EMC CLOUD TIERING APPLIANCE/VE

Trial Version Installation Instructions

File Tiering from VNX/Celerra to Atmos

Publication Date: September, 2011

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

For the most up-to-date regulatory document for your product line, go to the Technical Documentation and Advisories section on EMC Powerlink.

Contents

Installing Cloud Tiering Appliance/VE

The CTA/VE is installed on the VMware server. The table below shows the interoperability.

VMware ESX Server interoperability

Virtual Appliance	VMware ESX Server	Comments
CTA/VE	ESX 3.5 Update 3 ESXi 3.5 Update 3 ESX 4.0 ESXi 4.0 ESX 4.1 ESXi 4.1	Four virtual CPUs, 4 GB of RAM, 512 GB of disk space, 2 gigabit virtual interfaces are reserved.

This example shows the steps to install the CTA/VE on an ESX 3.5 Server host:

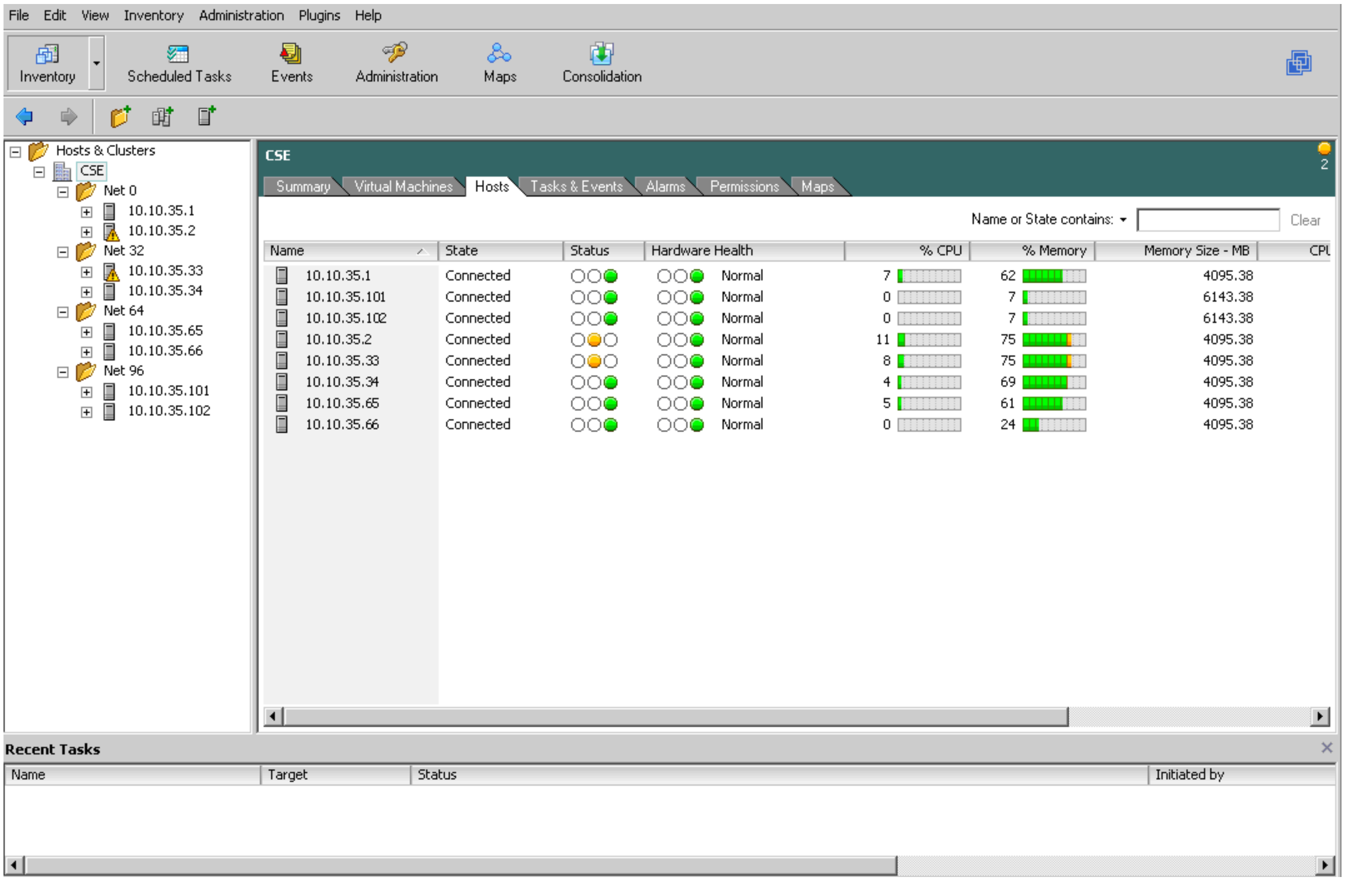
1. Unzip the ZIP file to create the directory for your virtual appliance. The ZIP file contains the .OVF file and .VMDK file.
   - For a CTA/VE, the zip file is: fmve-<*version*>.zip
2. Open the Virtual Infrastructure (VI) Client.

