Copyright

Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.
# Contents

About This Document ............................................................................................................. v
Document Conventions .......................................................................................................... vi

## Chapter 1

**System Overview** ........................................................................................................... 1

- Overview .......................................................................................................................... 1
- High Availability Overview ............................................................................................. 1
- HA Compliance of NCC Components ............................................................................. 3
- Hardware Configurations ................................................................................................. 4

## Chapter 2

**System Configuration** .................................................................................................. 7

- Overview .......................................................................................................................... 7
- Node Configuration .......................................................................................................... 7
- Connection Configuration ............................................................................................... 8
- Public Network Configuration .......................................................................................... 9
- HA Service Configuration ............................................................................................... 10

## Appendix A

- Oracle HA Agent ............................................................................................................. 13
- NCC Glossary of Terms ................................................................................................. 15
- Index ............................................................................................................................... 17
About This Document

Scope
This guide provides an overview of Oracle Communications Network Charging and Control (NCC). It also introduces the general concepts of NCC using Oracle Clusterware. This document is not intended as a detailed configuration guide and is not certified on any specific version of Oracle Cluster Server.

Audience
This document is intended for system administrators and system integrators who have some experience with implementing high-availability services and have an understanding of NCC.

Related documents
For more information, see the following document sets:

- Oracle Communications NCC:
  - NCC Release Notes
  - NCC Installation Guide
- Oracle Database:
  - Oracle Database High Availability Overview 11g Release 2
  - Oracle Database High Availability Best Practices 11g Release 2
  - Oracle Database Oracle Clusterware and Oracle Real Application Clusters Installation Guide 11g Release 2 (11.2) for Solaris Operating System
- Oracle Clusterware:
  - Sun Cluster Software Installation Guide for Solaris OS
  - Oracle Solaris 11 System Administration Guide: IP Services
## Document Conventions

### Typographical Conventions

The following terms and typographical conventions are used in the Oracle Communications Network Charging and Control (NCC) documentation.

<table>
<thead>
<tr>
<th>Formatting convention</th>
<th>Type of information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Special Bold</strong></td>
<td>Items you must select, such as names of tabs. Names of database tables and fields.</td>
</tr>
<tr>
<td><strong>Italics</strong></td>
<td>Name of a document, chapter, topic or other publication. Emphasis within text.</td>
</tr>
<tr>
<td><strong>Button</strong></td>
<td>The name of a button to click or a key to press. <strong>Example:</strong> To close the window, either click <strong>Close</strong>, or press <strong>Esc</strong>.</td>
</tr>
<tr>
<td><strong>Key+Key</strong></td>
<td>Key combinations for which the user must press and hold down one key and then press another. <strong>Example:</strong> <strong>Ctrl+P</strong>, or <strong>Alt+F4</strong>.</td>
</tr>
<tr>
<td><strong>Monospace</strong></td>
<td>Examples of code or standard output.</td>
</tr>
<tr>
<td><strong>Monospace Bold</strong></td>
<td>Text that you must enter.</td>
</tr>
<tr>
<td><strong>variable</strong></td>
<td>Used to indicate variables or text that should be replaced.</td>
</tr>
</tbody>
</table>
| **menu option > menu option** | Used to indicate the cascading menu option to be selected, or the location path of a file. **Example:** **Operator Functions > Report Functions**  
**Example:** /IN/html/SMS/Helptext/ |
| **hypertext link**    | Used to indicate a hypertext link on an HTML page. |

Specialized terms and acronyms are defined in the **Glossary** at the end of this guide.
Chapter 1

System Overview

Overview

Introduction

This chapter provides a high-level overview of NCC high availability (HA). It explains the basic functionality of the system and lists the main components.

In this chapter

This chapter contains the following topics.

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Availability Overview</td>
<td>1</td>
</tr>
<tr>
<td>HA Compliance of NCC Components</td>
<td>3</td>
</tr>
<tr>
<td>Hardware Configurations</td>
<td>4</td>
</tr>
</tbody>
</table>

High Availability Overview

Introduction

An HA environment should have minimal or no downtime caused by unplanned outages. Outages can be caused by disk drive failures, network failures, system processing unit (SPU) failures, improper system configuration, and application software failures due to application errors or temporarily unavailable system resources.

