Veritas™ Cluster Server One
Installation and Configuration Guide

Windows

5.0 Service Pack 2
Veritas Cluster Server One
Installation Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Product version: 5.0 Service Pack 2
Document version: 5.0.SP2.0

Legal Notice
Copyright © 2011 Symantec Corporation. All rights reserved.
Symantec, the Symantec Logo, Veritas, and Veritas Storage Foundation are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party (“Third Party Programs”). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice file accompanying this Symantec product for more information on the Third Party Programs.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.
Technical Support

Symantec Technical Support maintains support centers globally. Technical Support’s primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec’s maintenance offerings include the following:
- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers automatic software upgrade protection
- Global support that is available 24 hours a day, 7 days a week
- Advanced features, including Account Management Services

For information about Symantec’s Maintenance Programs, you can visit our Web site at the following URL:
www.symantec.com/techsupp

Contacting Technical Support

Customers with a current maintenance agreement may access Technical Support information at the following URL:
http://www.symantec.com/business/support/assistance_care.jsp

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:
- Product release level
- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/techsupp

Customer service

Customer service information is available at the following URL:

www.symantec.com/techsupp

Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and maintenance contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals
Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan
Asia-Pacific and Japan
customercare_apac@symantec.com

Europe, Middle-East, and Africa
Europe, Middle-East, and Africa
semea@symantec.com

North America and Latin America
North America and Latin America
supportsolutions@symantec.com

Documentation

Your feedback on product documentation is important to us. Send suggestions for improvements and reports on errors or omissions. Include the title and document version (located on the second page), and chapter and section titles of the text on which you are reporting. Send feedback to:

docs@symantec.com

About Symantec Connect

Symantec Connect is the peer-to-peer technical community site for Symantec’s enterprise customers. Participants can connect and share information with other product users, including creating forum posts, articles, videos, downloads, blogs and suggesting ideas, as well as interact with Symantec product teams and Technical Support. Content is rated by the community, and members receive reward points for their contributions.

http://www.symantec.com/connect/storage-management
Chapter 1  VCS One installation overview

VCS One architecture .................................................................12
Physical components of the VCS One cluster ...............................12
Shared storage in the VCS One cluster ......................................13
VCS One global clusters ............................................................14
Where to go for VCS One client configuration instructions ..........15
About installing VCS One on Windows ........................................15
About installing the VCS One agents ........................................16
About VCS One license keys ........................................................17
About the VCS One Product Authentication Service ....................17
   Removing earlier versions of the Symantec Product Authentication Service .........................................................17

Chapter 2  Installing and configuring the VCS One Policy Master on Windows

Setting up the VCS One cluster on Windows ...............................20
Preparing for installing the Policy Master on Windows ..................21
Required ports and firewall settings ............................................21
Installing the Policy Master on Windows .......................................23
   Installing the Policy Master using the installation wizard ..........23
   Installing the Policy Master using the command line ................25
About Policy Master configuration on Windows .........................27
Prerequisites for configuring the Policy Master on Windows ........28
Configuring the Policy Master on Windows .................................29
After you install and configure the Policy Master .........................31
   Verifying the Policy Master configuration on Windows ..........32
   Backing up the VCS One Product Authentication Service........33
      Service configuration .........................................................33
   Adding multiple network paths between the Policy Master and client systems .......................................................34
      Configuring global clustering .........................................34
      VCS One web console ....................................................35
      Web console prerequisites ..............................................35
   Setting who can access the VCS One web console ................35
   Accessing the VCS One web console .....................................36
Chapter 3  Installing and configuring the VCS One client

About installing and configuring the clients .................................................. 40
Preparing to install the VCS One client ...................................................... 40
General preparations ............................................................................... 40
Windows specific preparations ............................................................... 41
ESX-specific preparations ..................................................................... 41
ESXi-specific preparations .................................................................... 42
Installing the VCS One client on a Windows Server ........................... 42
Installing the VCS One client using the client installer .................... 43
Installing the client on Windows using the command line .................. 44
Before you install the VCS One client on Server Core ....................... 45
Parameters for setup.exe ..................................................................... 45
Installing the VCS One client on an ESX and ESXi Server .................. 46
Installing a Control node ....................................................................... 46
Launching the installer ......................................................................... 47
Specifying the target systems .............................................................. 47
Reviewing the package list ................................................................... 48
Configuring the client systems with a Policy Master Server
  on Windows ......................................................................................... 49
Before you configure the client systems .............................................. 49
Configuring the Windows client systems .......................................... 50
Configuring the ESX client systems ................................................... 52
  Configuring the ESX client systems using the wizard .................... 52
  Configuring the ESX client systems using CLI .............................. 54
Adding and configuring the virtual machines (vframes)
  with the Policy Master Server ....................................................... 56
Configuring the Windows client systems with a Policy Master Server
  on Unix .......................................................................................... 56
Before you configure the client systems ............................................. 56
Configuring the client systems .......................................................... 57

Chapter 4  Installing the Simulator

About the Simulator ............................................................................. 60
Before you install the Simulator ......................................................... 60
Installing the Simulator ..................................................................... 60

Chapter 5  Uninstalling VCS One software

About uninstalling the VCS One Policy Master .................................... 64
Preparing to uninstall the VCS One Policy Master .............................. 64
Uninstalling the VCS One Policy Master ............................................. 65
Chapter 1

VCS One installation overview

This chapter includes the following topics:

- VCS One architecture
- Where to go for VCS One client configuration instructions
- About installing VCS One on Windows
- About installing the VCS One agents
- About VCS One license keys
- About the VCS One Product Authentication Service
VCS One architecture

This section provides a high-level overview of the VCS One architecture.

Physical components of the VCS One cluster

VCS One uses a client-server architecture to provide a scalable and highly-available application management solution. The VCS One cluster consists of the following physical systems:

- **Policy Master systems** manage the VCS One cluster. These systems are the server in the client-server architecture. Symantec recommends that you do not use these systems to host managed applications. You need at least two Policy Master systems to ensure high availability.

- **Client systems** host managed applications. These systems host the managed applications and the virtual machines under the control of VCS One.

- **Redundant TCP/IP network connections** between the Policy Master and client systems.

Client systems that run different operating systems can co-exist inside the same VCS One cluster. Each system is connected to networking hardware.
Shared storage in the VCS One cluster

This section gives an overview of the VCS One storage architecture for the Policy Master and client systems.

- The Policy Master requires shared storage in a production environment. The shared storage must be Network Attached Storage (NAS) or Storage Area Network (SAN).
- The client systems can use shared storage (recommended) or local storage. If the client systems use shared storage, NAS, SAN, or other shared storage architectures are available. If your client systems use local storage, you can start, stop, or get status on the managed applications running on the client systems, but the managed applications do not fail over.
VCS One global clusters

A VCS One global cluster links the individual VCS One clusters at separate sites, and enables wide-area failover for the applications that you configure.

A VCS One global cluster consists of the following components:

- Local VCS One clusters. Local clustering provides local failover within a site.
- Local service groups (SGs). A service group contains all the hardware resources and software resources required to run a managed application. Service groups allow VCS One to control all the resources of the managed application as a single unit. When a failover occurs in VCS One, the entire service group fails over as a unit.
- Composite service groups (CSGs). A CSG is a collection of service groups. A composite service group can be local or global. A global composite service group is the unit of failover among different VCS One clusters.
- Replicated storage. Storage is replicated among global clusters so that both clusters can access the application and data files needed to enable replication and failover operations.
Where to go for VCS One client configuration instructions

The installation guide you reference for client installation and configuration instructions varies depending on your configuration.

<table>
<thead>
<tr>
<th>Client platform</th>
<th>Policy Master platform</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>UNIX, ESX, or ESXi</td>
<td>UNIX</td>
<td><em>Veritas Cluster Server One Installation Guide</em> AIX, ESX, HP-UX, Linux, Solaris, Windows</td>
</tr>
<tr>
<td>Windows</td>
<td>UNIX</td>
<td>“Installing and configuring the VCS One client” on page 39</td>
</tr>
<tr>
<td>Windows, ESX or ESXi</td>
<td>Windows</td>
<td>“Installing and configuring the VCS One client” on page 39</td>
</tr>
</tbody>
</table>

About installing VCS One on Windows

Installing Veritas Cluster Server (VCS) One with a Windows Policy Master involves the following procedures:

- Setting up the Policy Master and client system hardware
- Setting up the network communications among systems
- Installing and configuring the VCS One Policy Master and verifying the installation
- Connecting the VCS One client systems to the Policy Master cluster using the public network
- Installing and configuring the VCS One client software on client systems
- Installing the agents
- Installing the Simulator (optional)
About installing the VCS One agents

In addition to the agents that are bundled with the product, VCS One provides agents for the management of key enterprise applications. These agents start, stop, and monitor the corresponding resources and report state changes. The high availability agents are located on the Veritas High Availability Agent Pack software disc that is included with VCS One. The Agent Pack disc contains the currently shipping agents and is released quarterly to add new agents. See the following documentation available on the Agent Pack disc:

- For an overview of the supported high availability agents, read the *Veritas High Availability Agent Pack Getting Started Guide*.
- For installation instructions, read the agent installation and configuration guides.
About VCS One license keys

VCS One is a licensed product. You can embed a VCS One license key on your system, or enter it when you install the product.

On Windows, the Policy Master installation installs a permanent embedded license key by default.

Table 1-3 lists the embedded VCS One license key types.

<table>
<thead>
<tr>
<th>VCS One license key type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Evaluation</td>
<td>Permanent</td>
</tr>
</tbody>
</table>

Table 1-3 VCS One embedded license key types

About the VCS One Product Authentication Service

VCS One Product Authentication Service provides that issue credentials. These brokers allow trusted communications between users and processes on the Policy Master systems and client systems. All VCS One environments require the VCS One Product Authentication Service for trusted communications. The VCS One Product Authentication Service is installed when you install VCS One.

VCS One uses an embedded broker model where the root broker and authentication broker are always running on the active Policy Master system. The VCS One Product Authentication Service issues credentials to the Policy Master, the VCS One client processes, and all users in the VCS One cluster.

VCS One Product Authentication Service supports third-party private domain repositories, such as LDAP and Active Directory.

Removing earlier versions of the Symantec Product Authentication Service

If you have an earlier version of the Symantec Product Authentication Service left behind from a previous VCS One Policy Master installation, remove it before reinstalling VCS One. The VCS One Product Authentication Service is installed when you install VCS One. In addition, on the VCS One for Windows Policy Master systems, along with the VCS One Product Authentication Service, a version of the Symantec Product Authentication Service is installed. This service is used by the Windows Policy Master components.
VCS One installation overview

About the VCS One Product Authentication Service
Installing and configuring the VCS One Policy Master on Windows

This chapter includes the following topics:

■ Setting up the VCS One cluster on Windows
■ Preparing for installing the Policy Master on Windows
■ Installing the Policy Master on Windows
■ About Policy Master configuration on Windows
■ Prerequisites for configuring the Policy Master on Windows
■ Configuring the Policy Master on Windows
■ After you install and configure the Policy Master
■ VCS One web console
Setting up the VCS One cluster on Windows

The Policy Master cluster systems manage the client systems in the VCS One cluster. These systems are the server in the client-server architecture. Each physical cluster system is connected to networking hardware. A physical cluster system usually is connected to storage hardware as well.

