Symantec Product Authentication Service™ Installation Guide

Linux, Microsoft Windows, and UNIX

4.3

N18677C

Symantec Product Authentication Service Installation Guide

Symantec Product Authentication Service Installation Guide
Doc Version: 2,1

Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014
www.symantec.com

Printed in the United States of America.

Third-party legal notices

Third-party software may be recommended, distributed, embedded, or bundled with this Symantec product. Such third-party software is licensed separately by its copyright holder. All third-party copyrights associated with this product are listed in the accompanying release notes.

AIX is a registered trademark of IBM Corporation.

HP-UX is a registered trademark of Hewlett-Packard Development Company, L.P.

Linux is a registered trademark of Linus Torvalds.

Solaris is a trademark of Sun Microsystems, Inc.

Windows is a registered trademark of Microsoft Corporation.

Oracle is a registered trademark of Oracle Corporation.

Technical support

For technical assistance, visit http://support.veritas.com (rather than http://support/symantec.com) and select phone or email support. Use the Knowledge Base search feature to access resources such as TechNotes, product alerts, software downloads, hardware compatibility lists, and our customer email notification service.

Contents

Preface

This document is intended for those who will install and configure the Symantec Product Authentication Service. We assume that readers have a comprehensive understanding of the environment in which they wish to install the product.

The preface includes the following sections:

What's In This Manual?

This document does not contain introductory information about Symantec Product Authentication Service -- its purpose, its use, basic terminology and concepts, or high level descriptions of architecture. For those matters, see the Symantec Product Authentication Service *Administrator's Guide* and Symantec Product Authorization Service *Administrator's Guide*.

Table 1-1 Chapters in this Manual

Chapter or Appendix	Description
"System Requirements"	Explains the system requirements and recommendations for installing and running Symantec Product Authentication Services.
"Basic Installation Instructions"	Discusses methods of installing and uninstalling Symantec Product Authentication Service.
"Using Language Packages and Patches"	Discusses methods of installing and uninstalling Symantec translated language packages.
"High Availability Installation"	Explains how to install and configure Symantec Product Authentication Service for high availability

Table 1-1 Chapters in this Manual

Chapter or Appendix	Description
"Running the Administration Console"	Explains how to run the Administration Console, after you have installed and configured. For detailed information on performing the tasks you can perform through the Console, see the Administrators Guide.
"Installing with UNIX OS Tools"	Recognizing that some users may prefer to use the OS tools specific to their own UNIX system, this appendix provides instructions for doing so
"Configuring to Work with a Web Console"	Explains why a product web credential is needed when working with a web console and provides an example of configuring to use a web console with Symantec Enterprise Administrator.

Accessibility

Symantec products meet federal accessibility requirements for software as defined in Section 508 of the Rehabilitation Act:

- http://www.access-board.gov/508.htm

Conventions

The following describes typographical and other conventions used in this guide.

Typographic Conventions

Table 1-2 Typographic Conventions

Typeface	Usage
`Bold fixed width`	Input. For example, type **`cd`** to change directories.
`Fixed width`	Paths, commands, filenames, or output. For example: The default installation directory is `/opt/VRTSxx`.
Italics	Book titles, new terms, or used for emphasis. For example: Do *not* ignore cautions.

Table 1-2 Typographic Conventions

Typeface	Usage
Sans serif (italics)	Placeholder text or variables. For example: Replace *filename* with the name of your file.
Serif (no italics)	Graphical user interface (GUI) objects, such as fields, menu choices, etc. For example: Enter your password in the **Password** field.

Notes and Cautions

Note: This is a Note. Notes are used to call attention to information that makes using the product easier or helps in avoiding problems.

Caution: This is a Caution. Cautions are used to warn about situations that could cause data loss.

Key Combinations

Some keyboard command sequences use two or more keys at the same time. For example, holding down the **Ctrl** key while pressing another key. Keyboard command sequences are indicated by connecting the keys with a plus sign. For example:

Press **Ctrl+t**

Symantec Product Authentication Service Manuals

The following manuals, along with the online help, comprise the Symantec Product Authentication Service documentation set:

Table 1-3 Manuals in Product Authentication Service Documentation Set

Manual Title	Filename
Symantec Product Authentication Service *Installation Guide*	AT_InstallGuide.pdf
Symantec Product Authentication Service *Administrator's Guide*	AT_AdminGuide.pdf

Chapter 1

System Requirements

This section explains the system requirements and recommendations for installing and running Symantec Product Authentication Service.

The Symantec Product Authentication Service is responsible for validating identities and for protecting communications channels between Symantec application clients and Symantec Application services. System requirements for the Authentication Service will duplicate -- and occasionally expand upon -- the requirements for the applications with which it is running.

Hardware Requirements

The Symantec Product Authentication Service installers check for disk space and will generate an error message if sufficient space is not allocated.

Software

Individual Symantec resource management applications have their own hardware requirements. Consult the manual(s) for the individual resource management application(s) with which you will be running Symantec Product Authentication Service.

Supported Platforms: Authentication

The following chart shows support for Symantec Product Authentication Service:

Platform	Symantec Product Authentication Service Support
AIX 4.3.3.10, 5.1, 5.2, 5.3 (32 bit)	Server and Client
AIX 5.1, 5.2, 5.3 (PPC 64bit)	Client only
FreeBSD 4.9 (x86)	Client only
HPUX 11.00, 11.11, 11.23	Server and Client
HPUX 11.23 PI (32 bit)	Server and Client
HPUX 11.23 PI (64 bit)	Server and Client
IRIX 6.5.15-22 (MIPS-32)	Client only
Linux Redhat AS 2.1 (on x86)	Server and Client
Linux AS/ES 3.0 (on x86)	Server and Client
Linux Redhat AS/ES 3.0 (on IA64)	Server and Client (64 bit)
Linux Redhat EL 4.0 (on x86)	Server and Client
Linux Redhat EL 4.0 (on IA 64)	Server and Client (64 bit)
Linux Redhat EL 4.0 (on x86_64)	Server and Client (32 bit compatibility mode); Client (64 bit)
Linux SuSe SLES 8.0, 9.0 (on x86)	Server and Client
Linux SuSe SLES 8.0, 9.0 (on IA64)	Server and Client (64 bit)

Platform	Symantec Product Authentication Service Support
Linux SuSe SLES 9.0 (on x86_64)	Server and Client (32 bit compatibility mode); Client (64 bit)
Linux MontaVista 11.0 (on x86)	Client only
Linux WS 21, 30 (on x86)	Client only
Mac OS 10.3 (PPC)	Client only
Solaris 6	Desupported Symantec Product Authentication Service 4.2 and above
Solaris 7, 8, 9, 10	Server and Client
Solaris 7, 8, 9, 10 (64 bit)	Server and Client
Tru64 5.1, 5.2	Server and Client
Windows 2000, 2003 (on x86)	Server and Client
Windows XP SP1 and SP2 (on x86)	Server and Client
Windows Storage Server 2003 (on x86)	Server and Client
Windows 2000 SAK, SAK Business Server (on x86)	Client only
Windows 2003 (on x86_64)	Client only (64 bit and 32 bit compatibility mode)
Windows 2003 (on IA64)	Server and Client (64 bit and 32 bit compatibility mode)

Required Patches and Service Packs

Below is a list of patches for HPUX 11.x. Some or all of the patches mentioned in this document may have been revised. If the base patch is unavailable, the cumulative patch containing the base patch should be applied.

Patches Required for HP 11.00

The chart below lists patches for HP 11.00.

Table 1-4 Patches for HP 11.00

Patch ID	Patch Description
PHSS_26559	s700_800 11.00 ld(1) and linker tools cumulative patch
PHSS_24303	11.0 ld(1) and linker tools cumulative patch

Table 1-4 Patches for HP 11.00

Patch ID	Patch Description
PHSS_24627	11.0 HP aC++ -AA runtime libraries (aCC A.03.33)
PHSS_26945	11.0 HP aC++ -AA runtime libraries (aCC A.03.37)
PHCO_18227	11.0 libc cumulative patch
PHCO_29633	11.0 libc cumulative patch
PHCO_26960	Pthread library cumulative patch

Patches Required for HP 11.11

The chart below lists patches for HP 11.11.

Table 1-5 Patches for HP 11.11

Patch ID	Description
PHSS_26560	1.0 ld(1) and linker tools
PHSS_24304	1.0 ld(1) linker tools cumulative patch
PHSS_26946	1.0 ld(1) HO aC++ run-time libraries a3.37
PHSS_32226	s700_800 11.11 libcl patch

Patches Required for Solaris

For Sun Solaris 2.9 Sparc, we require users to install SUN patch 112907-03 and 112908-17.

Service Packs

The list below shows service packs required for successful installation of Symantec Product Authentication Service on the Windows platform:

- For NT 4.0, service pack 3
- For Windows 2000, service pack 2

Other Requirements

The minimum glibc version needed on a Linux RedHat EL 4.0 32bit machine is 2.3.4-2.9.

Before installing Symantec Product Authentication Service into a non-standard SUN Solaris OS, make sure SUN Enterprise Authentication Mechanism (SEAM) is installed. SEAM is needed to facilitate GSS-API authentication.

Dependencies

In preparing to install Symantec Product Authentication Service, it helps to understand the way the components depend upon each other.

- Least dependent of the components is the Authentication Client. An Authentication Client can reside alone on a machine. It does not require the Authentication Service or any part of Symantec Product Authorization Service to be present on the same machine, although the Authentication Service has to exist somewhere.
- The Authentication Service needs an Authentication Client on the same machine.

Configuration Requirements for Running the Console

The Administration Console can run in two modes: Authentication Only and Authentication Plus Authorization.

To run the Administration Console, you must meet the following prerequisites:

- For AIX, make sure Jave 1.3x is installed on your system and is pointed to in your PATH statement.
- For systems other than AIX, make sure Java 1.4.2 or above is installed on your system and is pointed to in your PATH statement. To download JDK/ JRE visit the following sites:
  - For SUN, Linux, Windows: the Java web site
  - For HP-UX: the Hewlett Packard web site
- For TRU-64 and HP-UX, semaphore queue size should be set to 256 or more. The number of processes should also be set to 256 or more. In some cases due to lack of availability of above systems resources the Authorization Service may fail to come up.
- On HP, in a cluster environment, memory size should be 1GB or more.
- Symantec Product Authentication Service requires JDK 1.4.0 or above for running the graphical user interface.
- You must have name resolution of hostnames.
- Perl 5.6 or above should exist on your system.

Note: Perl should reside in a directory whose path name has no spaces.

Chapter 2

Basic Installation Instructions

This chapter discusses installation of the Symantec Product Authentication Service. It includes the following topics:

- An overview of methods you can use to install, configure, and uninstall
- An overview of tasks involved in setting up Symantec Authentication Service
- Instructions for installing, configuring, and uninstalling on Windows platforms
- Instructions for installing, configuring, and uninstalling on UNIX platforms
- Instructions for starting and stopping the service

For information on installing in a cluster environment, see “High Availability Installation” on page 53.

For information on installing language packages, see “Using Language Packages and Patches” on page 43.

Methods for Installing and Configuring

You can install Symantec Authentication Service on Windows platforms or UNIX platforms. (See “System Requirements.”)

Note: If you upgrade, at the end of the upgrade process, the installer will prompt to reboot the machine. You should do so. It is necessary to restart the machine so that all the dependent products of the Symantec Product Authentication Service will pick up the newer version.

Windows Installation Methods

On a Windows platform, you can install in the following ways:

- Using a traditional wizard. You progress through the wizard by completing each wizard screen and clicking **Next**, and you complete by clicking **Finish**. Although a Wizard can be launched using the MSI file, our instructions for interactive installation describe using `VxSSVRTSatSetup.exec`.
- Using one of two silent modes:
  - Silent installation using `VxSSVRTSatSetup.exe`: requires one manual installation, but any number of silent installations can be performed thereafter.
  - Silent installation using an MSI file, "`VERITAS Authentication Service.msi`."

UNIX Installation Methods

For UNIX, Symantec Product Authentication Service is installed as part of Infrastructure Core Services. If you install on a UNIX platform, there are two installation methods:

- Interactively, using a method that is valid for all UNIX platforms. This method is described in the present chapter.
- Interactively, using the OS tools specific to your platform. For details on these types of installation, see “Installing Authentication with UNIX OS Tools.” .
- Silently by using a response file generated if you installed one time manually through the ICS installer.

  A response file is generated with every interactive install through the `installics` program. The full path name of the generated response file will be printed on the screen at the end of the install. It looks something like this:

`/opt/VRTS/install/logs/installics207163245.response`
Later this file can be used to silent install with the following command:
`installics -responsefile <response file>`
For more information on installing through `installics`, see the *ICS Installation Guide*.

Basic Tasks Involved in Setting Up Authentication

You must install at least one Root Broker, one Authentication Broker, and one Authentication Client. You should follow the order below:

1 Install a Root Broker
You can install a Root broker, either on the same machine as an Authentication Broker or on a separate machine:

- **Root + AB**: Installs the Root Broker and the Authentication Broker on the same machine. (There may or may not be a Client on this machine.) This is a single process listening on a single port.

Note: Root + AB is the simplest installation and configuration mode, but you should read about the other modes before deciding whether this is the one you want, because if you change your mind, you will need to uninstall.

- **Root Only**: Installs the Root Broker on a machine without an Authentication Broker. (There may or may not be a Client on this machine.) You may want to choose this mode if you feel that installing the Root Broker on a very secure machine separate from any other Authentication Brokers will increase security. You might also choose Root Only mode if you have multiple OS domains. For example, you could install a Root Broker on the host, and then an Authentication Broker for Windows on a second machine, an Authentication Broker for NIS on a third, an Authentication Broker for NISplus on a fourth, etc.

Note: If you select this mode, you will have to install at least one Authentication Broker elsewhere. Symantec Product Authentication Service cannot function without both a Root Broker and an Authentication Broker.

---

2 Install an Authentication Broker (required, if you did not select Root + AB)
The **AB Only** mode installs an Authentication Broker on a machine without the Root Broker. (There may or may not be a Client on this machine.) You may select this option because you have already installed the Root separately somewhere, and you therefore need to have an Authentication Broker. Or you may want more than one Authentication Broker.

In either case, installing in AB Only mode is a more complex process and requires several preparatory steps. You should not attempt to install in AB Only mode unless you have performed the preliminary procedures.