   Review the ESX Server's resource usage. To install CTA/VE Trial Version, the ESX server must have a minimum of:

   - One 64-bit Virtual CPUs (vCPU)
   - 1 GB memory
   - 20GB of disk space for CTA/VE

Note: System requirements are greater for the CTA/VE production version.

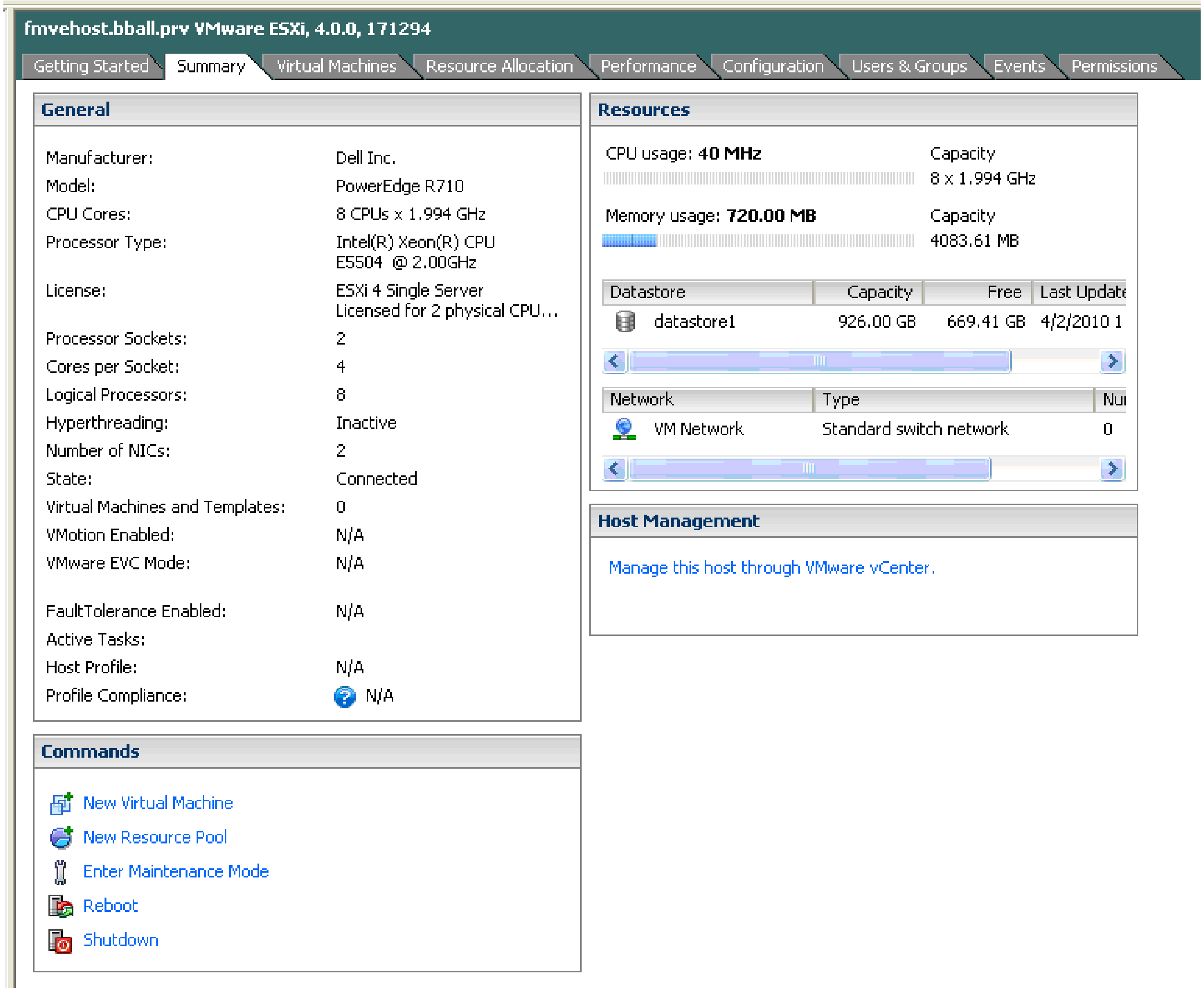
To find the appliance with the most free space, consider %CPU and %Memory.



Name	State	Status	Hardware Health	% CPU	% Memory	Memory Size - MB	CPU
10.10.35.1	Connected	○○●	○○● Normal	7	62	4095.38	
10.10.35.101	Connected	○○●	○○● Normal	0	7	6143.38	
10.10.35.102	Connected	○○●	○○● Normal	0	7	6143.38	
10.10.35.2	Connected	○●○	○○● Normal	11	75	4095.38	
10.10.35.33	Connected	○●○	○○● Normal	8	75	4095.38	
10.10.35.34	Connected	○○●	○○● Normal	4	69	4095.38	
10.10.35.65	Connected	○○●	○○● Normal	5	61	4095.38	
10.10.35.66	Connected	○○●	○○● Normal	0	24	4095.38	

Virtual Infrastructure Client

Select the line with the ESX server for the installation. A summary of the CPU, Memory, and Datastore capacities appears.



