Veritas™ Cluster Server One Agent for Sybase Installation and Configuration Guide

AIX, HP-UX, Linux, Solaris

5.0

March 2009

symantec™

Veritas Cluster Server One Agent for Sybase Installation and Configuration Guide

Agent version: 5.0

Document version: 5.0.1

Legal Notice

Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014

http://www.symantec.com

Technical Support

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

Symantec's maintenance offerings include the following:

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

For information about Symantec's Maintenance Programs, you can visit our Web site at the following URL:

www.symantec.com/techsupp/

Contacting Technical Support

Customers with a current maintenance agreement may access Technical Support information at the following URL:

www.symantec.com//business/support/assistance_care.jsp

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

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information
- Available memory, disk space, and NIC information
- Operating system

- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

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

www.symantec.com/techsupp/

Customer service

Customer service information is available at the following URL:

www.symantec.com/techsupp/

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

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

Documentation feedback

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

Maintenance agreement resources

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

Asia-Pacific and Japan	contractsadmin@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Additional enterprise services

Symantec offers a comprehensive set of services that allow you to maximize your investment in Symantec products and to develop your knowledge, expertise, and global insight, which enable you to manage your business risks proactively.

Enterprise services that are available include the following:

Symantec Early Warning Solutions	These solutions provide early warning of cyber attacks, comprehensive threat analysis, and countermeasures to prevent attacks before they occur.
Managed Security Services	These services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.
Consulting Services	Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring, and management capabilities. Each is focused on establishing and maintaining the integrity and availability of your IT resources.
Educational Services	Educational Services provide a full array of technical training, security education, security certification, and awareness communication programs.

To access more information about Enterprise services, please visit our Web site at the following URL:

www.symantec.com

Select your country or language from the site index.

Contents

Chapter 1

Introducing the Veritas Cluster Server One agent for Sybase

This chapter includes the following topics:

About the Veritas Cluster Server One agent for Sybase

The Veritas High Availability Agent for Sybase brings the configured Sybase servers online, monitors them, and takes them offline.

The package contains the following agents:

- Agent for SQL Server- Sybase
- Agent for Backup Server- SybaseBk

The agents include type declarations and agent executables, and are represented with Sybase and SybaseBk resource types, respectively. Both agents work together to make Sybase highly available in a VCS One cluster.

Note: The VCS One agent for Sybase provides "active/passive" support for Sybase. For "active/active" support, contact Sybase for their agent.

What's new in this release

The VCS One agent for Sybase includes the following new feature:

- The agent supports Red Hat Enterprise Linux 5 on VCS One 2.0.1.

Supported software

The VCS One agent for Sybase supports the following software versions:

Sybase	Sybase Adaptive Server Enterprise (ASE) 12.5.x and 15.0
Veritas Cluster Server One	VCS One 2.0 and VCS One 2.0.1 on AIX, HP-UX, Linux, and Solaris
AIX	AIX 5.3 and 6.1 Refer to the Veritas Cluster Server One Release Notes for more details. Note: The agent does not support WPAR.
HP-UX	HP-UX 11i version 2.0 HP-UX 11i version 3.0 Refer to the Veritas Cluster Server One Release Notes for more details.
Linux	The agent supports the following Linux distributions: ■ Red Hat Enterprise Linux 4 ■ SUSE Linux Enterprise Server 9 with SP3 The agent also supports Red Hat Enterprise Linux 5 on VCS One 2.0.1. Refer to the Veritas Cluster Server One Release Notes for more details.
Solaris	Solaris SPARC: Solaris 9 and Solaris 10 (64-bit) Solaris x64: Solaris 10 (64-bit) For Solaris, Symantec recommends applying the latest Solaris operating system patches available from Sun. Visit Sun's Web site for more information.

Note: VCS One can manage Sybase that is installed on different operating systems. But the application failover can occur only between the server farm systems that run the same operating system version and patch level.

How the agent makes Sybase highly available

The agent for Sybase can perform different levels of monitoring and different actions which you can configure. In the basic monitoring mode, the agent detects an application failure if a configured Sybase server process is not running. In the detail monitoring mode, the agent detects application failure if it cannot perform a transaction in the test table in the Sybase database server.

When the agent detects that the configured Sybase server is not running on a system, the Sybase service group is failed over to another server farm system in the server farm. The configured Sybase servers are started on the new system, thus ensuring high availability for the Sybase server and data.

On Solaris 10, VCS One provides high availability to applications that run in the context of Solaris Containers. You can configure the VCS One agent for Sybase to monitor these resources that run in the context of Solaris zones and projects.

See "Sybase instances running in Solaris zones" on page 13.

See "Sybase instances running in the context of Solaris Resource Managers" on page 14.

Sybase instances running in Solaris zones

Solaris 10 provides workload management through Solaris Resource Manager (SRM). SRMenables you to manage, allocate, and control resources at the workload level instead of the individual process level. A workload is a collection of all the process that constitute a one or more applications. VCS One lets you set workload at service group level to all the applications. VCS One enforces load restrictions through Solaris Resource Manager.

See Veritas Cluster Server One User's Guide.

VCS One provides high availability to applications running in the context of Solaris projects. For applications running in the context of projects, the agent's script entry points can execute the commands that run in the context of projects.

The Veritas Cluster Server One agent for Sybase is project-aware and can monitor Sybase instances running in the context of Solaris projects.

Sybase instances running in the context of Solaris Resource Managers

Solaris 10 provides workload management through Solaris Resource Manager (SRM).SRMenables you to manage, allocate, and control resources at the workload level instead of the individual process level. A workload is a collection of all the process that constitute a one or more applications.

VCS One lets you set workload at service group level to all the applications. VCS One enforces load restrictions through Solaris Resource Manager.

See Veritas Cluster Server One User's Guide.

VCS One provides high availability to applications running in the context of Solaris projects. For applications running in the context of projects, the agent's script entry points can execute the commands that run in the context of projects.

The Veritas Cluster Server One agent for Sybase is project-aware and can monitor Sybase instances running in the context of Solaris projects.

Agent functions

The functions an agent performs are called entry points. Review the functions for the following agents that are part of the Veritas Cluster Server One agent for Sybase:

Sybase agent functions

See "Agent for SQL server- Sybase" on page 14.

Sybase Bk agent functions

See "Agent for Backup server- SybaseBk" on page 15.

Agent for SQL server- Sybase

The agent for Sybase starts a Sybase SQL server, monitors the server processes, and shuts down the server.

Table 1-1 lists the Sybase agent for SQL server operations.

Table 1-1 Sybase agent for SQL server operations

Agent operation	Description
Online	Starts the Sybase SQL server by using the following command. `startserver -f $SYBASE/$SYBASE_ASE/install/RUN_$Server`

Table 1-1 Sybase agent for SQL server operations *(continued)*

Agent operation	Description
Monitor	In the basic monitoring mode, the agent scans process table for the dataserver process. In detail monitoring mode, the agent runs the script that is specified in Monscript as an option. See "Monitoring options for the Sybase agent" on page 16.
Offline	Stops the Sybase SQL server by using the `isql` command in the following manner. The agent first executes the command `shutdown with wait`. If this command fails, the offline script executes `shutdown with nowait`.
Clean	Forcefully stops the Sybase SQL server by using the `isql` command in the following manner. The agent first executes the command `shutdown with wait`. If this command fails, the clean script executes `shutdown with nowait`. If the process does not respond to the `shutdown` command, the agent scans the process table for the processes that are associated with the configured database and kills them.

