



Videoscape Distribution Suite Service Manager Software Installation Guide

First Published: August 06, 2012

Last Modified: December 18, 2013

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-30487-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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: <http://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)

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.

Adobe Systems, Inc.

Adobe LiveCycle Data Services ES2.5, Copyright © 2010, Adobe Systems, Inc. All Rights Reserved

Oracle

Copyright ©2012, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Red Hat, Inc.

Red Hat and Red Hat Enterprise Linux are trademarks of Red Hat, Inc., registered in the United States and other countries.

Other product names, symbols, and phrases used throughout this document (if any) are property of their respective owners.

VDS Software Installation Guide

© 2013 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface

Preface v

- Audience v
- Document Organization v
- Document Conventions vi
- Reporting Problems vii

CHAPTER 1

VDS-SM Software Installation Overview 1

- Software Installation Requirements 1
- VDS-SM Software 1

CHAPTER 2

VDS-SM Virtual Machine Deployment 3

- Deploying the VDS-SM Core Services Software onto a VM 3
- Deploying the User Interface Node Software onto a VM 12
- Deploying the CDN Manager Node Software onto a VM 17
- Deploying the Analytics Node Software onto VMs 22
- Verifying and Backing Up the VDS-SM OVF VMs 26
 - Verifying the VDS-SM VMs are Available 26
 - Snapshotting the VDS-SM VMs 27
- Configuring CSV Files 28
 - Lookups 29

CHAPTER 3

VDS-SM Installation and Configuration 31

- VDS-SM Installation and Configuration Overview 31
 - Installing VDS-SM Core Services 32
 - Configuring the Core Service Application Server 37
 - Installing the VDS-SM User Interface Node 39
 - Configuring the User Interface Node Application Server 40

Installing the VDS-SM CDN Manager Node	41	
Configuring the CDN Manager Node Application Server	42	
Installing the VDS-SM Analytics Search Head	43	
Configuring the Analytics Search Head Application Server	44	
Installing the VDS-SM Analytics Indexer	46	
Configuring the Analytics Indexer Application Server	47	
Installing the VDS-SM Analytics Forwarder	48	
Configuring the Analytics Forwarder Application Server	49	
Installing the VDS-SM Analytics Job Scheduler	51	
Configuring the Analytics Job Scheduler Application Server	52	
Adding an Analytics Indexer to VDS-SM	53	
Deploying CDS System Delivery Server/Services in Analytics Node	53	
Data Retention Policy	54	
Upgrade Procedure from 3.0 to 3.1	54	
Backup Existing Installations	54	
Upgrading VDS-SM Nodes	55	
Indexer	56	
Search Head	57	
Forwarder	57	
Job Scheduler	58	
Management Services	58	
CDN Manager	59	
UI Node	59	
Procedure to Resize Hard Disk	60	
Installing Software	62	
Configuring VDS-IS Transaction Log Settings	62	
Procedure to Restart the Nodes	63	
Shutting Down the VMs	64	
Browsers Supported	64	
CHAPTER 4	VDS-SM Port Utilization Details	67
	VDS-SM Port Utilization	67



Preface

- [Audience, page v](#)
- [Document Organization, page v](#)
- [Document Conventions, page vi](#)
- [Reporting Problems, page vii](#)

Audience

This guide provides instructions for Operators and Administrators responsible for installing the VDS-SM software.

Document Organization

This document is organized into the following chapters:

Chapter	Description
Introduction to Videoscape Distribution Suite Service Manager Software Installation Overview	Describes the Videoscape Distribution Suite Service Manager (VDS-SM) software installation process and prerequisites.
Videoscape Distribution Suite Service Manager Virtual Machine Deployment	Describes how to install, verify, backup, and deploy software onto Virtual Machines (VMs).
Videoscape Distribution Suite Service Manager Installation and Configuration	Describes how to install and configure the different VDS-SM services, Splunk on a VDS-IS, and how to configure SE/SR logging.

Document Conventions

This document uses the following conventions:

Table 1: Document Conventions

Convention	Description
^ or Ctrl	Both symbols represent the Control (Ctrl) key on the keyboard. For example, the key combinations ^D or Ctrl-D means that you hold down the Control key while you press D . (Keys are indicated in capital letters but are not case sensitive.)
bold font	Commands, keywords, and user-entered text appear in bold font .
<i>Italic font</i>	Document titles, new or emphasized terms, and arguments for which you need to enter values appear in <i>italic font</i> .
Courier font	Terminal sessions and information, which the system displays appear in <code>Courier font</code> .
Bold Courier font	Bold Courier font indicates the text that you must enter.
[x]	Elements in square brackets are optional.
...	An ellipsis (three consecutive non-bolded periods without spaces) after a syntax element indicates that the element can be repeated.
	A vertical line, called a pipe, indicates a choice within a set of keywords or arguments.
[x y]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
{x y}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x {y z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.
string	A non-quoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
<>	Nonprinting characters such as passwords appear in angle brackets.
[]	Default responses to system prompts appear in square brackets.

Convention	Description
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Reader Alert Conventions

This document uses the following conventions for reader alerts:



Note

Means *reader take note*. Notes contain helpful suggestions or references to material, which is not covered in the manual.



Tip

Means *the following information will help you solve a problem*.



Caution

Means *reader needs to be careful*. In this situation, you might do something that could result in equipment damage or loss of data.



Timesaver

Means *the described action saves time*. You can save time by performing the action described in the paragraph.



Warning

Means *reader beware*. In this situation, you might perform an action that could result in bodily injury.

Reporting Problems

If you have any query or experience problems when installing the VDS Service Manager software, contact your Cisco Technical representative.



VDS-SM Software Installation Overview

- [Software Installation Requirements, page 1](#)

Software Installation Requirements



Note

This software installation procedure is for Videoscape Distribution Suite Service Manager (VDS-SM) version 3.1. It is strongly recommended that this software installation be performed by a Cisco Systems representative.

Before installing the VDS-SM software, the following requirements must be completed:

- Download the VDS-SM software
- Install the VMware ESXi software

VDS-SM Software

The VDS-SM software is downloadable as Open Virtualization Format (OVF) files for deployment on a VMWARE ESXi host. The Red Hat Linux Operating System and all required software components are included in each OVF.

The following is a list of components and the order they should be installed within VDS-SM.

- Core Services
- User Interface
- CDN Manager
- Analytics
 - Search Head
 - Indexer
 - Forwarder
 - Job Scheduler

**Note**

The Core Services node must be installed first, as each node registers with the Core Services node at installation time.

Also, before beginning the software configuration process, gather all networking information (IP addresses, node names, and network parameters).

Downloading From Cisco.com

To download the software from Cisco.com:

- 1 Go to
<http://software.cisco.com/download/special/release.html?config=8ba4c124b180fbfb1bbcb3e26518ddd8>
- 2 Click **Download Now** and download the required images.
- 3 Click **Accept** to accept the license agreement and download the software. The File Download dialog box appears. If you do not want to accept the license agreement, click **Decline**. The License Agreement page appears when you download each file from Cisco.com.
- 4 Click **Save** to save the VDS-SM 3.1 software executable file on your system.

After downloading all the files from Cisco.com, ensure that the downloaded files have the following checksum values:

3.1.0 Images**Core-Svcs**

core-svcs-3.1.0-x86_64-ovf.tar.gz : d4c82238a29352b5e12d4f43b37cb6fd

UI

ui-3.1.0-x86_64-ovf.tar.gz : 7f3f42842b301dee24b1ea79e117e5d7

Cdn-mgr

cdn-mgr-3.1.0-x86_64-ovf.tar.gz : 2cd34a613b2eeb0aff3d65b7d17b5186

Analytics

analytics-3.1.0-x86_64-ovf.tar.gz : 62e63869edc375b1b0aab24bd01699db

Inline Upgrade Images**Core-Svcs**

cdn-mgr-3.1.0-upgrade.tar.gz : b6dc7086cbdbb6f35f83ee874638d2e3

UI

ui-3.1.0-upgrade.tar.gz : 0c6623b56afedbc8b0b83dc818ec2092

Cdn-mgr

cdn-mgr-3.1.0-upgrade.tar.gz : 273e294248903e5afa44c081d9293743

Analytics

bni-analytics-3.1.0-analytics-upgrade.tar.gz : 9ab07829afb7166194c513e9b42e0179

- 5 Extract the downloaded images to any accessible location. The extracted images should have two files with the extension .ovf and .vmdk.



VDS-SM Virtual Machine Deployment

- [Deploying the VDS-SM Core Services Software onto a VM, page 3](#)
- [Deploying the User Interface Node Software onto a VM, page 12](#)
- [Deploying the CDN Manager Node Software onto a VM, page 17](#)
- [Deploying the Analytics Node Software onto VMs, page 22](#)
- [Verifying and Backing Up the VDS-SM OVF VMs, page 26](#)
- [Configuring CSV Files, page 28](#)

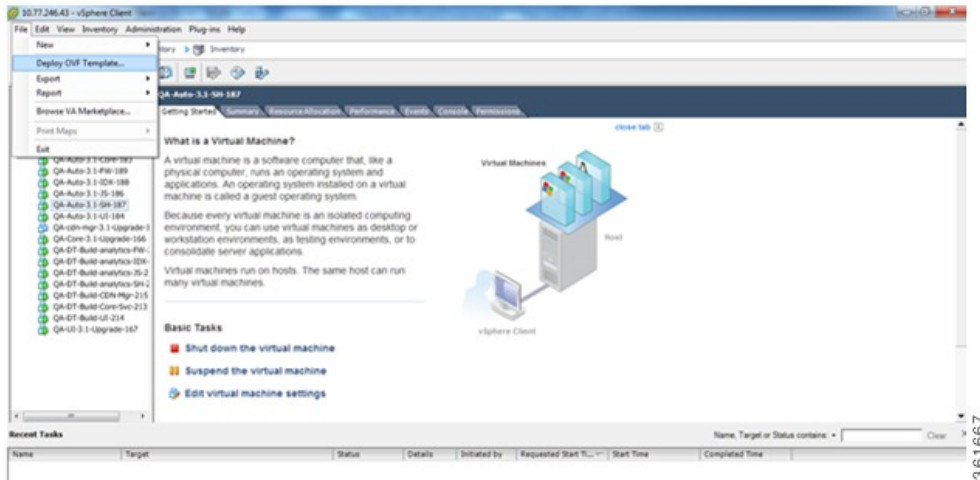
Deploying the VDS-SM Core Services Software onto a VM

The Core Services software must be deployed first, as each node registers with the Core Services node at installation time.

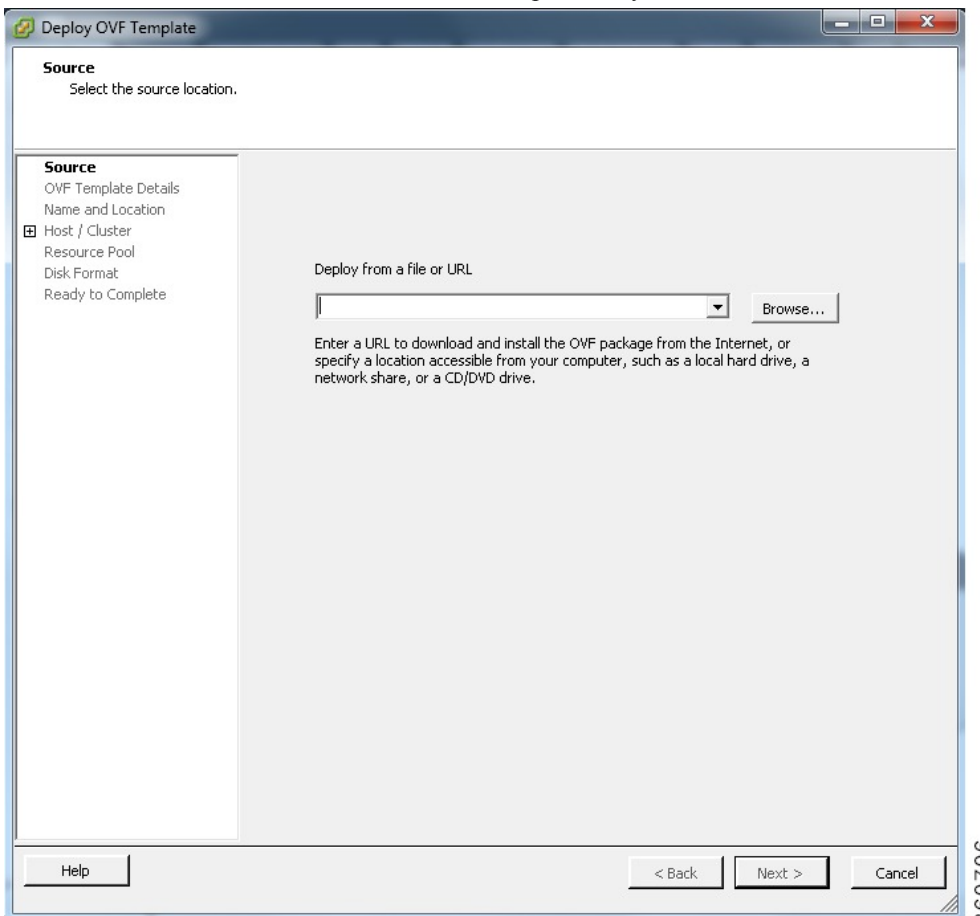
To deploy the Core Services software, perform the following steps:

-
- Step 1** Using the VMware's vSphere client, access the ESXi host or VCENTER server and import the OVF images from the extracted location.
- Step 2** Click **File > Deploy OVF Template**.

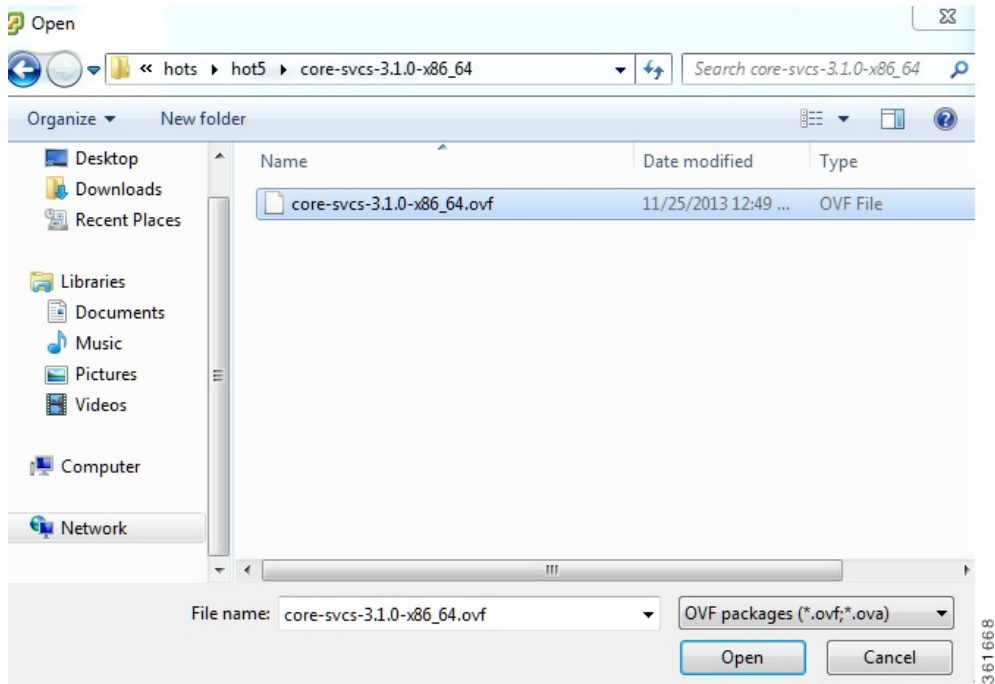
Deploying the VDS-SM Core Services Software onto a VM



Step 3 Click **Browse...** to locate the OVF files extracted previously.

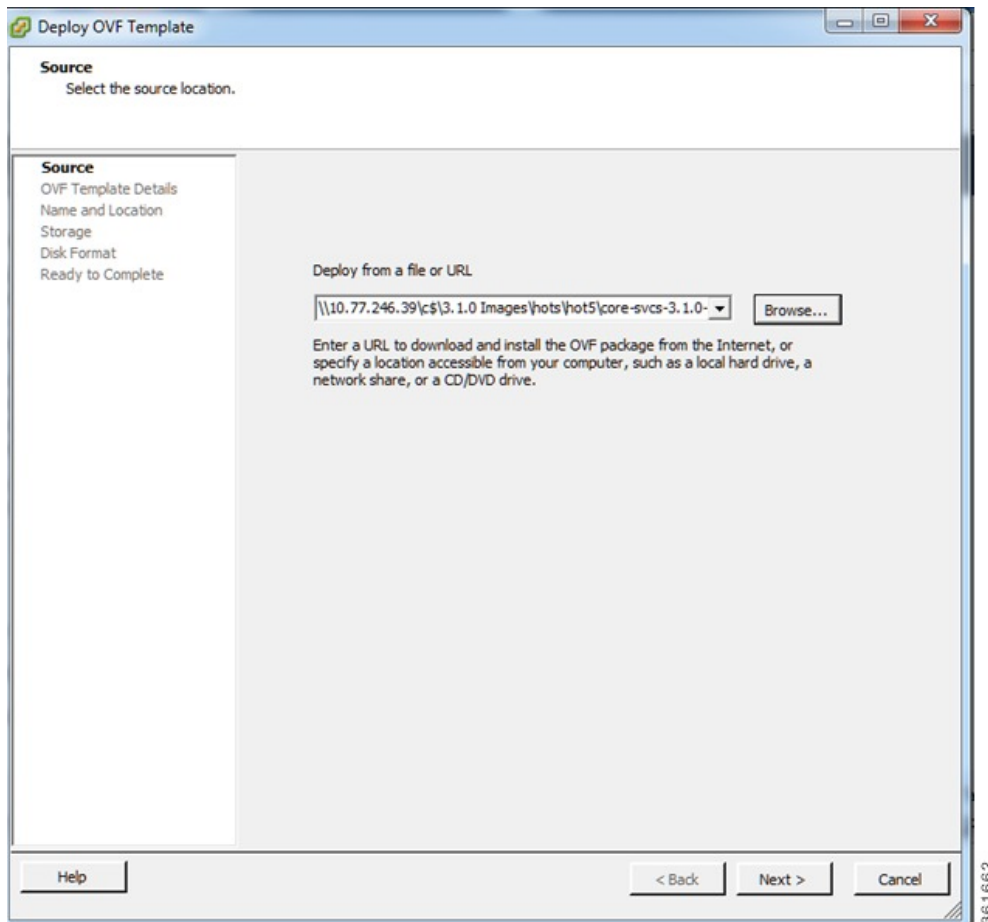


Step 4 Select the folder that contains the core services OVF file, and then click **Open**.

