Oracle® Communications Convergent Charging Controller

Security Guide

Release 12.0.6

September 2022

Copyright

Contents

About This Document

Audience

The audience for this document includes system administrators responsible for the monitoring, maintenance, and configuration of the Oracle Communications Convergent Charging Controller IN applications.   The reader will have a sound knowledge of Sun Solaris, Cisco IOS, and Intelligent Network concepts.

Scope

The scope of this document includes all the information required to install and operate the Oracle Communications Convergent Charging Controller platform securely.

Related Documents

The following documents are related to this document:

- *Installation Guide*

Document Conventions

Typographical Conventions

The following terms and typographical conventions are used in the Oracle Communications Convergent Charging Controller documentation.

Formatting Convention	Type of Information
Special Bold	Items you must select, such as names of tabs. Names of database tables and fields.
Italics	Name of a document, chapter, topic or other publication. Emphasis within text.
Button	The name of a button to click or a key to press. **Example:** To close the window, either click **Close**, or press **Esc**.
Key+Key	Key combinations for which the user must press and hold down one key and then press another. Example: **Ctrl+P** or **Alt+F4**.
`Monospace`	Examples of code or standard output.
`Monospace Bold`	Text that you must enter.
variable	Used to indicate variables or text that should be replaced with an actual value.
menu option > menu option >	Used to indicate the cascading menu option to be selected. Example: **Operator Functions > Report Functions**
hypertext link	Used to indicate a hypertext link.

Specialized terms and acronyms are defined in the glossary at the end of this guide.

Chapter 1

Introduction to Security

Chapter Overview

Introduction

This chapter provides an overview of Oracle Communications Convergent Charging Controller security.

In this chapter

This chapter contains the following topics.

Basic Security Considerations

Basic Security

Follow these fundamental principles to use any application securely:

- Keep your software up-to-date including the latest product release and any patches that apply to it. See https://edelivery.oracle.com and https://support.oracle.com for more information. These sites also include many of the documents referred to in this guide.
- Limit privileges as much as possible. Give users only the level of security access necessary for them to perform their work. Review user privileges periodically to determine the relevance to current work requirements.
  See the Oracle Solaris document *System Administration Guide: Basic Administration* for more information.
- Monitor system activity. Establish who should access which system components and how often and monitor those components.
- Install software securely. For example, use firewalls, secure protocols such as SSL, and secure passwords. See *Installing Convergent Charging Controller Securely* (on page 7) for more information.
- Learn about and use the security features. See *Implementing Security* (on page 11) for more information.
- Use secure development practices. For example, take advantage of existing database security functionality rather than creating your own application security. See *Security Considerations for Developers* (on page 14) for more information.
- Keep up-to-date on security information. Oracle regularly issues security-related patch updates and security alerts. You must install all security patches as soon as possible. See the "Critical Patch Updates and Security Alerts" on the Oracle Technology Network Web site:
  http://www.oracle.com/technetwork/topics/security/alerts-086861.html

About Security

Security Overview

Convergent Charging Controller uses Solaris and database as middleware. System security is managed in the following ways:

- To access the database, Convergent Charging Controller uses OPS$ accounts.
- Solaris security access policy is used for systems administrators' access.
- User access to the graphical user interface screens is managed through user name and password that are stored in the database.
- Batch scripts access are managed through read and write access granted to the specific directory where the scripts are stored.
- Batch provisioning is managed through limited read and execute rights to the executable program in the /IN/service_packages/PI/bin directory.
- External systems connecting to Convergent Charging Controller through Diameter, SIP, and the SOAP interface are identified by their IP addresses or hostname by the system.

The Convergent Charging Controller product is typically located and managed within the internal corporate network. The external connections to other non–management systems are also protected through other network elements, for example, by firewalls. For each interface, configurable overload protection is available to prevent the system from overloading.

Understanding the Environment

Planning Considerations

When planning your Convergent Charging Controller implementation, consider the following:

Which resources need to be protected?

- Customer data, such as traffic history.
- Internal data, such as proprietary source code.
- System components from being disabled by external attacks on the system or intentional system overloads.

Who are you protecting data from?

- You need to protect subscribers' data for others, but people in your organization will need to access that data to manage it.
- You can analyze workflows to determine who needs access to the data; for example, it is possible for a system administrator to manage system components without needing access to system data.

