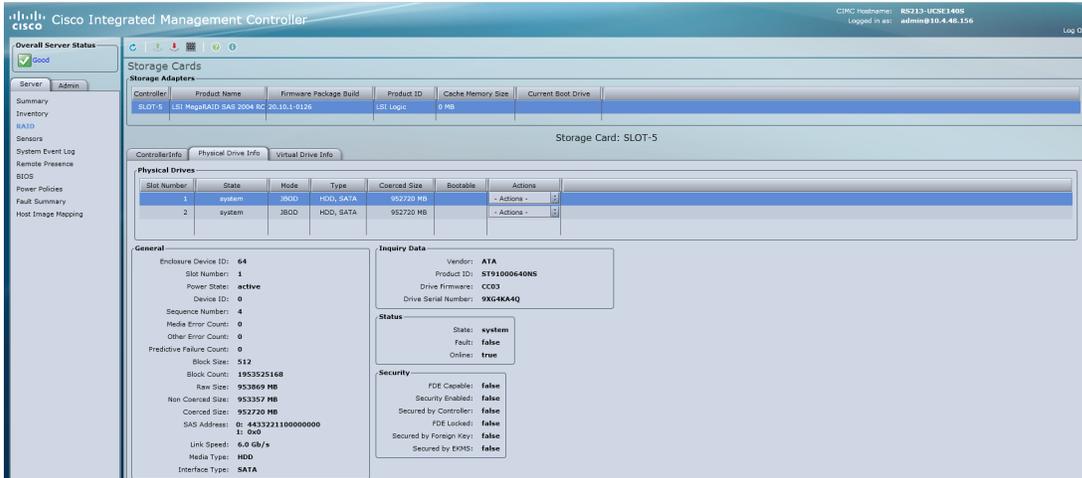


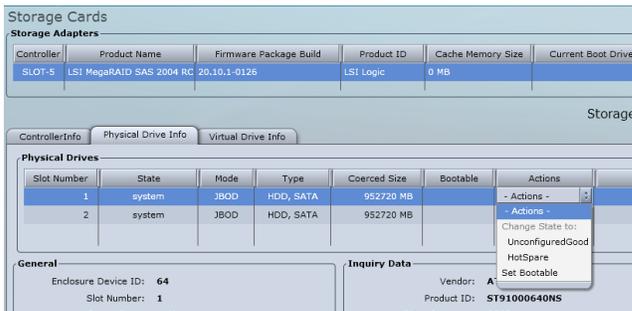
Figure 13 - UCS E-Series requiring the configuration of a virtual drive



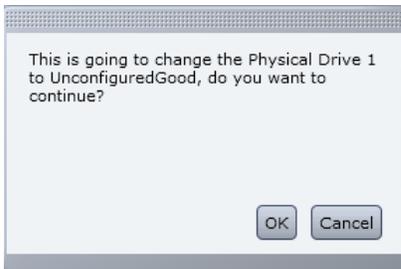
Step 2: Click the Physical Drive Info tab.



Step 3: For the drive in Slot Number 1, choose UnconfiguredGood from the Actions list.



Step 4: At the warning message, click OK.



Step 5: For any remaining drives, repeat Step 3 and Step 4.

Step 6: Verify that the state of all of the drives is **unconfigured good**.

The screenshot shows the 'Storage Cards' page in the Cisco IMC. Under 'Storage Adapters', there is a table with one entry: SLOT-5, LSI MegaRAID SAS 2004 RC, 20.10.1-0126, LSI Logic, 0 MB. Below this, the 'Physical Drives' tab is active, showing a table with two drives, both in 'unconfigured good' state.

Controller	Product Name	Firmware Package Build	Product ID	Cache Memory Size	Current Boot Drive
SLOT-5	LSI MegaRAID SAS 2004 RC	20.10.1-0126	LSI Logic	0 MB	

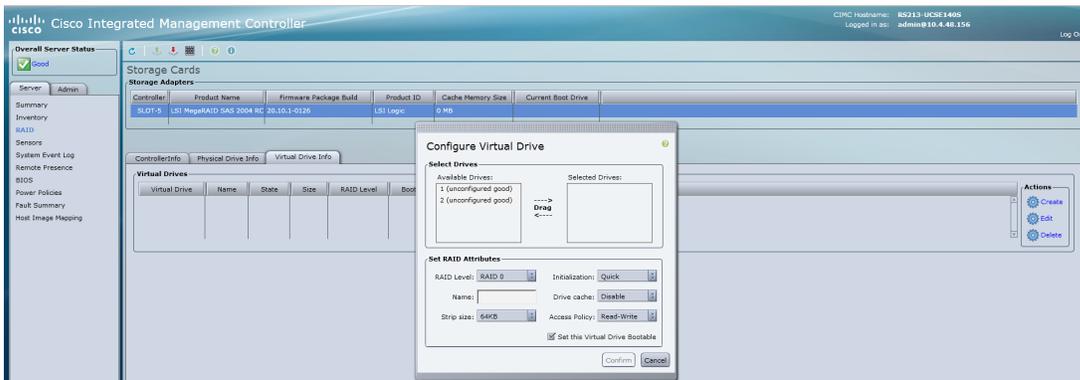
Slot Number	State	Mode	Type	Coerced Size	Bootable	Actions
1	unconfigured good		HDD, SATA	952720 MB		- Actions -
2	unconfigured good		HDD, SATA	952720 MB		- Actions -

Step 7: Click the **Virtual Drive Info** tab and then in the **Actions** pane, click **Create**.

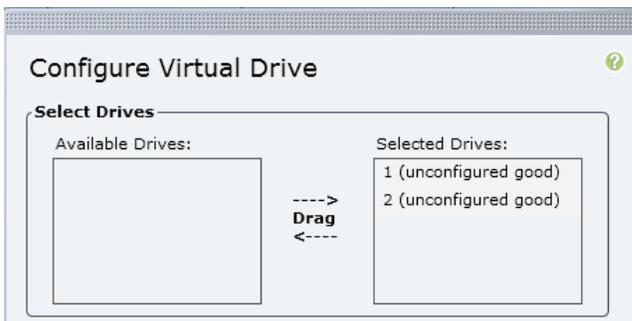


Tech Tip

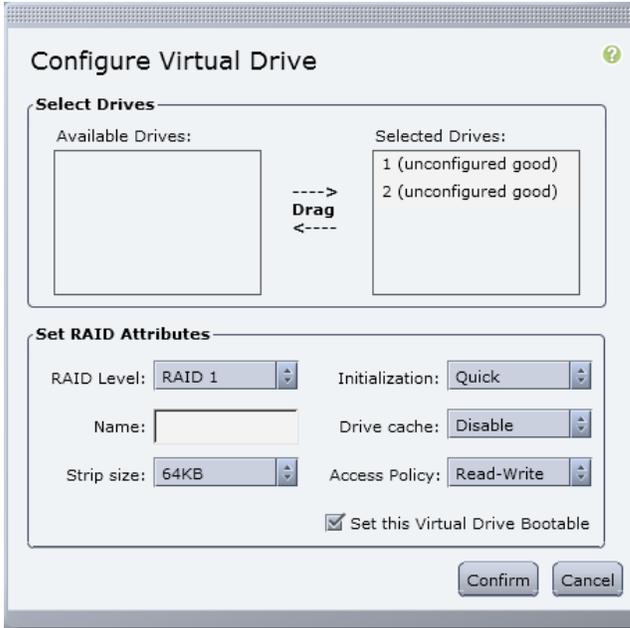
If you are configuring a Cisco UCS E-Series module with a single hard drive, you can select **RAID 0** and add the single drive to the list. Using two drives is recommended when possible.



Step 8: In the **Configure Virtual Drive** window, select the drives to be included in the RAID configuration, and then drag them from the Available Drives column to the Selected Drives column.

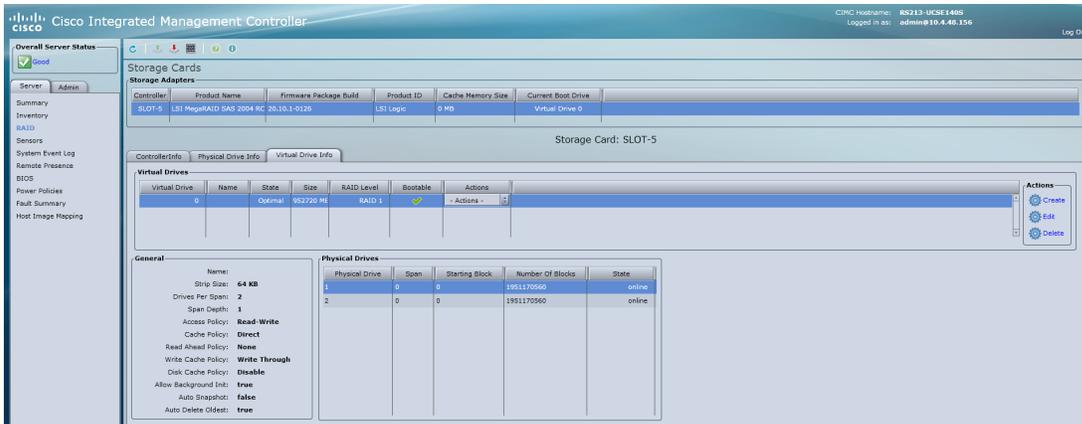


Step 9: Select RAID Level **RAID 1** from the drop down menu. If your system has only a single drive, select RAID Level **RAID 0** (this will be the only available option).



Step 10: Select **Set this Virtual Drive Bootable**, and then click **Confirm**.

Step 11: Navigate to the **Server** tab, select **RAID**, click the **Virtual Drive Info** tab, and then verify that the virtual and physical drives are properly assigned.



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 U2 GA Install CD**, click **Go to Downloads**.

Custom ISOs	Release Date	
OEM Customized Installer CDs		
HP Custom Image for ESXi 5.1.0 Update 2 Install CD	2014-06-17	Go to Downloads
Cisco Custom Image for ESXi 5.1.0 U2 GA Install CD	2014-03-15	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.

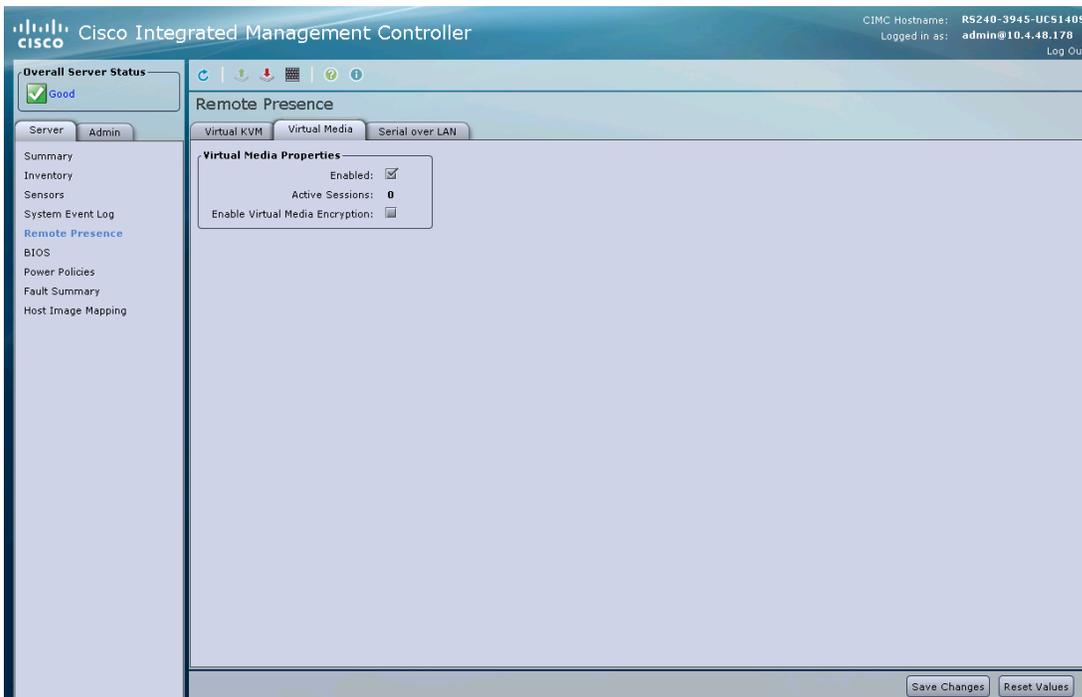
Tech Tip

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.

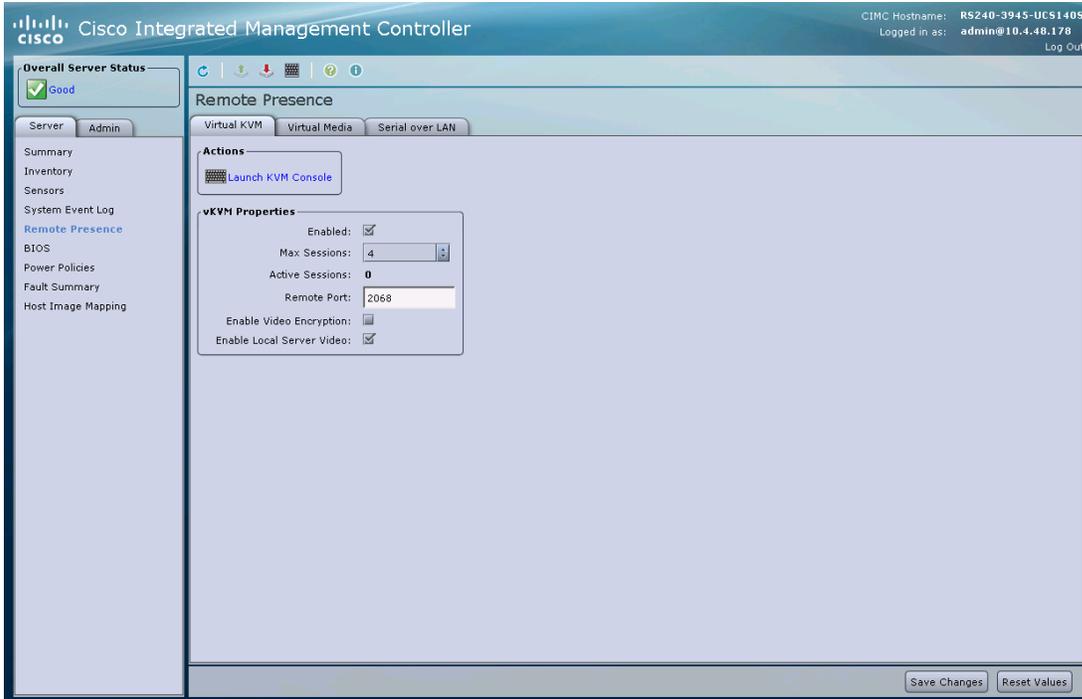
Step 1: Using your web browser, navigate to the CIMC address of the UCS E-Series Server module and log in (Examples: <https://10.5.252.10> and `admin/c1sco123`).

Step 2: Accept any messages regarding untrusted certificates.

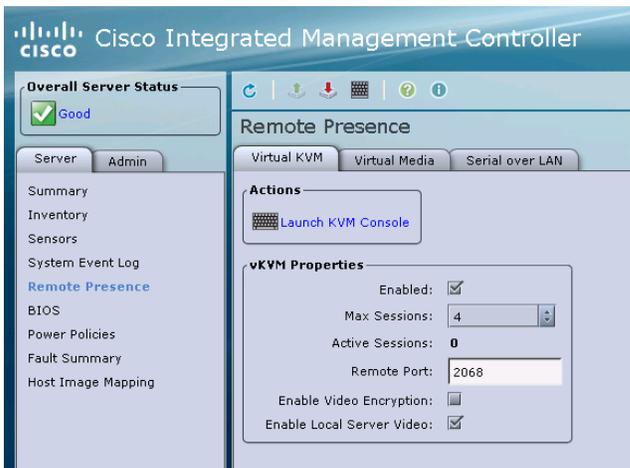
Step 3: In the **Server** tab, click **Remote Presence**, click the **Virtual Media** tab, and then ensure the **Enabled** check box is selected.



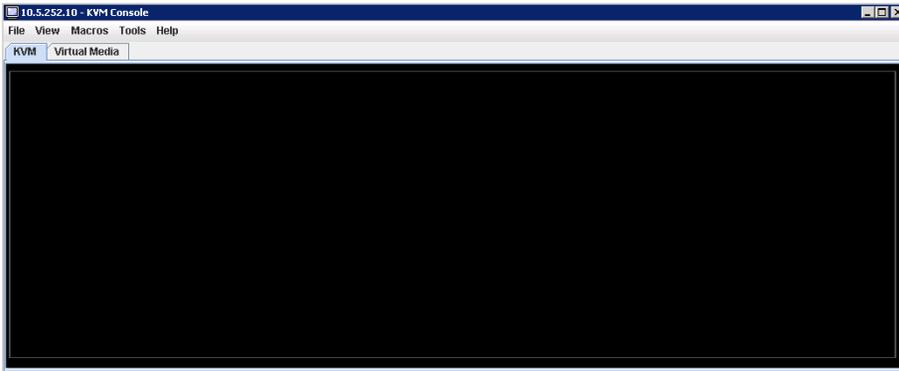
Step 4: Click the **Virtual KVM** tab, and then ensure the **Enabled** check box is selected.