fmvehost.bball.prv VMware ESXi, 4.0.0, 171294

General

Manufacturer:	Dell Inc.
Model:	PowerEdge R710
CPU Cores:	8 CPUs x 1.994 GHz
Processor Type:	Intel(R) Xeon(R) CPU E5504 @ 2.00GHz
License:	ESXi 4 Single Server Licensed for 2 physical CPU...
Processor Sockets:	2
Cores per Socket:	4
Logical Processors:	8
Hyperthreading:	Inactive
Number of NICs:	2
State:	Connected
Virtual Machines and Templates:	0
VMotion Enabled:	N/A
VMware EVC Mode:	N/A
FaultTolerance Enabled:	N/A
Active Tasks:	
Host Profile:	N/A
Profile Compliance:	N/A

Resources

CPU usage: **40 MHz** Capacity 8 x 1.994 GHz

Memory usage: **720.00 MB** Capacity 4083.61 MB

Datastore	Capacity	Free	Last Update
datastore1	926.00 GB	669.41 GB	4/2/2010 1

Network	Type	Nu
VM Network	Standard switch network	0

Host Management

Manage this host through VMware vCenter.

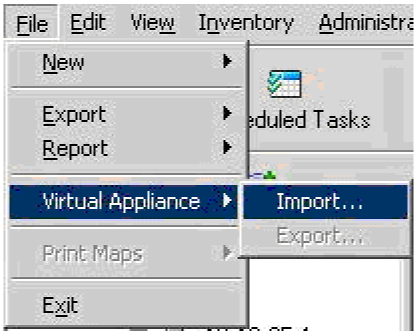
Commands

Example client

This ESX server has enough CPU and Memory available to install CTA/VE.

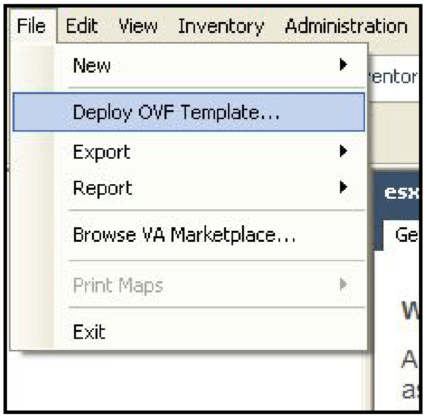
1. Import the OVF file. Instructions differ depending upon VMware version.

   - For ESXi 3.5, from the VI Client, select **File›Virtual Appliance›Import**.