3 Install clients
The installation process lets you install the Client at the same time as the service or separately.

Installing a Root or Root + Authentication Broker

Your first task is to install a Root, either without an Authentication Broker on a machine (Root Only mode) or on the same machine as an Authentication Broker (Root + AB mode). This section explains how to install on Windows and UNIX platforms.

Windows Installation of Root or Root + AB

On a Windows platform, you can install Root or Root + AB either interactively or in silent mode.

Note: We strongly recommend that consumers who directly consume native packages of Symantec Product Authentication Service 4.3 change the default broker admin passwords upon installation. See “Changing Passwords After Installation”.

Wizard Install of Root or Root + AB

The `VxSSVRTSatSetup.exe` install of Authentication uses a traditional Wizard.

To install on Windows using a traditional wizard

Note: Read “High Availability Installation.” for information about installing in cluster environments.

---

1 Log on as administrator on the machine where you want to install.

2 Confirm that the machine uses the NTFS filesystem. FAT does not provide any file system security and hence compromises the security of Symantec Product Authentication Service.

3 Run `VxSSVRTSatSetup.exe` from the CD.

4 When the opening InstallShield wizard screen is displayed, click **Next**.

5 When the Setup Type screen is displayed, select **Complete**, and click **Next**.

Note: Note that by default (that is, Typical) only the Client is installed. To install the Service as well, you must select Complete.

---

6 Complete the Authentication Broker Service Options screen:

   a Select either **Root Broker Only** or **Root + Authentication Broker** (the simplest configuration).
   (If you plan to select Root Broker Only, you may want to read "Installing and Configuring an Authentication Broker" to see the tasks that will be involved when you subsequently set up your Authentication Broker.)

   b If you want to enable clustering, click the Service is Clustered checkbox and type in the cluster name. Cluster name is case sensitive.

   c Indicate whether the service is to be started manually or automatically and whether it is to be started immediately after installation.

   d When you have completed your selections, click **Next**.

7 When the Summary screen is displayed, click **Next**.

8 After the files are copied, the InstallShield Wizard Complete screen is displayed.

9 Click **Finish**.

Note: If you installed in Root Only mode, you must install an Authentication Broker elsewhere. Symantec Product Authentication Service cannot function without an Authentication Broker.

Silent Install of Root or Root + AB

On Windows, you can install the Root or Root + AB silently either by using the `VxSSVRTSatSetup.exe` or by using the MSI.

Performing Silent Installation with VxSSVRTSatSetup.exe:

Silent installation using `VxSSVRTSatSetup.exe` requires a one time manual installation step. Thereafter, multiple silent installations are possible.

Install once by running the installer with the "/r" option:

```
VxSSVRTSatSetup.exe /r /f1"c:\at.rsp"
```

This command launches the GUI and walks you through a set of dialogs. After you respond to the dialogs, the installer stores that information in a response

file that can be used to install silently any number of times using the following command:

```
VxSSVRTSatSetup.exe /s /f1"c:\at.rsp"
```

Note: Remember that if you install in Root Only mode, you must install an Authentication Broker elsewhere. Symantec Product Authentication Service cannot function without an Authentication Broker. If you plan to select Root Only, you may want to read "Installing and Configuring an Authentication Broker" to see the tasks that will be involved when you subsequently do set up your Authentication Broker.)

Performing Silent Installation with the MSI

The following commands assume you have the MSI file ("`VERITAS Authentication Services.msi`") in your current directory.

Note: BROKERMODE, INSTALLLEVEL, PASSWORD1/ PASSWORD2 are mandatory parameters for broker installs using MSI.

- Installing Client-Server in Root Only Mode

  ```
  msiexec /qn /i "VERITAS Authentication Service.msi"
  INSTALLLEVEL=2 BROKERMODE=r PASSWORD1 = pass1
  ```

- Installing Client-Server in Root + AB Mode

  ```
  msiexec /qn /i "VERITAS Authentication Service.msi"
  INSTALLLEVEL=2
  BROKERMODE=rab PASSWORD1=pass1 PASSWORD2=pass2
  ```

Whether you installed in the default location or in a custom location, you can also add arguments to do the following,:

- Specify the Cluster Name

  ```
  CLUSTERNAME=abcd
  ```

- Specify the SCM Start Type

  ```
  SCMSTARTTYPE=auto
  ```

  The other accepted value is manual, which is the default.

- Specify that the Service should be started after configuration

  ```
  STARTSERVICE=YES
  ```

  The other accepted value is manual, which is the default.

- Specify that an upgrade should not be performed

  DOUPGRADE=NO

  The other accepted value is YES, which is the default.

- Specify that a hookup with PBX should not be performed

INSTALLPBX=NO
The other accepted value is YES, which is the default.

UNIX Installation of Root or Root + AB

You can install on a UNIX platform either interactively or in silent mode.

Note: We strongly recommend that consumers who directly consume native packages of Symantec Product Authentication Service 4.3 change the default broker admin passwords upon installation. See “Changing Passwords After Installation”.

Interactive Installation of Root or Root + AB on UNIX

You can install interactively on a UNIX platform, using the same instructions for all varieties of UNIX supported by Symantec Product Authentication Service. If you prefer to use the OS tools specific to your platform, see “Installing Authentication with UNIX OS Tools” on page 85.

To install on any variety of UNIX

1. Log on as root on the host.

Note: An OS limitation in Tru64 prevents the installation process from detecting any previous version of Symantec Product Authentication Service already installed on a given host. Manually remove previous versions before attempting to install the latest version.

---

2. Make sure that no clients are running (Console, etc.).
3. Move to the directory on the CD that holds the `installics` program, and run `installics`.
4. Select **(I) Install a Product**.
5. Select **Symantec Product Authentication Service**.
6. Answer the prompts.
7. When asked **Do you Want to Install the Authentication Broker Server [y, n, q]**, select **y** to install both client and server.

Note: Do not be concerned if you see a message saying `Cannot Copy`. It is a benign message and will have no effect on your installation.

---

8 When prompted, indicate whether you want to configure at this point. If you select **n,** you can configure later by running `installics` again and selecting **(C) Configure an Installed Product**. If you select **y**, answer the remaining prompts as they occur. See "Configuring Outside the Install Process on UNIX".

9 When asked to select a mode, select Root Broker, Authentication Broker Only, or Authentication + Root Broker. (If you plan to select Root Broker, you may want to read "Installing and Configuring an Authentication Broker" to see the tasks that will be involved when you subsequently do set up your Authentication Broker.)

10 Indicate whether to do a cluster configuration, and answer the remaining prompts as they occur.
You will be asked for such things as the systems that are part of the cluster, the logical name of the cluster, the process path, the IP address. See Symantec Cluster Server documentation for further information on working with clusters.

11 After installation, you will need to add MANPATH. If you are using `sh` or `ksh`, use the following command:

```
MANPATH=/opt/VRTS/man:$MANPATH
export MANPATH
```

If you are using csh or tcsh, use the following command:

```
setenv MANPATH /opt/VRTS/man:$MANPATH
```

Note: Remember that if you installed in Root Only mode, you must install an Authentication Broker elsewhere. Symantec Product Authentication Service cannot function without an Authentication Broker.

Silent Installation of Root or Root + AB on UNIX

A response file is generated with every interactive install through the `installics` program. The full path name of the generated response file will be printed on the screen at the end of the install. It looks something like this:

```
/opt/VRTS/install/logs/installics207163245.response
```

Later this file can be used to silent install with the following command:

```
installics -responsefile <response file>
```

For more information on installing through `installics`, see the *ICS Installation Guide*.

Installing and Configuring an Authentication Broker

If you plan to install an Authentication Broker on a machine separate from a Root Broker, you must perform the following tasks:

1. Provision an identity for the Authentication Broker. (See "Provisioning an Identity for the Authentication Broker".)
2. Copy the root hash file from the Root machine to the Authentication Broker machine. (See "Finding and Copying the Root Hash File".)
3. Run the install program again to install the Authentication Broker machine. (See "Windows Installation of Authentication Broker" or "UNIX Installation of Authentication Broker".)

Provisioning an Identity for the Authentication Broker

The Authentication Broker cannot function as intended unless it has an identity provisioned for it in the Root Broker's private domain repository.

To provision an identity for the Authentication Broker

1. Go to the machine where a Root or Root + AB is installed, and log on as root or administrator.
2. Move to the `/bin` directory relative to where you installed authentication, and run the following command:

   ```
   vssat listpd --pdrtype root
   ```

   A typical output will be:

   ```
   Domain(s) Found 1
   ****************************
   Domain Name root@hostname.fullyqualifieddomain
   Expiry Interval 0
   ****************************
   ```

Note: Make note of the domain name. You will need to use this value for further commands.

---

3. Create the Authentication Broker identity by running the `addprpl` command as follows:

   ```
   vssat addprpl --domain root@hostname.fullyqualifieddomain --
   pdrtype root --prplname <ABonHostName> --password
   <SomeSecurePassword>
   ```

   Here the `--domain` argument uses the "Domain Name" returned by step #2.

<*ABOnHostName*> represents the identity of the Authentication Broker. This name can contain the hostname of the machine where the Authentication Broker is running.

<*SomeSecurePassword*> represents the password for the newly created Authentication. You must use a secure password that is not predictable. After doing this, the Root is configured to authenticate the Authentication Broker in AB Only mode.

Finding and Copying the Root Hash File

The Authentication Broker cannot function as intended unless it has a copy of the Root hash file.

To provide the Authentication Broker with the Root hash file

1. Log onto the machine that holds the Root where you created the Authentication Broker's identity.
2. Locate the Root hash file, which is created by the Authentication service when it is run in Root or Root+AB mode.

   The root hash file is named `root_hash` and can be found in the `/bin` directory relative to the directory where you installed the Authentication Service:

   - By default, on UNIX: `/opt/VRTSat/bin/root_hash`
   - By default, on Windows: `Program Files\VERITAS\Security\Authentication\bin\root_hash`.
3. Copy `root_hash` from the Root machine into some directory on the machine where you are planning to install the new Authentication Broker.

Windows Installation of Authentication Broker

On a Windows platform, you can install the Authentication Broker either interactively or in silent mode.

Wizard Install of Authentication Broker

The `VxSSVRTSatSetup.exe` install of Authentication uses a traditional Wizard.

To install on Windows using a traditional wizard

Note: For instructions on setting up for clustering, see "High Availability Installation".

---

1. Log on as administrator on the machine where you want to install the Authentication Broker.
2. Confirm that the machine uses the NTFS file system. FAT does not provide any file system security and hence compromises the security of Symantec Product Authentication Service.
3. Run `VxSSVRTSatSetup.exe` from the CD.
4. When the opening InstallShield wizard screen is displayed, click **Next**.
5. When the Setup Type screen is displayed, select **Complete** and click **Next**:
6. Complete the Authentication Broker Service Options screen:
   a. Select **Authentication Broker Only** mode.
   b. If you want to enable clustering, click the Service is Clustered checkbox and type in the cluster name. Cluster name is case sensitive.
   c. Indicate whether the service is to be started manually or automatically and whether it is to be started immediately after installation.
   d. Click **Next**.
7. Complete the Authentication Broker Identity screen:
   - In the Root Broker area:
     - For Host Name, enter the host name or IP address that will allow the Authentication Broker to reach the Root Broker.
     - For Port, the default 2821 is displayed and can be changed.
     - For Hash File, click **Browse** to browse for the `root_hash` file you copied from the Root Broker.
   - In the Broker Identity area:
     - For Name, enter the identity of the Authentication Broker as configured in the Root Broker's private domain repository.
     - For Password, enter the password for the Authentication Broker as configured in the Root Broker's private domain repository.
     - For Domain Name, enter the domain in which the Root and this Authentication Broker reside.
   - When all fields are complete, click **Next**.
8. When the InstallShield Wizard Complete screen is displayed, click **Finish**.

Silent Install of Authentication Broker

On Windows, you can install the Authentication Broker silently either by using the `VxSSVRTSatSetup.exe` or by using the MSI.

Performing Silent Installation with `VxSSVRTSatSetup.exe`:

Silent installation using `VxSSVRTSatSetup.exe` requires a one time manual installation step. Thereafter, multiple silent installations are possible.

Install once by running the installer with the "/r" option:

```
VxSSVRTSatSetup.exe /r /f1"c:\at.rsp"
```

This command launches the GUI and walks you through a set of dialogs. After you respond to the dialogs, the installer stores that information in a response file that can be used to install silently any number of times using the following command:

```
VxSSVRTSatSetup.exe /s /f1"c:\at.rsp"
```

Performing Silent Installation with the MSI

The following commands assume you have the MSI file ("`VERITAS Authentication Services.msi`") in your current directory.

Note: BROKERMODE is a mandatory parameter for broker installs using MSI.

```
msiexec /qn /i "VERITAS Authentication Service.msi"
INSTALLLEVEL=2  BROKERMODE=ab IDENTITY=<broker account in the
root domain>  PASSWORD=<broker account password in root domain>
DOMAIN=root@<fully qualified root machine name> ROOTHOST=<fully
qualified root machine name> ROOTPORT=<root broker port number>
ROOTHASH=<root hash file>
```

The properties after BROKERMODE in the above command are ignored if brokermode is not ab.

To configure with the response file, run the `vssconfig.exe` command and point to the created `vssconfig.xml` file, as follows:

```
<InstallDir>\Authentication\bin\vssconfig.exe ..\vssconfig.xml
```

UNIX Installation of Authentication Broker

You can install on a UNIX platform either interactively or in silent mode.

Interactive Installation of Authentication Broker on UNIX

You can install interactively on a UNIX platform, using the same instructions for all varieties of UNIX supported by Symantec Product Authentication Service. If you prefer to use the OS tools specific to your platform, see “Installing Authentication with UNIX OS Tools” on page 85.

To install on any variety of UNIX

1 Log on as root on the host.

Note: An OS limitation in Tru64 prevents the installation process from detecting any previous version of Symantec Product Authentication Service already installed on a given host. Manually remove previous versions before attempting to install the latest version.

2 Make sure that no clients are running (Console, for example).

3 Move to the directory on the CD that holds the `installics` program, and run `installics`.

4 Select **(I) Install a Product**.

5 Select **Symantec Product Authentication Service**.

6 Answer the prompts.

7 When asked **Do you Want to Install the Authentication Broker Server [y, n, q]**, select **y** to install both client and server. (You cannot install the Root at this point if you select **n** to install client only.)

