## 

# **Newer Cisco SBA Guides Available**

This guide is part of an older series of Cisco Smart Business Architecture designs. To access the latest Cisco SBA Guides, go to http://www.cisco.com/go/sba

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



VDI

SOLUTIONS

F

1111111

CISCO

SBA

## VDI—Basic Implementation with Cisco UCS and Citrix Deployment Guide

SMART BUSINESS ARCHITECTURE

August 2012 Series

## Preface

## **Who Should Read This Guide**

This Cisco® Smart Business Architecture (SBA) guide is for people who fill a variety of roles:

- Systems engineers who need standard procedures for implementing solutions
- Project managers who create statements of work for Cisco SBA implementations
- Sales partners who sell new technology or who create implementation
   documentation
- Trainers who need material for classroom instruction or on-the-job training

In general, you can also use Cisco SBA guides to improve consistency among engineers and deployments, as well as to improve scoping and costing of deployment jobs.

## **Release Series**

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

The Release Notes for a series provides a summary of additions and changes made in the series.

All Cisco SBA guides include the series name on the cover and at the bottom left of each page. We name the series for the month and year that we release them, as follows:

#### month year Series

For example, the series of guides that we released in August 2012 are the "August 2012 Series".

You can find the most recent series of SBA guides at the following sites:

Customer access: http://www.cisco.com/go/sba

Partner access: http://www.cisco.com/go/sbachannel

### **How to Read Commands**

Many Cisco SBA guides provide specific details about how to configure Cisco network devices that run Cisco IOS, Cisco NX-OS, or other operating systems that you configure at a command-line interface (CLI). This section describes the conventions used to specify commands that you must enter.

Commands to enter at a CLI appear as follows:

configure terminal

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

ntp server 10.10.48.17

Commands with variables that you must define appear as follows:

#### class-map [highest class name]

Commands shown in an interactive example, such as a script or when the command prompt is included, appear as follows:

#### Router# enable

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

wrr-queue random-detect max-threshold 1 100 100 100 100 100

100 100 100

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

interface Vlan64

ip address 10.5.204.5 255.255.255.0

### **Comments and Questions**

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

If you would like to be notified when new comments are posted, an RSS feed is available from the SBA customer and partner pages.

August 2012 Series

## Table of Contents

What's In This SBA Guide	1
Cisco SBA Solutions	1
Route to Success	1
About This Guide	1
Introduction	2
Related Reading	2
Business Overview	3

Deployment Details7
Configuring Cisco UCS C-Series Server Hardware7
Loading XenServer Hypervisor Software8
Installing Citrix XenCenter15
Installing Citrix VDI-in-a-Box Manager
Creating First OS Image and Template for Virtualized Desktops22
Assigning Users to Work Templates and Testing Citrix Receiver34
Appendix A: Product List

## What's In This SBA Guide

## **Cisco SBA Solutions**

Cisco SBA helps you design and quickly deploy a full-service business network. A Cisco SBA deployment is prescriptive, out-of-the-box, scalable, and flexible.

Cisco SBA incorporates LAN, WAN, wireless, security, data center, application optimization, and unified communication technologies—tested together as a complete system. This component-level approach simplifies system integration of multiple technologies, allowing you to select solutions that solve your organization's problems—without worrying about the technical complexity.

Cisco SBA Solutions are designs for specific problems found within the most common technology trends. Often, Cisco SBA addresses more than one use case per solution because customers adopt new trends differently and deploy new technology based upon their needs.

## **Route to Success**

To ensure your success when implementing the designs in this guide, you should first read any guides that this guide depends upon—shown to the left of this guide on the route below. As you read this guide, specific prerequisites are cited where they are applicable.

## **About This Guide**

This *deployment guide* contains one or more deployment chapters, which each include the following sections:

- Business Overview—Describes the business use case for the design. Business decision makers may find this section especially useful.
- Technology Overview—Describes the technical design for the business use case, including an introduction to the Cisco products that make up the design. Technical decision makers can use this section to understand how the design works.
- **Deployment Details**—Provides step-by-step instructions for deploying and configuring the design. Systems engineers can use this section to get the design up and running quickly and reliably.

You can find the most recent series of Cisco SBA guides at the following sites:

Customer access: http://www.cisco.com/go/sba

Partner access: http://www.cisco.com/go/sbachannel



## Introduction

Desktop virtualization separates a personal desktop environment, including operating system, desktop applications, and personal files and settings, from the physical device on which the desktop environment runs. In a virtual desktop infrastructure (VDI) deployment, the operating system runs in a virtual machine on a server hosted in a data center.

The VDI—Basic Implementation with Cisco UCS and Citrix Deployment Guide is designed to be a comprehensive guide for an organization's initial needs for virtual desktops, deployed rapidly by using basic configuration options for VDI. With the end goal of rapid provisioning in mind, the basic setup uses a single Cisco Unified Computing System (UCS) C-Series server with integrated hard drives, teamed with Citrix virtualization components. It also uses the Citrix XenServer host hypervisor and the Citrix VDI-in-a-Box software appliance for desktop virtualization management.

## **Related Reading**

Even though the VDI—Basic Implementation with Cisco UCS and Citrix Deployment Guide offers a comprehensive solution, other guides in the Cisco SBA August 2012 Series may be beneficial for organizations wishing to customize or scale their deployments by using additional servers or blade servers, UCS Manager, RAID storage, a different hypervisor, or networking components.

- The Cisco SBA—Data Center Unified Computing System Deployment Guide provides the processes and procedures necessary to deploy a Cisco Unified Computing System using both the Cisco B-Series Blade Server system and Cisco C-Series Rack-Mount Servers to a point where they are ready to deploy an operating system or hypervisor software.
- The Cisco SBA—Data Center Virtualization with Cisco UCS, Nexus
   1000V, and VMware Deployment Guide describes how to deploy a
   VMware hypervisor on the Cisco Unified Computing System, including
   both the Cisco B-Series Blade Servers and Cisco C-Series Rack-Mount
   Servers. It also describes how to install and deploy Cisco Nexus 1000V
   Series Switches as a full-featured virtual switch for the VMware servers.

- The Cisco SBA—Data Center Design Overview provides an overview of the data center architecture. This guide discusses how the Cisco SBA data center architecture is built in layers—the foundation of Ethernet and storage networks and computing resources; the data center services of security, application resilience, and virtual switching; and the user services layer that contains applications and user services.
- The Cisco SBA—Data Center Deployment Guide focuses on the processes and procedures necessary to deploy your data center foundation Ethernet and storage transport. The data center foundation is designed to support the flexibility and scalability of the Cisco Unified Computing System and provides details for the integration of functionality between the server and the network for Cisco and non-Cisco servers. The foundation design includes data center services like security with firewall and intrusion prevention, and application resiliency with advanced server load-balancing techniques. This guide also discusses the considerations and options for data center power and cooling. The supplemental Data Center Configuration Files Guide provides snap-shots of the actual platform configurations used in the design.

There are also a number of related Cisco SBA Bring Your Own Device (BYOD) guides, which are helpful for deploying the client connectivity to the network for VDI access. They include:

- Cisco SBA Solutions—BYOD—Virtual Desktop Access Deployment Guide
- Cisco SBA Solutions—BYOD—Advanced Guest Wireless Access
   Deployment Guide
- Cisco SBA Solutions—BYOD—Identification and Authentication
   Deployment Guide
- Cisco SBA Solutions—BYOD—Internal Corporate Access Deployment Guide
- Cisco SBA Solutions—BYOD—Remote Mobile Device Access
   Deployment Guide

### **Business Overview**

Smaller organizations face many of the same IT challenges as larger organizations when trying to accommodate increasing demand for new IT capabilities and services. They often place even greater emphasis on cost savings and on protecting business-critical systems and data because they have smaller IT staffs and budgets, and they need to leverage IT assets to their fullest extent. Organizations require cost-effective solutions that can better leverage their existing server, storage, and network resources.

To improve availability and ensure business continuity, organizations need efficient ways to maintain production systems while minimizing downtime. Virtualization technology simplifies IT so that organizations can more effectively use their storage, network, and computing resources to control costs and respond faster. The virtual approach to IT management creates virtual services out of the physical IT infrastructure, enabling administrators to allocate these resources efficiently.

With virtualization, hardware management is completely separated from software management, and hardware equipment can be treated as a single pool of processing, storage, and networking resources to be reallocated as needed to various software applications. In a virtual infrastructure, users see resources as if they were dedicated to them—while administrators gain the ability to efficiently manage and optimize resources to serve the needs of the organization.

## **Technology Overview**

#### **Virtual Desktop Infrastructure**

VDI delivers a desktop and workspace virtualization solution that can dramatically improve business operations and data security while increasing end-user productivity, mobility, and flexibility. The premise of VDI is to decouple the location of the execution of the application from where the client resides allowing new client compute paradigms. These tools to help enterprises rapidly respond to events such as mergers and acquisitions, open new branch offices, and maintain business continuity across workplace interruptions. By keeping the work data centrally located and not available on storage of devices such as laptops leaving the organization's facilities, data is retained by the organization in the data center, where it can be protected. Managing the virtual machines on the physical servers and the connected networks requires a design that integrates all of these systems so that they work together without creating an operational burden on the IT staff who must maintain them. Using proven and tested designs lowers the time needed to deploy these new solutions and reduces the time required to deploy new applications.

In a VDI deployment, a worker's desktop operating system and applications run in a virtual machine on a server hosted in a data center or server room. A VDI client, which can be in the same building, the same network, or remotely accessing the network across the Internet, views and operates the worker's desktop. The organization can deploy VDI client software on desktops, laptops, or deploy dedicated appliances. When organizations also permit a Bring Your Own Device (BYOD) environment, workers can use personal laptops, tablets, and even smartphones, for similar remote desktop access.

In the data center or server room, this deployment uses Cisco UCS servers to host the virtual desktops and other data center services required to complete the solution, such as the Microsoft Active Directory servers, certificate authorities, and the Cisco Identity Solution Engine (ISE). Deploying the initial VDI solution with a Cisco UCS C-Series rack-mount server ensures that as an organization grows, the deployment can grow using advantages of unified computing, while integrating into the tested Cisco SBA data center architecture.

Cisco ASA Firewalls are used in the server room to implement security policies between the virtual desktop VLANs and organizational or customer confidential information running on application servers in the server VLANs. A separate set of Cisco ASA Firewalls are used in the Internet edge to isolate and protect the organization from Internet originated attacks. The firewalls also provide the remote access VPN termination point, allowing users to access the solution from remote locations.



This guide simplifies deployment, focuses on two vendors (Cisco and Citrix), and details the use of a non-high-availability, single server with local storage. Hypervisor modifications for performance and high availability setups are not covered for this basic deployment guide. The Citrix VDI-in-a-Box software used in this solution has the capability to easily add servers for high availability and scale as you grow.

#### Cisco Unified Computing System C-Series Rack-Mount Servers

Cisco UCS C-Series servers are rack-mount servers designed to operate in a standalone environment, or as part of the Cisco Unified Computing System. The Cisco UCS C-Series servers offer a wide array of processor, memory, network adapter, and disk options. They offer Cisco innovations such as extended memory and network-aware VN-Link technologies.