Agent for Backup server- SybaseBk

The agent for SybaseBk starts a Sybase Backup server, monitors the server process, and shuts down the server.

Table 1-2 lists the Sybase agent for Backup server operations.

Table 1-2 Sybase agent for Backup server operations

Agent operation	Description

Online	Starts the Sybase Backup server by using the following command.
	
	`startserver -f $SYBASE/$SYBASE_ASE/`
	
	`install/RUN_$BackupServer`

Monitor	Scans the process table for the backupserver process.

Table 1-2 Sybase agent for Backup server operations *(continued)*

Agent operation	Description
Offline	Stops the Sybase Backup server by using the `isql` command in the following manner. The agent first executes the command `shutdown SYB_BACKUP with wait`. If this command fails, the offline script executes `shutdown SYB_BACKUP with nowait`.
Clean	Forcefully stops the Sybase Backup server by using the `isql` command in the following manner. The agent first executes the command `shutdown SYB_BACKUP with wait`. If this command fails, the clean script executes `shutdown SYB_BACKUP with nowait`. If the process does not respond to the `shutdown` command, the agent scans the process table for the processes that are associated with the configured Sybase Backup server and kills them.

Monitoring options for the Sybase agent

The agent for Sybase provides two levels of application monitoring: basic and detail.

In the basic monitoring mode, the agent for Sybase monitors the Sybase daemon processes to verify whether they are running.

In the detail monitoring mode, the agent performs a transaction on a test table in the database to ensure that Sybase functions properly. The agent uses this test table for internal purposes. Symantec recommends that you do not perform any other transaction on the test table.

See "Setting up detail monitoring for the agent" on page 39.

When the agent detects that the configured Sybase server is not running on a system, the Sybase service group is failed over to another server farm system in the server farm. The configured Sybase servers are started on the new server farm system, thus ensuring high availability for the Sybase server and data.

Typical Sybase configuration in a VCS One sever farm

A typical Sybase configuration in a VCS One server farm has the following characteristics:

- The Policy Master runs on two nodes in the server farm.

- The VCS One client is installed on all server farms.
- The Sybase data is installed on shared storage.
- The Sybase binaries are installed locally on server farms or on shared disks.
- The Veritas Cluster Server One agent for Sybase is installed on server farm systems.

Figure 1-1 depicts a configuration where Sybase binaries and data are installed completely on shared disks.

Figure 1-1 Sybase binaries and data on shared disks

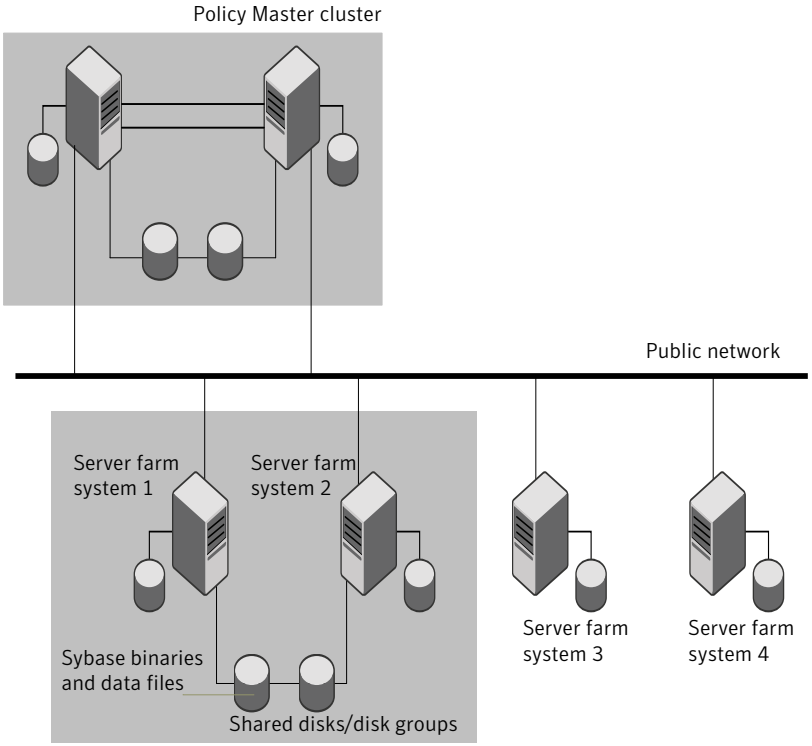
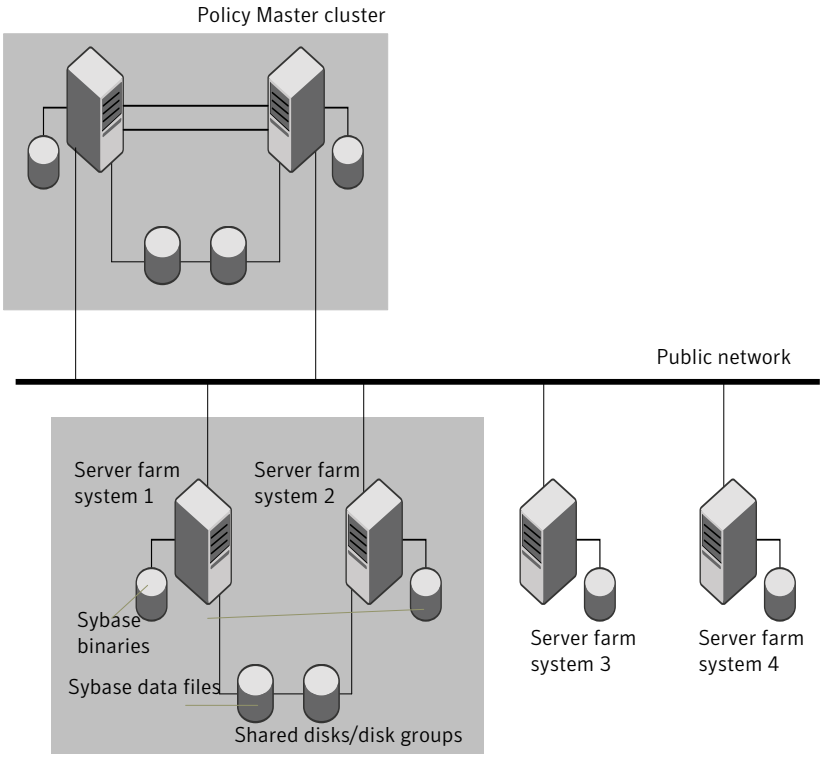


Figure 1-2 depicts a configuration where Sybase binaries are installed locally on each server farm system and Sybase data is installed on shared disks.