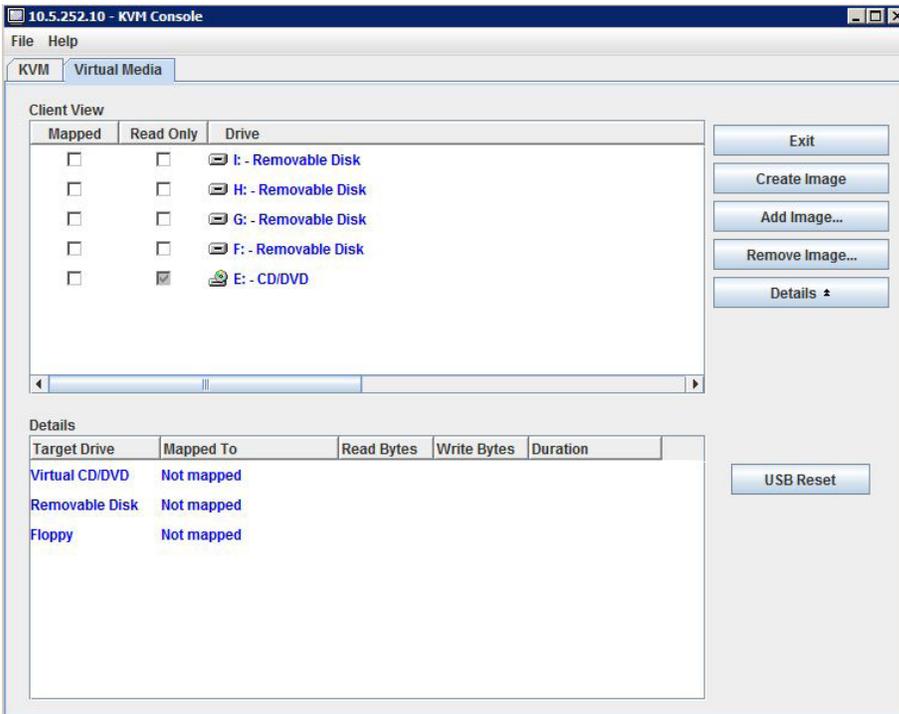
Step 5: On the **Virtual KVM** tab, under **Actions** click **Launch KVM Console**, and then accept any security warnings. The virtual KVM Console window opens.



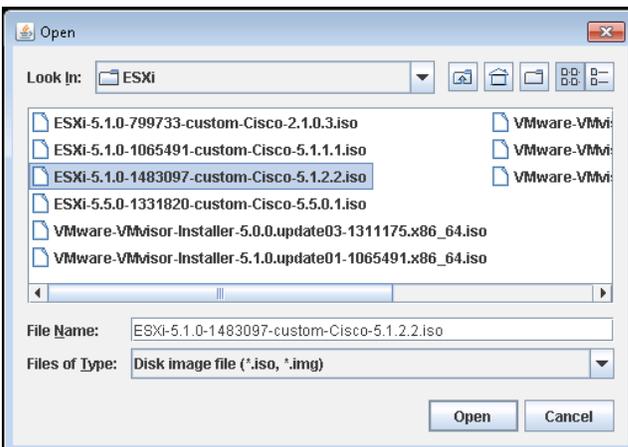
Step 6: In the KVM Console window, click the **Virtual Media** tab.



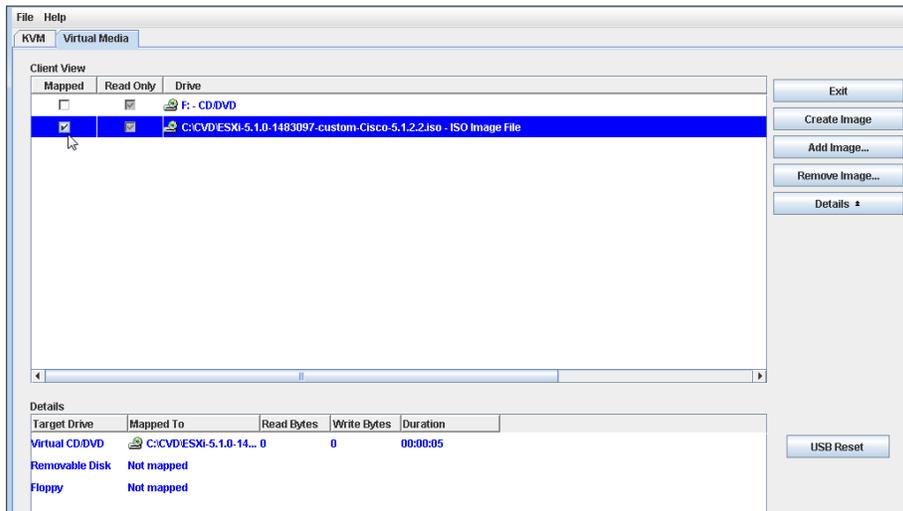
Step 7: In the KVM Console window, click **Add Image**.



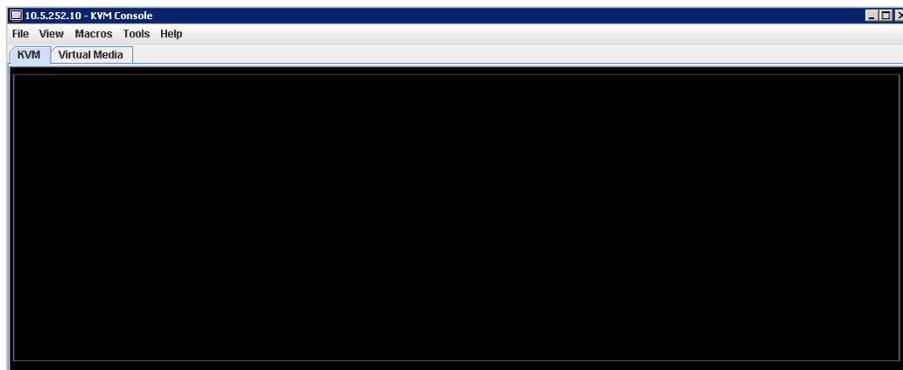
Step 8: Browse to the VMware ESXi ISO image, and then click **Open**.



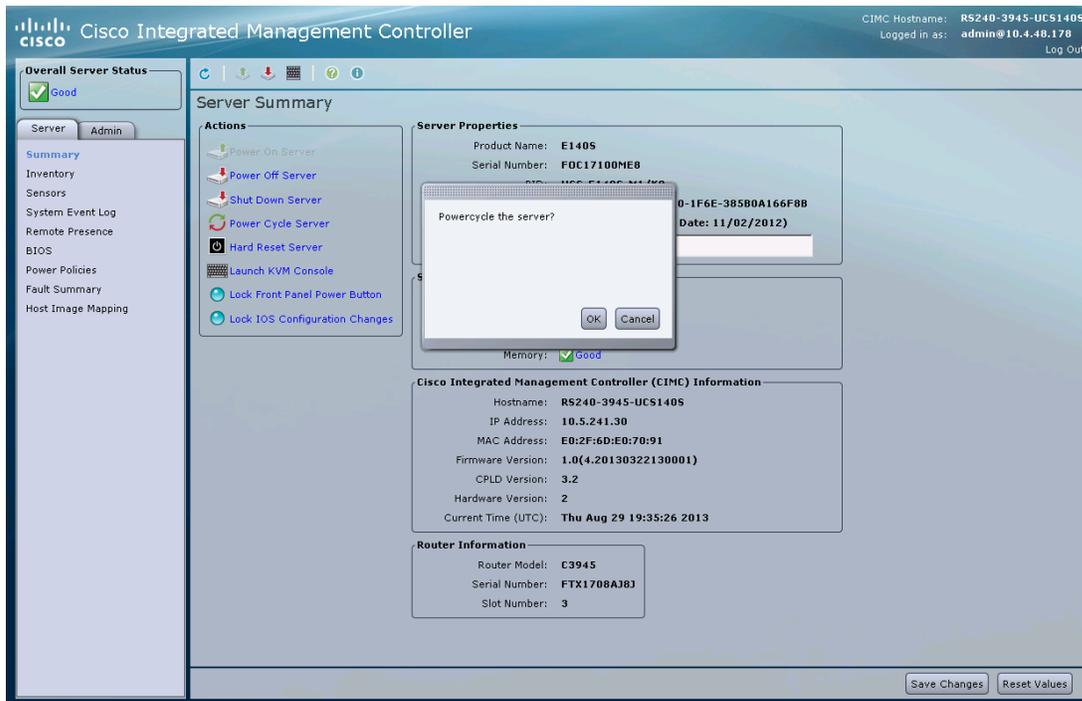
Step 9: For the newly added image, select **Mapped**. This maps the ISO file and completes the mount.



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.

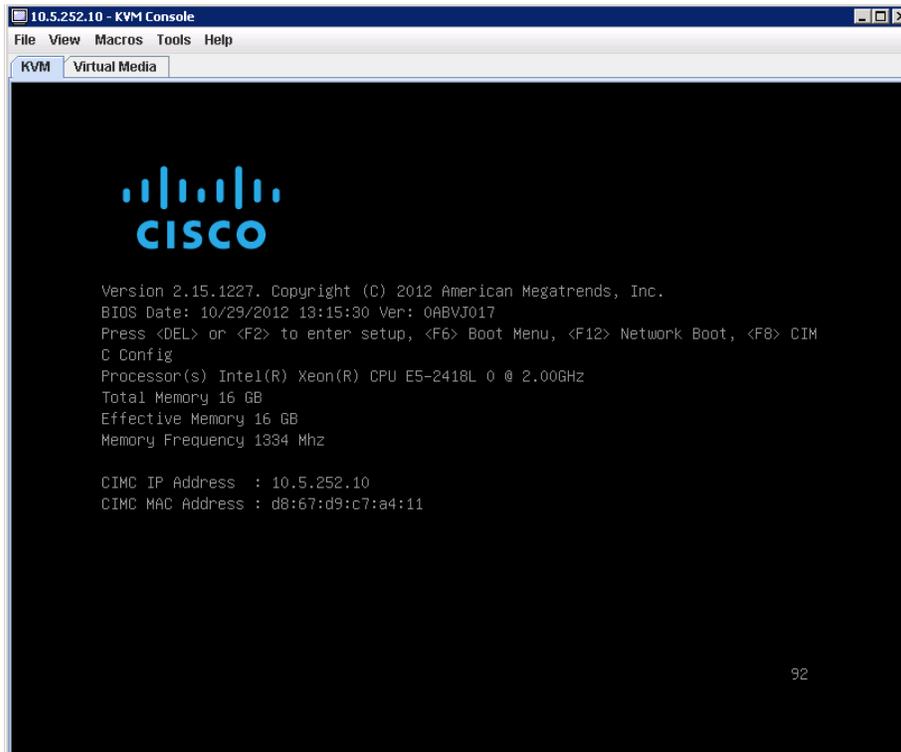


Step 12: Monitor the KVM Console window as the server boots, and, when prompted, enter the BIOS setup by pressing **F2**.

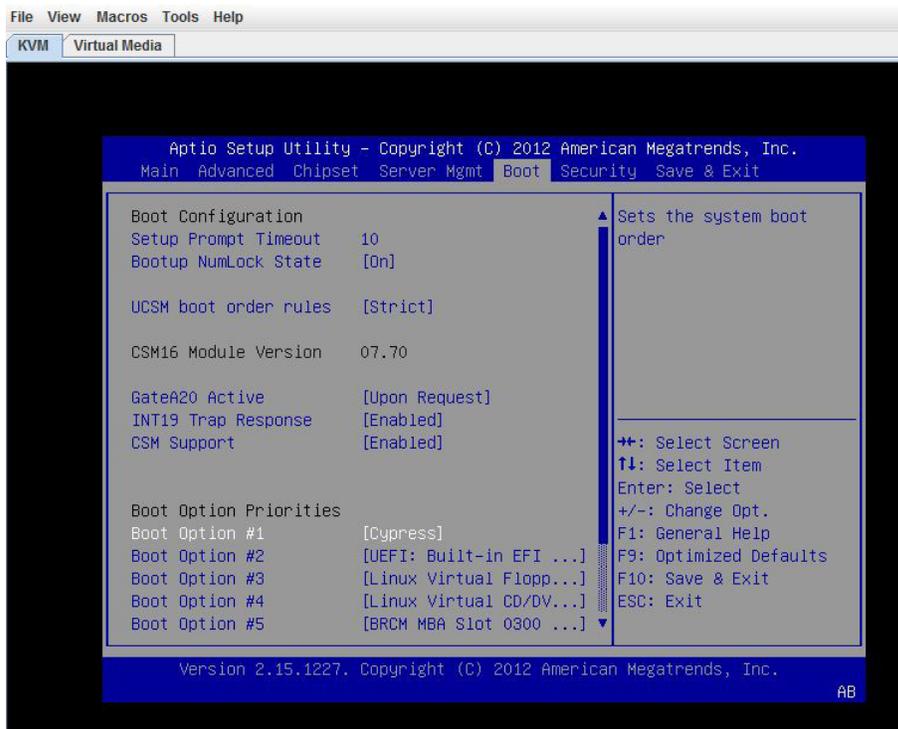
Step 13: When prompted, enter the password (Example: c1sco123). If this is the first time entering the BIOS, you are prompted to set a BIOS password (Example: c1sco123).

Tech Tip

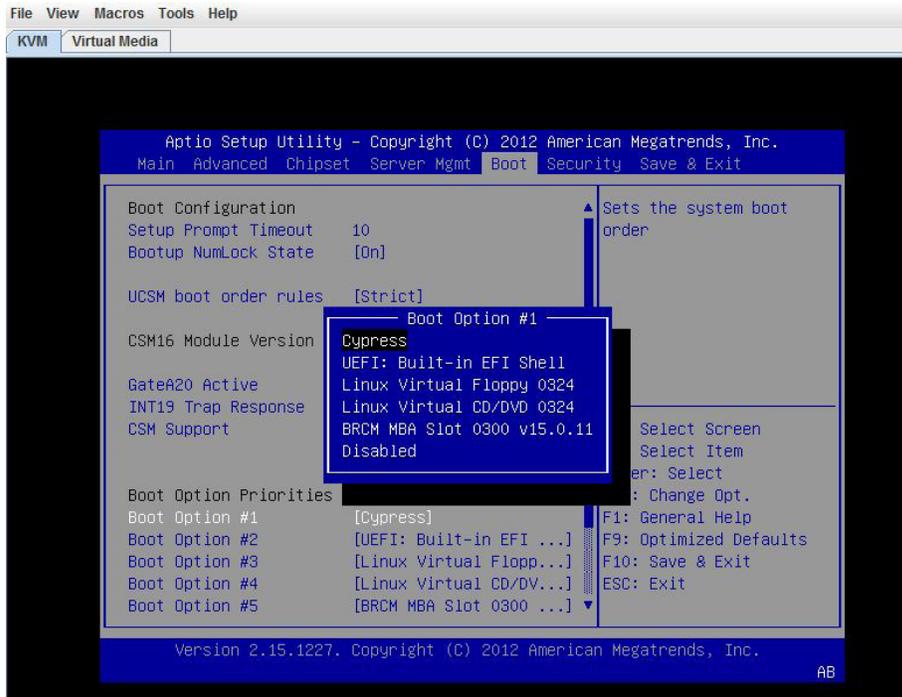
Pay close attention to the KVM console; the **F2** command is accepted for only a short period of time. If you fail to enter the BIOS setup, you must power cycle the server using CIMC and try again.



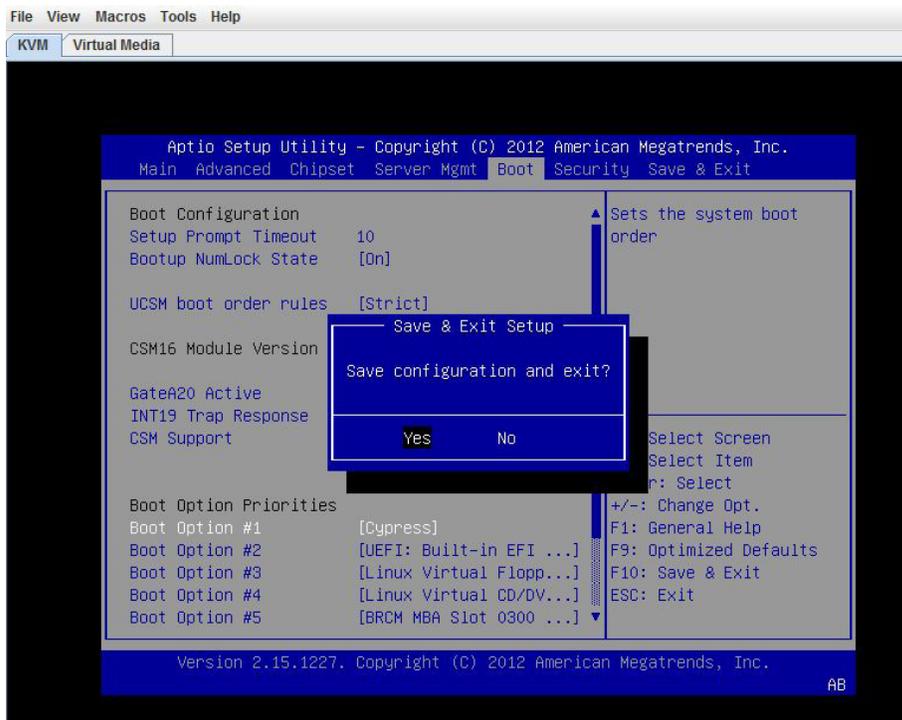
Step 14: Using the arrows on your keyboard, navigate to the **Boot** tab, highlight **Boot Option #1**, and then press **Enter**.