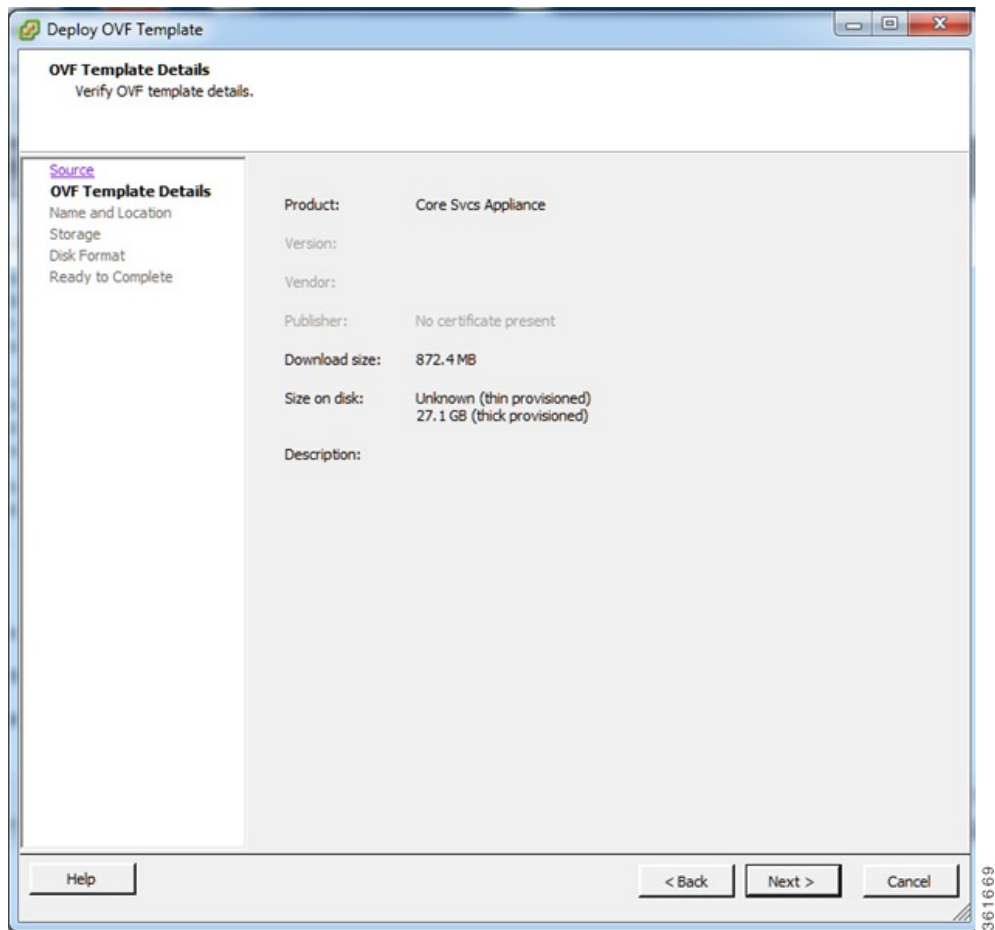


Step 5 Select the OVF file and click **Open**.

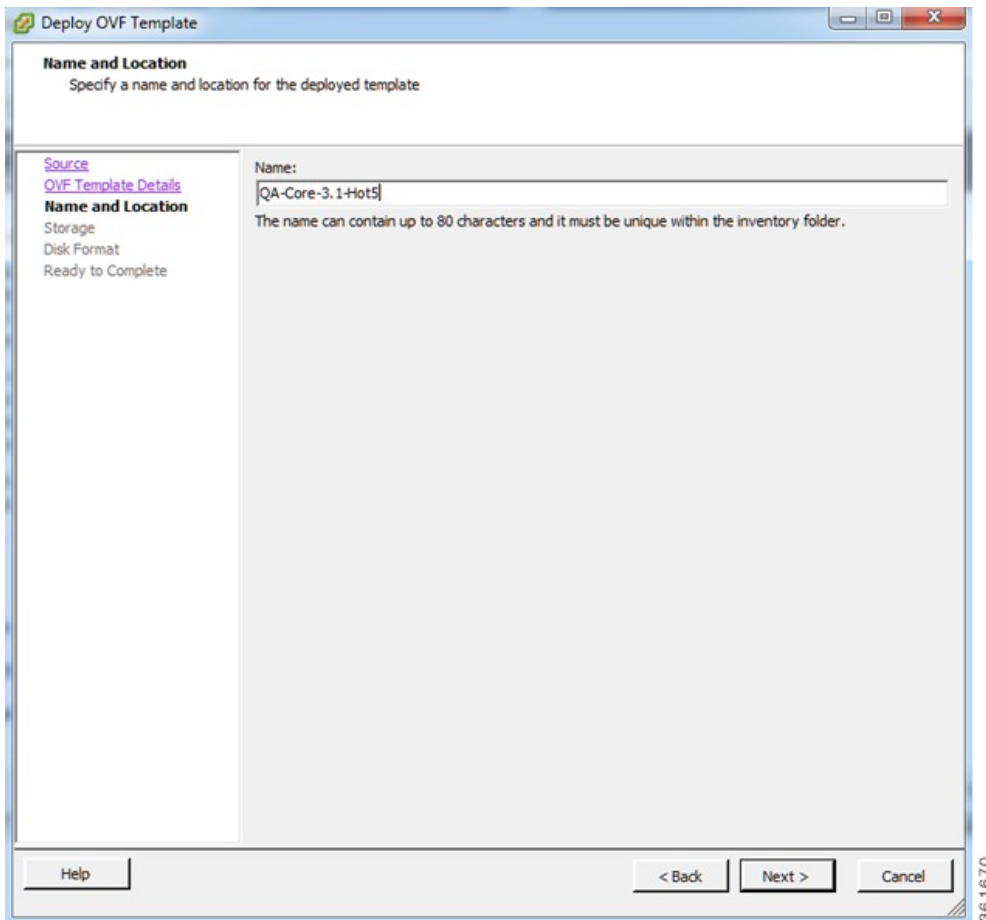
Step 6 When the OVF file is selected, click **Next >** to continue.



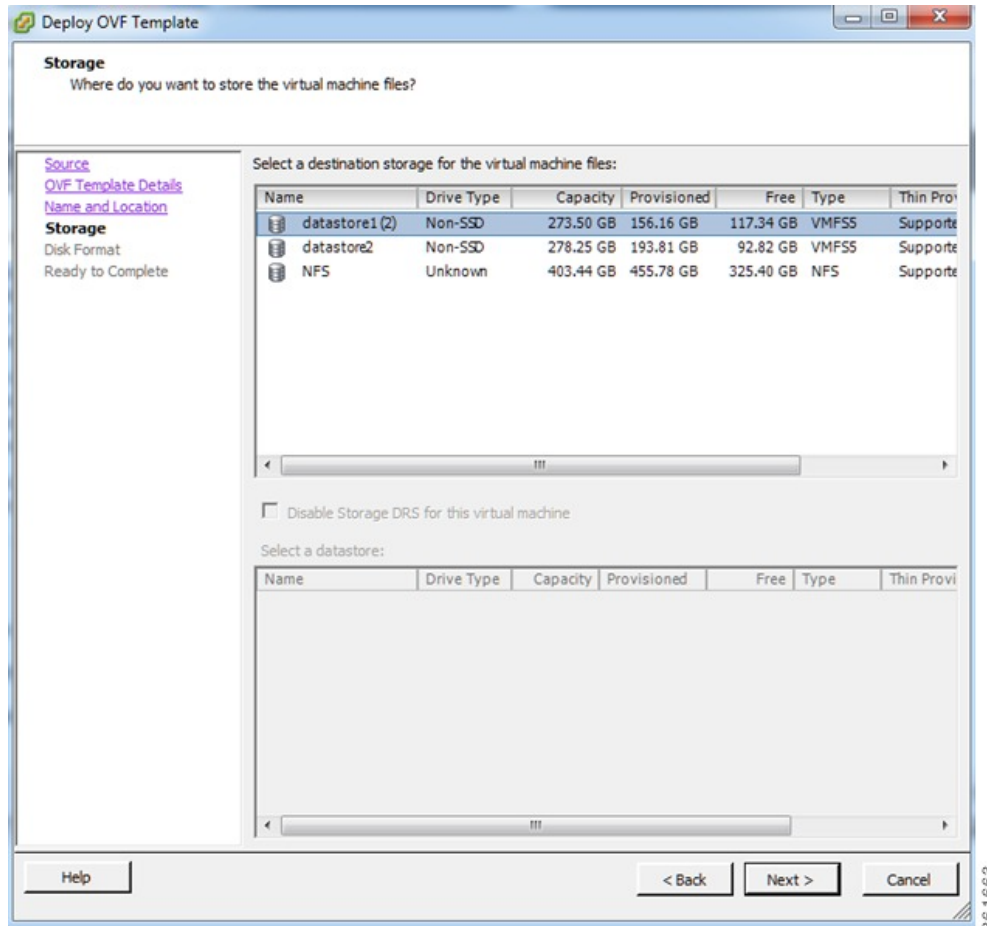
Step 7 Verify the product being deployed and then click **Next >**.



Step 8 Enter a name for the VM being deployed and select the ESX where the VM has to be deployed. When finished, click **Next >**.

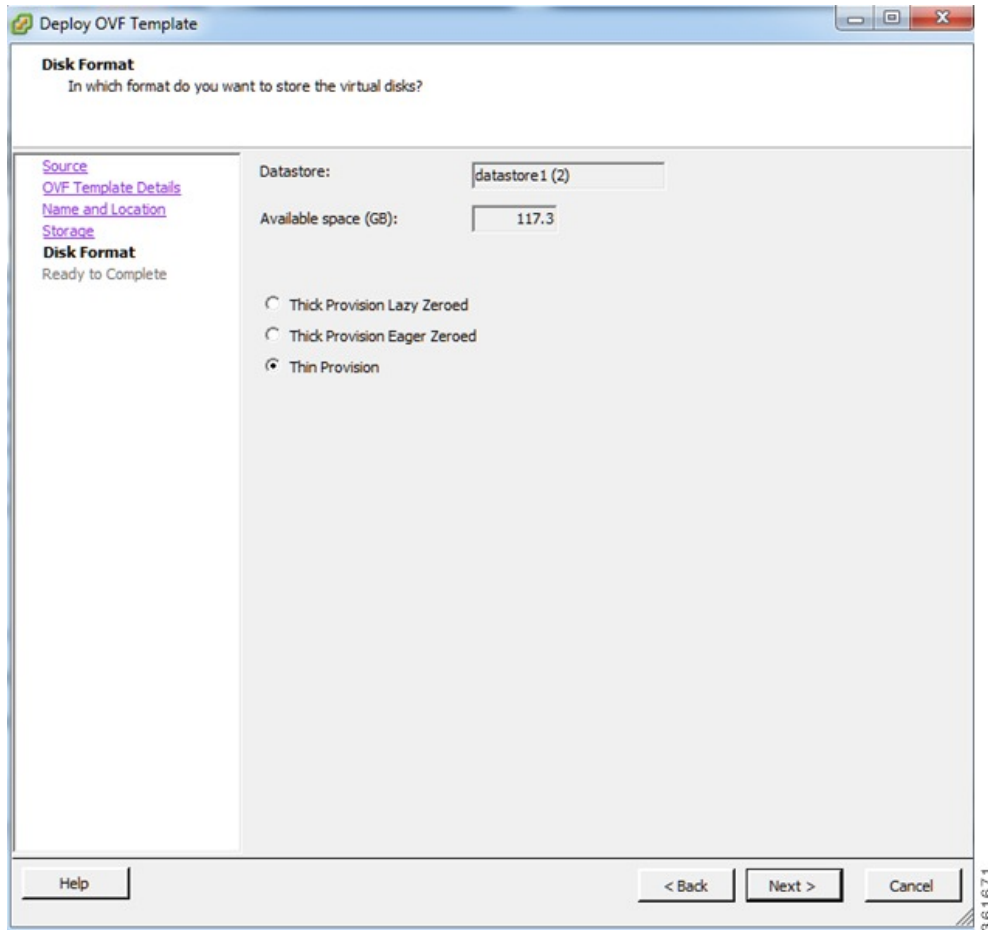


Step 9 Select the data store of the OVF file on the ESXi host, and then click **Next >**. This is the location where the OVF is deployed.

**Step 10**

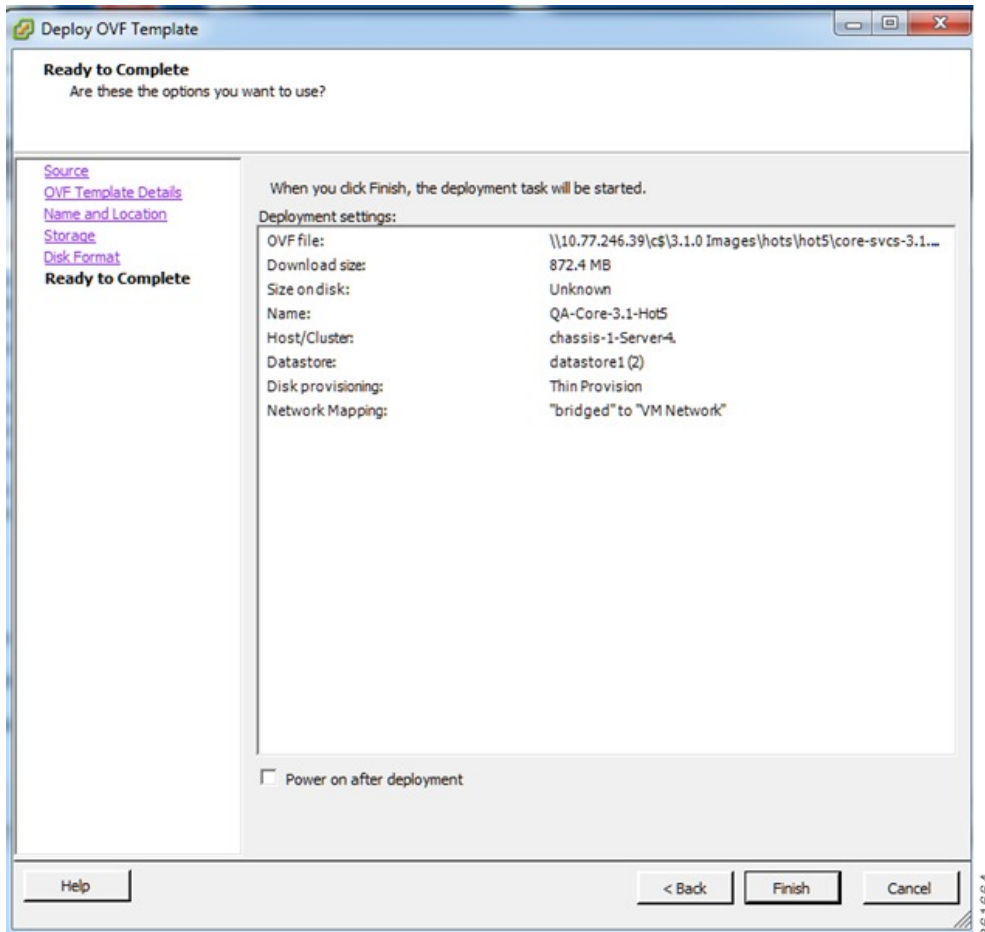
Select **Thin Provision** for the deployment disk format. Click **Next >**.

Nodes can be deployed as thin or thick, depending on the availability of data store. This will use only the disk space required for the VM functionality and not pre-provision the entire OVF allocation of space. However, thick provision will allocate the specified disk in the ovf.

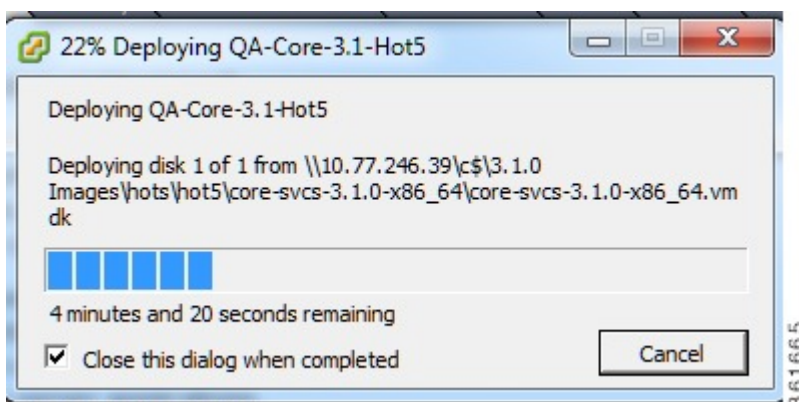


Step 11 Select the Network that the VM communicates with, and then click **Next >**.

Step 12 Verify whether the settings from earlier selections are correct. When finished, select **Finish** to deploy the VM.



A popup similar to the following is displayed. Depending on the resources available and the location of OVF, deployment time of the VM can vary.



Step 13 When the VM is successfully deployed, click **Close**.



Deploying the User Interface Node Software onto a VM

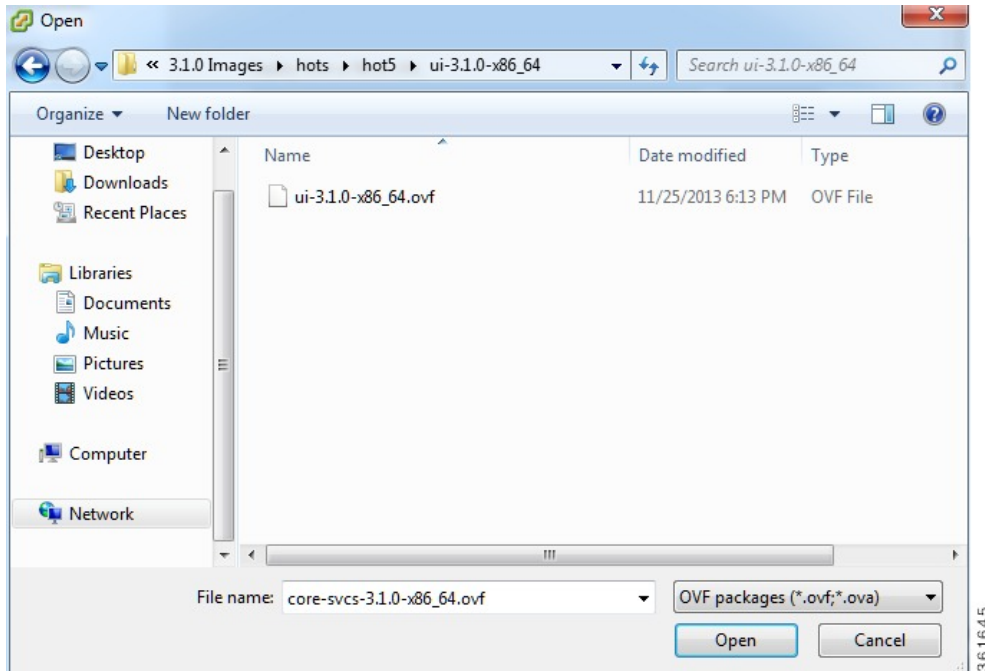
The User Interface (UI) node should be deployed after deploying the Core Services node.