Figure 1-2 Sybase binaries on local disk and Sybase data on shared disk



About setting up Sybase in a VCS One server farm

Tasks involved in setting up Sybase in a VCS One environment include:

- Setting up a VCS One server farm
  Refer to *Veritas Cluster Server One Installation Guide* for more information on installing and configuring VCS One.
- Installing and configuring Sybase.
  See "Installing Sybase in a VCS One environment" on page 25.
- Installing the Veritas Cluster Server One agent for Sybase.
  See "Before you install the agent for Sybase" on page 27.
- Configuring VCS One service groups for Sybase.
  See "About configuring a service group for Sybase " on page 35.

Chapter 2

Installing and configuring Sybase

This chapter includes the following topics:

About installing Sybase in a VCS One environment

The strategy for installing Sybase into a VCS One server farm is aimed at ensuring that installations on all server farm systems in the server farm are uniform.

See the Sybase documentation. You can install Sybase in the following ways in a VCS One environment:

$SYBASE_HOME on the shared disk	Sybase binaries and Sybase data are installed on shared disks.
$SYBASE_HOME on the local disk	Sybase binaries are installed locally on each server farm system and Sybase data is installed on shared disks.

When installing Sybase, ensure that the login_id, id_name, group_id, and group_name for the Sybase owner is the same on all the server farm systems.

VCS One requirements for installing Sybase

Review the following prerequisites and requirements before you install Sybase in a VCS One server farm. Before installing Sybase, make sure the systems in the server farm system have adequate resources to run Sybase and VCS One

Sybase installation directory

The Sybase installation directory can be located on a local disk or a shared storage.

Review the following prerequisites:

- If the Sybase binaries are installed on a local disk, verify that the installation path is same on all the nodes in the cluster. Make sure the Sybase configuration files are identical on all the nodes in the cluster.
- If the Sybase binaries are installed on shared disks, make sure the mount points for the shared disks are same on all the nodes. The Sybase installation directory is specified by the environment variable $SYBASE. Create the same $SYBASE mount points on each system.

$SYBASE directory on shared disks

All database devices, including master devices, sybsystemprocs, and information about Sybase user must be located on shared disks. If the database devices are created on file systems, the file systems must also be located on shared disks. Create the same file system mount points on each system to access the shared disks.

Database dbspaces

If you use shared disks for dbspaces, change the permissions, or access mode on the disk groups that store the Sybase data. Change the permissions for sybase to 660.

For example, if you use Veritas Volume Manager, type

```
# vxedit -g diskgroup_name set group= dba\

user=sybase mode=660 volume_name
```

Transparent TCP/IP failover

For Sybase server failover to be transparent to Sybase clients, create an IP address as part of the Sybase service group. This IP address must match the dataserver and backup server entries in the $SYBASE/interfaces file. For information on the

format for adding entries to the $SYBASE/interfaces file, refer to the Sybase documentation.

System user for Sybase home directory

Make sure you have a system user, with the same username and ID, on all cluster nodes. Also, the system user should have the ownership of the Sybase home directory on the shared disk. Type the following commands:

```
# useradd -u user_id user_name
# chown -R user_name $SYBASE
```

Long pathname limitation for $SYBASE

The AIX and Solaris process tables limit process names to 79 characters.

A process having a longer pathname is truncated in the table, making it unrecognizable. The Sybase home directory ($SYBASE) could possibly have such a long pathname. In this case, you can create a soft link to the $SYBASE directory and use it in place of the long filename in the appropriate Sybase installation files.

See "Using a soft link to a $SYBASE pathname" on page 21.

Using a soft link to a $SYBASE pathname

Using a soft link pathname avoids the problems that arise due to the long pathname.

After creating the soft link on each system, you must edit the following files, by making the appropriate substitutions.

- The file RUN_Server in the directory $SYBASE/$SYBASE_ASE/install.
- The file RUN_Server_back in the directory $SYBASE/$SYBASE_ASE/install.

Example- Replacing $SYBASE pathname with a soft link

The following example demonstrates how to replace a $SYBASE pathname with a soft link.

To replace a $SYBASE pathname with a soft link

1 On each system in the cluster, create a soft link to the long pathname.

For example,

```
# ln -s /opt/apps/sybase/home/directory/is/longer/than\
    eighty/characters/sybase /opt/link_to_longpath
```

Now the process is invoked with the short pathname of the soft link.

2 In the $SYBASE/$SYBASE_ASE/install directory, edit the two files RUN_Server and RUN_Backupserver_back. Find all instances of the long pathname, for example, /opt/apps/sybase/home/directory/is/longer/than/eighty/characters/sybase. Replace all the instances with the soft link, for example, /opt/link_to_longpath.

Example: The file RUN_Server resembles the following before the change:

```
/opt/apps/sybase/home/directory/is/longer/than/eighty
  /characters/sybase/ASE-12_5/bin/dataserver\
-d/dev/vx/rdsk/db_dg1/vol2\
-e/opt/apps/sybase/home/directory/is/longer
  /than/eighty  /characters/sybase/install/fw17i.log\
-M/opt/apps/sybase/home/directory/is/longer/than/eighty
  /characters/sybase\
-sfw17i\
```

After the replacement, the file resembles as follows:

```
/opt/link_to_longpath/ASE-12_5/bin/dataserver\
-sfw17i\
-d/dev/vx/rdsk/db_dg1/vol2\
-e/opt/link_to_longpath/install/fw17i.log\
-M/opt/link_to_longpath\
```

Make sure that the -s option and its argument (fw17i in the example) are the first to be listed. It must be placed within the first eighty characters of the file. Failure to do this will not bring the service group online.

For example, if you do not put the -s option and the argument in the first eighty characters, the command string that will be considered is as follows:

```
/opt/apps/sybase/home/directory/is/longer/than/eighty
  /characters/sybase/ASE-12_5/
```

In this case, the -s option will be omitted and the service group will fail to come online. However, if you moved the -s to be the first option, the first eighty characters of the command string for the same example will be as follows:

```
/opt/link_to_longpath/ASE-12_5/bin/dataserver\
  -sfw17i\
  -d/dev/vx/rdsk/db_dg1/vol2
```

In this case, the -s option is among the first eighty characters.

3 Edit the Home attribute for both the Sybase type and the SybaseBk type.

For example: Home = "/opt/link_to_longpath"

See "Sybase resource type" on page 49.

See "SybaseBk resource type" on page 52.

Configuring Sybase for detail monitoring

This section describes the tasks to be performed for configuring a Sybase server to be monitored in detail.

See "Setting up detail monitoring for the agent" on page 39.

Note: The steps that are described here are specific to the sample script, SqlTest.pl, provided with the agent. If you use a custom script for detail monitoring, you must configure the Sybase database accordingly.

Perform these steps only once in a Sybase cluster.

To set up Sybase for detail monitoring

1 Source the SYBASE.sh file or SYBASE.csh file (depending on the user shell) to set the $SYBASE and $SYBASE_ASE environment variables.

2 Start the Sybase server.

```
# $SYBASE/$SYBASE_ASE/install/RUN_server_name
```

3 Start the Sybase client on any cluster node.

```
# isql -Usa
```

Enter the administrator password when prompted to do so.