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

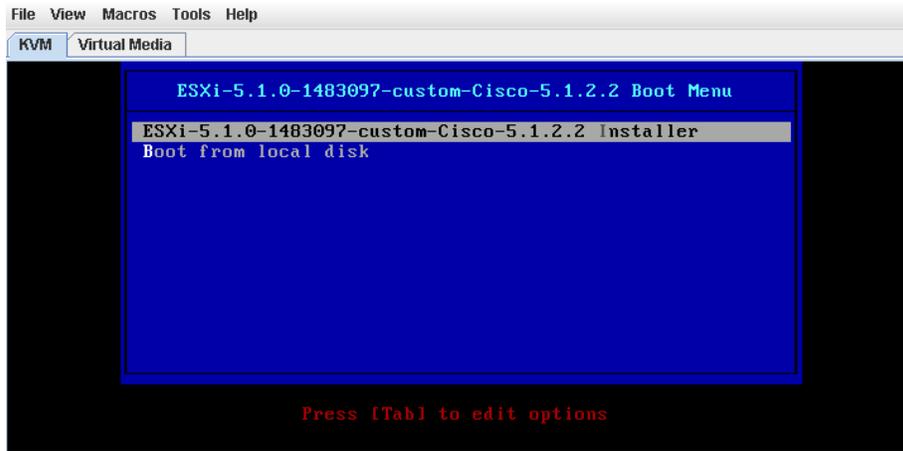


Step 16: Press **F10**. In the save and exit dialog box, choose **Yes**, and then press **Enter**. This saves the BIOS settings and exits BIOS. The system reboots.



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.

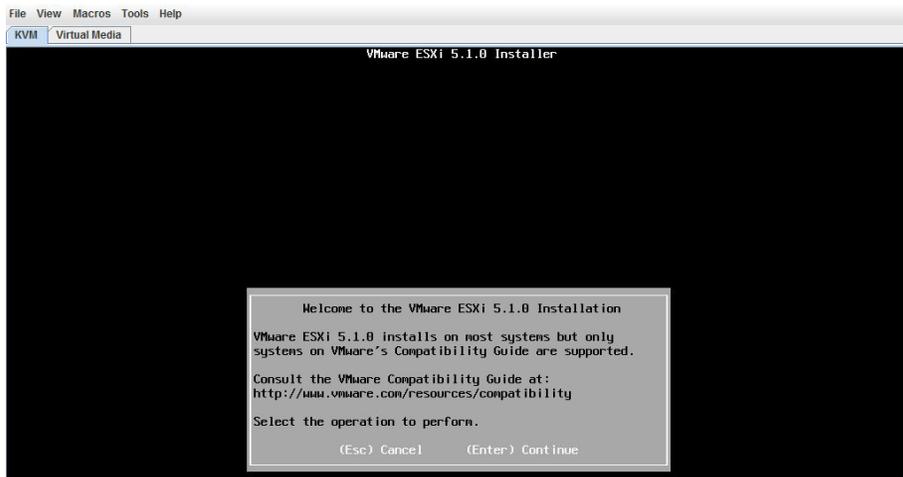
Step 18: When the VMware VMvisor Boot Menu appears, select ESXi Installer



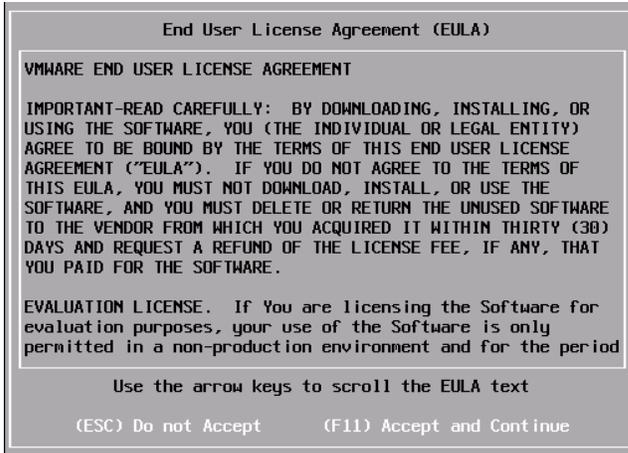
Tech Tip

If the VMvisor Boot Menu shown above does not load, one possible reason is that ESXi is already installed on the UCS-E flash. To force the boot-up sequence to use the remote media, enter the boot menu by pressing F6 instead of F2 during the BIOS POST and select the virtual CV/DVD as the preferred boot device instead of Cypress.

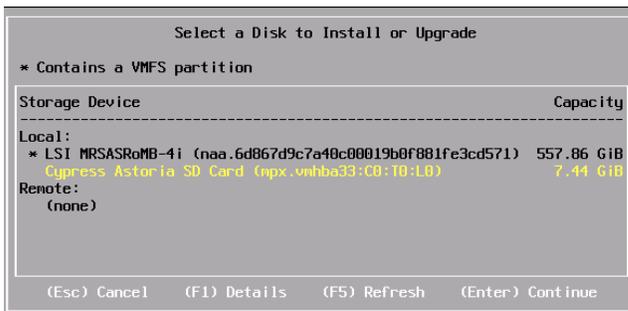
Step 19: In the Welcome dialog box, choose **Enter**. The installation of ESXi begins.



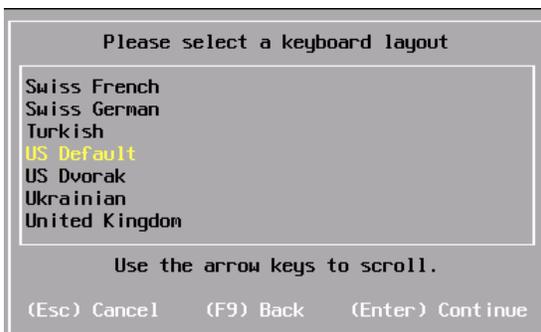
Step 20: Accept the End User License Agreement (EULA) by pressing F11.



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).

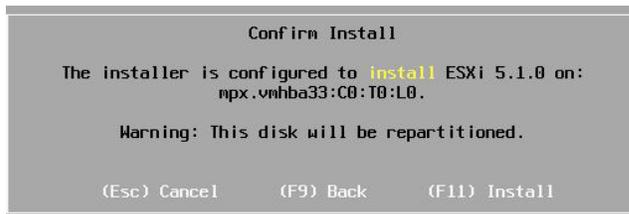


Please enter a root password (recommended)

Root password: _
Confirm password:

(Esc) Cancel (F9) Back (Enter) Continue

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.



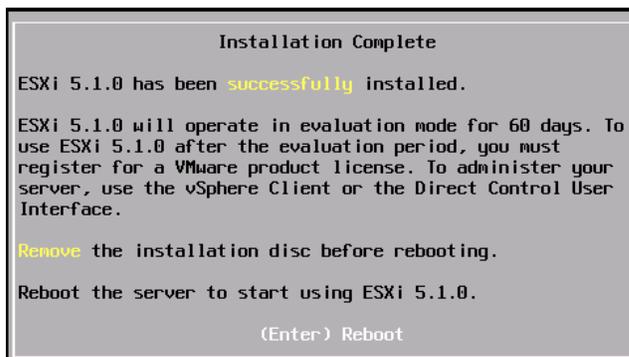
Confirm Install

The installer is configured to **install** ESXi 5.1.0 on:
npx.vnhba33:C0:T0:L0.

Warning: This disk will be repartitioned.

(Esc) Cancel (F9) Back (F11) Install

After the installation process finishes, The Installation Complete message appears. Do not reboot the server until after you complete Step 25.



Installation Complete

ESXi 5.1.0 has been **successfully** installed.

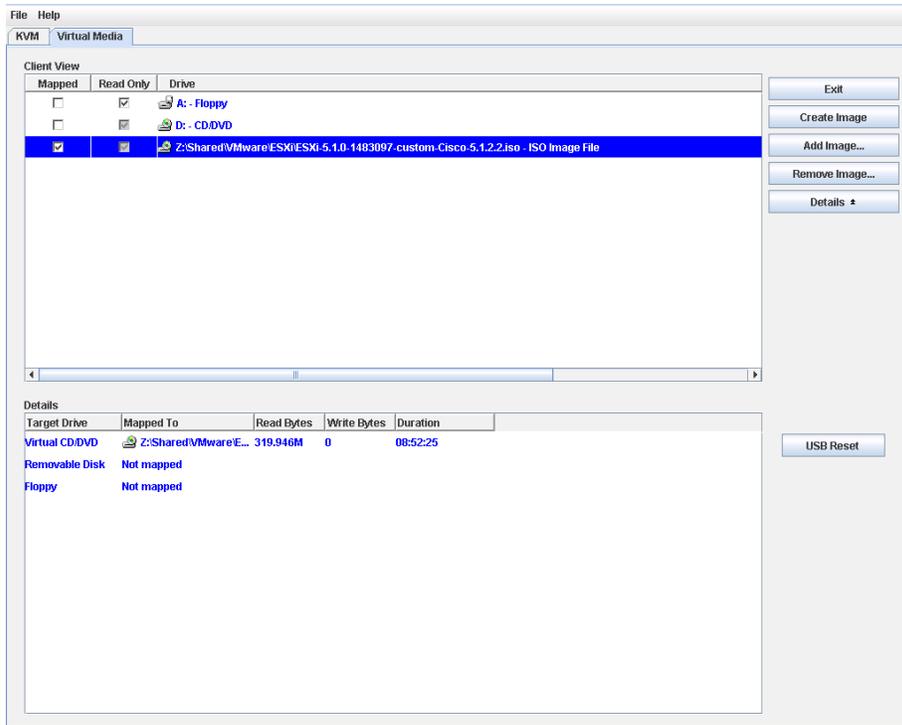
ESXi 5.1.0 will operate in evaluation mode for 60 days. To use ESXi 5.1.0 after the evaluation period, you must register for a VMware product license. To administer your server, use the vSphere Client or the Direct Control User Interface.

Remove the installation disc before rebooting.

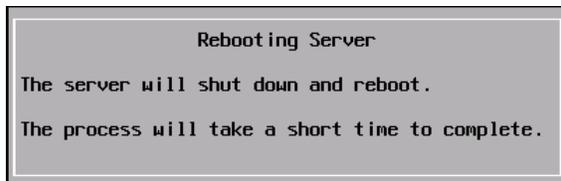
Reboot the server to start using ESXi 5.1.0.

(Enter) Reboot

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.



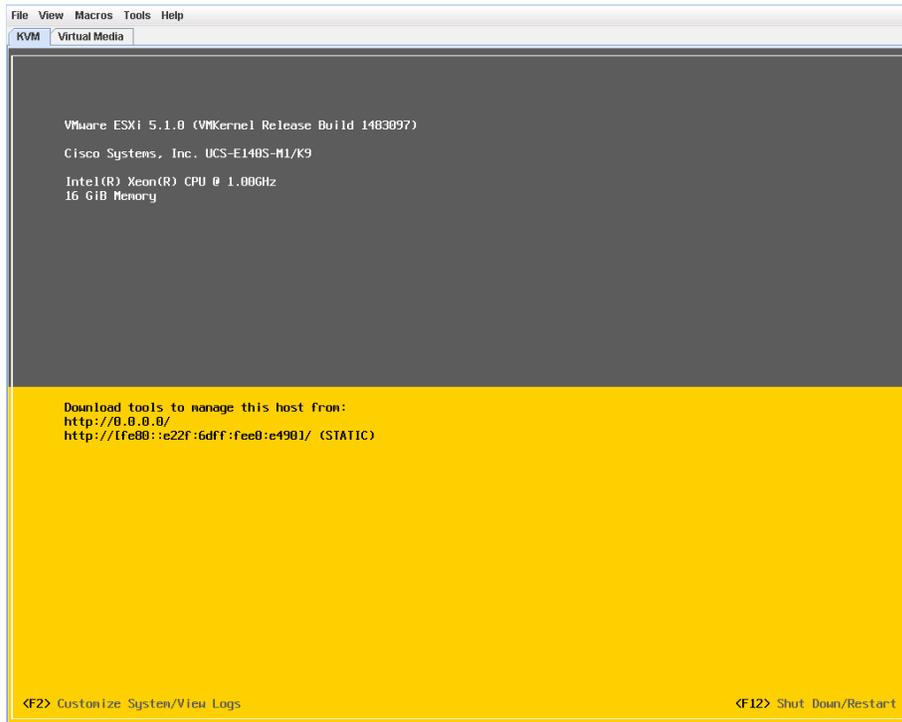
Step 26: On the KVM tab, press **Enter**. The system restarts, loading the ESXi image installed on the SD drive.



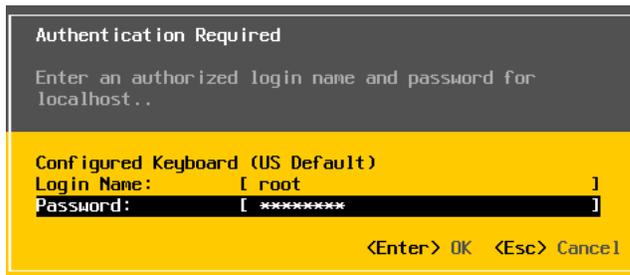
Procedure 3

Configure VMware ESXi Host Settings

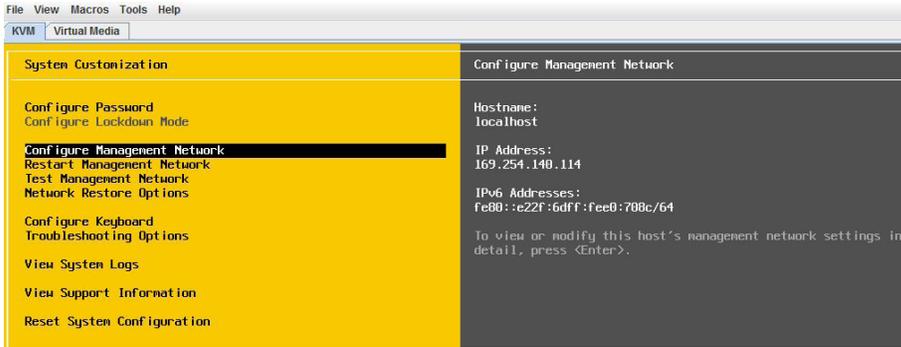
Step 1: In the ESXi home screen window, press F2. This enables you to customize the system after ESXi is finished booting.



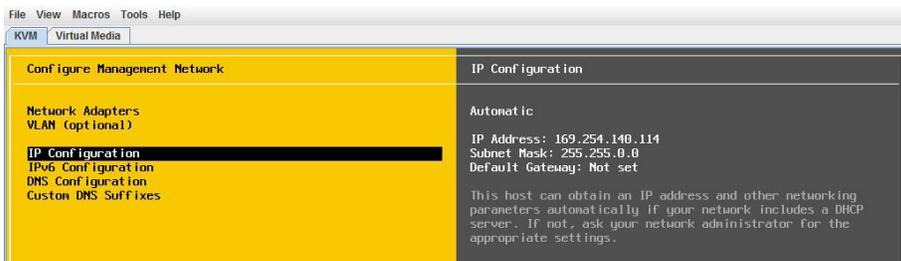
Step 2: Log in using the credentials you set during installation (Example: root/c1sco123).



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

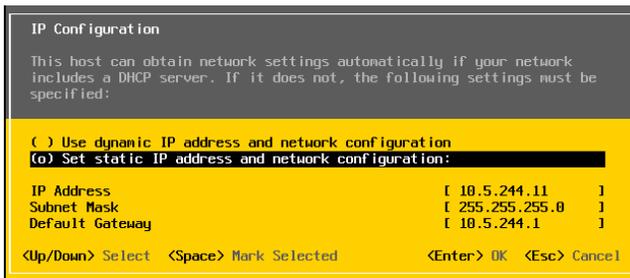


Step 4: Choose **IP Configuration**, and then press **Enter**.

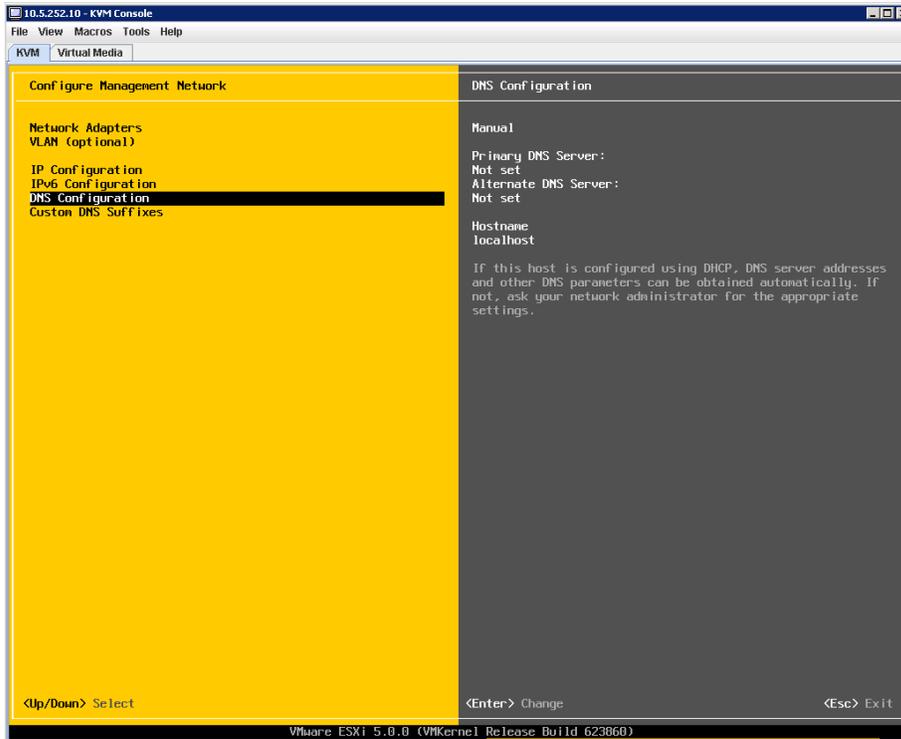


Step 5: Highlight **Set static IP address and network configuration**, and select it by pressing the space bar.