The Cisco Integrated Management Controller (Cisco IMC) is the management service for Cisco C-Series servers. Cisco IMC runs within the server and allows administrators to use a web-based GUI or Secure Shell (SSH) Protocol-based CLI to access, configure, administer, and monitor the server. Almost all tasks can be performed in either interface, and the results of tasks performed in one interface are displayed in the other. Cisco IMC is used to perform the following server management tasks, including (but not limited to):

- Power on, power off, power cycle, reset, and shut down the server
- · Configure the server boot order
- · View server properties and sensors
- Configure network-related settings, including network interface controller (NIC) properties and network security
- Configure communication services, including HTTP, SSH, Simple Network Management Protocol (SNMP), and Intelligent Platform Management Interface (IPMI) over LAN
- Update Cisco IMC firmware
- Monitor faults, alarms, and server status

#### Tech Tip

You use the anticipated quantities and types of workloads to choose an appropriately sized server. A guide and calculator for server sizing with VDI-in-a-Box workloads can be consulted at the Citrix web site, here:

http://www.citrix.com/products/vdi-in-a-box/resources-and-support. html

#### **Citrix VDI-in-a-Box**

Citrix is a computing virtualization provider, with technology solutions to equip organizations for optimizing the use of their existing IT assets and resources, as well as protecting the systems, data, and applications that run the business. As virtualization adoption increases, the benefits are making this compelling virtualization technology a mainstream mandate. Citrix XenServer technology allows virtual machines (VMs) to be easily created as needed, and migrated from one hardware platform to another.

This deployment guide uses Citrix VDI-in-a-Box — a single virtual appliance that provides all of the functionality needed to create, provision, manage, and load balance virtual desktops. VDI-in-a-Box has a built-in connection broker, load balancer, user manager, and desktop provisioning server, called vdiManager. It does not require separate shared storage, high-speed interconnects, or multiple management servers. The appliance runs on servers running a hypervisor, such as Citrix XenServer, Microsoft Hyper-V, or VMware ESXi. Citrix XenServer is chosen for the basic implementation in this deployment guide, easing deployment by using the minimum number of software suppliers.

Citrix vdiManager is the management component of the Citrix VDI-in-a-Box. Citrix vdiManager can run on a single physical server for a basic installation, or for high availability a collection of physical servers can run the vdiManager, referred to as a VDI-in-a-Box grid. For larger implementations, you can use the grid for one logical view of all vdiManager instances, which brokers client connections across servers in the grid for load balancing and high availability. For a basic VDI implementation for Cisco SBA, you use a single server.



Figure 2 - VDI-in-a-Box logical components

For more information about the Citrix VDI-in-a-Box solution, see the Citrix VDI-in-Box product documentation site, here:

http://support.citrix.com/proddocs/topic/vdi/vdi-landing-page-main. html

Cisco and Citrix offer a solution, "Cisco Solution for Citrix VDI-in-a-Box," which is an all-in-one reference package that is simple and affordable, combines the Cisco UCS C-Series Server with Citrix VDI-in-a-Box software to deliver a rich end-user experience. **Tech Tip** 

For more information about Cisco solutions with Citrix, see the site here:

http://cisco.com/go/citrix

#### **Citrix Receiver**

Citrix Receiver helps provide VDI-in-a-Box desktop users with secure connections to a high-definition user experience. Although the desktops run on remote servers, the user experience is equivalent to that of a local Windows desktop. From the user's perspective, logging on to a virtual desktop is the same as logging on to a local desktop. The Citrix Receiver client runs on PCs, tablets, and smartphones. Microsoft Windows 7, Apple iOS, and Android Citrix Receiver access is tested in this guide to validate solution functionality.

### Notes

## **Deployment Details**

#### Process

Configuring Cisco UCS C-Series Server Hardware

1. Configure Cisco IMC management access

You can use the Cisco Integrated Management Controller (Cisco IMC) to set up the Cisco UCS C-Series Rack-Mount Server and complete the basic configuration to prepare for Ethernet communications. Cisco IMC is the management service built into and running within the server. Cisco IMC allows you to use a web-based GUI or SSH-based CLI to access, configure, administer, and monitor the server. Almost all tasks can be performed in either interface, and the results of tasks performed in one interface are displayed in the other.

Cisco UCS C-Series Rack-Mount Servers are connected to available Ethernet interfaces in the Cisco SBA data center infrastructure. Dual 10-Gigabit Ethernet ports are used for virtual desktop communication. An additional 100-Mbps Ethernet connection is used for the integrated management, and another Gigabit Ethernet connection is used for hypervisor management. Details for data center core port configurations are covered in the Cisco SBA—Data Center Deployment Guide.

#### Procedure 1

**Configure Cisco IMC management access** 

**Step 1:** Connect a keyboard, video display, and mouse to the server for the initial setup, and then power up the server.

**Step 2:** When the server boots up, you have the option to set up BIOS, boot menu, network boot, and Cisco IMC Configuration. While in BIOS, press F8. The Cisco IMC Configuration starts.



Step 3: Under NIC mode, press the Spacebar. This enables Dedicated.

**Step 4:** You either statically assign a management IP address or have a DHCP server servicing the VLAN or subnet connected to the server management interface for remote Cisco IMC access. This procedure assigns a static IP address to the server and requires the following information:

- · IP address—10.4.63.69
- · Subnet mask-255.255.255.0
- · Default gateway-10.4.63.1
- Password

**Step 5:** Under IPV4 (Basic), press the **Spacebar**. This disables DHCP enabled.

Step 6: Enter values for CIMC IP, Subnetmask, and the default Gateway.

NIC Properties NIC mode		
		NIC redundancu
Dedicated:	[X]	None: []
Shared LOM:	[]	Active-standby: [X]
Shipping:	[]	Active-active: []
Shared LOM 10G:	ii	
Cisco Card:	i i	
IPV4 (Basic)		Factory Defaults
DHCP enabled:	[]	CIMC Factory Default:[]
CIMC IP:	10.4.63.69	Default User (Basic)
Subnetmask:	255.255.255.0	Default password:#########
Gateway:	10.4.63.1	Reenter password:#########
VLAN (Advanced)		
VLAN enabled:	[]	
VLAN ID:	1	
Priority:	0	
****	*****	*******
<up arrow="" down=""> \$</up>		<f10> Save <space bar=""> Enable/Disable</space></f10>
<f5> Refresh</f5>		<esc> Exit</esc>

Step 7: Under NIC redundancy, verify that Active-Standby is enabled.

**Step 8:** If you are using a server with a single management NIC, like the Cisco C200 Series, select a **NIC redundancy** of **None**.

**Step 9:** Under Default User (Basic), enter a value for **Default password**. The default username is **admin**.

Step 10: Press F10. This saves the settings.

**Step 11:** Press **F5** (**Refresh**). The display is updated to reflect the latest configuration.

**Step 12:** Wait until the new settings appear, and then press **ESC** (**Exit**). The server reboots, and this interface becomes available from a web browser.



tion with the Cisco IMC. You download the image and store it on the local management workstation.

**Step 1:** Open the Cisco IMC login page in a web browser, using the IP address assigned previously in the Cisco IMC configuration: http://10.4.63.69.

A security certificate warning may be received in your browser on initial login before you can connect to the login screen.

**Step 2:** Acknowledge and proceed past any browser certificate warnings, which vary by web browser. Acknowledgement allows you see the login screen and to proceed to the next step.



**Step 3:** Log in by using the default username **admin** and the password you configured earlier.



Step 4: On the Server tab, click Remote Presence.

Step 5: On the Virtual Media tab, verify that **Enabled** is selected.

Overall Server Status	C 🕴 🕹 🗮 🛛 😧 🛈
Good	Remote Presence
Server Admin	Virtual KVM Virtual Media Serial over LAN
Summary	Actions
Inventory	Launch KVM Console
Sensors	
System Event Log	vKVM Properties
Remote Presence	Enabled: 🗹
BIOS	Max Sessions: 4
Power Policies	Active Sessions: 0
Fault Summary	Remote Port: 2068
	Enable Video Encryption:
	Enable Local Server Video: 🗹

Tech Tip

If you do not select **Enabled** and you try to map a remote disk, an error is displayed, starting with "**Either Virtual Media is detached or**..."

#### Step 6: Click Save Changes.

**Step 7:** Click the keyboard image button. A keyboard, video, and monitor (KVM) console launches, allowing manipulation of the server and its drive mappings.

cisco Integrated Management Controller			
Overall Server Status	C   🕹 🛃   🔞 0		
Good	Remote Pre Launch KVM Console		
Server Admin	Virtual KVM Virtual Media Serial over LAN		

#### Step 8: Click the VM tab of the KVM console.

10.4.63.69 - KYM Console			>
File Help			
KVM VM			
Client View			
Mapped	Read Only	Drive	Exit
		🖃 I: - Removable Disk	
	$\checkmark$	🖃 H: - Removable Disk	Create Image
	V	🖃 G: - Removable Disk	Add Image
	$\checkmark$	F: - Removable Disk	Remove Image
	$\checkmark$	솔 E: - CD/DVD	Details ±

**Step 9:** Click **Add Image**. The Open dialog box for selecting an image is displayed.

Step 10: Select a local copy of the XenServer .ISO installation image.

🛓 Open		×
Look <u>i</u> n: 📑	admin	▼ A 🔂 C 88 5
	Windows 7 Enterprise 64Bit.ISO	XenServer-6.0.201-install-cd.iso
•		
File <u>N</u> ame:	XenServer-6.0.201-install-cd.iso	
Files of <u>T</u> ype:	Disk image file (*.iso, *.img)	•
		Open Cancel

**Step 11:** Select the check box in the **Mapped** column for the ISO file. Do not click **Exit** when complete. Instead, proceed to the next step.

Step 12: Click on the KVM tab of the KVM console.

Step 13: Above the KVM and VM tabs, click Macros, and then select Ctrl-Alt-Del. A server reboot is initiated, while the mapped XenServer .ISO file is available.

You can observe the server boot process from the same KVM Console. On new servers without BIOS changes to the boot sequence, the default boot sequence starts with booting from the Cisco Virtual CD/DVD, if it's available.

If the server does not boot from the XenServer ISO image, the following optional step can be used to force this boot behavior. Skip this step if you can see the XenServer installation begin, with a "Welcome to XenServer" screen.

Step 14: If you don't see the "Welcome to XenServer" screen, during the server's power-on self-test, press F6 (Boot Menu). Use the arrow key to select Cisco Virtual CD/DVD, and then press Enter. Do not close the virtual media screen while it is in use.

