Veritas Cluster Server One Agent for DB2 Installation and Configuration Guide

AIX

5.0

March 2009

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

Agent version: 5.0.0

Document version: 5.0

Legal Notice

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

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

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

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

Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014

http://www.symantec.com

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

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/techsupp/

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

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.

1

Introducing the Veritas Cluster Server One Agent for DB2

This chapter includes the following topics:

About the Veritas Cluster Server One Agent for DB2

The Veritas Cluster Server One Agent for DB2, version 5.0, for DB2 UDB is a high availability solution for the relational database management system.

How Veritas Cluster Server One Agent for DB2 makes DB2 highly available

The agent monitors DB2 UDB database processes at the partition level. If the system fails, the agent detects the failure and takes the applicable database partition offline. VCS One moves the failed instances to another client system in the server farm, where the agent brings the database partition or partitions online.

The agent performs different levels of monitoring and different actions, which you can configure. You can also configure many of the actions that the agent can perform.

Supported software

The Veritas Cluster Server One Agent for DB2, version 5.0, supports the DB2 Universal Database Enterprise Server Edition (ESE).

For the ESE multi-partition instance, it supports both of the following configurations:

- Symmetric Multiprocessing (SMP) hardware configuration
- Massively Parallel Processing (MPP) hardware configuration

Note: Contact Symantec support for information on installing and configuring an MPP hardware configuration.

The agent for DB2 ESE must support the following platforms for single and multi-partition instances.

Table 1-1 Supported operating systems and versions

Operating system	DB2 UDB version
AIX 5.3 or later	9.5
AIX 6.1	9.5

The memory requirements vary for different versions of DB2 being used. Check the relevant IBM DB2 guide for information about memory requirements.

Agent functions

The agent can perform different operations or functions on the database. These functions are online, offline, monitor, clean, info, and action. With the action agent function, you can add custom actions for the agent.

For information on how to define custom actions, refer to the *Veritas Cluster Server One Agent Developer's Guide*.

Online agent function

The agent uses the db2gcf program to start a DB2 instance or database partition. The command is:

```
su $DB2InstOwner -c "$InstHome/sqllib/bin/db2gcf -u -i
    $DB2InstOwner -p $nodenum
```

Offline agent function

The agent uses the db2gcf program to stop a DB2 database partition. For a database with only one partition, it stops the instance. The command is:

```
su $DB2InstOwner -c "$InstHome/sqllib/bin/db2gcf -d -i
    $DB2InstOwner -p $nodenum
```

Monitor agent function

The agent executes the `db2gcf -s -i $DB2InstOwner -p $nodenum` command to check the status of the database partition or client system number. If the exit status of the `db2gcf` command is 0, the monitor returns the exit code 110. Otherwise, the monitor returns an exit code of 100 and the resource is taken offline. The agent then restarts or fails over the resource. This action depends on other type-independent attributes, such as RestartLimit or ToleranceLimit.

Set the IndepthMonitor attribute to 1 for in-depth monitoring. The agent looks for the monitor_custom_$db2instance_$nodenum file in the /opt/VRTSagents/ha/bin/Db2udb directory. It executes this customized in-depth monitor file, if the file exists and is executable. You can find samples of custom monitor scripts in the /etc/VRTSagents/ha/conf/sample_db2udb directory.

If the custom monitor has any errors or problems, it checks the value of the WarnOnlyIfDBQueryFailed attribute of the Db2udb agent. If you have a db2error.dat file in the /opt/VRTSagents/ha/bin/Db2udb directory, the agent checks this file, and handles the error according to the error configuration.

If you set the WarnOnlyIfDBQueryFailed attribute to 1 (its default), and you have configured the Notifier resource, the agent performs the following actions:

- Sends a notification
- Returns the exit code 110

If you set the WarnOnlyIfDBQueryFailed attribute to 0, it performs error handling in the db2error.dat file. Note that the file needs to exist to perform error handling. If it does not exist, it returns the exit code 100, which is the default.

Clean agent function

The agent uses the db2gcf program to kill a DB2 database partition. The command is:

```
su $DB2InstOwner -c "$InstHome/sqllib/bin/db2gcf -k -i
    $DB2InstOwner -p $nodenum"
```

Info agent function

The agent supports the info function, which provides static and dynamic information about the database partition and its critical processes.