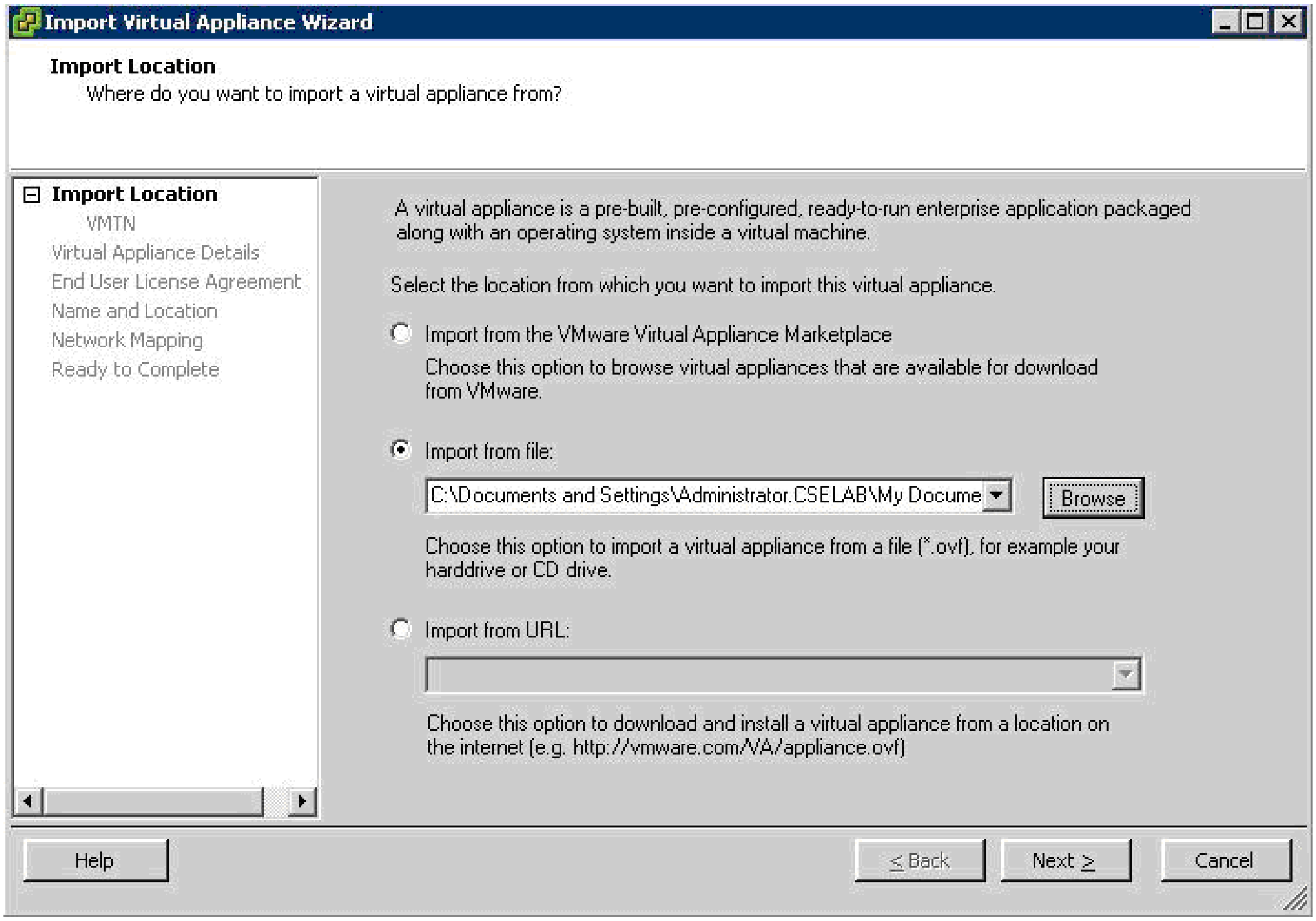
Virtual Appliance Import

- For ESX 4.0, from the VI Client, select **File › Deploy OVF Template**.



Deploy OVF Template

- Using the **Import from file** selection, type the path to the OVF file or click **Browse** to locate the file.



Import Virtual Appliance Wizard

Import Location

Where do you want to import a virtual appliance from?

A virtual appliance is a pre-built, pre-configured, ready-to-run enterprise application packaged along with an operating system inside a virtual machine.

Select the location from which you want to import this virtual appliance.

○ Import from the VMware Virtual Appliance Marketplace

Choose this option to browse virtual appliances that are available for download from VMware.

● Import from file:

C:\Documents and Settings\Administrator.CSELAB\My Docume

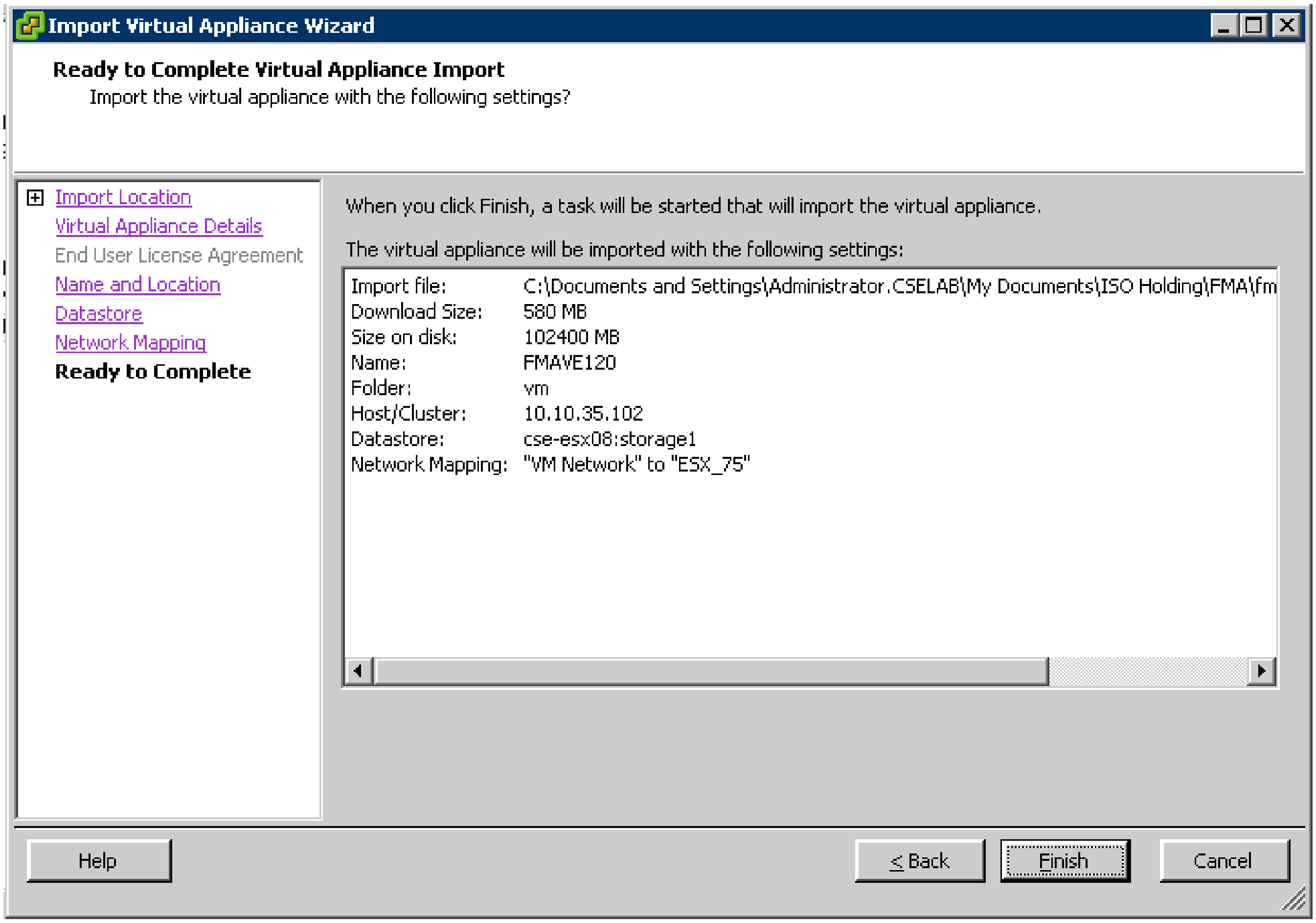
Choose this option to import a virtual appliance from a file (*.ovf), for example your harddrive or CD drive.