	HL-DT-STDVDRAM GT40N
Cisco	Virtual CD/DVD 1.22
Cisco	Virtual FDD/HDD 1.22
Cisco	Virtual Floppy 1.22
(Bus 0	95 Dev 00)PCI RAID Adapter
SanDis	-
VM	eUSB DISK 4109
	6.0.12 Slot 0300
	.0.12 Slot 0301
	.0.40 Slot 0400
	.0.40 Slot 0401
	NIC 14:0.0
	NIC 15:0.0
	NIC 28:0.0
	NIC 29:0.0
	al EFI Shell
Enter	seruh
T	and ↓ to move selection

#### **Procedure 2**

#### **Configure Citrix XenServer host**

After the boot sequence proceeds, a Citrix XenServer installation screen appears. Installation continues to proceed unassisted until the "Welcome to XenServer" screen is displayed.



This procedure assigns basic server network configuration options, and requires the following information:

- XenServer Management IP address—10.4.63.85
- Subnet mask—255.255.255.0
- Default gateway—10.4.63.1
- Hostname—viab-1
- · DNS Server-10.4.48.10
- NTP Server—10.4.48.17

Step 1: Use arrows to highlight the correct keyboard, if it is different from the default, press **Tab** to highlight **Ok**, and then press **F12**.

**Step 2:** Press **F12**. This accepts the default at the "Welcome to XenServer Setup" dialog box that warns about disk erasure.

**Step 3:** At the End User License Agreement dialog box, **Tab** to **Ok**, and then press **F12**. This accepts the EULA.

**Step 4:** If a previous version of XenServer is detected on the hard disk, and the Action To Perform screen is displayed, select **Perform clean installation**, **Tab** to **Ok**, and then press **F12**.

**Step 5:** On the Virtual Machine Storage dialog box, use arrow keys and space bar to highlight and select the appropriate storage destination, **Tab** and press **spacebar** to select **Enable thin provisioning (Optimized storage for XenDesktop)**, and then **Tab** to **Ok** and press **F12**.



This option enables a Citrix XenDesktop performance enhancement, named IntelliCache, which saves I/O operations.

## Step 6: For the Select Installation Source dialog box, select Local media, Tab to Ok, and then press F12.

Step 7: At the Supplemental Packs dialog box, Tab to select No, and then press F12.

**Step 8:** At the Verify Installation Source dialog box, select **Verify installation source**, **Tab** to **Ok**, and then press **F12**. There is a few minutes wait while the installation source files in the ISO image are verified. Step 9: At Verification Successful box, press F12.

Step 10: At the Set Password dialog box, enter a password, confirm the password, Tab to Ok, and then press F12.



**Step 11:** When the Networking dialog box is displayed, select the primary interface that is connected into the management network, **Tab** to **Ok**, and then press **F12**.

**Step 12:** When a second Networking dialog box appears, **Tab** and press spacebar. This selects **Static configuration**.

Step 13: Enter the following values and then press F12.

- IP address—10.4.63.85
- · Subnet mask-255.255.255.0
- · Gateway-10.4.63.1

**Step 14:** At the Hostname and DNS Configuration dialog box, use **Tab** to enter the **Hostname** and the appropriate **DNS Server**, **Tab** to **OK**, and then press **F12**.

🔲 10.4.63.69 - KYM Console
File View Macros Tools Help
KVM VM
Welcome to XenServer - Version 6.0.2 (#53456p) Copyright (c) 2011 Citrix Systems, Inc.
Hostname and DNS Configuration
Hostname Configuration Hostname: Viab-1
DNS Configuration
DNS         Server         1:         10.4.48.10           DNS         Server         2:
Back
<pre></pre>

**Step 15:** At **Select Time Zone**, use arrows to select the geographical area, **Tab** to **Ok**, and then press **F12**.

Step 16: At the second Select Time Zone screen, pick a location in the same time zone as the server, Tab to Ok, and then press F12.

Step 17: At the System Time dialog box, select Using NTP, Tab to Ok, and then press F12.

Step 18: At the NTP Configuration screen, enter the address of the NTP Server, Tab to Ok, and then press F12.

**Step 19:** At the **Confirm Installation** dialog box, press Tab to highlight **Install XenServer**, and then press the spacebar. Note that **F12** does not continue to next screen for this dialog box, but instead returns you to the previous screen.



The XenServer host hypervisor continues to install for several minutes. When the installation is nearly complete, it asks for any additional components to add onto the installation. **Step 20:** At the **New Media** dialog box, press **Tab** to highlight **Skip**, and then press the spacebar.



The Installation Complete dialog box appears, but do not press Enter.



Before you reboot, note that if the ISO installation image is still mapped to the server, the default is to boot from this image again. The next step validates the removal of the mapping, allowing the server to boot from the installation on the hard drive. **Step 21:** Click the **VM** tab in the KVM Console and verify that the XenServer ISO Image File does not have a check mark in the **Mapped** column.

	10.4.63.69 - K	WM Console		
Fil	e Help			
K	VM VM			
	Client View			
	Mapped	Read Only	Drive	Exit
		$\checkmark$	🖃 I: - Removable Disk	
		V	🖃 H: - Removable Disk	Create Image
		$\checkmark$	🖃 G: - Removable Disk	Add Image
		$\checkmark$	F: - Removable Disk	Remove Image
		$\checkmark$	🚔 E: - CD/DVD	Details ±
			A C:\Users\admin\XenServer-6.0.201-install-cd.iso - ISO Image File	

**Step 22:** Click the **KVM** tab on the KVM Console. This returns you to the Installation Complete screen.

**Step 23:** Select **OK** by pressing **Enter**. The server reboots and loads from the new XenServer installation.

It takes several minutes to load the Linux OS with Citrix components after the reboot. Upon completion, a graphical XenServer screen with progress bar is displayed.



The graphical screen is replaced by a text progress screen, as the server continues to boot into the XenServer host environment. Once the XenServer host is running, the status displays on the configuration screen of the KVM console.

ns Inc 2-C460 .0.2-53456p Network Parameters eth0
2-C460 .0.2-53456p Network Parameters eth0
2-C460 .0.2-53456p Network Parameters eth0
2-C460 .0.2-53456p Network Parameters eth0
- Network Parameters eth0
eth0
10.4.63.85
255.255.255.0 10.4.63.1
10.4.05.1
r> to display the SSL key
s for this host
r> to disp:

#### Process

Installing Citrix XenCenter

- 1. Install XenCenter management tool
- 2. Enable XenCenter to manage XenServer
- 3. Create XenServer network connections

**Step 6:** Accept the default destination folder and installation user by clicking **Next**.

Step 7: On the Ready to install Citrix XenCenter dialog box, click Install.

**Step 8:** Accept any security warnings as the Setup Wizard begins the installation.

Step 9: On the Completed the Citrix XenCenter Setup Wizard dialog box, click Finish.

Step 10: Citrix XenCenter is now installed on the management workstation.

#### **Procedure 1**

Install XenCenter management tool

You use the Citrix XenCenter management tool to manage any virtual machines that will be generated and running on Citrix XenServer. Citrix XenCenter comes with Citrix XenServer, and the installation image can be obtained via web browser access to an automatically started web server, enabled as a result of the Citrix XenServer host installation.

Step 1: Open a web browser from the management workstation, and then connect to the IP address of the XenServer by typing the IP address, 10.4.63.85, as the browser URL destination.

The browser now displays the following:

Citrix Systems, Inc. XenServer 6.0.2, with hyperlinks to:

XenCenter CD image and XenCenter installer.

Step 2: Click XenCenter installer. The link to the XenCenter.msi file opens.

**Step 3:** Click **Save File**. This saves the XenCenter.msi file to the management workstation.

**Step 4:** Double-click the **XenCenter** icon for the downloaded file to launch the installation, and accept any security warning that may be displayed as part of the installation.

Step 5: On the Citrix XenCenter Setup dialog box, Click Next.

Procedure 2

Enable XenCenter to manage XenServer

**Step 1:** From the Windows Start menu on the management station, launch Citrix XenCenter. The main XenCenter window appears.



Step 2: Click Add New Server.

**Step 3:** In the Add New Server dialog box, enter the Citrix XenServer name and the root password configured during the XenServer installation.

Add New Se	erver	? ×
	t name or IP address of the server you want to add and in credentials for that server.	
Server:	viab-1.cisco.local	•
User login cr	edentials	
User name:	root	
Password:		
<u></u>	Add Cance	

Citrix XenCenter connects and synchronizes with the XenServer installation, and displays information for the server.

file View Pool Server VM	Storage Templates Tools Window H	telp					
	Add New Server   🚏 New Pool 箇 New St		) Shut Down 🛞 Rebo	ot 🕕 Suspend			V No System Alert
w: Server View 🔎 🔹	😼 viab-1						Logged in as: Local root accour
<ul> <li>⊘ macrotreer</li> <li>⇒ book</li> <li>&gt; book</li></ul>	Starth   General   Memory   Storage   Network viab-1 Overview Search Options • Name Web-1 Default install of Xenderver	CPU Usage	Used Memory 2080 of 98163 MB	Disks (avg / max kBp)	Network (avg [ max (HB) 0/1	Address 10.4.63.85	Uptime 1 hour 11 minutes

Procedure 3

**Create XenServer network connections** 

The Cisco UCS C-Series server includes multiple Ethernet NIC connections. Two are associated for use together as dual active connections to the Cisco SBA data center, allowing resiliency and load sharing of desktops between links. Because the server is hosting client virtual desktop machines, its behavior can be characterized as being similar to the activity of many clients, and thus it is placed in the client VLAN in the data center. Traffic to and from the server network interfaces is tagged with the client data center VLAN 157.

Use Citrix XenCenter to configure the network, creating desktop VMs in later steps. To manage the server hardware and hypervisor, use NIC 0 and NIC 1 network interfaces. For traffic to the Citrix XenServer VMs, use 10Gbps NIC 4 and NIC 5 network interfaces.

Table 1 - Cisco UCS Server network interface assignments

Cisco UCS interface	Туре	Use	VLAN
NIC 0	100 Mbps Ethernet	CIMC	163 - Management
NIC 1	Gigabit Ethernet	Hypervisor	163 - Management
NIC 4	10-Gigabit Ethernet	VDI communication	157 - DC user
NIC 5	10-Gigabit Ethernet	VDI communication	157 - DC user

**Step 1:** In the XenCenter management console, highlight the installed XenServer instance, and then click the **NICs** tab. When the NICs are connected to data center switch ports that are enabled, the active network interfaces, NIC 4 and NIC 5, appear with a Link Status of **connected**.

**Step 2:** Click the **Networking** tab, and then click **Add Network**. A New Network dialog box appears.

Step 3: Select Bonded Network, and then click Next.