What will happen if the protection of a strategic resource fails?

In some cases, a fault in your security scheme is nothing more than an inconvenience. In other cases, a fault might cause extensive damage to either your business or to one or more of your customers. Understanding the security ramifications of each resource will help you protect your business properly.

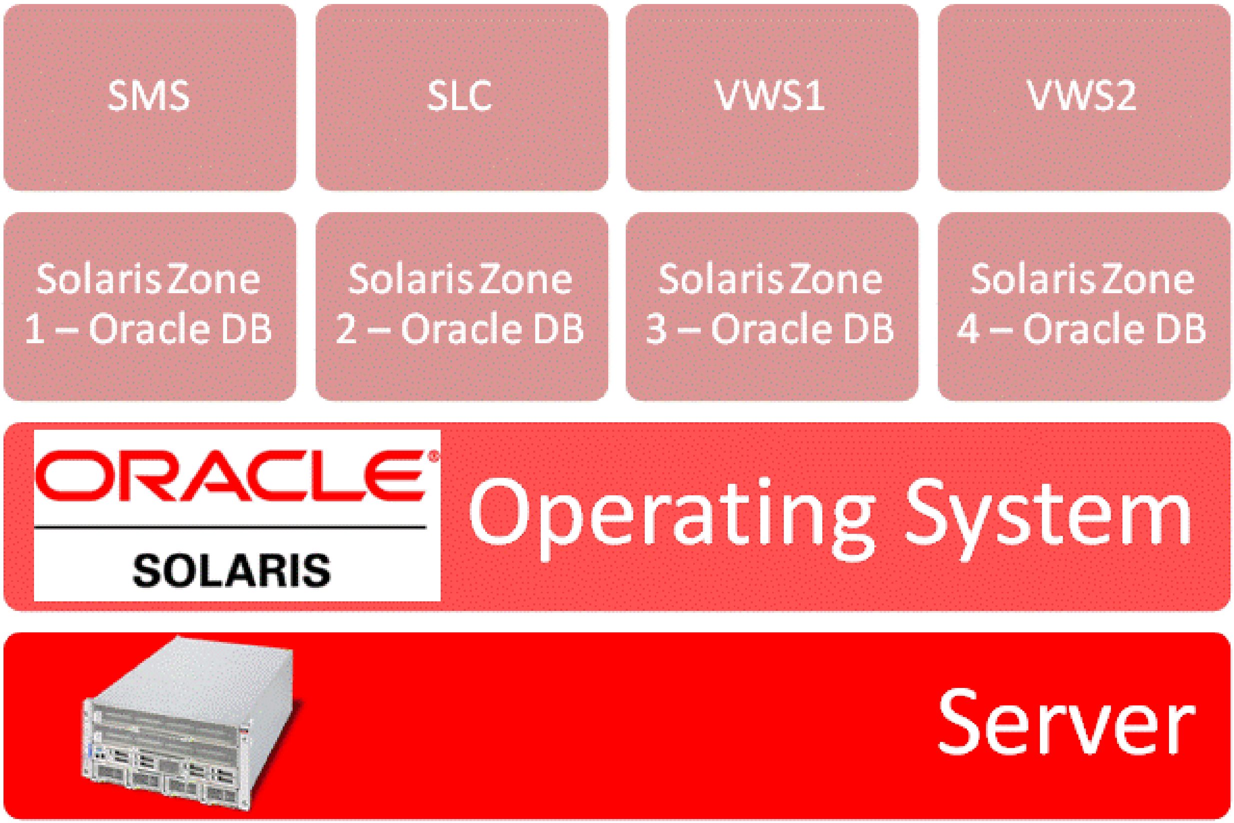
Recommended Deployment Configurations

Introduction

This section describes recommended deployment configuration options for your Convergent Charging Controller system.

Test Bed Deployment

The simplest test bed architecture is shown here. This single-server deployment is cost effective and provides a functional test environment; however, it only provides limited hardware redundancy as all nodes are installed on the same server.