Additionally, an HA environment should minimize downtime required for planned system and application maintenance and upgrades. Routine system and application upgrades, such as installing kernel, or application patches, or new applications, should occur without taking the critical application services offline.

General operating environment

NCC high availability is achieved by creating an uninterrupted operating environment that is protected and monitored by the Oracle Clusterware. The cluster server agents:

- Detect failures in the hardware and software
- Coordinate the transfer of failing components to their redundant backup components to minimize the impact of the failure
- Automatically start and stop the applications
- Automatically migrate the application from a server that cannot meet the resource requirements of the application (after a local failure, for instance) to a server that can

Application service

NCC configured as an HA system is implemented as an application service managed by the Oracle Clusterware. You configure the Oracle Clusterware to:

- Monitor the health status of NCC
- Control its startup and shutdown
Act on any failures in its operation according to defined rules

**Key HA features**

NCC can remain available in various failure conditions. The HA environment managed and maintained by Oracle Clusterware protects against critical hardware failures. NCC in an HA environment has the following key features:

- Distributed multiprocess, multi-node, multi-system, and multi-site deployment with application resiliency and fault tolerance
- Application high-availability with automatic process recycling and failover
- Hardware high-availability through redundancy and configuration

**Deployment considerations**

Consider the following when deploying NCC for HA:

- Whether the NCC system has any custom components
- NCC monitoring and management capabilities.

**Hardware requirements for HA**

You achieve hardware availability by using redundant backup components for each subsystem that may fail:

- Mirrored dual-port data disks to protect the application from loss of critical data
- Redundant network interfaces and networks to ensure that application clients can connect to the network
- Redundant SPUs to guard against entire system failures

For more information about hardware availability and configuration, see *Hardware Configurations* (on page 4).

**Software components**

Hardware redundancy on its own does not guarantee the high availability of application services offered by NCC. It is achieved by ensuring that all software components included in the entire solution are built and configured for fault tolerance. NCC HA service manages the availability of NCC and its dependent services, such as the database engine, and any other third-party applications required by NCC.

**Application services for third-party components**

When you design an NCC HA environment, you define the database service and services required by NCC third-party components, such as brass agent process for SNMP, as separate application services. These services are directly controlled by the Oracle Clusterware, which directly enforces the dependencies between these services and NCC. The dependency rules determine the proper startup and shut down sequence of the NCC services and ensure that the dependent services are available when NCC is running.

**Redundant node setup**

When you set up an HA environment, you must eliminate single points of failure that prevent NCC from processing orders for an extended period of time.
The Active/Passive setup comprises two near identical infrastructures, logically sitting side-by-side. One node hosts the database service or application, while the other rests idly waiting in case the primary system goes down. They share a storage component, and the primary server gracefully turns over control of the storage to the other server or node when it fails. On failure of the primary node, the inactive node becomes the primary and hosts the database or application. NCC HA can be configured as an NCC single package.

**HA Compliance of NCC Components**

**Introduction**

Applications running in an HA environment have reliable access to system resources because the cluster server ensures the continuous availability of the operating environment.

NCC components follow the criteria described below:

- Automatic application operation
- Minimizing data loss when a failure occurs
- Automatic reconnection
- Recovery when replicated backup nodes are geographically dispersed

**Automatic application operation**

An HA environment provides fully automatic system operation. No user input is required to start or stop the NCC services in any configuration. All startup and shut down procedures are command-line driven and have predictable maximum startup and shut down times. Upon completion, startup and shut down procedures return the correct status of the performed operation.

If NCC fails because of a hardware failure on one node and is migrated to another node, the NCC services are able to restart and recover automatically through the Oracle Clusterware.

NCC is not guaranteed to be associated with a (pseudo) terminal device. Therefore, NCC does not rely on input from a standard input device (stdin) because the input device can be closed right after the application process is initialized.

**Minimizing data loss**

NCC minimizes the amount of data lost when a failure occurs. All modified in-memory data that has not been saved at the time of the failure will be lost. NCC reloads the dynamic data and rolls back all modifications to the point immediately prior to the failure.

The NCC servers use database transaction logging to minimize the data loss in the event of a failure.