To deploy the UI node software onto a VM, perform the following steps:

**Note**

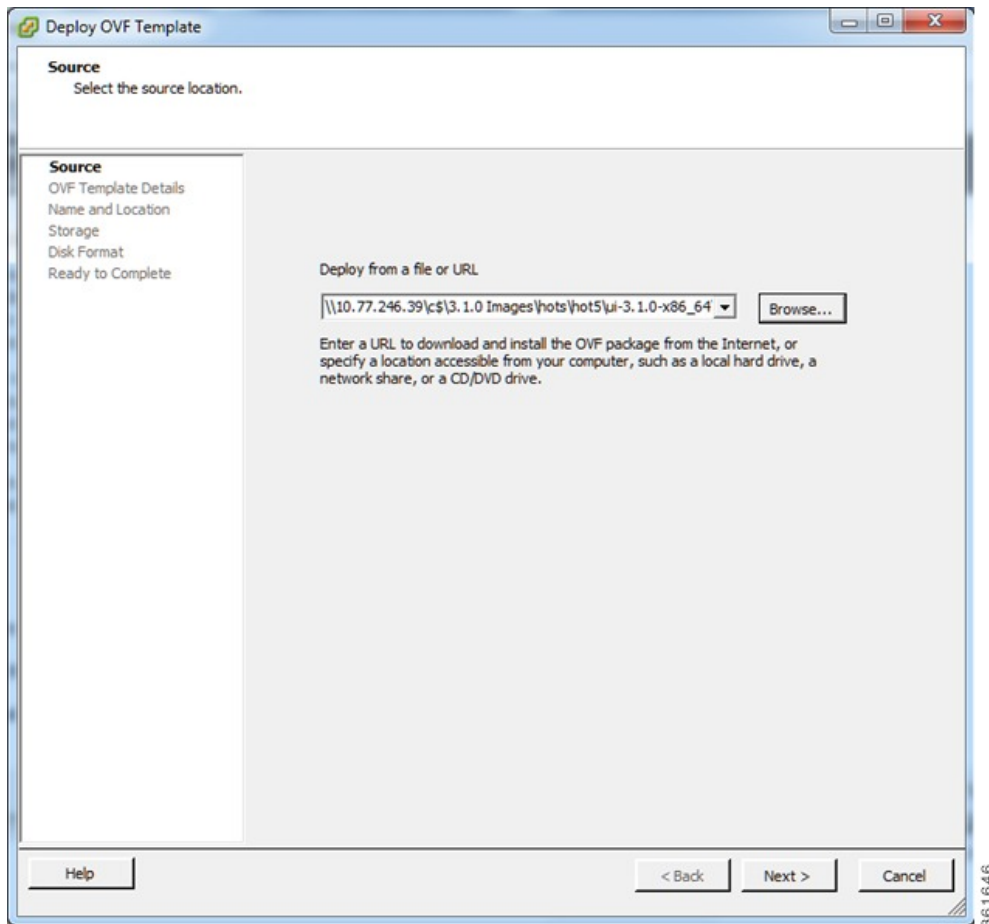
The procedure that follows uses the same procedure as the Core Services node. Refer to the [Deploying the VDS-SM Core Services Software onto a VM](#) for screens and additional information.

- Step 1** Using the VMware's vSphere client, access the ESXi host or VCENTER server and import the OVF images from the extracted location.
- Step 2** Click **File > Deploy OVF Template**.
- Step 3** Click **Browse...** to locate the OVF files extracted previously.
- Step 4** Select the folder that contains the ui OVF file, and then click **Open**.



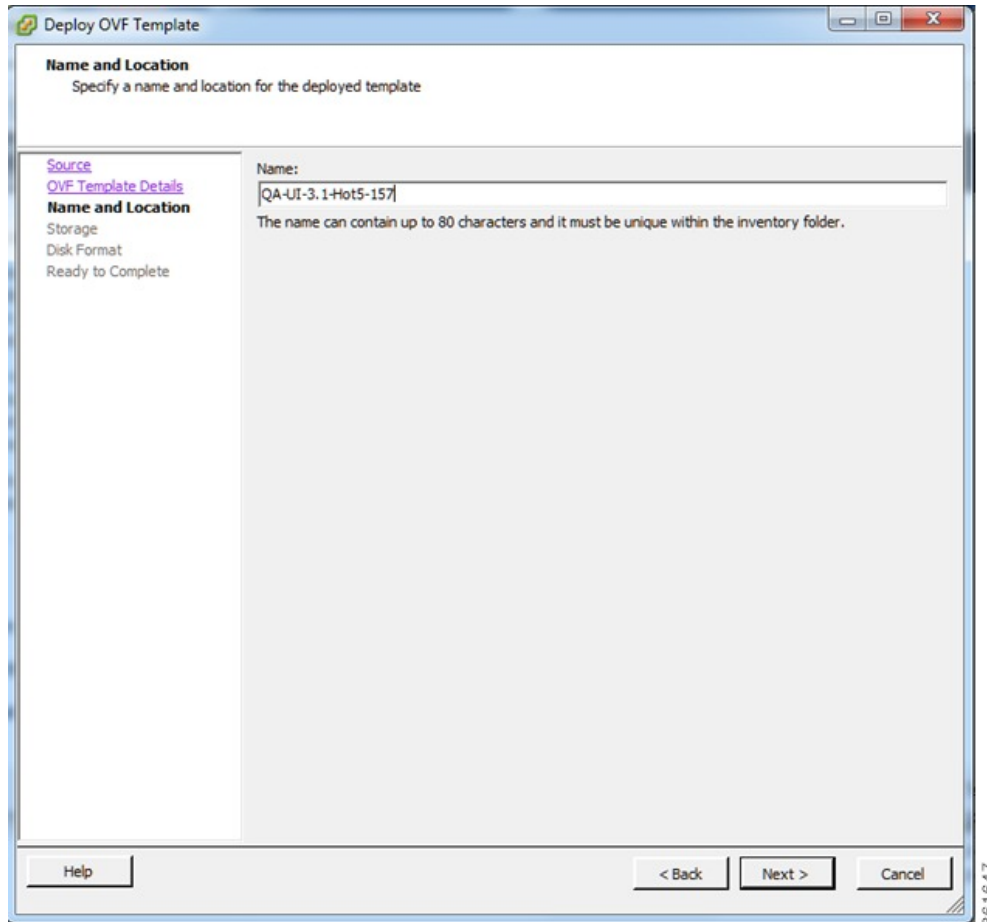
Step 5 Select the ui OVF file and then click **Open**.

Step 6 After the OVF file is selected, click **Next >** to continue.

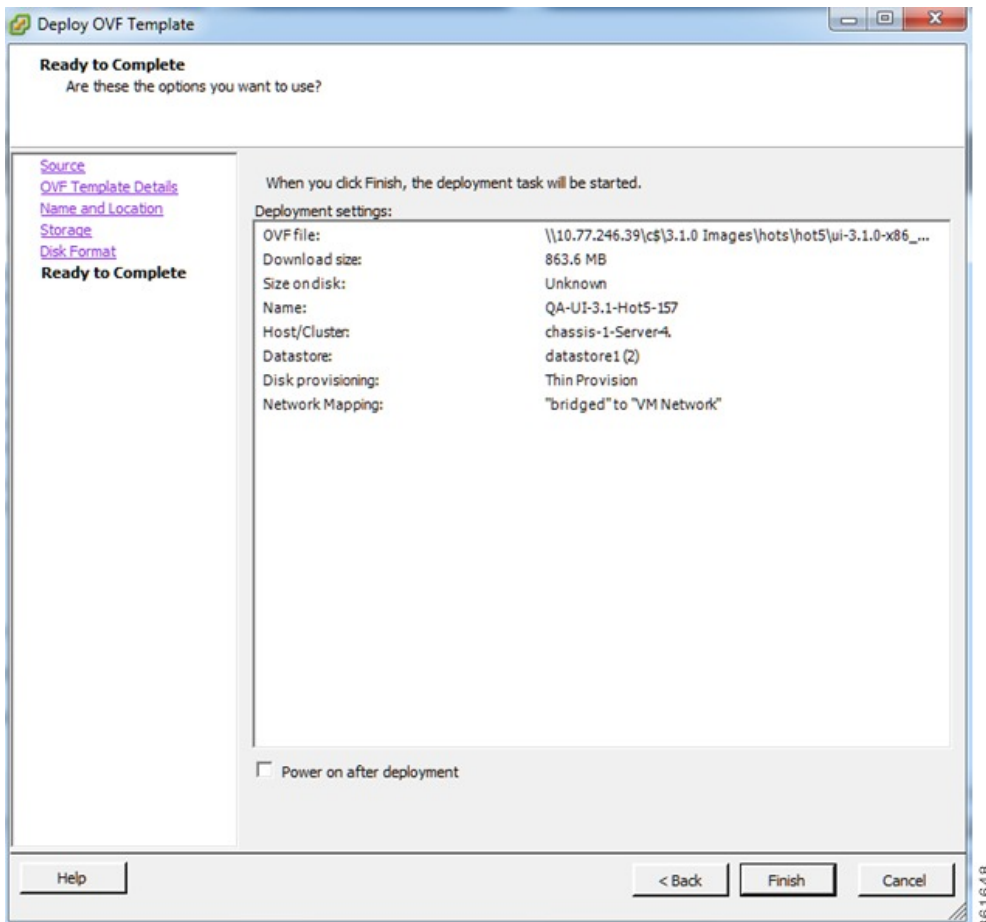


Step 7 Verify the product being deployed and then click **Next >**.

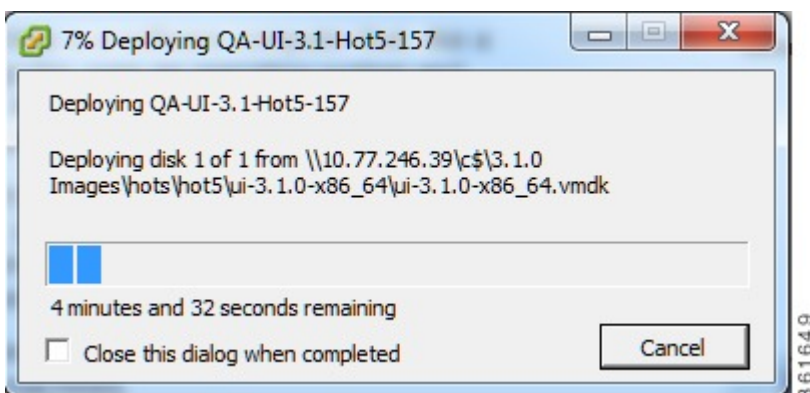
Step 8 Enter a name for the VM being deployed and select the ESX where the VM has to be deployed. When finished, click **Next >**.



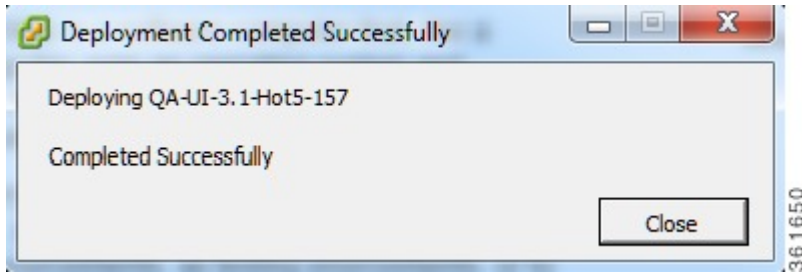
- Step 9** Select the data store of the OVF file on the ESXi host, then click **Next >**. This is the location where the OVF is deployed.
- Step 10** Select **Thin Provision** for the deployment disk format. Click **Next >**.
The nodes can be deployed as thick or thin depending on the availability of data store. Thin Provision will use only the disk space required for the VM functionality and not pre-provision the entire OVF allocation of space. However, thick provision will allocate the specified disk in the OVF.
- Step 11** Select the Network that the VM communicates with, and then click **Next >**.
- Step 12** Verify whether the settings from earlier selections are correct. When finished, select **Finish** to deploy the VM.



A popup similar to the following is displayed. Depending on the resources available and the location of OVF, deployment time of the VM can vary.



Step 13 When the VM is successfully deployed, click **Close**.



Deploying the CDN Manager Node Software onto a VM

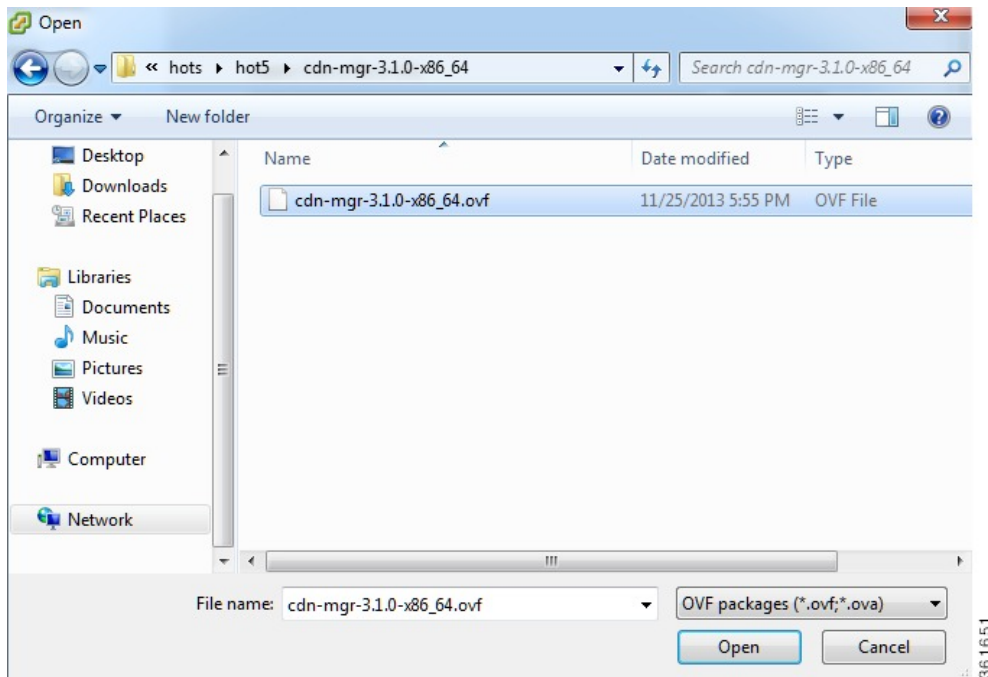
The CDN Manager node should be deployed after the UI node.

To deploy the CDN Manager node software onto a VM, perform the following steps:

**Note**

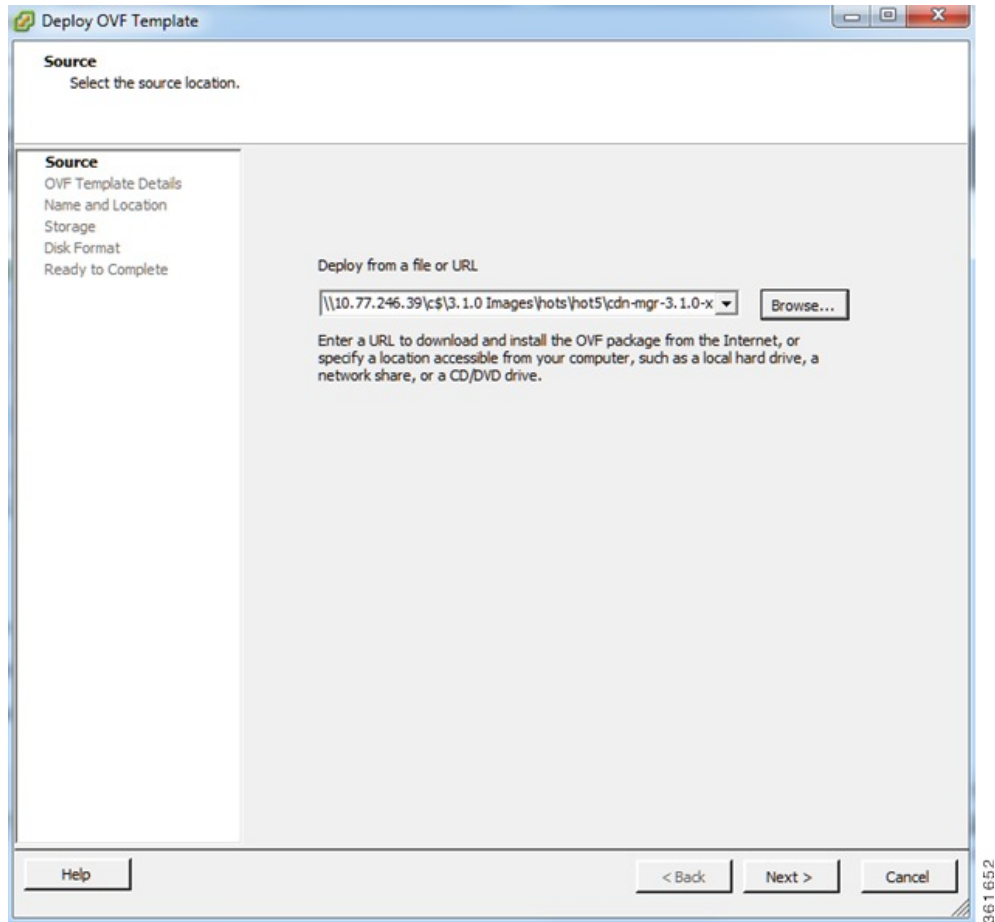
The procedure that follows uses the same procedure as the Core Services node. Refer to the [Deploying the VDS-SM Core Services Software onto a VM](#) for screens and additional information.

- Step 1** Using the VMware's vSphere client, access the ESXi host or VCENTER server and import the OVF images from the extracted location.
- Step 2** Click **File > Deploy OVF Template**.
- Step 3** Click **Browse...** to locate the OVF files extracted previously.
- Step 4** Select the folder that contains the VDS-MGR OVF file, and then click **Open**.



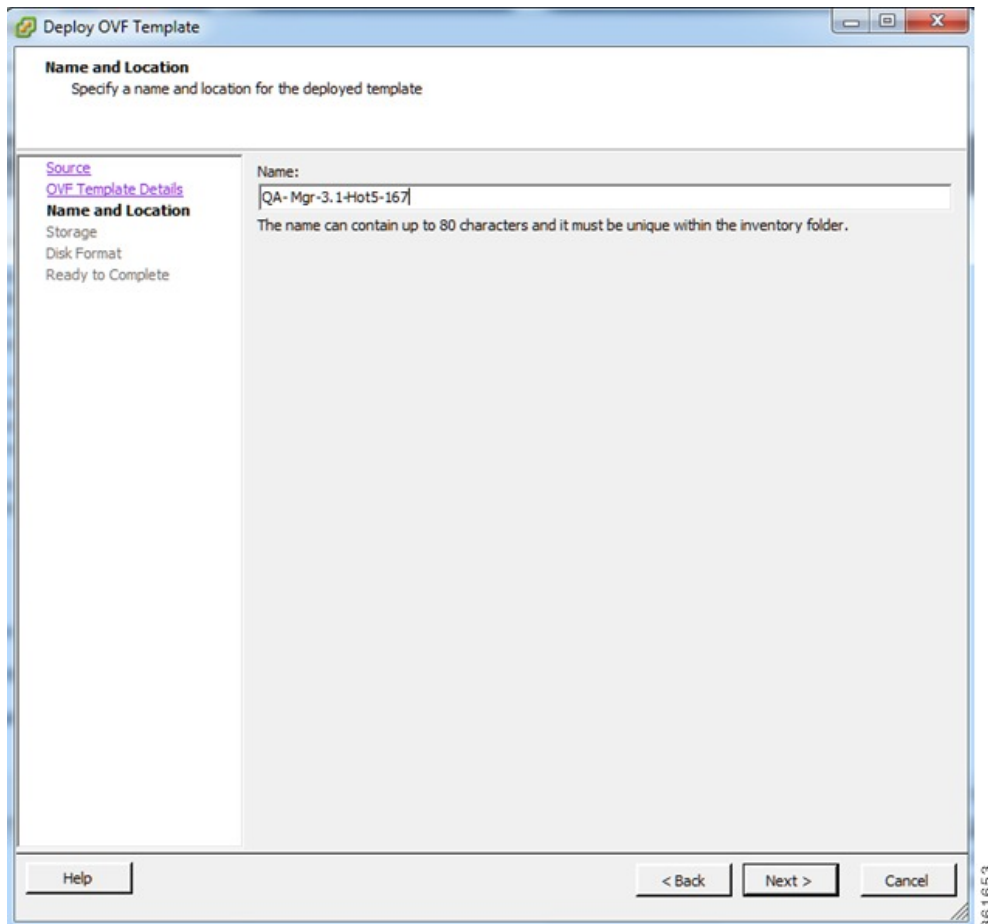
Step 5 Select the vds-mgr OVF file and then click **Open**.