The following is an overview of the process of setting up the VCS One cluster hardware.

**To set up the Policy Master in a production environment**

1. For the Policy Master cluster, select two to four Windows systems that meet the hardware and software server requirements for VCS One.
   - At least 2 gigabyte physical memory (for use by VCS One).
   - SCSI, Fibre Channel, iSCSI host bus adapters (HBAs), or iSCSI Initiator supported NICs to access shared storage.
   - At least two network interfaces (NICs) are required for private communication between the Policy Master cluster systems in a production environment. NIC teaming on the private NICs is not supported on the Policy Master cluster.
   - At least one network link between the Policy Master and the VCS One VCS One cluster system (also known as client systems); two links are preferable.

   For complete system requirements, refer to the *Veritas Cluster Server One Release Notes*.

2. Connect the TCP/IP network to the client systems.

3. Use the ping utility to test the network connections.

4. Select the storage device for the Policy Master configuration database. The device will be shared between the two systems.
Preparing for installing the Policy Master on Windows

To prepare for installing the Policy Master on Windows, ensure that you have met all prerequisites. For system requirements, refer to the Veritas Cluster Server One Release Notes.

Before you install the VCS One Policy Master ensure that you perform the following pre-installation tasks on all the systems where you plan to install the Policy Master:

- Install any required operating system patches. See the Veritas Cluster Server One Release Notes for the required operating systems patches.
- Ensure that all the systems run the same operating system, service pack level, and system architecture.
- Ensure that the operating system is identically installed on all the systems.
- Ensure that the Remote Registry and Windows Management Instrumentation (WMI) services are set to automatic and running (the default setting). You can confirm the status of Windows services by opening the Services console (run services.msc).
- For remote installation on Windows Server 2008 systems, ensure that the Computer Browser Service is set to automatic and running.
- Ensure that you have adjusted your firewall settings such that the specific ports needed for installing the VCS One Policy Master are enabled and required programs are added to the exceptions list. See “Required ports and firewall settings” on page 21.
- Ensure that you have network access and that you are a member of the Local Administrators group and a domain user for all nodes where you are installing. All systems must be part of the same domain.

After installation is complete, you must configure the Policy Master. There are additional prerequisites for configuration. See “Prerequisites for configuring the Policy Master on Windows” on page 28.

Required ports and firewall settings

The VCS One Windows Policy Master systems require access to certain ports for services used during configuration, operation, or administration of the Policy Master.

If you have configured the Windows firewall, ensure that the firewall settings allow access to these services or ports. In addition, ensure that ICMP, Windows
Management Instrumentation (WMI) service, and file and print sharing are included in the firewall exceptions list. For Policy Master configuration, ensure that the firewall settings enable the Policy Master systems to ping each other successfully.

Table 2-2 displays the services and ports to open, depending on whether the host system is the Policy Master, client, or Simulator system. You must ensure the required ports are open before installing VCS One on that system. For example, for installation on Policy Master systems, open all ports listed on the table rows that show the Policy Master as the host system.

<table>
<thead>
<tr>
<th>Host system</th>
<th>VCS One components</th>
<th>Port to open on host system</th>
<th>Outbound/inbound port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Master</td>
<td>Policy Master service</td>
<td>14151</td>
<td>Inbound</td>
</tr>
<tr>
<td>Policy Master</td>
<td>Policy Master configuration database</td>
<td>14157</td>
<td>Not modifiable</td>
</tr>
<tr>
<td>Policy Master</td>
<td>Web server</td>
<td>14171 (secure)</td>
<td>Inbound</td>
</tr>
<tr>
<td>Policy Master</td>
<td>Web server admin port</td>
<td>14172</td>
<td>Inbound</td>
</tr>
<tr>
<td>Policy Master</td>
<td>Root broker and authentication broker</td>
<td>14159</td>
<td>Inbound and outbound</td>
</tr>
<tr>
<td>Policy Master</td>
<td>Veritas Enterprise Administrator (VEA) Server</td>
<td>2148, 3207</td>
<td></td>
</tr>
<tr>
<td>Policy Master</td>
<td>Veritas High Availability (HAD) Engine</td>
<td>14141</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Veritas Cluster Manager (Java console)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>VCS Agent driver</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policy Master</td>
<td>VCS One Remoting Service</td>
<td>14150</td>
<td></td>
</tr>
<tr>
<td>Policy Master</td>
<td>Provider Access Layer (VxPAL.exe)</td>
<td>1099</td>
<td></td>
</tr>
<tr>
<td>Policy Master</td>
<td>Private Branch Exchange (pbx_exchange.exe)</td>
<td>1556</td>
<td></td>
</tr>
</tbody>
</table>
Installing and configuring the VCS One Policy Master on Windows

Installing the Policy Master on Windows

You can install the Windows Policy Master using the installation wizard or the command line.

See "Installing the Policy Master using the installation wizard" on page 23.
See "Installing the Policy Master using the command line" on page 25.

Installing the Policy Master using the installation wizard

The installation wizard is invoked once you select the Policy Master installation option from the CD browser.
You can install the Policy Master software on the local as well as remote systems belonging to the domain in which you have logged in.

Before you install the Policy Master software, review the set of prerequisites and preinstallation tasks to be performed.

See “Preparing for installing the Policy Master on Windows” on page 21.

To install the VCS One Policy Master using the installation wizard

1. On any system, insert the VCS One software disc. Once you insert the software disc, the CD Browser welcome panel appears. If the installer fails to launch the welcome panel, browse to the software disc contents and double-click the Setup.exe file.

2. On the CD Browser welcome panel, under Product Installation menu, click VCS One Policy Master.

3. On the VCS One Policy Master Installer wizard welcome panel, review the list of prerequisites and click Next.

4. On the License Agreement panel, review the End User License Agreement and select I agree to the terms of License Agreement and then click Next.

5. On the License panel, select the embedded evaluation or permanent license, and then click Next.

6. On the System Selection panel, add the systems on which you want to install the VCS One Policy Master. You can perform this in one of the following ways:
   - In the System Name text box, manually type the system name and click Add.
   - Alternatively, browse to select the systems.
     The systems that belong to the domain in which you have logged in are listed in the Available Systems list. Select one or more systems and click the right arrow to move them to the Selected Systems list. Click OK.

Once you add or select a system, the wizard performs the validation checks and notes the validation details. To review the details, select the system and click the corresponding information icon.

By default the wizard uses %ProgramFiles%\Veritas as the installation directory. However, you can customize your installation directory. To customize the installation directory, click the adjacent browse icon and select the desired location. Click OK.

Note: In case you are installing the Policy Master on more than one system, ensure that the installation directory path is similar on all the systems.
7 On the System Selection panel, click Next.
Note that the wizard fails to proceed with the installation, unless all the selected systems have passed the validation checks and are ready for installation. In case the validation checks have failed on any of the system, review the details and rectify the issue. Before you choose to proceed with the installation click Re-verify to re-initiate the validation checks for this system.

8 On the Pre-install Summary panel, review the install summary and click Next.
Note that the Automatically reboot systems after installer completes operation check box is selected by default. This will reboot all the selected remote systems immediately after the installation is complete on the respective system. If you do not want the wizard to initiate this auto reboot, clear the selection of Automatically reboot systems after installer completes operation check box.

9 On the Policy Master Installation panel, review the progress of installation and click Next when the installation is complete.

10 On the Post-install Summary panel, review the installation result and click Next.
If the installation has failed on any of the system, review the summary report and refer to the log file for details.

11 On the Finish panel, click Finish.
If you have chose to install the Policy Master on your local system, a message to reboot the local system appears. Click Yes to reboot immediately or No to reboot later.
Note that you must reboot the machine once the installation is complete. Also, in case you had not selected to initiate the auto reboot for the remote systems on which you have installed the Policy Master, ensure that you manually reboot these systems.
The next step is to configure the Policy Master.

Installing the Policy Master using the command line

You can perform a silent installation of the Windows Policy Master by running Setup.exe from the command line.

You can install the Policy Master software on the local as well as remote systems belonging to the domain in which you have logged in.

Before you install the Policy Master software, review the set of prerequisites and preinstallation tasks to be performed.
See “Preparing for installing the Policy Master on Windows” on page 21.
**Note:** For Windows Server 2008, all CLI commands must run in the command window in the “run as administrator” mode.

Table 2-3 contains information about the possible parameter values.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>/s</td>
<td>Set for silent mode.</td>
</tr>
<tr>
<td>INSTALL_MODE</td>
<td>Set to indicate an installation or uninstallation.</td>
</tr>
<tr>
<td></td>
<td>1 = To install</td>
</tr>
<tr>
<td></td>
<td>5 = To uninstall</td>
</tr>
<tr>
<td></td>
<td>Example: INSTALL_MODE=1</td>
</tr>
<tr>
<td>SOLUTION</td>
<td>Set to the type of installation</td>
</tr>
<tr>
<td></td>
<td>2 = VCS One Policy Master for Windows</td>
</tr>
<tr>
<td></td>
<td>Example: SOLUTION=2</td>
</tr>
<tr>
<td>INSTALLDIR</td>
<td>(Optional) Use only to set a non-default path for the installation</td>
</tr>
<tr>
<td></td>
<td>directory. The path must start and end with a quotation mark (“”).</td>
</tr>
<tr>
<td></td>
<td>Example: INSTALLDIR=&quot;C:\Application Installs&quot;</td>
</tr>
<tr>
<td></td>
<td>The default setting, used when you do not specify this parameter, is</td>
</tr>
<tr>
<td></td>
<td>%ProgramFiles%\Veritas.</td>
</tr>
<tr>
<td>REBOOT</td>
<td>(Optional)</td>
</tr>
<tr>
<td></td>
<td>0 = Do not reboot after operation (Default)</td>
</tr>
<tr>
<td></td>
<td>1 = Reboot after operation is complete</td>
</tr>
<tr>
<td></td>
<td>Example: REBOOT=1</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> You must reboot the Policy Master system once installation</td>
</tr>
<tr>
<td></td>
<td>is complete. If you do not specify to reboot as an installation</td>
</tr>
<tr>
<td></td>
<td>option, you must remember to reboot the system manually before</td>
</tr>
<tr>
<td></td>
<td>beginning configuration.</td>
</tr>
<tr>
<td>NODE</td>
<td>(Optional)</td>
</tr>
<tr>
<td></td>
<td>The product is installed on the local system by default.</td>
</tr>
<tr>
<td></td>
<td>To install on a remote system, specify the system name within</td>
</tr>
<tr>
<td></td>
<td>double quotes.</td>
</tr>
<tr>
<td></td>
<td>Example: NODE=&quot;SysA&quot;</td>
</tr>
</tbody>
</table>
Installing and configuring the VCS One Policy Master on Windows

About Policy Master configuration on Windows

VCS One supplies a Policy Master Configuration Wizard to configure the Policy Master.

The Policy Master installation installs components of the Storage Foundation for Windows HA (SFW HA) product, which the configuration wizard uses to configure the Policy Master for high availability.