○ Import from URL:

Choose this option to download and install a virtual appliance from a location on the internet (e.g. http://vmware.com/VA/appliance.ovf)

Import Wizard

2. After answering a few basic questions, the summary screen appears. Validate the information and click **Finish**.



Ready to Complete Virtual Appliance Import

Import the virtual appliance with the following settings?

When you click Finish, a task will be started that will import the virtual appliance.

The virtual appliance will be imported with the following settings:

```
Import file:       C:\Documents and Settings\Administrator.CSELAB\My Documents\ISO Holding\FMA\fm
Download Size:     580 MB
Size on disk:      102400 MB
Name:              FMAVE120
Folder:            vm
Host/Cluster:      10.10.35.102
Datastore:         cse-esx08:storage1
Network Mapping:   "VM Network" to "ESX_75"
```

Import Wizard Finish

The import may take up to 30 minutes depending on the network connection between the VI Client and the VMware ESX Server. Approximately 600 MB will initially be transferred across the network.

Note: If the CTA/VE will be configured for archiving from Celerra or VNX to EMC Centera or from Celerra or VNX to Atmos archiving, use the FileMover Settings as described on the Celerra Properties configuration page to configure the single set of credentials for recall. Then run **ccdsetup** or **acdsetup**.

Configuring CTA/VE

Before proceeding with the setup, ensure that you have the following information for the appliance.

- IP address
- Subnet mask
- Hostname
- Default gateway IP

- DNS server IP (optional)

To set up CTA/VE:

1. Power on the virtual machine.
2. Log in to the appliance. Type **root** as the login name. Type **rain** as the password.

   The File Management setup tool appears. This tool performs basic setup tasks that are not available through the Cloud Tiering Appliance GUI.
3. Select **Change File Management Appliance Password**, and change the password.
4. Select **Configure Date and Time** to set the time zone and date for the appliance.
5. Select **Configure File Management Networking.** The network configuration menu appears. Use the menu to change interface settings or set global settings such as hostname, DNS and domain servers.

Configuring the CTA network

To configure networking:

1. Select option 1 from the network configuration menu. The File Management Network Setup, Main Menu appears.
   - On the list of available physical interfaces on the appliance, eth0 will be highlighted. To highlight a different interface, use the up arrow and down arrow keys.
2. With eth0 highlighted, press **Enter**. The configuration menu for the eth0 interface appears:
   - Use the up arrow and down arrow keys to highlight the IP Address field. Press **Enter** and type a new IP Address value into the **New Value** column. Press **Enter.**
   - Repeat the process to provide the Network Mask, Gateway, MTU settings.
3. When the configuration for this interface is complete, press the left arrow to exit the eth0 interface configuration. To save the interface configuration, highlight **Yes** and press **Enter.** Note that the changes are saved, but will not be committed until the File Management Network Setup menu is exited.
4. Press the left arrow to exit from the File Management Network Setup menu. When prompted, select **Yes** to commit your changes.

Configuring the hostname, domain, and DNS server

Configure the hostname, domain, and DNS servers:

1. Select option 2 from the network configuration menu. The following menu appears:

```
EMC Rainfinity Setup Tool (Configure Hostname, Domain and DNS
Server(s))
Hostname           = rs
Domain             =
DNS Server         =

Do you want to change the configuration [N]?
```

2. Select **Y**. Use the menu to configure the hostname, domain, and DNS servers.
3. The new hostname, domain, and DNS server information will be summarized after all the changes are entered, and you will be given the ability to accept or make further changes to these settings. To keep the new settings and return to the network configuration menu, press **Enter**.
4. Verify that the network configuration has been committed and network connectivity can be established properly.

Deploying CTA/VE with Celerra or VNX

To use the CTA/VE with a Celerra or VNX Data Mover, first perform configuration steps on the CTA/VE, and then on the Celerra or VNX Control Station.

Note: Celerra supports DART versions 6.0 or earlier. VNX supports DART versions 7.0 or later.

Prerequisites for using Celerra or VNX as source storage

To archive any data from a Celerra or VNX Data Mover, the CTA/VE requires access to the FileMover API (TCP port 5080).

To archive NFS data, the CTA/VE will require the following:

- Mount v3 RPC service
- NFS v3 RPC service
- NLM v4 RPC service
- Root access with read/write export permissions for all NFS data that will be archived.

