Cluster Server Agent for Cisco UCS Installation and Configuration Guide

Linux

6.2

September 2015

VERITAS™

Cluster Server Agent for Cisco UCS Installation and Configuration Guide

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

Agent Version: 6.2

Document version: 6.2.Rev 1

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

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 support 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/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our website at the following URL:

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

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

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

www.symantec.com/business/support/contact_techsupp_static.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/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as 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 support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Support agreement resources

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

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

About Symantec Connect

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

http://www.symantec.com/connect/storage-management

Documentation

Product guides are available on the media in PDF format. Make sure that you are using the current version of the documentation. The document version appears on page 2 of each guide. The latest product documentation is available on the Symantec website.

https://sort.symantec.com/documents

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

doc_feedback@symantec.com

For information regarding the latest HOWTO articles, documentation updates, or to ask a question regarding product documentation, visit the Storage and Clustering Documentation forum on Symantec Connect.

https://www-secure.symantec.com/connect/storage-management/forums/storage-and-clustering-documentation

Contents

Chapter 1

Introducing the agent for Cisco UCS

This chapter includes the following topics:

About the Cluster Server agent for Cisco UCS

Cluster Server (VCS) agents monitor specific resources within an enterprise application.

The Cluster Server agent for Cisco Unified Computing System (UCS) provides high availability for all the associated service profiles within a specific Cisco UCS domain.

Supported software

For information on the software versions that the Cluster Server agent for Cisco UCS supports, see the Symantec Operations Readiness Tools (SORT) site: https://sort.symantec.com/agents.

Features of the Cluster Server agent for Cisco UCS

- Provides high availability to the associated service profiles within a specific UCS domain.
- Provides high availability to the service profiles for user-specified fault codes, fault severities and types on occurrence of faults.
- Enables you to include or exclude a specific service profiles from monitoring.
- Supports the following types of failover mechanisms:
  - Intelligent - The agent selects a suitable blade server and communicates with the UCS Manager to redeploy the faulted service profiles on the selected blade.
  - Automatic - The agent communicates with the UCS manager to redeploy the faulted service profile on available blade server within the server pool.
- Provides a Unified Computing System high availability (UCSHA) utility to configure high availability for the service profiles.

CiscoUCS agent functions

The Cluster Server agent for Cisco UCS can perform the following functions:

Online

The online function starts monitoring the health of the associated service profiles..

Offline

The offline function stops monitoring the health of the associated service profiles.

Monitor

This function monitors the health of the associated service profiles periodically. The function checks for the faults that occur on the associated blade servers. If the faults reported on the blade server match either fault code or severity and fault type listed in the UCS configuration file, the function redeploys the faulted service profiles to any available blade server within the UCS domain.

Clean

The clean operation stops monitoring the health of service profiles and cleans the cached service profile data.

UCSHA utility

This command line utility is shipped along with the CiscoUCS agent. It enables the user to configure high availability of service profiles in a specific UCS domain.

This utility has the following features:

- Configures the resources to monitor the service profile faults under the Cluster Server.
- Starts monitoring the health of the associated service profiles in a UCS domain.
- Stops monitoring the health of the associated service profiles in a UCS domain.
- Displays the associated service profiles and available free servers within a UCS domain.
- Unconfigures the solution from monitoring the service profile faults.
- Supports configuring of multiple UCS domains for service profile HA in the same cluster.

Usage

The usage of the UCSHA command is mentioned below:

```
  ucsha [ [ [-configure | -start | -stop | -display |
-refresh | -unconfigure] <configfile> ] | -help ]
```

-configure	Reads and validates configuration, configures CiscoUCS resource under VCS.
-start	Initializes and starts monitoring the health of associated service profiles.
-stop	Stops monitoring the health of associated service profiles.
-display	Displays service profiles and associated blade information.
-refresh	Reloads settings from the UCS configuration file and fetches the service profile data.

-help	Displays the usage of the utility.
-unconfigure	Unconfigures CiscoUCS resource under VCS.
configfile	Contains configuration information to connect to Cisco UCS manager and custom settings to monitor service profiles High Availability. See "Sample configuration files" on page 33.