**Automatic reconnections**

Oracle highly recommends that applications be configured so that they detect connection problems and automatically attempt to reconnect when a connection is lost. NCC attempts to establish an alternative connection to multiple servers, if available, and takes advantage of all available access paths to the data source, or network routes.

To increase system availability, transaction processing monitors can provide some help in managing client connections and controlling the queue of connection requests.
Disaster recovery

Disaster recovery requires that you set up a remote instance of NCC that can be activated in the event of a catastrophic failure at the production site. An HA system for NCC, consisting of multiple clustered servers, is usually limited by the length of the cables connecting the shared data disk devices and the network interfaces. A remote disaster recovery site that is geographically dispersed requires access to the same resources as the production site, including:

- Network connectivity to clients
- Hardware
- Up-to-date NCC configuration data
- Dynamic provisioning data

An HA environment requires regular system backups and data replication mechanisms. Data backup must be implemented independent of NCC.

Hardware Configurations

Introduction

The hardware configuration for HA depends on:

- The size of the NCC installation
- How available you need the system to be
- The performance required under normal operating conditions and after a node failure

If you install NCC as a single instance (on a single physical server) and the failure of a single node can degrade service during the short switch-over, then you configure your nodes for HA as either active/active pairs or active/passive pairs..
Diagram
The following diagram shows an example HA setup with two cluster nodes.

Hardware components
This table describes hardware components shown in the diagram.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster nodes</td>
<td>Each system is a multiprocessor machine with redundant backup hardware components configured for the best availability possible. The backup hardware components include, for example: power supplies, I/O cards, SCSI controllers, and network cards.</td>
</tr>
<tr>
<td>External shared disks</td>
<td>The external shared disks provide an HA data storage system. This can be a set of disk arrays, or a mirrored set of disk multi-packs connected to the cluster nodes through redundant backup SCSI or fiber optic channels. The shared disks contain all dynamic data required by the NCC application to operate.</td>
</tr>
</tbody>
</table>
## Component Description

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routers or Switches</td>
<td>The public network routers or switches are duplicated standard networking equipment. Routers and switches used for the private network are not accessible from the public network and provide a communication channel for the inter-cluster traffic only. Crossover cables can be used in a two-node cluster for the private network interconnect.</td>
</tr>
</tbody>
</table>

In this setup, the location between the two nodes should not be too far away geographically, to keep switch-over times as low as possible. There is no geographical redundancy in this setup. You can provide additional recovery security by setting up an NCC disaster recovery site and using Oracle Data Guard to synchronize the two sites.

### Active/Passive

A typical NCC-HA environment consists of a two-node cluster implemented in active/passive configuration. One node in the cluster is configured to run the database service and to run NCC while the other is configured to be in passive standby. Both nodes act as backup servers for each other. Therefore, if NCC fails on its primary node, it migrates to the database and application to the secondary node, which then becomes the primary node.

### Active/Active

An active/active system is a network of independent processing nodes for the services active on them, each having access to a common replicated database, so that all nodes participate in a common application. Any transaction can be routed within the application network to any node where the service is active which reads or updates any set of data items in the database.

This approach provides flexibility and better system investment as requests are load-balanced across all available processing capacity. If a node fails, the users at the failed node are quickly switched to surviving nodes, thus restoring their services in seconds or less.

An active/active network contains at least two copies of the application database. All database copies are kept in synchronization so that any copy can be used for a transaction. If a database copy fails, all transactions are routed to a surviving copy. Providing that the nodes and database copies are minimally geographically distributed, active/active systems provide a first level of disaster recovery for little or no cost. If a disaster knocks out a node or a database copy, there are others in the network to take its place.
Overview

Introduction

This chapter provides information about configuring the cluster software and HA application service.

In this chapter

This chapter contains the following topics.

<table>
<thead>
<tr>
<th>Node Configuration</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection Configuration</td>
<td>8</td>
</tr>
<tr>
<td>Public Network Configuration</td>
<td>9</td>
</tr>
<tr>
<td>HA Service Configuration</td>
<td>10</td>
</tr>
</tbody>
</table>

Node Configuration

Introduction

This topic describes the cluster node configuration.

Oracle Clusterware configuration

When you configure the Oracle Clusterware, you specify the cluster nodes, the service groups, and the service group composition. The configuration contains the following aspects.