Step 6 After the OVF file is selected, click **Next >** to continue.

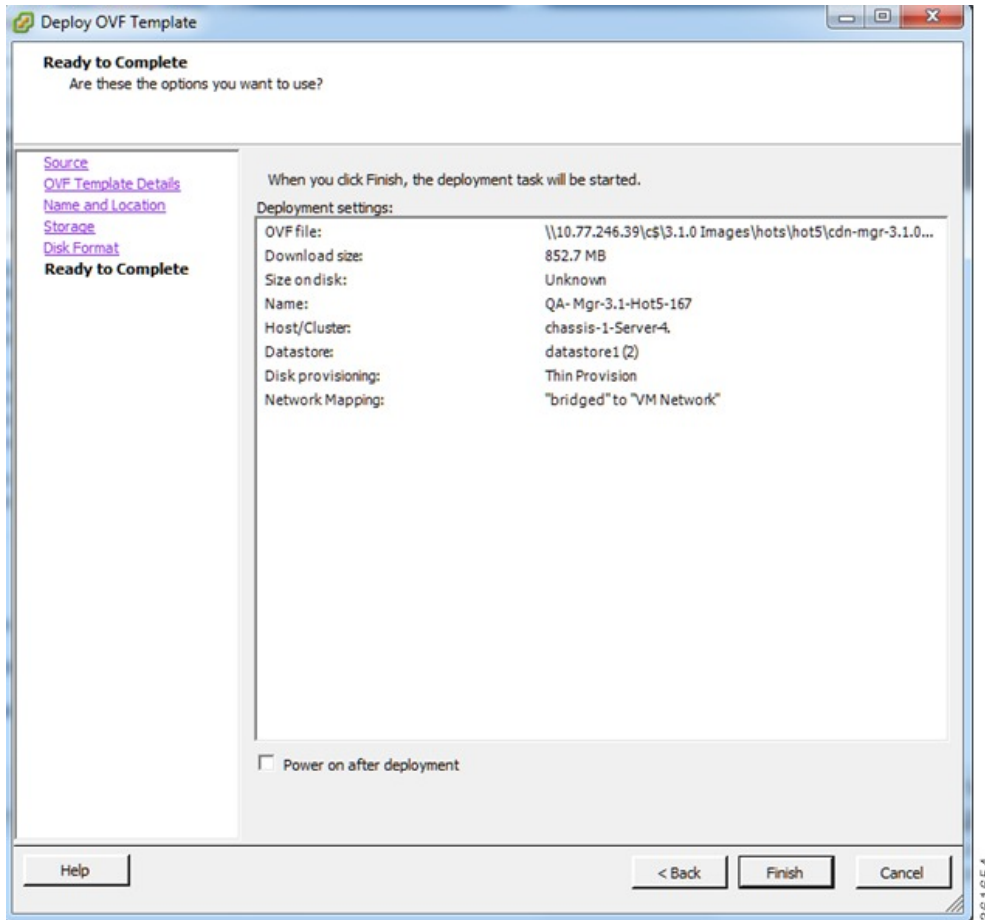


Step 7 Verify the product being deployed and click **Next >**.

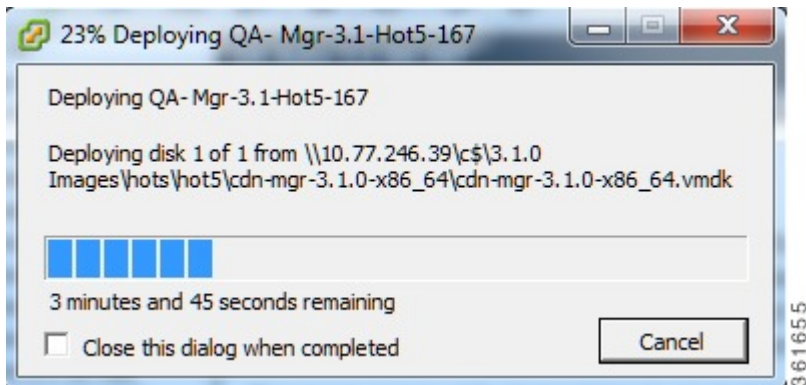
Step 8 Enter a name for the VM being deployed and select the ESX where the VM has to be deployed. When finished, click **Next >**.



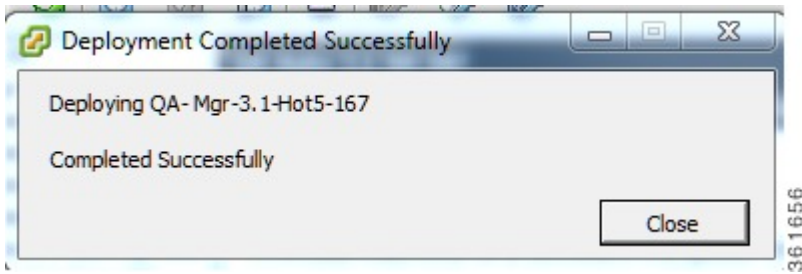
- Step 9** Select the data store of the OVF file on the ESXi host, then click **Next >**. This is the location where the OVF file is deployed.
- Step 10** Select **Thin Provision** for the deployment disk format. Click **Next >**.
Nodes can be deployed as thin or thick, depending on the availability of data store. This will use only the disk space required for the VM functionality and not pre-provision the entire OVF allocation of space. However, thick provision will allocate the specified disk in the ovf.
- Step 11** Select the Network that the VM communicates with, and then click **Next >**.
- Step 12** Verify whether the settings from earlier selections are correct. When finished, select **Finish** to deploy the VM.



A popup similar to the following is displayed. Depending on the resources available and the location of OVF, deployment time of the VM can vary.



Step 13 When the VM is successfully deployed, click **Close**.



Deploying the Analytics Node Software onto VMs

The VDS-SM Analytics nodes should be deployed after deploying the CDN Manager node. VDS system uses four analytics nodes: Search Head, Indexer, Forwarder, and Job Scheduler, and these have to be deployed on individual VMs. The deployment procedure for these analytics nodes is the same.

To deploy the VDS-SM Analytics node software onto a VM, perform the following steps:

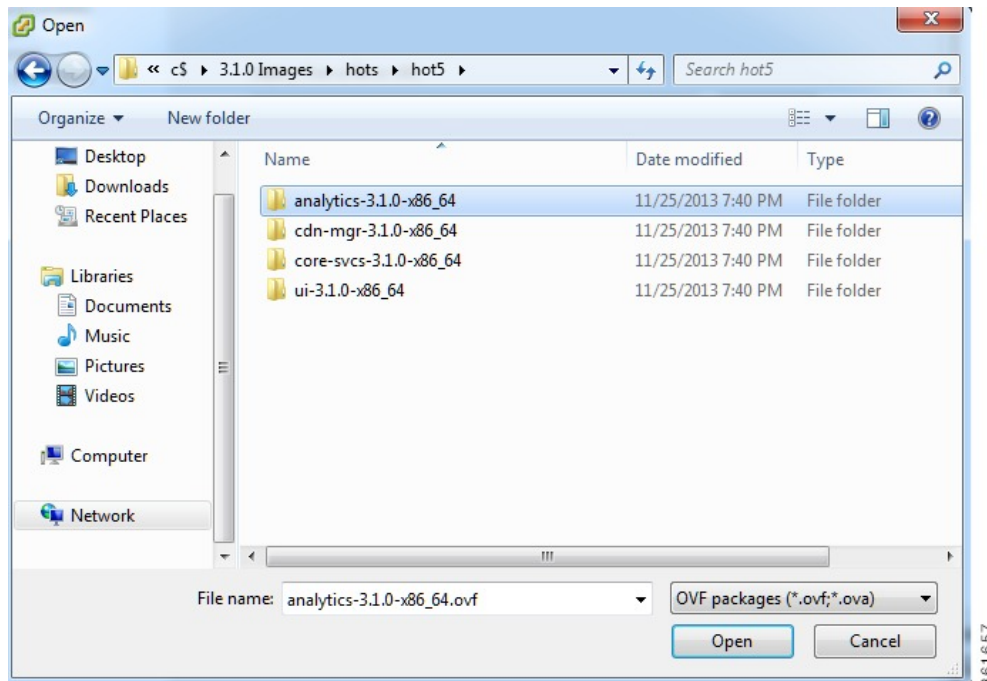


Note

The procedure that follows uses the same procedure as the Core Services node. Refer [Deploying the VDS-SM Core Services Software onto a VM](#) for screens and additional information. Also, all the nodes for Analytics are deployed with the same OVF file and the respective nodes name.

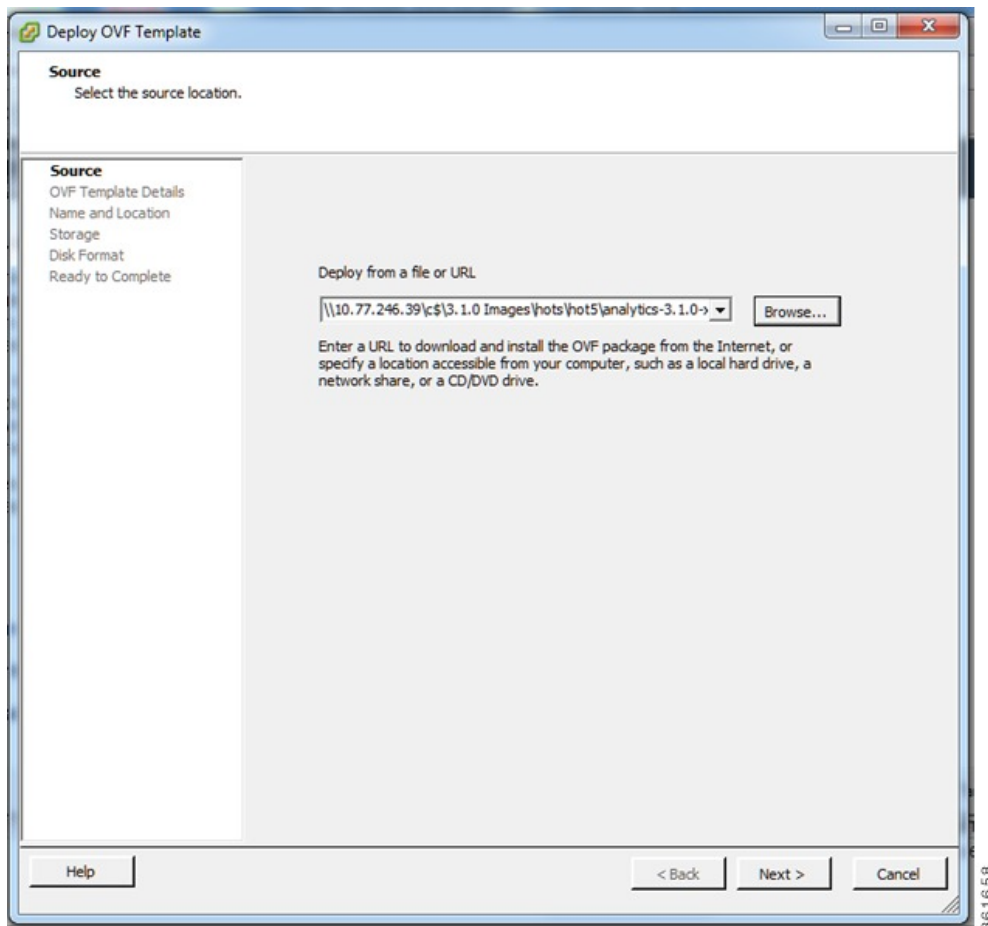
Installing the Search Head Node

- Step 1** Using the VMware's vSphere client, access the ESXi host or VCENTER server and import the OVF images from the extracted location.
- Step 2** Click **File > Deploy OVF Template**.
- Step 3** Click **Browse...** to locate the OVF files extracted previously.
- Step 4** Select the folder that contains the VDS-SM Analytics OVF file, and then click **Open**.

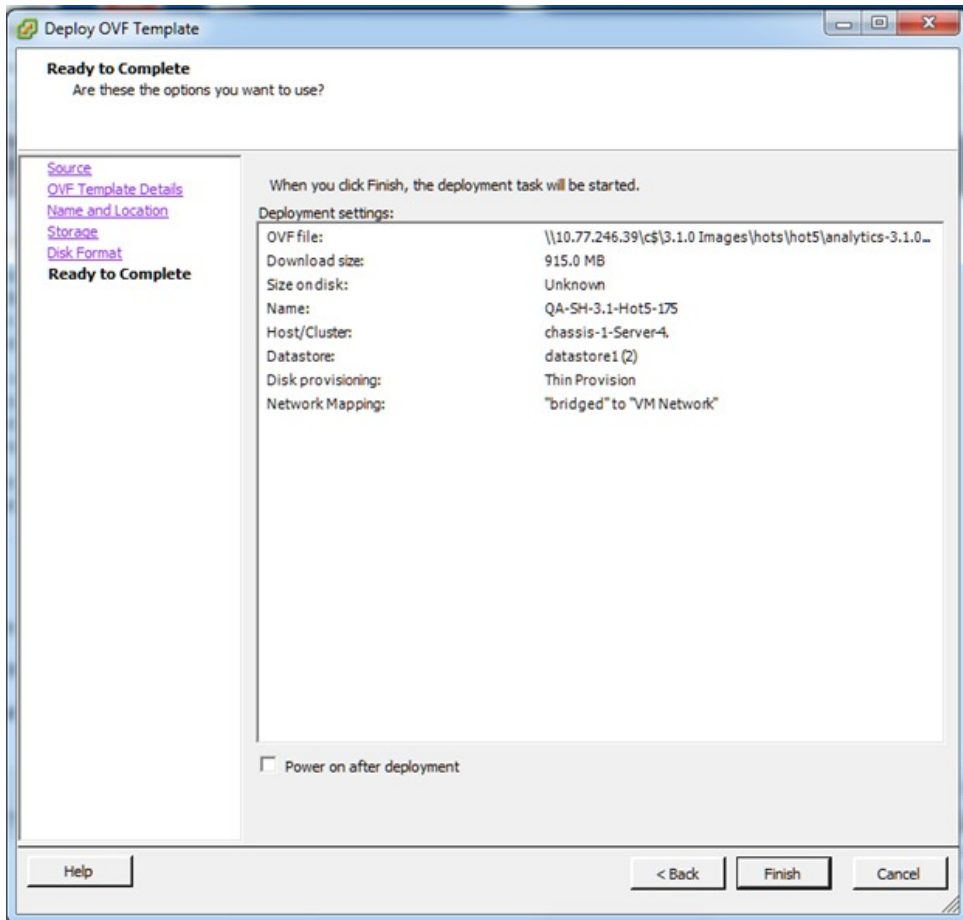


361657

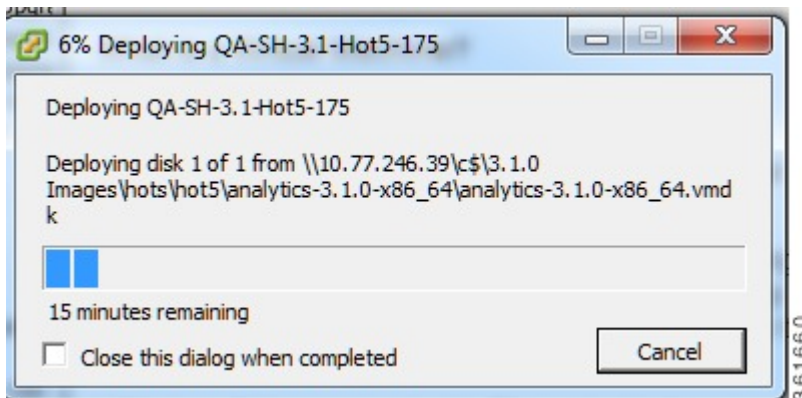
- Step 5** Select the analytics OVF file and then click **Open**.
- Step 6** After the OVF file is selected, click **Next >** to continue.



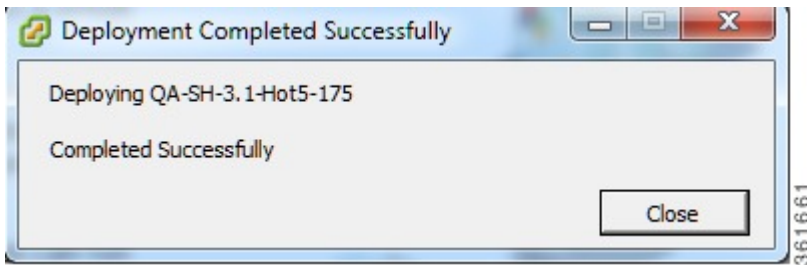
- Step 7** Verify the product being deployed and then click **Next >**.
- Step 8** Enter a name for the VM being deployed and select the ESX where the VM has to be deployed. When finished, click **Next >**.
- Step 9** Select the data store of the OVF file on the ESXi host, then click **Next >**. This is the location where the OVF is deployed.
- Step 10** Select **Thin Provision** for the deployment disk format. Click **Next >**.
Nodes can be deployed as thin or thick, depending on the availability of data store. This will use only the disk space required for the VM functionality and not pre-provision the entire OVF allocation of space. However, thick provision will allocate the specified disk in the OVF.
- Step 11** Select the Network that the VM communicates with, and then click **Next >**.
- Step 12** Verify whether the settings from earlier selections are correct. When finished, select **Finish** to deploy the VM.



Depending on the resources available and the location of OVF, deployment time of the VM can vary.



Step 13 When the VM is successfully deployed, click **Close**.



Note Follow the above steps for other Analytics nodes—Job Scheduler, Forwarder, and Indexer.

Verifying and Backing Up the VDS-SM OVF VMs

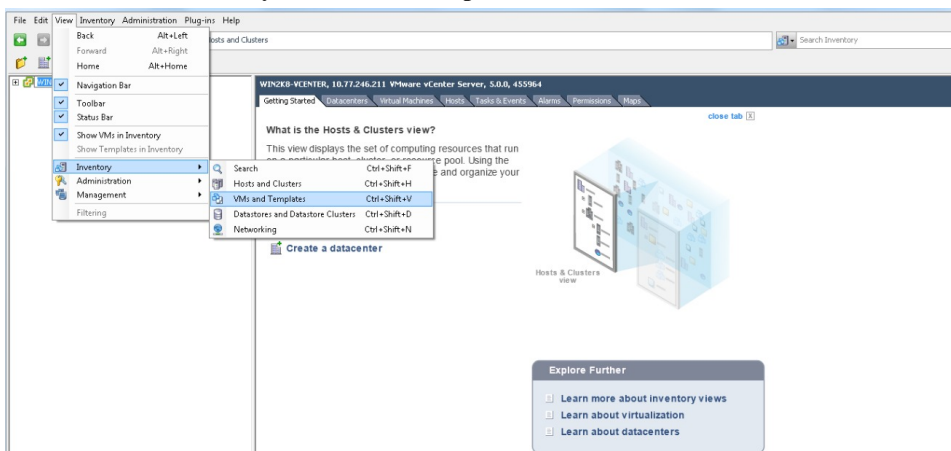
Before continuing the individual node configuration, it is important to verify and backup all VDS-SM OVF VMs.