The wizard will configure all components required for Policy Master operation, including the following:

- Policy Master cluster and service group
  The wizard configures these components using Veritas Cluster Server (VCS), which is part of the SFW HA product.
  The Policy Master is designed to run in a cluster for high availability in a production environment. Although the wizard enables you to configure the
Policy Master on one system for testing or evaluation purposes, the selected system must meet cluster requirements of at least two NICs, including one private NIC (without a static IP and with TCP/IP disabled). Three NICs are required in a cluster environment, one public and two private.

- **Policy Master storage**
  For a cluster environment with multiple systems, the wizard uses Storage Foundation for Windows (SFW) to create a volume on shared storage to store configuration data. Optionally, you can use SFW to configure a volume in advance and specify that volume during the Policy Master configuration process. If you have selected only one system for Policy Master configuration, the wizard enables you to select a drive on the local system for storing the configuration data.

- **Policy Master database**

- **VCS One Product Authentication Service**

After configuring the components, the wizard brings online the Policy Master service group and related web services.

---

**Prerequisites for configuring the Policy Master on Windows**

Policy Master configuration prerequisites include the installation prerequisites. See “Preparing for installing the Policy Master on Windows” on page 21.

In addition, verify the following:

- Ensure that the systems that you plan to select for Policy Master configuration are members of an Active Directory domain.

- For a cluster environment with multiple systems, the Policy Master Configuration Wizard will configure a new Storage Foundation for Windows (SFW) disk group and volume on shared storage for the configuration database. Ensure that the system where you run the wizard has access to the storage.

  You have the option to create the SFW disk group and volume yourself rather than having the wizard do it. If so, you must create it before running the wizard and the existing disk group and volume must be mounted on the node where you run the wizard.

- Ensure that at least 2 GB disk space is available for the Policy Master configuration, either on shared storage for a high availability configuration or on the local disk for a single node cluster.
Installing and configuring the VCS One Policy Master on Windows

Configuring the Policy Master on Windows

Ensure that your firewall settings permit the Policy Master systems to ping each other.

Review the following list and have the information ready to specify during the Windows Policy Master configuration process.

- Names of the systems on which you installed the Policy Master
- Cluster ID (a number from 0 - 255). For example: 11
  If you have other clusters (including VCS clusters) in your environment, make sure the cluster ID you assign is unique. Each cluster requires a unique ID.
- On each system, at least one private NIC with TCP/IP disabled; one public NIC with a static IP address
  A high availability configuration in a production environment requires three NICs, two private, one public.
  NIC teaming on the private NICs is not supported on the Policy Master cluster.
- Virtual IP address for the Policy Master cluster systems
  Do not use the same IP address that is used by a desired Policy Master system.
- Subnet mask used by the virtual IP address
- Names of the shared storage disks that are connected to the installation node and will be used for the Policy Master configuration

Configuring the Policy Master on Windows

After installing the Policy Master, you configure it with the VCS One Policy Master Configuration Wizard.

Before you begin the configuration process, review the following topics:

“About Policy Master configuration on Windows”

“Prerequisites for configuring the Policy Master on Windows”

You can run this wizard from any system on which the Policy Master is installed.

To configure the VCS One Policy Master on Windows

1. If the Policy Master Configuration Wizard has not been launched automatically after installation, click **Start > All Programs > Symantec > VCS One > Policy Master Configuration Wizard.**
2. On the Welcome panel, review the prerequisites and click **Next.**
3 On the System Selection panel, supply a cluster ID, which can be any number from 0 to 255. It must be unique. The wizard creates a unique default cluster name by appending the cluster ID to the value “PMCluster.”

The wizard lists and validates the systems on which you installed the Policy Master. You can manually add other Policy Master systems that may have been installed separately.

To add systems manually, do one of the following:

- In the System Name text box, manually type the system name and click **Add**.
- Click **Browse** and select the systems to be added and click **OK**.

Once you add a system, the wizard performs the validation checks and notes any failure in the Status column. To review the details of a failed check, click the message in the table.

To validate a system again, click **Re-verify**.

To delete a system, click the icon in the column that is farthest to the right. Click **Next**.

4 On the Private Network Configuration panel, select two network adapters (NICs) for the private network communication that is used by the Policy Master cluster.

For each system in the cluster, select the check boxes next to the two NICs to be assigned to the private network. TCP/IP must be disabled on NICs assigned exclusively to the private network. Optionally, one NIC can be used as a shared private and public NIC and use a static IP address, although Symantec does not recommend a shared private and public NIC in a production environment.

Click **Next**.

The wizard will validate your selection.

5 On the Network Configuration panel, specify the following:

- Enter a unique IP address that is currently not being used on your network, but is in the same subnet as the current node. This will be used as the virtual IP address for the Policy Master.
- Enter the subnet mask to which the IP address belongs.
- For each system listed, select the public NIC, which must have a static IP address separately assigned.

Click **Next**.

6 On the Storage Configuration panel, specify the storage configuration for the Policy Master. The wizard uses the Storage Foundation for Windows (SFW) product, installed with VCS One, to configure storage for the Policy Master cluster on shared storage.

If you are setting up a new configuration, select the following:
After you install and configure the VCS One Policy Master, you must do the following post-configuration tasks:

- “Verifying the Policy Master configuration on Windows” on page 32
- “Backing up the VCS One Product Authentication Service configuration” on page 33

The following tasks are optional:
Installing and configuring the VCS One Policy Master on Windows

After you install and configure the Policy Master

- “Adding multiple network paths between the Policy Master and client systems” on page 34
- “Configuring global clustering” on page 34

You can proceed with the following tasks in the recommended order shown:

- Access the web console
  See “VCS One web console” on page 35.
- Install the client systems
  See Chapter 4, “Installing and configuring the VCS One client on UNIX” on page 73.
- Add VCS One users and assign roles, create service groups for your applications, and administer groups, resources, and systems.
  See the Veritas Cluster Server One User’s Guide.

Verifying the Policy Master configuration on Windows

You can use the following steps to verify a Policy Master configuration.

To verify the Policy Master cluster

1. Check the state of the Policy Master service group on each node. At the command prompt, enter the following:
   ```
   %VCSONE_HOME%\bin\haadmin -state
   
   where %VCSONE_HOME% is the installation path, by default, C:\Program Files\Veritas\Cluster Server One.
   
   The output should show the PMSG is ONLINE on one node, OFFLINE on the other.
   
   2. Verify that the PMSG is online on one system and offline on the other. Enter the following:
   ```
   %VCSONE_HOME%\bin\haadmin -status -summary
   
   3. Display the status of each of the PMSG resources on each node. Enter the following:
   ```
   %VCSONE_HOME%\bin\haadmin -status
   
   The status of each resource in the Policy Master service group displays.
   
   For a new installation, the output of the `haadmin-status` command shows the following:
   
   - All cluster systems are running.
   - Persistent resources are ONLINE on all systems. These include the Product Authentication Service and the NIC resources.
   - All other resources are ONLINE on one system and OFFLINE on the other.
Table 2-4 describes the resources in the `haadmin -status` output for the Windows PolicyMaster.

**Note:** If you are using local storage, the `pmdg` or `pmvol` resources may not exist.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pmip</td>
<td>Policy Master virtual IP address</td>
</tr>
<tr>
<td>pmnic</td>
<td>Policy Master virtual IP NIC device</td>
</tr>
<tr>
<td>vcsonedb</td>
<td>VCS One database</td>
</tr>
<tr>
<td>pm</td>
<td>Policy Master daemon</td>
</tr>
<tr>
<td>atd</td>
<td>VCS One Product Authentication Service</td>
</tr>
<tr>
<td>VCSOneWeb</td>
<td>VCS One web console</td>
</tr>
<tr>
<td>pmdg</td>
<td>The disk group containing the database and repository</td>
</tr>
<tr>
<td>pmvol</td>
<td>The volume for the file system containing the database</td>
</tr>
</tbody>
</table>

### Backing up the VCS One Product Authentication Service configuration

You should back up the authentication service configuration. If one of the Policy Master systems is lost, you can use the backup directory to replace the faulted system and restore the authentication service configuration. It is time-consuming to manually recreate the configuration.

**To back up the VCS One Product Authentication Service configuration**

1. Determine where to back up the Policy Master cluster authentication information. Choose a safe location, such as a removable storage device. Avoid backing up to the system (C:) drive since a system crash can make the backup data available.

2. Back up the configuration. Enter the following:
   ```bash
   %VCSONE_HOME%\bin\haadmin -backup -vss full_path_to_backup_directory
   ``
   The command creates a directory with the information necessary to restore the authentication configuration if a Policy Master cluster system fails.
Installing and configuring the VCS One Policy Master on Windows

To restore the VCS One Product Authentication Service configuration

1. Locate the backup directory.
2. Mount the shared storage where the configuration storage will be restored.
3. Restore the authentication configuration. Enter the following:
   ```
   %VCSONE_HOME%/bin\haadmin -restore -vss full_path_to_backup_directory
   ```
   The haadmin utility correctly places the files on the new system.

**Note:** VCS One backup and restore commands apply to all Private Domain Repositories (PDRs) on the host where the command is executed. You cannot back up or restore individual PDRs. To restore a single PDR, the administrator must manually extract and place the pertinent files from the backup.

Adding multiple network paths between the Policy Master and client systems

Symantec recommends as a best practice to use multiple network paths between the Policy Master system and client systems. To implement this, you use the haadmin command.

You use the following haadmin options:

- `–addnic System MACAddress`
- `–addip ip_address nic netmask [-port port]`

The `nic` value for the IP is the name (not the MAC address) of a NIC added using the `–addnic` option. To get the NIC name, you can use the `–displaynic` option.

VCS One Windows does not support a multiple NIC resource. Each IP address depends on one NIC. For every NIC you add, a NIC resource is added to the Policy Master service group. NIC resources are named pmnic$index, where pmnic1 is the primary NIC that you specify using the VCS One Policy Master Configuration Wizard. The primary NIC cannot be deleted from the configuration. Any additional NICs you add will be named pmnic2, pmnic3, and so on. You can add only TCP/IP enabled MACs.

For more information on the haadmin command, see the [VCS One Command Reference Guide](#).

Configuring global clustering

Disaster recovery uses global clustering to protect against the types of outages that large-scale natural disasters cause. In such situations, VCS One global
clusters migrate applications to remote clusters located considerable distances apart. If you configure disaster recovery, VCS One monitors events between clusters. Using disaster recovery, the global cluster is aware of the state of the service groups in the global cluster at all times.

Global clustering is optional and is configured after the Policy Master installation and configuration is complete. Setting up global clustering has multiple steps and is covered in the VCS One User’s Guide. For the steps to enable the Policy Master for global clustering, see the chapter “Setting up VCS One global clusters” in the VCS One User’s Guide.

**VCS One web console**

You use the VCS One web console to administer the VCS One cluster.

**Web console prerequisites**

Before you access the VCS One web console for the first time, do the following:

- Install a supported browser.
  See the Veritas Cluster Server One Release Notes for supported browser versions.

- In the browser, do the following:
  - Enable cookies
  - Disable browser caching
  - Disable the pop-up blocker
  - Enable ActiveX controls (Internet Explorer only)

- Install a supported Flash version.
  See the Veritas Cluster Server One Release Notes for supported Flash versions.

- Open the ports that the web server uses.
  See “Required ports and firewall settings” on page 21.