Refer to the Oracle Clusterware documents listed in Related documents for details.

<table>
<thead>
<tr>
<th>Aspect</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include clauses</td>
<td>Used to include standard and custom resource type definitions. The resource type definitions are from other files residing in the current cluster configuration directory.</td>
</tr>
<tr>
<td>Cluster definition</td>
<td>Contains attributes that apply to the entire cluster.</td>
</tr>
<tr>
<td>System definition</td>
<td>Defines the cluster node and attributes applicable to the defined node. Keyword system followed by the system name.</td>
</tr>
<tr>
<td>Service group definitions</td>
<td>Specifies the systems configured to run the services defined in the service group and the list of systems where services are started automatically when the cluster server starts up.</td>
</tr>
<tr>
<td>Resource definitions</td>
<td>Defines resource type its resource name and all required attributes expected by the resource agent.</td>
</tr>
<tr>
<td>Resource dependencies</td>
<td>Used to control the startup and shutdown sequence of resources that belong to the same service group.</td>
</tr>
</tbody>
</table>
### Group dependencies

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Indicates that the parent group must be...</th>
</tr>
</thead>
<tbody>
<tr>
<td>online global</td>
<td>online anywhere in the cluster before the child can go online.</td>
</tr>
<tr>
<td>online local</td>
<td>online on the same node before the child can go online.</td>
</tr>
<tr>
<td>online remote</td>
<td>online on a different system in the cluster before the child can go online.</td>
</tr>
<tr>
<td>offline local</td>
<td>offline on the same node before the child can go online.</td>
</tr>
</tbody>
</table>

### About configuring active and passive nodes

**Active/Passive**

A sample of the NCC HA active/passive configuration is available in the appendix. The sample illustrates the service group definitions and dependencies between services that provide HA for NCC. Refer to the following guides to find more general information about active/passive setup:

- *Oracle Database High Availability Overview 11g Release 2*
- *Oracle Database High Availability Best Practices 11g Release 2*

**Active/Active**

Refer to the following guides to find an example of active/active configuration:

- *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Installation Guide 11g Release 2 (11.2) for Solaris Operating System*
- *Sun Cluster Software Installation Guide for Solaris OS*
- *NCC Installation Guide*. More specific detail is in Chapter 7, SMS Cluster Post Installation Tasks.

### Synchronizing system time

The local system time must be consistent on all cluster nodes. You can properly synchronize the time by enabling the Network Time Protocol (ntp) daemon on each node in the cluster. The ntp daemon configuration is in the `/etc/ntp.conf` file.

You can use the default configuration of the cluster NTP file, found in `/etc/inet/ntp.conf.cluster`.

For more information, see 'How to Configure Network Time Protocol (NTP)' in *Sun Cluster Software Installation Guide for Solaris OS*.

### Connection Configuration

**Introduction**

You perform the following tasks to configure the Oracle Clusterware inter-node communication services:

- Configure the Oracle Clusterware
- Register interconnects and ports
Configuring the Oracle Clusterware

During the configuration of the Oracle Cluster, when you run the configuration script (/usr/cluster/bin/scinstall), the configuration script probes the interconnects between the nodes. If it cannot detect the interconnections or cannot detect the other node over the interconnect due to a problem, you will be prompted with an error message, and the script is paused. After you have corrected the problem, you can continue to run the script and this time it properly detects the interconnects, as shown in the following example:

You can either attempt to correct the problem and try the probes again or manually configure the transport. To correct the problem might involve re-cabling, changing the configuration, or fixing hardware. You must configure the transport manually to configure tagged VLAN adapters and non tagged VLAN adapters on the same private interconnect VLAN.