Verifying the VDS-SM VMs are Available

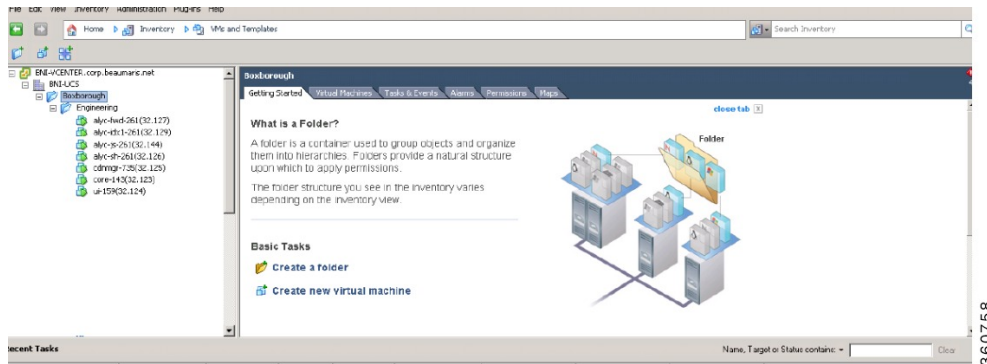
To verify whether the VDS-SM VMs are deployed and available, perform the following steps:

Step 1 Using the VMware's vSphere client, navigate to the location on the ESXI host where the OVF is deployed and the VMs are stored.

Step 2 Select **View > Inventory > VMs and Templates**.

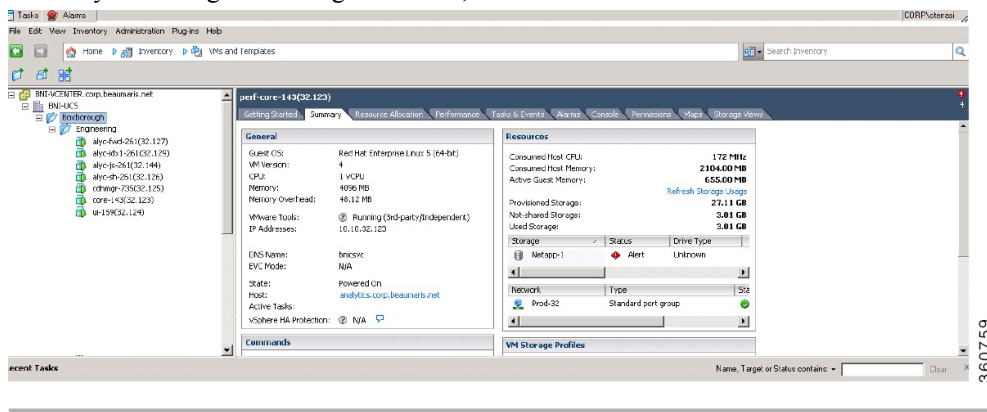


Step 3 Verify whether all previously deployed VMs are present.



360758

Step 4 To verify the configured settings for a VM, select the desired VM and then choose the **Summary** tab.



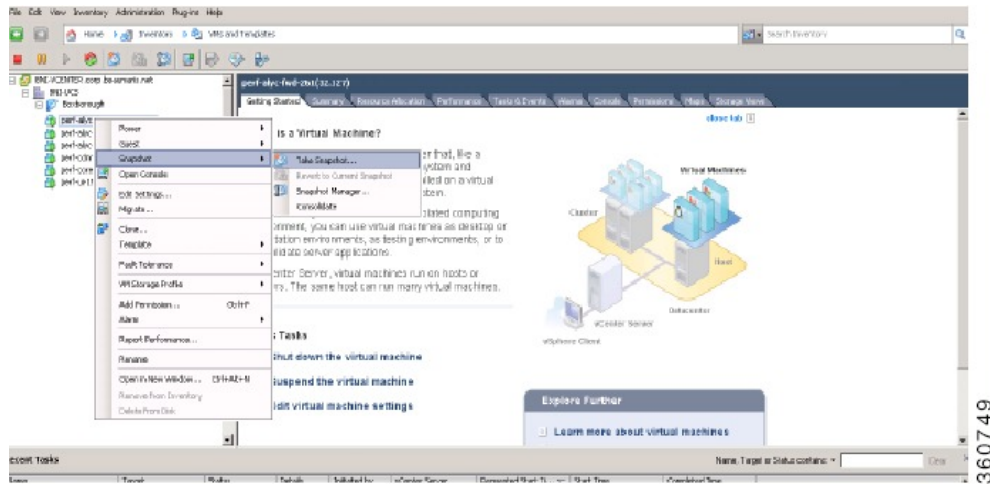
360759

Snapshotting the VDS-SM VMs

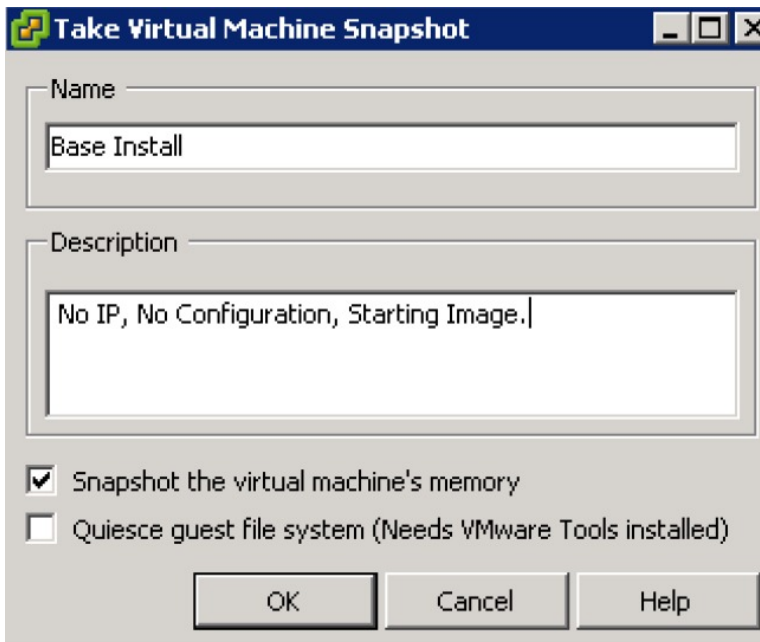
Snapshotting the VMs allows a means to rollback the configuration, should any of the initial configuration become corrupted.

To snapshot each of the VMs, perform the following steps:

- Step 1** Using the VMware's vSphere client, navigate to the location on the ESXI host where the OVF is deployed and the VMs are stored.
- Step 2** Right-click the desired VM and then select **Snapshot > Take Snapshot...**



Step 3 Enter the name and description for this VM.



Step 4 When finished, click **OK**.

Step 5 Repeat this procedure for each VMs.

Configuring CSV Files

After the installation is complete, CSV files need to be configured. Some of the CSV files are automatically configured (no manual intervention is required to enter the values) and some are manually configured (the CSV files will be empty and you need to manually enter the values).

CSV files that are automatically configured are listed below:

- delivery_server_topology.csv
- delivery_service_topology.csv
- service_router_topology.csv

CSV files that needs to be manually configured are listed below:

- delivery_server_capacity.csv
- profilename_bitrate.csv
- provider_title.csv
- useragent_device.csv

For content provider lookup, the content_provider.csv has to be configured.

For details, refer the Getting Started section in the Videoscape Distribution Suite Service Manager user Guide

Lookups

Lookup is a process, which replaces the raw data from the logs with meaningful information. In VDS-SM, lookups are performed during summary index creation and rendering charts. CSV files and third party databases are used in the lookup operations.

Following is the list of lookups:

Lookup Name	Description
Title	The raw logs has the URL field, which contains the 'asset' Information. Lookup is performed on provider_title.csv file to get meaningful Title name. This lookup is performed during summarization.
Genre, Resolution	The raw logs do not contain any information on Genre and Resolution. Based on 'asset', the Genre & Resolution are looked up from provider_title.csv file. This lookup is performed during summarization.
Bitrate	The ABR traffic type's (HLS and MobiTV) raw logs have 'profile name' to indicate bitrate. Lookup is performed on profilename_bitrate.csv to get the related bitrates for profile names. This lookup is performed during summarization.
ISP, Net Sped	The raw logs do not contain information on ISP and Net Speed. It has ClientIP. Lookup is performed on Maxmind DB using ClientIP to get ISP & Net Speed. The Lookup works for public IP addresses. This lookup is performed during summarization.
City	The raw logs do not contain City information. It has ClientIP. Lookup is performed on Maxmind DB using ClientIP to get City. The Lookup works for public IP addresses. This lookup is performed during chart rendering.
Client Type	The raw logs has User Agent related information. Lookup is performed on useragent_device.csv file using User Agent to get Client Type. This lookup is performed during summarization.
Capacity	The Bandwidth and Storage capacity of Delivery Servers are maintained in the delivery_server_capacity.csv file. These capacity values are looked up and added to the summary indexes during summarization.

Lookup Name	Description
Provider	When CP lookup is implemented, users extract CP ID from the URL. Lookup is performed on content_provider.csv file using CP ID to get CP name. This lookup is performed during summarization.



VDS-SM Installation and Configuration

- [VDS-SM Installation and Configuration Overview, page 31](#)
- [Procedure to Restart the Nodes, page 63](#)
- [Browsers Supported, page 64](#)

VDS-SM Installation and Configuration Overview

Once VDS-SM Virtual Machines (VMs) have been defined, deployed, and backed up, the next step is to set up and install the different VDS-SM Services. This installation consists, as a minimum, of the following:

- Power on and boot the VMs
- Login and change passwords
- Configure network settings
- Reboot VMs
- Log into the device UI and configure the service

This installation process should be performed in the following order:

- Core Services
- User Interface
- CDN Manager
- Analytics Nodes
 - Search Head
 - Indexer
 - Forwarder
 - Job Scheduler

Installing VDS-SM Core Services

Core Services consist of a Management Services node and a Database node. These services must be installed first. Each node registers with the Core Services node.

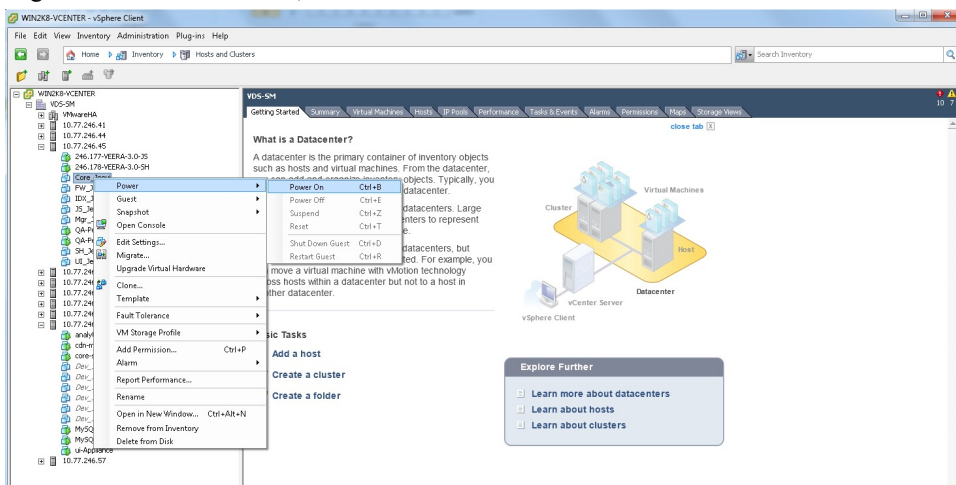


Note

The procedure that follows assumes that all VDS-SM VMs have been created and deployed. If this has not been completed, make sure that it is done before you proceed.

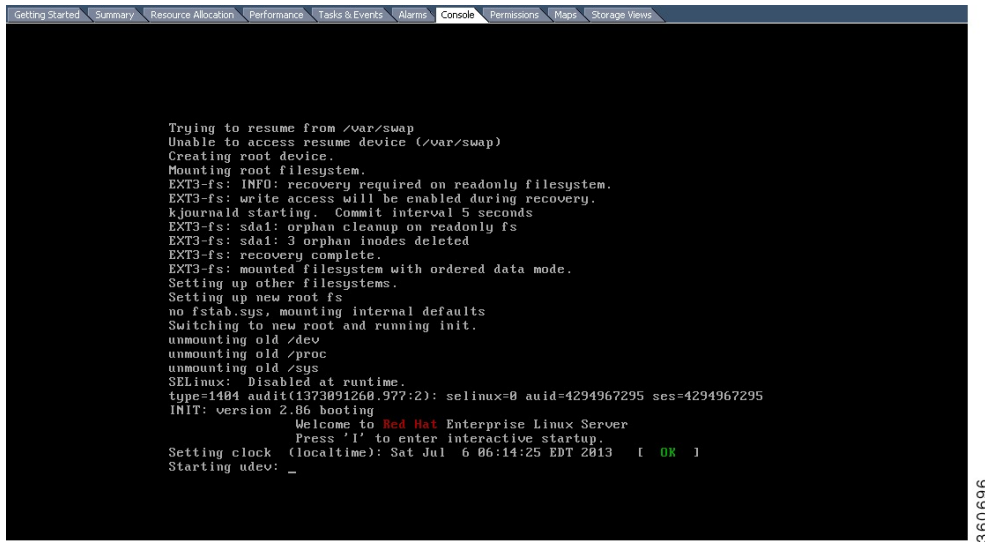
To install the VDS-SM Core Services node, perform the following steps:

- Step 1** Using the VMware's vSphere client, access the ESXi host or VCENTER server where the OVF VMs are located.
Step 2 Right-click the desired VM, select **Power > Power On**.



- Step 3** After the VM is powered on, right-click the VM again and select **Open Console**. Allow the VM to complete starting the boot procedure.

360694



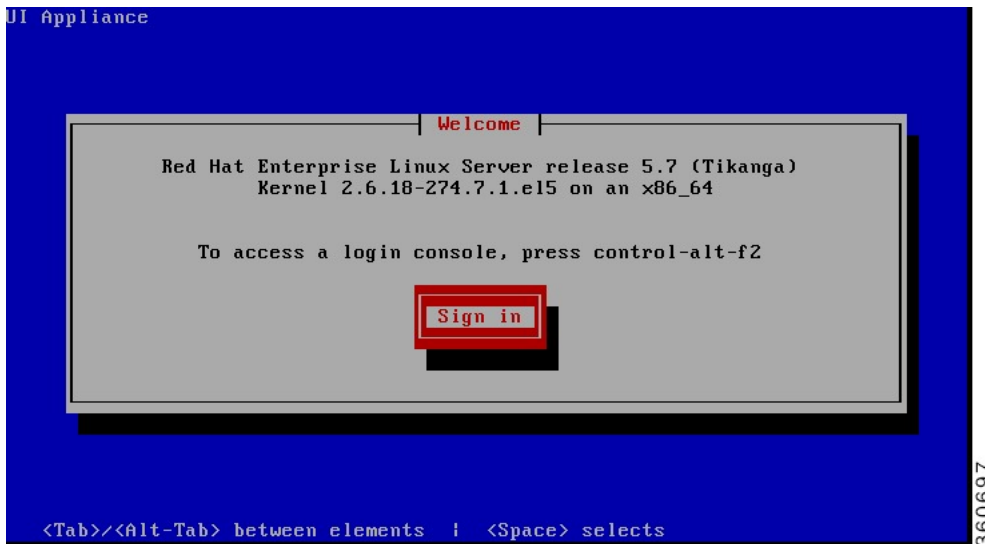
```

Getting Started Summary Resource Allocation Performance Tasks & Events Alarms Console Permissions Maps Storage Views
Trying to resume from /var/swap
Unable to access resume device (/var/swap)
Creating root device.
Mounting root filesystem.
EXT3-fs: INFO: recovery required on readonly filesystem.
EXT3-fs: write access will be enabled during recovery.
kjournald starting. Commit interval 5 seconds
EXT3-fs: sda1: orphan cleanup on readonly fs
EXT3-fs: sda1: 3 orphan inodes deleted
EXT3-fs: recovery complete.
EXT3-fs: mounted filesystem with ordered data mode.
Setting up other filesystems.
Setting up new root fs
no fstab.sys, mounting internal defaults
Switching to new root and running init.
unmounting old /dev
unmounting old /proc
unmounting old /sys
SELinux: Disabled at runtime.
type=1404 audit(1373091260.977:2): selinux=0 auid=4294967295 ses=4294967295
INIT: version 2.86 booting
       Welcome to Red Hat Enterprise Linux Server
       Press 'I' to enter interactive startup.
Setting clock (localtime): Sat Jul  6 06:14:25 EDT 2013  [ OK ]
Starting udev: _

```

360696

Step 4 When the boot process completes, select **Sign in**.



```

UI Appliance
Welcome
Red Hat Enterprise Linux Server release 5.7 (Tikanga)
Kernel 2.6.18-274.7.1.el5 on an x86_64

To access a login console, press control-alt-f2

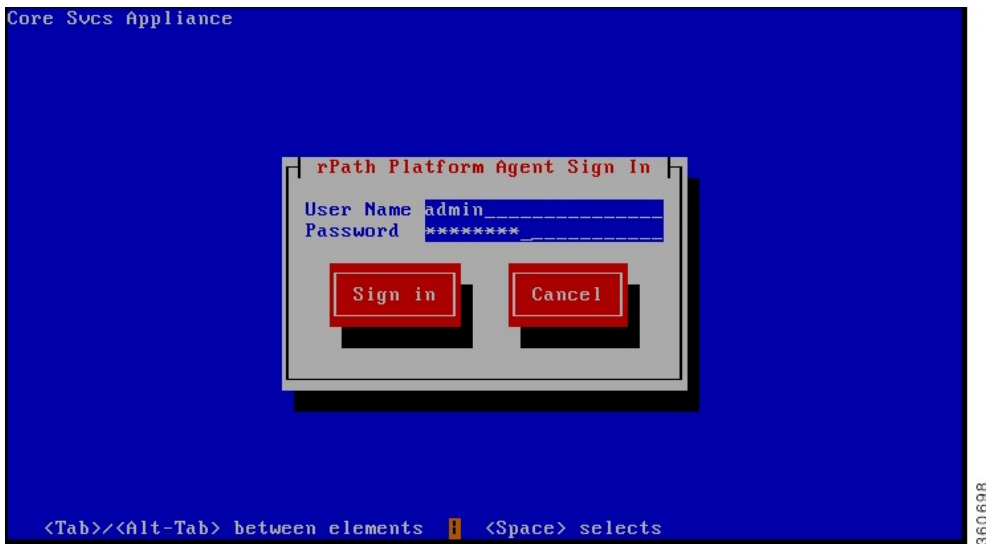
Sign in

<Tab>/<Alt-Tab> between elements | <Space> selects

```

360697

Step 5 Log in using the default credentials; User Name: **admin** and Password: **password**.

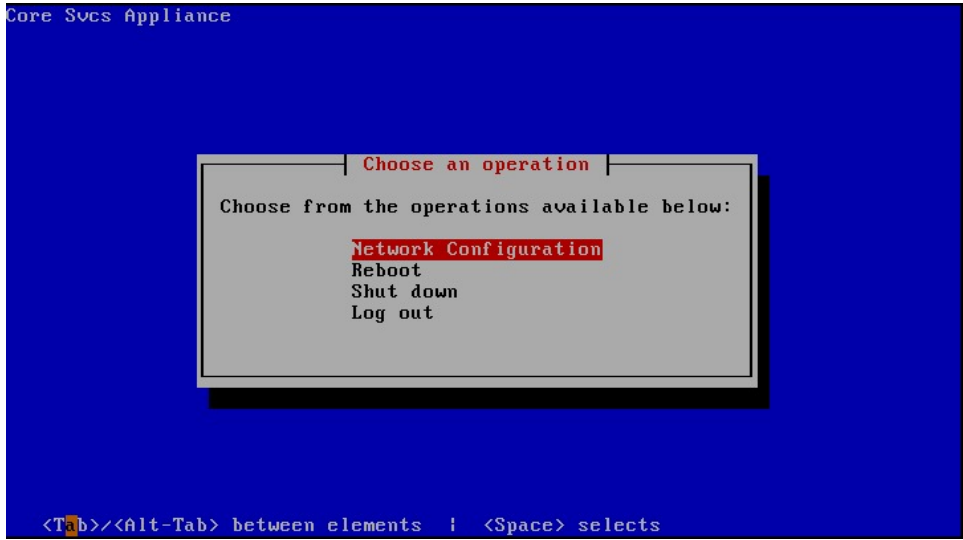


Step 6 If this is your initial login, the system prompts you to change the password.