Note: Do not be concerned if you see a message saying `Cannot Copy`. It is a benign message and will have no effect on your installation.

8 When prompted, indicate whether you want to configure at this point. If you select **n,** you can configure later by running `installics` again and selecting **(C) Configure an Installed Product**. If you select **y**, answer the remaining prompts as they occur. See "Configuring Outside the Install Process on UNIX".

9 When asked to select a mode, select Authentication Broker Only.

10 Answer prompts providing the following:

- Machine name to configure Authentication Broker
- Name of host running the Root Broker
- Broker port (2821)
- Authentication Broker's identity
- Password
- Domain name (such as `root@mydomain.mycompany.com`)
- Complete path and file name of the file containing the root's hash (see "Finding and Copying the Root Hash File".)

11 Indicate whether to do a cluster configuration, and answer the remaining prompts as they occur.

- In the case of Symantec Cluster Server, you will be asked for such things as the systems that are part of the cluster, the logical name of the cluster, the process path, the IP address. See Symantec Cluster Server documentation for further information on working with clusters.
- In case of TruCluster, you may be asked for the cluster name.
- In the case of SunCluster, you will be asked for:
  - The device to be mounted as the shared storage
  - The block device which corresponds to the device mounted as shared storage. It is assumed that a ufs file system already exists on the shared storage.

Silent Installation of Authentication Broker on UNIX

A response file is generated with every interactive install through the `installics` program. The full path name of the generated response file will be printed on the screen at the end of the install. It looks something like this:

```
/opt/VRTS/install/logs/installics207163245.response
```

Later this file can be used to silent install with the following command:

```
installics -responsefile <response file>
```

For more information on installing through `installics`, see the *ICS Installation Guide*.

Consulting Installation Logs

The Windows Installer creates an MSI log in : `%temp%\vrtsatinstall.log`

A postinstall configuration log for authentication is kept in `<InstallDir>\postinstll.log`.

Starting and Stopping the Authentication Service

The installation process concludes by starting the Symantec Product Authentication Service; and the uninstallation process begins by stopping the service. If, however, you want to start or stop the Authentication Service at other times, use the following methods.

Starting and Stopping the Service on Windows

The Symantec Product Authentication Service starts automatically at the completion of installation, and it stops automatically at the beginning of

uninstallation. There may be other times, however, when you want to start or stop the Authentication Service.

Note: The broker should be configured in a specific mode (Root, Root+AB, or AB only) before starting it. Otherwise the broker will not come up.

Starting the Service

To start the Symantec Product Authentication Service on Windows, do either of the following:

- Use the start option in the Windows Service pane, or
- Execute the command in a command console: `net start vrtsat`

Stopping the Service

To stop the Symantec Product Authentication Service on Windows, do either of the following:

- Use the stop option in the Windows Service pane, or
- Execute the command in a command console: `net stop vrtsat`

Starting and Stopping the Service on UNIX

The Symantec Product Authentication Service starts automatically at the completion of installation, and it stops automatically at the beginning of uninstallation. There may be other times, however, when you want to start or stop the Authentication Service.

Starting the Service

To start the Symantec Product Authentication Service on UNIX, move to the `/bin` directory relative to where you installed authentication and run the `vxatd` command as follows:

```
/opt/VRTSat/bin/vxatd
```

Note: The broker should be configured in a specific mode (Root, Root+AB, or AB only) before starting it. Otherwise the broker will not come up.

Stopping the Service

To stop the Symantec Product Authentication Service on UNIX, issue a `kill` command on the process id of the `vxatd` service (for example, kill 203).

Installing Client Only

In many cases, you will install the Authentication Client the same time you install the Root and/or the Authentication Broker. The present section tells how to install the Client separately.

Windows Installation of Client Only

On a Windows platform, you can install the Client either interactively by using the Windows `VxSSVRTSatSetup.exe` (InstallShield) or in silent mode.

Wizard Install of Authentication Client

Occasionally, you may want to install the Authentication Client separately on a machine.

To install on a Windows platform using a traditional wizard

1. Log on as administrator on the machine where you want to install the Client.
2. Confirm that the machine uses the NTFS file system. FAT does not provide any file system security and hence compromises the security of Symantec Product Authentication Service.
3. Run the `VxSSVRTSatSetup.exe` from the CD.
4. When the opening InstallShield wizard screen is displayed, click **Next**.
5. When the Setup Type screen is displayed, select **Typical** to install only the client side, and click **Next**.
6. When the Summary screen is displayed, click **Next**.
7. After the files are copied, the InstallShield Wizard Complete screen is displayed.
8. Click **Finish**.

Silent Install of Authentication Client

On Windows, you can install the Authentication Client silently either by using the `VxSSVRTSatSetup.exe` or by using the MSI.

Performing Silent Installation with VxSSVRTSatSetup.exe:

Silent installation using `VxSSVRTSatSetup.exe` requires a one time manual installation step. Thereafter, multiple silent installations are possible.

Install once by running the installer with the "/r" option:

```
VRTSatSetup.exe /r /f1"c:\at.rsp"
```

This command launches the GUI and walks you through a set of dialogs. After you respond to the dialogs, the installer stores that information in a response file that can be used to install silently any number of times using the following command:

```
VxSSVRTSatSetup.exe /s /f1"c:\at.rsp"
```

Performing Silent Installation with the MSI

The following commands assume you have the MSI file ("`VERITAS Authentication Services.msi`") in your current directory.

- Installing client-only to default location

  ```
  msiexec /qn /i "VERITAS Authentication Service.msi"
  ```

- Installing client-only to custom location

  ```
  msiexec /qn /i "VERITAS Authentication Service.msi"
  INSTALLDIR=d:\the\customdir
  ```

UNIX Installation of Client Only

Occasionally, you may want to install the Authentication Client separately on a machine.

Interactive Installation of Client Only on UNIX

You can install interactively on a UNIX platform, using the same instructions for all varieties of UNIX supported by Symantec Product Authentication Service. If you prefer to use the OS tools specific to your platform, see “Installing Authentication with UNIX OS Tools” on page 85.

To install the client on a UNIX platform

1 Log on as root on the host.

Note: An OS limitation in Tru64 prevents the installation process from detecting any previous version of Symantec Product Authentication Service already installed on a given host. Manually remove previous versions before attempting to install the latest version.

---

2 Make sure that no clients are running (Console, etc.).

3 Move to the directory on the CD that holds the `installics` program, and run `installics`.

4 Select **(I) Install a Product**.

5 Select **Symantec Product Authentication Service**.

6 Answer the prompts.

7 (SUN and HP-UX Only): When asked **Do you Want to Install the Authentication Broker Server [y, n, q]**, select **n** to install client only. (Select **q** if you want to quit installation.)

Note: Do not be concerned if you see a message saying `Cannot Copy`. It is a benign message and will have no effect on your installation.

Silent Installation of Client Only on UNIX

A response file is generated with every interactive install through the `installics` program. The full path name of the generated response file will be printed on the screen at the end of the install. It looks something like this:

```
/opt/VRTS/install/logs/installics207163245.response
```

Later this file can be used to silent install with the following command:

```
installics -responsefile <response file>
```

For more information on installing through `installics`, see the *ICS Installation Guide*.

Changing Passwords After Installation

Consumers who directly consume native packages of Symantec Product Authentication Service 4.3 should change the default broker admin passwords upon installation.

Changing the Authentication Broker Default Admin Password

These instructions assume that Symantec Product Authentication Service is installed into $INSTALLDIR.

To change the authentication broker default admin password

1 Obtain the Authentication Broker domain name:

```
$INSTALLDIR/bin/vssat listpd --pdrtype ab | grep "Domain Name" |
awk '{print $3}'
```

2 Change the Authentication Broker admin password:

```
$INSTALLDIR/bin/vssat resetpasswd --pdrtype ab --domain
<domainname> --prplname admin --newpasswd <new admin password> -
-repeatednewpasswd <new admin password>
```

- *<domain name>* is the Authentication Broker domain name obtained from Step 1.
- *<new admin password>* is the new admin password.

Changing the Root Broker Default Admin Password

These instructions assume that Symantec Product Authentication Service is installed into $INSTALLDIR.

To change the Root Broker default admin password

1. Obtain the Root Broker domain name:

   ```
   $INSTALLDIR/bin/vssat listpd --pdrtype root | grep "Domain Name"
   | awk '{print $3}'
   ```

2. Change the Root Broker admin password:

   ```
   $INSTALLDIR/bin/vssat resetpasswd --pdrtype root --domain
   <domain name> --prplname admin --newpasswd <new admin password>
   --repeatednewpasswd <new admin password>
   ```

   - *<domain name>* is the Root Broker domain name obtained from Step 1.
   - *<new admin password>* is the new admin password.

Optional Authentication Client Configurations

Optionally, the administrator can configure the Authentication Client by specifying outbound port ranges or by specifying the interface to which the library should be bound.

Specifying Outbound Port Ranges for Authentication Client

The Authentication Client supports port ranges for outbound ports. The port ranges can be specified in the registry on Windows and in `/etc/vx/vss/VRTSat.conf` on UNIX.

Specifying Outbound Port Range for Windows

On Windows, `HKEY_LOCAL_MACHINE\Software\VERITAS\Security\Authentication\Client` can have two keys - PortRangeMin and PortRangeMax.

- PortRangeMin specifies the starting port number.
- If PortRangeMax is not specified, PortRangeMax is defaulted to PortRangeMin + 1000.

Specifying Outbound Port Range for UNIX

On UNIX, the section is `Security\Authentication\Client`. The key name and semantics are identical to those in Windows.

Specifying an Interface for Authentication Client

On machines which have multiple interfaces, the VRTSat client library can be configured to bind to a specific interface. This interface can be specified in the following registry location:

Specifying a Client Interface for Windows

On Windows, use the following setting to specify a client interface:

HKEY_LOCAL_MACHINE\Software\VERITAS\Security\Authentication\Client,
UseInterface = "IP Address"

Specifying a Client Interface for UNIX

On UNIX, use the following setting to specify a client interface:

In the /etc/vx/vss/VRTSat.conf file,
in Security\Authentication\Client section,
UseInterface = "IP address"

Here IP address is the interface address.

Configuring Outside the Install Process on UNIX

You can configure either as part of the installation process or separately.

To configure outside the install process

1. Log on as root on the machine you want to configure.
2. Run `installics` from the CD and select **(C) Configure an Installed Product**.
3. When asked to select a mode, select either Root Broker, Authentication Broker Only, or Authentication + Root Broker. (If you had selected to install client only, you would not receive this prompt.)
4. See installation "UNIX Installation of Root or Root + AB" or "UNIX Installation of Authentication Broker" for detailed instructions.

Upgrading from Client-Only to Client Plus Server

If the Authentication Client is already installed, and if running Setup again does not cause you to be prompted for an upgrade, use the following workaround:

```
msiexec /qn /i "VERITAS Authentication Service.msi"
ADDLOCAL="Server" BROKERMODE=<r|ab|arb>
```

Note: BROKERMODE is a mandatory parameter for broker installs using MSI.

You can use all server specific properties on this command line. For example, you can add arguments to do the following:

- Specify the Cluster Name
  `CLUSTERNAME=abcd`
- Specify the SCM Start Type
  `SCMSTARTTYPE=auto`
  The other accepted value is manual, which is the default.
- Specify that the Service should be started after configuration
  `STARTSERVICE=YES`
  The other accepted value is manual, which is the default.

Uninstalling Authentication

This section explains how to uninstall on Windows and UNIX platforms.

Windows Uninstallation of Authentication

On a Windows platform, you can uninstall either interactively by using the Windows `VxSSVRTSatSetup.exe` (InstallShield) or in silent mode.

Wizard Uninstall of Authentication

To uninstall on Windows using a traditional wizard

1. Log on as administrator on the machine where you want to uninstall.
2. Use the Add/Remove programs panel from the Control Menu to remove the authentication package.
3. If you want to uninstall Symantec Product Authentication Service as a whole, select **Remove**.

Note: If you want to uninstall separate features rather than Symantec Product Authentication Service as a whole, make sure to read “Dependencies” on page 17 so that you do not attempt to uninstall a feature that is depended upon by others. Then, select **Modify** rather than **Remove**.

If you are a NetBackup client user, see “Cleanup Instructions for NBU Client Users of Symantec Product Authentication Service” on page 41.

Silent Uninstall of Authentication

On Windows, you can uninstall Symantec Product Authentication Service silently either by using the `VxSSVRTSatSetup.exe` or by using the MSI.

Performing Silent Uninstallation with VxSSVRTSatSetup.exe:

Silent uninstallation using `VxSSVRTSatSetup.exe` requires a one time manual uninstallation step. Thereafter, multiple silent uninstallations are possible.

Uninstall once by running the installer with the "/r" option:

```
VxSSVRTSatSetup.exe /r /f1"c:\at.rsp"
```

This command launches the GUI and walks you through a set of dialogs. After you respond to the dialogs, the installer stores that information in a response file that can be used to uninstall silently any number of times with the following command:

```
VxSSVRTSatSetup.exe /s /f1"c:\at.rsp"
```

Performing Silent Uninstallation with the MSI

The following commands assume you have the MSI file ("`VERITAS Authentication Services.msi`") in your current directory.

- Remove the Server from a client-server installation

  ```
  msiexec /qn /x "VERITAS Authentication Service.msi"
  REMOVE="Server"
  ```

- Uninstall Symantec Product Authentication Service completely with the MSI

  ```
  msiexec /qn /x "VERITAS Authentication Service.msi"
  ```

- Uninstall Symantec Product Authentication Service completely without the MSI

  ```
  msiexec /qn /x "{A824C2E4-8D3B-4D7A-8BBF-ACAB75E925CA}"
  ```

If you are a NetBackup client user, see “Cleanup Instructions for NBU Client Users of Symantec Product Authentication Service” on page 41.

UNIX Uninstallation of Authentication

You can uninstall on a UNIX platform, using the same instructions for all varieties of UNIX supported by Symantec Product Authentication Service.

To uninstall authentication on UNIX platforms

1. Make sure you are running as root user on the host.
2. Make sure that no Authentication Clients are running (Administration Console, etc.).

3. Move to the directory on the CD that holds the `installics` process and run `installics`.
4. Select **(U) Uninstall a Product** and answer the prompts as they occur.

