## CONTENTS

**Chapter 1**  
**EMC VSI for VMware vSphere: Unified Storage Management Overview**  
Executive summary ........................................................................................................... 6  
Product overview ........................................................................................................... 6  
  Audience ....................................................................................................................... 7  
  Scope ......................................................................................................................... 8  
  Key terms .................................................................................................................... 8  
  Related documents ..................................................................................................... 9  

**Chapter 2**  
**Prerequisites and System Requirements**  
  Downloading EMC VSI for VMware vSphere: Unified Storage Management... 12  
  Setting up the environment ......................................................................................... 12  
  Environment and system requirements ........................................................................ 13  
  Loading EMC VSI for VMware vSphere: Unified Storage Management................. 17  
    Remove quotes from system path ....................................................................... 17  
    DHSM/ASA setup instructions ............................................................................. 18  

**Chapter 3**  
**EMC VSI for VMware vSphere: Unified Storage Management Installation**  
  Installing EMC VSI for VMware vSphere: Unified Storage Management.............. 22  
  Installing the EMC Unified Storage Access Control Utility ..................................... 25  
  Common installation mistakes ..................................................................................... 28  

**Chapter 4**  
**EMC VSI for VMware vSphere: Unified Storage Management – Procedures**  
  Manage access profiles in the EMC Unified Storage Access Control Utility......... 30  
    Add an access profile .......................................................................................... 30  
    Remove an access profile ................................................................................... 35  
    Edit an access profile ......................................................................................... 35  
    Export an access profile ..................................................................................... 35  
  Manage storage systems and connection brokers .................................................. 37  
    Add storage systems or connection brokers ....................................................... 37  
    Import an access profile ..................................................................................... 50  
    Remove storage systems or connection brokers ................................................. 51  
    Edit credentials ................................................................................................. 52  
  Provision storage ..................................................................................................... 53  
    Provision storage for an NFS datastore ............................................................. 53  
    Provision storage on a new NFS export on EMC Celerra, EMC VNX, or EMC VNXe ................................................................. 53  
    Provision storage on an existing NFS export ..................................................... 63  
    Provision storage for a VMFS datastore or RDM volume on EMC CLARiiON, EMC VNX, EMC VNXe, or EMC VMAX............................ 68  
  Extend storage ........................................................................................................ 75  
  Compress a host, cluster, folder, virtual machine, or data center ......................... 76  
    Best practices for compression ....................................................................... 76  
    Known issues for compression ........................................................................ 78  
  Decompress a host, cluster, folder, virtual machine, or data center .................... 79  
    Best practices for decompression .................................................................... 79  
    Known issues for decompression .................................................................... 79
Contents

Cloning virtual machines ........................................................................................................ 79
  Fast Clone ...................................................................................................................... 79
  Full Clone .................................................................................................................... 82
  Integrate Fast Clones with VMware View ................................................................. 85
  Integrate Full Clones with VMware View .................................................................. 88
  Integrate Fast Clones with Citrix XenDesktop ....................................................... 90
  Integrate Full Clones with Citrix XenDesktop ....................................................... 94
  Refresh desktops ........................................................................................................ 98

Chapter 5 Uninstalling EMC VSI for VMware vSphere: Unified Storage Management
  Uninstall .......................................................................................................................... 102
    Uninstall EMC VSI for VMware vSphere: Unified Storage Management feature .............. 102
    Uninstall the EMC Unified Storage Access Control Utility ........................................ 102

Chapter 6 Troubleshooting EMC VSI for VMware vSphere: Unified Storage Management
  Known problems and limitations .................................................................................. 104
  Logs ............................................................................................................................... 111
  Technical notes .............................................................................................................. 111
  EMC Sales and Customer Service contacts ............................................................... 112

Appendix A Parameters within the EMC VSI for VMware vSphere: Unified Storage Management Configuration File
  Configuration file name and location ........................................................................... 114
  Parameters within the configuration file ................................................................... 114
CHAPTER 1
EMC VSI for VMware vSphere: Unified Storage Management Overview

This chapter presents these topics:

◆ Executive summary ................................................................................................... 6
◆ Product overview ...................................................................................................... 6
◆ Key terms .................................................................................................................. 8
◆ Related documents ................................................................................................... 9
Executive summary

EMC® VSI for VMware vSphere® Unified Storage Management is a feature of EMC Virtual Storage Integrator (VSI) for VMware vSphere designed to simplify storage administration of the EMC Celerra® NAS storage platform, the EMC CLARiiON® block storage platform, the EMC VNX® and VNXe® unified storage platforms, and the EMC Symmetrix® VMAX® platforms. The feature enables VMware® administrators to provision new Network File System (NFS) and Virtual Machine File System (VMFS) datastores, and Raw Device Mapping (RDM) volumes, directly from the vSphere Client.

The Unified Storage Management feature is accessed and run from within VSI.

For NFS datastores on NAS storage, users can use the feature to rapidly provision new virtual machines with Full Clones or space-efficient Fast Clones. Users seeking to improve storage utilization can access deduplication features that reduce storage consumption of virtual machines. VMware administrators who manage shared NFS storage should use this feature because it:

◆ Simplifies the process of creating NFS datastores in accordance with best practices
◆ Automatically mounts the NFS datastores to one or more VMware ESX® hosts
◆ Reduces the amount of storage consumed by virtual machines by using compression and Fast Clone technologies
◆ Reduces the duration of virtual machine copies by using Full Clone technology

For VMFS datastores and RDM volumes on block storage, users can use the feature to provision and mount new storage based on storage pools or RAID groups, and to select a tiering policy for the new storage. VMware administrators who manage shared block storage should use this feature because it:

◆ Simplifies the process of creating VMFS datastores and RDM volumes in accordance with best practices
◆ Automatically mounts the VMFS datastores and RDM volumes to one or more ESX/ESXi™ hosts

The EMC Unified Storage Access Control Utility (ACU) is included with the Unified Storage Management feature. The ACU is a standalone tool for storage administrators to use to create access profiles for VMware administrators, specifying the storage systems that the VMware administrators will have access to, and the storage pools and RAID groups on those systems that will be available to the VMware administrator.

Product overview

The EMC VSI for VMware vSphere: Unified Storage Management feature can provision NFS datastores on NAS storage, and VMFS datastores and RDM volumes on block storage. The feature also performs array-based compression and array-based cloning of virtual machines in NFS datastores. The cloning functions include Full Clones (copies) and Fast Clones (snaps) of Virtual Machine Disk (VMDK) files. VMware administrators can use the feature to manage NAS and block storage in VMware environments by using the existing vSphere Client user interface.
VMware administrators can use the feature to:
- Provision new NFS and VMFS datastores, and RDM volumes
- Extend existing NFS and VMFS datastores
- Compress virtual machines in NFS datastores
- Clone virtual machines in NFS datastores:
  - Fast Clones support – Limited to the same file system
  - Full Clones support – Limited to file systems on the same Data Mover
  - Integrate with VMware View™
  - Integrate with Citrix XenDesktop

To provision new NFS datastores, the feature:
- Creates a file system with automatic file system extension and EMC Virtual Provisioning™
- Exports the file system using NFS
- Provides one or more ESX/ESXi servers root access to the export
- Creates an NFS datastore on the newly created NAS file system

To provision new VMFS datastores, the feature:
- Binds a Fibre Channel (FC) or iSCSI LUN in a user-specified RAID group or storage pool
- Adds the newly bound LUN to the storage group associated with the selected ESX/ESXi hosts
- Creates a VMFS datastore on the newly created block LUN

To provision new RDM volumes, the feature:
- Binds a Fibre Channel (FC) or iSCSI LUN in a user-specified RAID group or storage pool
- Does not add the newly bound LUN to any storage group, so the user is able to assign it to any virtual machine

The EMC Unified Storage system ACU allows storage administrators to create access profiles for the VMware administrator. To create an access profile with the ACU, the storage administrator:
- Specifies the storage systems that the VMware administrator will be allowed to access
- Specifies whether the VMware administrator will have DHSM/ASA access on file storage systems
- Specifies the storage pools and RAID groups that will be available to the VMware administrator

This guide covers EMC VSI for VMware vSphere: Unified Storage Management version 5.4.

**Audience**

This solution was designed for VMware administrators who manage shared NFS or VMFS storage through the vSphere Client. After the storage administrator has planned and implemented the storage environment, the VMware administrator sets up the VMware
virtual environment and loads EMC VSI for VMware vSphere: Unified Storage Management. Using this feature, VMware administrators can reduce storage consumption for virtual machines as they grow, allocate or expand NFS and VMFS datastores, and provision virtual machines without the direct involvement of the storage administrator.

Scope

This guide is intended to give readers an overview of the EMC VSI for VMware vSphere: Unified Storage Management feature and its use in their environment. Topics covered in this guide include:

- Overview of the EMC VSI for VMware vSphere: Unified Storage Management solution
- VMware vSphere and EMC Celerra, CLARiiON, VMAX, VNX, and VNXe prerequisites and system requirements
- EMC VSI for VMware vSphere: Unified Storage Management
- Common installation mistakes
- EMC VSI for VMware vSphere: Unified Storage Management best practices
- Troubleshooting procedures

Key terms

- **Celerra**: The Celerra is a dedicated network server that is optimized for files and block access.
- **CLARiiON**: CLARiiON is a dedicated block storage array.
- **Cluster**: A group of hosts that share resources and have a common management interface. Changes made at the cluster level impact all the hosts within the cluster.
- **Compressed**: When an object is compressed, it uses less space on disk than it would normally occupy. In the context of EMC VSI for VMware vSphere: Unified Storage Management, the compressed field is either Yes or No (to indicate whether compression has been applied).
- **Data Mover**: In a Celerra Network Server, a Data Mover is a cabinet component running its own operating system that retrieves data from a storage device and makes it available to a network client. This is also referred to as a blade.
- **ESX/ESXi**: VMware ESX and ESXi are the virtualization applications that abstract processor, memory, storage, and networking resources into multiple virtual machines running side-by-side on the same physical server.
- **Fast Clone**: A method of making a thin copy of a virtual machine using Celerra, VNX, or VNXe NFS-based snapshots.
- **File system**: The file system is the Network File System (NFS). NFS is a network file system protocol that allows a user on a client computer to access files over a network as easily as if the network devices were attached to its local disks.
- **Full Clone**: A method of making a full copy of a virtual machine using native Celerra, VNX, or VNXe functionality.
LUN: Logical Unit Number. A SCSI identifier used by Fibre Channel and iSCSI to identify a disk, a subset of a disk, or an array of disks that is layered beneath a VMFS datastore or represented by an RDM volume.

Path: The path is the NFS path to the virtual machine.

RAID group: A group of disks that presents itself as a single unit on which to bind LUNs. Each LUN stored in a RAID group is distributed equally among the disks in the RAID group.

Snap: Also known as a snapshot, a snap is a point-in-time image of a file system that does not mirror the data on the file system, thereby using less disk space than a standard backup.

Space savings: If the volume is compressed, the feature lists the amount of space savings that is realized. If the volume is not compressed, the field lists N/A.

Storage Pool: An aggregation of disk storage from which datastores can be provisioned.

Storage Processor (SP): In a CLARiiON array, a storage processor is a cabinet component that runs its own operating system and provides access to the data stored on the array. Each SP has its own IP address.

Tiering Policy: The tiering policy is the method used by the array to balance cost and performance by moving data between different drive types within a storage pool. Tiering is not available for RAID group-based LUNs.

Virtual machine: A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. An operating system installed on a virtual machine is called a guest operating system.

VMAX: A series of high-end storage platforms that provide block storage capabilities.

VNX: A series of mid-range to high-end storage platforms that provide both file storage capabilities (VNX for file), block storage capabilities (VNX for block), or both.

VNXe: A series of entry-level storage platforms that provide both file and block storage capabilities.

Related documents

The following related documents are available at https://support.emc.com:

- EMC VSI for VMware vSphere: Unified Storage Management Release Notes
- Using EMC Celerra Storage with VMware vSphere and VMware Infrastructure (TechBook)
- Using EMC CLARiiON Storage with VMware vSphere and VMware Infrastructure (TechBook)
- Using EMC Symmetrix Storage with VMware vSphere (TechBook)
- Using EMC VNX Storage with VMware vSphere (TechBook)
- EMC CLARiiON Integration with VMware ESX (Applied Technology)
- VMware vSphere 4.1 on EMC VNXe Series Deployment Guide
CHAPTER 2
Prerequisites and System Requirements

This chapter presents these topics:

- Downloading EMC VSI for VMware vSphere: Unified Storage Management.......... 12
- Setting up the environment..................................................................................... 12
- Environment and system requirements ................................................................... 13
- Loading EMC VSI for VMware vSphere: Unified Storage Management....................... 17
Prerequisites and System Requirements

Downloading EMC VSI for VMware vSphere: Unified Storage Management

EMC VSI for VMware vSphere: Unified Storage Management is distributed as a zip file containing a single-file installer that is available for download from https://support.emc.com. This software is available with Celerra, CLARiiON, VNX, VNXe, or VMAX at no additional cost.