For more information about the Info agent function, see the following guides:

- *Veritas Cluster Server One User's Guide*
- *Veritas Cluster Server One Agent Developer's Guide*

Action agent function

The agent for DB2 supports the action function, which enables you to perform predefined actions or custom actions on a resource. To perform an action on a resource, type the following command:

```
# hares -action res token [-actionargs arg1 ...] \
[-sys system] [-user user@domain] [-domaintype domaintype]
```

The agent supports the following predefined actions:

- The VRTS_GetInstanceName token retrieves the DB2 instance name of the configured Db2udb resource.
- The VRTS_GetRunningServices token retrieves the list of processes that the agent monitors for the Db2udb resource.

For example:

```
# hares -action db2udb1 VRTS_GetInstanceName -sys systemName

VCS NOTICE V-16-13323 Resource (db2udb0): action
(VRTS_GetInstanceName) completed successfully. Output is:

db2inst1

# hares -action db2udb0 VRTS_GetRunningServices -sys systemName

VCS NOTICE V-16-13323 Resource (db2udb0): action
(VRTS_GetRunningServices) completed successfully. Output is:
```

```
PARTITION: 0

PID TTY TIME CMD

9800 ? 0:06 db2sysc
```

Running the info agent function to reteive database information

You can run the info agent function to return database information. In this example, the info agent function retrieves the database information.

To retrieve database information

1. Specify the periodic interval in seconds that the info agent function is invoked. The default value of 0 means info agent function is not invoked.

   ```
   # hatype -modify Db2udb InfoInterval 300
   ```

   In this command, Db2udb is the name of the DB2 resource type. InfoInterval 300 is the duration (in seconds) after which the info agent function executes the info script. The script gets the processes' information that the agent monitors.

2. Show the requested ResourceInfo value. The following example output shows the processes that the agent monitors for the DB2 resource.

   Note that ResourceInfo refreshes every 300 seconds (five minutes), since you set the InfoInterval to 300 in the previous step.

   ```
   # hares -value db2udb1 ResourceInfo
   State Valid
   Msg
   PARTITION: 0
       PID    TTY  TIME CMD
     413924    -   0:00 db2sysc

   TS Fri Jan 14 18:11:52 2005
   ```

Typical DB2 configuration in a VCS One server farm

A typical DB2 configuation in a VCS One server farm has the following characteristics:

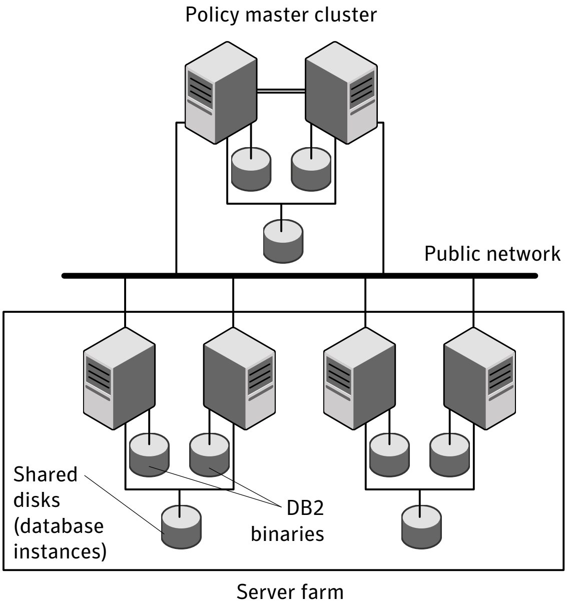
- The Policy Master runs on two nodes in the server farm.
- The VCS One client is installed on all server farm systems.

- The DB2 database instance is installed on shared storage.
- The DB2 binaries are installed locally on both server farm systems.
- The Veritas Cluster Server One Agent for DB2 is installed on both server farm systems.

In the case of the non-MPP configuration, an instance is online on only one system at a time. The other system is the failover system.

Figure 1-1 shows a DB2 installation with a non-MPP configuration.

Figure 1-1 DB2 installation with a non-MPP configuration



Road map for setting up DB2 UDB in a VCS One environment

Review the following tasks and information:

- Check the supported software.
- Review the agent functions.
- Check the agent requirements.
- Install and set up DB2.