Prerequisites for UCSHA failover

The following types of failover mechanism are supported:

- Automatic - For automatic failover mechanism, you must have the following configuration in the UCS domain:
  - You must configure the server pool of blade servers. The blade servers in the Server Pool should have identical hardware.
  - You must associate the service profiles to the Server Pool.
  - In case of fault on the associated service profile or its corresponding blade server the following actions are taken:
    - The service profile is disassociated from the server pool.
    - The blade server is decommissioned.
    - The service profile is redeployed onto the server pool.
- Intelligent - For intelligent failover, the user needs to have the following configuration in the UCS domain:
  - You must create service profiles and associate the service profiles to the blade servers in UCS domain.
  - In case of fault on the associated service profile or its corresponding blade server the following actions are taken:
    - The service profile is disassociated from the blade server.
    - The blade server is decommissioned.
    - The service profile is redeployed onto an available blade server within the Cisco UCS domain.

    The intelligent failover mechanism selects the available target blade for failover based on the hardware configuration of the faulted blade server.

- If the faulted server belongs to a configured server pool, the intelligent fail over gives preference to the available blade servers within the pool while selecting the target blade.

Setting up Cisco UCS HA in a VCS cluster

Follow the steps below to set up Cisco UCS HA in a cluster:

- Set up a VCS cluster.
  For more information on installing and configuring VCS, refer to the Cluster Server installation and configuration guides.
- Install the Cluster Server agent for Cisco UCS.
  See "Installing the agent in a VCS environment" on page 14.
- Configure the service profile monitoring for CiscoUCS agent.
  See "About configuring service profile HA for Cisco UCS" on page 24.

Chapter 2

Installing and removing the agent for Cisco UCS

This chapter includes the following topics:

Before you install the Cluster Server agent for Cisco UCS

You must install the Cluster Server agent for Cisco UCS on all the systems that will host Cisco UCS service profile HA.

Ensure that you meet the following prerequisites:

- Install and configure the Cluster Server.
  For more information on installing and configuring Cluster Server, refer to the Cluster Server installation and configuration guides.
- Install the latest version of ACC Library.
  To install or update the ACC Library package, locate the library and related documentation in the Agent Pack tarball.

About the ACC library

The operations of a Cluster Server agent depend on a set of Perl modules known as the ACC library. The library must be installed on each system in the cluster that runs the agent. The ACC library contains common, reusable functions that perform tasks, such as process identification, logging, and system calls.

Instructions to install or remove the ACC library on a single system in the cluster are given in the following sections. The instructions assume that the ACCLib tar file has already been extracted.

Note: The LogDbg attribute should be used to enable debug logs for the ACCLib-based agents when the ACCLib version is 6.2.0.0 or later and VCS version is 6.2 or later.

Installing the ACC library

Install the ACC library on each system in the cluster that runs an agent that depends on the ACC library.

To install the ACC library

1. Log in as superuser.
2. Download ACC Library.

   You can download either the complete Agent Pack tar file or the individual ACCLib tar file from the Symantec Operations Readiness Tools (SORT) site (https://sort.symantec.com/agents).
3. If you downloaded the complete Agent Pack tar file, navigate to the directory containing the package for the platform running in your environment.

   cd1/linux/generic/vcs/application/acc_library/*version*_library/rpms
4. If you downloaded the individual ACCLib tar file, navigate to the rpms directory.
5. Install the package. Enter **Yes** if asked to confirm overwriting of files in the existing package.

   ```
   # rpm -i \ VRTSacclib-VersionNumber-GA_GENERIC.noarch.rpm
   ```

Installing the agent in a VCS environment

Install the agent for Cisco UCS on each node in the cluster.

To install the agent in a VCS environment

1. Download the agent from the Symantec Operations Readiness Tools (SORT) site: https://sort.symantec.com/agents.

   You can download either the complete Agent Pack tar file or an individual agent tar file.

2. Uncompress the file to a temporary location, say /tmp.

3. If you downloaded the complete Agent Pack tar file, navigate to the directory containing the package for the platform running in your environment.

   ```
   cd1/linux/generic/vcs/application//ucsutil_agent/
   ```

   ```
   vcs_version/version_agent/rpms
   ```

   If you downloaded the individual agent tar file, navigate to the rpms directory.