4 Connect to the master database.

```
# use master
# go
```

5 Create a Sybase user account.

```
# sp_addlogin user_name, password
# go
```

The detail monitor script should use this account to make transactions on the database.

6 Create a database.

```
# create database database_name
# go
```

The detail monitor script should make transactions on this database.

7 If required, restrict the size of the log file for the database.

```
# sp_dboption database_name, " log on chkpt", true
# go
```

8 Connect to the database that is created in step 6.

```
# use database_name
# go
```

9 Associate the user created in step 5 with the database created in step 6.

```
# sp_adduser user_name
go
```

10 Change the user to the one created in step 5.

```
# setuser user_name
# go
```

11 Create a table in the database.

```
# create table table_name (lastupd datetime)
# go
```

The detail monitor script should make transactions on this table.

If you use the SqlTest.pl for detail monitoring, make sure you create a table with a lastupd field of type datetime.

12 Verify the configuration by adding an initial value to the table.

```
# insert into table_name (lastupd) values (getdate())
# go
```

13 Exit the database.

```
# exit
```

Installing Sybase in a VCS One environment

For information on how to install Sybase, refer to Sybase documentation.

Chapter 3

Installing and removing the VCS One agent for Sybase

This chapter includes the following topics:

Before you install the agent for Sybase

Meet the following prerequisites to install the Veritas Cluster Server One agent for Sybase:

- Make sure SSH or rsh communications is set up.
  You must be able to communicate from the client system where you run the installation program to the client systems where you want to install the VCS One agent pack software.
  For information on configuring SSH for remote communication, refer to *Veritas Cluster Server One Installation Guide*.
- Make sure the VCS One client is installed on Policy Master node or on all client systems.
  Refer to the *Veritas Cluster Server One Installation Guide*.
- If Veritas Cluster Server agent for Sybase is installed on any of the client systems, uninstall it.
- If a previous version of the agent is installed, uninstall it.
- Verify that Sybase is installed and configured.

See Sybase documentation.
See "About installing Sybase in a VCS One environment" on page 19.

Installing the Cluster Server One agent for Sybase

You must install the VCS One agent for Sybase on all the client systems of the server farm that will host the Sybase service group. You can install the VCS One agent for Sybase using the installagpack program. The installagpack program installs the VCS One agent for Sybase along with all the VCS One agents that the Veritas High Availability Agent Pack includes.

The installation of the agent packs typically involves the following phases:

Installing the agent packages	See "Installing the agent packages" on page 28.
Adding the agent resource type definitions	See "Adding the agent resource type definitions " on page 29.

Installing the agent packages

You can add the agent packages on one or more client system of a specific platform type.

To install the Veritas high availability agents

1. Mount the VCS One Agent Pack software disc on the client system where you plan to run the installation.
2. Depending on the platform type, navigate to the directory containing the installer for the VCS One agents:

AIX	`cd aix/high_availability_agents`
HP-UX	`cd hpux<os_version>/high_availability_agents` Where *os_version* is the HP-UX version.
Linux	`cd linux/dist_arch/high_availability_agents` Where *dist* is the Linux distribution and *arch* is the architecture.
Solaris	`cd solaris/arch/high_availability_agents` Where *arch* is the architecture.

3 Enter the command to start the agent pack installation:

```
# ./installagpack [-rsh]
```

You can use the `-rsh` option if rsh and rcp are used for communication between systems instead of the default ssh and scp. This option requires that systems be preconfigured such that the `rsh` commands between systems execute without prompting for passwords or confirmations.

4 Enter the name of a client system or client systems where you want to install the agents.

5 Review the output as the installation program installs the agent packages.

You can view installation logs in the /var/VRTS/install/logs directory.

Adding the agent resource type definitions

You must add the agent resource type definitions to the Policy Master database configuration. You can perform this task from any client system in the server farm.

Note: You must add the agent resource type definitions only one time per platform type.

To add the VCS One resource types to the PM database configuration

1 Set up rsh or SSH communications between the client system and the PM system.

For information on configuring SSH for remote communication, refer to *Veritas Cluster Server One Installation Guide*.

2 Make sure that the PM daemon is running.

```
# haclus -display
```

The output should show ClusterState is RUNNING.

3 If you have just installed the agents on VCS One client systems and still have the VCS One Agent Pack software disc mounted, skip to step 6.

4 Mount the VCS One Agent Pack software disc.

5 Depending on the platform type, navigate to the directory containing the installer for the VCS One agents:

AIX	`# cd aix/high_availability_agents`
HP-UX	`# cd hpux<os_version>/high_availability_agents` Where *os_version* is the HP-UX version.
Linux	`# cd linux/dist_arch/high_availability_agents` Where *dist* is the Linux distribution and *arch* is the architecture.
Solaris	`# cd solaris/arch/high_availability_agents` Where *arch* is the architecture.

6 Enter the command to start the agent pack installer for adding resource types to the Policy Master configuration database. Use the `-addtypes` option:

```
# ./installagpack -addtypes
```

7 When the installer prompts, enter the virtual IP address of the Policy Master.

8 Review the output as the installer verifies communication with the Policy Master system.

9 Review the output as the installer adds the agent types to the PM database configuration and copies the appropriates types.xml files to the PM system.

You can view installation logs in the /var/VRTS/install/logs directory.

Disabling the VCS One agent for Sybase

To disable the agent on a system, you must first change the Sybase service group to an OFFLINE state. You can stop the application completely, or switch the service group to another system.

To disable the agent

1 Determine if the service group is online. At the prompt, type:

```
# hagrp -state service_group -sys system_name
```

2 If the service group is online, take it offline. At the prompt, type:

```
# hagrp -switch service_group -to system_name
```

Or

```
# hagrp -offline service_group -sys system_name
```

3 Stop the agent on the system. At the prompt, type:

```
# haagent -stop Sybase -sys system_name
```

```
# haagent -stop SybaseBk -sys system_name
```

4 When you get the message "`Please look for messages in the log file,`" check the file /var/VRTSvcsone/log/engine_A.log for a message confirming the agent has stopped.

You can also use the `ps` command to verify that the agent has stopped.

5 When the agent has stopped, you can remove the system, the service group, or the resource type from the VCS One configuration.

For more information, see the chapter on reconfiguring VCS One from the command line in:

Veritas Cluster Server One User's Guide.

Removing the VCS One agent for Sybase

Make sure you disabled the agent on all client systems before you remove the service group, the resource type, or both from the VCS One configuration.

You can remove all the VCS One packages that the installagpack program installed, or remove only the VCS One agent package for Sybase. Removing the agent involves removing the agent files from each client system where you installed. Before you attempt to remove the agent, make sure the application service group is not ONLINE.

See "Removing all the VCS One agent packages" on page 32.

See "Removing the VCS One agent package for Sybase" on page 32.

You can remove the agent type definition from the Policy Master system after removing the agent packages.

See "Removing the agent type definition from the Policy Master system" on page 33.

Removing all the VCS One agent packages

You can remove all the VCS One agent packages that the installagpack program installed using the uninstallagpack program.