Step 4: Select NIC 4 and NIC 5, the two available Connected NICs, to bond. Leave Bond mode as Active-active, keep the default MTU, and enable Automatically add this network to new virtual machines by selecting the box next to the option.

elect Type and Members		ect the NJ led to nev		use in this bond	and the bond :	settings, an	d confirm whether this net	work should be
		NIC	MAC	Link Status	Speed	Duplex	Vendor	Device
		NIC 0	44:d3:ca:da:22:46	Connected	100 Mbit/s	Full	Broadcom Corporation	NetXtreme II BCM!
		NIC 1	44:d3:ca:da:22:48	Connected	1000 Mbit/s	Full	Broadcom Corporation	NetXtreme II BCM5
		NIC 2	44:d3:ca:da:03:c0	Disconnected		-	Broadcom Corporation	NetXtreme II BCM
		NIC 3	44:d3:ca:da:03:c2	Disconnected		-	Broadcom Corporation	NetXtreme II BCM5
	V	NIC 4	cc:ef:48:cf:33:fa	Connected	10000 Mbit/s	Full	Cisco Systems Inc	VIC Ethernet NIC
		NIC 5	cc:ef:48:cf:33:fb	Connected	10000 Mbit/s	Full	Cisco Systems Inc	VIC Ethernet NIC
		NIC 6	cc:ef:48:cf:22:75	Disconnected		-	Cisco Systems Inc	VIC Ethernet NIC
		NIC 7	cc:ef:48:cf:22:76	Disconnected	-	-	Cisco Systems Inc	VIC Ethernet NIC
	Bor	nd mode:	Active-active     Active-passive					<u>,</u>
	MT		1500	-				

Step 5: Click Finish. The new bonded network is displayed.

**Step 6:** On the Networking tab, click **Add Network** again. This time, select **External Network**, and then click the **Next**.

🛞 New Network - viab-1		_ 🗆 🗙
Enter a name and de	scription for the new network	0
Select Type Details	Provide a name and optional description for the new network.	
Interface	Name: VDI-Client Description: Network for VDI client traffic.	
CÎTRIX	Constant Landa - Califa	[
	< Previous Next > Finish	Cancel

Step 7: Click Details, in the Name box, enter VDI-Client, in the Description box, enter Network for VDI client traffic, and then click Next.

Step 8: Click Interface.

Step 9: In the NIC list, choose Bond 4+5, in the VLAN list, enter 157, in the MTU list, leave the default, and then enable Automatically add this network to new virtual machines by selecting the box next to the option.

New Network - viab-1     Choose the network	Location for the new network
Select Type Details Interface	Your new network will be mapped to an existing physical network interface and assigned a VLAN number to use on that interface. You can select the physical interface you would like to use below.         NIC:       Bond 4+5         VLAN:       157         MTU:       1500         Image: Automatically add this network to new virtual machines
CÎTRIX.	
	< Previous Next > Finish Cancel

Step 10: Click Finish. The newly created network interfaces are displayed.

_	
	Process
	Installing Citrix VDI-in-a-Box Manager
	1. Download and extract vdiManager
	2. Create and configure a single-server grid

Citrix has a virtual appliance called VDI-in-a-Box Manager, also known as vdiManager, which manages virtual desktop creation and assignments for the Citrix XenServer host hypervisor. The vdiManager virtual appliance provides a central installation resource to create, provision, manage, and load balance virtual desktops. This deployment uses the Citrix VDI-in-a-Box version 5.1, which has built-in functionality that includes a connection broker,

load balancer, user manager, and desktop provisioning server. Installation burden is eased by not having to install each function separately, and administrative and cost burdens are eased by not requiring separately provisioned shared storage, high-speed interconnects, or multiple management servers.

#### **Procedure 1**

Download and extract vdiManager

**Step 1:** From a web browser on the management station, navigate to https:// www.citrix.com and download the VDI-in-a-Box version 5.1 for XenServer, called VDI-in-a-Box\_XenServer\_v5\_1\_x.zip.

**Step 2:** Double-click on the .zip file icon. This opens and extracts the vdiManager\_Xen\_v5\_1\_x.xva file from the .zip file to the local hard drive.

Step 3: Return to the XenCenter management console, click File, and then click Import.

Click Browse, navigate to the extracted .xva file name, and then click Next.

🗴 Import	× II.
Success the file year the file	ou want to import ()
Import Source Location Storage Networking Finish	Enter the pathname of an exported VM or template, an OVF/OVA package or a virtual hard disk image file or click Browse to find the file you want. Filename: C:\Users\admin\VDI-in-a-Box_XenServer_vS_1_0\vdiManager_Xen_vS_1_0.xva Browse
CITRIX.	< Previous Next > Finish Cancel

**Step 4:** Ensure the previously created XenServer host is highlighted as the **Home Server**, and then click **Next**.

🛞 Import XVA	
Select the location w	where the imported VM will be placed
Import Source Home Server	Click on a server to nominate it as the home server for the imported VM or for any new VMs to be based on the imported template. The home server will be used by default to start up the VM and to provide resources such as local storage.
Storage Networking Finish	Click on a pool if you do not want to nominate a home server: the most suitable available server will be used.

**Step 5:** Select the default storage for the VMs on the UCS server, and then click **Import**. XenCenter prepares for the import, and the Select network to connect VM dialog box appears.

Step 6: Using the drop-down menu in the Network column, associate the VDI-Client network to the highlighted interface 0 in the Name column.

Select network to co	nnect VM			0
Import Source Home Server Storage	The default virtual delete virtual netw When you have fin Virtual network inte	ork interfaces, if required. ished, click "Next" to continue t	plate you have selected are listed below. You can add, modi o the next page.	'y or
Networking	Name	△ MAC Address	Network	
Finish	interface 0	e2:93:f4:63:26:2b	VDI-Client	-
<b>CITRIX</b>			AddDe	lete
			< Previous Next > Finish	Cancel

Step 7: On the Review the import settings dialog box, keep the default Start VM(s) after import selection, and then click Finish.

The operation takes several minutes to complete. You can view status at the bottom of the XenCenter screen, with text at the left bottom, and a progress bar at the right bottom. The vdiManager\_Xen\_v5\_1\_0 VM is displayed in the search tree on the left with a yellow status icon, signifying that the virtual machine has not started.

When the import is complete, and the virtual appliance is started, the VM status icon associated with the vdiManager changes to green.

**Step 8:** If you want to confirm the VM is operational, highlight the VM, and then click the **Console** tab. The following view of XenCenter shows an example confirmation that the vdiManager virtual appliance is running.

File View Pool Server VM		
🕒 Back 🝷 💮 Forward 🝷 🛙 📑 Ad	d New Server 📋 🏪 New Pool 는 New Storage 🛅 New VM 🕴 🍑 Shut Down 🥳	Reboot 🛛 🗸 No System Alerts
how: Server View 🔎 🔹	🐻 vdiManager_Xen_v5_1_0	Logged in as: Local root accou
<ul> <li>XenCenter</li> <li>viab-1</li> <li>viab-1</li> <li>DVD drives</li> <li>Local storage</li> <li>Removable storage</li> </ul>	General Memory Storage Networking Console Performance Snapshots Logs DVD Drive 1: <empty> Starting RPC idmapd: [ OK ] Starting system nessage bus: [ OK ] Mounting other filesystems: [ OK ] Starting system logger: [ OK ] Starting system logger: [ OK ] Detecting Linux distribution version: [ OK ] Starting system logger: [ OK ] Starting console nouse services: O00.oops(): [server_tow n /dev/input/mice. [ OK ] Starting xfs: 10:20:11 (CITRIX) FLEXnet Licensing version i66_1Sb 10:20:11 (CITRIX) Inrenove disabled [  OK ] Starting kmgr: tomcat started: /home/kum/kum/ Starting gos: Starting Quahi daemon [ OK ] Starting Quahi daemon [ OK ]</empty>	abled, assuming '-allowS pls.c(76)]: Could not op

#### Procedure 2

Create and configure a single-server grid

Once the vdiManager is started and powered on in the XenServer host hypervisor, initial configuration of vdiManager is done by web browser. The IP address for the vdiManager is initially assigned via DHCP. This dynamic address will be changed to a static IP address in a later procedure, to allow VDI-in-a-Box users to access the VDI-in-a-Box service by a well-known IP address and Domain Name System (DNS) entry.

Step 1: In the Citrix XenCenter management window, click the vdiManager\_Xen\_v5\_1\_X server instance in the navigation tree, and then click the Networking tab. The IP Address column shows the address dynamically assigned to the vdiManager server when booting. This IP address is used in the next step.

**Step 2:** In the web browser URL box, type the following, replacing the **10.4.57.39** address with the current dynamically assigned address obtained from the previous step:

https://10.4.57.39/admin/

Step 3: Open the vdiManager Administrator Login page by pressing Enter.

Depending on browser configuration, there may be a number of security warnings. Respond to the warnings in order to allow the connection to succeed. When the connection is made, a login prompt is shown. **Step 4:** At the Citrix Receiver Administrator Login prompt, enter the default **Username** and **Password** credentials, which are **vdiadmin** and **kaviza**, and then click **Log On**.



The VDI-in-a-Box Welcome! screen is displayed.

## Welcome!

VDI-in-a-Box

Thank you for choosing VDI-in-a-Box. We want this to be a fast and pleasant experience. Below is a brief overview of the set up process. If you want background information on VDI-in-a-Box before you get started, go to support.citrix.com/vdi-in-a-box.

#### Overview

Below are the 4 steps you will need to complete in order to generate desktops for your users.



#### Step 5: Click Get Started, and then click Continue.

The Citrix VDI-in-a-Box virtual appliance detects that the host hypervisor it is running on is Citrix XenServer. Automating the installation process requires the IP address, user name, and password previously assigned to the XenServer host hypervisor. Step 6: In the IP Address box, enter 10.4.63.85, in the User Name box, enter root, in the Password box, enter the previously assigned password, and then click Next.

Hypervisor	VDI-in-a-Box has detected that your hypervisor is <b>Citrix XenServer</b> . to the hypervisor, please enter the credentials below.					
Datastore						
Grid	IP Address:	10.4.63.85				
	User Name:	root				
Configuration	Password:	•••••				

Step 7: In the Datastore list, choose the Cisco UCS local storage, in the Network Label list, choose VDI-Client, and then click Next.

🖌 Hypervisor	Hypervisor selected: Citrix XenServer, 10.4.63.85					
Datastore	Select the datastore where your images and desktops reside and the network the desktops should be connected to.					
Grid						
Configuration	Datastore:	Local storage (2188 GB free/2188 GB total)	-			
, ř	Network Label:	VDI-Client	-			

Step 8: For the Grid option on the displayed window, select Create a new VDI-in-a-Box grid, and then click Next.

**Step 9:** This vdiManager becomes the only member of the single-server grid, and the next screen is displayed.

**Step 10:** For User Database, select **Microsoft Active Directory**. More fields become available to fill out.

Step 11: In the IP Address box, enter 10.4.48.10, in the Domain box, enter cisco.local, in the User Name box, enter Administrator, in the Password box, enter the password, and then click Next.

<ul> <li>Hypervisor</li> </ul>	Hypervisor selected: Citrix	XenServer, 10.4.63.85
🗸 Datastore	User Database:	○ VDI-in-a-Box workgroup
🗸 Grid		• Microsoft Active Directory
	IP Address:	10.4.48.10
Configuration		(Domain example: example.com)
	Domain:	cisco.local
	User Name:	Administrator
	Password:	•••••
		,

**Step 12:** Click **Yes**, which acknowledges that a reserved IP address is used, and then click **Done**.

The Generate a Base Desktop Image screen is displayed.