Do you want to try again (yes/no) [yes]? yes

The following connections were discovered:

| sms01:ce1 | switch1 | sms02:ce1 |
| sms01:ce2 | switch2 | sms02:ce2 |

Completed discovery of the cluster transport configuration

Registering interconnects and ports

This procedure shows an example of how to manually add four more cluster interconnects, by registering each VLAN on the switch and its ports.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1    | Register the switches, as root, by typing:  
/usr/cluster/bin/clinterconnect add switch3  
/usr/cluster/bin/clinterconnect add switch4  
/usr/cluster/bin/clinterconnect add switch5  
/usr/cluster/bin/clinterconnect add switch6 |
| 2    | Register the ports, as root, by typing:  
/usr/cluster/bin/clinterconnect add sms01:ce3,switch3  
/usr/cluster/bin/clinterconnect add sms02:ce3,switch3  
/usr/cluster/bin/clinterconnect add sms01:ce5,switch4  
/usr/cluster/bin/clinterconnect add sms02:ce5,switch4  
/usr/cluster/bin/clinterconnect add sms01:ce6,switch5  
/usr/cluster/bin/clinterconnect add sms02:ce6,switch5  
/usr/cluster/bin/clinterconnect add sms01:ce7,switch6  
/usr/cluster/bin/clinterconnect add sms02:ce7,switch6 |
| 3    | Check the status of the cluster transport paths, by typing:  
scstat -W  

Result: The configuration is displayed.  

<table>
<thead>
<tr>
<th>Transport path:</th>
<th>Path online</th>
</tr>
</thead>
<tbody>
<tr>
<td>sms02:ce3</td>
<td>sms01:ce3</td>
</tr>
<tr>
<td>sms02:ce2</td>
<td>sms01:ce2</td>
</tr>
<tr>
<td>sms02:ce1</td>
<td>sms01:ce1</td>
</tr>
<tr>
<td>sms02:ce5</td>
<td>sms01:ce5</td>
</tr>
<tr>
<td>sms02:ce7</td>
<td>sms01:ce7</td>
</tr>
</tbody>
</table>

Public Network Configuration

Introduction

Oracle Solaris includes standard agents that you can use to manage dynamic IP addresses required by the service groups. There are two ways to manage dynamic IP addresses. You can use:
Chapter 2

- NIC and IP: To control a single public interface card
- IP multipathing agents: To control a redundant backup set of network interface cards

Configuring a single NIC/IP pair

For Solaris, you configure NIC and IP pairs in two different configuration files: /etc/netmasks and /etc/hosts.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Add IP address and hostname, by typing:</td>
</tr>
<tr>
<td></td>
<td>vi /etc/hosts</td>
</tr>
<tr>
<td></td>
<td>192.168.46.41 sms01</td>
</tr>
<tr>
<td>2</td>
<td>Add the network mask of the added hosts, by typing:</td>
</tr>
<tr>
<td></td>
<td>vi /etc/netmasks</td>
</tr>
<tr>
<td></td>
<td>192.168.46.0 255.255.255.0</td>
</tr>
</tbody>
</table>

Configuring IP multipathing pair

Ensure each network port has a unique MAC address, as shown in the following example.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Type:</td>
</tr>
<tr>
<td></td>
<td>eeprom &quot;local-mac-address?=true&quot;</td>
</tr>
<tr>
<td>2</td>
<td>On Node 1, type:</td>
</tr>
<tr>
<td></td>
<td># vi /etc/hostname.ce0</td>
</tr>
<tr>
<td></td>
<td>and insert the following in the file:</td>
</tr>
<tr>
<td></td>
<td>sms01-mgmt-ce0 netmask + broadcast + group \</td>
</tr>
<tr>
<td></td>
<td>mgmt deprecated -failover up addif sms01 netmask + broadcast + \</td>
</tr>
<tr>
<td></td>
<td>failover up</td>
</tr>
<tr>
<td>3</td>
<td>Type:</td>
</tr>
<tr>
<td></td>
<td>vi /etc/hostname.ce9</td>
</tr>
<tr>
<td></td>
<td>and insert the following in the file:</td>
</tr>
<tr>
<td></td>
<td>sms01-mgmt-ce9 netmask + broadcast + group \</td>
</tr>
<tr>
<td></td>
<td>mgmt deprecated -failover standby up</td>
</tr>
<tr>
<td>4</td>
<td>On Node 2, type:</td>
</tr>
<tr>
<td></td>
<td>vi /etc/hostname.ce0</td>
</tr>
<tr>
<td></td>
<td>and insert the following in the file:</td>
</tr>
<tr>
<td></td>
<td>sms02-mgmt-ce0 netmask + broadcast + group \</td>
</tr>
<tr>
<td></td>
<td>mgmt deprecated -failover up addif sms02 netmask + broadcast + \</td>
</tr>
<tr>
<td></td>
<td>failover up</td>
</tr>
<tr>
<td>5</td>
<td>Type:</td>
</tr>
<tr>
<td></td>
<td>vi /etc/hostname.ce9</td>
</tr>
<tr>
<td></td>
<td>and insert the following in the file:</td>
</tr>
<tr>
<td></td>
<td>sms02-mgmt-ce9 netmask + broadcast + group \</td>
</tr>
<tr>
<td></td>
<td>mgmt deprecated -failover standby up</td>
</tr>
</tbody>
</table>