Cleanup Instructions for NBU Client Users of Symantec Product Authentication Service

The following cleanup instructions are applicable to all NBU client users. Upon removal of Symantec Product Authentication Service, users will need to:

1. Backup ~/.VRTSat if needed where "~/" is the user's home directory.
2. Remove ~/.VRTSat
   rm -rf ~/.VRTSat

Where to Find Instructions on Running the Console

For instructions on how to run the Administration Console, see “Running the Administration Console”.

Chapter 3

Using Language Packages and Patches

This chapter includes guidelines for installing the Symantec Product Authentication Service Chinese and Japanese language packages and patches. You should read it first before installing the language packages. Use the procedures outlined below in conjunction with any particular instructions given in the product-specific READMEs.

If you have not installed the Symantec Product Authentication Service base package, please do so by reading the documentation on how to install before continuing.

The chapter contains the following major sections:

Purpose of Language Packages and Patches

Symantec Product Authentication Service includes:

- The base program
- Language packages
- Language patches

After you install Symantec Product Authentication Service, you can install a language package to localize Authentication to the selected language.

After you install a language package, you should install the corresponding language patch to solve certain issues that exist in the language package itself.

Install and Uninstall Package and Patch on Windows

Locate the Language Packages and Patches

Language packages for windows are located in the following area:

```
CDROM_DRIVE:\<version>-lang\windows\authentication\pkgs
```

Install Language Package through the GUI

To install the Service language package through the GUI

1. Double click `VERITAS Authentication Service Chinese/Japanese Language pack.msi` to install.
2. Make sure the following fields are correct:
   - User name
   - Organization
   - Install this application for
3. When they are correct. click **Next**.
4. Select **Custom** and click **Next**.
5. Under the "Click on a icon in the list below to change how a feature is installed" field, click **+** to expand the feature lists.
6. From the Server Message Catalog drop-down menu, select **This feature will be installed on a local hard drive**. If you want to change the location of installation, click **Change** then click **Next**. If the location is accurate, click **Next** to continue.

7 If you need to make changes, click **Back** to make an adjustment. If you are ready to install, click **Next**.

8 Click **Finish** to complete the installation.

To install the Client language package through the GUI

1 Double click the `VERITAS Authentication Service Client Chinese/Japanese Language pack.msi`.

2 Make sure the following fields are correct:
- User name
- Organization
- Install this application for

3 When they are correct, click **Next**.

4 Select **Custom** and click **Next**.

5 If you want to change the location of installation, click **Change** then click **Next**. If the location is accurate, click **Next** to continue.

6 If you need to make changes, click **Back** to make an adjustment. If you are ready to install, click **Next**.

7 Click **Finish** to complete the installation.

Install Language Package through the CLI

To install the Service or Client language package through the CLI

There are two methods of installing the language package from the CLI.

- Command line interface install
  From command line: `msiexec /i "<package name>"`
- Silent install
  From command line: `msiexec /qn /i "<package name>"`

Install Patch through the GUI

To install the Service patch through the GUI

1 Double click `VERITAS Authentication Service Chinese/Japanese Language pack.msi`. (The name of the file is the same as for the language package.)

2 Make sure the following fields are correct:
- User name

- Organization
- Install this application for

3 When they are correct, click **Next**.

4 Select **Custom** and click **Next**.

5 Under the "Click on a icon in the list below to change how a feature is installed" field, click **+** to expand the feature lists.

6 From the Server Message Catalog drop-down menu, select **This feature will be installed on a local hard drive**. If you want to change the location of installation, click **Change** then click **Next**. If the location is accurate, click **Next** to continue.

7 If you need to make changes, click **Back** to make an adjustment. If you are ready to install, click **Next**.

8 Click **Finish** to complete the installation.

To install the Client patch through the GUI

1 Double click the `VERITAS Authentication Service Client Chinese/Japanese Language pack.msi` (The name of the file is the same as for the language package.)

2 Make sure the following fields are correct:

- User name
- Organization
- Install this application for

3 When they are correct, click **Next**.

4 Select **Custom** and click **Next**.

5 If you want to change the location of installation, click **Change** then click **Next**. If the location is accurate, click **Next** to continue.

6 If you need to make changes, click **Back** to make an adjustment. If you are ready to install, click **Next**.

7 Click **Finish** to complete the installation.

Install Patch through the CLI

To install the Service or Client patch through the CLI

There are two methods of installing the language patch from the CLI.

- Command line interface install
  From command line: `msiexec /i "<patch name>"`

- Silent install
  From command line: `msiexec /qn /i "<patch name>"`

Uninstall Language Package through the GUI

To uninstall the language package through the GUI

1. Right-click on the language packages which have been installed.
2. Select **uninstall**" from the dialog menu.

Uninstall Language Package through the CLI

To uninstall, you must know what `MSI` package is installed (client or server language package) on the system. MSIs do not show up in the "ADD/REMOVE programs".

To uninstall the language package through the CLI

1. Move to the directory where the proper MSI package is located and enter the following from the command line:

   ```
   C:\msiexec /x "<package name>"
   ```

2. OR uninstall silently by entering the following from commandline:

   ```
   C:\msiexec /qn /x "<package name>"
   ```

Locate Language Packages on UNIX

For UNIX we use the following directory layout.

```
CD\<language_code>\<platform or "doc">\<product>\pkgs
```

Where <language_code> can equal

- ja
- zh

where *<platform>* can equal

- aix: for both AIX4.3 and 5.x)
- hpux: for HP 11.00, HP 11i, and HP 11.23)
- linux: for Linux x86 and Linux ia64 variants)
- tru64: for OSF1/Tru64 5.x)
- sun: for Solaris 7, 8, 9, 10)

Where *<product>* can equal

- authentication

- authorization
- private_branch_exchange
- service_management_framework

Therefore, the final directory structure for Symantec Product Authentication Service would be something like:

```
<CD_MOUNT>\ja\sun\authentication\pkgs
```

Install and Uninstall Package and Patch on Solaris

Install Language Package on Solaris

To install the language package on Solaris

1. See "Locate Language Packages on UNIX" on page 47.
2. Run the `install_lp` script by typing:

   ```
   ./install_lp
   ```

3. When you are asked which language you want to install, select a language.
4. Enter the name of the system you want to install onto.
   The installer script will first verify which packages were installed -- Authentication, Authorization, or both. Then it will install the appropriate language package or packages onto the systems automatically.
5. Press **Enter** to exit.

Install Patch on Solaris

To install the patch on Solaris

1. See "Locate Language Packages on UNIX" on page 47.
2. Run the `installvp` script by typing:

   ```
   ./installvp
   ```

3. When you are asked which language you want to install, select a language.
4. Enter the name of the system you want to install onto.
   The installer script will first verify which packages were installed -- Authentication, Authorization, or both. Then it will install the appropriate language package or packages onto the systems automatically.
5. Press **Enter** to exit.

Configure PATH

On Solaris, you will need to add `PATH` into your startup profile. Be sure to use the `FULL PATH` name.

Uninstall Language Package on Solaris

To uninstall the language package on Solaris, type the following command:

```
pkgrm VRTSatZH or VRTSatJA
```

Uninstall Patch on Solaris

To uninstall the language patch on Solaris, type the following command:

```
patchrm <patch name>
```

Install and Uninstall Package and Patch on AIX

Install Language Package on AIX

To install the language package on AIX

1. See "Locate Language Packages on UNIX" on page 47.
2. Run the `install_lp` installation script by typing:
   ```
   ./install_lp
   ```
3. When you are asked which language you want to install, select the language.
4. Enter the name of the system you want to install onto.
   The installer script will first verify which packages were installed -- Authentication, Authorization, or both. Then it will install the appropriate language package or packages onto the systems automatically.
5. Press **Enter** to exit.

Install Patch on AIX

To install the language patch on AIX

1. See "Locate Language Packages on UNIX" on page 47.
2. Run the `installvp` script by typing:
   ```
   ./installvp
   ```
3. When you are asked which language you want to install, select a language.
4. Enter the name of the system you want to install onto.

The installer script will first verify which packages were installed -- Authentication, Authorization, or both. Then it will install the appropriate language package or packages onto the systems automatically.

5 Press **Enter** to exit.

Configure PATH

On AIX platforms, you will need to add `PATH` into your startup profile. Be sure to use the `FULL PATH` name.

Uninstall Package on AIX

- To uninstall the language package on AIX, do one of the following at the command prompt:

```
installp -u VRTSatJA
installp -u VRTSatZH
```

Uninstall Patch on AIX

We only allow patch removal on Solaris, not on other UNIX platforms.

Install and Uninstall Package and Patch on HP

Install Language Package on HP

To install the language package on HP

1 See “Locate Language Packages on UNIX” on page 47.

2 Run the `install_lp` installation script by typing:

```
./install_lp
```

3 When you are asked which language you want to install, select the language.

4 Enter the name of the system you want to install onto.
The installer script will first verify which packages were installed -- Authentication, Authorization, or both. Then it will install the appropriate language package or packages onto the systems automatically.

5 Press **Enter** to exit.

Install Patch on HP

To install the language patch on HP

1. See “Locate Language Packages on UNIX” on page 47.
2. Run the `install_lp` installation script by typing:
   ```
   ./install_lp
   ```
3. When you are asked which language you want to install, select the language.
4. Enter the name of the system you want to install onto.
   The installer script will first verify which packages were installed -- Authentication, Authorization, or both. Then it will install the appropriate language package or packages onto the systems automatically.
5. Press **Enter** to exit.

Configure PATH

On HP platforms, you will need to add `PATH` into your startup profile. Be sure to use `FULL PATH` name.

Uninstall Language Package on HP

To uninstall the language package on HP

1. Type the following command:
   ```
   swremove VRTSatZH or VRTSatJA
   ```
2. Or use the `swremove` CLI.

Uninstall Patch on HP

We only allow patch removal on Solaris, not on other UNIX platforms.

Chapter 4

High Availability Installation

Server clusters provide high availability of applications and data to users. In a server cluster, two or more servers (called *nodes*) are linked in a network, and run cluster software that allows each node access to the shared bus to which any number of disks can connect. If a node becomes unavailable, cluster resources migrate to an available node (this is called *failover*). The disks on the shared bus and the virtual server are kept available. During failover, users experience only a short interruption in service.

Symantec Product Authentication Service runs in the following clustering environments:

Table 4-1

Cluster Platform	OS Platform(s)
VCS 2.0	Windows 2000, Linux AS2.1
VCS 3.5	HPUX 11.0, AIX 5.1, Linux AS 2.1, Solaris 7
VCS 4.0	Solaris 7
VCS 4.1	Windows (2000, 2003 and XP), Solaris (7, 8, 9, 10), HP (11.0, 11.11, 11.23), AIX (5.1, 5.2)
HP Service Guard A.04.00	HP (11.11, 11.23)
MSCS 5.0	Windows 2000
SunCluster 3.1	Solaris 7, 8, 9, 10
TruCluster 5.1	Tru64 5.1

This chapter explains how to install and configure Symantec Product Authentication Service for high availability.

Cluster Capabilities of Symantec Product Authentication Service

Two essential features of high availability software are that it be failover capable and provide persistent data.

Failover Capability

To provide failover capability, Symantec Product Authentication Service adheres to the following best practices:

- Use of start/stop procedures/scripts where applicable
- Hostname Usage
  Authentication allows configuration of a cluster name tag. This is used for domain name uniqueness in the private domain database.
- Connectivity
  Authentication and Authorization allow configuration of a virtual IP address. Services listen on all interfaces to service requests (originating locally or remotely) to the local host or the virtual IP.

Data Persistence

To make persistent data available, Symantec Product Authentication Service follows these practices:

- The Authentication private domain database can be split into 2 parts. The local PDR can be configured to be on a local file system.
- Credential and key stores can be configured on a shared disk.

Note: See the Symantec Product Authorization Service *Installation Guide* for information on the data persistence practices followed regarding Authorization.

Special System Requirements for Clustered Environments

For installing Symantec Product Authentication Service in cluster mode, you should install in custom mode and choose a pathname with no spaces. For example, `c:\program_files\Veritas\Security\Authention`. This is because there is an issue in Symantec Cluster Server where some of the Symantec Cluster Server commands do not work when there is a space in the complete

path. This problem will cause the clustering configuration of Symantec Product Authentication Service to fail. For example in the path `c:\program files`, the space between the "program" and "files" will cause an issue.

If you have already installed Symantec Authentication Service in a path that has spaces, you must uninstall then reinstall in the custom path.

Configuration Recommendations

Note: We recommend that you allocate separate resources (shared disk, IP, network name) for Symantec Product Authentication Service. Doing so will ensure that the failure of any resource will affect only Symantec Product Authentication Service.

You can configure in any of the three following modes:

- Root Only
- Root+AB
- AB Only

Whichever mode you choose, you should install in the same mode on all nodes in the cluster.

Regardless of the platform, Root Brokers, when configured as Root Only brokers, do not need to be run on a Cluster. This is because they are very rarely used -- only during Authentication Broker Only setups.

Groups and Dependencies

Note: For Pre 4.1 Symantec Cluster Server clusters, MSCS clusters, Sun cluster, or TruCluster, the Authentication and Authorization services must reside on the same node in the cluster.

See the Symantec Product Authorization Service *Installation Guide* for information on establishing groups and dependencies if you will be using the Authorization.

Symantec Product Authentication Service with Microsoft Cluster Server

Below are the instructions for installing and configuring Symantec Product Authentication Service with Microsoft Cluster Server. For important platform-independent information, see "Configuration Recommendations."

Installing and Configuring Authentication for MSCS

Note: The cluster configuration for Symantec Product Authentication Service and for Symantec Product Authorization Service should be run only on one node in a cluster. After that, installation on all other nodes proceeds the same as non-cluster installation.
See the Symantec Product Authorization Service *Installation Guide* for further information.

To perform the setup

1. Install the Authentication Service. Doing so configures the Authentication Service for a cluster environment by asking the cluster name and setting it in the profile.

Note: Make sure that a Broker resides on each node of the cluster.

---

   a. When installing choose the clustering option.

   b. Enter the cluster name during the installation.

2. Go to the node that has the shared drive accessible, and run the following:
   `VxATclconf.bat <installdir> <shared_drive_letter>`
   For example:
   ```
   VxATclconf.bat "C:\Program
   Files\VERITAS\Security\Authentication" S
   ```
   This command needs to be run only once. On nodes that do not have access to the shared drive, it fails gracefully, asking the user to run the script on the node that has access to it.