	⁰ ≣	<sup>®</sup> '≣'≣	⁰ ♣
Set up your Hypervisor and VDI-in-a-Box Grid	Generate a Base Desktop Image	Create Desktop Templates from the Base Image	Assign Users to Desktops
To complete this step you w	/III need the following:		
<ul> <li>You have suf</li> </ul>	: y one DHCP server within ficient DHCP addresses a time is adjusted for short	wailable	
<ul> <li>There is only</li> <li>You have suf</li> <li>DHCP lease</li> </ul>	r one DHCP server within ficient DHCP addresses a time is adjusted for short	wailable	base desktop image
<ul> <li>There is only</li> <li>You have sufted</li> <li>DHCP lease</li> <li>A running Windows</li> <li>Credentials for an elemential</li> </ul>	r one DHCP server within ficient DHCP addresses a time is adjusted for short	ivailable release cycles 1 the hypervisor to copy as a 21	base desktop image
• There is only • You have suf • DHCP lease • A running Windows • Credentials for an o	r one DHCP server within ficient DHCP addresses a time is adjusted for short s XP or Windows 7 VM or existing domain controlle	ivailable release cycles 1 the hypervisor to copy as a 21	base desktop image

#### Process

Creating First OS Image and Template for Virtualized Desktops

- 1. Create the first Windows 7 VM image
- 2. Customize Windows image
- 3. Import Windows machine to vdiManager
- 4. Create template from published image

Citrix VDI-in-a-Box Manager has the ability to assign virtual desktops to users requesting them based on templates for the virtual desktop use case. A typical use case includes virtual desktops for task workers, where an identical desktop is assigned to all workers at each login or an unchanging desktop minimally customized per worker is assigned at login. Another use case is for knowledge workers with personalized desktops. In the knowledge worker use case, you create a Personal Virtual Desktop (PVD) for each worker. The base windows image is the same at login, but any file changes, application additions, and user customizations persist across logins.

The host hypervisor is used to create the base desktop image which is the basis for the vdiManager templates. In the Cisco SBA basic implementation for VDI using Citrix VDI-in-a-Box, the Citrix XenServer host hypervisor is used to create the guest Windows 7 64-bit desktop virtual machine image. The image is imported by vdiManager to create templates to allow for multiple guest machines to run on the host hypervisor.

#### **Procedure 1**

#### **Create the first Windows 7 VM image**

A Microsoft Windows 7 64-bit installation ISO must be available on the Citrix XenCenter management machine to use the following steps successfully. Alternatively, a network file server (NFS) mount or other remote disk could be used, as appropriate for the installation. The installation from a locally stored ISO image is covered in this guide. Step-by-step details for the Windows installation are not covered, as this is open for customization by the administrator.

Step 1: Copy the Microsoft installation ISO file to management machine.

Step 2: If the Cisco UCS C-Series KVM Console is not already open, direct a web browser to the CIMC management address (for this example, 10.4.63.69), and then click the Launch KVM Console icon. The console opens.

Step 3: In the KVM console, click the VM tab.

The Windows installation ISO file is mapped as a DVD drive available to the server, allowing the XenServer host to read it.

#### Step 4: Click Add Image.

**Step 5:** Navigate to the location of the stored Windows ISO image, select it, and then click **Open**.

10.4.63.69 - KVM Co	nsole	
File Help		
KVM VM		
Client View		
Mapped Read	I Only Drive	Exit
	I: - Removable Disk	Consta lucana
	H: - Removable Disk	Create Image
	G: - Removable Disk	Add Image
	F: - Removable Disk	Remove Image
	E: - CD/DVD	Details ±
Details     Target Drive     Virtual CD/DVD     Removable Media     Floppy	Open Look In: admin  Windows 7 Enterprise 64Bit.ISO XenServer-6.0.20 Image: Windows 7 Enterprise 64Bit.ISO File Name: Windows 7 Enterprise 64Bit.ISO Files of Type: Disk image file (*.iso, *.img) Open	
•	III	

Step 6: Under Mapped, select the check box for the ISO image.

	10.4.63.69 - K	VM Console	
File	e Help		
<b>K</b>	VM VM		
	Client View		
	Mapped	Read Only	Drive
		$\checkmark$	🖃 I: - Removable Disk
		$\checkmark$	H: - Removable Disk
		$\checkmark$	🖃 G: - Removable Disk
		$\checkmark$	F: - Removable Disk
		$\checkmark$	a E: - CD/DVD
			A C:\Users\admin\Windows 7 Enterprise 64Bit.ISO
	•	11	

After using this mapping, you will remove the mapping for the ISO at the end of the procedure to avoid the ISO being used as a boot device in case the Cisco UCS server is reset.

**Step 7:** Open the Citrix XenCenter management application, and then click **New VM**. The New VM wizard opens.

Step 8: Select the Windows 7 (64-bit) provisioning template, and then click Next.

Name			
Name		l ▲ L →	Template details
	Category		Clones of this template will
Citrix XenApp on Windows Server 2003 (32-bit)			automatically provision their storage when first booted and then
			reconfigure themselves with the
			optimal settings for Windows 7 (64-bit).
	Windows		
	Windows		
灯 Windows 8 (64-bit) (experimental)	Windows		
♣ Windows Server 8 (64-bit) (experimental)	Windows		
	<ul> <li>Citrix XenApp on Windows Server 2003 (64-bit)</li> <li>Citrix XenApp on Windows Server 2003 PAE (32</li> <li>Citrix XenApp on Windows Server 2008 (32-bit)</li> <li>Citrix XenApp on Windows Server 2008 (64-bit)</li> <li>Citrix XenApp on Windows Server 2008 R2 (64-bit)</li> <li>Windows 7 (32-bit)</li> <li>Windows 7 (64-bit)</li> <li>Windows 8 (32-bit) (experimental)</li> <li>Windows 8 (64-bit) (experimental)</li> </ul>	Citrix XenApp on Windows Server 2003 (64-bit) Windows     Citrix XenApp on Windows Server 2003 PAE (32 Windows     Citrix XenApp on Windows Server 2008 (32-bit) Windows     Citrix XenApp on Windows Server 2008 (64-bit) Windows     Citrix XenApp on Windows Server 2008 R2 (64-bit) Windows     Windows 7 (32-bit) Windows     Windows 7 (32-bit) Windows     Windows 8 (32-bit) Windows     Windows 8 (32-bit) Windows     Windows 8 (64-bit) Windows     Windows 8 (64-bit) Windows	Citrix XenApp on Windows Server 2003 (64-bit) Windows     Citrix XenApp on Windows Server 2003 PAE (32 Windows     Citrix XenApp on Windows Server 2008 (32-bit) Windows     Citrix XenApp on Windows Server 2008 (64-bit) Windows     Citrix XenApp on Windows Server 2008 (64-bit) Windows     Windows 7 (32-bit) Windows     Windows 7 (32-bit) Windows     Windows 8 (32-bit) (experimental) Windows     Windows 8 (64-bit) (experimental) Windows

Step 9: For the virtual machine image, enter values for Name and Description. Cisco SBA uses Win7-64bit-VM and Windows 7 64-bit base VM image. Click Next.

Step 10: Select Install from ISO library or DVD drive, from the drop-down menu, choose DVD drive 1 on viab-1, and then click Next.

Using the DVD drive allows booting from the Cisco UCS attached media, which you previously configured.

**Step 11:** Verify the default action is to **Place the VM on this server** with the default Citrix XenServer host instance highlighted, and then click **Next**.

Step 12: In vCPUs, enter 1, in Memory, enter 2048 MB (these are the minimum values), and then click Next.

**Step 13:** Select the default **Use these virtual disks**, select the default highlighted local storage, and then click **Next**.

Step 14: Highlight all network interfaces, and then click Delete.

Step 15: Click Add, and in the Network column, click VDI-Client. Leave the remaining defaults, and then click Add again to confirm and continue.

Step 16: Verify that the only Network listed in the Networking list is VDI-Client, and then click Next.

🗾 Configure netwo	orking on the new VM	0
Template Name Installation Media	The virtual machine template you have selected provides the virtual network interfaces listed below. You ca configure or delete the default virtual network interfaces here, and add more if required. Virtual network interfaces on Win7-64bit-VM	3D
Home Server	MAC Network	Add
CPU & Memory		Delete
Storage Networking		roperties
Finish	(i) Using a Default template, you can configure up to 4 virtual network interfaces during VM creation. To configure more than 4, create a Custom template or add extra virtual network interfaces from the Network tab after creating the new VM.	
CITRIX'		

Step 17: Click Finish. This confirms the virtual machine creation.

XenCenter displays work status in the bottom of the screen. After finishing, it then displays the name previously given to the VM in the navigation tree. The VM is started, and the Windows 7 installation and base configuration completes, before allowing the vdiManager to create a template from the VM.

**Step 18:** Within XenCenter, click the newly created server, and then click the **Console** tab. You can now observe the VM boot process in the console window. Complete the Windows 7 installation from this window.



The details required to complete a new Windows installation are not within the scope of this guide.

When the new installation is complete, the Windows desktop on the new guest VM is displayed.



Step 19: After the new Windows installation is complete, next to the DVD Drive 1 menu, click the underlined Eject text.

**Step 20:** Return to the KVM tab of the VM Console window, and then clear the **Mapped** check box next to the Windows ISO image.

Step 21: When the Unmap Drive Requested warning message appears, click Yes.



Undesired behavior results if the ISO image is not unmapped from the server and the server reboots. In those circumstances, the server boots from the mapped ISO image, and attempts to install Windows on the Cisco UCS hardware to replace the Citrix XenServer installation.

**Step 22:** For the highlighted Windows ISO file, click **Remove Image**. The ISO image, which is no longer needed, is disassociated from the Cisco UCS server.



**Customize Windows image** 

Once the Windows VM is running, there are some required customizations to be completed. XenServer Tools must be installed on each VM to have a fully supported configuration with enhanced disk and network performance.

A valid Administrator account with password is required for later steps in this procedure.

**Step 1:** Return to the Citrix XenCenter Window, in the navigation pane, select the XenServer host, and then click the **Search** tab. Observe that the "XenServer Tools not installed" blue status text appears next to the new Windows guest VM.

XenCenter				_ 🗆 🗙
File View Pool Server VM	Storage Templates Tools Window Help			
🕒 Back 👻 💽 Forward 👻 🛙 📑 4	dd New Server 🕴 🏪 New Pool  👘 New Storage	🛅 New VM   🔘 :	Shut Down 🛞 Reboot	V No System Alerts 👳
Show: Server View 🔎 🗸	🔁 viab-1		Lo	gged in as: Local root account
🖃 🔇 XenCenter	Search General Memory Storage Networking	NICs Console Perfe	ormance Users Logs	1
Viab=1 VdiManager_Xen_v5_1_0 Win7-64bit-VM	viab-1 Overview			
DVD drives	Search Options 💌			
Removable storage	Name	CPU Usage	Used Memory	Disks (avg / max KBs) (
	viab-1 Default install of XenServer	0% of 40 CPUs	5179 of 98163 MB	
	vdiManager_Xen_v5_1_0 Citrix vdiManager	0% of 1 CPU	391 of 1024 MB	1/4
	Win7-64bit-VM Windows 7 64-bit base VM image	0% of 1 CPU	Xe	nServer Tools not installed

**Step 2:** Click the **XenServer Tools not installed** link. The Install XenServer Tools setup wizard on the VM console opens.