- Install the Veritas Cluster Server One Agent for DB2.
- Configure the service groups for the Veritas Cluster Server One Agent for DB2.
- Optionally, configure in-depth monitoring and any automated actions.
- Bring the service group online.

Installing and configuring DB2

This chapter includes the following topics:

- VCS One requirements for installing DB2
- Installing DB2 in a VCS One environment
- Setting up the DB2 configuration

VCS One requirements for installing DB2

Review the preparations to install DB2 UDB.

Preparing to install DB2 UDB non-MPP versions

Review the following list:

- Verify that VCS One client is installed on Policy Master or on all client systems.
- Verify that all client systems in the server farm have adequate resources to run DB2 and VCS One.
- Verify that the network supports the TCP/IP protocol.
- Make sure that you meet the VCS One requirements to install.
- Define DB2 UDB user and group accounts.
  See "Defining user and group accounts" on page 20.
  For your particular version of DB2 UDB, refer to the appropriate DB2 UDB guide.
- Install the DB2 UDB system binaries locally.

- Install the DB2 UDB database instances on shared storage.
- Install and configure VCS One version 5.0 on all client systems in the server farm. For installation instructions, refer to the *Veritas Cluster Server One Installation Guide*.

Creating the file systems for non-MPP instances

To create a file system for non-MPP instances, you first create a disk group on the physically shared disk. You then create a volume of sufficient size within the disk group.

To create a file system for non-MPP instances

1. Create a disk group on the shared disk. List the disks using the `lsdev -Cc disk` command. In this case the group consists of one disk, hdisk5. For example:

   ```
   # vxdg init db2db_dg hdisk5
   ```

   Deport and import the disk group:

   ```
   # vxdg deport db2db_dg
   # vxdg import db2db_dg
   ```

2. Create a volume of three GB using the `vxassist` command:

   ```
   # vxassist -g db2db_dg make db2db_vol 3g
   ```

3. Create the file system:

   ```
   # mkfs -V vxfs -o largefiles /dev/vx/dsk/db2db_dg/db2db_vol
   ```

4. Create the mount point directory and mount the file system. Make sure that the mount point exists on all client systems in the cluster on the local file system—not on shared storage.

   ```
   # mkdir /db2_mnt/db2inst1
   # mount -V vxfs /dev/vx/dsk/db2db_dg/db2db_vol \
     /db2_mnt/db2inst1
   ```

Defining user and group accounts

Before you install DB2 UDB binaries and create instances, you must define DB2 UDB user and group accounts for each instance on each system.

Note the following requirements:

- The IDs for DB2 users and groups must be exactly the same across all server farm client systems.
- The DB2 instance owner's home directory must exist locally on each client system. This directory is the mount point that the DB2 instance uses. The database that you want to mount must be on shared storage. Create the mount point directory locally on each client system, if it does not already exist.
- All DB2 user accounts must exist on the local systems. Symantec does not recommend the use of NIS or NIS+ for users, because these services are not highly available. If their service is interrupted, VCS One may not be able to work correctly.

Creating user group accounts

Three user group accounts are required on each client system in the server farm.

To create the group accounts on each client system in the server farm on AIX

1. Create a group for the DB2 UDB instance owner. For example, enter:

   ```
   # mkgroup id=999 db2iadm1
   ```

2. Create a group for the user to execute fenced user-defined functions (UDFs) or store procedures. For example, enter:

   ```
   # mkgroup id=998 db2fadm1
   ```

3. Create a group for the database administration server. For example, enter:

   ```
   # mkgroup id=997 db2asgrp
   ```

Adding user accounts

Create the user accounts on each client system in the server farm. This example shows how to create the db2inst1 user. The db2inst1 user is the DB2 UDB instance owner. The instance's home directory is also the mount point, /db2_mnt/db2inst1. The file system that hosts the DB2 UDB instance home directory on shared storage uses this mount point. The DB2 UDB instance home directory must exist on every client system. For example:

```
# mkuser id=1004 pgrp=db2iadm1 groups=db2iadm1 home=/ \
db2_mnt/db2inst1 db2inst1
```

The following examples show how to create user accounts for db2fenc1 and db2as. These users' home directories are under /home in the local file system on each client system.

```
# mkuser id=1003 pgrp=db2fadm1 groups=db2fadm1 home=/home/ \
db2fenc1 db2fenc1
# mkuser id=1002 pgrp=db2asgrp groups=db2asgrp home=/home/ \
    db2as db2as
```

Installing DB2 in a VCS One environment

For installing DB2 in a VCS One environment, Symantec Corporation recommends that you follow the installation procedure in the relevant IBM DB2 UDB guide.