To remove all the VCS One agent packages from client systems

1. Mount the VCS One Agent Pack software disc on the client system where you plan to run the uninstallagpack program.
2. Depending on the platform type, navigate to the directory containing the uninstaller for the VCS One agents:

AIX	`cd aix/high_availability_agents`
HP-UX	`cd hpux<os_version>/high_availability_agents` Where *os_version* is the HP-UX version.
Linux	`cd linux/dist_arch/high_availability_agents` Where *dist* is the Linux distribution and *arch* is the architecture.
Solaris	`cd solaris/arch/high_availability_agents` Where *arch* is the architecture.

3. Start the uninstallagpack program.

```
# ./uninstallagpack
```

4. Enter the name of the client systems separated by spaces on which you want to uninstall the agent pack.
5. Review the output as the program verifies the agent pack that you installed and removes the agent packages.

   You can view logs in the /var/VRTS/install/logs directory.

Removing the VCS One agent package for Sybase

You must remove the agent for Sybase from each client system in the server farm.

To remove the agent for Sybase from an client system

- Type the following command on each client system to remove the agent. Answer prompts accordingly.

AIX	# installp -u VRTSvcssy.rte
HP-UX	# swremove VRTSvcssy
Linux	# rpm -e VRTSvcssy
Solaris	# pkgrm VRTSvcssy

Removing the agent type definition from the Policy Master system

After you remove the agent packages, you can remove the agent type definitions for all the agents for specific agents from the Policy Master system.

To remove the agent type definition from the Policy Master system

1. Navigate to the following directory on the server farm system

   ```
   # cd /opt/VRTS/install
   ```

2. Run the following command to remove the agent type definition from the Policy Master system:

   ```
   # ./installagpack -rmtypes
   ```

3. When the installer prompts, enter the virtual IP address of the Policy Master.
4. Choose whether to remove the type definitions for all the agents or for specific agents. Follow the installer prompts to remove the type definitions.

   You can view installation logs in the /var/VRTS/install/logs directory.

Chapter 4

Configuring VCS One service groups for Sybase

This chapter includes the following topics:

About configuring a service group for Sybase

Configuring the Sybase service group involves creating the Sybase service group, its resources, and defining attribute values for the configured resources. You must have administrator privileges to create and configure a service group.

You can configure VCS One agent for Sybase using the command-line.

Before you configure the service group

Before you configure the Sybase service group, you must:

- Verify that VCS One client is installed and configured on all server farm systems in the server farm where you will configure the service group. Refer to the *Veritas Cluster Server One Installation Guide* for more information.
- Verify that Sybase is installed and configured identically on all server farm systems in the server farm.

See "About installing Sybase in a VCS One environment" on page 19.

- Verify that the Veritas Cluster Server One agent for Sybase is installed on all server farm systems in the server farm.
  See "Before you install the agent for Sybase" on page 27.
- Make sure that the agent resource type definitions are added to the Policy Master database configuration.
  See "Installing the Cluster Server One agent for Sybase" on page 28.

Configuring the service group

You can configure Sybase in a VCS One environment in one of the ways that VCS One supports.

You can configure VCS One agent for Sybase using the command-line. You can modify an existing service group using the VCS One console.

See "Configuring the service group from the command line" on page 36.

See "Modifying the service group configuration" on page 45.

Review the following to configure the service group:

- Sample configuration files and resource dependency graphs of the Sybase service group.
  See "About the sample configurations for Sybase agent" on page 55.
- Resource type and the attribute definitions of the Sybase and SybaseBk agents.

Note: For Solaris 10, if you are configuring a service group for a Sybase instance running in a Solaris container, you must make sure that the ContainerOpts attribute for the agent is set to monitor these Sybase instances running. By default, the attribute is set to monitor these Sybase instances.

See "About the resource type and attribute definitions" on page 49.

Configuring the service group from the command line

A typical VCS One service group to monitor the state of an Sybase instance in a VCS One server farm has the following characteristics:

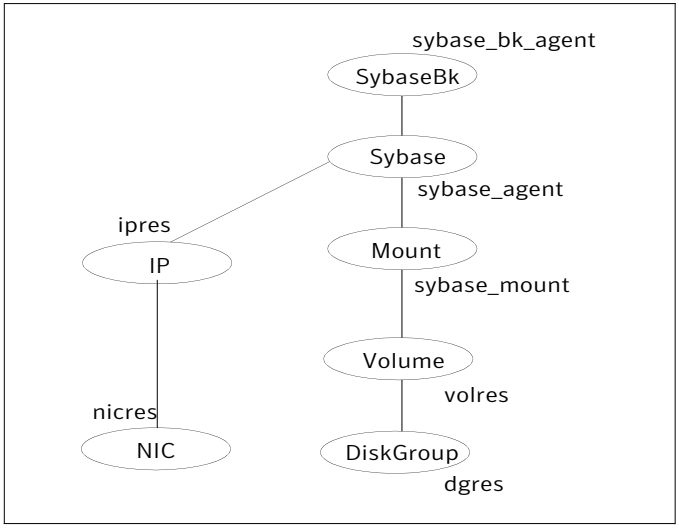
- The shared disk groups and volumes in the server farm are configured as resources of type DiskGroup and Volume respectively.
- The volumes are mounted using the Mount agent.

- The virtual IP address for the service group is configured using the IP and NIC resource types.
- The Sybase and SybaseBk processes are configured as resources of type Sybase and SybaseBk respectively.

You can start the Sybase server after each of these resources is brought online. For more information on the VCS One resources and their attributes, refer to the Veritas Cluster Server Bundled Agents Reference Guide.

Figure 4-1 illustrates the dependency graph for a typical VCS One service group for Sybase.

Figure 4-1 Dependency graph for typical VCS One service group for Sybase



To configure a typical service group using the command-line

1 Create the Sybase service group.

```
# hagrp -add  sybase_group
```

2 Specify the service group SystemList.

```
# hagrp -modify  sybase_group SystemList system_1 0  system_2 1 ...
system_n (n-1)
```

where 0, 1, are the priorities for the systems.

3 Configure the Mount, Volume, and DiskGroup resources.

4 Configure the NIC and IP resources.

SybaseBk requires the device name and the IP address for public network communication.

5 Add Sybase and SybaseBk resources to the service group.

```
# hares -add sybase_resource Sybase sybase_group
# hares -add sybasebk_resource SybaseBk  sybase_group
```

6 Configure the Sybase resource attributes. Review the example commands to configure the required resource attributes.

```
# hares -modify sybase_resource Home SYBASE_HOME
# hares -modify sybase_resource Owner  SYBASE_OWNER
```

See "About the resource type and attribute definitions" on page 49.

7 Configure the SybaseBk resource attributes. Review the example commands to configure the required resource attributes.

```
# hares -modify sybasebk_resource Home SYBASE_HOME
# hares -modify sybasebk_resource Owner  SYBASE_OWNER
```

You may also configure other optional resource attributes.

See "About the resource type and attribute definitions" on page 49.