Setting up the environment

Install EMC VSI for VMware vSphere: Unified Storage Management on a workstation that has the vSphere Client. Refer to “Installing EMC VSI for VMware vSphere: Unified Storage Management” on page 22 for specific instructions. After you install the feature, make sure there is network connectivity between the:

- NAS Data Mover(s) and ESX/ESXi servers
- NAS Control Station and Data Mover(s) and the vSphere Client
- One or more block storage processors and the ESX/ESXi servers
- One or more block storage processors and the vSphere Client
- The VMware vCenter™ Server and the vSphere Client
Environment and system requirements

Minimum system requirements for the vSphere Client with the feature, which are specified in the ESX and vCenter Server Installation Guide, are the same as the standalone vSphere Client.

Uninstall any previous installs of the EMC Celerra Plug-in for VMware or EMC Unified Storage Plug-in for VMware before installing EMC VSI for VMware vSphere: Unified Storage Management.

The Celerra must meet the following system requirements before use by the feature:

- Celerra Network Server software version 5.6.48.7 or later is installed.
- All Celerra Data Movers have Celerra Network Server software version 5.6.48.701 or later installed. To obtain the required software, contact EMC Customer Support.
- NFS license is enabled.
- One or more storage pools are created.
- Network ports are configured.
- Network connectivity exists between one or more Data Movers and ESX/ESXi servers.
Prerequisites and System Requirements

- Network connectivity exists between the Control Station and vSphere Client on port 22 (required to provision NFS storage).
- Network connectivity exists between one or more Data Movers and the vSphere Client on port 5080 (required to compress and clone virtual machines).
- Network connectivity exists between the vCenter Server and vSphere Client.
- DHSM must be set up on the Celerra to use the compression and cloning features.
- Celerra maintains the following limit:
  - Maximum file system size = 16 TB

The CLARiiON must meet the following system requirements before use by the feature:
- FLARE® software version 04.29 or later is installed. To obtain the required software, contact EMC Customer Support.
- Navisphere® Secure CLI version 7.32 or later is installed on the vSphere Client host.

Note: If Navisphere Secure CLI is not installed on the vSphere Client host, download Navisphere CLI for Windows from the EMC online support website. The Navisphere CLI package for Windows includes Navisphere Secure CLI.

- One or more storage pools or RAID groups are created.
- Network ports are configured.
- Network connectivity exists between one or more storage processors and ESX/ESXi servers.
- Network connectivity exists between one or more storage processors and the vSphere Client on port 443 (required for provisioning VMFS datastores and RDM volumes, and setting tiering policies).
- Network connectivity exists between the vCenter Server and vSphere Client.
- Each ESX/ESXi host that will access block storage must be connected to Storage Group on the array.

The VNX must meet the following system requirements.

VNX for file:
- VNX for file Operating Environment software version 7.0 or later is installed.
- VNX new Block OE (5.32) or later is required for Virtual Data Mover (VDM) support.
- All VNX Data Movers have VNX for file Operating Environment software version 7.0 or later installed. To obtain the required software, contact EMC Customer Support.
- NFS license is enabled.
- Storage pool is created.
- Network ports are configured.
- Network connectivity exists between one or more Data Movers and ESX/ESXi servers.
- Network connectivity exists between the Control Station and vSphere Client on port 22 (required to provision NFS storage).
Prerequisites and System Requirements

- Network connectivity exists between one or more Data Movers and the vSphere Client on port 5080 (required to compress and clone virtual machines).
- Network connectivity exists between the vCenter Server and vSphere Client.
- DHSM must be set up to use the compression and cloning features.
- VNX for file maintains the following limit:
  - Maximum file system size = 16 TB

VNX for block:

- VNX for block Operating Environment software version 05.31 or later is installed. To obtain the required software, contact EMC Customer Support.
- Navisphere Secure CLI version 7.32 or later is installed on the vSphere Client host.

**Note:** If Navisphere Secure CLI is not installed on the vSphere Client host, download Navisphere CLI for Windows from the EMC online support website. The Navisphere CLI package for Windows includes Navisphere Secure CLI.

- Storage pool or RAID group is created.
- Network ports are configured.
- Network connectivity exists between one or more storage processors and ESX/ESXi servers.
- Network connectivity exists between one or more storage processors and the vSphere Client on port 443 (required for provisioning VMFS datastores and RDM volumes, and setting tiering policies).
- Network connectivity exists between the vCenter Server and vSphere Client.
- Each ESX/ESXi host that will access block storage is connected to a Storage Group on the array.

The VNXe must meet the following system requirements:

- VNXe Operating Environment software version 2.0.3 or later is installed. To obtain the required software, contact EMC Customer Support.
  - VNXe Operating Environment software version 2.2 is required for Advanced StorageAccess (ASA), and the cloning and compression capabilities on VNXe.
- UEM CLI version 1.5 or later is installed on the vSphere Client host.

**Note:** If Unisphere® CLI is not installed on the vSphere Client host, download Unisphere CLI for Windows from the EMC Online Support website.

- NFS license is enabled (to provision file storage).
- iSCSI license is enabled (to provision block storage).
- Network ports are configured.
- Network connectivity exists between the VNXe and one or more ESX/ESXi servers.
Prerequisites and System Requirements

- Network connectivity exists between the VNXe and vSphere Client on port 443 (required for provisioning NFS and VMFS datastores, and RDM volumes).
- Network connectivity exists between the vCenter Server and vSphere Client.

The VMAX must meet the following system requirements before use by the feature:

- SMI-S Provider 4.5 is installed. SMI-S Provider 4.5 is available at the following location on the EMC Online Support site at http://powerlink.EMC.com:
  Home > Support > Software Downloads and Licensing > Downloads S > SMI-S Provider

- Bidirectional connectivity requirements:
  - vCenter Server and vSphere Client.
  - SMI-S server and vSphere Client (ports 5988, 5989, 5985, and 5986, configurable).
  - SMI-S server and VMAX arrays (VMAX arrays must be preconfigured into SMI-S Provider views).
  - VMAX arrays and ESXi hosts (ESXi hosts must be preconfigured in VMAX masking views).

- Storage systems:
  - VMAX: Enginuity 5773 or later.
  - SMI-S server: SMI-S Provider 4.5 or later (includes Solutions Enabler 7.5).
  - The SMI-S Provider runs on a variety of Windows and Linux releases. For more information see EMC SMI-S Provider V4.5 Release Notes, P/N 300-015-002.

- Symmetrix models supported:
  - Symmetrix VMAX 10K Series
  - Symmetrix VMAX 20K Series
  - Symmetrix VMAX 40K Series

- Symmetrix gatekeepers (on SMI-S Server):
  - Configure six gatekeepers for each Symmetrix array accessed by the provider.
  - Only set up these gatekeepers for the host on which the SMI-S Provider is running.

- When started, the SMI-S Provider automatically discovers all Symmetrix storage arrays connected to the host on which the array provider is running. No other action is required, such as a running the symcfg discover command.

- Setting up administrator authentication:
  - Authentication is required to query the EMC CIM Server:
    1. Go to the URL https://<ipaddress>:5989/ecomconfig, and log in using the username admin and the password #1Password.
    2. Click Add User and create a user with the role of Administrator.
  - This newly created username can now be used to obtain access to the SMI-S Provider.
The VMware environment must meet the following requirements prior to use by the feature:

- ESXi Server 4.1, 5.0, or 5.1 is installed.
- All ESX/ESXi servers belong to a DNS domain.
- VMware vCenter Server 4.1, 5.0, or 5.1 is installed.
- vSphere Client between 4.1 and 5.1 is installed.
- VMware View between 5.0 and 5.1 is installed.
- The preferred locale of the Windows client that runs the vSphere Client is en_US. However, if you have set a locale other than en_US, then input/output must be in US-ASCII characters.
- No previous installs of the EMC Celerra Plug-in for VMware or the EMC Unified Storage Plug-in for VMware earlier than 4.0.0.45.
- Versions prior to 4.0.0.45 are uninstalled before you install 5.4. (For versions 4.0.0.45 to 4.1, the installer will perform an upgrade.)
- EMC recommends uninstalling the EMC CLARiiON Plug-in for VMware if it is installed.

The Citrix XenDesktop environment must meet the following requirements prior to use by the feature:

- XenDesktop Controller 5.0 or later is installed.
- Windows Remote Management (WinRM) is installed on the XenDesktop Controller host and on the vSphere Client host.
- WinRM service is started and configured to listen to incoming service requests.
- Power Shell 2.0 must be installed on the XenDesktop Controller host and on the vSphere Client host.
- A minimum of one hypervisor connection is configured on XenDesktop with an address that points to the vCenter Server where the vSphere Client is registered.
- The XenDesktop Controller and the vSphere Client are in the same Active Directory domain.
- Virtual Desktop Agent is installed on virtual machine images to be cloned.

**Loading EMC VSI for VMware vSphere: Unified Storage Management**

After you install EMC VSI for VMware vSphere: Unified Storage Management on the workstation with the vSphere Client, you must complete the following procedures on the workstation to load the feature to make it operational.

**Remove quotes from system path**

1. Right-click **My Computer**.
2. Select **Properties**.
3. Click the **Advanced** tab.
4. Click **Environment Variables**.
5. Edit the Path variable. Change any entries that contain quotes to short notation (use the command `dir /x` to find the short notation of a folder).

**Example:**

*C:\Program Files\Common Files\emc*

Changes to:

C:\progra~1\common~1\emc

**DHSM/ASA setup instructions**

Distributed Hierarchical Storage Management (DHSM) can be set up on the EMC Celerra or EMC VNX in one of three ways. It can be set up in EMC VSI for VMware vSphere: Unified Storage Management by running the DHSM setup script or by manually entering the commands in the Celerra or VNX CLI.

On EMC VNXe storage systems, the DHSM functionality is called Advanced Storage Access (ASA). Configure ASA when adding VNXe systems to the feature.

**Set up DHSM/ASA in the feature**

You can set up DHSM/ASA when you are adding a Celerra, VNX, or VNXe to the feature. Refer to “Add EMC Celerra” on page 39 or “Add EMC VNX” on page 42 for instructions on setting up DHSM; refer to “Add EMC VNXe” on page 45 for instructions on setting up ASA.

**Set up DHSM using the setup script**

Included with the feature package is a perl script (dhsmsetup.pl) that automatically sets up DHSM on the EMC Celerra or EMC VNX. The script is usable only after it is copied to the Celerra or VNX Control Station.

1. Copy the script by downloading pscp.exe from the following website:
   http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html
2. Run pscp.exe on your local machine by executing the following command:
   ```
   pscp dhsmsetup.pl <user>@<hostname>:<path>
   ```
   The variables in this executable are:
   - `<user>` = Control Station user
   - `<hostname>` = Control Station hostname or IP address
   - `<path>` = Path on Control Station where the script should be saved
   
   The Control Station prompts you for your password. This process transfers the dhsmsetup.pl script to the path that you provide on the Control Station.

   **Example:**
   ```
   pscp dhsmsetup.pl nasadmin@celerra.emc.com:/home/nasadmin
   ```
3. After the script is successfully copied, log in to the Control Station and navigate to the path where you saved the script. The script is executed with the following command:

   perl dhsmsetup.pl <Data Mover> <User> <Host IP>

   The variables in this script are:
   • <Data Mover> = The name of the Celerra or VNX Data Mover for which you’d like to configure DHSM.
   • <user> = The name of the Celerra or VNX user to create that will be accessing DHSM.
   • <host IP> = The IP address of the host that will be accessing DHSM.

   The system prompts you for a User ID, Group ID, Home Directory, and password for the new user. The User and Group IDs must be numeric. If you attempt to use an existing User ID, you are prompted to retry your input. The Home Directory field can be left blank if you choose. The password for the new user must be at least 6 characters.

   After completing these tasks, the script displays the DHSM configuration and a message that the setup is successful.

   **Note:** You must run the script once for each Data Mover that you intend to use with the feature. The feature requires that Data Movers in a Celerra or VNX cabinet have the same DHSM username and password.

Set up ASA when adding a VNXe to the feature

1. After you enter the platform credentials, select *Configure Advanced Storage Access.*
2. In the *Password* field, type the ASA password.
3. Click *Finish.*

Manually set up DHSM on Celerra or VNX

This procedure sets up DHSM on all Data Movers. The manual setup is a procedure for users who choose not to use the DHSM setup script or set up DHSM in the feature GUI.

1. Create a new DHSM user:

   /nas/sbin/server_user <server name> -add -md5 -passwd <username>

   Example:

   /nas/sbin/server_user server_2 -add -md5 -passwd dhsm_user

2. Enable digest authentication:

   /nas/bin/server_http <server name> -modify dhsm -authentication digest -users <username>

   Example:

   /nas/bin/server_http server_2 -modify dhsm -authentication digest -users dhsm_user

3. Start DHSM service on the Data Mover:

   /nas/bin/server_http <server name> -service dhsm -start
4. Add your vSphere Client(s) IP to the DHSM access list:

   /nas/bin/server_http <server name> -append dhsm -hosts <clientIP1,clientIP2,clientIP3>

   Example:

   /nas/bin/server_http server_2 -append dhsm -hosts 100.100.100.1,100.100.100.2

   **Note:** Failure to set up DHSM on the Celerra or VNX, or failure to set up ASA on VNXe, will leave the user unable to do compression or create Full or Fast Clones.
CHAPTER 3
EMC VSI for VMware vSphere: Unified Storage Management Installation

This chapter presents these topics:

- Installing EMC VSI for VMware vSphere: Unified Storage Management .................. 22
- Installing the EMC Unified Storage Access Control Utility ..................................... 25
- Common installation mistakes ................................................................................... 28
Installing EMC VSI for VMware vSphere: Unified Storage Management

This section shows the EMC VSI for VMware vSphere: Unified Storage Management InstallShield Wizard screens and provides general instructions for installing the feature.