Install binaries on local disks of each node, and the database instances on shared storage, accessible by each cluster node.

To install DB2 in VCS One environment

1. Set shared memory parameters. Refer to the relevant IBM DB2 UDB guide to make sure that memory requirements are met.
2. Install the binaries. Install the DB2 UDB system binaries on local disks on each node (mirrored disks are recommended) not on shared storage. You can use IBM's db2setup tool.
3. Install the DB2 license. Install the DB2 license on each client system. For example, enter:

   ```
   # /opt/IBM/db2/V8.1/adm/db2licm -a db2ese.lic
   ```

4. Install the instances. Install the database instances on the shared storage only on the one node where the instance's home directory is currently mounted. You can choose to install single-partition instance or multi-partition instance. You can use IBM's db2setup tool.

   Keep in mind the following when you install:

   - When you use the db2setup, do not select the option to Auto start DB2 instance at system boot in the DB2 Instance Properties window. Note that this option does not exist on all DB2 versions. VCS One needs to bring up the resources for the DB2 instances in a specific order before it brings the instance online.
   - The instance's home directory is a mount point on the local system.

Setting up the DB2 configuration

Use the following procedures to configure DB2 UDB in a VCS One environment.

You need to do the following tasks:

- Check /etc/services.
  See "Checking /etc/services" on page 23.
- Create $DB2InstHome/.rhosts.
  See "Creating $DB2InstHome/.rhosts" on page 24.
- Modify the $DB2InstHome/sqllib/db2nodes.cfg file for DB2.
  See "Modifying the $DB2InstHome/sqllib/db2nodes.cfg file" on page 24.
- Confirm the setup of the DB2 installation.
  See "Checking /etc/services" on page 23.

Checking /etc/services

On each system in the cluster, use the `more` command to check the file /etc/services.

Remember to perform the following:

- Make sure each partition has a port number assigned. The number of reserved ports depends on the number of partitions.
- Make sure that no other services use the ports. Manually assign new numbers if necessary.
- Make sure all systems in the cluster have the same entries in the /etc/services file.

The following is an example for two DB2 instances: db2inst1 and db2inst2. Both instances have two partitions each. Each instance requires two ports plus one port per partition, hence four lines per instance.

```
# more /etc/services
DB2_db2inst1      60000/tcp
DB2_db2inst1_1    60001/tcp
DB2_db2inst1_2    60002/tcp
DB2_db2inst1_END  60003/tcp
DB2_db2inst2      60004/tcp
DB2_db2inst2_1    60005/tcp
DB2_db2inst2_2    60006/tcp
DB2_db2inst2_END  60007/tcp
```

Inspect the file and verify that no duplicate port numbers exist.

Creating $DB2InstHome/.rhosts

On each system, create a file named $DB2InstHome/.rhosts, and place a "+" character within it. This file permits a system to access the database without the use of a password.

If security is a concern, put the hostname and user ID inside the .rhosts file, as shown in the following examples:

```
dbmach01   db2inst1
dbmach02   db2inst1
dbmach03   db2inst1
dbmach04   db2inst1
```

Or

```
+   db2inst1
```

With the `rsh` *`system_name`* command, you can test password free remote logon. From one system in the cluster to another, the command tests that you can remotely log on with the DB2 instance (for example, db2inst1) account. You should not be prompted for a password. Test this command from each system in the cluster to all other systems.

Modifying the $DB2InstHome/sqllib/db2nodes.cfg file

DB2 uses the $DB2InstHome/sqllib/db2nodes.cfg file during failover from one node to another.

To modify the $DB2InstHome/sqllib/db2nodes.cfg file for non-MPP versions

1. Open the $DB2InstHome/sqllib/db2nodes.cfg file.
2. Create an entry for each database partition.
3. Assign the virtual IP address as the hostname, for example for this step and the previous step:

   ```
   0 virtualhostname 0
   1 virtualhostname 1
   ```

   Note that the *virtualhostname* corresponds to the virtual IP address in the /etc/hosts file. Make sure that the virtual IP address is up and works.