3. If the machine is configured for Authentication Broker Only, request the certificate and set it up, as follows.
   `vxatd -d -a -o -n <prplName> -p <password> -x vx -y <domain_name> -q <broker_host_ip> -z <brokerport>`

4. Make the Authentication Service a cluster service.

a Identify a Cluster Group into which the service can to be added. This generic service type resource has dependencies on the Cluster's shared disk, on IP address, and on the Cluster's network named resource. Therefore, the group that you select must have these two resources.

b If there is not already such a group, create one. We recommend naming it **vxss_service.** It must have the required resources: Shared disk/ mountpoint, IP address, and Network Name. (If you want details on how to create a group, see "Creating a New Group" on page 58.)

c If there is already a group with these resources, highlight it and configure the broker as a Generic Service resource in that group. (If you want details on how to create a resource, see "Creating a New Resource in a Selected Group" on page 60.)

- Complete the New Resource dialog by entering a name and a description. The resource type is **Generic Service**. For Group, select a group that has the Network Name resource, and IP resource.
- Complete the Possible Owners dialog by selecting the cluster nodes on which the resource can be brought online. For details on owners refer to Microsoft Cluster Server reference manual.
- Complete the Dependencies dialog. The dependencies, which must be brought online by the Cluster service first, are the Shared Disk and the Network Name resources. The Network Name resource depends on the IP resource. Therefore, the Authentication Service has indirect dependence on IP resource.
- Complete the Generic Service Parameters dialog. The service name is 'VRTSat', which is the name displayed on the top (uneditable) line of the Properties tab in the "Services" window if you do the following and highlight the service whose name you want to see:
  Control Panel > Administrative Tools > Services
- Complete the Registry Replication dialog by adding the registry key that should be replicated to all nodes:
  SOFTWARE\VERITAS\Security\Authentication\Credential Manager\Profiles\SYSTEM
  When the resource has been successfully added to the Group, the following message will be displayed:
  `Cluster resource 'VRTSat' created successfully.`

5 Bring the group with the Authentication Service online.

MSCS Procedures for Creating Groups and Resources

Below is a description of the procedures for creating new groups and new resources in a Microsoft Cluster Server environment.

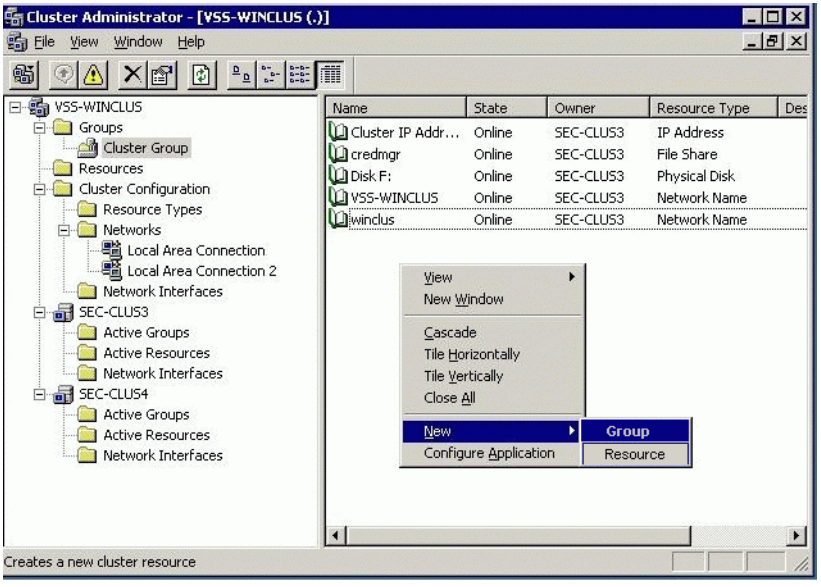
Creating a New Group

This procedure shows the menu choices and wizard screens you will use for creating a new group.

To create a new group

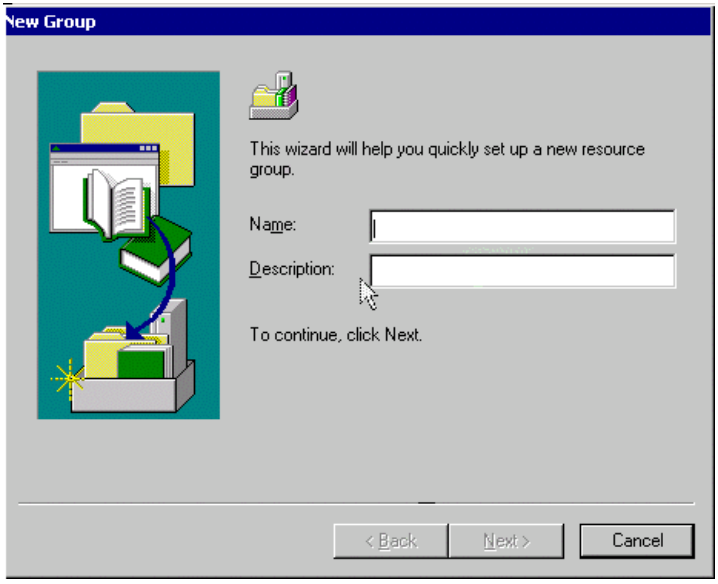
1 Right click on the right hand panel, and choose **New Resource**, as shown below:

Figure 4-1 Menu with New Group Option



2 The New Group dialog will be displayed:

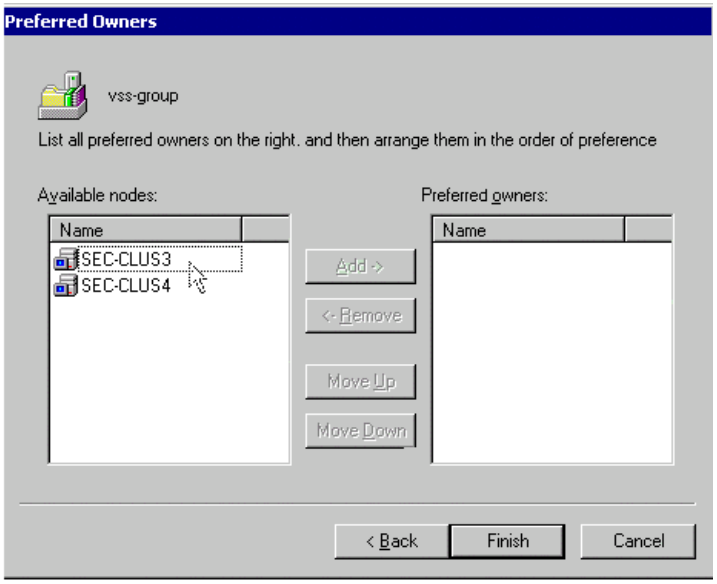
Figure 4-2 New Group Dialog



We recommend naming the group **`vxss_service`**.

3 Click **Next** to bring up the Preferred Owners dialog:

Figure 4-3 Preferred Owners Dialog



Move entries from the Available nodes list to the Preferred owners list, and use the **Move Up** or **Move Down** buttons to arrange the owners in order of preference.

4 Click **Finish** to complete the wizard.

Now that the group exists, you can add resources to it.

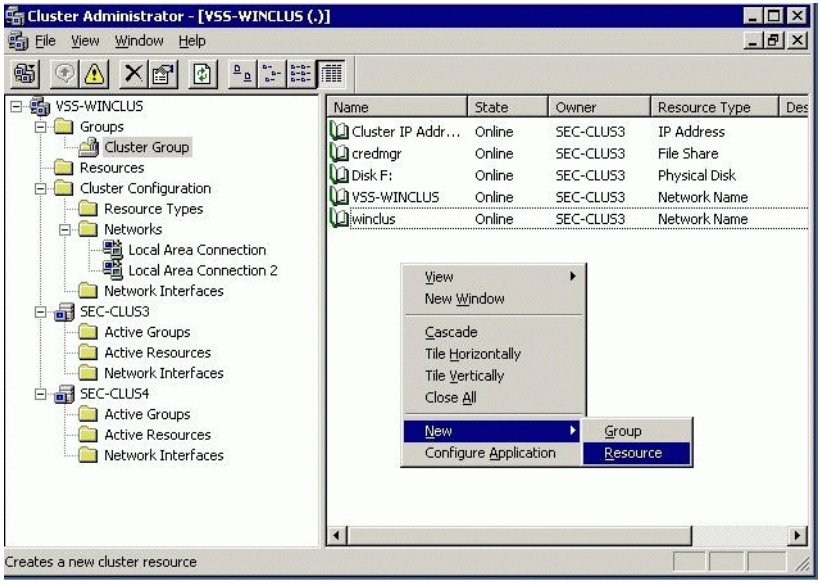
Creating a New Resource in a Selected Group

This procedure shows the menu choices and wizard screens you will use for creating a new resource.

To create a new resource in the selected group

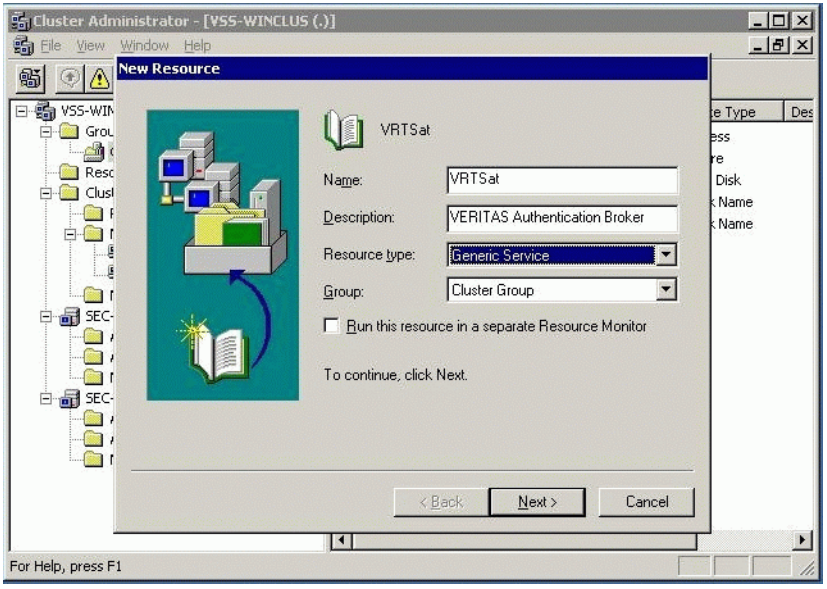
1 Right click on the right hand panel, and choose **New Resource** option, as shown below:

Figure 4-4 Menu with New Resource Option



The New Resource dialog will be displayed:

Figure 4-5 New Resource Dialog

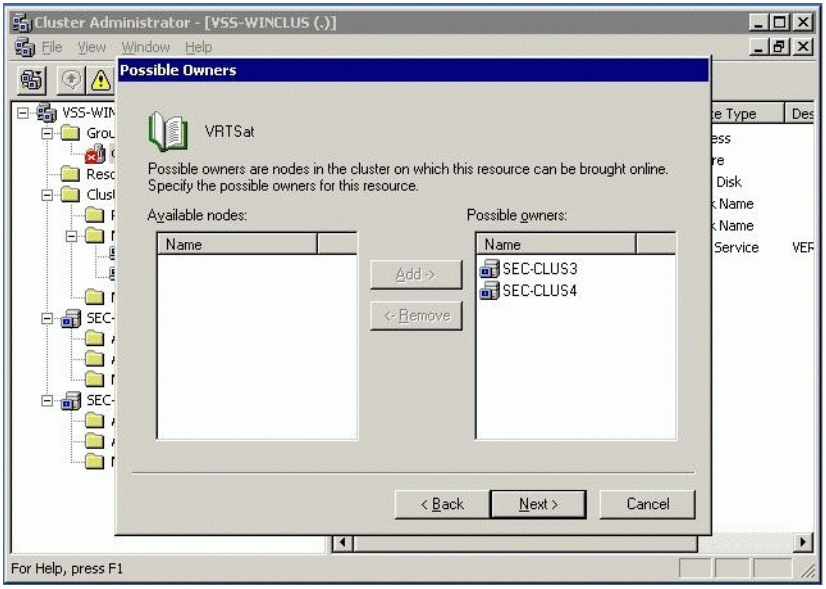


2 Complete the New Resource dialog:

- Enter a name and a description.
- For Resource type select **Generic Service**.
- For Group, select a group that has the Network Name resource, and IP resource.

3 Click **Next** to bring up the Possible Owners dialog:

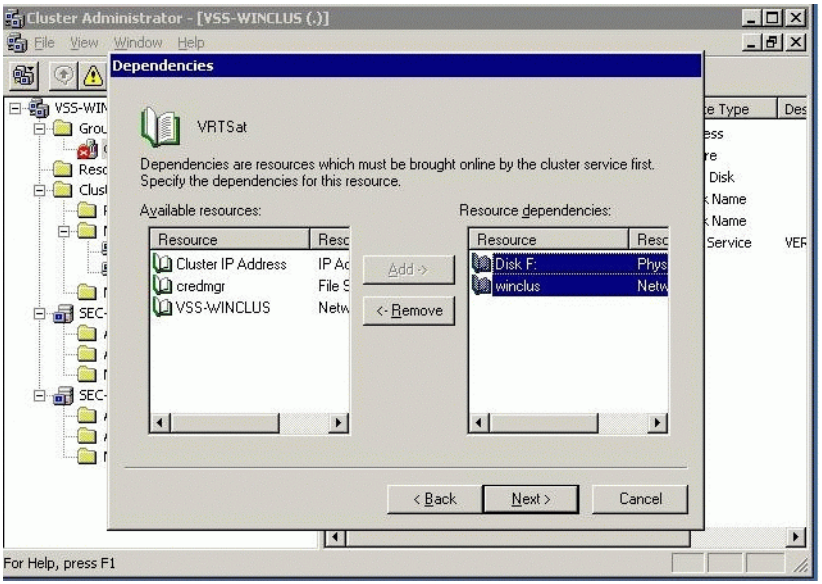
Figure 4-6 Possible Owners Dialog



Select the possible owners of this service type resource -- that is, the cluster nodes on which this resource can be brought online. For details on owners refer to Microsoft Cluster Server reference manual.