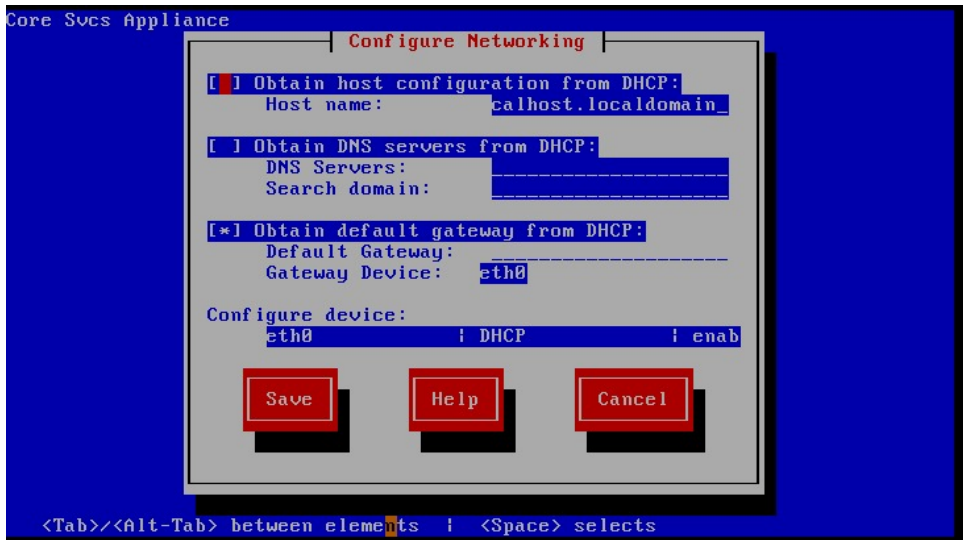
Step 7 Change the password as Beaumaris1. Click **Change** when finished. The Main Menu is displayed.



Step 8 Select **Network Configuration**. The default networking configuration is displayed.

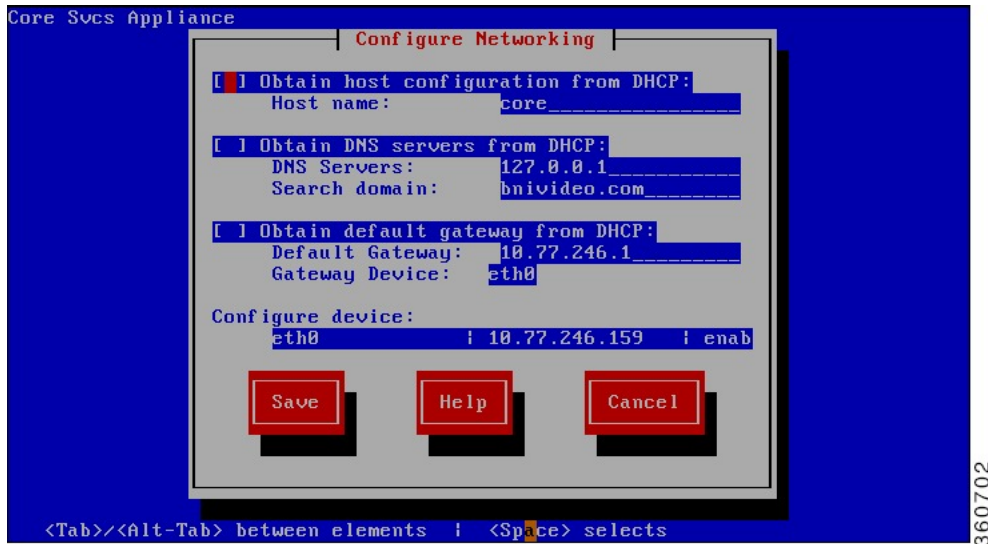


Step 9 If the IP addressing is not obtained via DHCP, enter the Default Gateway, choose the Eth0 interface, and press **Enter**.



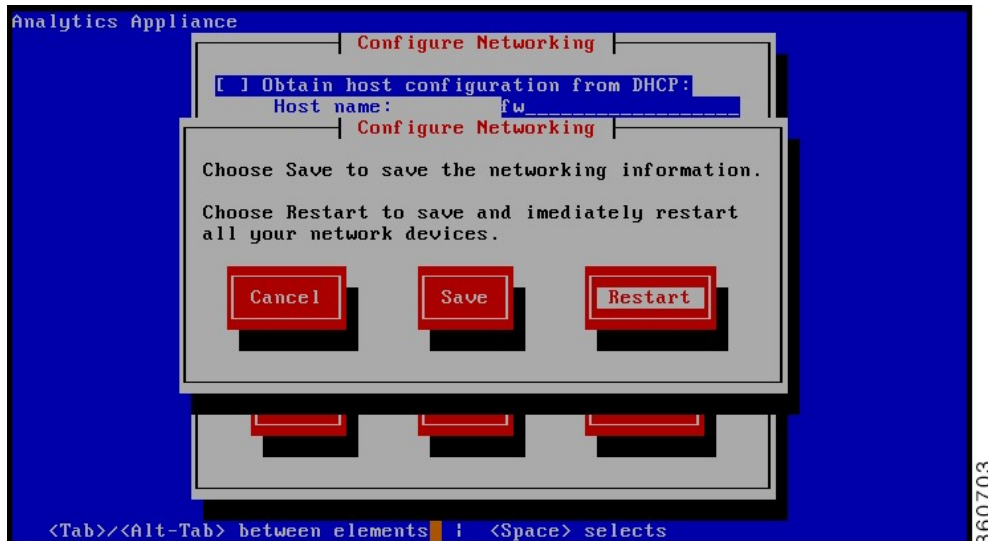
Step 10 Select a unique hostname for the Node.

Step 11 Set the DNS server setting to 127.0.0.1. All other nodes use the Core Services IP address as their DNS server. Press **Enter**.



360702

- Step 12** Enable Eth0. If configuring static addressing, deselect the DHCP option to specify the IP address and netmask.
- Step 13** Enter the IP Address and netmask. Select **Save**. The completed network configuration is displayed.
- Step 14** Select **Save**.
- Step 15** Select **Restart** to re-initialize the Eth0 interface and save the configuration.



360703

Note The window may be blank for some time. Wait for some time, as this is a normal behavior. When the re-initialization is complete, the following screen is displayed.



Step 16 Select **OK**. The Main Menu is displayed.

Step 17 Select **Log out**.

When the initial network configuration has been completed, the next step is to log into the UI and define the time and network settings.

Configuring the Core Service Application Server

To configure the core services application server, perform the following steps:

Step 1 Open a browser and enter the following URL:
`http://<ip_address>:8004`
Where the IP address is the address of the node.

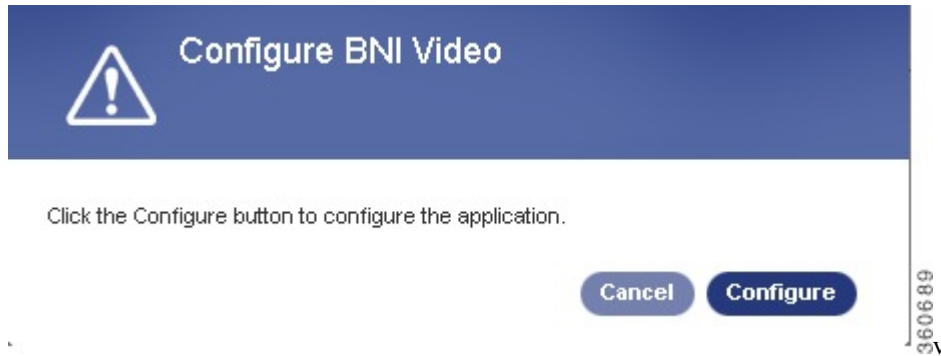
Step 2 Log in using the credentials; User Name: **admin** and the previously changed password. The Configuration Wizard is displayed.

Step 3 Assign the correct time zone to the node and click **Save**. Once the Time settings are saved successfully, the next step is to Configure the Appliance.

Configuring Network Time Protocol (NTP) server will keep all the nodes and CDS-IS network in the same time.

Step 4 The Appliance configuration information is derived from the previous console configuration of this device. On the Core services node, check the **Deploy Management Services** and **Deploy Database** check boxes. Within the **Ping IP for All HA Clusters** field, specify an ICMP ping reachable IP address, such as a default gateway. When finished, click **Configure**.

Step 5 You are prompted with the following popup.

**Step 6**

Click **Configure**. The configuration may take a few minutes and when finished, a screen similar to the following is displayed.



Installing the VDS-SM User Interface Node

**Note**

The procedure that follows assumes that all VDS-SM VMs have been created and deployed. If this has not been completed, make sure that you complete, before you proceed. Also, this procedure uses the same installation and configuration procedure as the Core Services node. Refer to the [Configuring the VDS Core Management Services Node](#) for screens and additional information that are generic to all installation and configuration.

To install the VDS-SM UI node, perform the following steps:

-
- Step 1** Using the VMware's vSphere client, access the ESXi host or VCENTER server where the OVF VMs are located.
 - Step 2** Right-click the desired VM, select **Power > Power On**.
 - Step 3** Once the VM is powered on, right-click the VM again and select **Open Console**. Allow the VM to complete starting the boot procedure.
 - Step 4** When the boot process completes, select **Sign in**.
 - Step 5** Log in using the credentials; User Name: **admin** and Password: **password**.
 - Step 6** If this is your initial login, the system prompts you to change the password.
 - Step 7** Change the password as Beaumaris1. Click **Change** when finished. The Main Menu is displayed.
 - Step 8** Select **Network Configuration**. The default networking configuration is displayed.
 - Step 9** If the IP addressing is not obtained via DHCP, enter the Default Gateway, choose the Eth0 interface, and press **Enter**.
 - Step 10** Select a unique hostname for the Node.
 - Step 11** Set the DNS server setting to that of the Core Services node. Press **Enter**.
 - Step 12** Enable Eth0. If configuring static addressing, deselect the DHCP option to specify the IP address and netmask.
 - Step 13** Enter the IP Address and netmask. Select **Save**. The completed network configuration is displayed.
 - Step 14** Select **Save**.
 - Step 15** Select **Restart** to re-initialize the Eth0 interface and save the configuration.
Note The window may be blank for some time. Wait for some time, as this is a normal behavior.
 - Step 16** Select **OK**. The Main Menu is displayed.
 - Step 17** Select **Log out**.
-

When the initial network configuration has been completed, the next step is to log into the UI and define the network settings.

Configuring the User Interface Node Application Server

To configure the user interface application server settings, perform the following steps:

-
- Step 1** Open a browser and enter the following URL:
`http://<ip_address>:8004`
Where the IP address is the address of the node.
 - Step 2** Log in using the default credentials; User Name: **admin** and the previously changed password. The Configuration Wizard is displayed.
 - Step 3** The UI configuration information is derived from the previous console configuration of the UI. Enter the IP address of the Core Services Node that is running the Management Services. When finished, click **Configure**. You are prompted again to configure the application.
 - Step 4** Click **Configure**. The configuration may take a few minutes.

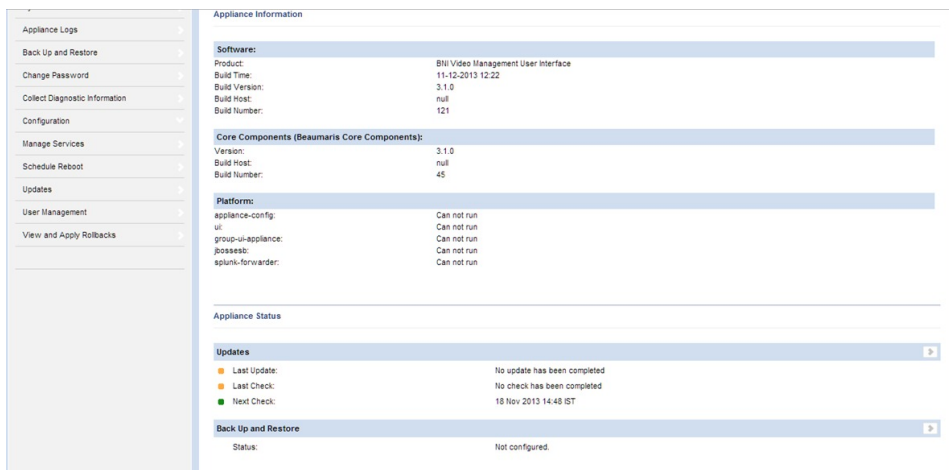


Click the Configure button to configure the application.



360693

The UI node should now be available in the browser.



361737

Installing the VDS-SM CDN Manager Node



Note

The procedure that follows assumes that all VDS-SM VMs have been created and deployed. If this has not been completed, make sure that you complete, before you proceed. Also, this procedure uses the same installation and configuration procedure as the Core Services node. Refer to the [Configuring the VDS Core Management Services Node](#) for screens and additional information that are generic to all installation and configuration.

To install the CDN Manager node, perform the following steps:

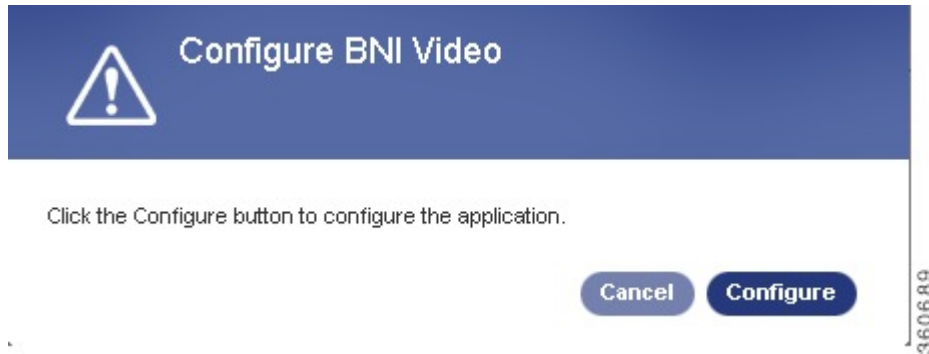
-
- Step 1** Using the VMware's vSphere client, access the ESXi host or VCENTER server where the OVF VMs are located.
 - Step 2** Right-click the Management Services VM, select **Power > Power On**.
 - Step 3** When the VM is powered on, right-click the VM again and select **Open Console**. Allow the VM to complete starting the boot procedure.
 - Step 4** When the boot process completes, select **Sign in**.
 - Step 5** Log in using the default credentials; User Name: **admin** and Password: **password**.
 - Step 6** If this is your initial login, the system prompts you to change the password.
 - Step 7** Change the password as Beaumaris1. Click **Change** when finished. The Main Menu is displayed.
 - Step 8** Select **Network Configuration**. The default networking configuration is displayed.
 - Step 9** If the IP addressing is not obtained via DHCP, enter the Default Gateway, choose the Eth0 interface, and press **Enter**.
 - Step 10** Select a unique hostname for the Node.
 - Step 11** Set the DNS server setting to that of the Core Services node. Press **Enter**.
 - Step 12** Enable Eth0. If configuring static addressing, deselect the DHCP option and specify the IP address and netmask.
 - Step 13** Enter the IP Address and netmask. Select **Save**. The completed network configuration is displayed.
 - Step 14** Select **Save**.
 - Step 15** Select **Restart** to re-initialize the Eth0 interface and save the configuration.
Note The window may be blank for some time. Wait for some time, as this is a normal behavior.
 - Step 16** Select **OK**. The Main Menu is displayed.
 - Step 17** Select **Log out**.
-

When the initial network configuration has been completed, the next step is to log into the UI and define the network settings.

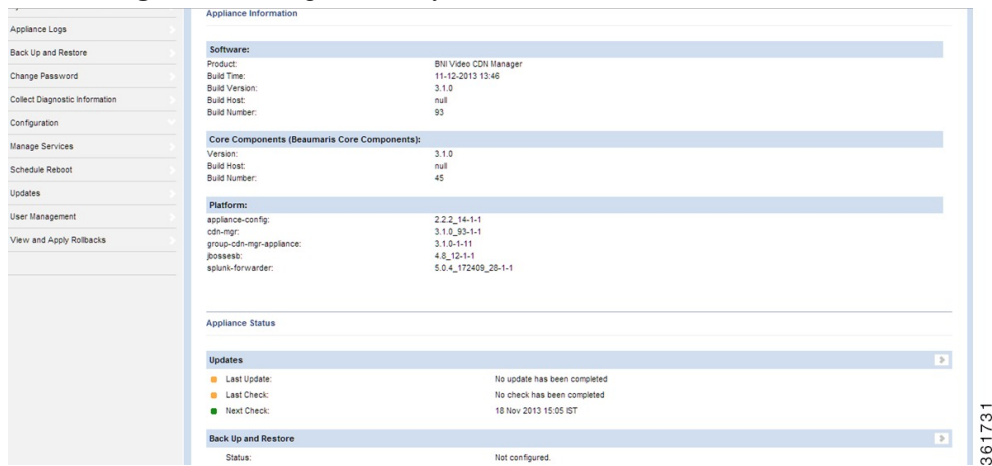
Configuring the CDN Manager Node Application Server

To configure the CDN Manager Application Server settings, perform the following steps:

-
- Step 1** Open a browser and enter the following URL:
`http://<ip_address>:8004`
Where the IP address is the address of the node.
 - Step 2** Log in using the credentials; User Name: **admin** and the previously changed password. The Configuration Wizard is displayed.
 - Step 3** The Management Services configuration information is derived from the previous console configuration of the Management Services node. Enter the IP address of the Core Services Node that is running Management Services. When finished, click **Configure**. You are prompted again to configure the application.



Step 4 Click **Configure**. The configuration may take a few minutes.



Installing the VDS-SM Analytics Search Head



Note

The procedure that follows assumes that all VDS-SM VMs have been created and deployed. If this has not been completed, make sure that it is done before you proceed. Also, this procedure uses the similar installation and configuration procedure as the Core Services node. Refer to the [Configuring the VDS Core Management Services Node](#) for screens and additional information that are generic to all installation and configuration.