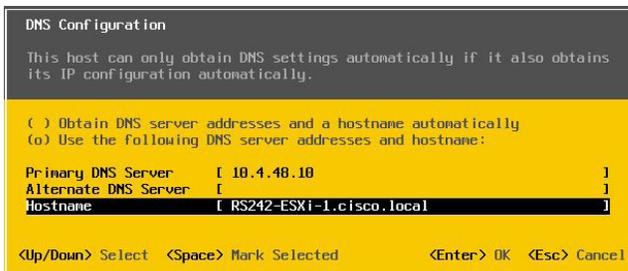
Step 6: Using the down arrow key, enter the assigned values from Table 4 for **IP address**, **subnet mask** and **default gateway**, and then press **Enter**. (Example:10.5.244.11, 255.255.255.0, 10.5.244.1)



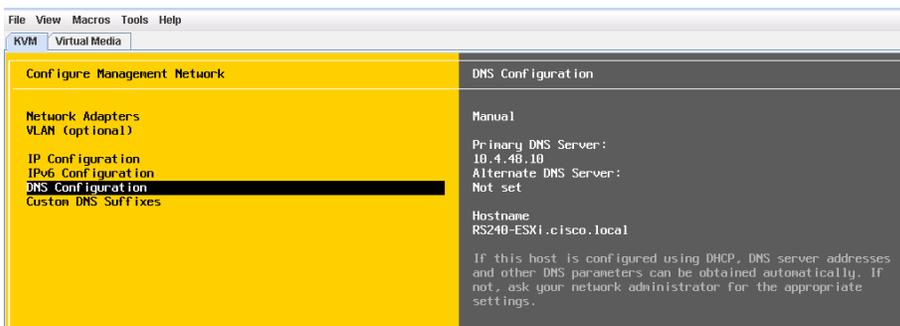
Step 7: Use the down arrow, select **DNS Configuration**, and then press **Enter**.



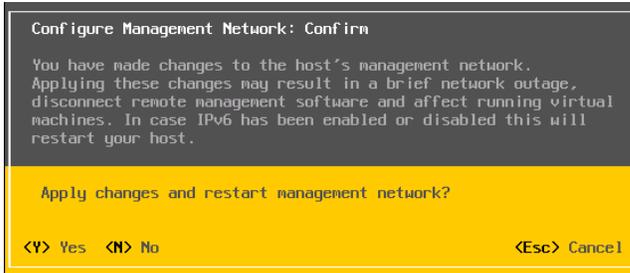
Step 8: Configure the primary DNS server and hostname (Example: 10.4.48.10 and RS240-ESXi.cisco.local), and then press **Enter**.



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



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



Procedure 4 Add VMware ESXi host to vCenter

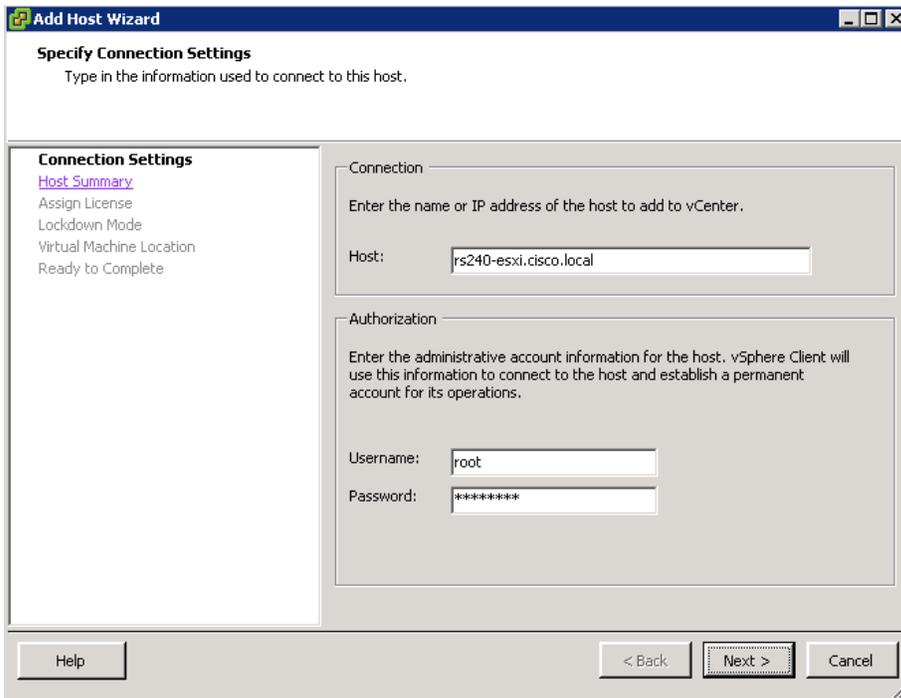
Step 1: From the VMware vSphere client, select the folder location where you want to add the ESXi host (Example: Remote Sites).

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

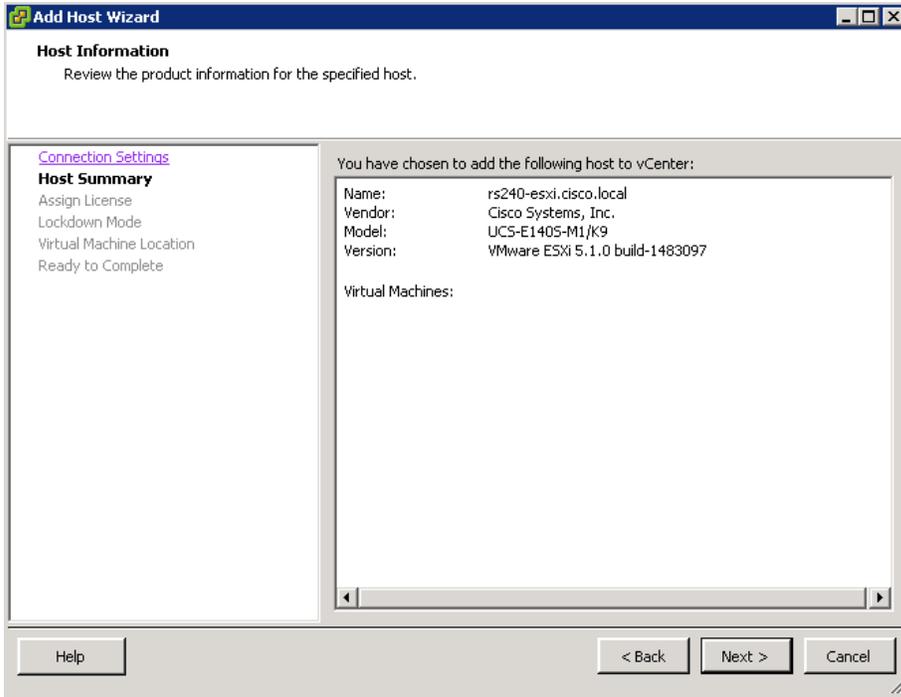
Tech Tip

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.

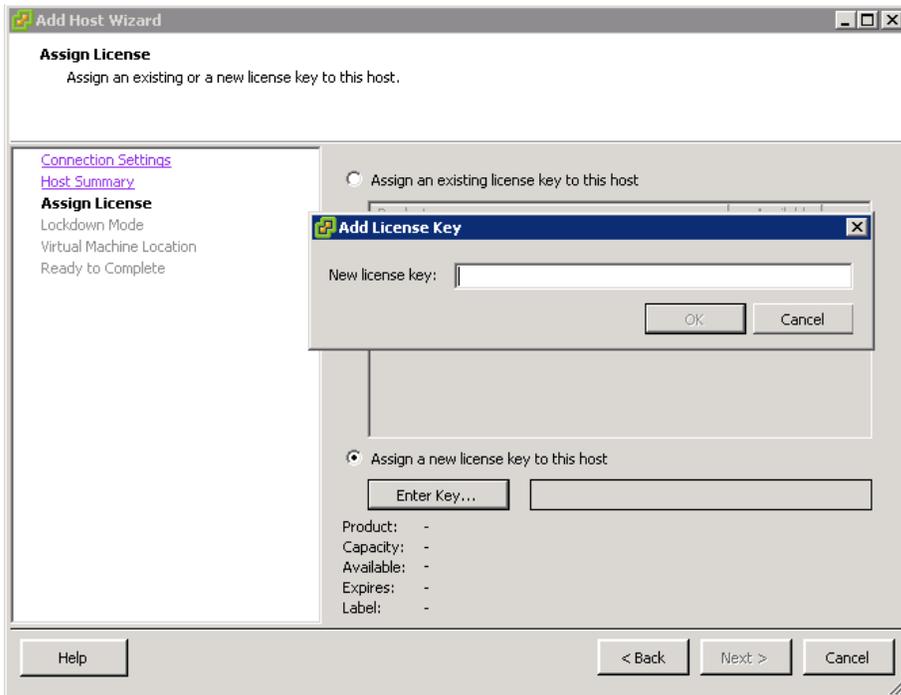
Step 3: In the Connection Settings pane, enter the host name of the ESXi host and the username and password (Example: root / c1sco123), and then click **Next**. If necessary, accept the Security Alert by clicking **Yes**.



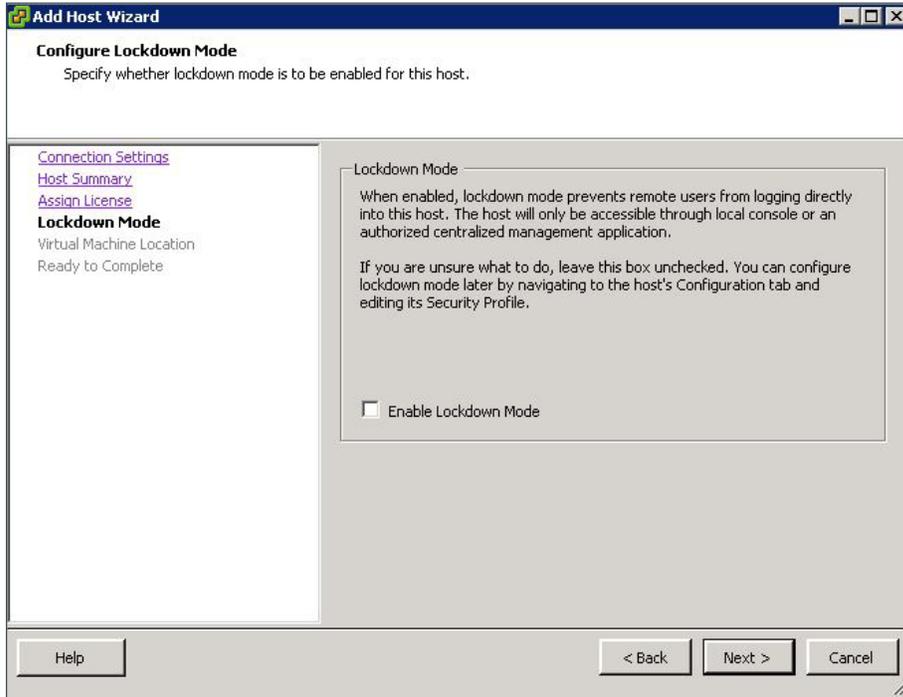
Step 4: In the Host Summary pane, verify the details of the ESXi host you want to add, and then click **Next**.



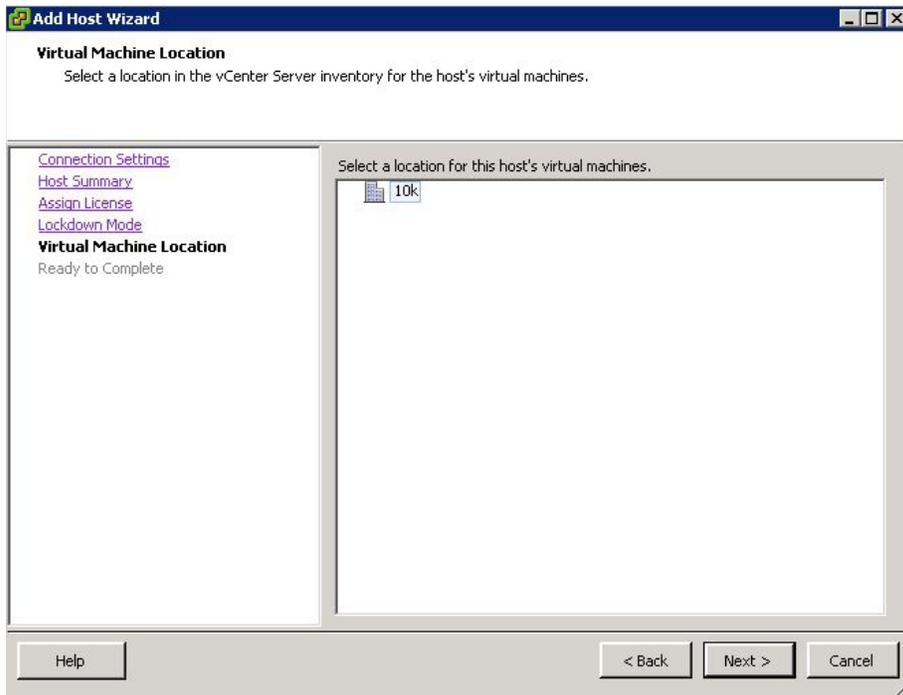
Step 5: In the **Assign License** window, click in the circle to assign the appropriate VMware license key or add a new license key and then click **Next**.



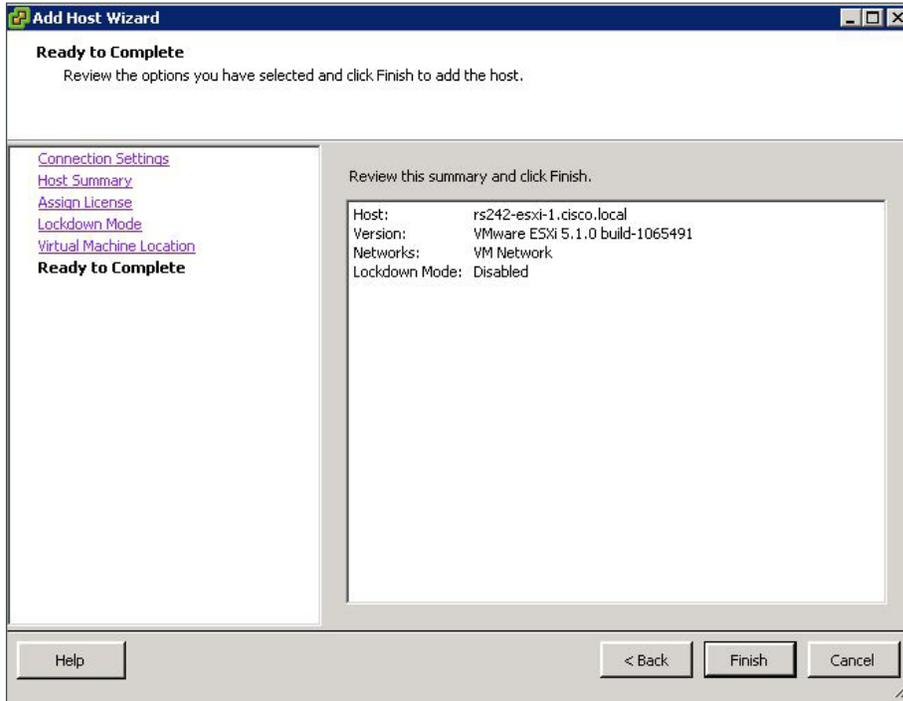
Step 6: In the Lockdown Mode pane, verify that **Enable Lockdown Mode** is cleared, and then click **Next**.



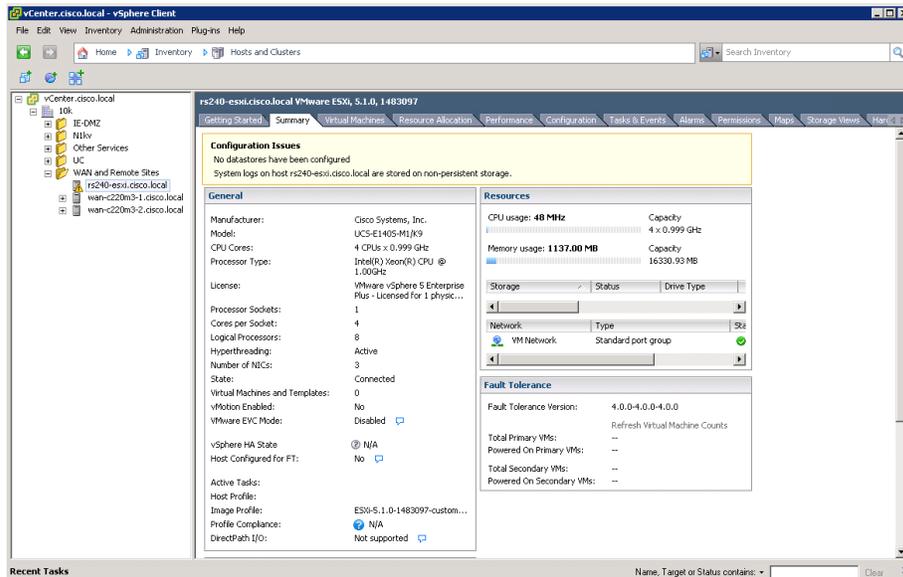
Step 7: In the Virtual Machine Location pane, select the proper location for the new EXSi host, and then click **Next**.