**Setting who can access the VCS One web console**

The administrator on the Policy Master system can log in without being added to the VCS One configuration. To allow other users to log in to the VCS One web console, you must explicitly add those users as VCS One users with assigned roles.
Accessing the VCS One web console

Follow the instructions in this section each time you access the VCS One web console.

When you access the VCS One web console for the first time, you see a message about authentication. Read the message and click OK to add and permanently store a trusted security certificate. After you add the security certificate, the VCS One web console login page appears in the browser.

To access the VCS One web console

1. Open a web browser and enter the following URL:
   https://PM_cluster_virtual_IP_address:14171
   Symantec recommends that you use the virtual IP address of the Policy Master (PM) cluster instead of the name of the active system in the Policy Master cluster. If you use the virtual IP address, the VCS One console maintains a connection with the Policy Master after a Policy Master cluster failover operation.
   You may want to create a shortcut to this URL.

2. In the web browser, click the VCS One web console link.

3. In the Log on page, specify the following details:
   - In the Select Language box, select the appropriate language. In this release, only English is supported.
   - In the User Name field, enter the name of the user.
   - In the Password field, enter the password.
   - In the Domain field, enter the domain name.
     You must specify a domain name for all domain types except unixpwd (which is the default domain type) and pam. To view a list of all the domains on the Policy Master system, enter the following command:
     haat showallbrokerdomains -j broker
     If you leave the Domain field blank and the domain type is unixpwd or pam, VCS One assumes that the domain type is the same as the Policy Master system’s domain type.
   - In the Domain Type field, select a domain type (unixpwd, nt, nis, nisplus, pam, vx, or ldap).
   - In the Broker:Port field, enter the authentication broker name and the port number separated by a colon (:). This field is optional and is populated automatically.

4. Click Log On.
   The web console is best viewed at 1024x768 screen resolution.
Recreating the SSL certificate

The VCS One installer creates an SSL certificate on each Policy Master system. The SSL certificate works if you access the VCS One web console using a VCS One Policy Master virtual IP address.

With Internet Explorer 7, using a host name that resolves to a VCS One Policy Master virtual IP address when accessing the VCS One web console may display invalid SSL certificate messages. To prevent these messages, you must recreate the SSL certificate.

This section provides the general steps and resources needed to recreate an SSL certificate. For more detailed information about SSL-related tasks, see the Apache Tomcat 6.0 SSL Configuration instructions available on the Internet.

To recreate the SSL certificate, you can use Java Keytool, or another tool of your choice. For your convenience, the Java Keytool utility is included in the VCS One installation, and located at:

```
%VCSONE_HOME%\jre\bin
```

where

%VCSONE_HOME% is the path that you specify during VCS One installation.

To recreate the SSL certificate

1. Locate the key store containing the certificate that the VCS One installer created at:
   
   %VCSONE_HOME%\web\tomcat\cert

2. Follow the Apache Tomcat 6.0 SSL Configuration instructions for creating an SSL certificate.

3. At the prompt, enter the information for the host name that you want to use to access the VCS One web console.

4. To restart the VCS One web console, use the `hastop` and `hastart` commands to take it offline and bring it online. From the command prompt, change directory as necessary to the `%VCSONE_HOME%\bin` directory and enter:
   
   `hastop -web`
   
   `hastart -web`

5. From the browser, choose to install the new certificate.
Installing and configuring the VCS One client

This chapter includes the following topics:

■ About installing and configuring the clients
■ Preparing to install the VCS One client
■ Installing the VCS One client on a Windows Server
■ Installing the VCS One client on an ESX and ESXi Server
■ Configuring the client systems with a Policy Master Server on Windows
■ Configuring the Windows client systems with a Policy Master Server on Unix
About installing and configuring the clients

The client systems host the applications you wish to manage using VCS One. Along with the application availability, VCS One also provides high availability to VMware virtual machines. To monitor virtual machines and provide advanced workload management functionality for VMware virtual machines, the VCS One client software must be installed on an ESX Server (for ESX 3.5 and 4.0). However, in case of ESXi Server, you must install the Control node and then install the VCS One client on this Control node.

You must install the VCS One client on all the systems that would be a part of the VCS One cluster. After you install the VCS One client you must configure these systems with the Policy Master server.

Preparing to install the VCS One client

This section lists the pre-requisites and the pre-installation tasks you must perform before you begin to install the VCS One client on both, Windows and ESX Server.

See “General preparations” on page 40.

In addition to these generic tasks you must also perform the platform specific tasks

See “Windows specific preparations” on page 41.

See “ESX-specific preparations” on page 41.

General preparations

- Ensure that you have adjusted your firewall settings and enabled the required ports.
  See “Required ports and firewall settings” on page 21.

- Ensure the client host name resolves to the client IP address, and vice versa.

- Install the required operating system patches. See the Veritas Cluster Server One Release Notes for the required operating systems patches.

- Mount the software disc on the system where you plan to run the installation.

Note: To install the VCS One client for managing VMware ESXi Servers, use the software disc for Red Hat Enterprise Linux 4 (RHEL 4) x86 (32-bit) or RHEL 5 x86_64.
Have the VCS One Policy Master virtual IP address ready. Communication must be enabled between the installer and the system with the Policy Master virtual IP address.

**Windows specific preparations**

If you are installing the VCS One client on a Windows Server, review the following product installation requirements for your systems. Minimum requirements and Symantec recommended requirements may vary.

For the latest information on installation requirements and supported software for this release, see the following Symantec Technical Support TechNote:

<table>
<thead>
<tr>
<th>Table 3-1 Installation Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory</td>
</tr>
<tr>
<td>System processor</td>
</tr>
<tr>
<td>Disk space</td>
</tr>
<tr>
<td>Operating systems</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

- Ensure that the Remote Registry and Windows Management Instrumentation (WMI) services are running.
- Ensure that the Veritas Cluster Server One Authentication (VCSONEatd) service is running.

**ESX-specific preparations**

Before you install the VCS One client on an ESX Server system, you must:

- Uninstall any earlier version of the VCS One client.
  See “About uninstalling the VCS One client from an ESX server” on page 71.
■ If the system uses DHCP, ensure that the DHCP IP addresses have a long-term lease and are not relinquished while the VCS One client daemon (vcsoneclientd) is running. The loss of connectivity may fault the VCS One client.

■ Refer to chapter *Managing objects in a VMware environment* from the *VCS One User's Guide* for detailed information on the following tasks:
  ■ Configure communications between VCS One and the VirtualCenter Management console.
  ■ Configure VCS One to discover the VMware VirtualCenter environment.
  ■ Monitor the discovery of VirtualCenter objects using the VCS One console logs.
  ■ Place applications in a VMware environment under VCS One control.

**ESXi-specific preparations**

Follow the steps in this section to configure virtual machines to start up automatically. Follow these steps for each ESXi server on behalf of which you configure VCS One client machines.

**To manually configure virtual machines for automatic startup**

1. From the VMware vSphere client, select an **ESXi server**.
2. Select the **Configuration** tab.
3. Select the **Virtual machine startup/shutdown** option in the Software panel.
4. Click the **Properties** link in the upper-right corner.
5. In Virtual Machine Startup and Shutdown dialog box, select the checkbox. **Allow virtual machines to start and stop automatically with the system**.
6. Select the virtual machine that is configured as a client for the ESXi server.
7. Click **Move Up** until the server is the first item under Automatic Startup.
8. Click **OK**.

**Installing the VCS One client on a Windows Server**

You can install the client components on Windows Server 2003 and Windows Server 2008, using the client installer.

You can also install the client components using the command line, on Windows Server 2008 Server Core systems only.
Installing the VCS One client using the client installer

The Client installer enables you to install the client software on the local as well as the remote systems belonging to the domain in which you have logged in.

.Net 2.0 SP1 framework is the base requirement for the installer. If you are installing the client on a Windows Server 2003 x64 system and if the .Net framework is not installed, the installer begins to install it before it actually proceeds with the client installation. You are required to re-launch the installer after the .Net 2.0 SP1 installation is complete.

Before you proceed with the installation process, review the set of pre-installation tasks and the prerequisites required for the client installation.

---

**Note:** If you have an earlier version of a VCS One client installed, you must completely uninstall it before installing the current version of the client. For uninstallation instructions, see the *Veritas Cluster Server One Installation Guide* for the VCS One version you want to uninstall.

---

**To install the VCS One client on Windows**

1. On any system, insert the VCS One software disc. Once you insert the software disc, the CD Browser welcome screen appears. In case if the installer fails to launch the welcome screen, browse to the software disc contents and double-click the Setup.exe file.

2. On the CD Browser welcome panel, under Product Installation menu, select **VCS One Client**.

3. On the VCS One Client installer welcome panel, review the list of prerequisites and click **Next**.

4. On the License Agreement panel, review the End User License Agreement and select **I agree to the terms of License Agreement** and then click **Next**.

5. On the System Selection panel, add the systems on which you want to install the VCS One client. You can perform this in one of the following ways:
   - In the System Name text box, manually type the system name and click **Add**.
   - Alternatively, browse to select the systems.

   On the Select Systems panel, the systems that belong to the domain in which you have logged in are listed in the Available Systems list. Select one or more systems and click the right arrow to move them to the Selected Systems list. Click **OK**.
Installing and configuring the VCS One client

Installing the VCS One client on a Windows Server

Once you add or select a system, the wizard performs the verification checks and notes the verification details. To review the details, click the corresponding information icon.

By default the wizard uses %ProgramFiles%\Veritas as the installation directory. However, you can customize your installation directory. To customize the installation directory, click the adjacent browse icon and select the desired location. Click OK.

6 On the System Selection panel, click Next.
   Note that the installer fails to proceed with the installation, unless all the selected systems have passed the verification checks and are ready for installation. In case the verification checks have failed on any of the system, review the details and rectify the issue. Before you choose to proceed with the installation click Re-verify to re-initiate the verification checks for this system.

7 On the Pre-install Summary panel, review the summary and click Next.

8 On the Client Installation panel, review the progress of installation and click Next when the installation is complete.

9 On the Post-install Summary panel, review the installation result and click Next.
   If the installation has failed on any of the system, refer to the log file for details.

10 On the Finish panel, click Finish.
   The client installation is complete. You can now configure the client on the systems where the installation was successful.
   See “Configuring the client systems with a Policy Master Server on Windows” on page 49.

Installing the client on Windows using the command line

You can install the client components using the command line on Windows Server 2008 Server Core Edition only.

Run the Setup.exe from the command line to silently install the VCS One client on Windows Server 2008 Server Core systems.

You can perform the silent installation only on a local system.

Note: For Windows Server 2008, all CLI commands must run in the command window in the “run as administrator” mode.
In case you are using Veritas Storage Foundation (SFW) as your storage manager, the Veritas Storage Agent (vxvm) service will be stopped during the client installation. This unables you to perform any of the SFW operations. The vxvm service will be resumed after the client is successfully installed.

**Before you install the VCS One client on Server Core**

Note the following requirements before you install the VCS One client on a Server Core system:

- You will require a user account that has sufficient privileges to install the software on the system.
- The product disc must be accessible from the system. If you have copied the software to a remote directory, map that directory as a network drive on the system. This is required for installation as well as uninstallation of the product.