HA Service Configuration

Introduction

The cluster can be one of two configurations:
- Active/active (Oracle Real Application Clusters (RAC))
- Active/passive (HA Oracle)

In both cases, you need to set up the:
- Oracle database resources - which manages the Oracle database instance.
Oracle listener resources - which manages the Oracle database listeners.

For more information about Cluster resource types, resources and resource groups, refer to Sun Cluster Software Installation Guide for Solaris OS.

### Setting up database resource

The Oracle database resource must be set up based on a resource type. These resource types can be, for example:

- oracle_rac_server (for active/active)
- oracle_server (for active/passive)

#### ORACLE resource parameters

To set up the Oracle resource, you might need the following parameters, described in the table below.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ORACLE_USER</td>
<td>UNIX user name of the Oracle RDBMS owner.</td>
</tr>
<tr>
<td>ORACLE_HOME</td>
<td>Full path to the Oracle home directory.</td>
</tr>
<tr>
<td>SID</td>
<td>Name of the Oracle instance.</td>
</tr>
<tr>
<td>PFILE</td>
<td>Full path to the Oracle startup parameter file.</td>
</tr>
<tr>
<td></td>
<td>The default is Oracle_Home/dbs/init$SID.ora.</td>
</tr>
<tr>
<td>LOG_FILE</td>
<td>The full path to the agent log file.</td>
</tr>
<tr>
<td></td>
<td>The default is the cluster log file located in the $VCS_LOG directory.</td>
</tr>
</tbody>
</table>

#### Example Oracle resource configuration command

Here is an example of how to configure an Oracle resource in active/passive configuration, by typing:

```shell
clresource create -g oracleha -r oracle_server -t SUNW.oracle_server -p ORACLE_HOME=/u01/app/oracle/product/11.2.0 -p Alert_log_file=/u01/app/oracle/diag/rdbms/smf/SMF/trace/alert_SMF.log -p ORACLE_SID=SMF -p Connect_string=monitor/monitor -p resource_dependencies=oracledisk-res oracleha-server-rs
```

### Setting up listener resource

The Oracle database listener resource must be set up based on a resource type, named oracle_listener.

#### Oracle listener resource parameters

To set up the Oracle Listener resource, you might need the following parameters, described in the table below.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ORACLE_USER</td>
<td>UNIX user name of the Oracle RDBMS owner.</td>
</tr>
<tr>
<td>ORACLE_HOME</td>
<td>Full path to the Oracle home directory.</td>
</tr>
<tr>
<td>LISTENERS</td>
<td>A value-pair list containing a sequence of Oracle listeners monitored by the</td>
</tr>
<tr>
<td></td>
<td>agent. The syntax is: ListenerName=OracleSID</td>
</tr>
<tr>
<td>USER</td>
<td>Oracle user name used by the monitor function to connect to the Oracle</td>
</tr>
<tr>
<td></td>
<td>instance to verify the status of Oracle SQLNet.</td>
</tr>
<tr>
<td>PASSWORD</td>
<td>Password for the Oracle user defined above.</td>
</tr>
</tbody>
</table>
### Chapter 2

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOG_FILE</td>
<td>The full path to the agent log file.</td>
</tr>
<tr>
<td></td>
<td>The default is the cluster log file located in the $VCS_LOG directory.</td>
</tr>
</tbody>
</table>

**Example Oracle listener resource configuration command**

Here is an example of how to configure an Oracle listener resource in active/passive configuration, by typing:

```
clresource create -g oracleha-rq \
-t SUNW.oracle_listener -p ORACLE_HOME=/u01/app/oracle/product/11.2.0 \
-p LISTENER_NAME=LISTENER \
-p resource_dependencies=oracledisk-res oracle-listener-rs
```
Appendix A

Oracle HA Agent

Introduction

This topic provides an example of an Oracle Clusterware setup that would be appropriate for an NCC Active/Passive configuration.