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

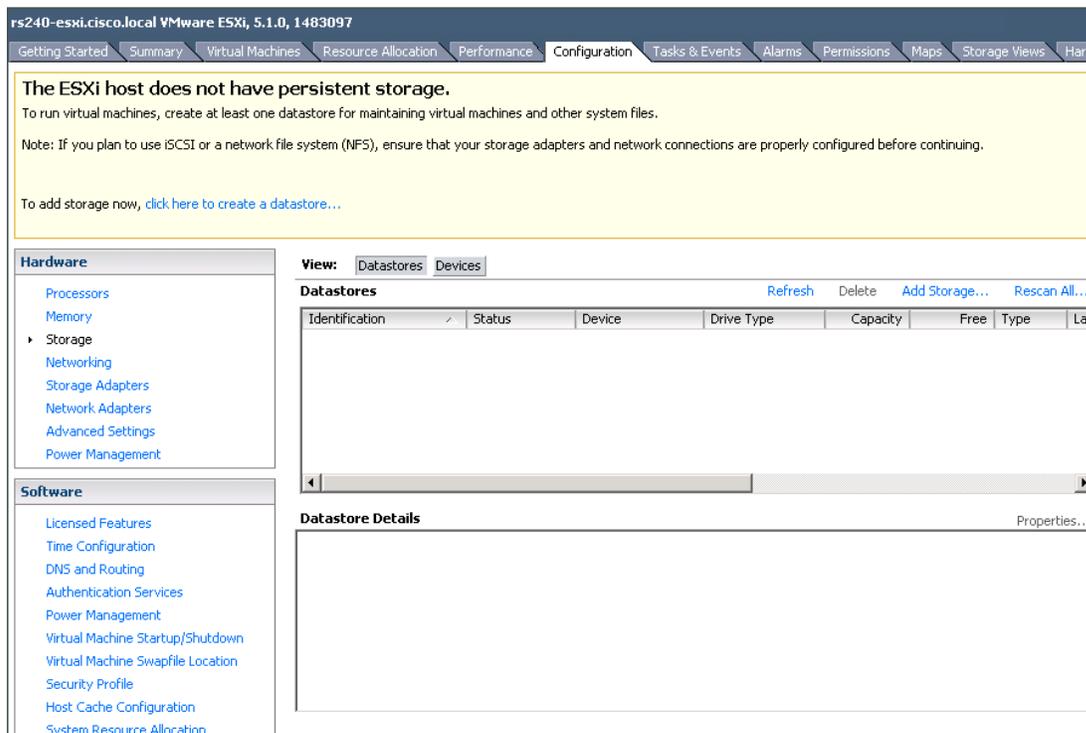
If you are installing the vSphere client on a server with USB storage for ESXi, you may receive a warning “System logging not Configured on host <hostname>”, which means that you do not have a location to store log files for ESXi on this host. In this case, you can store log files on a syslog server. More information can be found at:

http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=display&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**.



rs240-esxi.cisco.local VMware ESXi, 5.1.0, 1483097

Getting Started Summary Virtual Machines Resource Allocation Performance Configuration Tasks & Events Alarms Permissions Maps Storage Views Hard

The ESXi host does not have persistent storage.
To run virtual machines, create at least one datastore for maintaining virtual machines and other system files.
Note: If you plan to use iSCSI or a network file system (NFS), ensure that your storage adapters and network connections are properly configured before continuing.
To add storage now, [click here to create a datastore...](#)

Hardware

- Processors
- Memory
- Storage
- Networking
- Storage Adapters
- Network Adapters
- Advanced Settings
- Power Management

Software

- Licensed Features
- Time Configuration
- DNS and Routing
- Authentication Services
- Power Management
- Virtual Machine Startup/Shutdown
- Virtual Machine Swapfile Location
- Security Profile
- Host Cache Configuration
- System Resource Allocation

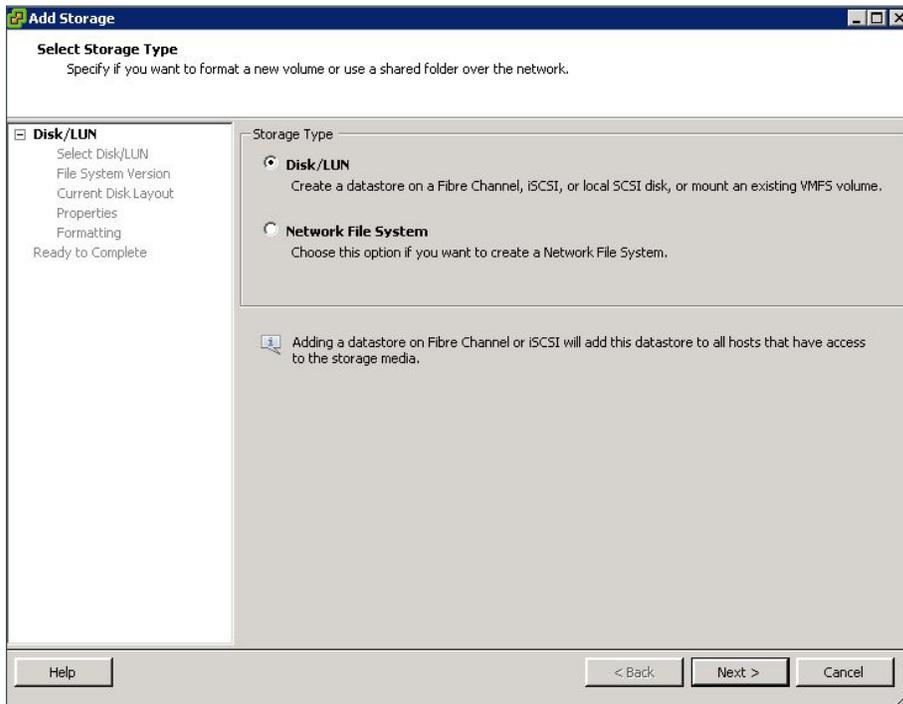
View: Datastores Devices

Datastores Refresh Delete Add Storage... Rescan All...

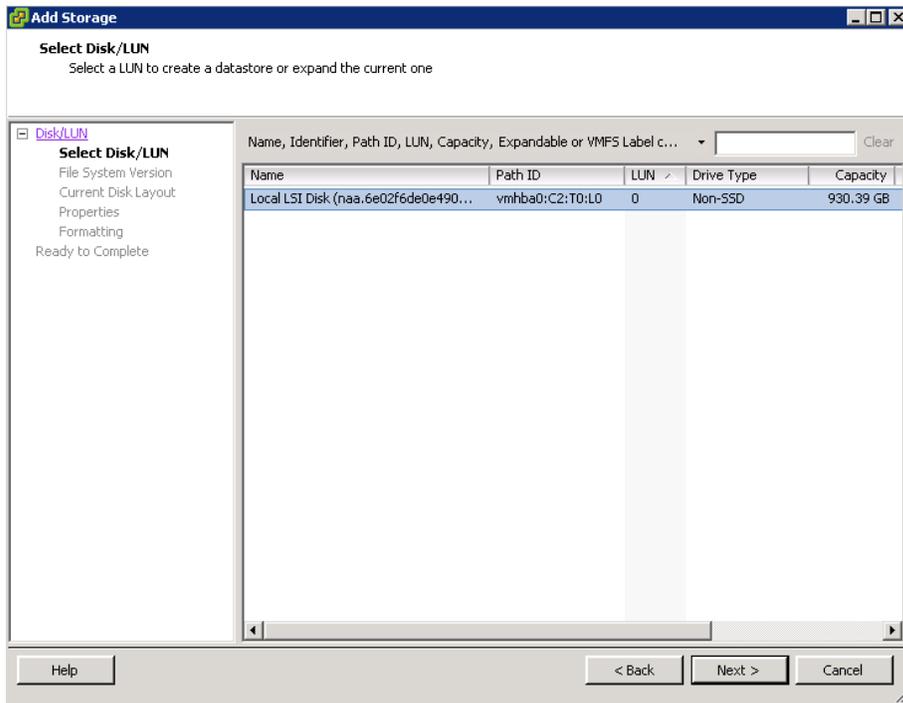
Identification	Status	Device	Drive Type	Capacity	Free	Type	Las
----------------	--------	--------	------------	----------	------	------	-----

Datastore Details Properties...

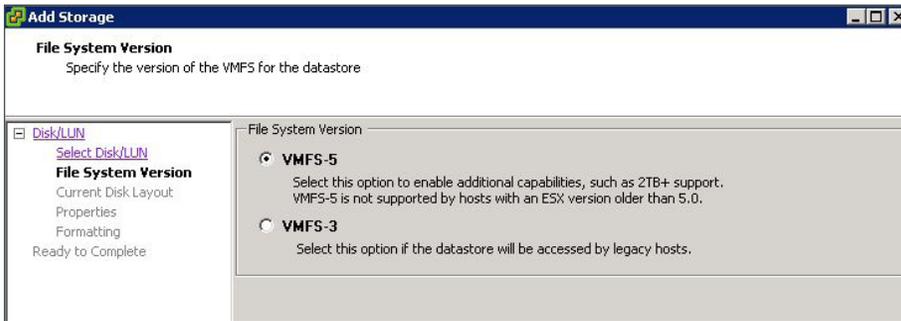
Step 4: In the Add Storage wizard, select **Disk/LUN**, and then click **Next**.



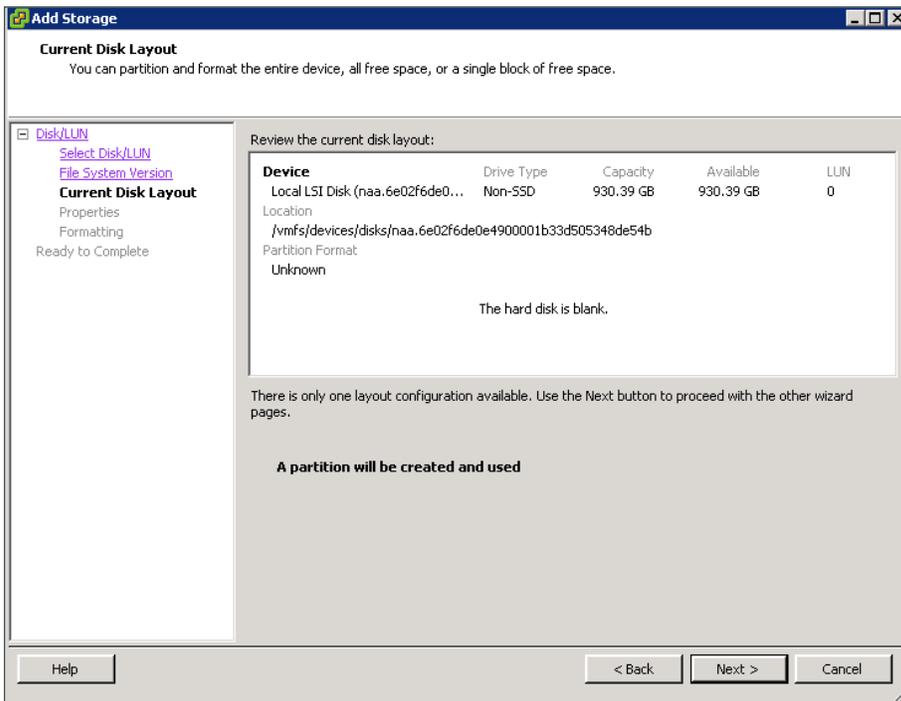
Step 5: On the Select Disk/LUN page, select the local disk and then click **Next**.



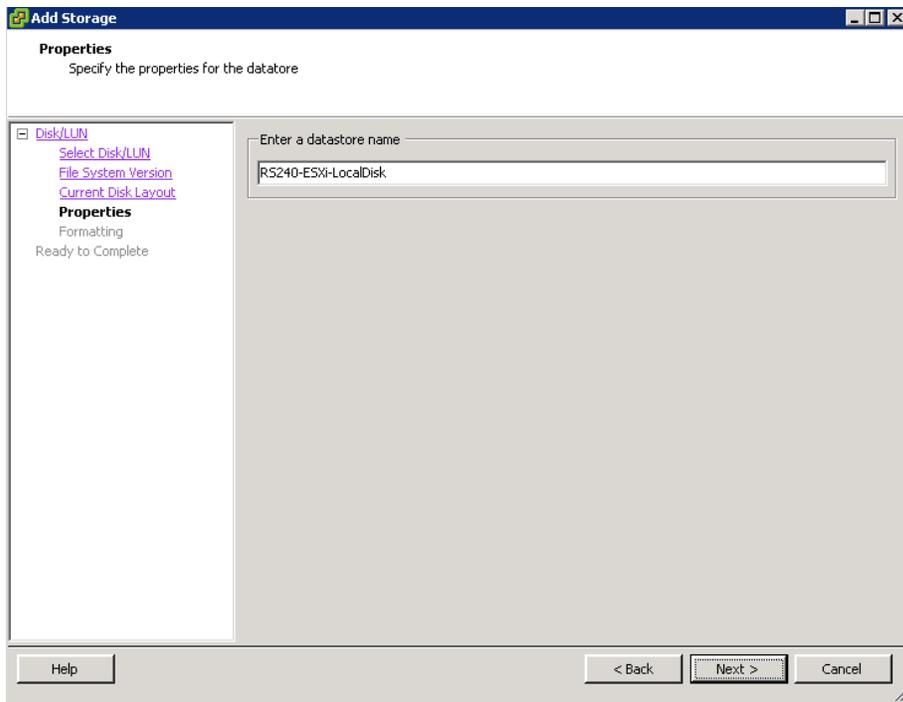
Step 6: On the File System Version page, select **VMFS-5** or **VMFS-3**. Hosts running ESXi 4.x will not be able to access VMFS-5 datastores. Unlike VMFS-3, VMFS-5 uses standard 1 MB file system block size with support of 2 TB+ virtual disks.



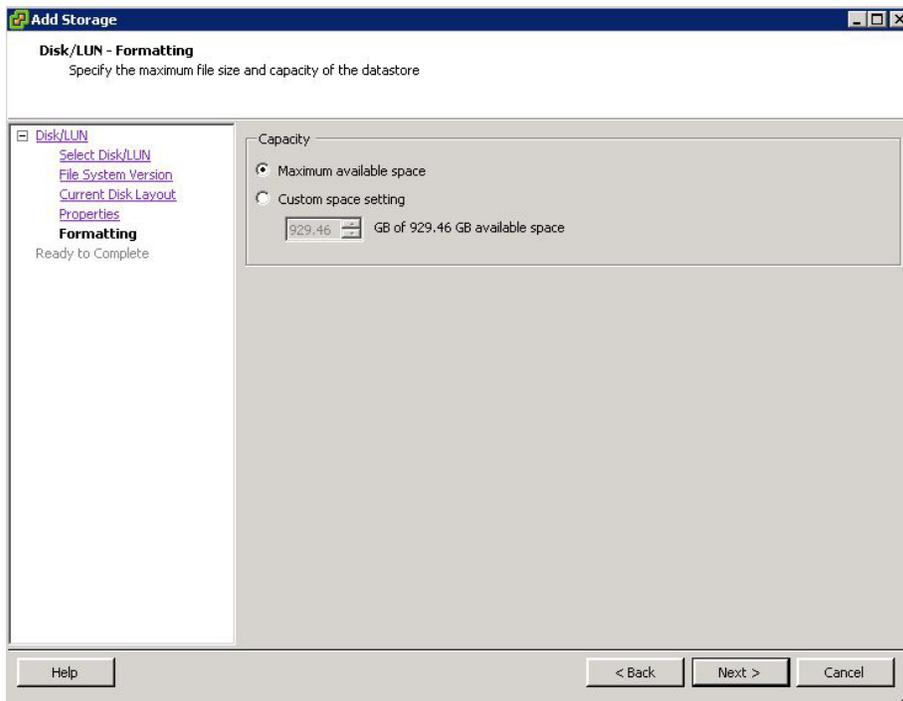
Step 7: Review the disk capacity and partition information, and then click **Next**.



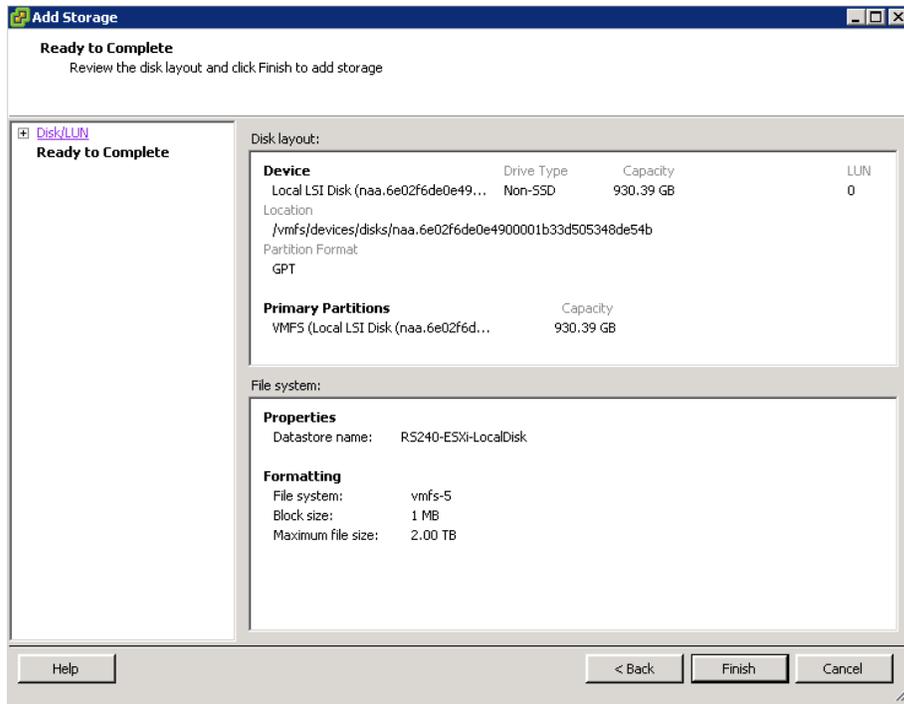
Step 8: Enter a datastore name, and then click **Next**.



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.