**Parameters for setup.exe**

Table 3-2 contains information about the possible parameter values.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>/s</td>
<td>Set for silent mode.</td>
</tr>
<tr>
<td>INSTALL_MODE</td>
<td>Set to indicate an installation or uninstallation. 1 = To install 5 = To uninstall Example: INSTALL_MODE=1</td>
</tr>
<tr>
<td>SOLUTION</td>
<td>Set to the type of installation 1 = VCS One Client 5.0 SP2 Example: SOLUTION=1</td>
</tr>
<tr>
<td>INSTALLDIR</td>
<td>Use only to set a non-default path for the installation directory. The path must start and end with a quotation mark (&quot;), Example: INSTALLDIR=&quot;C:\Application Installs&quot;</td>
</tr>
</tbody>
</table>

The default setting, used when you do not specify this parameter, is %ProgramFiles%\Veritas.
Installing the VCS One client on an ESX and ESXi Server

To start the silent installation from the command window

1. In the command window, navigate to the root directory of the product CD.
2. Use the following command syntax to install the VCS One client:
   
   ```
   Setup.exe /s INSTALL_MODE=1 SOLUTION=1 [INSTALLDIR="InstallDirPath"]
   ```
   
   The syntax is not case sensitive.
   
   The silent installer begins to perform the installation. Various messages indicate the installation progress.
   
   If the silent installation becomes unresponsive or fails for any reason, refer to the installer logs.
   
   The log files are available at the following location:
   
   On Windows Server 2008 Server Core:
   `%allusersprofile%\Veritas\VPI\log`

Installing the VCS One client on an ESX and ESXi Server

This section provides the details on installing the VCS One client on an ESX 3.5, 4.0 and ESX 4i Servers.

The VCS One client installation involves the following tasks:

- Installing a Control node (applicable in case of ESXi Servers only)
- Launching the installer
- Specifying the target systems
- Reviewing the package list

Installing a Control node

If you are installing the VCS One client in an ESXi environment, you must first install a virtual machine running on the Red Hat Enterprise Linux (RHEL) 4.0 (32 bit) or Red Hat Enterprise Linux (RHEL) 5.0 (64 bit) operating system, over the ESXi Server. This virtual machine, called as the Control node, manages the ESXi server.

You must launch the VCS One Client installer from the Control node.
Launching the installer

To launch the client installer

1. Insert the software disc for Red Hat Enterprise Linux 4 (RHEL 4) x86 (32 bit) or RHEL 5 x86_64.

2. Navigate to the platform-specific directory. Enter the following:
   ```
   # cd platform
   where platform is the platform-specific directory, such as
   - esx4_x86_64 for ESX 4.0,
   - esx30_i686 for ESX 3.0
   - rhel4_i686 for RHEL 4.0 in case of ESXi installation
   - rhel5_x86_64 for RHEL 5.0 in case of ESXi installation.
   Go to the directory cluster_server_one.
   For ESX 3.5 and 4.0, enter the following:
   # ./installvcsonecd -installonly
   For ESX 4.i, enter the following:
   ./installvcsonecd -esxi
   ```
   Note: The installonly option, only installs the VCS One Client. After the installation is complete, you must configure the systems with the Policy Master.
   See “Configuring the client systems with a Policy Master Server on Windows” on page 49.

3. Accept the End User License Agreement (EULA). At the EULA prompt, enter the following: y.
   The installer provides information about the installation and configuration.

4. Review the information on each page and press Enter to continue.

Specifying the target systems

You must specify the name of the target systems for each client system.

To specify the target systems

- At the system names prompt, enter the names of the systems on which you want to install the VCS One client. Separate each name with a space. (Do not enter fully-qualified domain names or IP addresses.) For example, enter the following: redhat100  redhat105
Installing and configuring the VCS One client

Installing the VCS One client on an ESX and ESXi Server

Reviewing the package list

The installer provides a list of packages to be installed.
To review the package list, refer to the list of packages to be installed and press Enter to continue.
For a list of the packages, see Appendix A, “Required UNIX packages” on page 75.
Configuring the client systems with a Policy Master Server on Windows

After you install the VCS One Client you must configure the systems such that they are now under the control of the VCS One Policy Master (PM) server and thus a part of the VCS One cluster.

You can configure the Windows and ESX client systems with a Policy Master Server on Windows.

See "Configuring the Windows client systems" on page 50.
See "Configuring the ESX client systems" on page 52.

Before you configure the client systems

Ensure that you perform the following tasks and have the required information ready before you proceed to configure the client with the Policy Master.

- Ensure that you have installed and configured a Policy Master (PM) server in the VCS One cluster.
  See "Installing and configuring the VCS One Policy Master on Windows" on page 19.

- Make sure the Policy Master is running. Run the following command on the Policy Master Server:
  haadmin -state
  The output of the command must be similar to the following:

<table>
<thead>
<tr>
<th>#Group</th>
<th>Attribute</th>
<th>System</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PMSG</td>
<td>State</td>
<td>VCSNET361</td>
<td>OFFLINE</td>
</tr>
<tr>
<td>PMSG</td>
<td>State</td>
<td>VCSNET362</td>
<td>ONLINE</td>
</tr>
</tbody>
</table>

- Ensure that you have installed the client components on the systems that you wish to configure.
  See “About installing and configuring the clients” on page 40.

- If a firewall is configured, ensure that the required ports are enabled for inbound and outbound communication. These ports are used for PM and client communication.
  See “Required ports and firewall settings” on page 21.

- Make sure that the clock times on each system are within 30 minutes of one another.

- Keep the following information handy to enter the details when the wizard prompts for.
  - For configuring clients on Windows Server,
Configuring the client systems with a Policy Master Server on Windows

- A domain user account with administrative privileges on all the client systems that you wish to configure.
- The user account having the privileges to add a system (hasys -add privilege) to the Policy Master server.
- The virtual IP address of the Policy Master server configured in the VCS One cluster.
- For configuring clients on ESX Server,
  - Ensure that the VCS One user has the administrative privileges to add and modify a pframe to the Policy Master server.
  - Ensure that the ESX name can be resolved from the Policy Master server.
  - Ensure that you have noted the correct user name (having administrative privileges) and password of the ESX server.

Configuring the Windows client systems

The following steps describe how to configure the VCS One client on Windows, using the Client Configuration Wizard for Windows.

You can run the wizard from the client systems or from the Policy Master system.

To configure the VCS One client on Windows

1. Click Start > Programs > Symantec > VCS One > Client Configuration Wizard (for Windows).
2. Review the prerequisites on the Welcome panel and click Next.
3. On the Policy Master Details panel, specify the following details.

   **Policy Master: IP Address: Port:**
   - Type the virtual IP address of the Policy Master (PM).
   - Do not specify the physical IP address of the PM server.
   - Type the port number used by the PM. The default port is 14151.
Configuring the client systems with a Policy Master Server on Windows

4 On the OUValue Details Panel, review the VCS One organization tree and specify the OUValue to which you want to attach the client systems. Click Next.

You can either type the OUValue or select the OUValue from the tree. Type the OUValue path in the format /OUName=OUValue.

For example, /VCSOneCO=Retail or /VCSOneCO=Marketing/B2B=Dept

You cannot configure a system to the OUName; you must specify a OUValue.

Note that the OUs to which the specified user has access to will be available.

5 On the System Selection panel, add the systems that you want to configure with the Policy Master. You can perform this in one of the following ways:

- In the System Name text box, manually type the system name and click Add.
- Alternatively, browse to select the systems.

On the Select Systems panel, the systems that belong to the domain in which you have logged in are listed in the Available Systems list. Select one or more systems and click the right arrow to move them to the Selected Systems list. Click OK.
Once you add or select a system, the wizard performs the verification checks and notes the verification details. To review the details, click the corresponding information icon.

6 On the System Selection panel, click **Next**. Note that the wizard fails to proceed with the configuration, unless all the selected systems have passed the verification checks and are ready for configuration. In case the verification checks have failed on any of the system, click the corresponding information icon and review the details. Rectify the issue and click **Re-verify** to re-initiate the verification checks for this system.

7 On the VCS One Remoting Service User Account panel, specify the name of a domain user for the VCS One remoting service. The VCS One Client Daemon, which runs in the context of the local system built-in account, uses the VCS One remoting service user context to access the network.

8 On the Client Configuration panel, review configuration progress and click **Next**, after the configuration is complete.

9 On the Summary panel, review the configuration summary and click **Finish**. If the configuration has failed on any of the system, review the summary report and refer to the log file for details.

On the systems where the configuration is successful, you can proceed to create application service groups.

Refer to *Veritas Cluster Server Users Guide* for details on creating the service groups.

### Configuring the ESX client systems

You can configure the ESX or ESXi client systems with the Windows Policy Master, using a wizard or through the CLI.

#### Configuring the ESX client systems using the wizard

The following steps describe how to configure the VCS One client on ESX Server, using the Client Configuration Wizard.

You must run the wizard from the Policy Master system.

**To configure the VCS One client**

1. Click **Start > Programs > Symantec > VCS One > Client Configuration Wizard**.
2. Review the prerequisites on the Welcome panel and click **Next**.
3 On the Policy Master Details panel, specify the following details.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Master: IP</td>
<td>The virtual IP address and port number of the Policy Master is populated by default.</td>
</tr>
<tr>
<td>Address: Port</td>
<td></td>
</tr>
<tr>
<td>Use Logged-on</td>
<td>This check box is selected by default.</td>
</tr>
<tr>
<td>User credentials</td>
<td>Continue with the selection if you want the wizard to use the logged on user account context to perform the client configuration tasks. The credentials values are populated in the respective fields below and the fields are disabled by default. If you do not want to use the logged on user account context, clear this check box and enter the relevant credentials in the fields below.</td>
</tr>
<tr>
<td>User Name</td>
<td>Type a user name.</td>
</tr>
<tr>
<td>Password</td>
<td>Type the password for the specified user.</td>
</tr>
<tr>
<td>Domain Type</td>
<td>Select the appropriate domain type from the drop-down list. For a Windows PM, select nt.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>Type the qualified domain name of the Policy Master (PM) server.</td>
</tr>
</tbody>
</table>

4 On the OUVValue Details Panel, review the VCS One organization tree and specify the OUVValue to which you want to attach the client systems. Click Next.

You can either type the OUVValue or select the OUVValue from the tree. Type the OUVValue path in the format /OUName=OUValue. For example, /VCSOneCO=Retail or /VCSOneCO=Marketing/B2B=Dept

You cannot configure a system to the OUName; you must specify a OUVValue.

Note that the OUs to which the specified user has access to will be available.

5 On the System Selection panel,

- Add the systems that you want to configure with the Policy Master. In the System Name text box, manually type the system name.
- Enter the username and password of the ESX box.
- Click **Add** and then click **Configure**.
Installing and configuring the VCS One client
Configuring the client systems with a Policy Master Server on Windows

Note: If you are configuring the VCS One client installed on an ESXi server, you must select the **This is a VMWare ESXi System** check box and then click **Add**.
On the Control Node Details Panel, enter the nodename, username, and password for the control node, in the respective fields.

Once you add or select a system, the wizard performs the verification checks and notes the verification details. To review the details, click the corresponding information icon.
Note that the wizard fails to proceed with the configuration, unless all the selected systems have passed the verification checks and are ready for configuration. In case the verification checks have failed on any of the system, click the corresponding information icon and review the details. Rectify the issue and click **Re-verify** to re-initiate the verification checks for this system.
If the wizard fails to authenticate the username and password entered, click **Edit** and enter the correct credentials of the ESX Server or the Control node you want to configure.