4. Log in as superuser.

5. Install the package.

   ```
   # rpm -ihv \
   VRTSucsutil-AgentVersion-GA_GENERIC.noarch.rpm
   ```

6. After installing the agent package, you must import the agent type configuration file.

Importing the CiscoUCSTypes.cf file

Before you configure the Cisco UCS service profiles, you must import the CiscoUCSTypes.cf file to the VCS engine.

To import the CiscoUCSTypes.cf file using the Cluster Manager (Java Console)

1. On one of the nodes in the cluster, start the Cluster Manager (Java Console).

2. Log in to the cluster and wait for the Cluster Explorer to launch.

3. From the File menu select Import Types. Switch to the read/write mode if prompted.

4. In the Import Types dialog box, select the file:

   ```
   /etc/VRTSagents/ha/conf/CiscoUCS/CiscoUCSTypes.cf
   ```

5. Click Import and wait for the file to import.

6. Save the configuration.

To import the CiscoUCSTypes.cf file using the command line

1. Log in to a cluster system as superuser.
2. Make the cluster configuration as read-only. This action ensures that all changes to the existing configuration have been saved and further changes are prevented while you modify main.cf:

   ```
   # haconf -dump -makero
   ```

3. To ensure that VCS is not running while you edit main.cf, issue the following command to stop the VCS engine on all systems. Leave the resources that are available online.

   ```
   # hastop -all -force
   ```

4. Make a backup copy of the main.cf file.

   ```
   # cd /etc/VRTSvcs/conf/config
   # cp main.cf main.cf.orig
   ```

5. Edit the main.cf file to include the CiscoUCSTypes.cf file.

   ```
   # include "/etc/VRTSagents/ha/conf/CiscoUCS/CiscoUCSTypes.cf"
   ```

   The CiscoUCS types definition is imported to the VCS engine. The agent for Cisco UCS can be configured without interrupting or stopping VCS.

Uninstalling the agent in a VCS environment

You must uninstall the agent for Cisco UCS from a cluster while the cluster is active.

To uninstall the agent in a VCS environment

1. Log in as a superuser.
2. Set the cluster configuration mode to read/write by typing the following command from any node in the cluster:

   ```
   # haconf -makerw
   ```

3. Remove all CiscoUCS resources from the cluster. Use the following command to verify that all resources have been removed:

   ```
   # hares -list Type=CiscoUCS
   ```

4 Remove the agent type from the cluster configuration by typing the following command from any node in the cluster:

```
# hatype -delete CiscoUCS
```

Removing the agent's type file from the cluster removes the include statement for the agent from the main.cf file, but the agent's type file is not removed from the cluster configuration directory. You can remove the agent's type file later from the cluster configuration directory (typically /etc/VRTSvcs/conf/config).

5 Save these changes. Then set the cluster configuration mode to read-only by typing the following command from any node in the cluster:

```
# haconf -dump -makero
```

6 Use the native software management program to remove the agent for Cisco UCS from each node in the cluster.

Execute the following command to uninstall the agent:

```
# rpm -e VRTSucsutil
```

Removing the ACC library

Perform the following steps to remove the ACC library.

To remove the ACC library

1 Ensure that all agents that use ACC library are removed.

2 Run the following command to remove the ACC library package.

```
# rpm -e VRTSacclib
```

Chapter 3

Configuring the agent for Cisco UCS

This chapter includes the following topics:

About configuring the Cluster Server agent for Cisco UCS

After installing the Cluster Server agent for Cisco UCS, you must import the agent type configuration file. After importing this file, review the attributes table that describes the resource type and its attributes, and then create and configure CiscoUCS resources.

To view the sample agent type definition:

See “Sample configuration files” on page 33.

CiscoUCS agent attributes

The UCSHA utility sets the UCSConfigFile attribute while configuring the HA solution for the CiscoUCS service profiles.