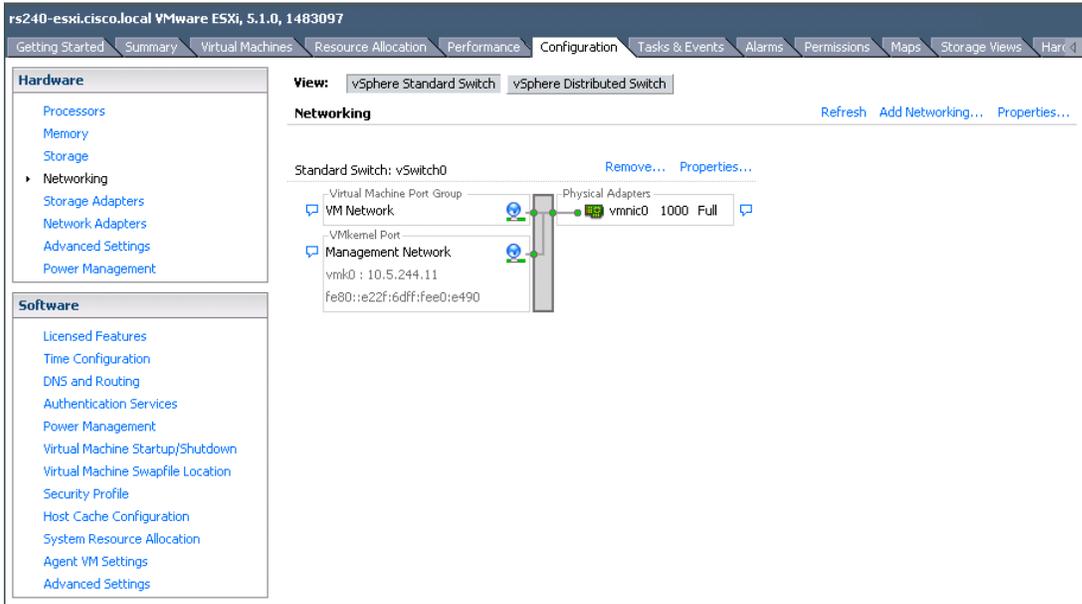
Procedure 6 Configure networking for ESXi host

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.

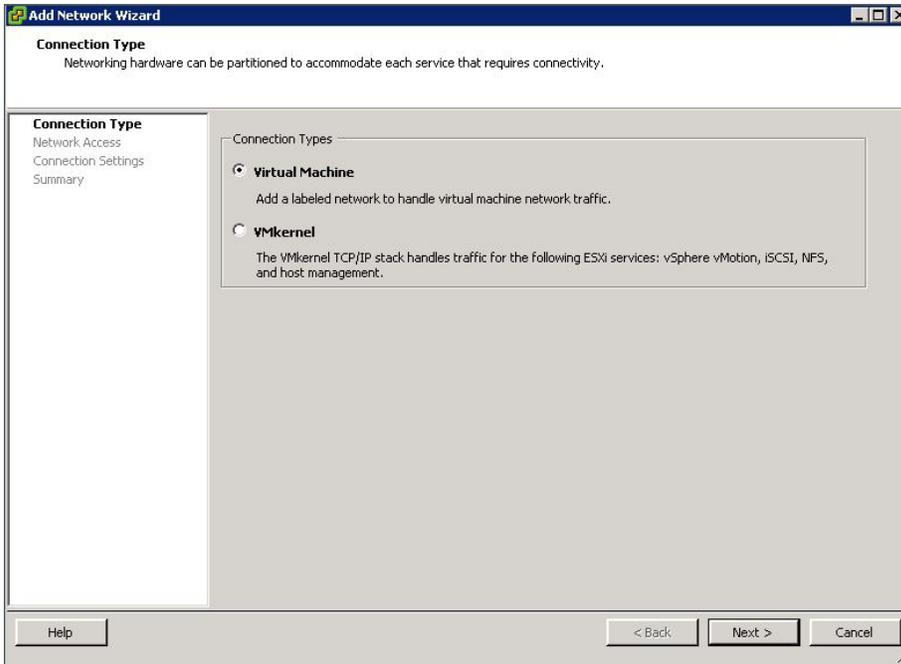
Table 5 - Cisco UCS E-Series Server interface assignments

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

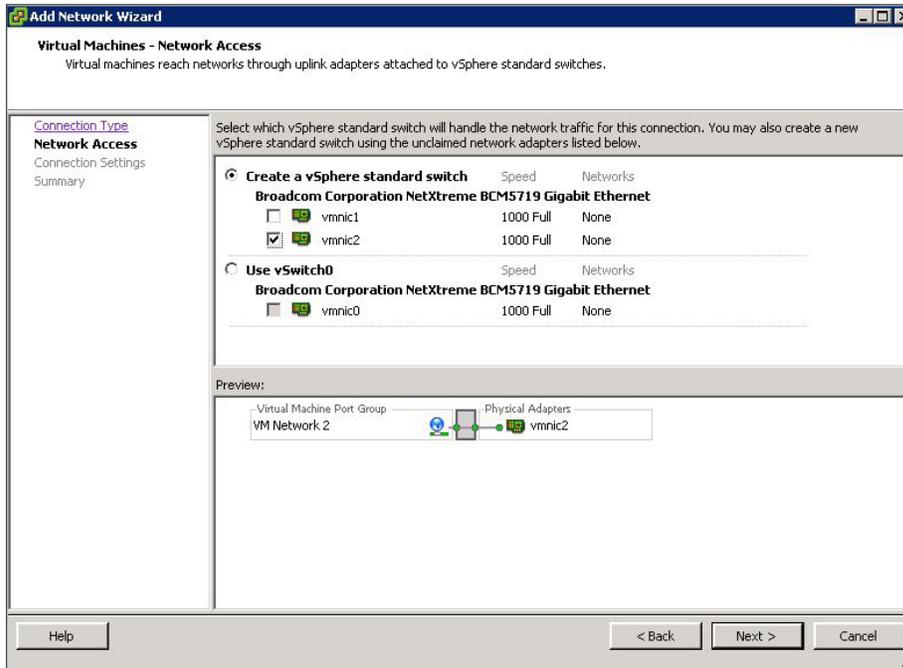
Step 1: Click the Configuration tab, click Networking, and then click Add Networking.



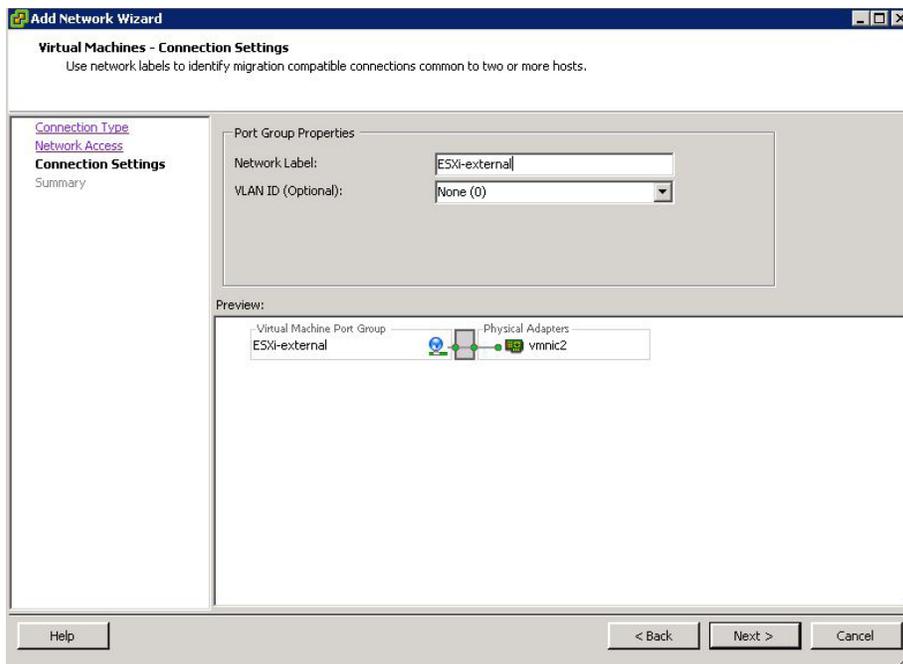
Step 2: In the Connection Type dialog box, select Virtual Machine, and then click Next.



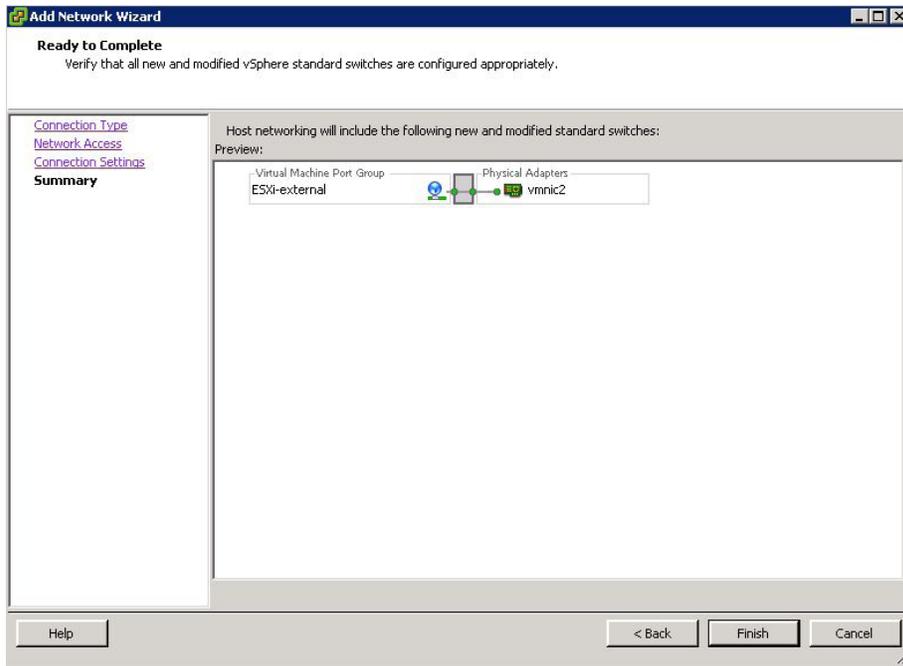
Step 3: Select the external NIC card, **vmnic2**, to be used for this vSwitch, and then click **Next**. This example uses a single interface.



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

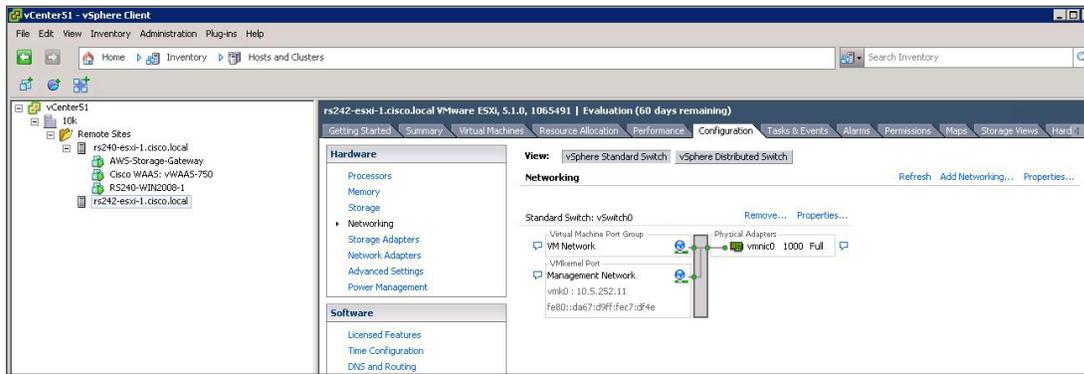
This procedure is required only if you have two external NICs connecting to external switches for resiliency. For redundancy, this example uses the default ESXi NIC teaming configurations.

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

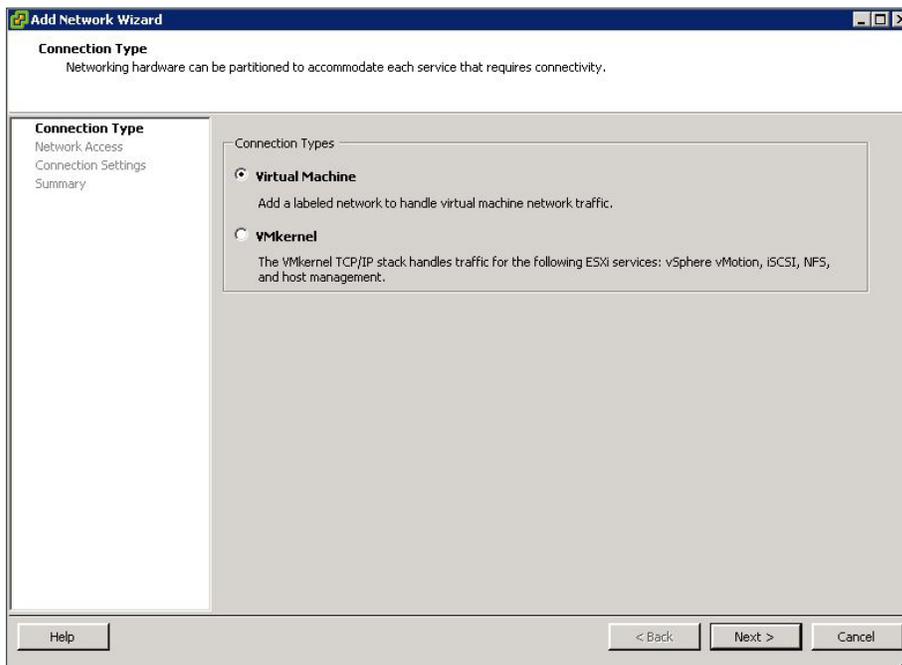
Table 6 - Cisco UCS E-Series Server interface assignments

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, click Networking, and then click Add Networking.



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



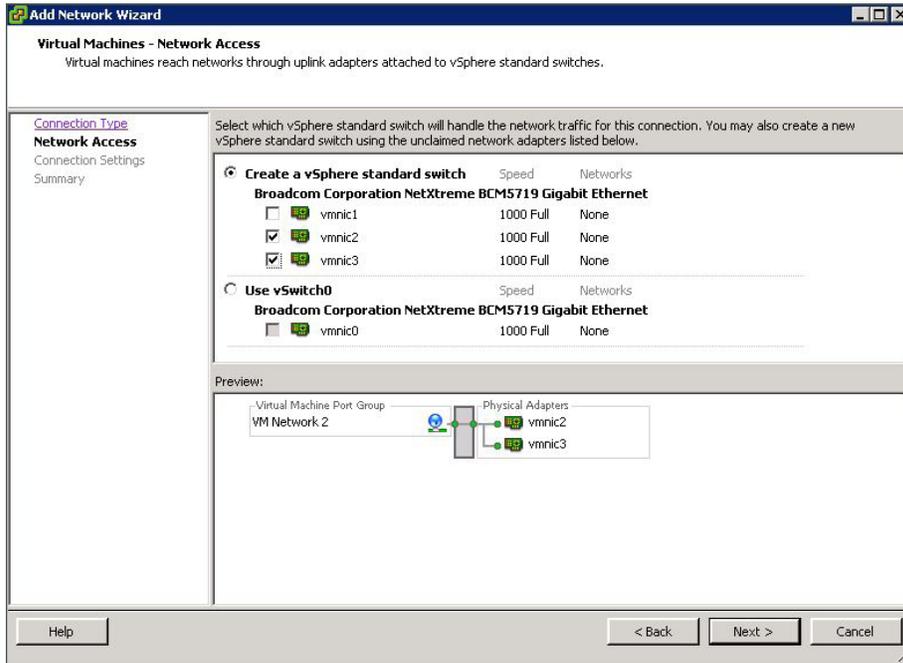
Step 3: Select the external NIC cards, vmnic2 and vmnic3, to be used for this vSwitch, and then click Next.



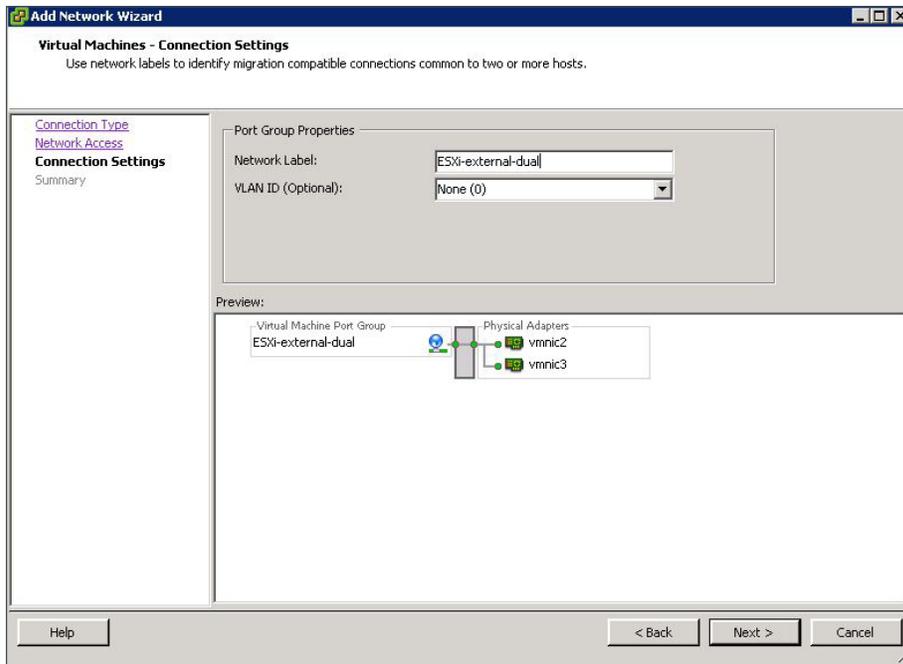
Tech Tip

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.