8 Define the dependencies of resources in the group.

```
# hares -link vol_res dg_res
# hares -link mnt_res vol_res
# hares -link ip_res nic_res
# hares -link sybase_resource mnt_res
# hares -link sybase_resource ip_res
# hares -link sybasebk_resource sybase_res
```

See Figure 4-1 on page 37.

9 Enable the resources in the Sybase service group.

```
# hagrp -enableresources  sybase_group
```

10 Monitor the resources on a system and verify whether the resources are ready to come online.

For example, type the following commands to verify whether the Sybase and SybaseBk resources are ready to come online:

```
# hares -probe sybase_resource -sys system_1
# hares -probe sybasebk_resource -sys  system_1
```

11 Bring the Sybase service group online on the system.

```
# hagrp -online  sybase_group -sys system_1
```

Encrypting passwords

VCS One provides an haencrypt utility to encrypt user passwords. Encrypt passwords before specifying them for Sybase and SybaseBk resource type definition.

To encrypt passwords

1 From the path $CLUSTER_HOME/bin/, run the haencrypt utility.

2 Type the following command.

```
# haencrypt -agent
```

The utility prompts you to enter the password twice. Enter the password and press Return.

```
Enter New Password:
Enter Again:
```

3 The utility encrypts the password and displays the encrypted password.

4 Enter this encrypted password as the value for the attribute.

Copy the encrypted password for future reference.

Setting up detail monitoring for the agent

The VCS One agent for Sybase provides two levels of application monitoring: basic and detail. In basic monitoring, Sybase resource monitors the Sybase daemon processes to verify that they are continuously active.

In detail monitoring, the Sybase resource performs transactions on a test table in the database to ensure that the Sybase server functions properly. The agent

uses this test table for internal purposes. Symantec recommends that you do not perform any other transaction on the test table. The agent uses the script that is defined in the attribute Monscript of the Sybase resource. During detail monitoring, the agent executes the specified script. If the script successfully executes, the agent considers the database available. You can customize the default script according to your configurations.

To activate detail monitoring, the DetailMonitor attribute must be set to a positive integer and User, UPword, Db, and Table attributes must not be empty (""). The attribute Monscript, which contains the path of the detail monitor script, must also exist and must have execute permissions for the root.

Enabling detail monitoring

Perform the following steps to enable detail monitoring on a database.

To enable detail monitoring

1. Freeze the service group to avoid automated actions by VCS One caused by an incomplete reconfiguration:

   ```
   # hagrp -freeze service_group
   ```

   See "Configuring Sybase for detail monitoring" on page 23.

2. Enable detail monitoring for Sybase.

   ```
   # hares -modify Sybase_resource DetailMonitor 1
   # hares -modify Sybase_resource User user
   # hares -modify Sybase_resource UPword encrypted password
   # hares -modify Sybase_resource Db database_name
   # hares -modify Sybase_resource Table table_name
   # hares -modify Sybase_resource Monscript
   "/opt/VRTSagents/ha/bin/Sybase/SqlTest.pl"
   ```

3. Unfreeze the service group.

   ```
   # hagrp -unfreeze service_group
   ```

Note: If detail monitoring is configured and the database is full, the SQL queries take considerable time to commit the results. In such a case, the monitor routine for the agent fails and attempts to fail over the service group. This issue is not encountered if detail monitoring is not configured.

Disabling detail monitoring

Perform the following steps to disable detail monitoring.

To disable detail monitoring

1. Freeze the service group to avoid automated actions by VCS One caused by an incomplete reconfiguration:

```
# hagrp -freeze service_group
```

2. Enable detail monitoring for Sybase.

```
# hares -modify Sybase_resource DetailMonitor 0
```

3. Unfreeze the service group.

```
# hagrp -unfreeze service_group
```

Chapter 5

Administering VCS One service groups for Sybase

This chapter includes the following topics:

About administering VCS One service groups

You can administer service groups in VCS One using the VCS One console or command-line. Review the procedures to administer the service groups using the VCS One console.

See *Veritas Cluster Server One User's Guide.*.

Bringing the service group online

Perform the following steps to bring the service group online.

To bring a service group online from the console

1. In the Cluster Server One console, locate the service group that you want to bring online.
2. In the right pane, under **All Service Groups**, click the service group that you want to bring online.

3 In the right pane, from the **Operations** menu, click **Online**.

The **Online Service Group** dialog box is displayed.

4 In the **Online Service Group** dialog box, select the system where the service group must be brought online.

To bring the service group online on any system that is listed in the service group's SystemList attribute, select **Anywhere**.

In case of parallel service groups, the **All Systems** option replaces the **Anywhere** option.

5 Select the **Evacuate lower priority service group** check box, if you want to evacuate other low priority service groups on the specified system.

Note that if the total load of all service groups exceeds the system capacity, then the low priority service groups are evacuated.

6 In the **Online Service Group** dialog box, click **OK**.

To bring a service group online from the command line

- Do one of the following:

To bring a service group online on a specific system, type:

```
# hagrp -online [-ejectlowpri | -propagate] group -sys system\
[-user user@domain] [-domaintype domaintype]
```

To bring the service group online on any system in the SystemList, type:

```
# hagrp -online [-ejectlowpri][-nointent] group -any\
[-user user@domain] [-domaintype domaintype]
```

Switching the service group

The process of switching a service group involves taking it offline on its current system and bringing it online on another system.

To switch a service group from the console

1 In the Cluster Server One console, locate the service group that you want to switch.

2 In the right pane, under **All Service Groups**, click the service group that you want to switch.

3 In the right pane, from the **Operations** menu, click **Switch**.

The **Switch Service Group** dialog box is displayed.

4 In the **Switch Service Group** dialog box, select the system where you want the service group to be switched.

   To switch the service group to any system in the *SystemList*, select **Anywhere**.

   In case of parallel service groups, the **All Systems** option replaces the **Anywhere** option.

5 Select the **Evacuate lower priority service groups** check box, if you want to evacuate other low priority service groups on the specified system.

   Note that if the total load of all service groups exceeds the system capacity, then the low priority service groups are evacuated.

6 In the **Switch Service Group** dialog box, click **OK**.

Modifying the service group configuration

You can dynamically configure the Sybase using the Cluster Server One console or the command-line interface.

Refer to the *Veritas Cluster Server One User's Guide*. for more information.

To modify a service group using the VCS One console

1 In the Cluster Server One console, locate the service group that you want to modify.

2 In the right pane, under **All Service Groups**, select the service group that you want to modify.

3 In the right pane, from the **Configuration** menu, click **Modify Service Group**.

   The **Service Group Configuration Wizard** is displayed.

   The **Service Group Configuration Wizard** is used for adding and modifying a service group.

4 Follow the service group wizard instructions and make modifications as per your configuration.

   Refer to the *Veritas Cluster Server One User's Guide*. for more information.