To archive CIFS data, the CTA/VE needs SMB over NetBIOS (TCP port 139).

Direct command line access to the Celerra or VNX Control Station is not used by the CTA/VE.

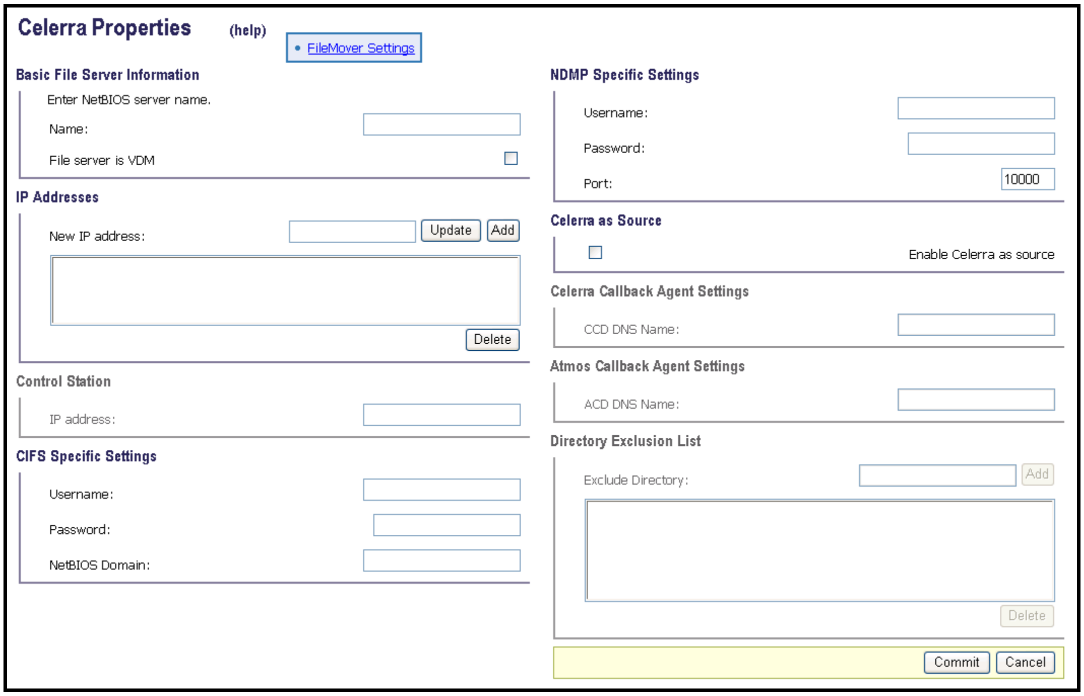
When configuring Celerra or VNX Data Mover properties on the CTA/VE, plan to provide:

- Credentials for a FileMover API user. This single set of credentials is used for both archive and recall.
- (For CIFS archiving only) The NetBIOS name of the filer.
- (For CIFS archiving only) Credentials for local administrator access through CIFS.

Adding a Celerra or VNX to the CTA configuration

Note: The VNX Properties page is not displayed. The configuration process is the same as for the Celerra. To add a VNX, follow the instructions for Celerra, substituting VNX for Celerra throughout.

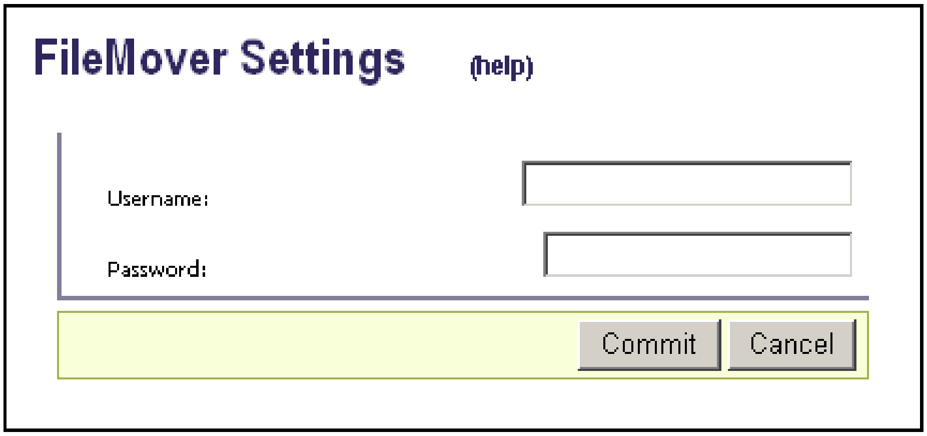
1. Click the **File Servers** link on the **Configuration** tab. The **File Server List** appears. Click **New.**
2. On the **File Server Properties** page that appears, select **Celerra** from the **Type** list box.



Celerra Properties

3. Click **FileMover Settings.**

   The **FileMover Settings** page appears.



FileMover Settings

Type the username and password for FileMover API authentication and callback HTTP authentication. The system uses this username and password to create an HTTP connection by using XML API.

This same username and password are used when creating the FileMover API user on the Control Station.