During installation, EMC VSI for VMware vSphere: Unified Storage Management checks to see if the EMC Virtual Storage Integrator (VSI) is installed. If VSI is not detected, it is automatically installed as part of the Unified Storage Management feature installation.

1. Unzip the zip file.
2. Double-click `emc-vsi-usm-5.4.0.x-vmware-vsphere-WINDOWS-x86.exe`.
3. Click Next.

![Figure 2 Welcome to the InstallShield Wizard for EMC VSI for VMware vSphere: Unified Storage Management](image)

**Note:** Navisphere CLI is not required for VMAX-only provisioning.

4. Select I accept the terms in the license agreement.
5. Click Next.
6. Click **Install**.

7. Click **Finish** to exit the EMC VSI for VMware vSphere: Unified Storage Management installer.
8. Launch the vSphere Client and connect to the vCenter Server.

Figure 5  Installation complete

Figure 6  vSphere Client Home screen
Installing the EMC Unified Storage Access Control Utility

This section shows the EMC Unified Storage Access Control Utility InstallShield Wizard screens and provides general instructions for installing the feature.

1. Unzip the zip file.
2. Double-click `emc-acu-5.1.0.x-WINDOWS-X86.exe`.
3. Click **Next**.

![Welcome to the InstallShield Wizard for the EMC Unified Storage Access Control Utility](image.png)

**Figure 7** Welcome to the InstallShield Wizard for the EMC Unified Storage Access Control Utility

4. Select **I accept the terms in the license agreement.**
5. Click **Next**.
6. Click **Install**.

7. Click **Finish** to exit the EMC Unified Storage Access Control Utility installer.
8. Launch the EMC Unified Storage Access Control Utility.

Figure 10  Installation complete

Figure 11  EMC Unified Storage Access Control Utility home screen
Common installation mistakes

Symptom: I receive a DHSM error when trying to connect to Celerra or VNX.

◆ Check to make sure the DHSM service is started.
  Example:
  `/nas/bin/server_http server_http server_2 -info`
  Confirm that the **Active** field is in the True state.

◆ Check to make sure the vSphere Client IP address is added to the DHSM access list.
  Example:
  `/nas/bin/server_http server_http server_2 -info`
  Confirm that the **Allowed IPs** field contains the correct client IP addresses.

Symptom: The feature does not load in vSphere Client.

◆ Remove quotes from from the Windows Environment path, as shown in the section “Remove quotes from system path” on page 17. Restart the VMware vSphere Client.

◆ Select **Plug-ins > Manage Plug-ins** and verify that **EMC Virtual Storage Integrator (VSI) for vSphere** is enabled.
CHAPTER 4
EMC VSI for VMware vSphere: Unified Storage Management – Procedures

This chapter presents these topics:
◆ Manage access profiles in the EMC Unified Storage Access Control Utility .......... 30
◆ Manage storage systems and connection brokers ................................................... 37
◆ Provision storage .................................................................................................... 52
◆ Extend storage ........................................................................................................ 74
◆ Compress a host, cluster, folder, virtual machine, or data center ......................... 75
◆ Decompress a host, cluster, folder, virtual machine, or data center ....................... 78
◆ Cloning virtual machines ......................................................................................... 78
◆ Integrate Fast Clones with Citrix XenDesktop .......................................................... 90
◆ Integrate Full Clones with Citrix XenDesktop ......................................................... 94
◆ Refresh desktops ..................................................................................................... 98
Manage access profiles in the EMC Unified Storage Access Control Utility

Double-click the **Access Control Utility** icon to start the EMC Unified Storage Access Control Utility.

![EMC Unified Storage Access Control Utility home screen](image)

**Figure 12** EMC Unified Storage Access Control Utility home screen

**Add an access profile**

Complete the following steps to add an access profile:

1. Click **Add**. The **Add Access Profile** wizard appears.
2. In the **Profile Name** field, type a name for the access profile.
3. In the **Description** field, optionally type a description for the access profile.
4. Click **Next**.

![Access Profile Details](image)

**Figure 13** Access Profile Details

5. Click **Add** to add a storage system.

To add storage systems, follow the directions in “Add EMC Celerra” on page 39, “Add EMC CLARiON” on page 40, “Add EMC VNX” on page 41, “Add EMC VNXe” on page 44, or “Add EMC VMAX” on page 45.

**Note:** For EMC Celerra and EMC VNX for file, VMware administrators cannot compress, decompress, or clone datastores without DHSM access. VMware administrators must have ASA access to compress, decompress, or clone datastores on EMC VNXe.

6. Select the level of storage pool access to allow on the storage system:

   a. **All storage pools** allows the VMware administrator to have unlimited access to all the storage pools on the system. With this setting, the VMware administrator will have access to any storage pools that are created at a later time.

   b. **No storage pools** does not allow the VMware administrator any access to the storage pools on the system. With this setting, the VMware administrator also will not have access to any storage pools that are created at a later time.

   c. **Selected storage pools** allows the VMware administrator to have access to a specified list of storage pools. With this setting, the VMware administrator will not have access to any storage pools that are created at a later time.
7. Click **Finish** if you selected **All storage pools** or **No storage pools**, or **Next** if you selected **Selected storage pools**.

8. If you selected **Selected storage pools**, choose storage pools from the **Available Storage Pools** table and click **Select**.

   To deselect a storage pool, select the storage pool from the **Selected Storage Pools** table and click **Remove**.
9. Click **Finish**.

![Choose Storage Pools](image)

**Figure 15  Choose Storage Pools**

The storage system now appears in the **Storage Systems** table.

- To edit a storage system, select it in the **Storage Systems** table, and click **Edit**.
- To remove a storage system, select it in the **Storage Systems** table, and click **Remove**.
10. Click **Add** to add another storage system to the profile, or click **Finish** to complete the profile.

**Figure 16  Define Storage Systems**

The new profile appears in the **Storage System Access Profiles** table.

**Figure 17  Storage System Access Profiles**
Remove an access profile

Complete the following steps to remove an access profile from the EMC Unified Storage Access Control Utility:

1. In the Storage System Access Profiles table, select an access profile.
2. Click Remove.

Edit an access profile

Complete the following steps to edit the credentials of a storage system or View Manager server already in the feature:

1. In the Storage System Access Profiles table, select an access profile and then click Edit.
2. Edit the fields in the Enter Credentials dialog box.

   Note: The Password field is not populated. If you do not know the password, you cannot edit the storage system.

3. Click Next.
4. Select the level of storage pool access to allow on the storage system:
   a. All storage pools allows the VMware administrator to have unlimited access to all the storage pools on the system. With this setting, the VMware administrator will also have access to any storage pools that are created at a later time.
   b. No storage pools does not allow the VMware administrator any access to the storage pools on the system. With this setting, the VMware administrator will also not have access to any storage pools that are created at a later time.
   c. Selected storage pools allows the VMware administrator to have access to a specified list of storage pools. With this setting, the VMware administrator will not have access to any storage pools that are created at a later time.
5. Click Finish if you selected All storage pools or No storage pools, or Next if you selected Selected storage pools.
6. If you selected Selected storage pools, choose storage pools from the Available Storage Pools table and click Select.
   To deselect a storage pool, select the storage pool from the Selected Storage Pools table and click Remove.
7. Click Finish.

Export an access profile

Complete the following steps to export an access profile:

1. In the Storage System Access Profiles table, select an access profile.
2. Click Export.

![Select a profile to export](image)

Figure 18 Select a profile to export

3. In the Save as field, type a name for the file.

4. Click ... (the browse button) to save the file in a location other than the default.

5. In the Passphrase field, type a passphrase for the file.

6. Click OK.

![Export access profile](image)

Figure 19 Export access profile
Manage storage systems and connection brokers

Navigate to Home > Solutions and Applications > EMC, and click Unified Storage Management in the Features list to manage storage systems and connection brokers.

Figure 20  Manage storage systems and connection brokers screen

Add storage systems or connection brokers

Complete the following steps to add a storage system or connection broker for the feature to manage:

1. From the EMC Unified Storage interface, click Add to add a storage system or connection broker to the feature.
2. Select **Enter Storage System Credentials**, or **Import Access Profile**, and click **Next**.

![Select Credentials Source](image)

**Figure 21 Select Credentials Source**

To enter storage system credentials, continue with Step 3. To import an access profile, skip to “Import an access profile” on page 49.

3. Select **EMC Celerra**, **EMC CLARiiON**, **EMC VNX**, **EMC VNXe**, **EMC VMAX**, **VMware View Manager**, or **XenDesktop Controller**.
4. Click **Next**.

Add EMC Celerra

1. In the **Celerra Control Station Hostname/IP Address** field, type the hostname or IP address of the Control Station.

2. In the **Celerra Control Station Username** field, type the Control Station username.

   To use LDAP authentication, type the username in this format:

   `<username>@<domain_name>`
3. In the **Celerra Control Station Password** field, type the Control Station password.

![Figure 23 Enter Celerra credentials](image)

4. Click **Finish**; or select the **Configure DHSM** checkbox to configure DHSM and click **Next**:
   a. To create a new DHSM user, select **Create New DHSM User**.
      1. In the **DHSM Username** field, type a DHSM username.
      2. In the **DHSM Password** field, type a DHSM password.
      3. Select the **Use next available User ID and Group ID** checkbox, or manually fill in the **User ID** and **Group ID** fields.

      **Note:** If you manually select a User ID and Group ID that are already in use, the system will become unresponsive. Reboot the Control Station, and add the storage system again.

   4. Select **Allow access from all hosts** or **Allow access from specific hosts**.
      To allow access from specific hosts, in the **Client IP Addresses** field, type the IP addresses of one or more vSphere Client hosts that will access the Celerra. Type each IP address on a separate line.

   5. Click **Finish**.

b. To use an existing DHSM user, select **Use Existing DHSM User**.
   1. In the **DHSM Username** list box, select the DHSM username.
   2. In the **DHSM Password** field, type the DHSM password.
   3. Select **Allow access from all hosts** or **Allow access from specific hosts**.
      To allow access from specific hosts, in the **Client IP Addresses** field, type the IP addresses of one or more vSphere Client hosts that will access the Celerra. Type each IP address on a separate line.
4. Click **Finish**.

![Configure DHSM on Celerra](image)

**Figure 24** Configure DHSM on Celerra

Add EMC CLARiiON

1. In the **EMC CLARiiON SP A** field, type the IP address of SP A.
2. In the **EMC CLARiiON SP B** field, type the IP address of SP B.
3. In the **Username** field, type the CLARiiON username.
4. In the **Password** field, type the CLARiiON password.
5. In the **Scope** list box, select a scope for CLARiiON access.

   To use LDAP authentication, type the username and select **LDAP** from the list box. Do not type the domain name as part of the username.
6. Click **Finish**.

![Figure 25 Add EMC CLARiiON](image)

**Figure 25 Add EMC CLARiiON**

**Add EMC VNX**

1. Select **Block**, **File**, or both.
2. Click **Next**.

![Figure 26 Select VNX storage access](image)

**Figure 26 Select VNX storage access**

To add VNX block:

1. In the **Storage Processor IP** field, type the storage processor IP address.
2. In the **Username** field, type the VNX block username.

3. In the **Password** field, type the VNX block password.

4. In the **Scope** list box, select a scope for VNX block access.
   
   To use LDAP authentication, type the username and select **LDAP** from the list box. Do not type the domain name as part of the username.

5. Click **Finish**.

   **Note:** To add both VNX block and VNX file, click **Next** to add the VNX file credentials.

---

Figure 27  Enter VNX block credentials

To add a VNX file:

1. In the **VNX Control Station Hostname/IP Address** field, type the Control Station hostname or IP address.

2. In the **VNX Control Station Username** field, type the Control Station username.
   
   To use LDAP authentication, type the username in this format:

   `<username>@<domain_name>`
3. In the **VNX Control Station Password** field, type the Control Station password.

![Figure 28 Enter VNX file credentials](image)

4. Click **Finish** to add the VNX; or select the **Configure DHSM** check box to configure DHSM, and click **Next**.
   a. To create a new DHSM user, select **Create New DHSM User**.
      1. In the **DHSM Username** field, type a DHSM username.
      2. In the **DHSM Password** field, type a DHSM password.
      3. Select the **Use next available User ID and Group ID** checkbox, or manually fill in the **User ID** and **Group ID** fields.

      **Note:** If you manually select a User ID and Group ID that are already in use, the system will become unresponsive. Reboot the Control Station, and add the storage system again.

   4. Select **Allow access from all hosts** or **Allow access from specific hosts**.
      To allow access from specific hosts, in the **Client IP Addresses** field, type the IP addresses of one or more vSphere Client hosts that will access the VNX. Type each IP address on a separate line.