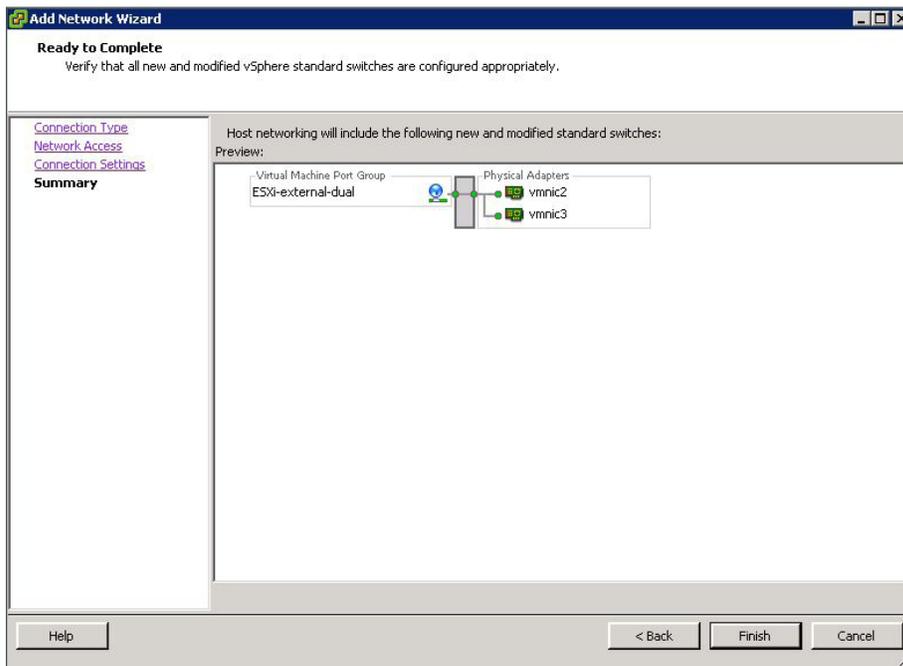
When selecting `vmnic2` and `vmnic3` for dual NIC configurations ESXi automatically configures failover for these interfaces and balances traffic based on port.



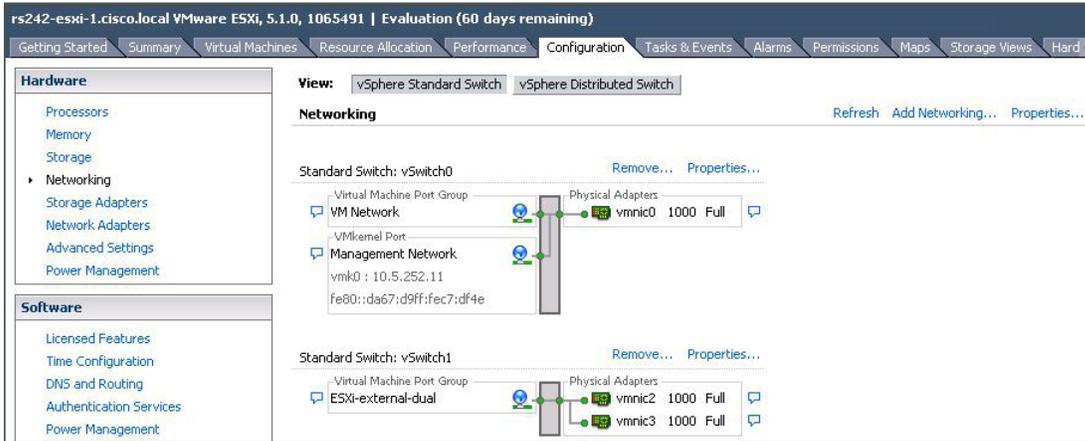
Step 4: In the Port Group Properties pane, edit the Network Label (Example from Table 6: ESXi-external-dual), set the VLAN ID to **None (0)**, and then click **Next**.



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



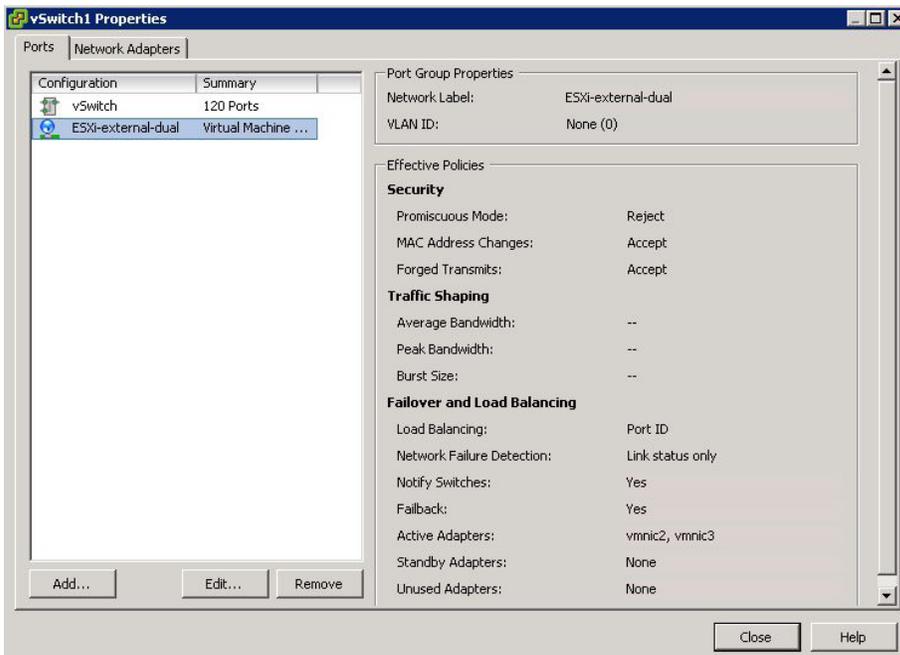
Step 6: View properties by clicking **Properties** for the newly created vSwitch (Example: vSwitch1).



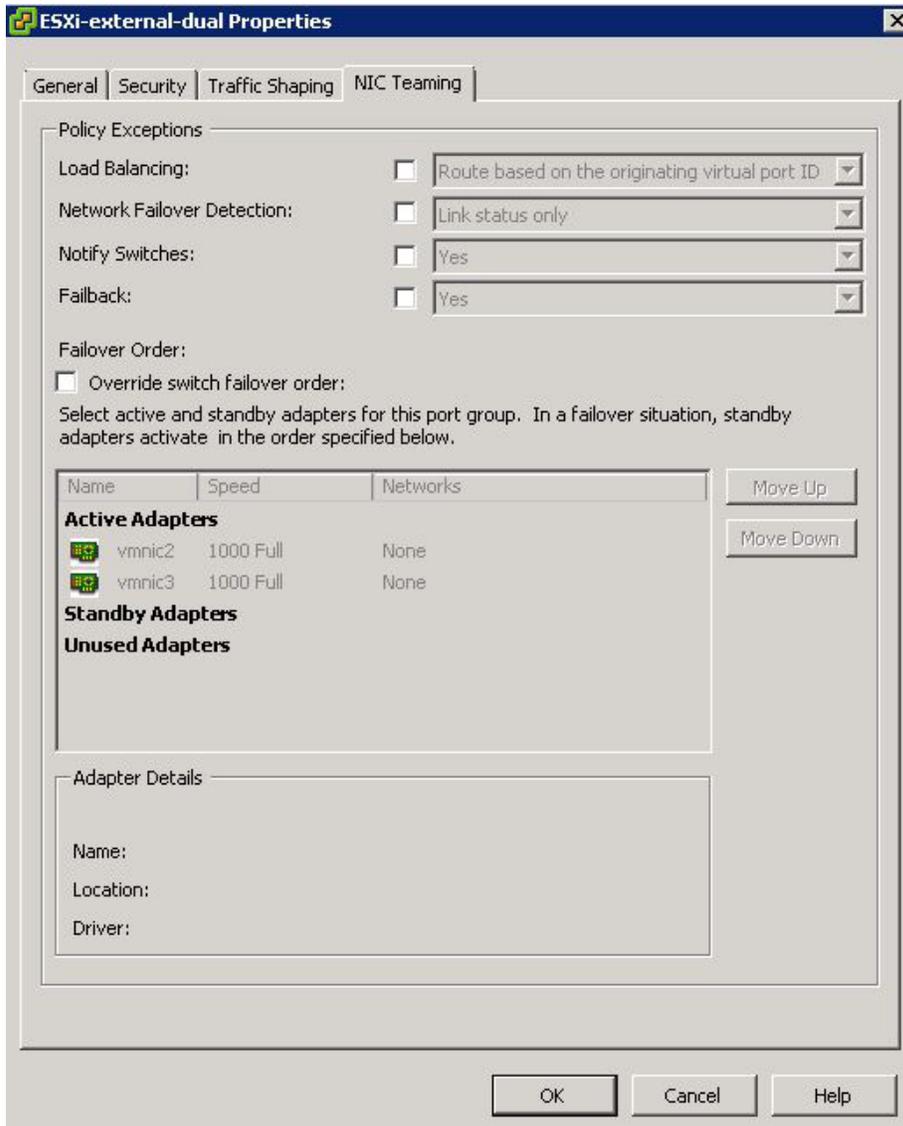
Step 7: In the vSwitch Properties pane, select the Port Group (Example: ESXi-external-dual), and click **Edit**.

i 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.



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.

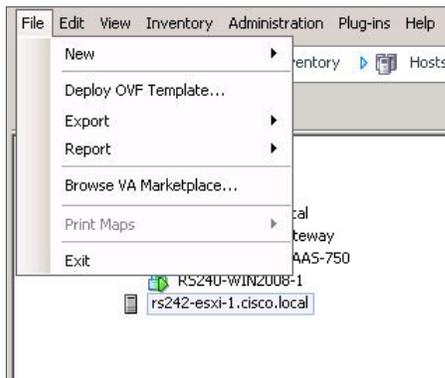
Most Cloud Connector applications are available as OVA and are designed to be installed into a virtual environment. The OVA is an industry standard format with prepackaged disk, memory, CPU, NICs, and other virtual-machine-related configuration parameters.

Procedure 1 Deploy OVA for hosted cloud connector applications

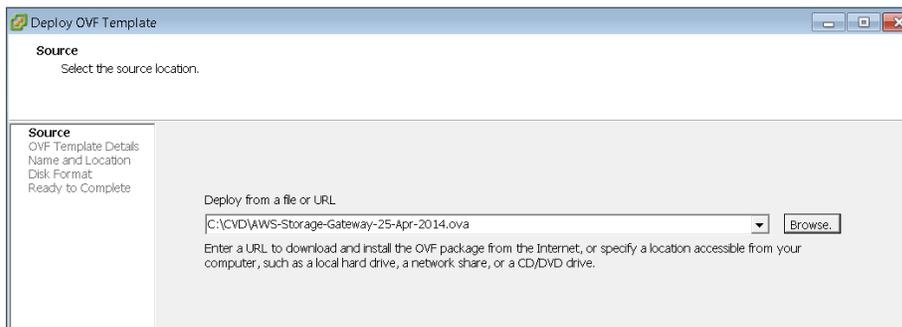
This procedure shows how to install an OVA using VMware vCenter.

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**.



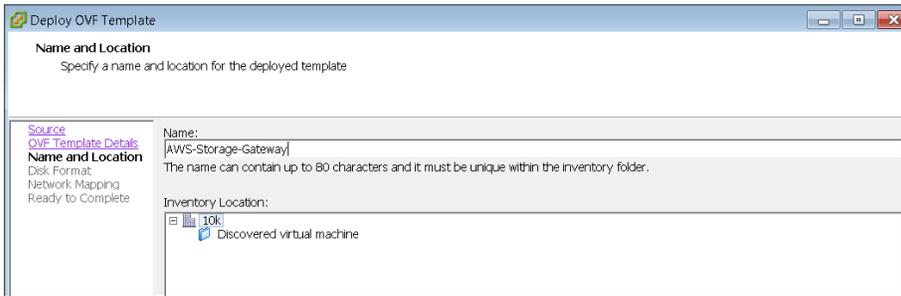
Step 3: Browse to the local OVA file to install, and then click **Next**.



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



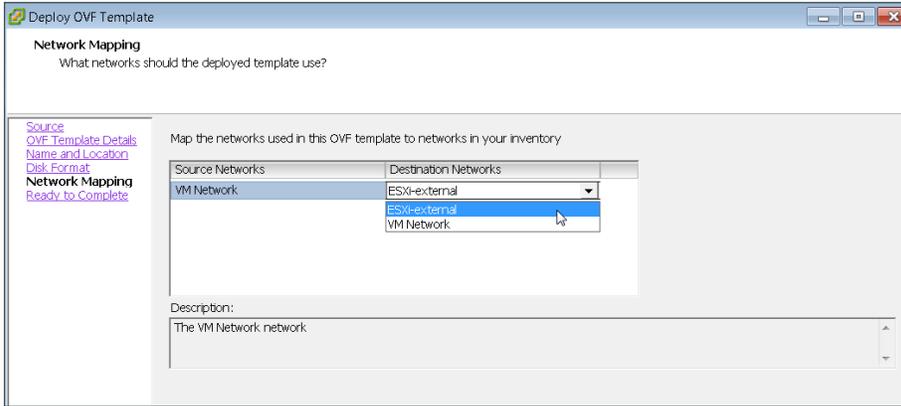
Step 5: Enter a name for the OVA (Example: AWS-Storage-Gateway-2), select the proper location, and then click **Next**.



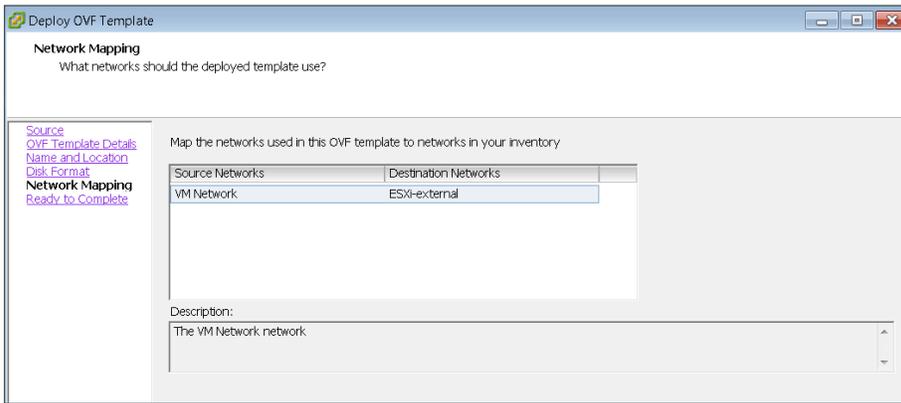
Step 6: Verify the data store and the provisioning according to the recommendations of the application vendor. To accept the recommended Disk Format Settings, click **Next**.



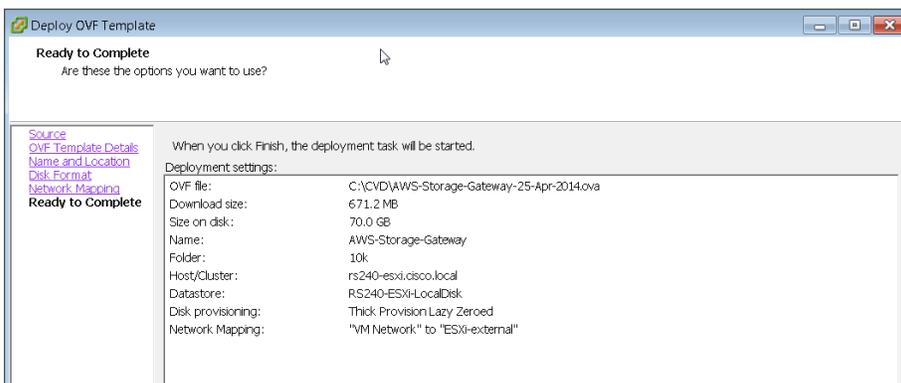
Step 7: Click the current setting for Destination Networks. All destination network choices are displayed. (Example: ESXi-external-dual, ESXi-external)



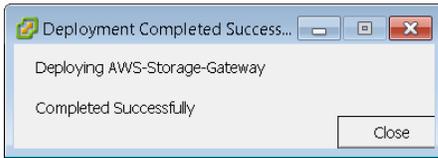
Step 8: Select the destination network by choosing the ESXi networking profile created in Procedure 6, Step 4 (Example: ESXi-external, ESXi-external-dual), and then click **Next**.



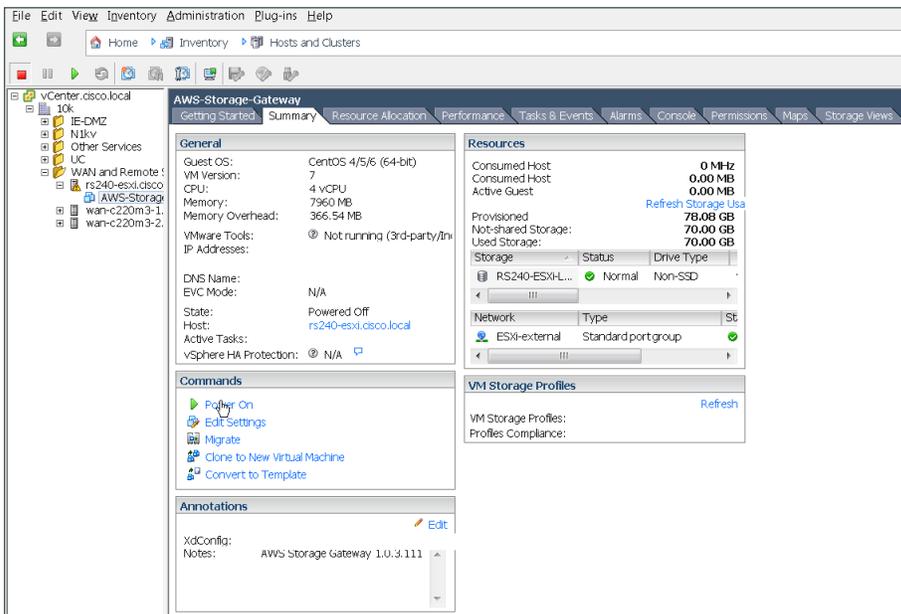
Step 9: Review the OVA summary information, select **Power on after deployment**, and then click **Finish**.