**Step 3:** On the Install XenServer Tools dialog box, click **Install XenServer Tools**.



There is a pause before the next step.

**Step 4:** After the Windows CD Drive **AutoPlay** dialog appears on the VM **Console** tab, click the **Run xensetup.exe** AutoPlay option.



**Step 5:** When prompted, click **Yes** for User Account Control. This allows the program to make changes to the computer.

Step 6: Select the I accept the terms in the License Agreement check box, and then click Next.

Step 7: Click Install. This accepts the default destination folder.

**Step 8:** Ensure that the default **Reboot now** option is selected, and then click **Finish**. The installation of the required tools on the Windows machine completes. You can observe the reboot for tools installation on the VM console.

Step 9: At the prompt, click Restart Now.

**Step 10:** After the Windows VM has restarted, next to the DVD Drive 1 menu, click the underlined **Eject** text. The **xs-tools.iso** image disconnects.

Next, configure the Windows Firewall to permit inbound connections to support Citrix Receiver functionality.

**Step 11:** Log in to the VM console, click the desktop VM Windows **Start** button, and then click **Control Panel**. The Windows Control Panel opens.

Step 12: In the Control Panel, click System and Security.

Step 13: Under the Windows Firewall section, click Allow a program through Windows Firewall.

**Step 14:** Permit changes by clicking **Change settings**, select the check boxes in the **Home/Work (Private)** column next to File and Printer Sharing and Remote Desktop. The services are enabled through Windows Firewall.

**Step 15:** If access is required in a Public network configuration, then also select the check boxes in the previous step for **Public** column next to the File and Printer Sharing and Remote Desktop.

#### Step 16: Click OK.

The services are enabled through Windows Firewall.

<b>○ ○ ○ ○ ○ ○ ○ ○ ○ ○</b>	<ul> <li>System and Security          Windows Firewall         Allowed Programs     </li> </ul>	✓ 4 Search C	Control Panel	Q
2	Allow programs to communicate through Windows F To add, change, or remove allowed programs and ports, click Change What are the risks of allowing a program to communicate?	settings.	nge settings	
	Allowed programs and features:			
	Name	Home/Work (Private)	Public ^	
	Distributed Transaction Coordinator			
	File and Printer Sharing HomeGroup			
	iSCSI Service			
	Key Management Service			
	Media Center Extenders  Netlogon Service			
	Network Discovery			
	Performance Logs and Alerts			
	Remote Assistance	$\checkmark$		
	Remote Desktop     Remote Event Log Management			
		Details	Remove	
		Allow anothe	er program	]
		ОК	Cancel	]

Step 17: Under the System section of the Control Panel, click Allow Remote Access.

Step 18: In System Properties, click the Remote tab, and then, under Remote Desktop, select Allow connections from computers running any version of Remote Desktop (less secure).

System Properties	×
Computer Name Hardware Advance	ed System Protection Remote
Remote Assistance	
Allow Remote Assistance conne	ctions to this computer
What happens when I enable Rem	ote Assistance?
	Advanced
Remote Desktop	
Click an option, and then specify w	no can connect, if needed.
Don't allow connections to this of	computer
<ul> <li>Allow connections from compute Remote Desktop (less secure)</li> </ul>	rs running any version of
Allow connections only from con Desktop with Network Level Au	
Help me choose	Select Users
	OK Cancel Apply

Step 19: Click OK.

Step 20: Click the Windows Start button, right-click Computer, and then click Manage.



**Step 21:** On the Computer Management screen, under System Tools, Local Users and Groups, open the **Users** folder, right-click the **Administrator** account, and then click **Properties**.

Computer Management			
File Action View Help	? 🗊		
Computer Management (Local	Name	Full Name	Description
System Tools	🖉 Admini	strator	Built-in account for admir
	🛃 Gues	Set Password	Built-in account for guest
Shared Folders		All Tasks 🕨	
Local Users and Groups           Users		Delete	
Groups		Rename	
Note: Not		Properties	
▲ Storage		Help	
Disk Management Services and Applications			

Step 22: If it is selected, clear the Account is Disabled check box, and then click OK.

Step 23: Right-click Administrator again, and then click Set Password.

Step 24: At the warning, click Proceed, enter the password for the administrator in the New password and Confirm Password boxes, and then click OK.

**Step 25:** At the acknowledgement, click **OK**, and then close the Computer Management window. Initiate a Windows update , and apply any available Windows patches.

### Caution

Not applying the latest Windows patches may keep the VM from fully booting, and may not allow required agent software to install.

After Windows updates are completed, the next step is to disable Automatic updates started by the Windows Update service, so that the Citrix VDI-in-a-Box installation can run to completion. Click the Windows **Start** button, in the search box, type **automatic up**, and then click **Turn automatic updating on or off**. The Change settings Control Panel opens.

Control Panel (10)	
Turn automatic updating on or off	
Check for updates	
📷 View installed updates	
Windows Update	
L Auto-hide the taskbar	
L Turn toolbars on the taskbar on or off	
Show or hide inactive icons on the taskbar	
Show or hide the notification area on the taskbar	
K Change Font Settings	
Manage Windows credentials	
	1
	P
See more results	
automatic up × Shut down +	
👌 🥖 📜 🔍	

Step 26: Under Important updates, choose Never check for updates (not recommended) from the drop-down menu, and then select OK.



At this time, complete any additional customizations that you want to be replicated by all virtual desktops. Notably, a Windows machine needs to have a Microsoft Volume Activation key, since duplicate keys exist on all replicated virtual machines. All machines should be joined to a domain, and the domain configuration should be completed before proceeding.

#### Procedure 3

Import Windows machine to vdiManager

**Step 1:** Return to the web browser window showing the Citrix VDI-in-a-Box first setup procedure, click **Continue**, and then, in the new window, click **Refresh View**.

		⁰ ≣	∎'≣'	₫ 🚔
<ul> <li>There is only one DHCP server within range</li> <li>You have sufficient DHCP addresses available</li> <li>DHCP lease time is adjusted for short release cycles</li> <li>A running Windows XP or Windows 7 VM on the hypervisor to copy as a base desktop image</li> <li>Credentials for an existing domain controller</li> </ul>				
<ul> <li>A running Windows XP or Windows 7 VM on the hypervisor to copy as a base desktop image</li> <li>Credentials for an existing domain controller</li> </ul>	<ul> <li>Verify DHCP set up:</li> <li>There is only</li> <li>You have suff</li> </ul>	one DHCP server within icient DHCP addresses a	available	
		-	-	base desktop image
( <u>optional</u> , required only in you are connecting to a windows AD dontain)				

**Step 2:** If the following dialog box is displayed after clicking **Refresh View**, click the VM to get hints as to what still needs to be configured before the VM can be imported.

Impo	rt new VM		×
	Import Image	Select the virtual machine you would like to import as a base desktop image.	
	Install Agent	If the VM you would like to import shows up as "Not importable", select it to see why it cannot be imported.	
	Edit Image	Select VM Refresh View	
	Prepare Image	Win7-64bit-VM - Not importable	
	Test Image		
		There are no importable VMs.	
		Please select a virtual machine above to see why it is not importable.	

**Step 3:** On the new window, click **Refresh View**, and then select the Windows VM just created and configured, named **Win7-64bit-VM** in this example.

Step 4: Enter values for the New Image Name and Description boxes (Cisco SBA uses ViaB-Win7-64bit and Standard Windows image),and then click Import.

Import new VM		×
Install Agent	Select the virtual machine you would like to import as a base desktop image. If the VM you would like to import shows up as "Not importable", select it to see why it cannot be imported. Select VM Refresh View Win7-64bit-VM Selected VM Win7-64bit-VM New Image Name ViaB-Win7-64bit Description Standard Windows image	
	Help	

**Step 5:** In the Specify Administrator Credentials box, in the User Name box, enter **Administrator**, and then, in the Password box, enter the assigned password.



If any changes to administration control need to be made to complete this step, the console is available in Citrix XenCenter for administrative activities. **Step 6:** Click **Import**. The credentials are verified and progress screens are displayed.

Activity on image in progress			×
Name	IP address	Status	
ViaB-Win7-64bit		Copying	
Activity			
Task/Event	Progress	Status	
Shutting down imported ∨M 'Win7-64bit-∨M'	69	<sub>‰</sub> Shutting down ∀M	
Events			
Date		Status	
Sep 13, 2012 11:30:06 AM	;	Shutting down ∨M	
Sep 13, 2012 11:30:06 AM	(	Creating VM	
Sep 13, 2012 11:30:05 AM	(	Queuing VM creation	

The automated steps to import the Windows VM and install the agent take several minutes to complete. Wait for the steps to be completed before performing the Edit Image step.

Edit image 'ViaB-Win7-64bit	r	×
<ul> <li>Import Image</li> <li>Install Agent</li> <li>Edit Image</li> <li>Prepare Image</li> <li>Test Image</li> </ul>	<ul> <li>Optional: Edit the image by adding or updating pre-installed applications</li> <li>Connect to ViaB-Win7-64bit, IP address 10.4.57.48</li> <li>Connect Difficulty connecting?</li> <li>Add or update applications on the image (optional)</li> <li>View and verify the following information is accurate 5 of 5 items have not been verified You must verify all information before proceeding</li> <li>View</li> </ul>	
	Help Image Controls Nex	t

**Step 7:** If any of the automated installation does not complete, correct the problem before you complete the next two steps. For example, not applying Windows Updates may make the agent installation fail.

**Step 8:** Click the **View** button. This displays the View and Verify Information dialog box.

**Step 9:** On the View and Verify Information dialog box, verify all configuration details by selecting **Yes** next to all five items, and then click **Done**. The dialog box closes.

**Step 10:** Proceed past the Edit Image phase by clicking **Next**. The Prepare Image phase displays.

**Step 11:** In the Organizational Unit (OU) box, type the OU for Active Directory, select **Pooled and personal desktops**, and then click **Prepare**.



**Step 12:** Click **Confirm**. This acknowledges you are starting a lengthy process.

Activity status updates and eventually states VM Ready.

**Step 13:** If you need to test or change the VM image with either RDP or ICA clients, select **Connect**.

**Step 14:** Click **Save**, and then click **Confirm**. This acknowledges you are starting a lengthy operation.

Desktops	Edit image "ViaB-Win7-64bit"	×
Images Add Image ViaB-Win7-64bit Draft im	<ul> <li>✓ Import Image</li> <li>✓ Install Agent</li> <li>✓ Edit Image</li> <li>✓ Prepare Image</li> <li>Test Image</li> <li>✓ Test Image</li> <li>✓ To rectify problems or make further modifications, navigate back to the Edit Image page.</li> </ul>	
other servers This is a lenç Once the ima	*         *         *         *         in the grid. Changes made to the test desktop will not be saved.         thy operation.         age is saved and the image status shows 'Published' or 'Distributing', you can plate to provision the desktops.         Back       Save	
	Cancel Confirm VM is ready	

#### Procedure 4

#### **Create template from published image**

After the Base Desktop Image is created, it can be used to create desktop templates. The next screen starts this process.