4. Specify the following for the Celerra Data Mover:

- Basic File Server Information — Type the Celerra name. If the Data Mover will be involved in CIFS archiving, the NetBIOS name of the CIFS server must be used. Do not use the fully qualified domain name (FQDN) or IP address.

Note: To identify the Celerra as a Virtual Data Mover, select the checkbox. Virtual Data Movers support only the CIFS protocol.

- IP Addresses — Type the Celerra Data Mover IP address:
  - When editing an existing server, click **Update** to retrieve the IP address from the DNS that is based on the server name.
  - To specify an additional IP address, click **Add**.
  - To delete an existing IP address, select an IP and click **Delete**.
- Control Station — Type the IP address of the Celerra Control Station. This is required for all source Celerra servers. It is not required for destination Celerra servers. In file migration transactions, it is used to create a snapshot of the source. It also allows the CTA to automatically perform some prerequisite tasks for archiving. If this field is empty, the CTA takes no action and the prerequisite tasks must be performed manually.
  - CIFS Specific Settings — This is the Windows domain user to be used by the appliance. The domain user must be a member of the local administrator's group on the Celerra.

Note: The CIFS credential is not required if the Celerra performs only NFS archiving.

  - NDMP Specific Settings — For file migration, type the username and password for an NDMP user on the source and destination servers. By default, the port for NDMP traffic is 10000.

To create an NDMP user on a Celerra Data Mover, log in to the Celerra Control Station as root, and type:

```
/nas/sbin/server_user <data_mover> -add -md5 -passwd <user>
```

where data_mover is the name of the source or destination server, and user is the username for login. The command will prompt for a password.

- Celerra as Source — This option configures the CTA to archive data from the Celerra Data Mover. If multiple appliances are connected to the same Celerra Data Mover, only one appliance should be configured with the Celerra as Source. This option is required only if the Celerra is serving as a source for archiving.

CAUTION: **Multiple appliances may be configured to archive data from a single Celerra Data Mover, but only one CTA or CTA/VE should be used to archive data from a single filesystem.**

- Celerra Callback Agent Settings

  This option is required if archiving to an EMC Centera. For the CCD DNS name, type the FQDN of the Celerra Callback DNS entry. Note that the FQDN is case-sensitive.

- Atmos Callback Agent Settings

  This option is required if archiving to an Atmos server. For the ACD DNS name, type the FQDN of the Atmos Callback DNS entry. Note that the FQDN is case-sensitive.

Note: The DNS names for the Celerra Callback agent and Atmos Callback agent must be distinct. They cannot be the same.

- Directory Exclusion List — These are the directories to exclude for all tasks that use scanning. Migration tasks do not scan, so this setting does not apply to file migration. The CTA ignores all system directories such as, etc, lost+found, and ckpt by default.

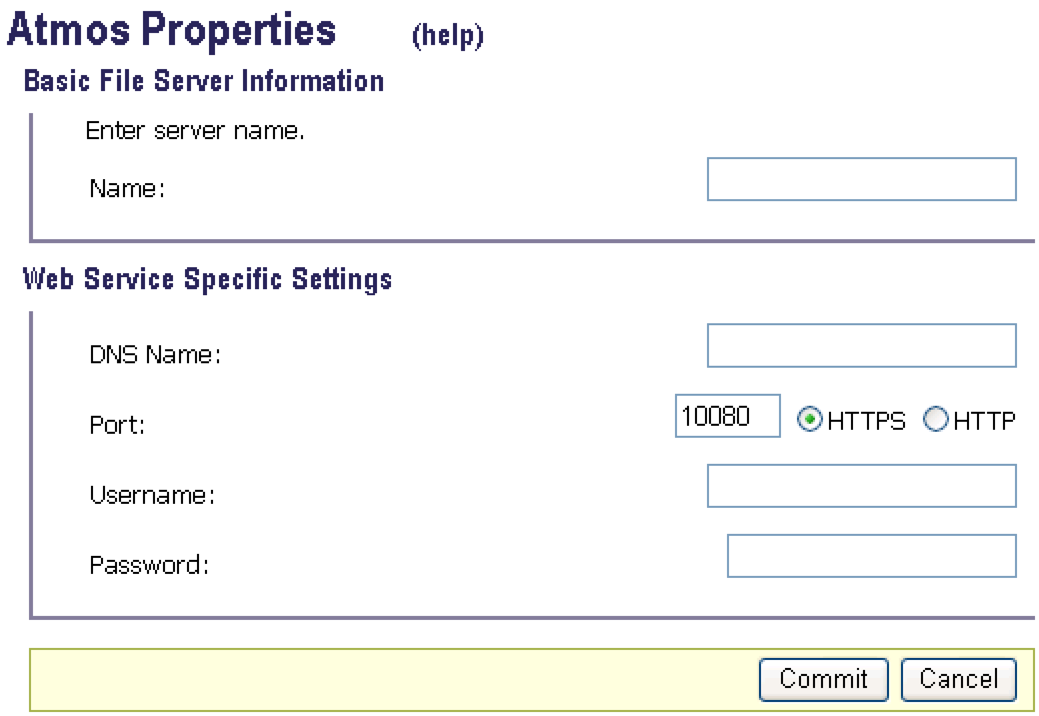
CAUTION: Verify that stub files are not in the excluded directories. CTA will not access the excluded directories and the stub files will become orphans.