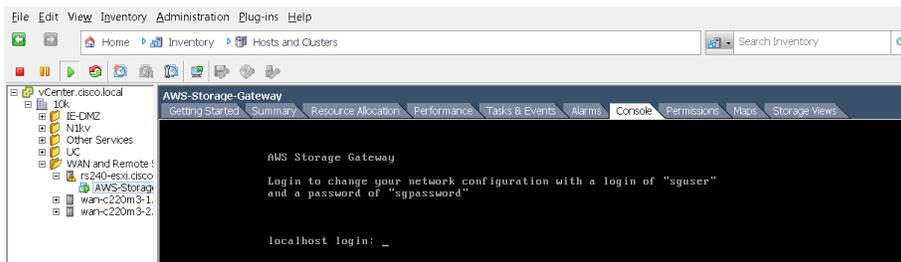
Step 10: Monitor the deployment.



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



Step 12: Start the virtual machine and finish configuring the Cloud Connector application according to the guidelines provided by the third-party vendor.



Appendix A: Product List

Hosted Cloud WAN Deployment Guide

WAN Remote Site

Functional Area	Product Description	Part Numbers	Software
Modular WAN Remote-site Router	Cisco ISR 3945 w/ SPE150, 3GE, 4EHWIC, 4DSP, 4SM, 256MBCF, 1GBDRAM, IP Base, SEC, AX licenses with; DATA, AVC, and WAAS/ vWAAS with 2500 connection RTU	C3945-AX/K9	15.3(3)M3 securityk9 feature set datak9 feature set
	Cisco ISR 3925 w/ SPE100 (3GE, 4EHWIC, 4DSP, 2SM, 256MBCF, 1GBDRAM, IP Base, SEC, AX licenses with; DATA, AVC, WAAS/ vWAAS with 2500 connection RTU	C3925-AX/K9	
	Cisco ISR 2951 w/ 3 GE, 4 EHWIC, 3 DSP, 2 SM, 256MB CF, 1GB DRAM, IP Base, SEC, AX license with; DATA, AVC, and WAAS/ vWAAS with 1300 connection RTU	C2951-AX/K9	
	Cisco ISR 2921 w/ 3 GE, 4 EHWIC, 3 DSP, 1 SM, 256MB CF, 1GB DRAM, IP Base, SEC, AX license with; DATA, AVC, and WAAS/ vWAAS with 1300 connection RTU	C2921-AX/K9	
	Cisco ISR 2911 w/ 3 GE, 4 EHWIC, 2 DSP, 1 SM, 256MB CF, 1GB DRAM, IP Base, SEC, AX license with; DATA, AVC and WAAS/ vWAAS with 1300 connection RTU	C2911-AX/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	CMIC 2.2.2
	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	5.1.2.2

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 15.3
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
!
!
!
enable secret 5 $1$n0mF$ISe9QVYXC/Ot8NCRvLsqm.
!
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
!
!
!
!
key chain WAN-KEY
  key 1
    key-string 7 121A0C041104
voice-card 0
!
!
license udi pid C3900-SPE150/K9 sn FOC14314JFF
license accept end user agreement
license boot module c3900 technology-package datak9
!
!
username admin password 7 130646010803557878
!
redundancy
!
!
ip ssh source-interface Loopback0
ip ssh version 2
ip scp server enable
!
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 match-any BGP-ROUTING
  match protocol bgp

```

```

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
class-map type inspect match-any INSPECT-ACL-IN-CLASS
  match access-group name ACL-RTR-IN
!
policy-map MARK-BGP
  class BGP-ROUTING
    set dscp cs6
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
    service-policy MARK-BGP
  class class-default
    bandwidth percent 25

```

```

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 15000000
    service-policy WAN
policy-map WAN-INTERFACE-G0/1
  class class-default
    shape average 10000000
    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 10.4.32.151 key cisco123
  pre-shared-key address 10.4.32.152 key cisco123
  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 policy 15
  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
!
!
crypto gdoi group GETVPN-GROUP
  identity number 65511
  server address ipv4 10.4.32.151
  server address ipv4 10.4.32.152
!
!
crypto map GETVPN-MAP local-address Loopback0
crypto map GETVPN-MAP 10 gdoi
  set group GETVPN-GROUP
!
!
interface Loopback0
  ip address 10.255.251.240 255.255.255.255
  ip pim sparse-mode
!
interface Tunnel10
  description DMVPN-1 tunnel interface
  bandwidth 10000
  ip address 10.4.34.240 255.255.254.0
  no ip redirects
  ip mtu 1400
  ip pim dr-priority 0
  ip pim nbma-mode
  ip pim sparse-mode
  ip nhrp authentication cisco123
  ip nhrp group RS-GROUP-10MBPS
  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
ip virtual-reassembly in
ip virtual-reassembly out
zone-member security INSIDE
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 GigabitEthernet0/0
description MPLS-A (remote-as 65401 - 192.168.3.50)
bandwidth 15000
ip address 192.168.3.49 255.255.255.252
zone-member security INSIDE
ip tcp adjust-mss 1360
duplex auto
speed auto
no cdp enable
crypto map GETVPN-MAP
service-policy output WAN-INTERFACE-G0/0
!
interface GigabitEthernet0/1
description Internet Connection
ip dhcp client default-router distance 10
ip dhcp client route track 62
ip address dhcp
no ip redirects
no ip unreachable
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-G0/1
!
interface GigabitEthernet0/2

```

```

description To RS240-A3650 G1/0/24
no ip address
duplex auto
speed auto
!
interface GigabitEthernet0/2.64
description Wired Data
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 GigabitEthernet0/2.69
description Wired Voice
encapsulation dot1Q 69
ip address 10.5.245.1 255.255.255.0
ip helper-address 10.4.48.10
ip pim sparse-mode
zone-member security INSIDE
!
!
interface ucsel/0
ip unnumbered GigabitEthernet0/2.64
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
!
interface ucsel/1
description Internal switch interface connected to Service Module
no ip address
!
!
router eigrp WAN-DMVPN-1
!
address-family ipv4 unicast autonomous-system 200
!
af-interface default
passive-interface
exit-af-interface
!
af-interface Tunnel10
summary-address 10.5.240.0 255.255.248.0
authentication mode md5

```

```

authentication key-chain WAN-KEY
hello-interval 20
hold-time 60
no passive-interface
exit-af-interface
!
topology base
  distribute-list route-map BLOCK-DEFAULT in
exit-af-topology
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
eigrp router-id 10.255.251.240
eigrp stub connected summary
exit-address-family
!
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 ucse1/0
ip route 10.5.244.11 255.255.255.255 ucse1/0
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 standard WAVE
  permit 10.5.244.8
!
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 access-list extended WAAS-REDIRECT-LIST
  remark WAAS WCCP Redirect List
  deny tcp any any eq 22
  deny tcp any eq 22 any
  deny tcp any eq telnet any
  deny tcp any any eq telnet
  deny tcp any eq tacacs any
  deny tcp any any eq tacacs
  deny tcp any eq bgp any
  deny tcp any any eq bgp
  deny tcp any any eq 123
  deny tcp any eq 123 any
  deny tcp any any eq 161
  deny tcp any eq 161 any
  deny tcp any any eq 162
  deny tcp any eq 162 any
  deny tcp any any eq 2000
  deny tcp any eq 2000 any
  deny tcp any any eq 2443
  deny tcp any eq 2443 any
  deny tcp any any eq 5060

```

```

deny tcp any eq 5060 any
deny tcp any any eq 5061
deny tcp any eq 5061 any
deny tcp any any eq 1718
deny tcp any eq 1718 any
deny tcp any any eq 1720
deny tcp any eq 1720 any
deny tcp any any eq 2428
deny tcp any eq 2428 any
deny tcp any any eq 443
deny tcp any eq 443 any
deny tcp any any eq 8443
deny tcp any eq 8443 any
deny tcp any any eq 6970
deny tcp any eq 6970 any
deny tcp any any eq 689
deny tcp any eq 689 any
permit tcp any any
!
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
access-list 55 permit 10.4.48.0 0.0.0.255
!
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 55
snmp-server community cisco123 RW 55
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 0812494D1B1C113C1712
!
!
line con 0
  logging synchronous
  transport preferred none
line aux 0
line vty 0 4
  access-class 55 in
  transport preferred none
  transport input ssh
line vty 5 15
  access-class 55 in
  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 15.3
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname RS242-2951-1
!
!
no logging buffered
enable secret 5 $1$Mqp4$YjiAg3ACxQOH9CurAwX2/
!
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
ipv6 spd queue min-threshold 62
ipv6 spd queue max-threshold 63
no ipv6 cef
!
multilink bundle-name authenticated
!
key chain LAN-KEY
  key 1
    key-string 7 030752180500
!
!
license udi pid CISCO2951/K9 sn FTX1446AKDL
license accept end user agreement
license boot module c2951 technology-package securityk9
license boot module c2951 technology-package datak9
username admin password 7 121A540411045D5679
!
redundancy
!
ip ssh source-interface Loopback0
ip ssh version 2
ip scp server enable
!
track 50 ip sla 100 reachability
!
class-map match-any DATA
  match dscp af21
class-map match-any BGP-ROUTING
  match protocol bgp
class-map match-any INTERACTIVE-VIDEO
  match dscp cs4  af41
class-map match-any CRITICAL-DATA
  match dscp cs3  af31
class-map match-any VOICE

```

```

match dscp ef
class-map match-any SCAVENGER
  match dscp cs1 af11
class-map match-any NETWORK-CRITICAL
  match dscp cs2 cs6
!
policy-map MARK-BGP
  class BGP-ROUTING
    set dscp cs6
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
    service-policy MARK-BGP
  class class-default
    bandwidth percent 25
policy-map WAN-INTERFACE-G0/0
  class class-default
    shape average 20000000
    service-policy WAN
policy-map WAN-INTERFACE-G0/1
  class class-default
    shape average 10000000
    service-policy WAN
!
crypto isakmp policy 15
  encr aes 256
  authentication pre-share
  group 2
crypto isakmp key cisco123 address 10.4.32.151
crypto isakmp key cisco123 address 10.4.32.152
!
crypto gdoi group GETVPN-GROUP
  identity number 65511
  server address ipv4 10.4.32.151
  server address ipv4 10.4.32.152

```

```

!
crypto map GETVPN-MAP local-address Loopback0
crypto map GETVPN-MAP 10 gdoi
  set group GETVPN-GROUP
!
!
interface Loopback0
  ip address 10.255.252.242 255.255.255.255
  ip pim sparse-mode
!
interface Port-channel1
  description Etherchannel link to RS242-2960X
  no ip address
  hold-queue 150 in
!
interface Port-channel1.64
  description Data
  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
  description Voice
  encapsulation dot1Q 69
  ip address 10.5.253.2 255.255.255.0
  ip helper-address 10.4.48.10
  ip pim dr-priority 110
  ip pim sparse-mode
  standby version 2
  standby 1 ip 10.5.253.1
  standby 1 priority 110
  standby 1 preempt
  standby 1 authentication md5 key-string 7 070C705F4D06485744
  standby 1 track 50 decrement 10
!
interface Port-channel1.99
  description Transit Net
  encapsulation dot1Q 99
  ip address 10.5.248.9 255.255.255.252

```

```

ip pim sparse-mode
!
!
interface GigabitEthernet0/0
bandwidth 10000
ip address 192.168.4.49 255.255.255.252
ip tcp adjust-mss 1360
duplex auto
speed auto
no cdp enable
crypto map GETVPN-MAP
service-policy output WAN-INTERFACE-G0/0
!
interface GigabitEthernet0/1
description RS242-A2960Xa G1/0/24
no ip address
duplex auto
speed auto
channel-group 1
!
interface GigabitEthernet0/2
description RS242-A2960Xb G2/0/24
no ip address
duplex auto
speed auto
channel-group 1
!
interface ucse2/0
ip unnumbered Port-channell1.64
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
description Internal switch interface connected to Service Module
no ip address
!
!
router eigrp LAN
!
address-family ipv4 unicast autonomous-system 100
!
af-interface default
passive-interface
exit-af-interface
!
af-interface Port-channell1.99
authentication mode md5

```

```

authentication key-chain LAN-KEY
no passive-interface
exit-af-interface
!
topology base
default-metric 100000 100 255 1 1500
redistribute bgp 65511
redistribute static route-map STATIC-IN
exit-af-topology
network 10.4.0.0 0.1.255.255
network 10.255.0.0 0.0.255.255
eigrp router-id 10.255.252.242
exit-address-family
!
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 10.255.253.242 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
remark UCSE CIMC & ESXi host routes
permit 10.5.252.11
permit 10.5.252.10
!
ip sla auto discovery
ip sla 100

```

```
icmp-echo 192.168.4.50 source-interface GigabitEthernet0/0
threshold 1000
timeout 1000
frequency 15
ip sla schedule 100 life forever start-time now
access-list 55 permit 10.4.48.0 0.0.0.255
!
nls resp-timeout 1
cpd cr-id 1
route-map STATIC-IN permit 30
  match ip address STATIC-ROUTE-LIST
!
!
snmp-server community cisco RO 55
snmp-server community cisco123 RW 55
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 097F4B0A0B0003390E15
!
!
!
line con 0
  logging synchronous
line aux 0
line vty 0 4
  access-class 55 in
  transport preferred none
  transport input ssh
line vty 5 15
  access-class 55 in
  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 15.3
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
!
!
enable secret 5 /DtCCr53Q4B18jSim1UEqu7cNVZTOhxTZyUnZdsSrs
!
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
!
no ip domain lookup
ip domain name cisco.local
ip multicast-routing
ip inspect log drop-pkt
ipv6 spd queue min-threshold 62
ipv6 spd queue max-threshold 63
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
!
key chain WAN-KEY
  key 1
```

```

    key-string 7 05080F1C2243
key chain LAN-KEY
    key 1
        key-string 7 045802150C2E
voice-card 0
!
license udi pid CISCO2951/K9 sn FTX1446AKDD
license accept end user agreement
license boot module c2951 technology-package securityk9
license boot module c2951 technology-package datak9
!
username admin password 7 15115A1F07257A767B
!
redundancy
!
!
ip ssh source-interface Loopback0
ip ssh version 2
ip scp server enable
!
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-PROFILE1
  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 pim dr-priority 0

```

```

ip pim nbma-mode
ip pim sparse-mode
ip nhrp authentication cisco123
ip nhrp group RS-GROUP-10MBPS
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 tcp adjust-mss 1360
tunnel source GigabitEthernet0/0
tunnel mode gre multipoint
tunnel route-via GigabitEthernet0/0 mandatory
tunnel protection ipsec profile DMVPN-PROFILE1
!
interface Port-channel2
description Etherchannel link to RS242-2960X
no ip address
hold-queue 150 in
!
interface Port-channel2.64
description Data
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 04585A150C2E1D1C5A
!
interface Port-channel2.69
description Voice
encapsulation dot1Q 69
ip address 10.5.253.3 255.255.255.0
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 priority 105
standby 1 preempt
standby 1 authentication md5 key-string 7 0007421507545A545C
!
interface Port-channel2.99
description Transit Net
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
description Internet Connection
ip dhcp client default-router distance 10
ip dhcp client route track 62
ip address dhcp
no ip redirects
no ip unreachable
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 GigabitEthernet0/1
description RS242-A2960Xa (Gig1/0/24)
no ip address
duplex auto
speed auto
channel-group 2
!
interface GigabitEthernet0/2
description RS242-A2960Xb (Gig2/0/24)
no ip address
duplex auto

```

```

speed auto
channel-group 2
!
interface ucse2/0
ip unnumbered Port-channel2.64
ip nat inside
ip virtual-reassembly in
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
description Internal switch interface connected to Service Module
no ip address
!
router eigrp WAN-DMVPN-1
!
address-family ipv4 unicast autonomous-system 200
!
af-interface default
passive-interface
exit-af-interface
!
af-interface Tunnel10
summary-address 10.5.248.0 255.255.248.0
authentication mode md5
authentication key-chain WAN-KEY
hello-interval 20
hold-time 60
no passive-interface
exit-af-interface
!
topology base
redistribute eigrp 100 route-map REDISTRIBUTE-LIST
exit-af-topology
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
eigrp router-id 10.255.253.242
eigrp stub connected summary redistributed
exit-address-family
!
!
router eigrp LAN
!
address-family ipv4 unicast autonomous-system 100
!

```

```

af-interface default
  passive-interface
  exit-af-interface
!
af-interface Port-channel2.99
  authentication mode md5
  authentication key-chain LAN-KEY
  no passive-interface
  exit-af-interface
!
topology base
  redistribute eigrp 200
  redistribute static route-map STATIC-IN
  exit-af-topology
  network 10.4.0.0 0.1.255.255
  network 10.255.0.0 0.0.255.255
  eigrp router-id 10.255.253.242
  exit-address-family
!
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
  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
access-list 55 permit 10.4.48.0 0.0.0.255
!
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 STATIC-IN permit 10
  match ip address DHCP-DEFAULT
!
route-map BLOCK-DEFAULT permit 10
  match ip address NO-DEFAULT
!
route-map REDISTRIBUTE-LIST permit 10
  match ip address R1-LOOPBACK
!
route-map STATIC-IN permit 30
  match ip address STATIC-ROUTE-LIST
!
!
snmp-server community cisco RO 55
snmp-server community cisco123 RW 55
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 142417081E013E002131
!
!
line con 0
  logging synchronous
line aux 0
line vty 0 4
  access-class 55 in
  transport preferred none
  transport input ssh
line vty 5 15
  access-class 55 in
  transport preferred none
  transport input ssh
!
scheduler allocate 20000 1000
ntp source Loopback0
ntp server 10.4.48.17
!
end

```

Appendix C: Changes

This appendix summarizes the changes Cisco made to this guide since its last edition.

- We updated the guide to include EIGRP named mode configurations.
- We added the **ip scp server enable** command to the router configuration.

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.

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2014 Cisco Systems, Inc. All rights reserved.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)