To install the VDS-SM Analytics Search Head, perform the following steps:

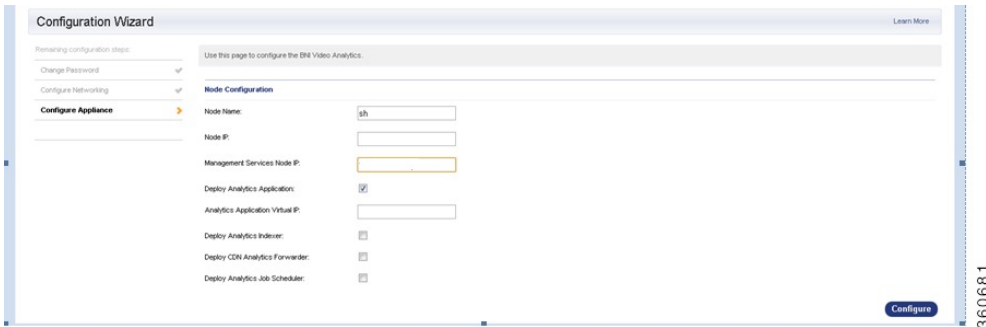
-
- Step 1** Using the VMware's vSphere client, access the ESXi host or VCENTER server where the OVF VMs are located.
 - Step 2** Right-click the Analytics Search Head VM, select **Power > Power On**.
 - Step 3** When the VM is powered on, right-click the VM again and select **Open Console**. Allow the VM to complete starting the boot procedure.
 - Step 4** When the boot process completes, select **Sign in**.
 - Step 5** Log in using the default credentials; User Name: **admin** and Password: **password**.
 - Step 6** If this is your initial login, the system prompts you to change the password.
 - Step 7** Change the password as Beaumaris1. Click **Change** when finished. The Main Menu is displayed.
 - Step 8** Select **Network Configuration**. The default networking configuration is displayed.
 - Step 9** If the IP addressing is not obtained via DHCP, enter the Default Gateway, choose the Eth0 interface, and press **Enter**.
 - Step 10** Select a unique hostname for the Node. This must be unique from all analytics nodes.
 - Step 11** Set the DNS server setting to that of the Core Services node. Press **Enter**.
 - Step 12** Enable Eth0. If configuring static addressing, deselect the DHCP option and specify the IP address and netmask.
 - Step 13** Enter the IP Address and netmask. Select **Save**. The completed network configuration is displayed.
 - Step 14** Select **Save**.
 - Step 15** Select **Restart** to re-initialize the Eth0 interface and save the configuration.
Note The window may be blank for some time. Wait for some time, as this is a normal behavior.
 - Step 16** Select **OK**. The Main Menu is displayed.
 - Step 17** Select **Log out**.
-

When the initial network configuration has been completed, the next step is to log into the UI and define the network settings.

Configuring the Analytics Search Head Application Server

To configure the Analytics Search Head Application Server settings, perform the following steps:

-
- Step 1** Open a browser and enter the following URL:
`http://<ip_address>:8004`
Where the IP address is the address of the Analytics Search Head.
 - Step 2** Log in using the credentials; User Name: **admin** and the previously changed password. The Configuration Wizard is displayed.



360681

Step 3

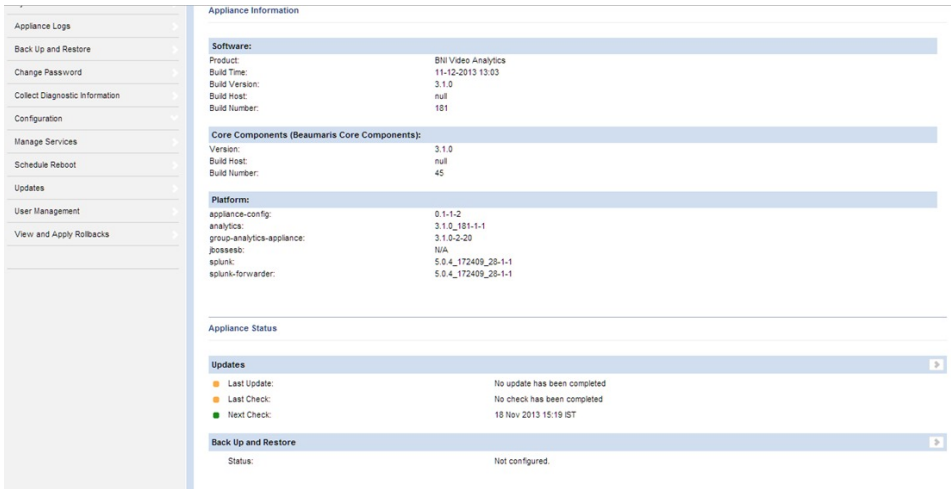
The Appliance configuration information is derived from the previous console configuration of this device. Enter the IP address of the Core Services node that is running the Management Services, and check the **Deploy Analytics Application** check box. When finished, click **Configure**. You are prompted with the following popup.



360689

Step 4

Click **Configure**. The configuration may take a few minutes and when finished, a screen similar to the following is displayed.



361736

Installing the VDS-SM Analytics Indexer



Note

The procedure that follows assumes that all VDS-SM VMs have been created and deployed. If this has not been completed, make sure that it is done before you proceed. Also, this procedure uses the similar installation and configuration procedure as the Core Services node. Refer to the [Configuring the VDS Core Management Services Node](#) for screens and additional information that are generic to all installation and configuration.

To install the VDS-SM Analytics Indexer, perform the following steps:

-
- Step 1** Using the VMware's vSphere client, access the ESXi host where the OVF VMs are located.
 - Step 2** Right-click the Analytics Indexer VM, select **Power > Power On**.
 - Step 3** When the VM is powered on, right-click the VM again and select **Open Console**. Allow the VM to complete starting the boot procedure.
 - Step 4** When the boot process completes, select **Sign in**.
 - Step 5** Log in using the default credentials; User Name: **admin** and Password: **password**.
 - Step 6** If this is your initial login, the system prompts you to change the password.
 - Step 7** Change the password as Beaumaris1. Click **Change** when finished. The Main Menu is displayed.
 - Step 8** Select **Network Configuration**. The default networking configuration is displayed.
 - Step 9** If the IP addressing is not obtained via DHCP, enter the Default Gateway, choose the Eth0 interface, and press **Enter**.
 - Step 10** Select a unique hostname for the Node. This hostname must be unique from all other analytics nodes.
 - Step 11** Set the DNS server setting to that of the Core Services node. Press **Enter**.
 - Step 12** Enable Eth0. If configuring static addressing, deselect the DHCP option and specify the IP address and netmask.
 - Step 13** Enter the IP Address and netmask. Select **Save**. The completed network configuration is displayed.
 - Step 14** Select **Save**.
 - Step 15** Select **Restart** to re-initialize the Eth0 interface and save the configuration.
Note The window may be blank for some time. Wait for some time, as this is a normal behavior.
 - Step 16** Select **OK**. The Main Menu is displayed.
 - Step 17** Select **Log out**.
-

When the initial network configuration has been completed, the next step is to log into the UI and define the network settings.

Configuring the Analytics Indexer Application Server

To configure the Analytics Indexer Application Server, perform the following steps:

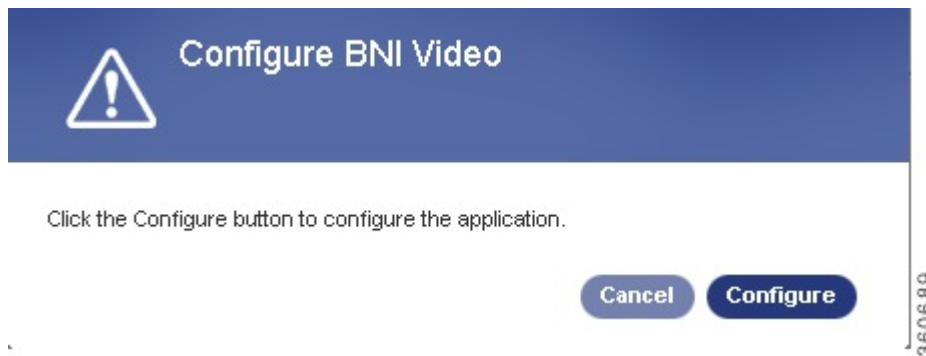
Step 1 Open a browser and enter the following URL:

`http://<ip_address>:8004`

Where the IP address is the address of the Analytics Indexer.

Step 2 Log in using the credentials; User Name: **admin** and the previously changed password. The Configuration Wizard is displayed.

Step 3 The Appliance configuration information is derived from the previous console configuration of this device. Enter the IP address of the Core Services node that is running the Management Services, and check the **Deploy Analytics Indexer** check box. When finished, click **Configure**. You are prompted with the following popup.



Step 4 Click **Configure**. The configuration may take a few minutes and when finished, a screen similar to the following is displayed.

Software:	
Product:	BNI Video Analytics
Build Time:	11-12-2013 13:03
Build Version:	3.1.0
Build Host:	null
Build Number:	181

Core Components (Beaumaris Core Components):	
Version:	3.1.0
Build Host:	null
Build Number:	45

Platform:	
appliance-config:	0.1-1-2
analytics:	3.1.0_181-1-1
group-analytics-appliance:	3.1.0-2-20
jbossesb:	N/A
splunk:	5.0.4_172409_28-1-1
splunk-forwarder:	5.0.4_172409_28-1-1

Updates	
Last Update:	No update has been completed
Last Check:	No check has been completed
Next Check:	18 Nov 2013 15:17:57

Back Up and Restore	
Status:	Not configured.

Note Analytics Indexer can be deployed in a separate network using the Analytics ISO image.

Installing the VDS-SM Analytics Forwarder



Note The procedure that follows assumes that all VDS-SM VMs have been created and deployed. If this has not been completed, make sure that it is done before you proceed. Also, this procedure uses the similar installation and configuration procedure as the Core Services node. Refer to the [Configuring the VDS Core Management Services Node](#) for screens and additional information that are generic to all installation and configuration.

To install the VDS-SM Analytics Forwarder, perform the following steps:

-
- Step 1** Using the VMware's vSphere client, access the ESXi host where the OVF VMs are located.
 - Step 2** Right-click the Analytics Forwarder VM, select **Power > Power On**.
 - Step 3** When the VM is powered on, right-click the VM again and select **Open Console**. Allow the VM to finish starting the boot procedure.
 - Step 4** When the boot process completes, select **Sign in**.
 - Step 5** Log in using the default credentials; User Name: **admin** and Password: **password**.
 - Step 6** If this is your initial login, the system prompts you to change the password.
 - Step 7** Change the password as Beaumaris1. Click **Change** when finished. The Main Menu is displayed.
 - Step 8** Select **Network Configuration**. The default networking configuration is displayed.
 - Step 9** If the IP addressing is not obtained via DHCP, enter the Default Gateway, choose the Eth0 interface, and press **Enter**.
 - Step 10** Select a unique hostname for the Node. The hostname must be unique from all analytics nodes.
 - Step 11** Set the DNS server setting to that of the Core Services node. Press **Enter**.
 - Step 12** Enable Eth0. If configuring static addressing, deselect the DHCP option and specify the IP address and netmask.
 - Step 13** Enter the IP Address and netmask. Select **Save**. The completed network configuration is displayed.
 - Step 14** Select **Save**.
 - Step 15** Select **Restart** to re-initialize the Eth0 interface and save the configuration.
Note The window may be blank for some time. Wait for some time, as this is a normal behavior.
 - Step 16** Select **OK**. The Main Menu is displayed.
 - Step 17** Select **Log out**.
-

When the initial network configuration has been completed, the next step is to log into the UI and define the network settings.

Configuring the Analytics Forwarder Application Server

To configure the Analytics Forwarder Application Server settings, complete the following steps:

-
- Step 1** Open a browser and enter the following URL:
`http://<ip_address>:8004`
Where the IP address is the address of the Analytics Forwarder.
 - Step 2** Log in using the credentials; User Name: **admin** and the previously changed password. The Configuration Wizard is displayed.

Configuration Wizard

Remaining configuration steps:

- Change Password
- Configure Networking
- Configure Appliance**

Use this page to configure the BNI Video Analytics.

Node Configuration

Node Name:

Node IP:

Management Services Node IP:

Deploy Analytics Application:

Analytics Application Virtual IP:

Deploy Analytics Indexer:

Deploy CDN Analytics Forwarder:

Deploy Analytics Job Scheduler:

Configure

360675

Step 3 The Appliance configuration information is derived from the previous console configuration of this device. Enter the IP address of the Core Services node that is running the Management Services, and check the **Deploy CDN Analytics Forwarder** check box. When finished, click **Configure**. You are prompted with the following popup.



360689

Step 4 Click **Configure**. The configuration may take a few minutes and when finished a screen similar to the following is displayed.

Appliance Logs

- Back Up and Restore
- Change Password
- Collect Diagnostic Information
- Configuration
- Manage Services
- Schedule Reboot
- Updates
- User Management
- View and Apply Rollbacks

Software:

Product:	BNI Video Analytics
Build Time:	11-12-2013 13:03
Build Version:	3.1.0
Build Host:	null
Build Number:	181

Core Components (Beaumaris Core Components):

Version:	3.1.0
Build Host:	null
Build Number:	45

Platforms:

appliance-config:	0.1-1-2
analytics:	3.1.0_181-1-1
group-analytics-appliance:	3.1.0-2-20
jobsdb:	18A
spunk:	5.0.4_172409_28-1-1
spunk-forwarder:	5.0.4_172409_28-1-1

Appliance Status

Updates

Last Update:	No update has been completed
Last Check:	No check has been completed
Next Check:	18 Nov 2013 15:17 IST

Back Up and Restore

Status:	Not configured.
---------	-----------------

361733

Installing the VDS-SM Analytics Job Scheduler



Note The procedure that follows assumes that all VDS-SM VMs have been created and deployed. If this has not been completed, make sure that you complete it now. Also, this procedure uses the similar installation and configuration procedure as the Core Services node. Refer to the [Configuring the VDS Core Management Services Node](#) for screens and additional information that are generic to all installation and configuration.

To install the VDS-SM Analytics Job Scheduler, perform the following steps:

-
- Step 1** Using the VMware's vSphere client, access the ESXi host where the OVF VMs are located.
 - Step 2** Right-click the Analytics Job Scheduler VM, select **Power > Power On**.
 - Step 3** When the VM is powered on, right-click the VM again and select **Open Console**. Allow the VM to finish starting the boot procedure.
 - Step 4** When the boot process completes, select **Sign in**.
 - Step 5** Log in using the default credentials; User Name: **admin** and Password: **password**.
 - Step 6** If this is your initial login, the system prompts you to change the password.
 - Step 7** Change the password as Beaumaris1. Click **Change** when finished. The Main Menu is displayed.
 - Step 8** Select **Network Configuration**. The default networking configuration is displayed.
 - Step 9** If the IP addressing is not obtained via DHCP, enter the Default Gateway, choose the Eth0 interface, and press **Enter**.
 - Step 10** Select a unique hostname for the Node. The hostname used must be unique from all other analytics nodes.
 - Step 11** Set the DNS server setting to that of the Core Services node. Press **Enter**.
 - Step 12** Enable Eth0. If configuring static addressing, deselect the DHCP option and specify the IP address and netmask.
 - Step 13** Enter the IP Address and netmask. Select **Save**. The completed network configuration is displayed.
 - Step 14** Select **Save**.
 - Step 15** Select **Restart** to re-initialize the Eth0 interface and save the configuration.
Note The window may be blank for some time. Wait for some time, as this is a normal behavior.
 - Step 16** Select **OK**. The Main Menu is displayed.
 - Step 17** Select **Log out**.
-

When the initial network configuration has been completed, the next step is to log into the UI and define the network settings.

Configuring the Analytics Job Scheduler Application Server

To configure the Analytics Job Scheduler network settings within the UI, complete the following steps:

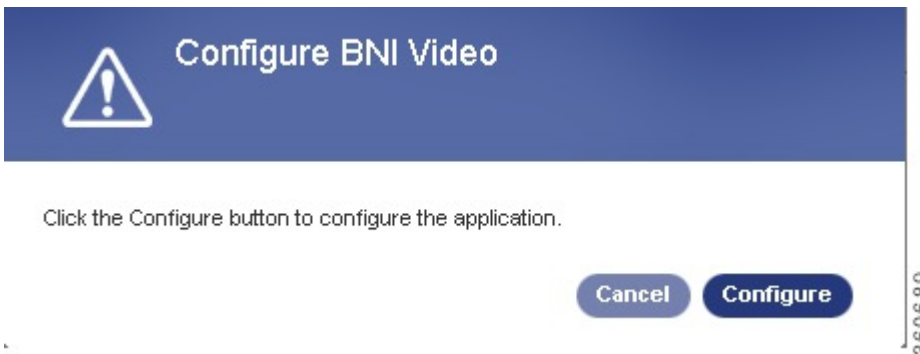
Step 1 Open a browser and enter the following URL:

`http://<ip_address>:8004`

Where the IP address is the address of the Analytics Job Scheduler.

Step 2 Log in using the credentials; User Name: **admin** and the previously changed password. The Configuration Wizard is displayed.

Step 3 The Appliance configuration information is derived from the previous console configuration of this device. Enter the IP address of the Core Services node that is running the Management Services, and check the **Deploy Analytics Job Scheduler** check box. When finished, click **Configure**. You are prompted with the following popup.



Step 4 Click **Configure**. The configuration may take a few minutes and when finished, a screen similar to the following is displayed.

Adding an Analytics Indexer to VDS-SM

To add the Analytics Indexer, complete the following:

- Step 1** On the Job Scheduler node, log in as bnispunk user.
- Step 2** At the prompt, enter the following command:
- ```
cd /opt/splunk/etc/deployment-apps/CDN_JS/bin
```
- Step 3** Add the indexer using the following command:
- ```
/opt/splunk/bin/splunk cmd python configure_indexers.py add bniindexer1
```
- Where the bniindexer is the name of the indexer being added.
- Note** If you want to add more than one Indexers, leave a space after the first Indexer name.

Deploying CDS System Delivery Server/Services in Analytics Node

To deploy CDS Delivery Server/Services in an analytics node, complete the following:

- Step 1** On the Job Scheduler node, log in as bnispunk user.
- Step 2** At the prompt, enter the following command:
- ```
crontab -e
```
- Step 3** Add the following string to #b:
- ```
*/5 * * * * /opt/splunk/bin/splunk cmd python /opt/splunk/etc/apps/CDN_JS/bin/getCDSTopology.py
```

Data Retention Policy

To purge older data, set the retention period. To set the data retention policy, complete the following:

On Job Scheduler, edit `/opt/splunk/etc/deployment-apps/CDN_IDX/local/indexes.conf`

The indexes without the attribute " frozenTimePeriodInSecs" will take up a default value of 6 years as the retention policy.

For 955_Billing, the index retention period is set to 10 years by default.

Upgrade Procedure from 3.0 to 3.1

The upgrade from 3.0 to 3.1 requires the following necessary actions:

- Taking a backup of existing installations.
- Upgrading the VDS-SM nodes in the following order.
 - a) Indexer
 - b) Search Head
 - c) Forwarder
 - d) Job Scheduler
 - e) Management Services
 - f) CDN Manager
 - g) UI

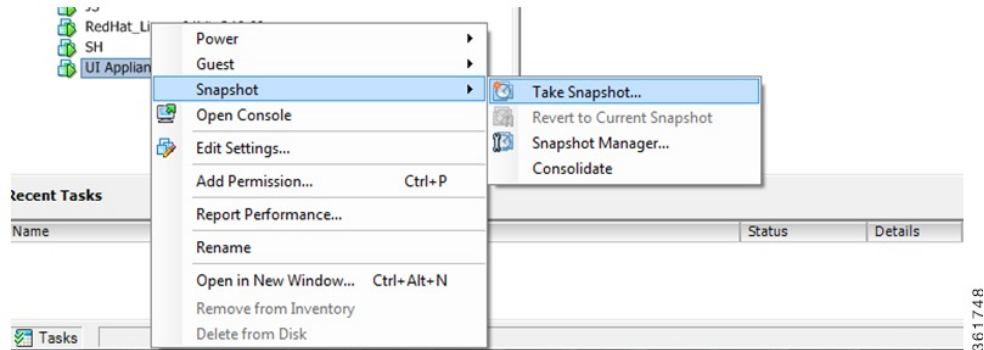
Backup Existing Installations

The existing VDS-SM installation should be backed up to protect your data, in case of any failure at any stage of the upgrade process. To back up, take a snapshot of the VM of all the nodes using your ESX server management client.