Table 3-1 CiscoUCS agent attributes

Attribute	Description
ResLogLevel	Controls the agent's logging detail for a specific instance of a resource. Values are ■ ERROR: Logs error messages ■ WARN: Logs error and warning messages ■ INFO: Logs error, warning, and informational messages ■ TRACE: Logs error, warning, informational, and trace Type and dimension: string-scalar Default: INFO Example: "TRACE"
UCSConfigFile	Specifies the absolute path of the CiscoUCS configuration file. The configuration file contains the Cisco UCS Manager connection parameters, distinguished names of the service profiles to include or exclude from monitoring, and fault codes, fault severity, fault type as well as failover mechanism parameter values.. For example: `/etc/VRTSagents/ha/conf/CiscoUCS/UCSConfig_Sample_Include.cfg` See "Sample configuration files" on page 33.

UCSHA configuration file's parameters

The configuration file contains various configurable parameters for monitoring the health of service profiles within the UCS domain.

Table 3-2 Configurable parameters for monitoring the health of service profiles within the UCS domain

Parameter	Description
UCS_MANAGER_URL	Specifies the URL of the UCS Fabric interconnect where the UCS Manager resides. For example: `UCS_MANAGER_URL= [http://xxx.xxx.xxx.xxx/nuova]` You can specify either IP address or hostname in the URL. If the UCS Manager hostname is specified, make sure that it is available from the cluster nodes.

UCS_ADMIN	Specifies the CiscoUCS admin user for the Cisco UCS domain.
	For example:
	`UCS_ADMIN=[admin]`
	For a remotely authenticated user, if an authentication domain is configured, provide the UCS_ADMIN parameter as follows,
	`UCS_ADMIN=[ucs-<domain_name>\<user>]`
	For example:
	`UCS_ADMIN=[ucs-ABC_XYZ\ucs1]`
	Where ABC_XYZ is the authentication domain and ucs1 is the user.

UCS_PASSWORD	Specifies the CiscoUCS admin user's password. The password should be in VCS encrypted format. Use the command `vcsencrypt -agent` to encrypt the password. For example: `UCS_PASSWORD=[COFoROqOIoLOj]`

Table 3-2 Configurable parameters for monitoring the health of service profiles within the UCS domain *(continued)*

Parameter	Description
SP_INCLUDE_LIST	Specifies the names of the service profiles that need to be monitored. Use a comma-separated list to include more than one service profile. If this parameter is specified then the agent monitors only the specified service profiles for HA. By default the agent monitors all associated service profiles in the UCS domain. For example: `SP_INCLUDE_LIST=[org-root/ls -DataLab_SP,org-root/ls-Finance_SP]`
SP_EXCLUDE_LIST	Specifies the names of the service profiles that need to be excluded from monitoring. Use a comma-separated list to exclude more than one service profile. The agent monitors all the associated service profiles except the ones specified in this list. For example: `SP_EXCLUDE_LIST=[org-root/ls -DataLab_SP,org-root/ls-Finance_SP]` **Note:** You must configure either SP_INCLUDE_LIST or SP_EXCLUDE_LIST. If both are configured only SP_INCLUDE_LIST will be considered for monitoring.

Table 3-2 Configurable parameters for monitoring the health of service profiles within the UCS domain *(continued)*

Parameter	Description
FAULT_SEVERITY_LIST	Specifies the fault severity levels to be monitored for the associated service profiles. Use a comma-separated list to include more than one fault severity level. Supported fault severities: ■ Major ■ Critical ■ Minor ■ Warning ■ Info ■ Condition For example: `FAULT_SEVERITY_LIST=[major,critical]`
FAULT_TYPE_LIST	Specifies the fault types to be monitored for the associated service profiles. Use a comma-separated list to monitor more than one fault. Supported fault severities ■ Configuration ■ Connectivity ■ Equipment ■ Environment ■ Fsm ■ Management ■ Network ■ Operational ■ Server For example: `FAULT_TYPE_LIST=[equipment,server]`

Table 3-2 Configurable parameters for monitoring the health of service profiles within the UCS domain *(continued)*

Parameter	Description
FAULT_CODE_LIST	Specifies the fault codes to be monitored for the associated service profiles and their corresponding servers. The solution will monitor only the specified fault codes in the UCS configuration file. For example: `FAULT_CODE_LIST=[F0327,F0310]`

FAILOVER_MECHANISM	Specifies the failover mechanism for the faulted service profiles that need to be redeployed on the available blade servers. The HA solution supports automatic and intelligent failover mechanisms.
	Default: Automatic
	For example:
	`FAILOVER_MECHANISM=[INTL]`
	or
	`FAILOVER_MECHANISM=[intelligent]`
	Note: You must specify either FAULT_CODE_LIST, FAULT_SEVERITY_LIST or FAULT_TYPE_LIST. If the values for the parameters are unspecified, the solution does not monitor service profiles for HA.