4 Click **Next** to bring up the Dependencies dialog:

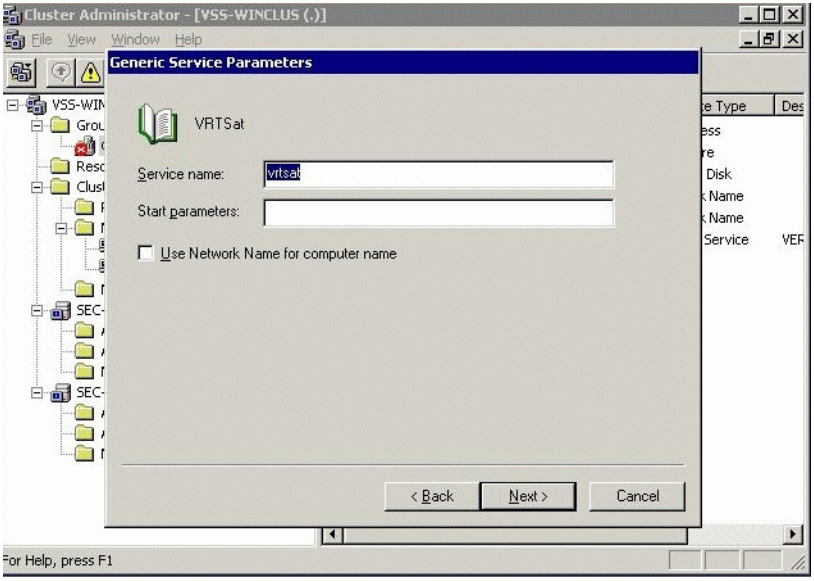
Figure 4-7 Dependencies Dialog



Dependencies are those resources which must be brought online by the Cluster service first, before the resource you are adding can function.

5 Click **Next** to bring up the Generic Service Parameters dialog:

Figure 4-8 Generic Service Parameters Dialog

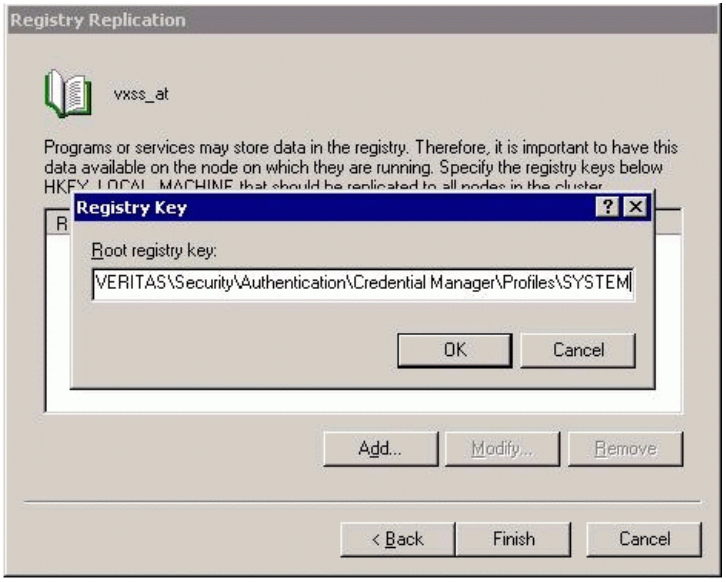


In this panel, enter the service name. The service name is the name displayed on the top (uneditable) line of the Properties tab in the "Services" window, if you do the following and highlight the service whose name you want to see:

Control Panel > Administrative Tools > Services

6 Click **Next** to bring up the Registry Replication dialog. Click **Add** to add the registry key that should be replicated to all nodes.

Figure 4-9 Registry Replication Dialog



7 Click **Finish**. When the resource has been successfully added to the Group, the following message will be displayed:

```
Cluster resource 'ResourceName' created successfully.
```

Symantec Product Authentication Service with Symantec Cluster Server for Windows

This section offers instructions for installing and configuring Symantec Product Authentication Service with Symantec Cluster Server for Windows (previously called VCS). For important platform-independent information, see "Configuration Recommendations".

What Domain Name to Use

For Symantec Cluster Server 3.5, ClusterName is configured at the installation time. For Symantec Cluster Server 4.0, both ClusterName and ClusterPDR are configured at the installation time.

Different versions of Symantec Cluster Server handle domain names differently:

- For Symantec Cluster Server 3.5, use `root@ClusterName`, `broker@ClusterName`, etc.

- For Symantec Cluster Server 4.0, use `root@FQHN`, `broker@FQHN` and `SomeClusterPDRDomain@ClusterName`

Installing and Configuring Authentication

1. Install Symantec Cluster Server according to the instructions in the Symantec Cluster Server manual.

Note: The present release of Symantec Cluster Server does not allow the use of white space in path names.

Note: The diskgroups where Symantec Product Authentication Service and Symantec Product Authorization Service reside must be of type "clustered". Otherwise, Symantec Cluster Server will not see them, and hence failover/ failback will not take place.

---

2. Select a node which has access to the shared drive.
   The node on which you start installing Symantec Product Authentication Service must have access to the shared drive. Otherwise, when you run the Perl script later, you will receive "drive not found" errors.
3. Install the Authentication component:
   a. Select **Service is Clustered**.
   b. Type the cluster name, which is case sensitive. The cluster name must match exactly what was configured during Symantec Cluster Server install. Failure to match exactly will result in an erroneous install.
4. Update system and cluster configuration parameters in the text file `VxATclinput.txt`, which is shipped in the `<InstallDir>/bin` directory.

Note: Parameters such as cluster name, host names, etc., must match exactly what was configured during Symantec Cluster Server install. Failure to match case sensitivity will result in an erroneous install.

Specify the cluster input parameters in this file. This config file is a "tag=value" format. Change the value part to suit the system, but do not change the tag names. Edit the following tag values:

- BeginIPSection
  Address=<the virtual IP address goes here>
- NetMask=<netmask for this interface>
  Device=<the network interface device. e.g. hme0>

- BeginNICSection
  Device=<same device as in the BeginIPSection above>
- BeginMountSection
  BlockDevice=<block device for the mount point. If VxVM is used, it would be something like /dev/vx/dsk/somedg/somevol>
  FSType=<file system type. If VxFS is configured it will be vxfs>
- BeginDiskGroupSection
  DiskGroup=<the disk group name. only applicable if VxVM is used>
- BeginVolumeSection
  Volume=<volume name. only applicable if VxVM is used>
- BeginGENSection
  SystemList=<space separated list of cluster nodes>
- ClusterName=<name of the cluster>

5 Run the perl script `VxATclconf.pl` for configuration: <InstallDir>/bin/VxATclconf.pl. Usage is as follows:

  #perl <InstallDir>/bin/VxATclconf.pl [options]

  Where options are -

  - -Mi: for interactive mode
  - -Mn: for non-interactive mode. Input is read from the file VxATclinput.txt present in the same directory.
  - -F: <file> specify alternative location/name for the cluster input file.
  - -help: displays help

6 Be sure to install Authentication bits/binaries on other node(s) of the cluster as well. Install it in the same location on all nodes in the cluster.

7 Start the Authentication Service from the command line if cluster configuration is successful.

Note: Choose **Yes** when prompted **Y / N** on a cluster install. This is paramount.

---

8 Since the Authentication Service is set to manual by default, it must be started on all nodes.

9 Bring Authentication online.

Note: If you plan to install Symantec Product Authorization Service, make sure that the shared drive is still available to the node on which you intend to install it. Make sure that Authentication is running on the node on which you intend to install Authorization.

Symantec Product Authentication Service on Symantec Cluster Server and xpg4 Platforms

1 Install Symantec Cluster Server according to the instructions in the Symantec Cluster Server manual.

Note: The present release of Symantec Cluster Server does not allow the use of white space in path names.

Note: The diskgroups where Symantec Product Authentication Service and Symantec Product Authorization Service reside must be of type "clustered". Otherwise, Symantec Cluster Server will not see them, and hence failover/ failback will not take place.

---

2 Select a node which has access to the shared drive.
The node on which you start installing Symantec Product Authentication Service must have access to the shared drive. Otherwise, when you run the Perl script later, you will receive "drive not found" errors.

3 Install the Authentication component. If you are using installvss or the ICS installer to install, you will be prompted for the cluster configuration. You can either choose to do it now or do it manually later.

- If you choose 'yes' for cluster configuration now, you will need to follow the prompts and enter information like cluster name, IP, shared disk.
- To configure manually, run `vrtsat_clconf.pl` from the primary cluster node. (See Steps 4 and following.)

4 (Manual configuration) Update system and cluster configuration parameters in the text file `VxATclinput.txt`, which is shipped in the `<InstallDir>/bin` directory.

Note: Parameters such as cluster name, host names, etc., must match exactly what was configured during Symantec Cluster Server install. Failure to match case sensitivity will result in an erroneous install.

Specify the cluster input parameters in this file. This config file is a "tag=value" format. Change the value part to suit the system, but do not change the tag names. Edit the following tag values:

- BeginIPSection
  Address=<the virtual IP address goes here>
- NetMask=<netmask for this interface>

Device=<the network interface device. e.g. hme0>

- BeginNICSection
  Device=<same device as in the BeginIPSection above>
- BeginMountSection
  BlockDevice=<block device for the mount point. If VxVM is used, it would be something like /dev/vx/dsk/somedg/somevol>
  FSType=<file system type. If VxFS is configured it will be vxfs>
- BeginDiskGroupSection
  DiskGroup=<the disk group name. only applicable if VxVM is used>
- BeginVolumeSection
  Volume=<volume name. only applicable if VxVM is used>
- BeginGENSection
  SystemList=<space separated list of cluster nodes>
- ClusterName=<name of the cluster>

5 (Manual configuration) After you have updated the config file, run the perl script `VxATclconf.pl` from the primary cluster node. Usage is as follows:

#perl <InstallDir>/bin/VxATclconf.pl [options]

Where options are -

- -Mi: for interactive mode
- -Mn: for non-interactive mode. Input is read from the file VxATclinput.txt present in the same directory.
- -F: <file> specify alternative location/name for the cluster input file.
- -help: displays help

6 (Manual configuration) Start the Authentication Service from the command line if cluster configuration is successful.

7 (Manual configuration) Bring Authentication online.

Note: If you plan to install Symantec Product Authorization Service, make sure that the shared drive is still available to the node on which you intend to install it. Make sure that Authentication is running on the node on which you intend to install Authorization.

Symantec Product Authentication Service on SunCluster

You can configure Symantec Product Authentication Service as failover dataservices on SunCluster.

Before You Begin

At least one Sun Cluster global device should be registered, to hold shared data between nodes. It can be Symantec Volume Manager diskgroup, or any other device that can be failed over from one node of the cluster to the other. On failover, this device would be switched to other nodes of the cluster. Therefore, it is important that this device is not be used by services other than those which should failover if Symantec Product Authentication Service does. (Since Symantec Product Authentication Service and Symantec Product Authorization Service failover simultaneously, Authentication and Authorization resources can use the same global device group.)

Configuring Authentication Service

You can configure Symantec Product Authentication Service for SunCluster either by using the `scvxat` script or by using the UNIX method described in Chapters 2 and 3.

Configuration with the scvxat Script

Note: Symantec Security Packages packages must be installed on each node of the cluster.

SunCluster configuration of Symantec Product Authentication Service is done in three steps.

To configure

1. Prepare the nodes of the cluster.
2. Configure the service.
3. Create the SunCluster resources.

The configuration script, `scvxat`, residing in `/opt/VRTSat/bin` is used in each of these steps.

Step 1: Preparing the Cluster Nodes

To enable creation of a SUNW.HAStoragePlus resource, all nodes of the cluster must have appropriate mount point entries in their `/etc/vfstab` file. You can create the entry manually, or you can use `scvxat` with the `-pernode` option on each of the nodes of the cluster.

In the `-pernode` form, `scvxat` requires two inputs. They are:

- The device to be mounted as the shared storage
- The block device which corresponds to the device mounted as shared storage

It is assumed that a ufs file system already exists on the shared storage.

For example, assuming, you are using a Symantec Volume Manager volume `at_vol` in a diskgroup `shared_dg` as the shared storage, the following command should be used:

```
# scvxat -pernode /dev/vx/dsk/shared_dg/at_vol /dev/vx/rdsk/shared_dg/
at_vol
```

All that `scvxat` does in the `-pernode` mode is create the following entry in the `/etc/vfstab` file:

```
/dev/vx/dsk/shared_dg/at_vol /dev/vx/rdsk/shared_dg/at_vol /var/
VRTSat57 ufs 2 no -
```

If these do not match your settings, you will need to change the contents of this file. For instance, if the file system in use is not ufs, you'll need to change the corresponding entry.

Step 2: Configuring the Service

The second step is to configure the service.

Note: While creating resources, `scvxat` moves service configuration files and the generated key material to the shared storage. Therefore, it is essential that the service be configured *before* it is made highly available.

Configuring the service involves setting the cluster name and generating the key material. By default, Symantec Product Authentication Service uses the fully qualified host name in the private domain name. Since we do not want to tie a clustered service to a specific host, we instruct the service to use the clustername instead. This should be done before key generation.

Setting the Cluster Name

You can set the cluster name using `scvxat` with the `-setclustername` option. For example: If your cluster name is `surya`, you can register it using:

```
# scvxat -setclustername surya
```

The broker domains would now be `root@surya` and `broker@surya`, instead of `root@FQHN`.

Generating the Keys

Keys can be generated invoking `vxatd` with the `-o` option. Refer to the `Administrators Guide` for details.

The following command line generates keys for the broker in Root+AB mode:

```
# vxatd -o -a -r
```

Step 3: Creating SunCluster Resources

The final step of configuration is to create the resources.

Note: This step be must be performed on any one node of the cluster. (The node where the global device is currently online, should be preferred.)

This step can be done by executing `scvxat` with the `-create` option. In this form, `scvxat` requires two inputs. They are:

- The logical hostname
- The name of the global device hosting the shared storage

For example, if logical hostname associated with your cluster is `surya` and the name of global device is `shared_dg`, the following command needs to be invoked.

```
scvxat -create surya shared_dg
```

The command creates a resource group named `vxss_resource` containing the required Authentication resources and brings it online. You can query the status of the resource group, either from the SunPlex Manager GUI or from the command line by using the following command:

```
scstat -g | grep "vxss_resources"
```

Configuring Without Using the Script

You can install and configure the Symantec Product Authentication Service without manually invoking the cluster configuration scripts. In this case, the process takes you through a series of questions and invokes the command lines behind the screens.