VDI-in-a-Box			
Set up your Hypervisor and VDI-in-a-Box Grid      The Create Desi	Generate a Base Desktop Image	Teate Desktop Templates from the Base Image     from the Base In	Assign Users to Desktops
To complete this step you wi • Names and descript	l need the following: ons of desktop templati ttops you want for each user desktops	es you will create	-
(			Continue

Step 1: Click Continue. The template process begins.

**Step 2:** On the Template Information tab, enter the following values, and then make any additional updates you want to the template for the virtual machine:

- Template name—TaskWork
- Description—Template for Task Workers
- · Prefix-taskwork
- Suffix—00
- Memory (MB)-1536

Create a New Desktop Templ	ate - TaskWork		×
Template Information Template Policies	Template name: Image name: Description:	TaskWork ViaB-Win7-64bit Template for Task Workers	
	Computer name: Memory (MB): Virtual CPUs:	Prefix: taskwork Suffix: 00 1-11 characters 0-4 digits 1536 1 1 1	]
	☑ Disk drives ☑ □ Smart cards ☑ Color depth: True c	Other USB devices	
	Help	Next	

#### Tech Tip

Using less than 1536 MB of memory for Windows 7 virtual machines may keep them from becoming fully operational. The minimum memory required for allocation to the machine may increase beyond 1536 MB, dependent on application requirements.

#### Step 3: Click Next. Template Policies displays.

The policy created for task workers has five desktops available, with two pre-started for performance reasons. The virtual desktops are a pooled resource, which do not have any personal disk space reserved.

Next, fill in the template policy.

Step 4: For Maximum desktops, enter 5, for Pre-started desktops, enter 2, and then keep the default selection for Pooled desktop.

Step 5: Select Make this the default template, click Save, and then click Close.

Create a New Desktop Tem	plate - TaskWork	×
✓ Template Information Template Policies	Maximum desktops: 5 Pre-started desktops: 2 Template will provision: © Pooled desktop © Personal desktop Refresh desktop: On logout © Do not reassign desktops "On Hold" to new users	_
	<ul> <li>Enable fast refresh of desktops</li> <li>Make this the default template</li> <li>Help</li> <li>Back</li> <li>Save</li> </ul>	-

Two VMs are created and started, which you can observe in the XenCenter window.

#### Process

Assigning Users to Work Templates and Testing Citrix Receiver

- 1. Assign templates for use cases
- 2. Migrate vdiManager to static IP
- 3. Create and install SSL cert for vdiManager
- 4. Test connectivity to virtual desktops



Assign templates for use cases

This procedure relies on information existing in Active Directory for user and group assignments. The existing viab-user group is used as the basis to assign the default TaskWork template to users.

**Step 1:** Click **Continue**. This begins the Assign Users to Desktops stage of the VDI-in-a-Box installation.

VDI-in	-a-Box			
	t up your Hypervisor	Oenerate a Base	TETE     Create Desktop Templates	4 Assign Users
	d VDI-in-a-Box Grid	Desktop Image	from the Base Image	to Desktops
•	· ·	s you want to assign to end points you want to	desktop templates you crea assign to desktop templates	
				Continue

The final pop-up window in the browser disappears and reveals the vdiAdmin screen behind it. **Step 2:** Under the Users tab of the VDI-in-a-Box administration, next to User Groups, click **Add**, type the name of the Active Directory group you want to associate to allow access. Use **viab-users** for this example, and then press **Enter.** 

This example uses beginning letters of **viab** as a search to find the **viab**-users group.

VDI-in-a-Bo	))X <sup>**</sup>					Welcome vdiadmin	About Logout	CİTRIX
Desktops	Images	Templates	Servers	Users	Admin			
View All	]					User Database: Configure	Synchronize	Hel;
User Group	S Add							
Group Name		Des	cription			mplates		
viab	]				De	<i>fault</i> (TaskWork)	Sa	ive   Cancel
Users Add								
User ID	First Name		Last Name		Group	# Templates		
IP Addresse	S Add							
IP Address Rang	jes		Temp	ate Name		Description		
Tip: IP address m	appings can be add	iresses (192.168.1	.23), prefixes (192	.168), or ranges (1:	92.168.1.128-143).	Specify multiple mappings with	spaces or new lines.	

Users in the viab-users Active Directory group are assigned the default template upon login. Templates can also be configured for specific users or IP addresses.

#### Procedure 2

Migrate vdiManager to static IP

VDI-in-a-Box users need to have a consistent host name and IP address to use when connecting to the VDI-in-a-Box broker service, which assigns the virtual desktop. In this procedure, you migrate the IP address from the one assigned by DHCP to one that you statically assign. To make these changes, you must use maintenance mode for the grid containing the single server. Making these changes will disrupt active VDI-in-a-Box service. The warnings in the following steps that are related to these changes are safely ignored. **Step 1:** Returning to the web browser display for vdiManager, click the **Servers** tab, click the active XenServer IP address under the **Name** column, and then, in the Server Properties box, click **Deactivate**.

VDI-in-a-Box <sup>™</sup>					ıt Logout <b>CİTRİX</b>
Desktops	Images Templa	ates <b>Servers</b> Users	Admin		
O	Server Properties	- 10.4.63.85			8
Servers in grid					Help
	Host name:	viab-1	Memory (GB):	95.86	
10.4.63.85	Name: Server hardware:	10.4.63.85	CPU (Cores): Total CPU (GHz):	40 79.8	Desktops   Images
	Hypervisor version:	XenServer, 6.0.2, 53456p	VM network:	VDI-Client	
	Datastore:	Local storage (2148 GB free of 21	88 GB total)		
	VDI manager:	10.4.57.39	Status:	ACTIVATED	
	MAC address:	E2:93:F4:63:26:2B	VDI-in-a-Box build:	5.1.0 v5g1r0 v5g1r0_20120720123824	
					Help
	VDI manager service				
	Activate	Jeactivate Quiesce Leav			
	Hypervisor settings				
	Configure				

**Step 2:** Confirm the server deactivation and disconnect of sessions and shut down of VMs by clicking **Confirm**, and then wait for the server status display to show Deactivated.

Step 3: In vdiManager, click Admin tab, click Grid Maintenance, and then, in the Take grid into maintenance mode dialog box, click Ok.

VDI-in-a-Box <sup>≈</sup>									CİTRIX
Desktops Images	Templates	Servers	Users	Admin					
Grid									Help
"  "  " Advanced Properties	Grid Time		🔀 Grid Mainte	enance	Grid and	License Upgrade	4	Manage Adr	inistrators
Server									
Server	Downloa	Take grid int	o maintenance	mode	x				
Server	Downloa		<b>o maintenance</b> to move the grid		Help	rver			

**Step 4:** Click the **Servers** tab, click the XenServer IP address, and then, in the Server Properties box, click **Modify**. A VDI-in-a-Box Manager Network Settings window appears.

Step 5: Select Static IP configuration, use the pull-down selectors to change the DHCP address to the correct static IP address outside the DHCP scope, which is 10.4.57.9 for the Cisco SBA user VLAN, and then click Ok.

VDI-in-a-Box Manager Network Settings	×
	Help
Configuring the VDI-in-a-Box Manager network is a hazardous and potentially disruptive operation that can result in the VDI-in-a-Box Manager being disconnected from the network. If you are in doubt about your network configuration, consult network administrator.	your
Please select the option that matches your network requirements.	
C Dynamic configuration (DHCP)	
The dynamic (DHCP) configuration is recommended if you can reserve the VDI-in-a-Box Manager address in the DHC server. This reservation allows the VDI-in-a-Box Manager to get the same IP address every time it starts up without conflicting with any other machine on the network.	Þ
Note the following MAC address for VDI-in-a-Box Manager and reserve it in DHCP: E293F463262B	
• Static IP configuration	
The static configuration is recommended if you have been assigned a static IP address to use for VDI-in-a-Box Manag The static IP address entered here is constrained by the current netmask of the VDI-in-a-Box Manager. Do not enter an address that clashes with another machine or with future DHCP pool addresses.	ler.
address: 10 💌 4 💌 57 💌 9 💌	
netmask: 255.255.2	
broadcast: 10.4.57.255	
gateway: 10.4.57.1	
macaddress: E2:93:F4:63:26:2B	
C Manual network configuration	
Select this option if you have manually configured networking on the VDI-in-a-Box Manager system, usually because complex networking requirements <b>This option will not change the existing network configuration.</b>	of
Cancel Ok	

A progress screen is displayed while the vdiManager virtual appliance restart operation takes place, resulting in the restarted vdiManager server now available using the newly assigned static IP address. The open web browser session to vdiManager now automatically redirects to the new vdiManager IP address to allow the administrator to reconnect.

**Step 6:** Accept any browser security and certificate warnings required during the connection to the new IP address.

Step 7: On the new vdiManager display in the web browser, click the Admin tab, click Grid Maintenance, click the Take grid into maintenance mode dialog box, and then click Ok.

VDI-in-a-Box <sup>™</sup>									<b>citrix</b> .
Desktops Images	Templates	Servers	Users	Admin					
Grid									Help
"≣ "≣ Advanced Properties	Grid Time		K Grid Mainte	enance	Grid and	License Upgrade	<b>±</b>	Manage Adn	ninistrators
Server									
Ex View Audit Log	Downloa	Take grid into	o maintenance	mode	×	rver			
		Do you want t	o move the grid	to maintenance	Help mode?				
				Cancel	Ok				

**Step 8:** Click the XenServer IP address again, in the Server Properties dialog box, click **Modify**. The VDI-in-a-Box Manager Settings window displays.

**Step 9:** For the VDI-in-a-Box manager service settings, click **Activate**, and then click **Confirm**.

Server Properties	- 10.4.63.85			×
				Hel
Host name:	viab-1	Memory (GB):	95.86	
Name:	10.4.63.85	CPU (Cores):	40	
Server hardware:		Total CPU (GHz):	79.8	
Hypervisor version:	XenServer, 6.0.2, 53456p	VM network:	VDI-Client	
Datastore:	Local storage (2154 GB free of 21	88 GB total)		
VDI manager:	10.4.57.9	Status:	DEACTIVATED	
MAC address:	E2:93:F4:63:26:2B	VDI-in-a-Box build:	5.1.0 v5g1r0 v5g1r0_2012072012	3824
				Hel
VDI manager service				
Activate D				
Hypervisor settings				
Confige Confirm			6	0
VDI Man				
Modif Activate	e the desktop server - 10.4.63.85?			
				Hel
Advance		Can	cel Confirm	
Self 7	nootan onataonn			

The dialog box closes, and the server status transitions to Activated. The number of desktop VM templates that are configured to pre-start is also made available for use.