6 On the Client Configuration panel, review configuration progress and click **Next**, after the configuration is complete.

7 On the Summary panel, review the configuration summary and click **Finish**.
If the configuration has failed on any of the system, review the summary report and refer to the log file for details.

8 From the VCS One Web Console, verify whether the configured ESX client system (pframe) is in the Running state.
On the systems where the configuration is successful, you can proceed to add and configure virtual machines (vframes) in the VCS One cluster. Subsequently create the application service groups for high availability. For details, refer to *VCS One User’s Guide*.

### Configuring the ESX client systems using CLI

Perform the following steps, to configure the ESX client systems, using the CLI.

Note: If UAC is enabled, open the command prompt as “administrator”.

1 Make sure the Policy Master is running. On the Policy Master Server, enter the following:
```bash
haadmin -state
```
2 On the Policy Master system perform the following steps:
   a Add the pframe to the configuration.
      \%VCSONE_HOME\%\bin\hapframe -add pframeName -vtype esxserver OUName
   b Set the User attribute for the pframe.
      \%VCSONE_HOME\%\bin\hapframe -modify -refreshvars pframeName ESXServer: User esx machine admin username
   c Set the Password attribute for the pframe.
      \%VCSONE_HOME\%\bin\hapframe -modify -refreshvars pframeName ESXServer: Password esx machine admin password
   d Set the HealthCheckIPs attribute for the pframe.
      \%VCSONE_HOME\%\bin\hapframe -modify pframeName ESXServer: HealthCheckIPs -update IP1 IP of ESX machine
   e Create the authentication principals in the domain. Enter the following:
      \%VCSONE_HOME\%\bin\haat addprpl -t ab -d VCSONE_USERS@vcsone_cluster -p pframeName
   f At the password prompt, create and verify your password.

3 On the client system, perform the following steps:
   a Specify the virtual IP address for the Policy Master and the authentication port; and set the security level. Enter the following:
      # \%VCSONE_HOME\%\bin\haat setuptrust -b policy_master_virtual_IP_address: 14159 -s low
   b Obtain a credential for an authentication principal from an authentication broker. Enter the following:
      \%VCSONE_HOME\%\bin\haat authenticate -d vx:VCSONE_USERS@vcsone_cluster -p pframeName -b policy_master_virtual_IP_address: 14159
   c When you are prompted for a password, enter the password you created in step 2f.
   d Create \%VCSONE_HOME\%\vcsone.conf file with the following entries:
      PM_IPS=[policy_master_virtual_IP_address]:14151
      Username= pframeName@VCSONE_USERS@vcsone_cluster
      BrokerHost=policy_master_virtual_IP_address
      BrokerPort=14159
Adding and configuring the virtual machines (vframes) with the Policy Master Server

After you have configured the pframes, with the VCS One Policy Master, you must add and configure the virtual machines (vframes) in the cluster. See *Managing objects in a VMware environment* from the *VCS One User’s Guide*.

Configuring the Windows client systems with a Policy Master Server on Unix

Before you begin to configure the client systems, ensure that you have performed the following tasks:

**Before you configure the client systems**

- Ensure that you have installed the client components on the systems that you wish to configure. See “About installing and configuring the clients” on page 40.
- Ensure that you have installed and configured the Policy Master Server. For details, refer to *VCS One Installation and Configuration Guide on Unix*.
- Make sure the Policy Master is running. Run the following command on the Policy Master Server:
  ```
  haadmin -state
  ```
  The output of the command must be similar to the following:
  ```
  #Group       Attribute             System     Value
  PMSG         State                 VCSNET361  |OFFLINE|
  PMSG         State                 VCSNET362  |ONLINE|
  ```
- If a firewall is configured, ensure that the required ports are enabled for inbound and outbound communication. These ports are used for PM and client communication. See “Required ports and firewall settings” on page 21.
- Make sure that the clock times on each system are within 30 minutes of one another.
Make sure that the user is a local administrator, and the username and password that you specify, must be that of a domain user.

Keep the following information handy to enter the details.

- For configuring clients on Windows Server,
  - A domain user account with administrative privileges on all the client systems that you wish to configure.
  - The user account having the privileges to add a system (`hasys -add privilege`) to the Policy Master server.
  - The virtual IP address of the Policy Master server configured in the VCS One cluster.

Configuring the client systems

To configure the Windows client systems with a Policy Master on Unix

1. Add the client system to the configuration, and specify Windows as the platform. Run the following commands on the Policy Master Server and provide a password when prompted.

   ```bash
   /opt/VRTSvcsone/bin/hasys -add ClientSystemName -platform windows
   ```

   Note that the `ClientSystemName` is case sensitive.

2. Create the authentication principals in the domain. Enter the following:

   ```bash
   /opt/VRTSvcsone/bin/haat addprpl -t ab -d VCSONE_USERS -p ClientSystemName -q service
   ```

3. At the password prompt, create and verify your password.

4. Specify the virtual IP address for the Policy Master and the authentication port; and set the security level. Run the following commands on the client system command prompt.

   ```bash
   %VCSONE_HOME%/bin/haat setuptrust -b PM_VIP:ATPort -s low
   ```

   Where, 14159 is the ATPort by default.

5. Obtain a credential for an authentication principal from an authentication broker. Enter the following:

   ```bash
   %VCSONE_HOME%/bin/haat authenticate -d vx:VCSONE_USERS -p ClientSystemName -b PM_VIP:ATPort
   ```

   Where, 14159 is the ATPort by default.

6. When you are prompted for the password, provide the one you had specified in step 3.
7. Create `%VCSONE_HOME%\vcsone.conf` file with the following entries on the client systems:

```
PM_IPS=[PM1_VIP]:14151[PM2_VIP]:14151
Username=ClientSystemName@VCSONE_USERS
BrokerHost=PM_VIP
SystemIPAddrs=ClientSystem_VIP
LOCAL_NAME=ClientSystemName
BrokerPort=14159
```

8. Start the Client Service (vcsoneclientd) on the client system.
```
net start vcsoneclientd
```

9. Configure the VCS One Client Helper service on the client systems, as the domain administrator.
For example,
```
%VCSONE_HOME%\bin> VCSONEClientHelper.exe /configure
/user:win\administrator /password:abcd
```
In the above example, `win` is the windows domain in which the client has been added and `abcd` is the password for its “administrator”.
On the systems where the configuration is successful, you can proceed to create application service groups.
Refer to *Veritas Cluster Server Users Guide* for details on creating the service groups.
Installing the Simulator

This chapter includes the following topics:

- About the Simulator
- Before you install the Simulator
- Installing the Simulator
Installing the Simulator

About the Simulator

You can use the Simulator to view, modify, and test the VCS One cluster configuration and behavior in a safe simulation that does not affect your production environment.

For more information about using the Simulator, see the *Veritas Cluster Server One User’s Guide*.

Before you install the Simulator

You can install the VCS One Simulator software on one or more Windows systems. A Simulator is available for Windows only.

Before you install the Simulator, ensure that the Windows version of the system where you plan to install the Simulator is at a level supported by this release.

For supported operating system levels, see the *Veritas Cluster Server One Release Notes*.

Installing the Simulator

The Simulator included in this release of VCS One can co-exist with earlier versions. Earlier versions of the Simulator use the same ports as the Simulator included in this release. If you have an earlier version of the Simulator, make sure that it is not running before you install the version included in this VCS One release.

You can install the Simulator, in any one of the following ways:

- Insert the VCS One installation software disc and run the vcsonesim.exe available in the simulator directory.
- Alternatively, you can choose to run the Setup.exe and then choose to install the Simulator from the product installation options available.

To install the Simulator

1. Insert the VCS One software disc for any supported platform into the disc drive.

2. Navigate to the simulator directory. From there, open the windows directory and double click on vcsonesim.exe to start the VCS One Simulator installation wizard.

   Alternatively, click **VCS One Simulator** from the product installation options displayed on the CD Browser welcome panel.
Installing the Simulator

Note: After you insert the VCS One software disc, if the installer fails to launch the CD Browser welcome screen, browse to the software disc contents and double-click the Setup.exe file.

3 Click Next on the Welcome screen.

4 Accept the End-User Software License Agreement and click Next.

5 On the Destination Folder panel, check the destination folder where the VCS One Simulator will be installed.
   - If you want to install the software in the displayed directory, click Next. By default, the Simulator is installed on the desktop in a directory named VCSOne.
   - If you want to change the location for software installation, click Browse...
     Browse to the desired directory and click OK. Then, click Next. If you change the directory, the VCS One Simulator software is installed in the specified directory.

6 On the Start Installation panel, click Next. The VCS One Simulator installation wizard takes a few minutes to install the software.

7 When the VCS One Simulator installation wizard indicates that the installation is complete, click Finish.

The Simulator installer does not add any files outside of the directory where it installs the Simulator. The Simulator does not appear in Add or Remove Programs, the Start Up program, or in the registry. You may move the directory where the Simulator is installed to any location.
Uninstalling VCS One software

This chapter includes the following topics:

- About uninstalling the VCS One Policy Master
- Preparing to uninstall the VCS One Policy Master
- Uninstalling the VCS One Policy Master
- About uninstalling the VCS One client on Windows
- Preparing to uninstall the VCS One Client on Windows
- Uninstalling the VCS One client on Windows- using the installer
- Uninstalling the VCS One client on Windows Server Core
- About uninstalling the VCS One client from an ESX server
- Uninstalling the VCS One client from an ESX Server
- Uninstalling the Simulator
About uninstalling the VCS One Policy Master

The Policy Master Installer wizard enables you to uninstall the Policy Master software from the local as well as the remote systems.

In order to uninstall the Policy Master from the remote systems, the local system from where you run the un-installation must have the VCS One Policy Master installed on it.

Before you proceed to uninstall the Policy Master software, review the pre-uninstall steps to be performed on all the systems from which you want to uninstall the Policy Master software.

Preparing to uninstall the VCS One Policy Master

Before you begin with the un-installation, ensure that you have the required administrative rights and privileges. Also, ensure that you perform the following tasks before you uninstall the Policy Master software.

- Ensure that the Remote Registry and Windows Management Instrumentation (WMI) are running.
- For remote uninstallation from Windows Server 2008 systems, ensure that the Computer Browser Service is enabled.
- For remote uninstallation, ensure that you have adjusted your firewall settings such that the specific ports needed for uninstalling the VCS One Policy Master are enabled. See “Required ports and firewall settings” on page 21.
- Ensure that the system is not a part of any existing Policy Master cluster service groups configurations.

The following step is recommended before un-installation to ensure deletion of all installed files:

Bring offline the Policy Master service group (PMSG) and Policy Master DR service group (DRSG). You can use the following command for this step:

```bash
%VCSONE_HOME%\hastop -pmm -all
```
Uninstalling the VCS One Policy Master

To uninstall the VCS One Policy Master

1. Go to the Windows Programs and Features. ([Start] > [Settings] > [Control Panel] > [Programs and Features])
2. Scroll to Veritas Cluster Server One Policy Master 5.0 SP2 for Windows and select it.
3. Click Uninstall.
4. On the VCS One Policy Master Installer wizard welcome page, review the list of prerequisites and click Next.
5. On the System Selection panel, add the systems from which you want to uninstall the VCS One Policy Master. You can perform this in one of the following ways:
   - In the System Name text box, manually type the system name and click Add.
   - Alternatively, browse to select the systems. The systems that belong to the domain in which you have logged in are listed in the Available Systems list. Select one or more systems and click the right arrow to move them to the Selected Systems list. Click OK.
   Once you add or select a system, the wizard performs the validation checks and notes the validation details. To review the details, click the corresponding information icon.