   5. Click **Finish**.

   b. To use an existing DHSM user, select **Use Existing DHSM User**.
      1. In the **DHSM Username** list box, select a DHSM username.
      2. In the **DHSM Password** field, type the DHSM password.
      3. Select **Allow access from all hosts** or **Allow access from specific hosts**.
      To allow access from specific hosts, in the **Client IP Addresses** field, type the IP addresses of one or more vSphere Client hosts that will access the VNX. Type each IP address on a separate line.
4. Click Finish.

![Configure DHSM on VNX](image)

Figure 29 Configure DHSM on VNX

Add EMC VNXe

1. In the **Management Address** field, type the management IP address.
2. In the **User** field, type the username.
3. To use LDAP authentication, type the username in this format:
   `<domain_name>/<username>`
4. In the **Password** field, type the password.
5. Select the **Configure Advanced Storage Access** checkbox to configure ASA.
6. In the ASA **Password** field, type the password.
7. Click **Finish**.

![Figure 30 Add VNXe](image)

**Add EMC VMAX**

1. In the **SMI-S Provider IP** field, type the SMI-S Provider IP address.
2. In the **Username** field, type the SMI-S Provider username.
3. In the **Password** field, type the SMI-S Provider password.
4. Click **Next**.
Note: The SMI-S Provider is a proxy for VMAX 10K, VMAX 20K, and VMAX 40K.

Figure 31 Add VMAX

5. Select the VMAX system from the list.

Note: You can select only one system to add at a time.
Figure 32  Select VMAX storage system

**Note:** Multiple entries in this table might have the same Management IP.

6. Click **Finish**.

**Add VMware View Manager**

1. In the **VMware View Manager Server** field, type the View Manager server IP address.
2. In the **Username** field, type the View Manager server username.
3. In the **Password field**, type the View Manager server password.
4. Click Finish.

Figure 33 Add View Manager server

Add Citrix XenDesktop Controller

1. In the XenDesktop Controller Name/IP field, type the name or IP address of the XenDesktop Controller.

2. In the Domain Admin User field, type the domain and administrator username for the XenDesktop controller in the <domain\username> format.

3. In the Password field, type the password for the XenDesktop Controller.

4. Click Finish.
**Note**: If the system where the vSphere Client is installed is not part of the same domain as the XenDesktop Controller, the add operation will fail.

![Add XenDesktop Controller](image)

**Figure 34 Add XenDesktop Controller**

**Import an access profile**

Complete the following steps to import an access profile:

1. Click ... (the browse button) to browse to the location where the access profile file is saved.

2. Double-click the access profile xml file, or click **Open**.

3. In the **Passphrase** field, type the passphrase.
4. Click Finish.

**Figure 35 Import Access Profile**

If any storage systems specified in the access profile are already added to the Unified Storage Management feature, the credentials and permissions from the access profile will overwrite the existing credentials.

5. Click **OK** to overwrite any existing credentials, or click **Cancel** to stop the import operation.

**Figure 36 Overwrite Systems**

**Remove storage systems or connection brokers**

Complete the following steps to remove a storage system or View Manager server from the feature:

1. From the EMC Unified Storage interface, select a storage system or connection broker from the list and click **Remove** to remove a storage system or View Manager server from the feature.
2. Click Yes.

![Figure 37 Remove a storage system or View Manager server](image)

**Edit credentials**

Complete the following steps to edit the credentials of a storage system or View Manager server already in the feature.

1. From the EMC Unified Storage interface, select a storage system or View Manager server from the list and click **Edit**.

2. Edit the fields in the **Add Credentials** dialog box.

   **Note:** The **Password** field is not populated. If you do not know the password, you cannot edit the storage system.

3. Click **Finish**.

![Figure 38 Edit a storage system or View Manager server](image)
Provision storage

Storage provisioning prepares a NAS NFS file system, block VMFS file system, or block RDM volume for use by the ESX/ESXi server(s). If you choose to provision storage on a cluster, folder, or data center, then all hosts within the selected object will mount the newly provisioned NFS datastore, VMFS datastore, or RDM volume.

Provision storage for an NFS datastore

There are two options when provisioning storage when using the feature to provision NFS datastores: create a new NFS export, or use an existing NFS export. In some environments, if the VMware administrators do not have the privileges necessary to create NAS file systems and NFS exports, or even the need to do so if such tasks are completed by a storage administrator, they can use the provision storage feature to attach ESX/ESXi hosts to existing NFS exports.

NFS datastores can be provisioned on EMC Celerra, EMC VNX, and EMC VNXe platforms.

Provision storage on a new NFS export on EMC Celerra, EMC VNX, or EMC VNXe

Complete the following steps to provision NAS storage on a new NFS export:

**Note:** Do not create iSCSI LUNs on file systems that are exported over NFS and mounted by ESX/ESXi server(s).

1. Right-click the object. (The object can be a host, cluster, folder, or data center.)

   **Note:** If you choose a cluster, folder, or data center, then all ESX/ESXi hosts within the object will be attached to the newly provisioned storage.

2. Select EMC > Unified Storage.
5. Click **Next**.

![Figure 39 Provision NFS datastore](image)

Figure 39 Provision NFS datastore

6. Select a storage system from the table.

   If there are no storage systems listed, click **Add**. The **Add Credentials** wizard appears. Refer to “Add EMC Celerra” on page 39, “Add EMC VNX” on page 41, or “Add EMC VNXe” on page 44 to add a storage system.

7. Click **Next**.

![Figure 40 Select storage system](image)

Figure 40 Select storage system
8. In the **Datastore Name** field, type a name for the datastore.

**Note:** Datastore names with the `/\%` characters, names that contain spaces, and names that consist only of numeric characters are not supported by the feature.

9. Click **Next**.

![Figure 41 Enter datastore name](image)

Continue to Step 10 to provision an NFS datastore on EMC VNXe. Skip to step 19 on page 58 to provision an NFS datastore on EMC Celerra or EMC VNX.

10. Select **Create New NFS Export**.
11. Click **Next**.

![Figure 42 Provision new NFS export on VNXe](image)

12. Select a storage pool from the table.

**Note:** If the storage system was added by importing an access profile from the EMC Unified Storage Access Control Utility, only storage pools specified by the storage administrator will be available for provisioning.
13. Click **Next**.

**Figure 43  Select storage pool on VNXe**

14. In the **Shared Folder Server** list box, select a shared folder server.

15. In the **Size** field, type the size for the NFS export and then select the unit of measure from the list box to the right.

16. If desired, enable Thin Provisioning.

17. Click **Finish**.

**Figure 44  Finish new NFS export on VNXe**
18. Skip to step 30 on page 61 to view the new NFS datastore on VNXe.

To provision an NFS datastore on EMC Celerra or EMC VNX, proceed with Step 19.

19. In the **Data Mover Name** list box, select a Data Mover.

20. In the **Data Mover Interfaces** list box, select a Data Mover interface.

21. Click **Next**.

*Figure 45  Select Data Mover*

22. Select **Create New NFS Export**.
23. Click **Next**.

![Image](image.png)

**Figure 46  Create new NFS export**

24. In the **Storage Pool** list box, select a storage pool.

*Note:* If the storage system was added by importing an access profile from the EMC Unified Storage Access Control Utility, only storage pools specified by the storage administrator will be available for provisioning.

25. In the **Initial Capacity** field, type an initial capacity for the NFS export and then select the unit of measure from the list box to the right.

26. If desired, select **Thin Enabled**.

*Note:* Thin Enabled is a best practice with VMware on Celerra and VNX and is enabled by default. If you choose to use Virtual Provisioning, you must type a maximum capacity in the **Max Capacity** field.

27. If **Thin Enabled** is selected, in the **Max Capacity** field, type a maximum capacity for the NFS export and then select the unit of measure from the list box to the right.

28. Select **Edit Advanced Settings** to see the advanced features available. Click **Next**. You can select or deselect the following:

*Note:* There are no advanced options for an EMC VNXe.

- **Export Path** allows the user to export to a custom path. (The feature will export the default file system path.)
- **High Water Mark** specifies the file system usage threshold at which to initiate automatic file system extension. The threshold is an integer in the range of 50 to 99 percent. (The default is 90 percent.)
- **Direct Writes Enabled** enhances write performance to the Celerra or VNX over the NFS protocol. This mechanism allows well-formed writes to be sent directly to the disk without being cached on the server. (This is enabled by default.)

- **No Prefetch** turns the prefetch mechanism off. The prefetch mechanism performs read ahead processing for file systems. This mechanism is designed to optimize read operations of large files. Turning this mechanism off may affect performance. (This is disabled by default.)

- **Virus Checking Enabled** turns on the Common AntiVirus Agent (CAVA). As a best practice, this checkbox is unselected. By disabling AV scanning when provisioning storage for virtual machines, the overall performance can be improved.

- **Export to Subnet** allows the user to export the file system to an entire subnet. By default, the feature exports the file system to each ESX/ESXi host VMkernel IP address. (This is disabled by default.)

- **Set Timeout Settings** sets the NFS heartbeat settings on ESX to the best practices for VMware with Celerra or VNX. (This is enabled by default.)

29. Click Finish.
After clicking Finish, the Unified Storage Management feature:

- Creates a file system on the selected storage pool.
- Mounts the newly created file system on the selected Celerra or VNX Data Mover.
- Exports the newly created file system over NFS and provides root and access privileges to the ESX/ESXi hosts that will mount the NFS datastore.
- Creates the NFS datastore on the selected ESX/ESXi hosts.
- Updates the selected NFS options on the chosen ESX/ESXi hosts.

30. Click the Summary tab to see the newly provisioned storage.

Known issues for provisioning storage on a new NFS export

If the user who is logged in to the NAS storage platform does not have sufficient privilege to create file systems or NFS exports, the provision storage operation will fail.

If the user who is logged in to the vCenter Server does not have sufficient privilege to create NFS datastores, the provision storage operation will fail.
Using Common AntiVirus Agent with VMware vSphere

Common AntiVirus Agent (CAVA) provides an antivirus solution to file-based clients using an EMC Celerra Network Server, or EMC VNX. It uses industry-standard Common Internet File System (CIFS) protocols in a Microsoft Windows Server 2003, Windows 2000, or Windows NT domain. CAVA uses third-party antivirus software to identify and eliminate known viruses before they infect files on the storage system. CAVA provides benefits such as scan on first read, scan on write, and automatic update of virus definition files to ensure that infected files are not stored in the Celerra- or VNX-based shared storage.

Further details on CAVA can be found in the Using Celerra AntiVirus Agent technical module on Powerlink.

The antivirus solution is only for clients running the CIFS protocol. If NFS or FTP protocols are used to move or modify files, the files are not scanned for viruses. Therefore, files accessed by ESX as part of the virtual machine deployment (as in files virtualized in virtual disks) are not scanned for viruses. Furthermore, since CAVA is a file-based solution, block-level storage that is presented to ESX from Celerra, or VNX is not scanned for viruses either.

However, files accessed by Windows virtual machines through the CIFS protocol (by using mapped network shares from Celerra or VNX) are scanned for viruses.

CAVA is most suitable for virtual machines' user data that is accessed using CIFS such as home directories, and network shares. This permits you to architect a centralized solution for virus scanning, avoiding the need to scan these files locally on each virtual machine.

When CAVA is used, action is required to ensure that the third-party antivirus software that is configured as part of the CAVA will not even attempt to scan virtual disk files. However, if CAVA is not used in the system no further action is required.

Therefore, if CAVA is used, take one of the following steps:

- For NFS file systems that are presented to ESX, mount the file system on the Celerra or VNX Data Mover with the noscan option. This instructs CAVA not to scan the file system. This is the optimal alternative, as it has CAVA focus solely on the file systems that hold files that should be scanned.

- Alternatively, if a file system is presented to ESX using NFS and simultaneously also to virtual machines using CIFS, then CAVA can be configured to exclude all file types that are used for file encapsulation of a virtual machine. This involves using the excl= parameter in the viruschecker.conf configuration file.

The latter alternative is less favorable, mainly because typically virtual machines should not be granted access to the encapsulated files of the virtual machines. Therefore, the reminder of this section focuses on the first alternative.

Disable CAVA virus scanning on new NAS datastores

EMC recommends disabling Common AntiVirus scanning when provisioning storage for virtual machines.

The best practice is a cleared checkbox for Common AntiVirus scanning as the default on the Advanced Options dialog box.

Testing shows that disabling AV scanning can improve performance. To verify the AV scanning settings as part of the provisioned storage operation, the user selects Provision Storage > Advanced Options.
Provision storage on an existing NFS export

Complete the following steps to provision storage on an existing NFS export:

**Note:** Do not create iSCSI LUNs on file systems that are exported over NFS and mounted by ESX/ESXi server(s).

1. Right-click the object. (The object can be a host, cluster, folder, or data center.)

   **Note:** If you choose a cluster, folder, or data center, then all ESX/ESXi hosts within the object will be attached to the newly provisioned storage.

2. Select **EMC > Unified Storage**.

3. Select **Provision Storage**. The **Provision Storage** wizard appears.

4. Select **Network File System**.

5. Click **Next**.

![Provision NFS datastore](image)

**Figure 50** Provision NFS datastore

6. Select a storage system from the table.

   If there are no storage systems listed, click **Add**. The **Add Credentials** wizard appears. Refer to “Add EMC Celerra” on page 39, “Add EMC VNX” on page 41, or “Add EMC VNXe” on page 44 to add a storage system.
7. Click **Next**.