SMS
SLC
VWS1
VWS2
Solaris Zone 1 – Oracle DB
Solaris Zone 2 – Oracle DB
Solaris Zone 3 – Oracle DB
Solaris Zone 4 – Oracle DB
ORACLE SOLARIS
Operating System
Server

Single Server Deployment

The single-server deployment reduces the network vulnerability as the inter-node communication does not leave the server. This does not mean that network security is not required for such a deployment.

Generally, a test bed is only used inside a controlled environment within the company's intranet. The network access that must be controlled by a firewall includes the following interfaces: provisioning, Diameter, SOAP, REST, and the screen access for SMS, ACS, CCP and VPN.

Depending on the Oracle virtualization technology used, good security practices related to the chosen technology need to be put in place. More information on best practices for these technologies is available in the following Oracle guides:

- Secure Deployment of Oracle VM Server for SPARC
- Solaris Zones Administration

Production Deployment

For the production environment, Oracle recommends the use of the Firewall-DMZ-Firewall-Intranet architecture shown in Figure 2, for all non voice and data based connections, with the exception of the SOAP interface. Servers can be deployed in a single location or be geographically distributed. This implies that there is a requirement for additional firewalls to handle access between sites.

The Convergent Charging Controller product is designed to handle real time telecommunication traffic so it is essential that any security infrastructure is designed for optimal performance. The implementation of firewall rules must be effective, but also efficient. For this reason, the platform should be deployed inside a DMZ.

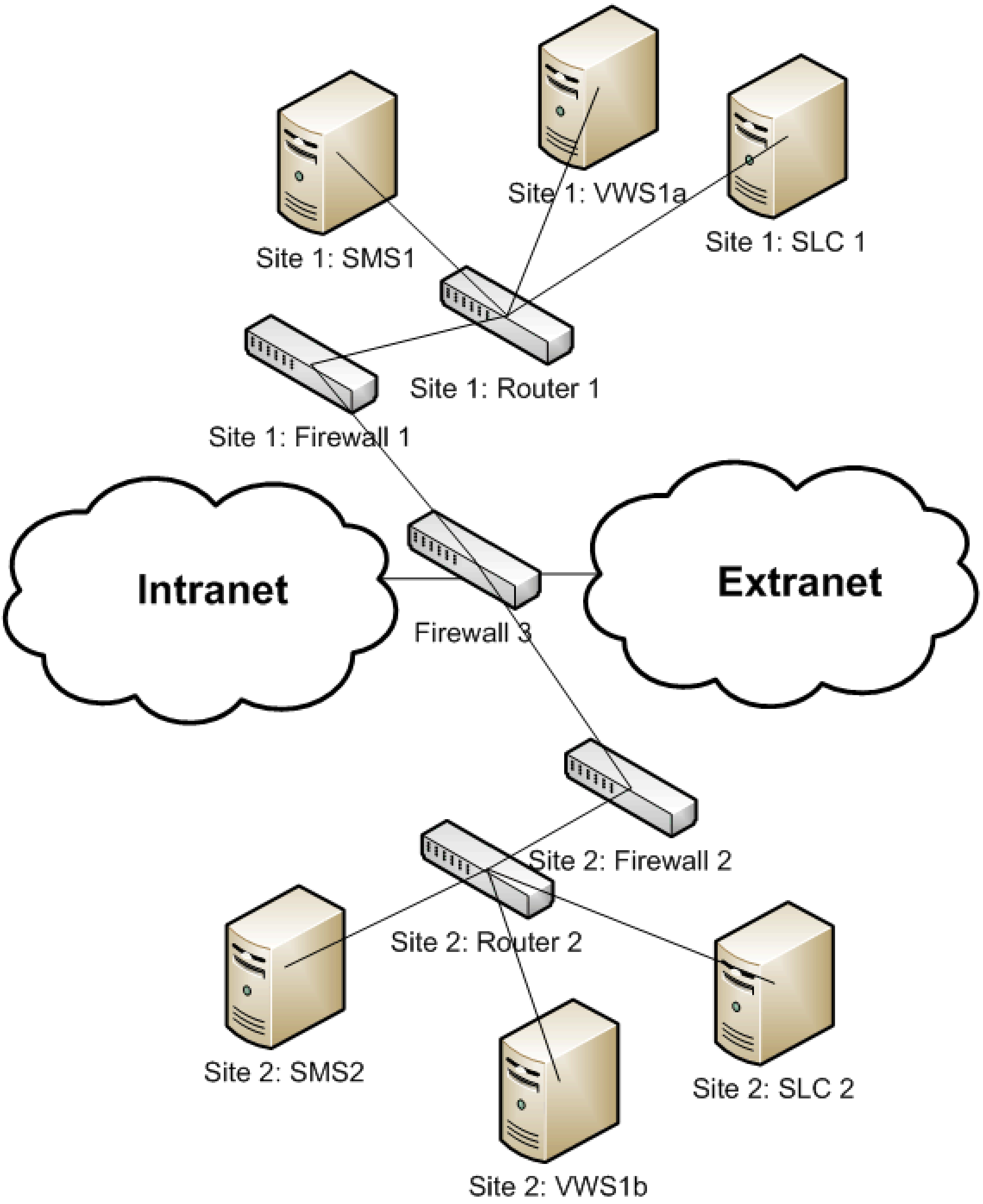
When considering a disaster recovery strategy for the SMS, the requirement for sufficient bandwidth to handle fail over in the event of a problem occurring in the primary node is essential.