Note: By default the local system is selected for un-installation. In case you are performing a remote un-installation and do not want to uninstall the Policy Master from the local system, click the corresponding <remove> icon to remove the system from the list.

6. Click Next.
   Note that the wizard fails to proceed with the un-installation, unless all the selected systems have passed the verification checks and are ready for un-installation. In case the verification checks have failed on any of the system, review the details and rectify the issue. Before you choose to proceed with the un-installation click Re-verify to re-initiate the verification checks for this system.
7. On the Pre-uninstall Summary panel, review the summary and click Next.
   Note that the Automatically reboot systems after installer completes operation check box is selected by default. This will reboot all the selected
remote systems immediately after the un-installation is complete on the respective system. If you do not want the wizard to initiate this auto reboot, clear the selection of *Automatically reboot systems after installer completes operation* check box.

8 On the Policy Master Un-installation panel, review the uninstallation progress and click **Next** when the uninstallation is complete.

9 On the Post-uninstall Summary panel, review the uninstallation results and click **Next**.
   If the uninstallation has failed on any of the system, review its summary report and check the log file for details.

10 On the Finish panel, click **Finish**.
   If you had chose to uninstall the Policy Master from the local system, a message to reboot the local system appears. Click **Yes** to reboot immediately or **No** to reboot later.
   Note that you need to reboot the machine once the un-installation is complete.
   Also, in case you had not selected to initiate the auto reboot for the remote systems from which you have uninstalled the Policy Master software, ensure that you manually reboot these systems.
About uninstalling the VCS One client on Windows

The VCS One client un-installation is a wizard based un-installation for Windows 2003 and Windows 2008 systems. In case of Server Core systems however, you need to uninstall the client components silently.

In the wizard based un-installation you can uninstall the client components from the local as well as multiple remote client systems. In case of Server Core systems, you can uninstall the client components only from the local system.

Note that during the wizard based un-installation, in order to uninstall the client components from the remote systems, the local system from where you run the un-installation must have the VCS One client installed on it.

Before you proceed to uninstall the client software, review the pre-uninstall steps to be performed on all the systems from which you want to uninstall the client software.

**Note:** The enterprise agents are automatically uninstalled with the VCS One client software.

Preparing to uninstall the VCS One Client on Windows

Before you begin with the un-installation, ensure that you have the required administrative rights and privileges. Also, ensure that you perform the following tasks before you uninstall the client software.

- Ensure that the Remote Registry and Windows Management Instrumentation (WMI) are running.
- Ensure that the system is not a part of any existing service groups configurations.
  For more details on bringing the service group offline and deleting the same refer to, Veritas Cluster Server Users Guide.
- Ensure that you have unconfigured the client system from the cluster.
  See “Unconfiguring the VCS One client” on page 67.

Unconfiguring the VCS One client

You must unconfigure the client before you uninstall it from the desired cluster system.
To unconfigure the client, perform the following steps on the Policy Master server:

1. Stop the VCS One client.
   
   `hasstop -client -sys <systemName>`

2. Delete the system from the Policy Master server.
   
   `hasys -delete <systemName>`

3. On each client system from which you want to unconfigure the client, Click Start > Run and type `%vcsone_home%` It explores the VCS One installation path. Delete the Data folder from the directory.

---

Uninstalling the VCS One client on Windows - using the installer

To uninstall the VCS One client on Windows:

1. Go to Start > Settings > Control Panel > Add or Remove Programs.
   
   In case you are working on Windows Server 2008, go to Programs and Features. (Start > Settings > Control Panel > Programs and Features)

2. Scroll to Veritas Cluster Server One Client 5.0 SP2 for Windows and select it.

3. Click Remove.
   
   In case of Windows Server 2008, click Uninstall.

4. On the VCS One Client Installation wizard welcome page, review the list of prerequisites and click Next.

5. On the System Selection panel, add the systems from which you want to uninstall the VCS One client. You can perform this in one of the following ways:
   
   - In the System Name text box, manually type the system name and click Add.
   - Alternatively, browse to select the systems.
     
     The systems that belong to the domain in which you have logged in are listed in the Available Systems list. Select one or more systems and click the right arrow to move them to the Selected Systems list. Click OK Once you add or select a system, the wizard performs the verification checks and notes the verification details. To review the details, click the corresponding information icon.
Uninstalling VCS One software

Uninstalling the VCS One client on Windows Server Core

Note: By default the local system is selected for un-installation. In case you are performing a remote un-installation and do not want to uninstall the client from the local system, click the corresponding <remove> icon to remove the system from the list.

6  Click Next.
   Note that the wizard fails to proceed with the un-installation, unless all the selected systems have passed the validation checks and are ready for un-installation. In case the validation checks have failed on any of the system, review the details and rectify the issue. Before you choose to proceed with the un-installation click Re-verify to re-initiate the verification checks for this system.

7  On the Pre-uninstall Summary panel, review the summary and click Next.

8  On the Client Un-installation panel, review the uninstallation progress and click Next when the uninstallation is complete.

9  On the Post-uninstall Summary panel, review the uninstallation results and click Next.
   If the un-installation has failed on any of the system, review its summary report and check the log file for details.

10 On the Finish panel, click Finish.

Uninstalling the VCS One client on Windows Server Core

To uninstall the VCS One client on Server Core

1  Open a command window by clicking Start > Run.

2  Enter cmd in the Open field and click OK.

3  In the command window, navigate to the root directory of the product CD.

4  Use the following command syntax to silently uninstall the client:
   
   ```cmd
   Setup.exe /s INSTALL_MODE=5 SOLUTIONS="1"
   [INSTALLDIR="InstallDirPath"]
   ```
Parameters for setup.exe

Table 5-1 contains information about the possible parameter values.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/s</td>
<td>Set for silent mode. If not set, boots the product installer GUI.</td>
</tr>
</tbody>
</table>
| INSTALL_MODE  | Set to indicate an installation or uninstallation.  
1 = To install  
5 = To uninstall  
Example: INSTALL_MODE=5 |
| SOLUTIONS     | Set to the type of installation  
1 = VCS One Client 5.0 SP2  
Example: SOLUTIONS=1 |
| INSTALLDIR    | Use only to set a non-default path for the installation directory. The path must start and end with a quotation mark (").
Example: INSTALLDIR="C:\InstallationDirectory"
The default setting, used when you do not specify a path, is SystemDrive:\Program Files\Veritas  
If the path has blank spaces in it, the path should be set off with back slashes as in the following example:  
Example: INSTALLDIR="C:\Program Files (x86)" |
About uninstalling the VCS One client from an ESX server

To uninstall the VCS One client software from an ESX Server, use the uninstallation programs provided. On systems where the software has been installed, you can find the uninstallation programs in the directory /opt/VRTS/install.

The uninstallation programs are also provided on the VCS One software discs.

Note: Before you begin to uninstall the client software, ensure that no VFrame is configured on this ESX Server.
For more details on unconfiguring and removing the VFrames, refer to Veritas Cluster Server Users Guide.

Uninstalling the VCS One client from an ESX Server

The uninstallation script uninstalls the VCS One client, which communicates securely with the Policy Master, and starts and stops the agents on the local system.

Launching the installer

To Launch the installer

1. Navigate to the directory containing the uninstallvcsonecd program. Enter the following:
   cd /opt/VRTS/install

2. If you plan to use the uninstallation program on the software disc, mount the software disc for Red Hat Enterprise Linux 4 (RHEL 4) x86 (32-bit) or RHEL 5 x86_64, on the system where the VCS One client is installed.
   Enter the following:
   cd platform
   where platform is the platform-specific directory, such as esx4_x86_64 for ESX 4.0 or esx30_i686 for ESX 3.0.
   Navigate to the directory cluster_server_one.

3. Start the client uninstallation script. Enter the following:
   ./uninstallvcsonecd
**Uninstalling VCS One software**

**Uninstalling the VCS One client from an ESX Server**

**Specifying the system to uninstall**

To specify the system to uninstall

1. At the system name prompt, enter the name of each system where you want to uninstall the VCS One client daemon software. If you have more than one system, separate the names by a space. (Fully-qualified domain names and IP addresses are acceptable.)

2. At the uninstallation confirmation prompt, enter the following: `y`.

**Deciding about evacuating service groups**

If there are any service groups that are online or intended to go online on the system, you can choose to evacuate them from this system or leave them in the current state. If you evacuate the service groups, they are brought offline and fail over to another system, if possible. If you do not evacuate the service groups, the installer leaves them in their current state.

To decide about evacuating service groups

- At the service group evacuation prompt, specify if you want to evacuate the service groups that are currently online. Enter one of the following: `y` or `n`.

**Removing residual directories**

Symantec recommends that you remove the following residual VCS One program directories: `/opt/VRTSvcsone`, `/etc/VRTSvcsone`, and `/var/VRTSvcsone`.

To remove residual directories

- Remove the recommended residual VCS One program directories. Enter `y`.

The program uninstalls the software and indicates where uninstallation logs are placed.
Uninstalling the Simulator

The following section describes how to uninstall the Simulator.

To uninstall the Simulator

1. Make sure that all Simulator instances are stopped. If a Simulator instance is running, stop it using one of the following methods:
   ■ Stop all running instances using the VCS One Simulator Launch Pad shortcut on the desktop.
   ■ Use the following command at the Windows command prompt:
     
     ```
     installation_location\VCSOne\hamultisim -stopsim instance_name
     ```

     where `installation_location` is the directory location where you installed the Simulator and `instance_name` is the name of the running Simulator instance. If multiple Simulator instances are running, enter this command for each Simulator instance.

     To stop the default Simulator instance, do one of the following:
       ■ At the Windows command prompt, run the following batch file script:
         
         ```
         installation_location\VCSOne\stopsim.bat
         ```
       ■ At the Windows command prompt, enter the following command:
         
         ```
         installation_location\VCSOne\hamultisim -stopsim default
         ```

2. Go to the directory where you installed the Simulator.

3. Select the `VCSOne` subdirectory.

4. Delete the `VCSOne` subdirectory and its contents.
   Deleting the `VCSOne` subdirectory removes the Simulator from the system.

5. Delete the VCS One Simulator Launch Pad shortcut from the desktop.
Uninstalling VCS One software

Uninstalling the Simulator
Required UNIX packages

This appendix provides information about the VCS One client packages. If you choose to install the client on an ESX Server, ensure that you install these mandatory client packages.

Mandatory client packages for UNIX

Table A-1 lists the packages to install.