Chapter 6

Troubleshooting Cluster Server One agent for Sybase

This chapter includes the following topics:

About troubleshooting Cluster Server One agent for Sybase

Review the description of the error messages for the following agents and the possible solutions:

- Sybase agent
- Sybase Bk agent

Error messages

`Monitor procedure %s did not exit. Return value is %s`

The in-depth monitor procedure specified using the [Monscript] attribute did not exit. The return code is as reported by the waitpid() system call for the execution of in-depth monitor script. For additional information, refer to man page for waitpid() system call.

Verify for correctness, the in-depth monitor procedure specified using [Monscript] attribute. Fix the in-depth monitor procedure and ensure that it exits with correct value as understood by the VCS One agent framework.

Refer to the Veritas Cluster Server One Agent Developer's Guide for possible values that a script based monitor entry point (agent function) can return.

```
Setting cookie for proc = %s, PID = %s
```

The specified process is identified to be running and its process identifier (PID) is cached in the agent in the form of an internal cookie.

No action needed. This is an informational message.

Viewing the agent log

The VCS One agent for Sybase logs messages to the following files:

```
/var/VRTSvcsone/log/engine_A.log
```

```
/var/VRTSvcsone/log/vcsoneclientd_A.log
```

```
/var/VRTSvcsone/log/Sybase_A.log
```

```
/var/VRTSvcsone/log/SybaseBk_A.log
```

Appendix A

Resource type definitions

This appendix includes the following topics:

About the resource type and attribute definitions

The resource type represents the VCS One configuration definition of the agent and specifies how the agent is defined in the configuration file main.xml. The Attribute Definitions explain the attributes associated with the agent. The Required attributes explain the attributes that must be configured for the agent to function properly.

Refer to the sample SybaseTypes.platform.xml files in /etc/VRTSagents/ha/conf/Sybase directory.

Sybase resource type

The VCS One agent for Sybase is represented by the Sybase resource type in VCS One.

Attribute definitions for Sybase

The Sybase resource has several required and optional attributes.

Table A-1 lists the required attributes.

Table A-1 Required attributes

Required Attributes	Definition
Server	The $DSQUERY ASE name. Only one server must be configured in a Sybase service group. Type and dimension: string-scalar
Owner	Sybase user as the defined owner of executables and database files in any of the sources (such as NIS+, /etc/hosts, and so on) specified in the /etc/nsswitch.conf file for passwd entry. The Sybase executables and database files are accessed in the context of this user. Type and dimension: string-scalar See "System user for Sybase home directory" on page 21.
Home	The $SYBASE path to Sybase binaries and configuration files. Type and dimension: string-scalar
Version	Version of Sybase ASE. Type and dimension: string-scalar
SA	Sybase database administrator. This attribute is required to connect to the ASE for shutdown. Type and dimension: string-scalar
SApswd	Encrypted password for Sybase database administrator. This password is required to connect to the ASE for shutdown. Type and dimension: string-scalar See "Encrypting passwords" on page 39. **Note:** You need not specify a value for this attribute if the SA user does not require a password.

Table A-2 lists the optional attributes.

Table A-2 Optional attributes

Optional Attributes	Definition
AgentDirectory	This attribute is for internal use only. Type and dimension: static-string Specifies the location of the binaries, scripts, and other files related to the agent for Sybase. Symantec recommends not to modify the value of this attribute.
DetailMonitor	Specifies whether the Sybase server is monitored in detail. Value 1 indicates that the resource monitors the Sybase server in detail. Value 0 denotes it does not. Default is 0. Type and dimension: int-scalar
User	The database user, in the context of which, the transactions are performed on the database. Type and dimension: string-scalar **Note:** You must specify a value for this attribute if DetailMonitor is set to a non-zero value.
UPword	Encrypted password for the database user. See "Encrypting passwords" on page 39. Type and dimension: string-scalar **Note:** You must specify a value for this attribute if DetailMonitor is set to a non-zero value. However, you need not specify a value for this attribute if the database user does not require a password.
Db	Name of the database used for detailed monitoring. The table used by the detail monitor script resides in this database. Type and dimension: string-scalar **Note:** You must specify a value for this attribute if DetailMonitor is set to a non-zero value.
Table	Name of the table on which the detail monitoring script performs the transactions. Type and dimension: string-scalar **Note:** You must specify a value for this attribute if DetailMonitor is set to a non-zero value.

Table A-2 Optional attributes *(continued)*

Optional Attributes	Definition
Monscript	The path to the detail monitor script; the default value for this attribute is the path for the script, SqlTest.pl, provided with the agent. Type and dimension: string-scalar **Note:** You must specify a value for this attribute if DetailMonitor is set to a non-zero value.
ContainerOpts (Only Solaris 10)	Container options for Sybase instances running in the context of Solaris containers (zones or projects). This attribute has the following keys, which can take values 0 or 1: ■ RunInContainer (RIC) Set the key value as 1 for the Sybase agent to monitor Sybase instances running in the context of Solaris container. Set the key value as 0 if you do not want to run the Sybase resource in the context of Solaris container. Default is 1. ■ PassCInfo (PCI) Set the key value as 1 for the Sybase resource to get the container information defined in the VCS One service group's ContainerInfo attribute. Set the key value as 0 if you do not want to get the container information. Default is 1. ■ PassLoadInfo (PLI) Set the key value as 1 for the Sybase resource to get the load dimensions defined in the VCS One service group's Load attribute. Set the key value as 0 if you do not want to get the load information. Default is 0. See *Veritas Cluster Server One User's Guide.* Type and dimension: static-assoc-int

SybaseBk resource type

The VCS One agent for Sybase is represented by the SybaseBk resource type in VCS One.

Attribute definitions for SybaseBk

The SybaseBk resource has several required and optional attributes.

Table A-3 lists the required attributes for SybaseBk resource.

Table A-3 Required attributes

Attributes	Definition
Server	The $DSQUERY Backup server name. Type and dimension: string-scalar
Owner	Sybase user as the defined owner of executables and database files in any of the sources (such as NIS+, /etc/hosts, and so on) specified in the /etc/nsswitch.conf file for passwd entry. The Sybase executables and database files are accessed in the context of this user. Type and dimension: string-scalar
Home	The $SYBASE path to Sybase binaries and configuration files. Type and dimension: string-scalar
Version	Version of Sybase Backup Server. Type and dimension: string-scalar
Backupserver	The $BACKUP SYBASE Backup Server name. Type and dimension: string-scalar
SA	Sybase database administrator. This attribute is required to connect to the ASE for shutdown. Type and dimension: string-scalar
SApswd	Encrypted password of Sybase database administrator. This password is required to connect to the ASE for shutdown. Type and dimension: string-scalar See "Encrypting passwords" on page 39. **Note:** You need not specify a value for this attribute if the SA user does not require a password.

Table A-2 lists the optional attributes.