Configuring the active/passive

Here is an example procedure for configuring an active/passive setup. This is the same for both nodes.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 1    | Allow users to allocate large amounts of SHM, by entering:  
prctl -i project default  
projmod -s -K "process.max-sem-nsems=(priv,256,deny)" default  
projmod -s -K "project.max-sem-ids=(priv,100,deny)" default  
projmod -s -K "project.max-shm-ids=(priv,100,deny)" default  
prctl -i project default |
| 2    | Enable all users to read/write to the /tmp file system, by entering:  
# chmod 777 /tmp  
# chmod +t /tmp  
(Change the default UMASK for root)  
# vi /etc/default/login  
UMASK=022  
# create monitor user  
$ sqlplus / as sysdba  
sql> grant connect, resource to monitor identified by monitor;  
sql> alter user monitor default tablespace users quota 1m on users;  
sql> grant select on v_sysstat to monitor;  
sql> grant select on v_archive_dest to monitor;  
sql> grant create session to monitor;  
sql> grant create table to monitor; |
| 3    | Create the failover resource group to contain all of the resources, by entering:  
# ciresourcegroup create oracleha-rg  
(Add the logical hostname resource to the resource group.)  
# ciresourcegroup create oracleha-rg -h usms oraclelh-res  
(Register the SUNW.HAStoragePlus resource type.)  
# ciresourcetype register SUNW.HAStoragePlus |
| 4    | Add a resource of type SUNW.HAStoragePlus to the resource group, by entering:  
# clrs create -g oracleha-rg -t SUNW.HAStoragePlus -p  
FilesystemMountPoints="/oracle/historicalcdr/SMF,/oracle/activecdr/SMF,  
-p AffinityOn-TRUE  
oracledisk-res |
| 5    | Bring the resource group online in a managed state, by entering:  
# ciresourcegroup online -M oracleha-rg  
(Register the Oracle resource types.)  
# ciresourcetype register SUNW.oracle_server  
# ciresourcetype register SUNW.oracle_listener |
| 6    | Add the Oracle application resources to the resource group, by entering: |
Step | Action
--- | ---
# clrs create -g oracleha-rg -t SUNW.oracle_server \
-p ORACLE_HOME=/u01/app/oracle/product/11.2.0 \
-p Alert_log_file=/u01/app/oracle/diag/rdbms/smf/SMF/trace/alert_SMF.log \
-p ORACLE_SID=SMF -p Connect_string=monitor/monitor \
-p resource_dependencies=oracledisk-res oracleha-server-rs
# clresource create -g oracleha-rg \
-t SUNW.oracle_listener -p ORACLE_HOME=/u01/app/oracle/product/11.2.0 \
-p LISTENER_NAME=LISTENER \
-p resource_dependencies=oracledisk-res oracle-listener-rs
NCC Glossary of Terms

DTMF
Dual Tone Multi-Frequency - system used by touch tone telephones where one high and one low frequency, or tone, is assigned to each touch tone button on the phone.

HTML
HyperText Markup Language, a small application of SGML used on the World Wide Web. It defines a very simple class of report-style documents, with section headings, paragraphs, lists, tables, and illustrations, with a few informational and presentational items, and some hypertext and multimedia.

IN
Intelligent Network

IP
1) Internet Protocol
2) Intelligent Peripheral - This is a node in an Intelligent Network containing a Specialized Resource Function (SRF).

IP address
Internet Protocol Address - network address of a card on a computer

Oracle
Oracle Corporation

SGML

SLC
Service Logic Controller (formerly UAS).

SMS
Depending on context, can be:
- Short Message Service
- Service Management System platform
- NCC Service Management System application

SNMP
SRF
Specialized Resource Function - This is a node on an IN which can connect to both the SSP and the SLC and delivers additional special resources into the call, mostly related to voice data, for example, play voice announcements or collect DTMF tones from the user. Can be present on an SSP or an Intelligent Peripheral (IP).

SSP
Service Switching Point