To install and configure without invoking the script

1. Install the Authentication component. (See “Basic Installation Instructions”.)
2. Choose the server installation and configuration options.
3. Choose the cluster configuration option. You will see the following message:

```
You can choose to prepare this system as a cluster node.
Alternatively, if all other nodes are prepared, you can
choose to create resources on this node.
    1) Prepare this cluster node.
    2) Prepare this cluster node & create resources.
What do you want to do? [1-2,q]
```

4 Choose 1 to perform the steps described in section "Step 1: Preparing the Cluster Nodes", and choose 2 if you have prepared all other nodes of the cluster, and are ready to creates resources using this node.

5 Answer platform specific cluster configuration queries. You will be asked for:

- The device to be mounted as the shared storage
- The block device which corresponds to the device mounted as shared storage. It is assumed that a ufs file system already exists on the shared storage.

At the completion of this process, the Authentication Service will start.

6 Verify that the Authentication Service started by using the following command:

```
scstat -g | grep "vxss_resources"
```

STATE should be ONLINE.

Cleaning AT Resources if Retrying Configuration

In case of any failure, you should clean resources before retrying configuration. To remove the resources created by `scvxat`, use the command with the `-clean` option.

For example, the following command cleans the SunCluster resources created as a part of configuring Authentication.

```
scvxat -clean
```

Note: For instructions on configuring Authorization, see the Symantec Product Authorization Service *Installation Guide*.

Symantec Product Authentication Service on TruCluster

You can configure Symantec Product Authentication Service as failover dataservices on TruCluster.

Overview

On TruCluster, Symantec Product Authentication Service is configured as single-instance application resources. That is, they run on only one cluster member at a time. If the cluster member where the services are installed fails, the Cluster Application Availability (CAA) subsystem can fail the application over to another running member. Thus, configuring Symantec Product Authentication Service for TruCluster involves two steps:

- Creating these application resource profiles and
- Registering them with the CAA subsystem

Note: The TruCluster Cluster File System (CFS) supports a single cluster-wide namespace and uniform coherent access to all file systems in a cluster. Therefore, unlike Symantec Cluster Server and SunCluster configuration of Authentication, a separate shared-storage configuration is not required for Tru64.

Configuring Symantec Product Authentication Service

You can configure Symantec Product Authentication Service for TruCluster either by using the `tcvxat` script or by using the UNIX method described in Chapter 2.

Configuration with the tcvxat Script

You can configure by using `tcvxat`, which resides in `/opt/VRTSat/bin`. TruCluster configuration is essentially a matter of creating and registering the application resource profile with the CAA subsystem. However, since the Symantec Product Authentication Service might require some configuration before it is brought up, the service configuration step needs to precede the resource profile creation.

Step 1: Configuring the Authentication Service

By default, `VRTSat` service uses the FQHN (fully qualified host name) as the private domain name. Since you should not tie a clustered service to a specific host, you must instruct the service to use the clustername instead. This should be done before key generation.

Set the clustername using `tcvxat` with the `-setclustername` option.

Example

If your cluster name is `trucluster`, register it using the following command:

```
/opt/VRTSat/bin/tcvxat -setclustername trucluster
```

The broker domains would now be `root@trucluster` and `broker@trucluster`, instead of `root@FQHN`. Keys can be generated invoking `vxatd` with the `-o` option. Refer to the *Administration Guide* for details on using `vxatd`.

Example

The following command line generates keys for the broker in Root+AB mode:

```
/opt/VRTSat/bin/vxatd -o -a -r
```

Step 2: Creating and Registering the Application Resource

Having configured the service and generated the key material, next you must create and register the application profile for `VRTSat` service. This is done using the `-register` option for `tcvxat`, as follows:

```
/opt/VRTSat/bin/tcvxat -register
```

Output will be similar to the following:

```
Creating VRTSat application profile
Validating profile
caa_profile -validate VRTSat
Registering profile
caa_register VRTSat
Starting VRTSat service
caa_start VRTSat
Attempting to start `VRTSat` on member `ssclus08`
Start of `VRTSat` on member `ssclus08` succeeded.
VRTSat successfully registered as a caa application
```

The command creates a resource profile named `VRTSat`, containing the `VRTSat` daemon, and brings it online. To query the status of the resource, use the following command:

```
/usr/sbin/caa_stat VRTSat
```

Output will be similar to the following:

```
NAME=VRTSat
TYPE=application
TARGET=ONLINE
STATE=ONLINE on ssclus08
```

Installing and Configuring Without Invoking Script

You can install and configure the service and register it with the CAA without manually invoking the cluster configuration scripts. In this case, the process takes you through a series of questions and invokes the command lines behind the screens.

To install and configure without invoking the script

1. Install Symantec Product Authentication Service. (See “Basic Installation Instructions”.)
2. Choose the server installation and configuration options.

3 Choose the cluster configuration option.

4 Answer platform specific cluster configuration queries.
You may be asked for the cluster name for Authentication cluster configuration. At completion of this step, the Authentication Service will start.

5 Verify that the service started by using the following command:

```
/usr/sbin/caa_stat VRTSat
```

STATE should be ONLINE.

Note: For instructions on configuring Authorization, see the Symantec Product Authorization Service *Installation Guide*.

Unregistering from CAA

To remove the resources created and registered by `tcvxat`, use the command with the `-unregister` option.

If you have registered the Symantec Product Authorization Service, unregister Authorization before you unregister Authentication from CAA The command to unregister Authorization is:

```
/opt/VRTSaz/bin/tcvxaz -unregister
```

The following command, cleans the TruCluster resource profiles and scripts that were created as a part of configuring the Authentication Service.

```
/opt/VRTSat/bin/tcvxat -unregister
```

Caution: In case of any failure, resources should be unregistered before retrying configuration.

Symantec Product Authentication Service on HP

You can configure Symantec Product Authentication Service as failover dataservices on HP ServiceGuard.

Design Requirements

Following are the design requirements for configuring Symantec Product Authentication Service on HP ServiceGuard Cluster:

- Symantec Product Authentication Service can be configured on the cluster without Symantec Product Authorization Service being installed. Authorization can be configured later when it is installed.

- Symantec Product Authentication Service (and Symantec Product Authorization Service, if you are using it) should run on the cluster in failover mode.
- Symantec Product Authentication Service (and Symantec Product Authorization Service, if you are using it) should be on the same node.

Design Features

A single package contains both Symantec Product Authentication Service and Symantec Product Authorization Service. This is the same configuration as the Symantec Product Authentication Service Service Group in Symantec Cluster Server where the Symantec Product Authorization Service resource depends on the Symantec Product Authentication Service resource.

Symantec Product Authentication Service will be added as Service[0] and Symantec Product Authorization Service will be added as Service[1]. Authorization can be installed and configured after Authentication has been configured.

Resource Dependencies

In HP ServiceGuard there is no concept of a dependency tree. Instead of that, HP Service Guard ensures that the LVs and IP addresses belonging to the package are up before bringing the services up. Also it brings up the services in the order in which they are listed. For offlining it follows the reverse order.

Configuring Authentication on HPServiceGuide Cluster

This section includes steps to configure Authentication on HPServiceGuard cluster using SGManager GUI.

To configure

1. Make a cluster package: vxss_service.
2. Add the services to the package: Symantec Product Authentication Service and Symantec Product Authorization Service.
3. Give their respective service commands:
   - `/opt/VRTSat/bin/vxatd`
   - `/opt/VRTSaz/bin/vrtsaz`
4. Set retry limit to 0 so that HP ServiceGuard will immediately failover the package to the other node on failure of one of the services.
5. Set the IP addresses and LV for Symantec Product Authentication Service and Symantec Product Authorization Service. The Authentication shared LV

should be set to be mounted on `/var/VRTsat` whereas the Authorization shared LV should be set to be mounted on `/var/VRTsaz/` shared.

6 For Authentication, copy the entire `/var/VRTSat` folder to a temporary location. Mount the Authentication shared LV and copy this folder to `/var/VRTSat`. Edit the file `/var/VRTSat/.VRTSat/profile/VRTSatlocal.conf` and set the clustername(the DNS name for the shared IP address) as the value for the key `Security\Authentication\Authentication Broker\ClusterName`. This can be done using the `/opt/VRTSat/bin/vssregctl` command.

7 For Authorization copy the `/var/VRTSaz/objdb` folder to a temporary location. Mount the Authorization shared LV and copy this folder to `/var/VRTSaz/` shared.

Now you are ready to start the package on the cluster.

Chapter 5

Running the Administration Console

This chapter tells how to run the Administration Console, after you have installed and configured.

Sections include:

- Preparing to Run the Administration Console
- Starting the Console to Administer Authentication

For detailed information on performing the tasks you can perform through the Console, see the *Administrator's Guide*.

Preparing to Run the Administration Console

Caution: Consult the Readme for up-to-date instructions pertaining to the specific build of Authentication you have installed.

The Symantec Product Authentication Service Administration Console does not have a separate installable. It is installed as part of the basic installation process.

- On a Windows Platform:
  - All binaries and script files can be found at <*authentication install directory*>\bin
- On a Solaris Platform
  - `libAtWrapper.so`, `AtWrapper.jar`, `vssatgui.jar`, `VxHelpViewer.jar` and `VxHelpViewerl10n.jar` can be found at <*authentication install directory*>`/lib`

- `runvssatgui.sh` can be found at <*`authentication install directory`*>`/bin`

To run the Administration Console, you must meet the following prerequisites:

- For AIX, make sure Java 1.3.x is installed on your system and is pointed to in your PATH statement.
- For systems other than AIX, make sure Java 1.4.2 or above is installed on your system and is pointed to in your PATH statement. To download JDK/JRE visit the following sites:
  - For SUN, Linux, Windows: the Java web site
  - For HP-UX: the Hewlett Packard web site
- Install the following:
  - If you want to run the Administration Console in full authentication and authorization mode, install both Symantec Product Authentication Service and the Authorization Client. The console will recognize whether the Authorization Client is installed on the system and will display the Authorization screens accordingly.
  - If you want to run the console in Authentication-Only mode, install Symantec Product Authentication Service.
  - If you want to run in Client-Only mode (to view and use the Credentials area only), install the Authentication Client.

Understanding Authentication Console Security

The Symantec Product Authentication Service Administration Console has two parts. You can think of them as two separate modes:

- Authentication only
- Authentication plus Authorization

Since it is not appropriate for all users to be able to work with the Administrative Console, certain security measures have been established.

To administer the Authentication Service through the Administration Console, you must login to the actual machine where the Symantec Product Authentication Service is installed and perform the administration tasks from that machine. Furthermore, you must login as administrator (on Windows) or root (on UNIX) to perform administration of the broker.

Starting the Console to Administer Authentication

You can use either the CLI or the Administration Console to manage Symantec Product Authentication Service.

To use the console

1. Log on with administrative rights (on Windows) or as root (on UNIX) on the actual machine where the Symantec Product Authentication Service is installed.
   You will perform the administration tasks from the Administration Console on that machine. You cannot administer the Authentication Service remotely through an Administration Console.
2. Start the Administration Console as follows:
   - On Windows:
     - Modify your path statement, if necessary, so that it points to the <*authentication install directory*>\bin directory for authentication and the <*authorization install directory*>\bin directory for authorization (if you have installed it).
     - Run the Administration Console in either of the two following ways:
       Select **Start Menu** or
       Run runvssatgui.bat from the <*authentication install directory*>\bin directory.
   - On UNIX:
     - Modify your path statement, if necessary, so that it points to the <*authentication install directory*>/bin directory for authentication and the <*authorization install directory*>/bin directory for authorization (if you have installed it).
     - Run <authentication install directory>/bin/runvssatgui.sh

Note: If you will be installing Symantec Product Authorization and you want to run in Authentication plus Authorization mode, see the Symantec Product Authorization Service I*nstallation Guide*.

If You Have Trouble Authenticating

If you receive an error message, check the following:

- Make sure the service is running.
- Make sure that you are logging in as the local administrator.
- If you are on a UNIX platform, make sure you entered the domain name. For UNIX, this is a required field.

Performing Management Tasks

See the Symantec Product Authentication Service *Administrator's Guide* for detailed information on management tasks for Authentication.

Appendix A

Installing with UNIX OS Tools

Chapter 2 of this guide provides instructions for installing Symantec Product Authentication on UNIX platforms through a process that lets you use the same instructions for all platforms. Recognizing that some users may prefer to use the OS tools specific to their own UNIX system, this appendix provides instructions for doing so.

Installing Authentication with UNIX OS Tools

This section provides instructions on installing Symantec Product Authentication on the following UNIX systems, using OS tools specific to those platforms:

- AIX
- HP-UX
- Linux
- Solaris
- Tru64

From UNIX OS tools, the user can also install Authentication in client only mode on Solaris, Linux and Tur64.

Installing Authentication on AIX

This section tells how to install Symantec Product Authentication on AIX platforms.

To install Authentication

1. Make sure you are running as root user on the host.
2. Stop the Authentication Service if it is currently running. For example,

```
$ kill -9 `ps -ef | grep vxatd | grep -v grep | awk '{print
$2}'`
```

3. Uninstall the previous Authentication Service.

```
$ installp -u VRTSat
```

4. From the installation CD, change directory to `/cdrom/aix/authentication /pkgs`, assuming that the installation CD is mounted on `/cdrom`.
5. Install the Authentication Service:

```
$ installp -aXd ./VRTSat.image VRTSat
```

6. See Chapter 2for information on configuring and starting the Authentication Service. Instructions provided there are applicable to all UNIX platforms.

Installing Authentication on HP-UX

This section tells how to install Symantec Product Authentication on HP-UX platforms.

To install

1. Make sure you are running as root user on the host.
2. Stop the Authentication Service if it is currently running. For example:

```
$ kill -9 `ps -ef | grep vxatd | grep -v grep | awk '{print
$2}'`
```

3. Uninstall the previous Authentication Service:

```
$ swremove VRTSat
```

4. From the installation CD, change directory to `/cdrom/hpux/ authentication /pkgs`, assuming that the installation CD is mounted on `/cdrom`.
5. Install the Authentication Service.

```
$ swinstall -s /cdrom/hpux/authentication/pkgs/VRTSat VRTSat
```

6. See Chapter 2 for information on configuring and starting the Authentication Service. Instructions provided there are applicable to all UNIX platforms.