Firewalls separating DMZ zones provide two essential functions:

- Blocking traffic types known to be illegal
- Providing intrusion containment, should a successful attack take over processes or processors

Network Access

The product specific network access should be controlled by a firewall on the following interfaces: provisioning, diameter, SOAP, REST, and the screen access for SMS, ACS, CCP and VPN.



Operation System and Database Security

Oracle Solaris Security

This section describes how to install and configure the OS infrastructure component securely for Convergent Charging Controller.

For installation of Convergent Charging Controller on Solaris, Oracle Solaris 11 Security Guidelines provides general guidelines for a secure default configuration. Exceptions are described in more detail in *Installation Guide*. This guide also describes the installation and configuration of any third-party software.

Oracle Database Security

This section describes how to securely install and configure the database infrastructure component.

For a secure installation of the database, refer to *Oracle 12c Database Security Guide*. Archive logging should be enabled on the SMS and VWS as explained in *Oracle Database Administrator's Guide*. This allows a second layer of redundancy. More product specific information is available in *Installation Guide*.

Example configuration files for the database can be found in *Installation Guide*.

The product is designed to be easily adapted and flexible. Depending on the node type (SMS, VWS, or SLC) and the services configured, a number of options to optimize the security of the system are possible. More information on these options is provided in this document.

Oracle Security Documentation

Overview

To implement security, Convergent Charging Controller uses other Oracle products, such as Solaris and the Oracle Database. See the following documents:

- *Oracle Solaris 11 Security Guidelines*
- *Oracle 12c Database Security Guide*
- *Oracle 12c Database Administrator’s Guide*

Oracle documentation is available from Oracle Help Center: http://docs.oracle.com

Chapter 2

Performing a Secure Convergent Charging Controller Installation

Chapter Overview

Introduction

This chapter describes how to install the Convergent Charging Controller and provides overall guidelines to configure the platform components securely.

The installation of the product is done through the use of the Convergent Charging Controller Installation Manager. The usage is described in *Installation Guide*.

In this chapter

This chapter contains the following topics.

Installing Convergent Charging Controller Securely

Pre-Installation Configuration

The planning and preparation required prior to installing Convergent Charging Controller is explained in the pre-installation tasks of *Installation Guide*.

Installing Securely

When installing Convergent Charging Controller using the installer, you can choose to install:

- Each component separately
- Only the packages
- The packages and some basic component configuration
- A full installation which includes all of the packages, basic component configuration and installation of the service templates

For the first three options, the installation will need to be correctly configured to interact with the non Convergent Charging Controller elements in the network. The default parameters will need to be modified and are documented in the component administration guides.

By choosing to install each component separately, you should be aware of the component dependencies, which are described in the component release notes and *Installation Guide*.

Installing only the packages will allow you to configure only what is required by your business without the need to be concerned with the component dependencies.

Post-Installation Configuration

Post-install Security

This section documents any post-installation security amendments.