8. In the **Datastore Name** field, type a name for the datastore.

9. Click **Next**.

10. Select **Use Existing NFS Export**.

Figure 51  Select a storage system

Figure 52  Enter the datastore name

Continue to Step 10 to provision an NFS datastore on EMC VNXe. Skip to step 14 on page 66 to provision an NFS datastore on EMC Celerra or EMC VNX.
11. Click **Next**.

![Figure 53 Use Existing NFS Export](image1)

**Figure 53 Use Existing NFS Export**

12. Select an NFS export from the table.

**Note:** If the storage system was added by importing an access profile from the EMC Unified Storage Access Control Utility, only NFS exports on storage pools specified by the storage administrator will be available for provisioning.

13. Click **Finish**.

![Figure 54 Select NFS export](image2)
To provision an NFS datastore on EMC Celerra or EMC VNX, proceed with Step 14.

14. In the **Data Mover Name** list box, select a Data Mover.

15. In the **Data Mover Interfaces** list box, select a Data Mover interface.

16. Click **Next**.

![Figure 55 Choose Data Mover](image)

17. Select **Use Existing NFS Export**.

18. Click **Next**.

![Figure 56 Use existing NFS export](image)
19. In the **NFS Export Name** list box, select an NFS export.

   **Note:** If the storage system was added by importing an access profile from the EMC Unified Storage Access Control Utility, only NFS exports on storage pools specified by the storage administrator will be available for provisioning.

20. Select **Edit Advanced Settings** to see the advanced features available. Here, you can select or clear the option to **Set Timeout Settings**.

   **Set Timeout Settings** is selected by default.

   **Note:** There are no advanced options for an EMC VNXe.

21. Click **Finish**.

![Figure 57 Existing NFS Export](image1.png)

![Figure 58 Advanced Options](image2.png)

**Known issues for provisioning storage on an existing NFS export**

Each ESX/ESXi host can only create one NFS datastore on each NFS export.

When you are mounting an existing NFS export, the best practices such as uncached and prefetch that are configured automatically by the Create New NFS Export option must be configured manually on the Celerra or VNX.
Provision storage for a VMFS datastore or RDM volume on EMC CLARiiON, EMC VNX, EMC VNXe, or EMC VMAX

Complete the following steps to provision block storage on a new FC or iSCSI LUN:

1. Right-click the object. (The object can be a host, cluster, folder, or data center.)

   **Note:** If you choose a cluster, folder, or data center, then all ESX/ESXi hosts within the object will be attached to the newly provisioned storage.

2. Select EMC > Unified Storage.


4. Select Disk/LUN.

5. Click Next.

![Select Disk/LUN](image)

6. Select a storage array from the table.

   If there are no storage systems listed, click Add. The Add Credentials wizard appears. Refer to “Add EMC Celerra” on page 39, “Add EMC VNX” on page 41, “Add EMC VNXe” on page 44, or “Add EMC VMAX” on page 45 to add a storage system.

7. Click Next.

   **Note:** For VMAX, multiple entries in this table might have the same Management IP address.
Figure 60  Choose storage array

8. From the table, select the storage pool where the new LUN will reside.

**Note:** If the storage system was added by importing an access profile from the EMC Unified Storage Access Control Utility, only storage pools specified by the storage administrator will be available for provisioning.
9. Click **Next**.

![Choose storage pool](image)

**Figure 61 Choose storage pool**

Step 10 applies only to EMC VNXe systems.

If you are provisioning storage on VMAX, skip to step 11 on page 71.

If you are provisioning storage on an EMC VNX or EMC CLARiiON, skip to step 13 on page 72.

10. In the **iSCSI Node** list box, select an iSCSI node and then click **Next**.
11. Choose the masking view for VMAX.

Figure 62 Choose masking view

Figure 63 Select the storage pool
12. If prompted, select **VMFS-5** or **VMFS-3**

**Note:** Do not select **VMFS-5** if the datastore is going to be accessed by ESXi hosts with an ESX version older than 5.0.

a. For VMFS-3 datastores, in the **Maximum File Size** list box, select a maximum file size.

b. Click **Next**.

![Figure 64 Choose VMFS type](image)

13. Select **VMFS Datastore** or **RDM Volume**.

**Note:** Unlike VMFS datastores, which can be shared across multiple VMs, RDM volumes are bound to a single VM and can be shared across multiple VMs. EMC recommends using VMFS datastores unless a one-to-one mapping between physical and virtual storage is required.

14. For VMFS datastores:

   a. In the **Datastore Name** field, type a name for the datastore.

   b. In the **Maximum File Size** list box, select a maximum file size.

15. In the **LUN Number** list box, select a LUN number.

**Note:** The **LUN Number** list box does not appear when provisioning block storage on VNXe.

16. In the **LUN Ownership** list box, select which storage processor will own the LUN.
17. In the **Capacity** field, type an initial capacity for the datastore and then select the unit of measure from the list box to the right.

For VMAX only, if the provisioned capacity is equal to or smaller than 240 GB, the device will be created as a TDEV device; if the provisioned capacity is larger than 240 GB, the device will be created as a concatenated meta device. Striped meta devices are not supported by USM.

18. Click the **Advanced** button to configure the CLARiiON Fully Automatic Storage Tiering policy settings for the selected LUN.

**Note:** There are no advanced options for an EMC VNXe or EMC VMAX.

There are four tiering policy options:

- **Start High Then Auto-Tier:** Sets the initial data placement to the highest available tier, with subsequent data movement controlled by auto-tier.

  **Note:** For VNX systems, this option is supported only on block OE 5.32 or later.

- **Auto-Tier:** The software distributes the initial data placement across all drive types in the pool, to maximize spindle usage for the LUN. Subsequent data relocation is based on the LUN performance statistics such that data is relocated among tiers according to I/O activity.

- **Highest Available Tier:** Sets the preferred tier for initial data placement and subsequent data relocation (if applicable) to the highest performing disk drives with available space.

- **Lowest Available Tier:** Sets the preferred tier for initial data placement and subsequent data relocation (if applicable) to the most cost-effective disk drives with available space.

**Note:** If the datastore was provisioned on a storage system that was added by importing an access profile from the EMC Unified Storage Access Control Utility, the tiering policy cannot be changed if the storage administrator did not grant access to the storage pool where the datastore resides.
19. Click **Finish**.

![Choose Storage Details (CLARiiON, VNX, VNXe)](image1)

**Figure 65** Choose Storage Details (CLARiiON, VNX, VNXe)

![Choose Storage Details (VMAX)](image2)

**Figure 66** Choose Storage Details (VMAX)
After clicking Finish, the Unified Storage Management feature:

- Creates a LUN in the selected Storage Pool.
- Assigns the LUN to the designated SP.
- Adds the newly bound LUN to the storage group associated with the selected ESX/ESXi hosts, and provisions the LUN to the hosts over FC or iSCSI.
- Creates the VMFS datastore on the selected ESX/ESXi hosts if VMFS is chosen.

20. Click Configuration > Storage to see the newly provisioned storage.

**Extend storage**

NFS and VMFS datastores can be extended when they start to run out of free space.

All NFS datastores can be extended, but the following restrictions apply when extending VMFS datastores:

- The datastore to be extended must be on a thick or thin LUN on an EMC CLARiiON or EMC VNX, EMC VMAX, or a thin LUN on EMC VNXe.
- The datastore must not be provisioned from a RAID group.
- The datastore must not be an RDM volume.
- The datastore must not be on a metaLUN.
- The datastore must not span multiple extents.
- The datastore must not be on a thick LUN on a VNXe iSCSI virtual disk.

**Note:** If the datastore was provisioned on a storage system that was added by importing an access profile from the EMC Unified Storage Access Control Utility, the extend operation will fail if the storage administrator did not grant access to the storage pool where the datastore resides.

To extend a datastore, complete the following steps:

1. From the vSphere Client home screen, click **Hosts and Clusters**.
2. Select a virtual machine that is connected to the vCenter Server.
3. Right-click the datastore to extend, and select **EMC > Unified Storage > Extend Storage.**

![Figure 68 Extend storage](image)

4. In the **Extend Capacity by** field, type the additional capacity to add to the datastore and then select a unit of measure from the list box to the right.

5. In the **Extend Max Capacity by** field, type the additional capacity to add to the datastore maximum capacity and then select a unit of measure from the list box to the right.

6. Click **OK.**

![Figure 69 Specify extension values](image)

**Compress a host, cluster, folder, virtual machine, or data center**

**Best practices for compression**

The compress operation can be performed on the following objects in vSphere:

- **VM:** The virtual machine will be compressed.
- **Host:** All virtual machines on the host will be compressed.
- **Cluster:** All virtual machines in the cluster will be compressed.
- **Datastore:** All virtual machines in the datastore will be compressed.
- **Folder:** All virtual machines in the folder will be compressed.
- **Data center:** All virtual machines in the data center will be compressed.
If the Celerra Data Deduplication or VNX File Deduplication and Compression feature is turned off for the datastore on which a compress operation is executed, the feature will automatically turn on deduplication on the underlying Celerra or VNX file system. This feature has to be enabled to allow compression to occur on the file system.

- Compression ratios observed in preliminary tests are generally between 30 and 50 percent, depending on the data that is being compressed.
- The overall performance of compressed virtual machines is within 10 percent of uncompressed virtual machines.
- Full cloning a compressed virtual machine takes about 25 percent longer than cloning a non-compressed virtual machine.
- Enable caching on the file system that you are performing compress operations on, as a best practice.

A virtual disk that is added to a compressed virtual machine will not be compressed because it was not present when the compression operation was performed. To compress the new virtual disk, repeat the compression operation on the virtual machine. It is not necessary to decompress the VM first. Only the new, uncompressed virtual disks will be affected by the compression. Virtual disks that are already compressed will be skipped.

Virtual machine compression can be used when archiving gold image virtual machines. The feature does not allow compression of a virtual machine that has or has had working Fast Clones. The solution is to Full Clone the Master virtual machine that has Fast Clones to create a copy of the virtual machine, which can then be compressed and archived.

Compressing a virtual machine decreases the size on disk beyond its nominal size. If you choose to compress a host, cluster, folder, datastore, resource pool, or data center, then the .vmdk files associated with all virtual machines within the selected object will be compressed by the NAS storage platform. The feature does not compress .vswp files.

Note: The compression operation will fail if the storage administrator did not provide DHSM credentials. Compression on VNXe requires ASA access.

1. Right-click the virtual machine to compress.
2. Select EMC > Unified Storage.
3. Select Compress.

![Compress an object](image1.png)

Figure 70  Compress an object

The compress task can be followed in the Recent Tasks pane at the bottom of the page.

![Compression progress](image2.png)

Figure 71  Compression progress

**Note:** If Celerra is not found, the message "Celerra not found for <virtual machine name>" appears. The user must navigate to Home > Solutions and Applications > EMC Celerra to add the Celerra and try again.

4. Right-click EMC > Unified Storage and select Properties to show space usage before and after compression.

**Known issues for compression**

- The compress operation cannot be done on a Version file (a base file that has or has had Fast Clones).
- The compress operation cannot be done on a Branch File (a Fast Clone).
- If compression is run on a file that resides on a file system without AutoExtend enabled and with less than 1 MB of available space, the compress operation will fail with a "No Space" error. The user will be given the option to extend the file system for a successful compression.
Decompress a host, cluster, folder, virtual machine, or data center

Best practices for decompression

Decompressing a virtual machine restores the size on disk to its nominal size before it was compressed. If you decompress a host, cluster, folder, or data center, then the files associated with all virtual machines within the selected object will be decompressed by the NAS storage platform.

**Note:** The decompression operation will fail if the storage administrator did not provide DHSM credentials. Decompression on VNXe requires ASA access.

1. Right-click the compressed virtual machine.
2. Select EMC > Unified Storage.
3. Select Decompress.

**Note:** The Decompress task can be followed in the Recent Tasks pane at the bottom of the page.

Known issues for decompression

When decompressing one or more virtual machines, there must be adequate storage capacity in the NFS datastore. If there is not enough space available, the user is given the option to extend the file system for a successful decompression.

Cloning virtual machines

Fast Clone

Best practices for Fast Cloning virtual machines

Fast Clone is a NAS feature that creates a file-based snapshot of a virtual machine that maintains a relationship with its parent virtual machine.

**Note:** Once a virtual machine has Fast Clones, it can no longer be compressed. Fast Clones are created in the same NFS datastore as the parent VM.

1. Right-click the virtual machine to Fast Clone.

**Note:** Only uncompressed volumes can be Fast Cloned.

**Note:** The Fast Clone operation will fail if the storage administrator did not provide DHSM credentials. Cloning on VNXe requires ASA access.

2. Select EMC > Unified Storage.
3. Select **Fast Clone**. The **Fast Clone** wizard appears.

![Image](image.png)

**Figure 72 Create a Fast Clone**

4. Select the destination for the clone.

5. Click **Next**.

![Image](image.png)

**Figure 73 Clone destination**

6. Complete the fields in the **Clone Details** window.
   
   - The **Clone Count** is the number of clones to create.
Note: If one clone is created, the name will be the Clone Name you specify. If multiple clones are created, they will be numbered. For example, virtual machine X would have clones called X00001, X00002, X00003, and so on.