5. Click **Commit** to define the Celerra file server.

Using CTA/VE with Atmos

To configure the CTA/VE for an Atmos:

1. Click the **File Servers** link on the **Configuration** tab. The File Server List appears.
2. Click **New**. The File Server Properties page appears.
3. Select **Atmos** from the **Type** list box. The Atmos Properties page appears.



Atmos Properties (help)

Basic File Server Information

Enter server name.

Name:

Web Service Specific Settings

DNS Name:

Port: 10080 ● HTTPS ○ HTTP

Username:

Password:

Atmos Properties

4. Specify the following for Atmos:

   - Name — Type the logical name to identify Atmos.
   - DNS Name — Specify the name used to resolve the IP addresses in the Atmos cluster.
   - Port — The GUI access method. HTTPS is the default and is typically used when Atmos is deployed remotely.

     Select HTTPS or HTTP to specify the communication protocol. The default port for HTTPS (10080) or HTTP (80) automatically appears. If your Atmos connects to HTTPS or HTTP through a different port, type the number.
   - Username — Type the UID or Subtenant on the Atmos. FMA uses this UID to access storage on the cluster. If there is a subtenant, specify the username as: <*Subtenant_ID*>/<*UID*>, where *Subtenant_ID* is an alphanumeric string generated by the Atmos.

Note: The UID is not the Tenant Name, the Subtenant Name, or the Subtenant ID.

   - Password — Type the Shared Secret associated with the UID on the Subtenant Information page of the Atmos.

5. Click **Commit** to define Atmos.

Windows domain user

When a new file server is added to the CTA/VE configuration, CIFS specific settings include the username and password for the Windows domain user to be used by the CTA/VE. Before adding a new CIFS file server, you must set up the Windows domain user.

In addition, when using CTA/VE in a Windows 2008 domain, the domain controller Group Policy Object (GPO) must be configured to support NTLM versions 1 and 2 for CIFS authentication. Configuring Windows 2008 for NTLM provides information on how to modify the domain controller configuration.

Creating a Windows domain user

To create an administrator in the Windows 2000, 2003, or 2008 domain:

1. Log in to the primary domain controller as the **Domain Administrator**.
2. From the **Start** menu, select **Start › Programs › Administrative Tools › Active Directory Users and Computers**.
3. Right-click **Users**.
4. Select **New › User**. The **New Object — User** dialog box appears:
   - In the **Full name** box, type **CTA Administrator**.
   - In the **Login name** box, type **CTAdmin**.

     CTAdmin is the CTA Administrator Windows Domain user.
     - Type a password.

     This password is the CTAdmin Windows password.
     - (Optional) select **Password Never Expires**.
5. Click **Finish**.

Adding an admin user to the local administrator group

The CTAdmin account must be added to the administrators group on the CIFS file servers that will be involved in CTA/VE archiving. To add a CTA/VE Windows domain user on a NetApp filer:

1. Log in to the primary domain controller as the **Domain Administrator**.
2. From the **Start** menu, select **Start › Programs › Administrative Tools › Computer Management**. The **MMC** application appears.
3. To start a Computer Management session with the file server:
   - From the **Action** menu, select **Connect to another computer**. The **Select Computer** dialog box appears.
   - Click **Browse** or type the file server name to select the NetApp to connect to.

- Click **OK.**

4. To include the CTAdmin user in the administrator group for the CIFS File Server:

    - Under **System Tools,** in the folder **Local Users and Groups**, select **Groups.**
    - Select **Administrators.** The **Administrators Properties** dialog box appears.
    - Click **Add.** The **Select Users or Groups** dialog box appears.
        - Click **Locations**. From the **Locations** menu, select the domain instead of the local computer.
        - Under **Enter the object names to select,** type **CTAdmin** to add the domain user.
    - Click **OK.** The **Administrator's Properties** dialog box reappears with the newly added CTAdmin user.
    - Click **OK.**

Repeat this process for any other file servers that will be involved in CTA/VE archiving.

Configuring Windows 2008 for NTLM

By default, the Windows 2008 domain controller supports Kerberos authentication only and disables NTLM authentication. The CTA/VE only supports NTLM versions 1 and 2 authentication for CIFS. Kerberos is not supported. To use CTA/VE in a Windows 2008 domain, confirm that the domain controller is configured for NTLM authentication:

1. Log in to the Windows 2008 domain controller as the **Domain Administrator.**
2. From the **Start** menu, select **Run.** In the **Run** dialogue box that appears, type **gpmc.msc** and click **OK.** The **Group Policy Management** dialog box appears.
3. Expand the domain. Under **Group Policy Objects,** right-click **Default Domain Policy** and select **Edit.** The **Group Policy Management Editor** appears.
4. Under **Computer Configuration,** select **Policies › Window Settings › Security Settings › Local Policies › Security Options.**

    In the list of policies, scroll down to **Network security: LAN Manager Authentication**. Confirm that the policy setting shows that NTLM is configured for authentication.
5. Close the **Group Policy Management Editor.**