Confirming the DB2 installation

On the host where the shared file system is mounted, check whether you can start and stop each instance. Do this procedure to verify the DB2 installation.

To check if a DB2 instance can start and stop

1. Log on as the instance owner:

   ```
   # su - db2inst1
   ```

2. Attempt to start the instance:

   ```
   $ db2start
   ```

   DB2 should start on the partitions in the db2nodes.cfg file. If DB2 does not start, check the error codes.

3. Assuming that the previous command is successful, stop the instance:

   ```
   $ db2stop
   ```

4. If the application does not stop correctly on each node, check for configuration errors. Review the DB2 UDB documentation for error codes.

5. Create a database.

   ```
   $ db2 create database dbname
   ```

6. List the database directory

   ```
   $ db2 list database directory
   ```

To check the rest of the DB2 configuration in the cluster

1. For each node in the VCS One cluster, import the disk group and start all the volumes in the disk group.
2. Mount the file system for the volume that contains the DB2 instance and database.
3. Unmount and deport the disk group.
4. Repeat this procedure for each node in the cluster.

3

Installing and removing the Veritas Cluster Server One Agent for DB2

This chapter includes the following topics:

Before you install or upgrade the Veritas Cluster Server One Agent for DB2

Meet the following prerequisites to install the Veritas Cluster Server One Agent for DB2:

- 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 DB2 is installed on any of the client systems, uninstall it.

Installing the Veritas Cluster Server One agent for DB2

You must install the VCS One agent for DB2 on all the client systems of the server farm that will host the DB2 service group. You can install the VCS One agent for DB2 using the installagpack program. The installagpack program installs the VCS One agent for DB2 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

Adding the agent resource type definitions

Note: The installagpack program supports only the -addtypes, -rmtypes, -responsefile, and -rsh options. Symantec recommends that you do not use any of the other options from the `installagpack` command help output.

Installing the agent packages

You can add the agent packages on one or more client systems 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`

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 agent 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`

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 Veritas Cluster Server One Agent for DB2

To disable the Veritas Cluster Server One Agent for DB2, you must change the agent for DB2 service group to an OFFLINE state. You can stop the application completely or switch the agent to another system.

To disable the agent

1. To remove a system from the service group's SystemList, check if the service group is online:

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

2. If the service group is online, take it offline. Use one of the following commands:

   - To take the service group offline on one client system and online it on another client system, you can use the -switch option:

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

   - To take the service group offline without bringing it online on any other client system in the server farm, enter:

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

3. Stop the agent on the client system:

   ```
   # haagent -stop Db2udb -sys system_name
   ```

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

   You can also use the `ps` command to confirm the agent is stopped.

5. You can now remove the service group, the resource type, or both from the VCS One configuration after disabling the agent on all client systems.

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

Removing the Veritas Cluster Server One Agent for DB2

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 DB2. 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.

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

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
   ```

3. Start the uninstallagpack program.

   ```
   # ./uninstallagpack
   ```

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

   You can view installation logs in the /var/tmp/uninstallagpack-*uniquestring*/ directory.

Removing the VCS One agent package for DB2

You must remove the VCS One agent for DB2 from each client system in the server farm.

To remove the VCS One agent for DB2 from a client system

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

AIX