ENABLE_DEBUG	Specifies if the debug logs need to be enabled for CiscoUCS HA solution. If the parameter is not specified no debug logs are logged. To enable debug logs set this parameter to 1. For example: `ENABLE_DEBUG=1`

Chapter 4

Configuring the service profile HA for Cisco UCS using UCSHA

This chapter includes the following topics:

About configuring service profile HA for Cisco UCS

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

Use the UCSHA utility to configure the service profile HA.

See "Providing service profile HA for Cisco UCS using the UCSHA utility" on page 25.

Before configuring the service profile HA for Cisco UCS

Before you configure the CiscoUCS service profile HA, you must:

- Verify that VCS is installed and configured on all nodes in the cluster where you will configure the service profile HA.
  For more information on installing and configuring Cluster Server, refer to the Cluster Server installation and configuration guides.
- Make sure that VCS cluster nodes which needs to be monitored are outside the UCS domain.
- Verify that the Cluster Server agent for Cisco UCS is installed on all nodes in the cluster.

Prerequisites for configuring the CiscoUCS agent

You must increase the number of HTTP/HTTPS sessions that are required by a user account, from a default level of 32 to a higher value (256).

Note: You must enable HTTP protocol in the communication services of UCS manager to allow communication to between UCSHA utility and UCS manager.

For increasing the maximum number of HTTP and HTTPS sessions, refer to the following example:

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /system/services # scope web-session-limits
UCS-A /system/services/web-session-limits* # set peruser 256
UCS-A /system/services/web-session-limits* # commit-buffer
UCS-A /system/services/web-session-limits #
```

Providing service profile HA for Cisco UCS using the UCSHA utility

This section lists the configurations that are required for providing service profile HA for Cisco UCS using the UCSHA utility.

Creating UCSHA configuration file

You must create a UCSHA configuration file before you can start using the UCSHA utility. This file is required by the utility to communicate with the UCS Manager within a specific domain for providing high availability to the associated service profiles.

The following example lists a sample UCSHA configuration file:

```
/etc/VRTSagents/ha/conf/CiscoUCS/UCSConfig_Sample_Exclude.cfg

UCS_MANAGER_URL=[http://XX.X.XX.X/nuova]
UCS_ADMIN=[admin]
UCS_PASSWORD=[COFoROqOIoLOj]
SP_INCLUDE_LIST=[]
SP_EXCLUDE_LIST=[org-root/ls-Finance_SP]
FAULT_SEVERITY_LIST=[major,critical]
FAULT_TYPE_LIST=[server]
FAULT_CODE_LIST=[F0123]
FAILOVER_MECHANISM=[intelligent]
ENABLE_DEBUG=1
```

For information on configuration parameters, See "UCSHA configuration file's parameters" on page 19.

Configuring service profile HA with the ucsha utility

You must provide the UCSHA configuration file as a parameter to the UCSHA utility for configuring the service profile HA.

For example:

```
# /opt/VRTSagents/ha/bin/CiscoUCS/ucsha
-configure /etc/VRTSagents/ha/conf/CiscoUCS/UCSConfig_Sample_Exclude.cfg
Reading Configuration..
Config File:[/etc/VRTSagents/ha/conf/CiscoUCS/UCSConfig_Sample_Exclude.cfg]
Configuration Validated.
Proceeding to configure ucsha.