- **Clone Name** is the name you choose for the clone(s).
- **Add Leading Zeroes to Index** checkbox allows users to decide whether the clones will have leading zeroes in the file names.
- **Number of Digits in Index** field specifies the total number of digits that will be appended to the end of the clone name.
- **Preview** field shows the name of the clones to be created.
- **Customization Specification** provides a dropdown of all customized definitions from the customization specifications manager.
- **Destination NFS Datastore** is the target to store the clones.
- **Automatically Power On** checkbox automatically powers on the virtual machine clone(s).
- **Integrate with Connection Broker** checkbox allows users to integrate desktops with VMware View Manager or Citrix XenDesktop.
- **Max clone count** (to the right of the **Clone Count** field) is the maximum number of clones that can be created as determined by the number of CPU cores on the selected destination. By default, the maximum number of virtual machines per core is 12.

7. **Click** Finish.

---

![Figure 74 Fast Clone details](image)

**Figure 74 Fast Clone details**

Note: You cannot compress a Fast Clone virtual machine or its parent.
The progress of the Fast Clone can be followed in the **Recent Tasks** pane at the bottom of the page.

**Figure 75  Fast Clone progress**

**Known issues for Fast Cloning virtual machines**

Users cannot Fast Clone a virtual machine that is a Fast Clone itself.

Users can create Fast Clones of a gold image virtual machine only on the same file system. Fast cloning across file systems is not allowed.

A gold image virtual machine that has Fast Clones cannot be deleted. Using the "Delete from Disk" option in vCenter on a virtual machine of this nature simply removes the virtual machine from inventory; the .vmdk file associated with the virtual machine is retained and all other files (for example swap, vmx, and so on) are deleted.

A master virtual machine that has Fast Clones cannot be compressed.

**Full Clone**

**Best practices for Full Cloning virtual machines**

The Full Clone feature creates a complete and independent copy of a virtual machine.

**Note:** The Full Clone operation will fail if the storage administrator did not provide DHSM credentials. Cloning on VNXe requires ASA access.

1. Right-click the virtual machine to clone.
2. Select **EMC > Unified Storage.**
3. Select Full Clone.

4. Select a destination for the Full Clone.

5. Click Next.

6. Complete the fields in the **Clone Details** window.
   - **Clone Count** is the number of clones to create.

**Note:** If one clone is created, the name will be the Clone Name you specify. If multiple clones are created, they will be numbered. For example, virtual machine X would have clones called X00001, X00002, X00003, and so on.
- **Clone Name** is the name you choose for the clone(s).
- **Add Leading Zeroes to Index** allows users to decide whether the clones will have leading zeroes in the file names.
- **Number of Digits in Index** specifies the total number of digits that will be appended to the end of the clone name.
- **Preview** shows the name of the clones that will be created.
- **Customization Specification** provides a drop-down list of all customized definitions from the customization specifications manager.
- **Destination NFS Datastore** is the target to store the clones.
- **Automatically Power On** automatically powers on the virtual machine clone(s).
- **Integrate with Connection Broker** allows users to integrate desktops with VMware View Manager or Citrix XenDesktop.
- **Max Clone Count** (to the right of the **Clone Count** field) is the maximum number of clones that can be created as determined by the number of CPU cores on the selected destination. By default, the maximum number of virtual machines per core is 12.

7. Click **Finish**.

![Figure 78 Clone Details](image)

The progress of the Full Clone can be followed in the **Recent Tasks** pane at the bottom of the page.

![Figure 79 Full Clone progress](image)
After each Full Clone is completed, the virtual machine is reconfigured.

**Known issues for Full Cloning virtual machines**

You can only Full Clone to file systems on the same Data Mover.

File systems with auto extend enabled will automatically extend during the Full Clone task if space runs out.

**Integrate Fast Clones with VMware View**

Fast Clone integration with VMware View allows users to add desktops to VMware View pools. Follow the normal Fast Clone steps as shown previously, until you reach the Fast Clone Details dialog box.

1. Select **Integrate with Connection Broker** and then **Integrate with VMware View** to add desktops to VMware View pools.
2. In the **Clone Name** field, type a name for the clone.
3. Optionally, select **Add Leading Zeros to Index**.
4. Click **Next**.

![Integrate Fast Clone with VMware View](image)

**Figure 80** Integrate Fast Clone with VMware View

5. In the **VMware View Server** list box, select a VMware View Server.
6. Select **Add VMs to a new pool** or **Add VMs to Existing Pool**.
   - The **Add VMs to a New Pool** selection allows you to add the virtual machines to a new pool that you create. If you choose this option, you must create a new pool.
   - The **Add VMs to Existing Pool** selection allows you to add the virtual machines to a pool that has already been created.
7. Click **Next**.

![Figure 81 Pool Choice](image1)

8. For a new pool, in the **Unique ID** field, type a unique pool name.

9. Optionally, in the **Display Name** field, type a display name.

10. In the **Desktop Persistence** list box, select **Persistent** or **Non-Persistent**.

11. Click **Next**.

![Figure 82 Pool Name](image2)
12. Complete the new pool settings.

- The **When the VM is not in use** list box provides the following options:
  - Do nothing (VM remains powered on)
  - Always on (Ensure VM is always powered on)
  - Suspend VM
  - Power on VM

- The **Automatic logoff after disconnect** list box provides the following options:
  - Immediately
  - Never
  - After... x minutes after disconnect

- The **Allow users to reset their desktop** checkbox allows users to reset their own desktops.

- The **Default display protocol** field allows users to select either Microsoft RDP or Teradici PC over IP.

- The **Adobe Flash quality** dropdown allows you to select Low, Medium, or High quality.

- The **Adobe Flash throttling** dropdown allows you to select Disabled, Conservative, Moderate, or Aggressive levels of Adobe Flash throttling.

13. Click **Finish**.
Integrate Full Clones with VMware View

Full Clone integration with VMware View allows users to add desktops to VMware View pools. Follow the normal Full Clone steps as shown previously, until you reach the Full Clone Details dialog box.

1. Select Integrate with Connection Broker and then Integrate with VMware View to add desktops to VMware View pools.
2. In the Clone Name field, type a name for the clone.
3. Optionally, select Add Leading Zeroes to Index.
4. Click Next.

![Figure 84 Integrate Full Clone with VMware View](image)

5. In the VMware View Server list box, select a VMware View Server.
6. Select Add VMs to a new pool or Add VMs to Existing Pool.
   - The Add VMs to a New Pool selection allows you to add the virtual machines to a new pool that you create. If you choose this option, you must create a new pool.
   - The Add VMs to Existing Pool selection allows you to add the virtual machines to a pool that has already been created.
7. Click **Next**.

8. For a new pool, in the **Unique ID** field, type a unique pool name.

9. Optionally, in the **Display Name** field, type a display name.

10. In the **Desktop Persistence** list box, select **Persistent** or **Non-Persistent**.

11. Click **Next**.

12. Complete the new pool settings.
   - The **When the VM is not in use** list box provides the following options:
     - Do nothing (VM remains powered on)
Always on (Ensure VM is always powered on)
– Suspend VM
– Power on VM

• The **Automatic logoff after disconnect** list box provides the following options:
  – Immediately
  – Never
  – After... x minutes after disconnect

• The **Allow users to reset their desktop** checkbox allows users to reset their own desktops.

• The **Default display protocol** allows users to select either Microsoft RDP or Teradici PC over IP.

• The **Adobe Flash quality** dropdown allows you to select Low, Medium, or High quality.

• The **Adobe Flash throttling** dropdown allows you to select Disabled, Conservative, Moderate, or Aggressive levels of Adobe Flash throttling.

13. Click **Finish**.

---

**Integrate Fast Clones with Citrix XenDesktop**

Fast Clone integration with XenDesktop allows users to add desktops to XenDesktop Machine Catalogs. Follow the normal Fast Clone steps up to when the **Clone Details** window appears.

1. Select **Integrate with Connection Broker**.
2. Select **Integrate with XenDesktop**.
3. Click **Next**.

4. In the **XenDesktop Controller** list box, select the IP address of a XenDesktop Controller.

5. Select **Add VMs to a New Machine Catalog** or **Add VMs to an Existing Machine Catalog**.

6. To use an existing Machine Catalog, select the Machine Catalog from the list box.

7. Select **Add VMs to a New Desktop Group** or **Add VMs to an Existing Desktop Group**.

8. To use an existing Desktop Group, select the Desktop Group from the list box.
9. Click **Next** or **Finish**.

![Select Machine Catalog and Desktop Group](image)

**Figure 89  Select Machine Catalog and Desktop Group**

10. To create a new Machine Catalog, in the **Machine Catalog Name** field, type a name for the new Machine Catalog.

    **Note:** The USM feature will reject a Machine Catalog name that is the same as a Machine Catalog that already exists, is longer than 64 characters, or uses the following prohibited characters: \/:;#.*?<>\[\]()."

11. In the **Description** field, optionally type a description for the new Machine Catalog.
12. Click **Next** or **Finish**.

![Image](VM_BASE_-_EMC_VSI_for_VMware_vSphere_-_Unified_Storage_Management_-_Fast_Cloning.png)

**Figure 90 Create a new Machine Catalog**

13. To create a new Desktop Group, in the **Desktop Group Name** field, type a name for the new Desktop Group.

**Note:** The USM feature will reject a Desktop Group name that is the same as a Desktop Group that already exists, is longer than 64 characters, or uses the following prohibited characters: \/:.*?=o[()]"{).

14. In the **Display Name** field, optionally type a display name for the new Desktop Group.

**Note:** The USM feature will reject a Desktop Group display name that uses the following prohibited characters: \/:.*?=o[()]"{).

15. In the **Description** field, optionally type a description for the new Group.
16. Click **Finish**.

![Create a new Desktop Group](image)

**Figure 91  Create a new Desktop Group**

### Integrate Full Clones with Citrix XenDesktop

Full Clone integration with XenDesktop allows users to add desktops to XenDesktop Machine Catalogs. Follow the normal Full Clone steps until the **Clone Details** window appears.

1. Select **Integrate with Connection Broker**.
2. Select **Integrate with XenDesktop**.
3. Click **Next**.

![Image of Full Clone Details](image)

**Figure 92** Integrate Full Clone with Citrix XenDesktop

4. In the **XenDesktop Controller** list box, select the IP address of a XenDesktop Controller.

5. Select **Add VMs to a New Machine Catalog** or **Add VMs to an Existing Machine Catalog**.

6. To use an existing Machine Catalog, select the Machine Catalog from the list box.

7. Select **Add VMs to a New Desktop Group** or **Add VMs to an Existing Desktop Group**.

8. To use an existing Desktop Group, select the Desktop Group from the list box.
9. Click **Next** or **Finish**.

![Select Machine Catalog and Desktop Group](image)

**Figure 93  Select Machine Catalog and Desktop Group**

10. To create a new Machine Catalog, in the **Machine Catalog Name** field, type a name for the new Machine Catalog.

    **Note:** The USM feature will reject a Machine Catalog name that is the same as a Machine Catalog that already exists, is longer than 64 characters, or uses the following prohibited characters: \/:#.*?=o[{}\]()’

11. In the **Description** field, optionally type a description for the new Machine Catalog.
12. Click **Next** or **Finish**.

![Create a new Machine Catalog](image)

**Figure 94  Create a new Machine Catalog**

13. To create a new Desktop Group, in the **Desktop Group Name** field, type a name for the new Desktop Group.

   **Note:** The USM feature will reject a Desktop Group name that is the same as a Desktop Group that already exists, is longer than 64 characters, or uses the following prohibited characters: \/*?\\[]()"{}.

14. In the **Display Name** field, optionally type a display name for the new Desktop Group.

   **Note:** The USM feature will reject a Desktop Group display name that uses the following prohibited characters: \/*?\\[]()"{}.

15. In the **Description** field, optionally type a description for the new Group.
16. Click Finish.

![Image](image.png)

**Figure 95  Create a new Desktop Group**

**Refresh desktops**

The refresh operation can be performed on the following objects in vSphere:

- **VM**: The Fast Cloned virtual machine will be refreshed.
- **Host**: All Fast Cloned virtual machines on the host will be refreshed.
- **Cluster**: All Fast Cloned virtual machines in the cluster will be refreshed.
- **Folder**: All Fast Cloned virtual machines in the folder will be refreshed.
- **Data center**: All Fast Cloned virtual machines in the data center will be refreshed.

1. Right-click the object to refresh.
2. Select **EMC > Unified Storage**.
3. Click **Refresh Desktop**.

![Refresh Desktop screenshot](image)

**Figure 96 Refresh a desktop**
CHAPTER 5
Uninstalling EMC VSI for VMware vSphere: Unified Storage Management

This chapter presents this topic:
◆ Uninstall ............................................................................................................... 102
Uninstall

Uninstall EMC VSI for VMware vSphere: Unified Storage Management feature

To uninstall the EMC VSI for VMware vSphere: Unified Storage Management feature from the VSI client, complete the following steps:

1. From the vSphere client Home screen, click EMC. The VSI home window appears.
2. Right-click Unified Storage Management.
3. Click Uninstall.
4. Close vSphere Client.

Note: Uninstalling the Unified Storage Management feature does not uninstall the VSI framework.