```
# installp -u VRTSvcsdb
```

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 the logs in the /var/tmp/installagpack-*uniquestring*/ directory.

4

Configuring VCS One service groups for Veritas Cluster Server One Agent for DB2

This chapter includes the following topics:

About configuring service groups

Configuring the DB2 service group involves creating the DB2 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 a VCS One service group for DB2 using the command-line.

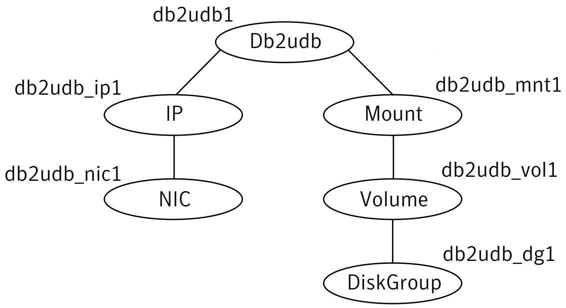
About DB2 configurations in VCS One

You can configure DB2 service groups in non-MPP configurations.

Non-MPP configuration service groups

Figure 4-1 illustrates the dependencies among the resources that are configured for a non-MPP DB2 instance resource group.

Figure 4-1 Dependency graph for a DB2udb resource



This configuration shows a service group for a Db2udb resource. The db2udb1 resource (the database) requires the IP resource and the Mount resource. The service group IP address for the DB2 server is configured using the IP resource (db2udb_ip1) and the NIC resource (db2udb_nic1). The mount resource (db2udb_mnt1) requires the Volume resource (db2udb_vol1), which in turn requires the DiskGroup resource (db2udb_dg1). You can start the service group after each of these resources is available.

Before you configure the service group

Before you configure the agent for DB2 service group, you must:

- Verify that VCS One client is installed and configured on all client 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 DB2 UDB is installed and configured identically on all client systems in the server farm.
- Verify that the Veritas Cluster Server One Agent for DB2 is installed on all client systems in the server farm.
- Make sure that the agent resource type definitions are added to the Policy Master database configuration.

About configuring Veritas Cluster Server One Agent for DB2

You can configure DB2 in a VCS One environment in one of the ways that VCS One supports.

You can configure VCS One agent for DB2 using the command-line. You can modify an existing service group using the VCS One console.

Configuring the VCS One service group for DB2 using the command-line

A typical VCS One service group to monitor the state of an agent for DB2 instance in a VCS One server farm has the following characteristics:

- Configure the shared disk groups and volumes in the server farm as DiskGroup and Volume resources.
- Mount the volumes using a Mount resouce.
- Configure the virtual IP address for the service group using the IP resource and the NIC resource.

You can start the agent for DB2 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 One Bundled Agents Reference Guide.

To configure a typical service group using the command-line

1. Create the agent for DB2 service group.

   ```
   # hagrp -add  db2udb_group
   ```

2. Specify the service group SystemList.

   ```
   # hagrp -modify  db2udb_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.
5. Configure the Db2udb resource attributes. Review the example commands to configure the required resource attributes.

   ```
   # hares -modify  db2udb_resource DB2InstHome INSTANCE_HOME
   # hares -modify db2udb_resource DB2InstOwner  INSTANCE_OWNER
   ```

   You can also configure other optional resource attributes.

6. 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 db2udb_resource
    mnt_res
# hares -link db2udb_resource
    ip_res
```

7. Enable the resources in the DB2 service group.

```
# hagrp -enableresources  db2udb_group
```

8. 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 DB2 resources are ready to come online:

```
# hares -probe  db2udb_resource -sys system_1
```

9. Bring the DB2 service group online on the system.

```
# hagrp -online  db2udb_group -sys system_1
```

Setting up in-depth monitoring of a DB2 instance

To dynamically reconfigure the Veritas Cluster Server One Agent for DB2, use Cluster Manager (Java Console) or the VCS One command line. The following description of configuration changes to include in-depth monitoring shows the use of VCS One commands from the command line. For information on reconfiguring VCS One from the command line the *Veritas Cluster Server One User’s Guide*.

Enabling in-depth monitoring of a DB2 instance

Shallow monitoring of a DB2 instance involves checking the exit status of the `db2gcf` command.

In contrast, in-depth monitoring provides a higher level of confidence in the availability of the instance or partition and its database. It makes additional queries to the database to verify whether the database is available.

Enabling in-depth monitoring from the command line

You can dynamically configure in-depth monitoring. Symantec Corporation recommends that you successfully run DB2 with the agent’s default (shallow) monitoring before you start the in-depth monitoring.

You need to have custom monitoring scripts. Refer to the following table for information on the Indepth Monitor attribute:

See “Db2udb resource type attributes” on page 45.

To start the in-depth monitor for a given instance

1. Freeze the service group so VCS One does not perform actions automatically based on an incomplete reconfiguration:

   ```
   # hagrp -freeze db2udb_group
   ```

2. Enable in-depth monitoring using the command:

   ```
   # hares -modify db2udb_resource DatabaseName name
   # hares -modify db2udb_resource IndepthMonitor 1
   ```

   For example:

   ```
   # hares -modify db2udb_resource DatabaseName SAMPLE
   # hares -modify db2udb_resource IndepthMonitor 1
   # hagrp -unfreeze db2udb_group
   ```

Handling DB2 error codes during in-depth monitoring

The agent for DB2 comes with enhanced ability to handle DB2 errors during in-depth monitoring. The agent classifies DB2 errors according to their severity and associates predefined actions with each error code.

You can create a custom error handling file, db2error.dat. The file lists the DB2 errors and the associated actions that you want the agent to take when it encounters an error.

The file stores information in the following format:

```
SQL_error_string:action_to_be_taken
```

For example:

```
SQL1034N: IGNORE
SQL1039N: WARN
SQL1234N: FAILOVER
```

Table 4-1 shows the available actions for in-depth monitoring.

Table 4-1 Available actions for in-depth monitoring

Action	Description
`IGNORE`	Ignores the error.
`UNKNOWN`	Marks the resource state as UNKNOWN and sends a notification if the Notifier resource is configured. For more information about VCS One notification: See the *Veritas Cluster Server One User's Guide*. This action is typically associated with configuration errors.
`WARN`	Marks the resource state as ONLINE and sends a notification if the Notifier resource is configured. This action is typically associated with low-severity errors.
`FAILOVER` (Default)	Marks the resource state as OFFLINE. This faults the service group, which fails over to the next available system. This action is the agent's default behavior. If the DB2 error code that the agent encounters does not exist in the db2error.dat file, then the agent assumes this default behavior.
`NOFAILOVER`	Freezes the service group temporarily and marks the resource state as OFFLINE. The agent also sends a notification if the Notifier resource is configured. This action is typically associated with the errors that are not system-specific. For example a failover to another client system does not help a corrupt database, .

Disabling in-depth monitoring

You can dynamically disable in-depth monitoring.

To dynamically disable in-depth monitoring

1. Freeze the service group so VCS One does not perform actions automatically based on an incomplete reconfiguration:

   ```
   # hagrp -freeze db2udb_group
   ```

2. Assign the InDepthMonitor attribute a null value to disable in-depth monitoring. Use the command:

   ```
   # hares -modify db2udb_resource IndepthMonitor 0
   ```

   For example:

   ```
   # hares -modify db2udb_resource IndepthMonitor 0
   # hagrp -unfreeze db2udb_group
   ```

Administering VCS One service groups for DB2

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. Select the **Do not add intent Online entries** check box, if you do not want to mark the service group as INTENTONLINE until it comes online.

7. 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]
```

Taking the service group offline

Perform the following steps to take the service group offline.

To take a service group offline from the console

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

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

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

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

4. In the **Offline Service Group** dialog box, click **OK**.

To take a service group offline from the command line

◆ Do one of the following:

To take a service group offline on a specific system, type:

```
# hagrp -offline [-propagate] group -sys system\
[-user user@domain] [-domaintype domaintype]
```