<table>
<thead>
<tr>
<th>Package</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRTSperl</td>
<td>Veritas Perl 5.10 redistribution</td>
</tr>
<tr>
<td>VRTSvcsoneut</td>
<td>Veritas Cluster Server One by Symantec - utilities</td>
</tr>
<tr>
<td>VRTSvcsonemg</td>
<td>Veritas Cluster Server One by Symantec - message catalogs</td>
</tr>
<tr>
<td>VRTSvcsonenm</td>
<td>Veritas Cluster Server One by Symantec - man pages</td>
</tr>
<tr>
<td>VRTSvcsonec</td>
<td>Veritas Cluster Server One by Symantec - command line utilities</td>
</tr>
<tr>
<td>VRTSvcsonecd</td>
<td>Veritas Cluster Server One by Symantec - client daemon</td>
</tr>
<tr>
<td>VRTSvcsoneag</td>
<td>Veritas Cluster Server One by Symantec - bundled agents</td>
</tr>
<tr>
<td>VRTSvcsoneesx</td>
<td>Veritas Cluster Server One by Symantec - VMware ESX agents</td>
</tr>
</tbody>
</table>

Note: This package is mandatory if your client is required to manage an ESX or ESXi server.

<table>
<thead>
<tr>
<th>Package</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRTSspt</td>
<td>Veritas Cluster Server One by Symantec - Veritas software support tools</td>
</tr>
</tbody>
</table>
Required UNIX packages
Mandatory client packages for UNIX

<table>
<thead>
<tr>
<th>Package</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRTSsfmh</td>
<td>Veritas Storage Foundation Managed Host by Symantec (Linux only)</td>
</tr>
</tbody>
</table>
Troubleshooting

This appendix includes the following topics:

- Re-authenticating the client on Windows
- Failure in configuring the Windows Policy Master
- Updated list of remote Windows Server 2008 x64 systems is not available during the Policy Master installation or uninstallation
- Policy Master installation has partially or completely failed on any system
- Client configuration fails on Windows
- Handling the user authentication failure
- Client authentication fails with an error - The Policy Master user does not have privileges to add the system to the cluster
- Restarting the Veritas Storage Agent service
- Policy Master is successfully installed on a remote node but shows the status as Failed
- Handling the system validation failure
Re-authenticating the client on Windows

If authentication fails, the VCS One client does not start. If the client fails to start, check the client log for details about the failure, and follow the instructions in this section to reauthenticate the client.

How to recognize if authentication has failed

This section provides a sample client log message for an authentication failure. The following error message is shown in the client log file at: %vcsone_home%\log (typically, C:\Program Files\Veritas\Cluster Server One\log):

2008-08-25 15:26:31 VCS One ERROR V-97-19-12358 Failed to obtain the credential from Local cache, please ensure that the System credential is deployed on the node and the System does not lag behind the PM node

If authentication fails, the product installer does not display an error message during installation, but the installer log contains the following message:

haat execpkg ERROR V-18-7135 Failed to execute package

The installer log file is at %allusersprofile%\application data\Veritas\VPI\log.

Reasons authentication might fail

When you install the VCS One client on UNIX or Windows, authentication can fail for the following reasons:

- Incorrectly set firewall ports that cause communication issues.
- The client system time lags behind the Policy Master server time by more than 30 minutes.
- The installer did not add a principle for the client.

If you upgrade the client, the credential may no longer be valid for one of the following reasons:

- The credentials were not backed up
- The client credential cache is deleted
- You did not re-deploy the client
- Credentials are not valid with the current broker

Re-authenticating the client

If the client log file indicates that authentication failed, follow the steps in this section to re-authenticate the client on Windows or UNIX.
To re-authenticate the client

1. From the Policy Master, create a new credential. For instructions on creating a deployment credential, see: "Creating a permanent credential package" on page 80.

2. Do one of the following:

   On Linux or UNIX Skip to step 4.

   On Windows Open a command prompt and set the environment variables. Enter the following:
   - set EAT_HOME_DIR=%vcsone_home%
   - set EAT_CATALOG_DIR=%vcsone_home%
   Set these environment variables from the command line. Do not set them from the VCS One web console.
   Then, go to step 4.

3. Do one of the following:

   On Linux or UNIX Change directories to the /bin directory. Enter the following:
   - cd /opt/VRTSvcsone/bin

   On Windows change directories to %vcsone_home%\bin. Enter the following:
   - cd %vcsone_home%\bin

4. On Windows or UNIX, from the bin directory, reauthenticate the client. Enter the following:
   haat execpkg -i full_path_to_deployment_package -o
   The full path to the deployment package should include the file name.

5. Restart the VCS One client.

Policy Master installation has partially or completely failed on any system

If the Policy Master installation has partially or completely failed on any of the system, refer to logs and rectify the reason for its failure.

After you rectify the issue, uninstall the Policy Master software from the system where the installation had failed and then relaunch the installation wizard.
Failure in configuring the Windows Policy Master

While running the Windows Policy Master Configuration Wizard, one of the configuration tasks may fail. If such a failure occurs, do the following:

- Leaving the wizard running, review logs and rectify the cause of the failure. Then, return to the Policy Master Configuration Wizard and click **Next** to continue with the configuration steps.

- If the wizard again shows that a configuration task failed, you can check for another cause of failure and rectify it. You can click **Next** multiple times, each time after rectifying an error that caused the failure.

- If you cancel the wizard with some tasks completed and others failed, and then restart the wizard, system verification may fail. If this occurs, you can use the following command to remove the existing Policy Master configuration (unconfigure the completed tasks):
  ```bash
  %VCSONE_HOME%\bin\ConfigureVCOne.bat -unconfigure -wizard
  ```
  After the command completes the configuration cleanup, launch the Policy Master Configuration Wizard again to create a new configuration.
  The command does not remove an SFW disk group or volume, if one was included in the configuration.

- If the unconfigure command fails to unconfigure the Policy Master, it may be necessary to uninstall the Policy Master software to recover from the error. After you complete uninstalling the software and rebooting the Policy Master systems, you can again install and configure the Policy Master software.

Updated list of remote Windows Server 2008 x64 systems is not available during the Policy Master installation or uninstallation

The Microsoft Computer Browser service helps maintain an updated list of domains, workgroups, and server computers on the network and supplies this list upon request. This service must be enabled to discover and display all the systems within the domain.

By default, systems running Windows Server 2008 x64 disable the Computer Browser service. With this service disabled, an updated list of systems available in the domain are not displayed during the Policy Master installation.

Enable the Computer Browser Service on your Windows Server 2008 x64 before installing the Policy Master. Refer to your Microsoft documentation for information about enabling the Computer Browser service.
Client configuration fails on Windows

The Windows client configuration could fail with the error message “Failed to create system user deployment package.” This could happen if the client system name cannot be resolved or the client system IP address is not reachable from the Policy Master Server.

This situation occurs if IPv6 is configured on the client or the Policy Master system.

To resolve the issue, unconfigure IPv6 from the network settings of the client and Policy Master system and then delete the client system from the list of systems added to the Policy Master Server. After the client system is deleted from the Policy Master Server, relaunch the client configuration wizard.

Windows client configuration wizard error

During the client configuration, the client configuration wizard could display the error message “Unable to determine the status of Veritas Storage Foundation Messaging Service.” If you see this message, the server logs show a Server not found error.

This issue could be caused by:

■ A mismatch between the client system authentication keys (public and private) and the certificate issued by the authentication broker to the Policy Master.

■ Corrupt or non-existent authentication keys.

Workaround:

Regenerate the local system’s credentials on the Policy Master.

To regenerate the local system’s credentials, perform the following steps on the Policy Master:

1. Navigate to the following directory and delete the file 4b72cd6.0
   %ProgramData%\Veritas\Security\Authentication\VRTSat_lhc

2. Run the following commands from the command prompt:
   net stop xprtld
   net start xprtld
   Alternatively, you can also opt to run the services console and restart the Veritas Storage Foundation Management Service.
Handling the user authentication failure

During the client configuration or while creating a service group, the user authentication may fail if your user name exceeds 20 characters.

This issue occurs because, the Windows Active Directory allows you to create a user with the user name having more than 20 characters. VCS One also supports user name with more that 20 characters. However the authentication broker does not support user names exceeding 20 characters.

In a situation where you attempt to login with the user name exceeding 20 characters, the authentication fails.

**Workaround:**

While creating users, ensure that you do not exceed 20 characters or use the pre-Windows 2000 logon name (truncated user name up to 20 characters) to login or work with VCS One.

Client authentication fails with an error - The Policy Master user does not have privileges to add the system to the cluster

During the client configuration the client configuration may fail with the above error, even though the user has administrative privileges on the Policy Master.

This issue occurs if the user is a part of any usergroup that is added to the administrator’s group on the Policy Master.

**Workaround:**

Add the user as an individual to the administrator's group of the Policy Master server.

Restarting the Veritas Storage Agent service

During the client installation the installer stops the Veritas Storage Agent service (VxVM), if running, and restarts it after the client is successfully installed.

However, in case of installation failure, the installer may fail to restart the VxVM service.

**Workaround:**

Manually start the service, following the steps below:

1. Open the Services panel. Click **Start > Run**.
Policy Master is successfully installed on a remote node but shows the status as Failed

During the Policy Master installation, the installer may successfully complete the installation on a remote system, but the status would reflect a failure. This situation typically occurs due to slow network.

**Workaround:**
Ignore the incorrect status and proceed with the cluster configuration.

Handling the system validation failure

During the VCS One Client or Policy Master installation you may experience the system validation failure (on the System Selection page), with the “Failed to check package.....” error.

**Workaround:**
Select the system and click **Reverify**.
Alternatively, exit the wizard session and relaunch the installer.
Troubleshooting
Handling the system validation failure
A
  authentication service 17

C
  client license 17
  client, uninstalling 71
  commands
    ./uninstallvcsonecd, uninstalling client 71
    haadmin 32
    hamultisim -stopsim 73
  configuration
    Policy Master on Windows

D
  disaster recovery 34

F
  firewalls 21

G
  global clustering 34

H
  haadmin command 32

I
  Installation
    prerequisites for Windows Policy Master 21
    installation
      Policy Master 23
      Simulator 60
    installation prerequisites
      Simulator 60
    installing
      Simulator 60
    installvcsonecd installation program 47

L
  license key 17
  licensing 17

P
  PMSG (Policy Master service group) 32
  Policy Master
    configuration prerequisites on Windows 28
    configuration wizard 29
    configuration wizard on Windows 29
    installation on Windows 23
    required ports on Windows 21
    troubleshooting configuration 80
    verifying configuration on Windows 32
  Policy Master cluster
    displaying status with haadmin 32
  Policy Master service group (PMSG)
    checking state after installation 32
    ports used by the Windows Policy Master 21
    product licensing 17

R
  remove Policy Master configuration 80

S
  server farm, setting up 20
  services used by Windows Policy Master
    Policy Master
      services on Windows 21
  setting up server farm 20
  Simulator
    installation 60
    installation prerequisites 60
    installing 60
  Simulator, stopping 73
  stopping the Simulator 73
  Symantec Product Authentication Service
    backing up configuration 33
U
unconfigure Policy Master 80
uninstalling
  VCS One client daemon
    Windows 64, 67
uninstalling VCS One 63

V
VCS One
  license 17
VCS One client daemon
  packages 75
  uninstalling on Windows 64, 67
VCS One client daemon software
  installing 47
VCS One Product Authentication Service 17
VCS One Simulator
  installation prerequisites 60
VCS One simulator
  installing 60

W
Windows Policy Master
  services 21
Windows Policy Master ports 21