Uninstall the EMC Unified Storage Access Control Utility

To uninstall the EMC VSI client, complete the following steps:

1. Navigate to the Control Panel.
2. Double-click Add or Remove Programs.
3. Click Remove on the entry for EMC Unified Storage Access Control for VMware.
4. Click Yes.
CHAPTER 6
Troubleshooting EMC VSI for VMware vSphere: Unified Storage Management

This chapter presents these topics:

◆ Known problems and limitations ................................................................. 104
◆ Logs .................................................................................................................. 111
◆ Technical notes .............................................................................................. 111
◆ EMC Sales and Customer Service contacts ............................................... 112
Known problems and limitations

EMC VSI for VMware vSphere: Unified Storage Management has the following known problems and limitations.

Table 1 Known problems and limitations

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Resolution</th>
</tr>
</thead>
</table>
| ACU uninstall/upgrade issue.                                 | 1. Uninstall the old ACU.  
2. Manually delete the folder: (C:\Program Files (x86)\EMC\Unified Storage Tools for VMware\Access Control Utility)  
3. Install the new ACU package again. |
| When you are provisioning on CLARiiON/VNX block, an error is logged:  “The selected host or hosts not connected to the selected array”  
The USM log shows a similar message:  “EMC.Solutions.VMware.Unified.Engine.Controller - Host sumavihv entry not found in Block Storage System Storage groups.” | Correct the config FQDN for the ESXi host before using USM to do storage provisioning. |
| When creating multiple RDMs on the same VNXe and you start the next RDM creation before the last RDM creation has completed, you may encounter the following error:  “The first created successfully but the second RDM export error message: Can't create ISCSI Resource. And failed to create the second RDM.” | To prevent this from happening, you must guarantee that you cannot create multiple RDMs at the same time. Create the RDM after the previous RDM creation has completed. |
| USM cannot provision VNXe storage to ESX hosts that were previously entered in Unisphere using different hostnames than the hostnames known to the USM. | Delete the manually created generic host record from Unisphere. |
| VSI USM installer does not support downgrade installation. Installing a VSI USM with a lower version than the existing VSI framework or the existing VSI USM feature has an unknown impact on the system. | Do not try this on your system. A downgrade can be done by using uninstall on the higher version first and then proceeding with the installation of the lower version. |
### Table 1  Known problems and limitations

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>After uninstalling the USM using the vSphere Client, trying to uninstall the framework using <strong>add/remove program</strong> in the control panel causes the framework uninstall to fail.</td>
<td>If the uninstall of the framework failed in the control panel, try to uninstall the framework again in the control panel.</td>
</tr>
<tr>
<td>When doing a compression, if the target datastore is a manually created compression that has a datastore path that does not start with &quot;/&quot;, the compression does not succeed.</td>
<td>If the compression functionality is to be used, the target datastore must have a datastore path starting with &quot;/&quot;.</td>
</tr>
<tr>
<td>When an older version of USM is uninstalled using the vSphere Client, the installation of a newer version using USM installer fails with a pop-up window indicating &quot;Error 1720.&quot;</td>
<td>Uninstall the older version of USM using the USM installer.</td>
</tr>
</tbody>
</table>
| On Windows server 2008x64 R2, downgrading from newer VSI USM to an older one might fail with error message: "a newer version is installed..." even when the newer VSI USM was uninstalled using vSphere Client and the VSI framework was uninstalled from OS's Programs and Features program. | Delete register key folders under HKEY_CLASSES_ROOT\Installers\Features that has register key of 'EMC Celerra Plugin'.
Do the following:
1. Run 'Regedit' command.
2. Navigate to HKEY_CLASSES_ROOT\Installers\Features.
3. Right-click on above Features and click **Find** to input "EMC Celerra Plugin."
4. Delete all found register key folders that have register key of "EMC Celerra Plugin." |
| When doing multiple Fast Clone operations on a virtual machine that resides in a VNXe NFS datastore after VSI USM 5.2, and when these operations were triggered concurrently or before previous Fast Clone operations were completed, an error message like the following might be displayed: "Cannot complete the operations because the file or folder <file or folder name> already exists." | When doing multiple Fast Clone operations on a virtual machine that resides in a VNXe NFS datastore on a version of VSI USM after version 5.2, you must wait until a previous Fast Clone operation is completed before starting another Fast Clone operation. |
Troubleshooting EMC VSI for VMware vSphere: Unified Storage Management

Table 1 Known problems and limitations

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Resolution</th>
</tr>
</thead>
</table>
| The Unified Storage Management feature cannot be enabled in the vSphere Client Plug-in Manager. | Complete the following steps to uninstall and reinstall the Unified Storage Management feature:  
  1. In the VSI Feature Manager, right-click the **Unified Storage Management** feature and select **Uninstall** to uninstall the feature.  
  2. Exit the vSphere Client.  
  3. Wait several minutes for the uninstall operation to be completed, and then reinstall the Unified Storage Management feature. |
| Installing the ACU causes previously installed version of the Unified Storage Management feature not to work. | Upgrade the feature to the latest version after installing the ACU. |
| The feature does not install because a previous version exists.          | Delete the **EMC Celerra Plug-in** or the **EMC Unified Storage Plug-in** folder from the directory where the previous version of the plug-in was installed. |
| Previous versions of the EMC Celerra Plug-in for VMware or the EMC Unified Storage Plug-in for VMware cannot be installed after uninstalling the EMC VSI for VMware vSphere: Unified Storage Management feature. | Manually remove EMC VSI for VMware vSphere: Unified Storage Management from the registry of the Windows client, and attempt to install the previous version of the plug-in again. |
| The USM feature does not uninstall from the vSphere Client if the vSphere Client is not run with administrator privileges. | Exit and restart the vSphere Client. Right-click the vSphere Client icon on the desktop and then select **Run as administrator**. |
| “Could not connect to File Storage System <IP_address>” error message appears when adding VNX file credentials. | The VNX Control Station does not recognize Unisphere usernames. Add the VNX again using a valid Control Station SSH username. |
| Feature does not load in vSphere Client.                                | Remove quotes from the system path and restart the vSphere Client, as shown in “Remove quotes from system path” on page 17. |
| The feature displays an error message when attempting to remove a VNX from the list of available storage systems in environments where the feature was installed at the same time as the VSI: Storage Viewer feature. | Attempt to remove the VNX again. |
Troubleshooting EMC VSI for VMware vSphere: Unified Storage Management

Table 1 Known problems and limitations

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The feature returns a “Could not add IPs to VNXe host system” message when attempting to provision storage on a VNXe.</td>
<td>This problem occurs when a single ESX host has multiple host records in Unisphere. To resolve the problem, delete from Unisphere all host records that refer to the same ESX host by either hostname or IP address. Do not delete ESX host records that were added to Unisphere Hosts &gt; VMware window by using the Find ESX Host Wizard. Instead, click Refresh on the Unisphere Hosts &gt; VMware window to ensure that the host record includes all IP addresses currently configured on the host.</td>
</tr>
<tr>
<td>Provisioning NFS datastore fails on VNXe.</td>
<td>The maximum capacity reported by the VNXe is incorrect. Use Unisphere to view the correct maximum capacity available for an NFS datastore.</td>
</tr>
<tr>
<td>VNXe fails to create an RDM volume immediately following the creation of a previous RDM volume.</td>
<td>The creation of the previous RDM volume is not complete. Wait for the previous operation to complete, and create the RDM volume again.</td>
</tr>
<tr>
<td>Provisioning VMFS datastore using maximum capacity fails on CLARiiON and VNX block.</td>
<td>The maximum capacity reported by the CLARiiON or VNX block system is not the actual space available. The true maximum size is not reported by Unisphere. Try again using a smaller capacity.</td>
</tr>
<tr>
<td>The feature displays an error message about an invalid license when attempting to provision storage on a VNXe.</td>
<td>Verify the status of the VNXe license, and attempt the provisioning operation again.</td>
</tr>
<tr>
<td>Extend shared folder server fails on VNXe.</td>
<td>The maximum capacity reported by the VNXe is incorrect. Use Unisphere to extend shared folder servers on VNXe.</td>
</tr>
<tr>
<td>Unable to compress virtual machine that had Fast Clones.</td>
<td>Full Clone the virtual machine and compress the Full Clone; then delete the original virtual machine.</td>
</tr>
<tr>
<td>“The operation is not allowed in the current state“ error when performing a Full Clone with XenDesktop integration.</td>
<td>Retry the cloning operation.</td>
</tr>
<tr>
<td>“Thread is being aborted“ error message when closing vSphere Client.</td>
<td>Ensure that all feature tasks are complete before closing the vSphere Client.</td>
</tr>
<tr>
<td>A virtual machine appears on a different host in the same cluster after a refresh operation.</td>
<td>This is an expected behavior of the VMware environment.</td>
</tr>
</tbody>
</table>
### Table 1  Known problems and limitations

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual machines perform poorly.</td>
<td>Verify that all NAS Data Mover network interfaces are in the same subnet as the ESX servers that are hosting the virtual machines.</td>
</tr>
<tr>
<td>Networking does not work in a virtual machine.</td>
<td>Ensure there are sufficient ports on the ESX server vSwitch to accommodate the virtual machines that are powered on.</td>
</tr>
<tr>
<td>Provision Storage produces an error “Error during the configuration of the host: Cannot open volume.”</td>
<td>Restart the ESX host and try again.</td>
</tr>
<tr>
<td>After booting the NAS Control Station, feature operation receives error message: “The remote server returned an error: (500) Internal Server Error.”</td>
<td>Wait for 15 minutes for NAS services to start and try again.</td>
</tr>
<tr>
<td>Error when right-clicking after disabling feature in vSphere Client.</td>
<td>Restart the vSphere Client and try again.</td>
</tr>
<tr>
<td>Feature right-click menus do not appear in vSphere Client after installation.</td>
<td>Load the vSphere Client. Select Plug-ins &gt; Manage Plug-ins. Right-click EMC Virtual Storage Integrator (VSI) for vSphere and select Enable.</td>
</tr>
<tr>
<td>Receive the error message “Could not customize VM with spec because fault.CustomizationPending. summary.”</td>
<td>Users cannot apply a Customization Specification to a Full Clone or Fast Clone whose parent virtual machine already has a Customization Specification applied; this operation fails because it is not supported by VMware.</td>
</tr>
<tr>
<td>Not able to run compression or create Fast Clones or Full Clones.</td>
<td>DHSM is incorrectly set up on Celerra or VNX. “DHSM/ASA setup instructions” on page 18 provides instructions for proper setup of DHSM.</td>
</tr>
<tr>
<td>Celerra or VNX fails to complete parallel provision operations.</td>
<td>This is expected because the file system table is locked during a provision operation, thereby preventing a parallel provision operation.</td>
</tr>
<tr>
<td>Feature does not connect to the storage array.</td>
<td>Run the following command from the CLI: Naviseccli -removeusersecurity</td>
</tr>
<tr>
<td>LUN ownership may not be set correctly on LUNs provisioned after changing the failover mode on the ESX server.</td>
<td>Reboot the ESX server and change the LUN ownership to the correct SP.</td>
</tr>
</tbody>
</table>
### Table 1  Known problems and limitations

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The feature reports &quot;The selected operation is only supported on EMC Unified Storage datastores&quot; or &quot;The storage system for datastore &lt;datastore name&gt; was not found&quot; when attempting to view the properties of a VMFS datastore or a virtual machine residing on a VMFS datastore.</td>
<td>There are two possible causes: 1. The virtual machine or datastore does not reside on Unified Storage. The plug-in should not be used to obtain properties on a datastore or virtual machine that does not reside on Unified Storage. 2. The array where the newly provisioned storage is located has been removed from the feature. Add the array again, and retry the operation.</td>
</tr>
<tr>
<td>Newly created LUNs are not visible to the ESX host and new datastores are not created.</td>
<td>The ESX host adapters may be disabled, or the static targets may have been removed. Re-enable the host adapters, re-create the static targets, and attempt to provision the storage again.</td>
</tr>
<tr>
<td>When cloning an NFS datastore with Virtual Provisioning enabled, the feature reports that there is insufficient space to complete the operation.</td>
<td>Wait 10 minutes and start another cloning operation to complete the remaining clones.</td>
</tr>
<tr>
<td>The vSphere Client crashes when provisioning block storage.</td>
<td>There are three potential causes for this issue: • NaviSecCLI was not installed to the default path. Run naviseccli -help from the vSphere Client command prompt. If the command is not recognized, reinstall NaviSecCLI. • An incorrect password was set when the array was added to the feature. Correct the password and attempt to provision the storage again. • No RAID groups or Pools are defined on the array. Create RAID groups or Pools on the array and attempt to provision the storage again.</td>
</tr>
<tr>
<td>Block provisioning fails when binding LUNs on R30 pools if LUN ownership is set to auto.</td>
<td>Select the SP to which the LUN should be assigned.</td>
</tr>
<tr>
<td>The active step in the provisioning wizard is not displayed in the list of steps in the left-hand pane of the wizard.</td>
<td>This issue does not impact the functionality of the provisioning wizard.</td>
</tr>
<tr>
<td>Before setting the maximum capacity while provisioning an NFS datastore, the feature warns &quot;Initial capacity must be smaller than max capacity.&quot;</td>
<td>This issue does not impact the functionality of the provisioning wizard.</td>
</tr>
<tr>
<td>The feature reports that it cannot find a datastore, host, or virtual machine in the VMware vCenter Server database.</td>
<td>Exit the operation you are attempting to perform and restart it.</td>
</tr>
</tbody>
</table>
When provisioning NFS storage on an existing NFS export, the feature may display more NFS exports than are displayed in Unisphere.