To take a service group offline on any system where the group is online, type:

```
# hagrp -offline [-propagate] 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 Veritas Cluster Server One Agent for DB2 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.

Resource type attributes for DB2

This appendix includes the following topics:

- Db2udb resource type attributes

Db2udb resource type attributes

The DB2 resource has several required and optional attributes.

Table A-1 shows the required attributes for the agent for DB2.

Table A-1 Required attributes for the agent for DB2

Required attributes	Description
DB2InstHome	Path to DB2 UDB instance home directory that contains critical data and configuration files for the DB2 instance. Type and dimension: string-scalar
DB2InstOwner	User ID of Instance Owner that starts a DB2 UDB instance. Each instance requires a unique user ID. Type and dimension: string-scalar **Caution:** Incorrect changes to this attribute can result in DB2 entering an inconsistent state.

Table A-2 shows the optional attributes for the agent for DB2.

Table A-2 Optional attributes for the agent for DB2

Optional attributes	Description
DatabaseName	Name of the database for in-depth monitoring; required if in-depth monitor is enabled (IndepthMonitor = 1). **Note:** Be careful when you change the DataBase name attribute as you can fault all the partitions in the database. Do not change the DataBaseName attribute to an invalid or an incorrect value. Type and dimension: string-scalar
NodeNumber	Node number or partition number of the database. Used when monitoring a specific database partition. Default: 0 Type and dimension: integer-scalar
StartUpOpt	Provides start up options. The allowed values are: START, ACTIVATEDB, or CUSTOM. Review the following options: ■ START (default) Starts the DB2 instance or partition. ■ ACTIVATEDB Performs activate database command after db2 processes start. ■ CUSTOM The agent leaves all the online function completely to the user when the StartUpOpt attribute is set to CUSTOM. It looks for a file named start_custom_$db2instance_$nodenum in the /opt/VRTSagents/ha/bin/Db2udb directory. If this file exists and is executable, it executes this customized online file instead. Example: To customize the online function for partition/nodenum 1 for the db2 instance named db2inst1, the agent for DB2 runs this customized file start_custom_db2inst1_1. It runs this file under the /opt/VRTSagents/ha/bin/Db2udb directory. Type and dimension: string-scalar

Table A-2 Optional attributes for the agent for DB2 *(continued)*

Optional attributes	Description
ShutDownOpt	The allowed values for this attribute are STOP and CUSTOM. Review the following options: ■ STOP Shuts the Db2 instance or partition down in the usual way. ■ CUSTOM Leaves all the offline function completely to the user when the ShutDownOpt is set to CUSTOM. It looks for a file named stop_custom_$db2instance_$nodenum in the /opt/VRTSagents/ha/bin/Db2udb directory. If this file exists and is executable, it executes this customized offline file instead. Example: You want to customize the offline function for partition/nodenum 0 for the db2 instance named db2inst1. You have the agent for DB2 run this customized file: stop_custom_db2inst1_0. The file is in the /opt/VRTSagents/ha/bin/Db2udb directory. Type and dimension: string-scalar
IndepthMonitor	Set the value of the IndepthMonitor attribute to 1 to enable in-depth monitoring. Before this release, IndepthMonitor performed a default SQL query to the database. In 5.0, this default query no longer exists. The agent now looks for the monitor_custom_$db2instance_$nodenum file in the /opt/VRTSagents/ha/bin/Db2udb directory. It executes this customized indepth monitor file if the file exists and is executable. You can find samples of custom monitor scripts in the sample_db2udb directory. Type and dimension: string-integer
Encoding	Specifies the operating system encoding corresponding to DB2 UDB encoding for display of DB2 UDB output. Type and dimension: string-scalar

Table A-2 Optional attributes for the agent for DB2 *(continued)*

Optional attributes	Description
AgentDebug	When the value of this attribute is 1, it causes the agent to log additional debug messages. Type and dimension: boolean-scalar
WarnOnlyIfDBQueryFailed	This attribute either logs SQL errors, or checks the errors to handle them specially. Set the value of the WarnOnlyIfDBQueryFailed attribute to 1 to enable it. When this attribute is enabled, it ignores all SQL errors and logs a warning message in the agent log once a day. Set the value of the WarnOnlyIfDBQueryFailed attribute to 0 to disable it. When disabled, it checks if an error code needs to be handled specially in the db2error.dat file. If the error code does not exist in the db2error.dat file, then it returns OFFLINE for monitor. Otherwise, it follows the action of that particular error code in the db2error.dat file. Type and dimension: boolean-scalar

Table A-3 shows the internal attributes for the agent for DB2.

Table A-3 Internal attributes for the agent for DB2

Required attributes	Description
AgentDirectory	Specifies the location of other files and scripts that are related to the agent. Do not use. For internal use only.

Troubleshooting Veritas Cluster Server One Agent for DB2

This appendix includes the following topics:

- Creating a db2profile for environment variables
- Setting the RestartLimit attribute

Creating a db2profile for environment variables

You can create a profile file for each instance of DB2 and place environment variables in the profile file. You can use this profile to create unique variables for each database user. Each DB2 instance has a home directory that is associated with the instance's log on ID, for example:

```
$InstHome/sqllib/db2profile
```

Where db2profile is the name of the logon ID.

Place the variables that you are interested in using (for example the TimeZone variable) in the profile file. When you then issue a `su -db2instX` command (where X is the instance's name), the environment variables are sourced.

Setting the RestartLimit attribute

VCS starts multiple partitions simultaneously, which can lead to a race condition. The agent's RestartLimit attribute is set to a value of three to help avoid this condition. You can alleviate the potential for this condition by building resource dependencies for each partition. For example, within a service group you can have the Db2udb resource 4 (where nodenum=1) depend on Db2udb resource 3 (where nodenum=2) etc. With the partitions built in a dependency tree, you can set the value of the RestartLimit to zero.