Installing Authentication on Linux

This section tells how to install Symantec Product Authentication Service on Linux platforms.

To install and run

1. Make sure you are running as root user on the host.
2. Stop the Authentication Service if it is currently running. For example:

```
$ kill -9 `ps -ef | grep vxatd | grep -v grep | awk
'{print $2}'`
```

3. Uninstall the previous Authentication Service:

```
$ rpm -e --nodeps VRTSatServer
$ rpm -e --nodeps VRTSatClient
```

4. From the installation CD, change directory to `/cdrom/linux/authentication/rpms`, assuming that the installation CD is mounted on `/cdrom`.
5. Install the Authentication Service:

```
$ rpm -i *.rpm
```

6. See Chapter 2 for information on configuring and starting the Authentication Service. Instructions provided there are applicable to all UNIX platforms.

Installing Authentication on Solaris

This section tells how to install, run, and uninstall the Symantec Product Authentication Service on a Solaris system.

To install

1. Make sure you are running as root user on the host.
2. Stop the Authentication Service if it is currently running. For example:

```
$ kill -9 `ps -ef | grep vxatd | grep -v grep | awk
'{print $2}'`
```

3. Uninstall the previous Authentication Service:

```
$ pkgrm -n VRTSat
```

4. From the installation CD, change directory to `/cdrom/sun/authentication/pkgs`, assuming that the installation CD is mounted on `/cdrom`.
5. Install the Authentication Service:

```
$ pkgadd -d . VRTSat
```

6 See Chapter 2 for information on configuring and starting the Authentication Service. Instructions provided there are applicable to all UNIX platforms.

Installing Authentication on Tru64

This section tells how to install Symantec Product Authentication Service on a Tru64 system.

To install

1 Make sure you are running as root user on the host.

2 Stop the Authentication Service if it is currently running. For example:

```
$ kill -9 `ps -ef | grep vxatd | grep -v
grep | awk '{print $2}'`
```

3 Uninstall the previous Authentication Service.

a First, find out what version of Authentication Service, if any, is installed on the host:

```
$ setld -i | grep VATSER
```

If Authentication Service is currently installed on the host, you will see something like this. The version is the three digits after VATSER. In this case, the version is 427.

```
VATSER427 installed VERITAS Authentication Server
(Version 4.1.1.17)
```

b Remove the Authentication Service by issuing the following command:

```
$ setld -d VATSER### VATCLI###
```

Where `###` is the version number.

4 From the installation CD, change directory to `/cdrom/osf1/authentication/pkgs`, assuming that the installation CD is mounted on `/cdrom`.

5 Install the Authentication Service:

```
$ setld -l ./VRTSat
```

6 See Chapter 2 for information on configuring and starting the Authentication Service. Instructions provided there are applicable to all UNIX platforms.

Appendix B

Configuring to Work with a Web Console

For many resource management applications, Symantec provides web consoles, which look and act much like desktop consoles, but which can be accessed through the internet. For web consoles, authentication is different and requires explanation.

This section explains why a product web credential is needed when working with a web console. It then provides an example of configuring to use a web console with Symantec Enterprise Administrator.

When and Why a Product Web Credential is Needed

A regular product credential is a digital certificate obtained from an Authentication Broker after providing it a username/password, which can be verified by that broker. The product credential consists of two parts: a private key and a public key.

Both these parts are required when a client wants to establish an SSL connection to a service. Typically, when an entity seeks to be authenticated, the Symantec library returns only the public part, while the private part is safeguarded by the library itself.

For web consoles, however, the client is a browser. Therefore, it cannot store and present a product credential. In such a case, a credential must be obtained by the web console *on* behalf of the browser.

To achieve single sign-on from one web console to another, the credential obtained by the first web console must be appended to the end of the URL which points to the other web console. When someone clicks on the URL, the credential gets submitted to the second web console as a part of the HTTP request. The second web console extracts that credential and lets the principal in.

However, it is important to remember the two following facts:

- Different web consoles could potentially be running on different machines.
- The credential consists of just the public part. Therefore, the credential in itself cannot be used by the second web console to establish a secure connection with the service on behalf of the principal.

For these reasons, web consoles have to obtain a special kind of credential called the *product web-credential*, which works along with a *proxy-capable credential*.

Product Web Credential

A product web credential tells the Symantec library that there is no corresponding private part stored in the library. Such a product web credential cannot be used alone; it must be used along with a proxy-capable credential of the web console.

Proxy-Capable Credential

The proxy-capable credential is obtained by the web console during configuration. It is a special long-term credential for each service that the console is set up to access. The special quality of this type of credential is that it has proxy rights. That means that the proxy credential lets the web console proxy on behalf of the actual user. It works like this:

- When a user logs in, the web console first establishes a secure connection to the service, using its own credential.
- It then passes along the user's product web credential over the secure channel. This way, the service knows which principal is trying to access the service and applies authorization accordingly.

Example: Configuring a Web Console to Access VEA

The steps below describe the process of configuring a web console. For the purposes of our example, we assume that the user wants to configure to work with Symantec Enterprise Administrator.

To configure the web console to work with VEA

1. When you install a service that has been enabled to use Symantec Product Authentication Service and that has a web console, you should create a user in its Authentication Broker that has proxy rights. For example, when you are installing Symantec Enterprise Administrator, you could create an account called "veawebconsole" in its Authentication Broker's private domain and assign proxy rights to that account. The user will need to remember the password for this account.

2 When you configure the web console (on either the same or a remote system) to access the service, the console prompts the user for the identity/password of the proxy account – veawebconsole -- created when you installed the service.

Note: The initial communication between the web client and the web server, when the client transports the username/password, should be over a secure channel (https).

---

3 The web console uses the supplied identity/password to obtain a long-term credential from that service's Authentication Broker. This credential has proxy rights and can be used to establish an SSL connection to the service.

4 After obtaining the proxy credential, the web console can discard the password and is now set up to access the service. If a single console is designed to access multiple services (each with a different ROOT hierarchy), it must obtain one such credential for each of those services.

Accessing the Application through the Web Console

Assuming that the web console has already been configured to access VEA, the following steps occur:

1 When the user accesses the console for the first time, the console prompts for a valid identity/password authorized to access the service.

2 The console contacts the service's Authentication Broker and obtains a product web credential for the user by providing the specified identity/password.

3 The console establishes an SSL connection to the service using its own proxy-enabled credential (not the user's product web credential).

4 The service accepts the connection and examines the console's proxy credential. From the credential it knows that the web console is trying to connect to it on behalf of the user and therefore waits for the console to send it the user's product web credential next.

5 The console sends the product web credential of the logged in user over the secure channel. The exact manner in which this piece of data is transmitted will be application specific.

6 The service verifies the product web credential using the `vrtsAtWebCredentialVerify()` method, and if successful, extracts information from the product web credential. Based on this information, it then applies the proper authorization.

Glossary

Access Token

A data structure generated for an authentication principal when the principal logs on and containing that authentication principal's security identifier, identifiers for groups the principal belongs to, and a list of the privileges the principal has on the local computer where he or she logged in. The access token defines the security context for the authentication principal.

Account Name

An alternative term for “authentication principal.

Administration Console

A graphical interface used to administerAuthentication. For example, the administrator uses it to indicate the location of the different components, trust relationships, plugins, private Symantec domains, etc.

Application Client

A program that accesses a service or function provided by another program, called an application service. An example of an application client is the Symantec Volume Manager GUI. An application client uses Authentication to validate the ID of the user of that client.

Application Host

The machine on which an application is running.

Application Service

A program that is contacted by, and provides services to, an application client.

AT

In CLI command usage and in certain graphics, an abbreviation referring to Authentication.

Authentication Broker

The component that serves, one level beneath the Root Broker, as an intermediate registration authority and a certification authority. The Authentication Broker can authenticate clients, such as users or services, and grant them a certificate that will become part of the product credential. An Authentication Broker cannot, however, authenticate other brokers. That task must be performed by the Root Broker.

Authentication Broker Tree

A three level certificate hierarchy which includes all the identified entities whose certificates chain up to a single root certificate.

Authentication Group

A named collection of authentication principals, established in a native operating system, and treated as a single entity for the sake of convenience and ease. All members of an authentication group will be from the same authentication domain. The product credential

will contain a list of all groups the principal belongs to in that authentication domain. Also called OS Group.

Authentication Library

The part of the Symantec Product Authentication Service that links with an application client and implements the program calls it must make in order to request authentication.

Authentication Mechanism

The method by which authentication is conducted for principals in a specific name-space defined by a domain. For example, a Kerberos domain uses Kerberos tickets and password. In UNIX platforms, Kerberos domains are used through the GSS-API. An authentication mechanism encapsulates all the details of the authentication algorithm, including APIs, protocols, token formats, token contents semantics and database objects formats. Not all the ingredients are relevant in all mechanisms.

Authentication Plugin

A component used by the Authentication Broker to validate identities within a particular domain. An authentication plugin exists for each supported authentication mechanism. For example, one plugin can validate NIS identity and password combinations against an NIS database, while another uses a Kerberos ticket to authenticate the principal.

Authentication Principal

A user, computer, or process such as a command line interface (CLI) or service that has the ability to authenticate to Symantec Product Authentication Service with a unique identity. An authentication principal differs from a security principal in that not all security principals can validate; nor are they all accountable for their actions.

Authentication Private Domain

A specialized authentication domain used to hold identities and password hashes for authentication principals unique to, and managed by, Symantec products for which customers do not want to reuse an existing identity in another domain. Authentication private domains can be used to hold identities of point products, such as SAN Point Control and Volume Manager.

Authentication Private Domain Repository (PDR)

A store of one or more authentication private domains. The Authentication Broker loads this repository, and principals are checked against it in order to be validated.

Boundary Condition

The starting point or initial state of something.

Certificate

A type of electronic passport or ID card that vouches for the identity of its holder and ties the principal's name to his or her public key. product credentials require a certificate and the client’s private key.

Certification Authority

A trusted third party responsible for issuing, managing, and revoking certificates that vouch for the identities of the certificate holders. In Symantec Product Authentication Service, the certification authority is a part of the Authentication Broker.

CLI

Command line interface.

Communications Library

A part of Authentication that provides secure communication between an application client and an application service, using the product credential acquired in a preceding authentication interaction.

Cyphertext

The encrypted output of an encryption process.

Digital Certificate

See Certificate.

Digital Signature

A block of data appended to a message such that the recipient of the message can verify the contents and the originator of the message. There are a number of digital signature algorithms in use.

Domain

See "Authentication Private Domain".

Mapping, Domain-Broker

The set of information telling which Authentication Broker should be approached, for each domain, when attempting to authenticate.

Message Digest Function

An algorithm that generates a digest from its input (for example, a message). The digest is statistically unique. That is, different inputs are extraordinarily unlikely to have the same fingerprint. Moreover, small changes in its input lead to large changes in its output and therefore are easily detected.

Object

An entity, whether visible and tangible or not, that can be manipulated by a process or program.

Plaintext

The unencrypted input to an encryption process.

Principal

See "Authentication Principal".

Private Domain

See "Authentication Private Domain." .

Product Credential

An entitlement to be recognized as a valid identity. A product credential requires both (1) the principal's private key and (2) a X.509v3 certificate with special extensions, produced and signed by the Authentication Broker or Root Broker, to bind the principal's name to the public key. The product credential provides single-sign-on capability for all Symantec applications that use the Symantec Product Authentication Service and that choose to participate in the Symantec single sign-on session.

Product Web Credential

A special kind of credential that tells the Symantec Product Authentication Service library that there is no corresponding private part stored in the library. Such a credential must be used along with a proxy-capable credential of the web console.

Protected Application

A shorthand way or referring to a resource management application that has been configured to be protected by Symantec Product Authentication/Authorization Service.

Public Key Encryption

A security method that requires using one key to encrypt a piece of data and another distinct but mathematically-related key to decrypt it. The two keys are the public key, which can be used by anyone, and the private key, which relates to this specific public key and must be kept secret. Either key can be used for encryption, but its companion must be used for decryption. Without both keys, the process fails. Public key encryption is also called *asymmetric encryption*.

Public Key Infrastructure (PKI)

A framework established to issue, maintain, and revoke public key certificates.

Resource Management Application

A Symantec product whose resources are being protected by Symantec Product Authentication Service.

Root Broker

The first Authentication Broker, which has a self-signed certificate. The Root Broker has a single private domain that holds only the names of brokers that shall be considered valid. The name of the Root Broker itself is stored as the fully qualified domain name.

Root Certificate

The self-signed digital validation, with specific information stating that it is a certification authority certificate.

Root Certification Authority

The entity at the top of the hierarchy of authorities allowed to sign digital certificates vouching for the validity of principals, therefore the most trusted certification authority.

Root Hash

The thumbprint of the Root Broker's credential, it takes the form of a binary file and uniquely identifies a Root Broker. The Root Hash is used for establishing trust relationships. It can be found in `/opt/VRTSat/bin` for UNIX and `<InstallDir>\Authentication\bin` on Windows.

Secure Sockets Layer Protocol (SSL)

A public key protocol originally created by Netscape and used for secure communications between clients and servers over the Web. In context of Symantec Product Authentication Service, Secure Sockets Layer technology provides secured communications between the client, Authentication Broker, and service. The acronym SSL is nearly always used for this term.

Security Context

The identity of an authentication principal, the groups to which it belongs, and the set of privileges the principal has on the local computer where he or she logged in. The security context is established by the access token.

Security Identifier

A unique value identifying a secured principal that holds an account within an enterprise.

Security Policy

A well-thought-out set of decisions regarding how your product should be used in a customer's environment, how your product could be misused, and what range of access rules your customers would like to see enforced by your product.

Security Principal Name

The unique name used to identify a human user, a group, or a computer within a domain.

SSPI

Security Support Provider Interface (SSPI) from Windows, which provides a set of authentication and communication security services between applications running on Microsoft platforms.

Subject

A thread executing on behalf of (i.e., with the permissions of) an authentication principal. Those permissions would have been granted by an administrator explicitly to the security principal which includes that authentication principal.

Symantec Product Authentication Service

A component that validates identities and sets up secured communications between authenticated entities, sometimes referred to as *peers*. It provides a single sign-on service for all Symantec products that the administrator configures to be protected by it.

User

A human authentication principal whose name, recognized by Symantec Product Authentication Service, is the name of their operating system access account. The term "human user" will be used to refer to this type of principal.

Index

W