The additional NFS exports displayed by the feature were unexported but not permanently removed from NAS_DB on the storage system.

Provisioning a block datastore with the size set to the maximum capacity fails because of insufficient free space.

There is not enough free space in the storage pool for the LUN and the required LUN metadata. Retry the provisioning operation with a smaller LUN size.

The feature crashes when trying to cancel CLARiiON provisioning if the table of available storage pools is still loading.

Wait for the table of available storage pools to load completely before clicking Cancel.

The feature displays an error message when attempting to view the properties for, or extend a VMFS datastore on, an EMC CLARiiON if a CLARiiON that is no longer available remains in the storage systems list.

Remove the unavailable CLARiiON from the storage systems list, and attempt to view the properties or extend the datastore again.

The feature displays an exception when you attempt to add a XenDesktop Controller, add a virtual machine to a XenDesktop Controller, or refresh or clone a virtual machine that is registered with XenDesktop.

XenDesktop requires users to have domain administrator privileges and access the vSphere Client as an administrator. Verify that these privileges are in place and attempt the operation again.

The feature displays an error message saying “A newer version is installed…” even if all the VSI products are cleanly uninstalled and files/folders removed.

There are two possible solutions to this problem:

- Run the following command in the Windows Command Prompt to clear the DNS cache:
  `ipconfig/flushdns`
- As a Windows administrator, run the following command in the Windows Command Prompt to enable the listener for the Windows Remote Management service and open an exception in the firewall for the port:
  `winrm -quickconfig`

USM compression fails when a datastore is mounted manually without a “/” at the beginning of the export path for VNX and VNXe file storage systems.

Unmount the datastore, and remount it with a ‘/’ at the beginning of the export path. Additional storage side configurations might be necessary to get the correct export path.
Logs

The log file for EMC VSI for VMware vSphere: Unified Storage Management can be viewed in the VSI log viewer.

1. Navigate to Home > Solutions and Applications > EMC.
2. Click Logging in the Settings pane.

Technical notes

The EMC VSI for VMware vSphere: Unified Storage Management feature adheres to the limits defined by VMware in the document titled Configuration Maximums VMware vsphere 5.0 (or Configuration Maximums VMware vsphere 5.1), which is available on the VMware website:

http://www.vmware.com

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>USM datastore extend failed on VNXe file storage that is created manually in the Unisphere interface that has an NFS share name different than the NFS Shared folder name.</td>
<td>Manually created NFS shares in the Unisphere interface are not fully supported from VSI USM. Provision datastore through the VSI USM interface and proceed with other operations such as datastore extension.</td>
</tr>
<tr>
<td>The feature displays an error message “Could not find valid software header for entry” when you are adding VNX credentials after installing the feature with Navisphere CLI 7.32.</td>
<td>Uninstall Navisphere CLI and reinstall it, with the verification level set to “Low” during the reinstallation.</td>
</tr>
<tr>
<td>When provisioning storage on VMAX 10K and VMAX 20K in a VMware vSphere 4.x environment, you receive errors like “Failed to create datastore...” or “Verify that iSCSI LUN naa....”</td>
<td>This error happens less frequently in VMware vSphere 5.x environments. Upgrade to VMware vSphere 5.x if this error is critically impacting your environment.</td>
</tr>
<tr>
<td>When you try to extend a renamed VMFS datastore that resides on a VMAX storage array, the extend operation fails, producing the following error: “The storage system for datastore ... was not found. Probable causes are 1) the datastore does not reside on EMC Unified Storage or 2) the EMC Unified Storage System is not yet added.”</td>
<td>USM does not support extension of a renamed VMAX datastore; in USM 5.4, as a workaround, change the datastore name back to the name used in the provisioning process.</td>
</tr>
</tbody>
</table>
If you want to extend the size of your gold image virtual machine, you must extend the gold image datastore with the desired size and increase the hard disk size of the virtual machine in the virtual machine settings.

For maximum performance, run vSphere Client on the same network as the vCenter Server and/or storage system.

The feature does not support Celera Nested Mount File Systems (NMFS).

Compression is not supported for virtual machines protected by VMware Fault Tolerance.

Fast Clones are not supported for virtual machines protected by VMware Fault Tolerance.

Celerra or VNX file system names and mount paths with special characters are not supported by the feature.

EMC Sales and Customer Service contacts

For EMC VSI for VMware vSphere: Unified Storage Management support, review the application-specific Help files or Product Guide. If the documentation does not address your question, and if you have a valid EMC service contract, contact EMC Customer Support at:

- United States: 1-800-782-4362 (SVC-4EMC)
- Canada: 1-800-543-4782 (543-4SVC)
- Worldwide: +1-508-497-7901

Include the following information in your support request:

- Type of hardware, including any network hardware, if applicable.
- Operating system.
- Exact wording or screenshots of any messages that appeared on the screen.
- Complete description of the issue, including action taken prior to the incident.
- Log file(s) from the following path (non-64-bit Windows operating systems): \Program Files\VMware\Infrastructure\Virtual Infrastructure Client\Plugins\EMC Unified Storage\log
- Log file(s) from the following path (64-bit Windows versions): \Program Files (x86)\VMware\Infrastructure\Virtual Infrastructure Client\Plugins\EMC Unified Storage\log
- Troubleshooting steps.

EMC product and licensing information can be obtained as follows:

**Product information:** For documentation, release notes, software updates, or for information about EMC products, licensing, and service, go to https://support.emc.com.
APPENDIX A
Parameters within the EMC VSI for VMware vSphere: Unified Storage Management Configuration File

This appendix presents these topics:

- Configuration file name and location ................................................................. 114
- Parameters within the configuration file ......................................................... 114
Parameters within the EMC VSI for VMware vSphere: Unified Storage Management Configuration File

**Configuration file name and location**

EMC VSI for VMware vSphere: Unified Storage Management stores the configuration file at the following location:

\AppData\Roaming\EMC\Unified Storage\Config\unified_plugin.ini

**Parameters within the configuration file**

**HostNfsMaxVolumes_ESX3**
- Default = 32
- The maximum number of NFS datastores that can be mounted on an ESX server with version 3.x. This value is dictated by VMware. If an ESX server has a lesser value set and has maxed out its NFS mounts, then the plug-in will automatically increase the NFS.MaxVolumes parameter on the ESX server to this value.

**HostNfsMaxVolumes_ESX4**
- Default = 64
- The maximum number of NFS datastores that can be mounted on an ESX server with version 4.x. This value is dictated by VMware. If an ESX server has a lesser value set and has maxed out its NFS mounts, then the plug-in will automatically increase the NFS.MaxVolumes parameter on the ESX server to this value.

**HostNfsMaxVolumes_ESX5**
- Default = 256
- The maximum number of NFS datastores that can be mounted on an ESX server with version 5.x. This value is dictated by VMware. If an ESX server has a lesser value set and has maxed out its NFS mounts, then the plug-in will automatically increase the NFS.MaxVolumes parameter on the ESX server to this value.

**HostVmfsMaxVolumes_ESX**
- Default = 256
- This is the maximum VMFS type datastore that can be created on an ESX host.

**HostTcpIpHeapSize_ESX3**
- Default = 30
- When a datastore is provisioned by the plug-in, the plug-in checks the Net.TcpipHeapSize setting. If it does not equal this value, then the plug-in will display a message to the user indicating that they should change the setting and reboot their ESX server.
Parameters within the configuration file

HostTcpIpHeapSize_ESX4

- Default = 32
- When a datastore is provisioned by the plug-in, the plug-in checks the Net.TcpipHeapSize setting. If it does not equal this value, then the plug-in will display a message to the user indicating that they should change the setting and reboot their ESX server.

HostTcpIpHeapSize_ESX5

- Default = 32
- When a datastore is provisioned by the plug-in, the plug-in checks the Net.TcpipHeapSize setting. If it does not equal this value, then the plug-in will display a message to the user indicating that they should change the setting and reboot their ESX server.

HostTcpIpHeapMax_ESX3

- Default = 120
- When a datastore is provisioned by the plug-in, the plug-in checks the Net.TcpipHeapMax setting. If it does not equal this value, then the plug-in will display a message to the user indicating that they should change the setting and reboot their ESX server.

HostTcpIpHeapMax_ESX4

- Default = 128
- When a datastore is provisioned by the plug-in, the plug-in checks the Net.TcpipHeapMax setting. If it does not equal this value, then the plug-in will display a message to the user indicating that they should change the setting and reboot their ESX server.

HostTcpIpHeapMax_ESX5

- Default = 128
- When a datastore is provisioned by the plug-in, the plug-in checks the Net.TcpipHeapMax setting. If it does not equal this value, then the plug-in will display a message to the user indicating that they should change the setting and reboot their ESX server.

DHSMTTimeout

- Default = 86400000
- This value represents the amount of time in milliseconds that the feature will wait for a DHSM request before timing out. DHSM requests are sent to the Data Mover for the cloning, compression, and properties features of the feature.

HttpTimeout

- Default = 0 (infinite)
- This value represents the amount of time in milliseconds that the plug-in will wait for an HTTP request before timing out. HTTP requests are sent to the Celerra or VNX Control Station for all features of the plug-in.
PingTimeout

- Default = 5000
- When the user adds a Celerra or VNX for file to the plug-in, the plug-in will first ping the network address that has been input by the user to verify that it exists. This value represents the ping timeout in milliseconds.

HostHeartbeatFrequency

- Default = 12
- When the user provisions a datastore with the plug-in and leaves the “Set Timeout Settings” box checked on the “Advanced” dialog, the plug-in will set the NFS.HeartbeatFrequency value on the ESX server to this value (if it is not already set).

HostHeartBeatMaxFailures

- Default = 10
- When the user provisions a datastore with the plug-in and leaves the “Set Timeout Settings” box checked on the “Advanced” dialog, the plug-in will set the NFS.HeartbeatMaxFailures value on the ESX server to this value (if it is not already set).

HostHeartBeatDelta

- Default = 5
- When the user provisions a datastore with the plug-in and leaves the “Set Timeout Settings” box checked on the “Advanced” dialog, the plug-in will set the NFS.HeartbeatDelta value on the ESX server to this value (if it is not already set).

HostHeartBeatTimeout

- Default = 5
- When the user provisions a datastore with the plug-in and leaves the “Set Timeout Settings” box checked on the “Advanced” dialog, the plug-in will set the NFS.HeartbeatTimeout value on the ESX server to this value (if it is not already set).

DatastoreNameMaxLength

- Default = 42
- The maximum length allowed for the datastore name when the user provisions a datastore with the plug-in.

MaxNumberOfVmsPerCore

- Default = 12
- This value is used to calculate the maximum number of clones that can be assigned to a host or cluster. If a user is fast or full cloning a VM to a destination host or cluster, the plug-in will determine how many cores are in the host/cluster and multiply that by this value to determine the maximum number of clones for that destination.
HttpRetries
- Default = 10
- If a plug-in HTTP request fails, it auto-retries a number of times as specified by this value. HTTP requests are sent to the Celerra or VNX Control Station for every feature of the plug-in.

MaxFileSystemSizeMB
- Default = 16769024
- The maximum Celerra or VNX file system size in megabytes. This value is dictated by EMC.

MinFileSystemSizeMB
- Default = 3
- This is the minimum size that VSI USM will display in the list of storage pools when creating new NFS typed datastore for VNX and Celerra. Storage pools will not be displayed if their available capacity is smaller than this size.

MinSharedFolderSizeMB
- Default = 10240
- This is the minimum size of an NFS-typed shared folder server on VNXe. It impacts the minimum size of a NFS datastore that can be created on VNXe. This value will be checked when user input the NFS datastore size in the VSI USM provision wizard for VNXe. If the user input a smaller value, the wizard will not be able to proceed with any consequent steps.

HighWaterMarkMin
- Default = 50
- The minimum file system high watermark percentage that is allowed by Celerra or VNX. This value is dictated by EMC.

HighWaterMarkMax
- Default = 99
- The maximum file system high watermark percentage that is allowed by Celerra or VNX. This value is dictated by EMC.

DefaultHighWaterMark
- Default = 90
- The default high watermark percentage for Celerra or VNX file systems with virtual provisioning enabled on the "Advanced" dialog when provisioning a datastore in the plug-in.

CreateFileSystemTimeout
- Default = 240000
- The timeout for storage provisioning and extension tasks in milliseconds.
Parameters within the EMC VSI for VMware vSphere: Unified Storage Management Configuration File

LogLevel
- Default = Info
- Specifies the type of messages that get logged. Options are:
  1. Error
  2. Info
  3. Debug

NeoCIMXMLPort
- Default = 5958
- This is a deprecated setting, which is no longer valid for the current VSI USM. However, it is referenced in the storage profile for VNXe. "DO NOT" change the value of this field. Storage profiles breakage is expected with any new value other than the default value.

CustomizeScsiLunDisplayName
- Default = True
- Specifies whether VMFS datastores and RDM volumes are displayed with friendly device names. Options are:
  1. True
  2. False