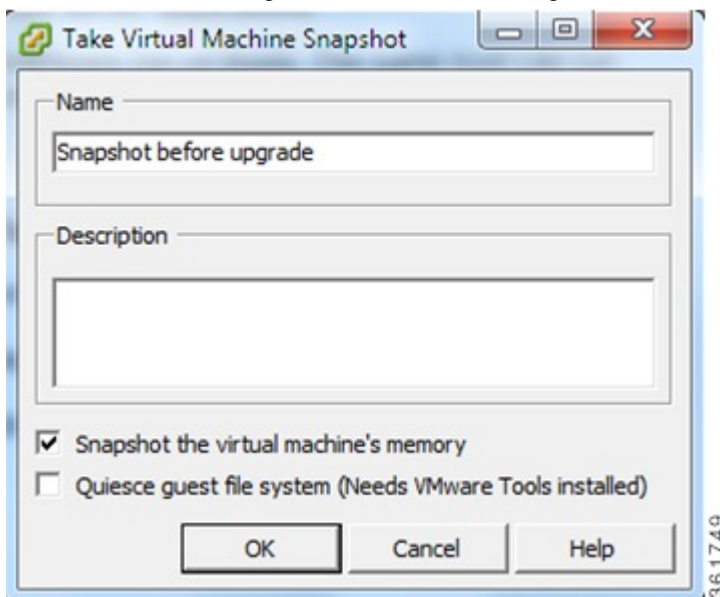
Taking a Snapshot

Using the VMWareVSpere Client, you can take a snapshot of VM node. The following are the steps to take the snapshot:

Step 1 Right-click on the node and choose **Snapshot > Take Snapshot**.



Step 2 Enter a name for the snapshot and click **OK**. A snapshot will be created for that node.



Upgrading VDS-SM Nodes

Splunk should be upgraded in the VDS-SM analytics nodes in the following order:

- 1 Indexer Node
- 2 Search Head Node
- 3 Forwarder Node
- 4 Job Scheduler Node

Before you Begin

Before upgrading, make sure that you take a snapshot of all the nodes.

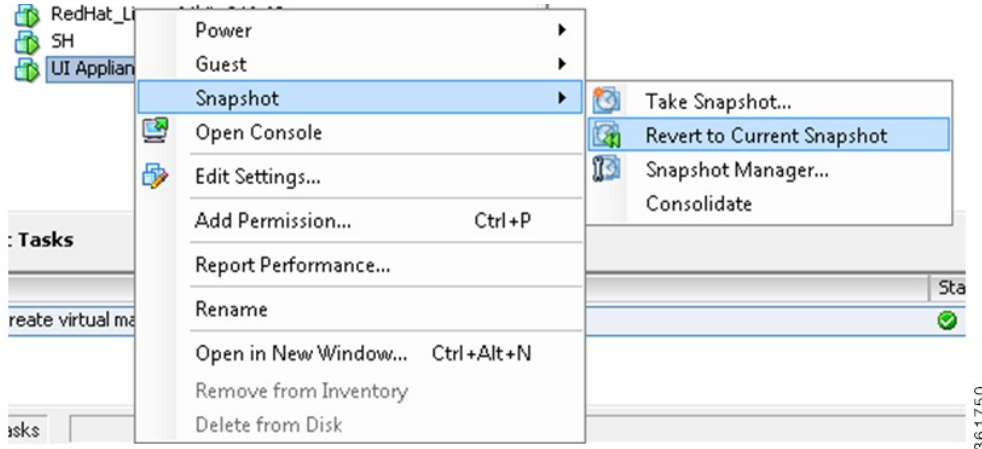


Note Upgrade log file is created in the following location:
/home/bninet/bni/upgrade/log directory.

Upgrade Failure

If the upgrade process fails on a node, apply snapshot and restore the node. To restore the snapshot using the VMWareVSphere Client, perform the following steps:

Step 1 Open VMWareVSphere Client and right-click on the node.



Step 2 Choose **Snapshot > Revert to Current Snapshot** to apply the latest snapshot on the node.

Indexer

To upgrade the Indexer node, perform the following steps:



Note

To prevent data loss, the forwarder node should be stopped before upgrading indexer and then started again as soon as the indexer node is upgraded. Also, in case of multiple indexers, repeat the following steps in all of the indexers.

Step 1 Login to the forwarder node as user **bnisplunk** with password as **password**.

Step 2 Stop the splunk process using the command:

```
$ splunk stop
```

Step 3 Login to the Indexer node as user **bninet** with password as **password**.

Step 4 Copy the file **bni-analytics-3.1.0-analytics-upgrade.tar.gz** into the `/home/bninet/bni/` directory.

Step 5 Extract the file using the command:

```
$ tar -zxvf bni-analytics-3.1.0-analytics-upgrade.tar.gz
```

Step 6 This creates a directory named **upgrade** under `/home/bninet/bni/`

Step 7 Go to `/home/bninet/bni/upgrade/bin` using the command:

```
$ cd /home/bninet/bni/upgrade/bin
```

Step 8 Run the following command to upgrade the node:


```
$ sudo sh upgradeAnalyticsNode.sh
```

The Indexer node has been upgraded successfully to version 3.1.

- Step 9** Go to the forwarder node and start the splunk process using the command:
\$ splunk start
-

Search Head

To upgrade the Search Head node, perform the following steps:

- Step 1** Login to the Search Head node as user **bninet** with password as **password**.
- Step 2** Copy the file **bni-analytics-3.1.0-analytics-upgrade.tar.gz** into the */home/bninet/bni* directory.
- Step 3** Extract the file using the command:
\$ tar -zxvf bni-analytics-3.1.0-analytics-upgrade.tar.gz
- Step 4** This creates a directory named **upgrade** under */home/bninet/bni*.
- Step 5** Go to */home/bninet/bni/upgrade/bin* using the command:
\$ cd /home/bninet/bni/upgrade/bin
- Step 6** Run the following command to upgrade the node:
\$ sudo sh upgradeAnalyticsNode.sh
- The Search Head node has been upgraded successfully to version 3.1.
-

Forwarder

To upgrade the Forwarder node, perform the following steps:

- Step 1** Login to the Forwarder node as user **bninet** with password as **password**.
- Step 2** Copy the file **bni-analytics-3.1.0-analytics-upgrade.tar.gz** into the */home/bninet/bni* directory.
- Step 3** Extract the file using the command:
\$ tar -zxvf bni-analytics-3.1.0-analytics-upgrade.tar.gz
- Step 4** This creates a directory named **upgrade** under */home/bninet/bni*.
- Step 5** Go to */home/bninet/bni/upgrade/bin* using the command:
\$ cd /home/bninet/bni/upgrade/bin
- Step 6** Run the following command to upgrade the node:
\$ sudo sh upgradeAnalyticsNode.sh
- The Forwarder node has been upgraded successfully to version 3.1.
-

Job Scheduler

To upgrade the Job Scheduler node, perform the following steps:

-
- Step 1** Login to the Job Scheduler node as user **bninet** with password as **password**.
- Step 2** Copy the file **bni-analytics-3.1.0-analytics-upgrade.tar.gz** into the */home/bninet/bni* directory.
- Step 3** Extract the file using the command:
\$ tar -zxvf bni-analytics-3.1.0-analytics-upgrade.tar.gz
- Step 4** This creates a directory named **upgrade** under */home/bninet/bni*.
- Step 5** Go to */home/bninet/bni/upgrade/bin* using the command:
\$ cd /home/bninet/bni/upgrade/bin
- Step 6** Run the following command to upgrade the node:
\$ sudo sh upgradeAnalyticsNode.sh
- The Job Scheduler node has been upgraded successfully to version 3.1.
-

Management Services

To upgrade the Management Services node, perform the following steps:

-
- Step 1** Login to the Management Services node as user **bninet** with password as **password**.
- Step 2** Copy the file **mgmt-svcs-3.1.0-upgrade.tar.gz** into the */home/bninet/bni* directory.
- Step 3** Extract the file using the command:
\$ tar -zxvf mgmt-svcs-3.1.0-upgrade.tar.gz
- Step 4** This creates a directory named **upgrade** under */home/bninet/bni*.
- Step 5** Go to */home/bninet/bni/upgrade/bin* using the command:
\$ cd /home/bninet/bni/upgrade/bin
- Step 6** Run the following command to upgrade the node:
\$ sudo sh upgradeMgmtSvcNode.sh
- The Management Services node has been upgraded successfully to version 3.1.
-

CDN Manager

To upgrade the CDN Manager node, perform the following steps:

-
- Step 1** Login to the CDN Manager node as user **bninet** with password as **password**.
- Step 2** Copy the file **cdn-mgr-3.1.0-upgrade.tar.gz** into the */home/bninet/bni* directory.
- Step 3** Extract the file using the command:
\$ tar -zxvf cdn-mgr-3.1.0-upgrade.tar.gz
- Step 4** This creates a directory named **upgrade** under */home/bninet/bni*.
- Step 5** Go to */home/bninet/bni/upgrade/bin* using the command:
\$ cd /home/bninet/bni/upgrade/bin
- Step 6** Run the following command to upgrade the node:
\$ sudo sh upgradeCdnMgrNode.sh
- The CDN Manager node has been upgraded successfully to version 3.1.
-

UI Node

To upgrade the UI node, perform the following steps:

-
- Step 1** Login to the UI node as user **bninet** with password as **password**.
- Step 2** Copy the file **ui-3.1.0-upgrade.tar.gz** into the */home/bninet/bni* directory.
- Step 3** Extract the file using the command:
\$ tar -zxvf ui-3.1.0-upgrade.tar.gz
- Step 4** This creates a directory named **upgrade** under */home/bninet/bni*.
- Step 5** Go to */home/bninet/bni/upgrade/bin* using the command:
\$ cd /home/bninet/bni/upgrade/bin
- Step 6** Run the following command to upgrade the node:
\$ sudo sh upgradeUINode.sh
- The UI node has been upgraded successfully to version 3.1.
- A manifest file listing all the files that has been added, removed or modified as part of the upgrade will be created at */home/bninet/bni/upgrade/log* in each of the following nodes once the upgrade has been successfully completed on that node.
- 1 Job Scheduler
 - 2 Management Services
 - 3 CDN Manager
 - 4 UI
-

Procedure to Resize Hard Disk

The nodes are shipped with the following default size:

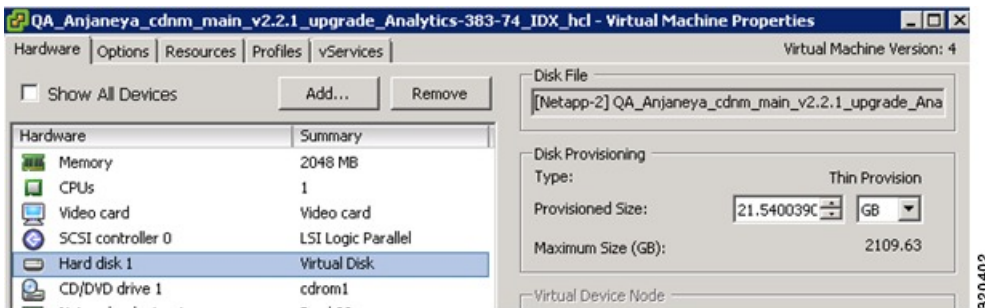
Node	Default Hard Disk Size
Core Service node	27 GB
User Interface node	21 GB
CDN Manager node	21 GB
Each Analytics node	21 GB



Note Most of the time, you need to resize only the Indexer and the Forwarder.

To increase the hard disk space of any node, you need to perform the following steps:

- Step 1** From the VMware vSphere Client, login to the ESX Server.
- Step 2** Select the node to which you want to increase the hard disk size and power-off the node.
- Step 3** Once the node is powered-off, right-click the node, navigate to Edit Settings, and choose Hard disk 1.



- Step 4** Increase the size of the node, as required, and power-on the node.
- Step 5** Once the node is powered-on, ssh as 'root' to the respective server. For example, Job Scheduler Hard Disk size is increased from 21 GB to 100 GB

```
[root@JS ~]# df -hl
```

```
Filesystem Size Used Avail Use% Mounted on
/dev/sda1 22G 5.9G 15G 29% /
tmpfs 1006M 0 1006M 0% /dev/shm
```

```
[root@JS ~]# sudo fdisk /dev/sda
```

The number of cylinders for this disk is set to 102400. However, this could cause the following problems in certain setups as this is larger than 1024:

- 1) Software which runs at boot time (for example, old versions of LILO)
- 2) Booting and partitioning software from other OSs (for example, DOS FDISK, OS/2 FDISK)

Enter expert mode, print the partition table, and make sure that there is only a single partition starting at cylinder 1 (the lines with all zeroes represent unused primary partitions. Therefore, these can be ignored.

Command (m for help): x

Expert command (m for help): p

Disk /dev/sda: 64 heads, 32 sectors, 102400 cylinders

Nr AF Hd Sec Cyl Hd Sec Cyl Start Size ID

1 80 4 1 0 63 32 1023 128 45170560 83

2 00 0 0 0 0 0 0 0 0 0

3 00 0 0 0 0 0 0 0 0 0

4 00 0 0 0 0 0 0 0 0 0

Note Make a note of the Start Value for the partition, as you will need this later.

Return to the main menu from the expert mode.

Expert Command (m for help): r

Delete the partition

Command (m for help): d

Selected partition 1

Add a new partition, starting at the same cylinder as the one just deleted, and using the entire

Command (m for help): n

Command action

e extended

p primary partition (1-4)

p

Partition number (1-4): 1

First cylinder (1-102400, default 1): 1

Last cylinder or +size or +sizeM or +sizeK (1-102400, default 102400): 102400

Enter expert mode, and change the start of the partition Command (m for help): x

Expert command (m for help): b

Partition number (1-4): 1

New beginning of data (32-209715199, default 32): 128

This step is necessary because rBuilder-generated disk images always align the first partition to a cylinder boundary for performance reasons.

Return to the main menu from expert mode

Expert command (m for help): r

Make the partition bootable

Command (m for help): a

Partition number (1-4): 1

Write the partition table and exit

Command (m for help): w

The partition table has been altered!

Calling ioctl() to re-read partition table.

WARNING: Re-reading the partition table failed with error 16: Device or resource busy. The kernel still uses the old table.

The new table will be used at the next reboot.

Syncing disks.

[root@JS ~]# sudo reboot

Broadcast message from root (pts/0) (Fri Feb 1 12:39:37 2013):

The system is going down for reboot NOW!

login, and run: `resize2fs <devicename>` (where devicename is the partition, e.g., `/dev/sda1`)

[root@JS ~]# sudo /sbin/resize2fs /dev/sda1

resize2fs 1.39 (29-May-2006)

Filesystem at `/dev/sda1` is mounted on `/`; on-line resizing required

Performing an on-line resize of `/dev/sda1` to 26214384 (4k) blocks.

The filesystem on `/dev/sda1` is now 26214384 blocks long.

[root@JS ~]# df -h

Filesystem Size Used Avail Use% Mounted on

`/dev/sda1` 100G 5.9G 89G 7% /

`tmpfs` 1006M 0 1006M 0% `/dev/shm`

Installing Software

To install the required software, refer to the Getting Started section in the Videoscape Distribution Suite Service Manager User Guide.

Configuring VDS-IS Transaction Log Settings

To configure the VDS-IS transaction log settings, first configure the SE log and then the SR log.

To configure the SE/SR logs, complete the following:

- 1 Log into CDSM and then navigate to **Device > Select a SE and Edit > Service Control > Transaction Logging**.
 - a Within the General Settings, complete the following:
 - Enable **Transaction Log Enable**.
 - Enable **Snapshot Counter Log Enable**.
 - **Compress Files before Export** must be unchecked.
 - Select **custom format for CDNM**, which enables `webengine_clf` to use the CDNM customized format.
 - b Within the Archive Settings, configure the **Archive occurs:** interval to 300 seconds.
 - c Within the Windows Media Settings and Web Engine Settings, configure the following:
 - Enable **ABR Session Log**.
 - Enable **Enable Windows Media Settings**.
 - Select **extended wms-90** from within the Log File Format.
 - d Within the Splunk UF Export Settings, configure the following:
 - Enable **Export Enable** and select the log types to export.
 - Enter **Analytics Forwarder node IP address** as the export server or enter Port as 9998.
- 2 To configure the SR Log, log into CDSM and then navigate to **Device > Select a SR and Edit > General Settings > Notification and Tracking > Transaction Logging**. Configure the SR Log configuration using the steps a to d, as shown in Step 1.

Procedure to Restart the Nodes

If the VMs where the application is deployed stops unexpectedly, the nodes should be re-started in the following order:

- 1 Core Services node
- 2 UI node
- 3 CDN Manager node
- 4 Analytics nodes (you can follow any order in starting the Analytics nodes)

**Note**

After the node has completely started (wait for the sign in page to appear in the Console tab), ensure that at least five minutes is provided for each node to sync.

For manual restart, perform the following:

- First stop UI, then CDN Manager, and finally the Core Services node.

- After this, perform the above mentioned procedure in the same order.
- If only UI or CDN Manager node stops in between, stop the node that is up (UI or CDN Manager, whichever is up), and then stop the Core Services node. Restart Core Services first, and then UI and CDN Manager nodes respectively.
- If any of the Analytics node stops in between, then that particular node alone should be started.

If all the Analytics nodes are restarted, then you need to validate whether or not the indexer is configured properly, using the following procedure:

Step 1 On the Job Scheduler node, log in as bnispunk user.

Step 2 At the prompt, enter the following command:
cd /opt/splunk/etc/deployment-apps/CDN_JS/bin

Step 3 Verify the Indexer using the following command and ensure that the indexers are configured as shown in the following example:
/opt/splunk/bin/splunk cmd python configure_indexers.py list

Example

Search peers for host: 10.77.246.193 (analyticsJS)

Server at URI "bniindexer1:8089" with status as "Up" and peerType "configured"

Search peers for host: 10.77.246.194 (bnianalytics.bnivideo.com)

Server at URI "bniindexer1:8089" with status as "Up" and peerType "configured"

Shutting Down the VMs

For smooth shutting down of the VMs, follow the order mentioned here:

- 1 Forwarder
- 2 Indexer
- 3 Search Head
- 4 Job Scheduler
- 5 CDN Manager
- 6 UI
- 7 Core Services

Browsers Supported

VDS-SM 3.1 supports the following browsers:

- Mozilla Firefox versions 12 to 20

- Internet Explorer versions 8 and 9

VDS-SM 3.1 supports VDS-IS 3.1, 3.2, 3.2.1, and 3.3.



VDS-SM Port Utilization Details

- [VDS-SM Port Utilization, page 67](#)

VDS-SM Port Utilization

The ports used by each node are mentioned below.

Sl. No.	Node	Services	Port Number
1	Core	Jboss	22, 80 and 8080
2	CDN Manager	Jboss	22, 80 and 8080
3	User Interface	Jboss	22, 80 and 8080
4	Search Head	Splunk	22, 8000 and 8089
5	Job Scheduler	Splunk	22, 8000 and 8089
6	Indexer	Splunk	22, 8000 and 8089
7	Forwarder	Splunk	22, 8000 and 8089
8	Forwarder	LWF log receiving port	9998

The other required ports are mentioned below:

SSH - 22

http - 80

Jboss - 8080

Splunk - 8000 and 8089

RAPA GUI - 8004

https (used in NB API) - 8443