==========================================
UCS_MANAGER_URL=[http://XX.X.XX.X/nuova]
UCS_ADMIN=[admin]
SP_INCLUDE_LIST=[]
SP_EXCLUDE_LIST=[org-root/ls-Finance_SP]
FAULT_SEVERITY_LIST=[major,critical]
FAULT_TYPE_LIST=[server]
FAULT_CODE_LIST=[F0123]
```

```
FAILOVER_MECHANISM=[intelligent]
ENABLE_DEBUG=1
==========================================
ucsha configured successfully.
```

After successful configuration of the utility, VCS resource automatically gets created for the UCS domain. You can verify the VCS resource using the following command:

```
# /opt/VRTSvcs/bin/hares -state
#Resource                          Attribute    System       Value
CiscoUCS_Res_XX_X_XX_X             State        sysA       OFFLINE
CiscoUCS_Res_XX_X_XX_X             State        sysB       OFFLINE
```

Starting service profile HA using the UCSHA utility

After successful configuration of the utility, user must start monitoring the service profiles for high availability using the following command on the VCS node sysA:

```
# /opt/VRTSagents/ha/bin/CiscoUCS/ucsha -start

Connecting with UCS Manager [http://XX.X.XX.X/nuova]...
Authentication with UCS Manager [http://XX.X.XX.XX/nuova] successful...
Fetching Service Profile information...
Fetching available server information...
ucsha successfully started.
Service Profiles inside UCS domain identified
by http://XX.X.XX.XX/nuova will be monitored
```

The state of the VCS resource should be online after UCSHA has started,

For example:

```
Example:
# /opt/VRTSvcs/bin/hares -state

Resource                        Attribute         System      Value
CiscoUCS_Res_XX_X_XX_X          State             sysA      ONLINE
CiscoUCS_Res_XX_X_XX_X          State             sysB      OFFLINE
```

Displaying the UCSHA service profile data

After starting the UCSHA for providing HA to the service profiles, you can see the information of the service profiles that are monitored for high availability using the following command:

```
# /opt/VRTSagents/ha/bin/CiscoUCS/ucsha -disp

Cisco UCS Manager [XX.X.XX.X]

Cisco UCS Service Profile Association...
_____________________________________________________________________
Service Profile          Server                 Model      Server Pool
_____________________________________________________________________
org-root/ls-HR_SP      sys/chassis-1/blade-2  N20-B6620-1

org-root/ls-Admin_SP   sys/chassis-1/blade-4  N20-B6620-1
_____________________________________________________________________

Available Free Servers...

         - - -      sys/chassis-1/blade-5            N20-B6620-2

         - - -      sys/chassis-1/blade-3            N20-B6620-2

         - - -      sys/chassis-1/blade-1            N20-B6620-1

         - - -      sys/chassis-1/blade-6            N20-B6625-1
_____________________________________________________________________
```

UCSHA logs

After the UCSHA utility starts monitoring the service profiles within a UCS domain, you can verify the details of the monitoring using the domain-specific log file that is created by the utility using the following command:

```
# tail -f /var/VRTSvcs/log/ucsha_log_XX_X_XX_X.log
```

If hostname is specified in the UCS Admin URL while configuring UCSHA, the log file name will be changed to `/var/VRTSvcs/log/ucsha_log_hostname.log`.

Stopping service profile HA using the UCSHA utility

You can stop monitoring the associated service profiles within a UCS domain using the following command:

```
# /opt/VRTSagents/ha/bin/CiscoUCS/ucsha -stop
/etc/VRTSagents/ha/conf/CiscoUCS/UCSConfig_Sample_Exclude.cfg
ucsha has stopped monitoring health of Service Profiles for
UCS Manager URL [http://XX.X.XX.X/nuova]
```

The state of the VCS resource should be online after UCSHA has started,

For example:

```
Example:
# /opt/VRTSvcs/bin/hares -state

Resource                      Attribute          System      Value
CiscoUCS_Res_XX_X_XX_X         State              sysA       OFFLINE
CiscoUCS_Res_XX_X_XX_X         State              sysB       OFFLINE
```

Unconfiguring service profile HA with the ucsha utility

You can unconfigure the service profile HA using the following command,