Table A-4 Optional attributes

Optional Attributes	Definition
AgentDirectory	This attribute is for internal use only. Type and dimension: static-string Specifies the location of the binaries, scripts, and other files related to the agent for Sybase. Symantec recommends not to modify the value of this attribute.
ContainerOpts (Only Solaris 10)	Container options for SybaseBk instances running in the context of Solaris containers (zones or projects). This attribute has the following keys, which can take values 0 or 1: ■ RunInContainer (RIC) Set the key value as 1 for the SybaseBk agent to monitor Sybase instances running in the context of Solaris container. Set the key value as 0 if you do not want to run the Sybase resource in the context of Solaris container. Default is 1. ■ PassCInfo (PCI) Set the key value as 1 for the SybaseBk resource to get the container information defined in the VCS One service group's ContainerInfo attribute. Set the key value as 0 if you do not want to get the container information. Default is 1. ■ PassLoadInfo (PLI) Set the key value as 1 for the SybaseBk resource to get the load dimensions defined in the VCS One service group's Load attribute. Set the key value as 0 if you do not want to get the load information. Default is 0. See *Veritas Cluster Server One User's Guide.* Type and dimension: static-assoc-int

Appendix B

Sample Configurations

This appendix includes the following topics:

About the sample configurations for Sybase agent

The sample configuration include descriptions for typical service groups that are configured to monitor the state of Sybase in a VCS One server farm.

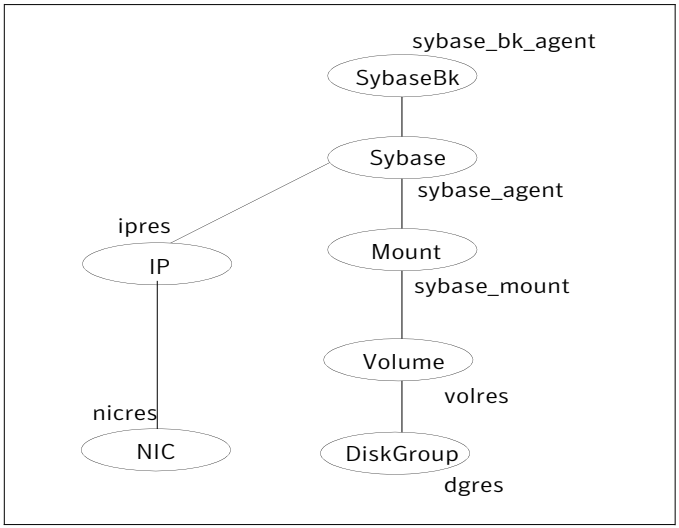
The sample dependency graphs depict the resource types, resources, and resource dependencies within the service group. Review these dependencies carefully before configuring the agent.

For more information about VCS One resource types, see the *Veritas Cluster Server One Bundled Agents Reference Guide*.

Sample Sybase instance configuration

Figure B-1 describes a typical service group configured to monitor the state of a Sybase instance in a VCS One server farm

Figure B-1 Dependency graph



The dependency graph depicts a single Sybase instance configuration. The configuration contains a disk group with a single volume. The volume is monitored using a Volume resource and mounted using a Mount resource. The Mount resource requires Volume resource, which in turn requires the DiskGroup resource. The service group IP address for Sybase server is monitored using the IP and NIC resource types. The Sybase server can be started after each of these resources are brought online. The Backup Server is started after the Sybase SQL Server is online.

Note: If your configuration does not use Veritas Volume Manager, use the DiskReservation resource type to configure shared storage instead of the DiskGroup and Volume resource types.

Resource dependency for Sybase configured in Solaris zones

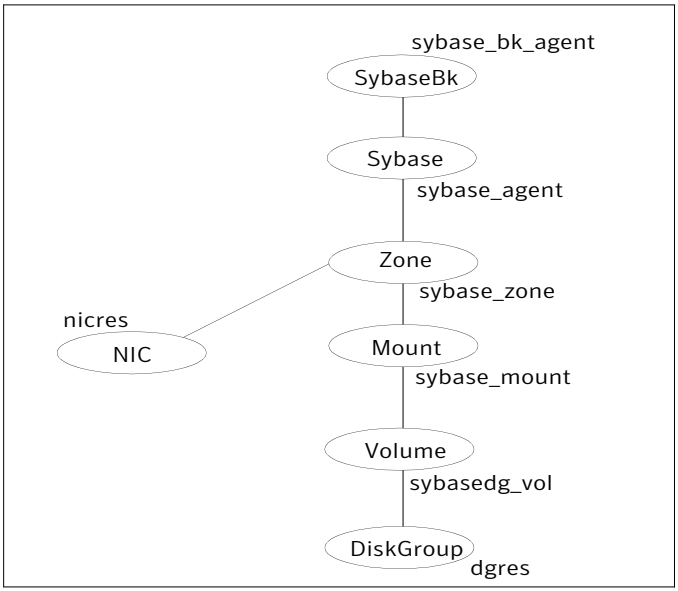
The following examples describe a typical service group that is configured to monitor the state of a Sybase instance that is configured in a Solaris zone.

Zone root on local disk

If the root file system of a zone is on the local disk of each node, the file system is mounted when the system is booted. Hence, the service group does not need to have separate DiskGroup and Volume resources for the zone.

Figure B-2 shows a configuration in which zone root is on the local disk.

Figure B-2 Zone root on local disk

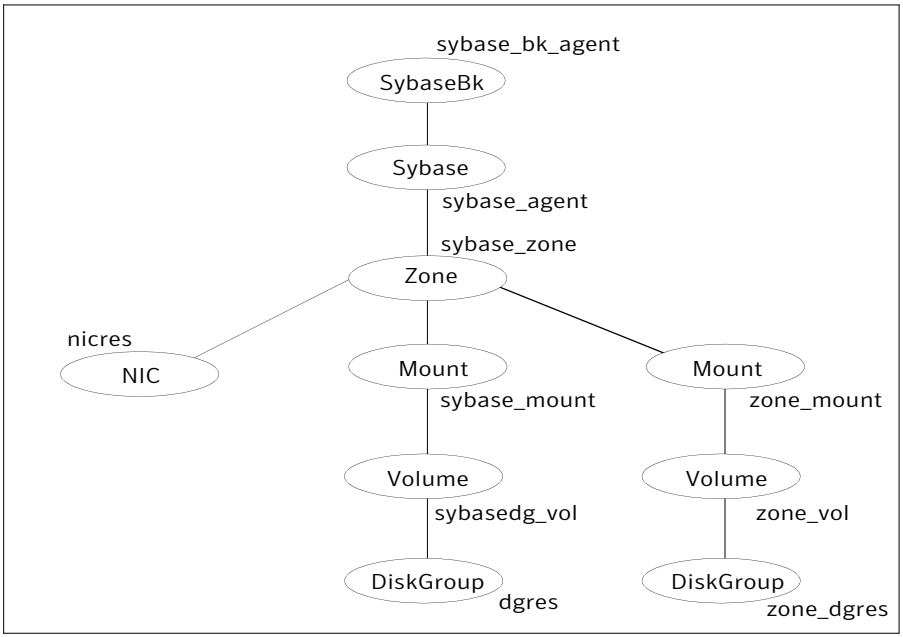


Zone root on shared disk

If the root file system of a zone is on a shared disk, VCS One should mount the file system. Hence, separate DiskGroup and Volume resources are required for the zone.

Figure B-3 shows a configuration in which zone root is on the shared disk.

Figure B-3 Zone root on shared disk



Index

T

U