#### Procedure 3

Create and install SSL cert for vdiManager

To access their virtual desktop, remote devices run the Citrix Receiver client over Secure Sockets Layer (SSL) transport for secure connectivity to the vdiManager virtual appliance. To do so requires a certificate to be installed on the vdiManager, which the client validates with the appropriate Trusted Certificate Authority to make the connection. Without a valid and trusted certificate, the client may display an error message, such as, "Certificate provided by the server is not trusted. Account information cannot be added."

To address this situation, administrators should plan to request a certificate from their preferred certificate authority (CA).



#### **Tech Tip**

For more information about the certificate process in relationship to vdiManager, see:

http://support.citrix.com/article/CTX132235

In the Cisco SBA topology, the certificate request and installation for this procedure uses the local Microsoft Active Directory server as the root CA, for a non-vendor-specific certificate signing example. A Java utility named "keytool" is accessed at the Citrix VDI-in-a-Box Linux command line to manage the certificate request and installation process.

**Step 1:** Using an SSH terminal client, open a connection to the VDI-in-a-Box appliance by its DNS name or IP address, and then log in by using the default credentials of **kvm** with a password of **kaviza123**.

**Step 2:** Create a directory for key storage, and then change the local directory to the created directory location.

mkdir /home/kvm/keystore

cd /home/kvm/keystore

Step 3: Generate a server key.

keytool -genkey -alias vdimgr.cisco.local -keyalg RSA -keysize 2048 -keystore kmgr.keystore

where the -alias vdimgr.cisco.local parameter is the vdiManager DNS name.

The command triggers a prompt for a 6-character minimum length password to be entered, and then prompt for confirmation. After confirmation, there are a number of prompts for information related to the certificate, with the first question being the most critical. The prompt, "What is your first and last name?" is a request for the certificate Common Name (CN) field information, and needs to be interpreted as asking for the fully qualified domain name (FQDN) of the server. Step 4: Answer the series of prompts.

What is your first and last name?

[Unknown]: vdimgr.cisco.local

What is the name of your organizational unit?

[Unknown]: SBA

What is the name of your organization?

[Unknown]: Cisco

What is the name of your City or Locality?

[Unknown]: San Jose

What is the name of your State or Province?

[Unknown]: CA

What is the two-letter country code for this unit?

[Unknown]: US

Is CN=vdimgr.cisco.local, OU=SBA, O=Cisco, L=San Jose, ST=CA, C=US correct?

[no]: **yes** 

Enter key password for <vdimgr.cisco.local>

(RETURN if same as keystore password):

Step 5: Press Enter. The command completes and Linux prompt displays.

Step 6: Generate a Certificate Signing Request (CSR).

keytool -certreq -alias vdimgr.cisco.local -file kmgr.csr -keystore kmgr.keystore

The command asks to enter the keystore password. Enter the password previously used.

**Step 7:** List the directory contents by typing the Linux **Is** command and pressing **Enter**, and then verify that both the kmgr.csr and kmgr.keystore files exist.

**Step 8:** Connect to the **vdimgr.cisco.local** machine by using a Stream Control Transmission Protocol (SCTP) utility, enter credentials by using the **kvm** username and **kaviza123** password, retrieve the /home/kvm/keystore/ kmgr.csr file, and then store the file on the local management machine.

The information contained in the **kmgr.csr** file is used with the CA to request a certificate signing.

**Step 9:** Using the contents of the **kmgr.csr** file, connect to the CA and request a certificate signing. For the Microsoft Active Directory CA, use the following URL:

#### http://cacisco.local/certsrv/

**Step 10:** Click the **Request a certificate**, click **Submit an advanced certificate request** link, and then fill out the displayed web form by opening the kmgr.csr file with Notepad and pasting the contents into the Saved Request box.

Step 11: In the Certificate Template list, choose Web Server, and then click Submit.

Microsoft Active Directory Certificate Services cisco-AD-CA								
Submit a Certi	ficate Request or Re	enewal Request						
		paste a base-64-encoded C n as a Web server) in the Sa	MC or PKCS #10 certificate request or PKCS #7 renewal request ved Request box.					
Saved Request:								
certificate request	bF7RYDDTJuzImP48mc. tBhVHDEaxg1IXY21Nz IOpJ0Y7ShfaetJ2OpC END NEW CERTI:	15YJWI204Xw62vQPYjkW3C Sddpz6REbaeF2pko1U6125 Mariexz7D2cCDV6fKJ2DC hprJlmxQSFPk4kdwZcobkK FICATE REQUEST						
Ceruncate remp	Web Server	•						
Additional Attrib	utes:							
Attributes:		.::						
		Submit >						

Step 12: Click the **Download certificate** in order to download and save a **certnew.cer** file, containing the certificate information for the server.

Step 13: Click Home, click Download a CA certificate, certificate chain, or CRL, and then click Download CA certificate.

Step 14: Rename the file to certroot.cer, and then save it.

**Step 15:** Use the SCTP utility to copy the certnew.cer and certroot.cer files to the /home/kvm/keystore/ directory on the vdimgr.cisco.local machine. For credentials, enter the **kvm** username and **kaviza123** password.

**Step 16:** Return to the SSH command line, and input the following two Linux commands:

keytool -import -trustcacerts -alias root -file certroot.cer keystore kmgr.keystore

keytool -import -trustcacerts -alias vdimgr.cisco.local -file certnew.cer -keystore kmgr.keystore

**Step 17:** After each command, enter the password again, and then, in response to the query, "Trust this certificate?", enter **yes**. You receive the following replies:

- Certificate was added to keystore
- Certificate reply was installed in keystore

**Step 18:** Replace the existing self-signed certificate with the new certificate.

- cd /home/kvm/kvm/install/servlet container/conf
- mv .keystore old.keystore
- cp /home/kvm/keystore/kmgr.keystore .keystore

**Step 19:** The web server configuration must now be updated to use the password for the keystore.

Step 20: Edit the server.xml file with the vi editor.

sudo vi server.xml

**Step 21:** In the vi editing session, find the clientAuth line by using the following vi search.

/clientAuth=

Then, go to the end of the line found, by typing the following keys for a vi search.

/>

Cursor back a character over the slash character, and then enter insert mode by typing the keys.

hi

In vi insert mode, type space and the text **keystorePass="password"**, where the password between the quotes is the one previously used for keystore.

The full line in the file should look like the following.

clientAuth="false" sslProtocol="TLS" URIEncoding="UTF-8"
keystorePass="password"/>

Step 22: Save and exit vi by typing two uppercase Z letters.

**Step 23:** Restart the web server Tomcat services need by typing the following. This enables the new settings to take effect.

tc\_start

77

The web server with correct certificates is now ready to be used.

#### **Procedure 4**

#### • Test connectivity to virtual desktops

Download the appropriate Citrix Receiver for the remote client, and then install the Citrix Receiver application.

Android clients are available from Google Play, and iOS clients for the iPad are available at the Apple App Store. Windows clients are available from the Citrix website, here:

#### http://www.citrix.com

This guide uses the Windows version for testing in this procedure.

**Step 1:** Launch the Windows Citrix Receiver, click the **Settings** gear icon at the top, click **Accounts**, click **Add account**, and then click **Add**. The Add Account dialog box is displayed.

**Step 2:** In the **Enter your work email or server address** box, enter the following vdiManager virtual appliance URL:

https://vdimgr.cisco.local/dt/PNAgent/config.xml

#### Step 3: Click Next.



Step 4: When the account with check box is displayed, click OK.

The Please log on to vdimgr dialog box displays.

Step 5: For Domain\User, enter a user available in Active Directory, such as cisco\viab-user-1, enter the Password for that user, and then click Log On.

**Step 6:** In Citrix Receiver, click the **Add Apps** icon, and then click **All Applications**. The configured TaskWork group appears.

**Step 7:** Click the **TaskWork** icon. The Citrix Receiver client connects to the desktop virtual machine, generated as part of the template by that name, and the virtual desktop Windows screen displays.

#### Figure 3 - Example of Citrix Receiver Windows desktop screen



Figure 4 - Example of Citrix Receiver Android smart phone display



Figure 5 - Example of Citrix Receiver for iPad IOS display



**Step 8:** If you want to confirm that the VDI-in-a-Box service is operational and that the desktops are active, use the vdiManager application Servers and Desktops tabs.

VDI-in-a-E	3ox <sup>™</sup>					We	elcome vd	iadmin	About	Logout	CİTRIX <sup>.</sup>
Desktops	Images	Templates	Servers	Users	Admin						
Servers in	grid										Help
		Deskto ''In Us									
10.4.63.85			3	0	1 1 A0	CTIVATE	Ð	1	8%	Deskto	ips   Images
	Server Status - * Capacity				8%		In L On	Hold		Relp tjust Help	
		Te	mplate		In U	se C	On Hold	New	Starting	Broken	
		TaskWo	ork (default)			3	0	1	1	0	
						3	0	1	1	0	
									C	lose	
/DI-in-a-B	ox⁼					We	elcome vd	liadmin	About	Logout	<b>citrix</b> .
Desktops	Images	Templates	Servers	Users	Admin						

Desktop	s Images	Templates	Servers	Users	Admin				
Summar	y User Session	ns							
Üser Ses	Jser Sessions Help								
								Γ	Show all sessions
Search O	ptions								
Showing 1 - 3	3 of 3						<<	First   < Prev	Next >   Last >>
User ID	Template	Server	VM Name	A	ddress	Client	Login	Duration 🛦	Status
viab-user-3	TaskVVork	10.4.63.85	taskwork09	10	.4.57.30	10.4.16.31	Oct 3, 2012 3:29 PM	0:02	Actions
viab-user-2	TaskVVork	10.4.63.85	taskwork10	10	.4.57.27	localhost	Oct 3, 2012 3:06 PM	0:25	Actions
viab-user-1	TaskWork	10.4.63.85	taskwork08	10	.4.57.25	10.4.63.200	Oct 3, 2012 2:54 PM	0:37	Actions
Showing 1 - 3	3 of 3						~~	First   < Prev	Next >   Last >>

## Appendix A: Product List

## **Computing Resources**

Functional Area	Product Description	Part Numbers	Software
UCS C-Series Rack-mount	Cisco UCS EZ C260 Pack w/E7-2870 24x8GB DIMMs 1 VNIC	UCS-EZ-C260-E7192	1.4(3c)
Servers	300GB 6Gb SAS 10K RPM SFF HDD/hot plug/drive sled mounted(Quantity-8)	A03-D300GA2=	Cisco UCS Release
Hypervisor	Citrix XenServer	XenServer	6.0.2
VDI	Citrix VDI-in-a-Box	VDI-in-a-Box	5.1

### Feedback

Click here to provide feedback to Cisco SBA.



SMART BUSINESS ARCHITECTURE

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, WITH-OUT 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 DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY OF USE THE DESIGNS, EVEN 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 OF 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 ON ON 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.

© 2012 Cisco Systems, Inc. All rights reserved.



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.

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)