```
# /opt/VRTSagents/ha/bin/CiscoUCS/ucsha -unconfigure
/etc/VRTSagents/ha/conf/CiscoUCS/UCSConfig_Sample_Exclude.cfg
ucsha unconfigured successfully for UCS Domain [http://XX.X.XX.X/nuova].
```

Note: When you unconfigure the solution, the associated VCS resource for CiscoUCS gets deleted.

The UCSHA unconfigure option currently does support any Mount or DiskGroup resource configured under the VCS resource for CiscoUCS.

Chapter 5

Troubleshooting the agent for Cisco UCS

This chapter includes the following topics:

Using the correct software and operating system versions

Ensure that you use correct software and operating system versions.

For information on the software versions that the agent for Cisco UCS supports, see the Symantec Operations Readiness Tools (SORT) site: https://sort.symantec.com/agents.

Meeting prerequisites

Before installing the agent for Cisco UCS, ensure that you meet the prerequisites.

For example, you must install the ACC library on VCS before installing the agent for Cisco UCS.

Reviewing error log files

If you encounter problems while using the agent for Cisco UCS service profile high availability, use the log files described in this section to investigate the problems.

For example,

You can access the logs at the following locations:

- UCS domain specific UCSHA utility logs:
  `/var/VRTSvcs/log/ucsha_log_xx_xxx_xx_xxx`
- Cisco UCS resource specific log information: `/var/VRTSvcs/log/Cisco_A.log`

Cisco UCS privileges

The Cisco UCS Admin user has sufficient privileges as specified in the Cisco UCS configuration file to carry out service profile related operations such as associating the service profiles, dissociating the service profiles, and decommissioning the faulted server.

Appendix A

Sample Configurations

This appendix includes the following topics:

About sample configurations for the agent for Cisco UCS

The sample configuration file contains information regarding the resource types, resources, and resource dependencies within the service group. Review these dependencies carefully before configuring the agent for Cisco UCS. For more information about these resource types, refer to the *Cluster Server Bundled Agents Reference Guide*.

Sample agent type definition

This section lists the sample agent type definition files for the CiscoUCS agent on VCS.

```
type CiscoUCS (
        static boolean AEPTimeout = 1
        static boolean IntentionalOffline = 1
        static str AgentFile = "/opt/VRTSvcs/bin/Script51Agent"
        static str AgentDirectory = "/opt/VRTSagents/ha/bin/CiscoUCS"
        static str ArgList[] = { ResLogLevel, State, IState, UCSConfigFile }
        static int MonitorTimeout = 300
        static int MonitorInterval = 300
        str ResLogLevel = INFO
```

```
        str UCSConfigFile
)
)
```

Sample configuration files

A sample main.cf file for a configuration is as follows:

```
include "types.cf"
include "CiscoUCSTypes.cf"

cluster CiscoUCS_CLUSTER (
        UserNames = { admin = aHIaHChEIdIIgQIcHF }
        Administrators = { admin }
        )

system sysA (
        )
system sysB (
        )

group CiscoUCS_SVG_xx_xxx_xx_xxx (
        SystemList = { sysA = 0, sysB = 1 }
)

CiscoUCS CiscoUCS_Res_xx_xxx_xx_xxx (
                Critical = 0
                ResLogLevel = TRACE
                UCSConfigFile = "/etc/VRTSagents/ha/conf/Cisco UCS/
                                UCSConfig_Sample_Exclude.cfg"
)
```

A sample UCS configuration file with the list of service profiles to be included:

```
UCS_MANAGER_URL=[http://xx.xxx.xx.xx/nuova]
UCS_ADMIN=[admin]
UCS_PASSWORD=[EQHqTQsQKqNQl]
SP_INCLUDE_LIST=[org-root/ls-ISV_SP]
SP_EXCLUDE_LIST=[]
FAULT_SEVERITY_LIST=[major,critical]
FAULT_TYPE_LIST=[equipment,server]
FAULT_CODE_LIST=[F0327]
```

```
FAILOVER_MECHANISM=[intelligent]
```

A sample UCS configuration file with list of service profiles to be excluded:

```
UCS_MANAGER_URL=[http://xx.xxx.xx.xx/nuova]
UCS_ADMIN=[admin]
UCS_PASSWORD=[COFoROqOIoLOj]
SP_INCLUDE_LIST=[]
SP_EXCLUDE_LIST=[org-root/ls-DataLab_SP,org-root/ls-Finance_SP]
FAULT_SEVERITY_LIST=[major,critical]
FAULT_TYPE_LIST=[equipment,server]
FAULT_CODE_LIST=[F0327,F0310]
FAILOVER_MECHANISM=[automatic]
```

Index