After the installation of the full platform, some security actions need to be undertaken:

- Change the default password for the all x_oper usernames on each product server:
  - acs_oper
  - smf_oper
  - ebe_oper
  - ccs_oper
  - uis_oper
  - upc_oper
  - rim_oper
  - xms_oper
  - lcp_oper
  - is41_oper
  - ses_oper
- Ensure that su is used so that if off root permissions are needed, all actions can be tracked.
- Set the security levels of the file and directory permissions of /IN and all child sub-directories:
  - All Convergent Charging Controller installed directories need to be set to permission level 750.
  - All executables need to be set to permission level 750.
  - All other files need to be set to permission level 640.
  - The system and application password stored in the /etc/shadow file are encrypted.
- Set the password policy "all passwords for system users and application users should be changed."
- Disable remote access for root user.
- Network
  - Only essential traffic should be allowed, especially on the Convergent Charging Controller external network.
  - Network requirements are described in *Installation Guide*, where more specific information about latency, bandwidth, security, redundancy and routing can be found.
  - It is recommended that an internal LAN is used for the HTTP/SOAP traffic from the VWS and SMS to the SLC nodes, if available.
  - Use an external encrypted connection (VPN, SSL,...) for the HTTP/SOAP/REST traffic coming from external system.
  - Make sure that the internal networks described in *Installation Guide* are only reachable by the Convergent Charging Controller servers and any directly linked servers, such as a third-party billing server, in the case of converged billing.
  - The access for administration of the platform is enabled on the management network through secure protocols only: ssh, sftp, scp.
  - Protocols such as ftp and telnet are blocked from external networks.
  - To allow easy access for the Oracle Advanced Customer Care VPN, check with their latest requirements.
  - For REST security, refer *REST Technical Guide*.

Convergent Charging Controller Backup

Backup Overview

Database

- Enable database archive logging on the SMS and VWS nodes.

- Make sure that database backups are taken from the SMS and the non-active of each VWS pair. These live backups need to be planned in off peak hours to keep the impact of the additional traffic as low as possible. See Oracle *Database Backup and Recovery User's Guide* for more information.
- The Oracle Secure Backup literature provides extensive information on how to securely backup your data.

Flat file

Run the Remote Diagnostic Agent on all Convergent Charging Controller nodes. The tool will collect flat file configuration and other useful system information. For more information, see Oracle Support.

The following configuration items are described in *Installation Guide*:

- On each node, add SSH host keys to the SSH known hosts file, and set SSH StrictHostKeyChecking for user smf_oper on each node. More detailed information on this topic can be found in Oracle Support Documentation.
- Set up IP addresses and hostnames for servers.
- Update the tablespace storage allocation on each node in accordance with system implementation type.
- Update Oracle SGA parameters on each node.
- Set shared memory limits for the Convergent Charging Controller system.

Chapter 3

Implementing Security

Chapter Overview

Introduction

This chapter provides an overview of the threats that the system is designed to counter and how the individual security features combine to prevent attacks.

To prevent loss and corruption of data, the design of the product is discussed together with a number of the implementation options.

In this chapter

This chapter contains the following topics.

Product Design

Functional Layers

The design of Convergent Charging Controller can be viewed in multiple functional layers. On the server, which is designed to provide redundancy, there is:

- The VWS 2N design. The VWS nodes are always installed as a pair (primary and secondary) where the secondary VWS node works in active stand-by mode at the application level.
- The SMS node or the SMS cluster. The SMS cluster can be installed in either active/active or active/passive mode.
- The SLC nodes. All SLC nodes are designed to receive the same data through replication of the database.

At the application level additional functionality is provided:

- All SLC have a read–only database. Writes to these databases are only allowed through replication application, which is controlled by the SMS
- Data update requests from the network coming in through the SLCs are sent to the SMS and from SMS pushed through replication to all nodes that require the data.
- In the case where SMS and VWS data inconsistency or loss occurs, the master subscriber data is held on the SMS and the error can be corrected by the use of the replication and resynchronization mechanisms: options include: enhanced, compare and full resynchronization.
- PI commands are executed in serial mode to prevent data inconsistency.

Implementation Options

Common Options

This section focuses on the most common implementation options. To prevent data loss, some examples of the most common implementation strategies are:

- Usage of internal SSDs storage for SLCs, VWSs, and SMS with a data redundant and fast RAID configuration.
- Usage of disk arrays for SMS. Install the VWSs primary and secondary on a different disk array.
- Raid configuration on all nodes, which are also focused on data redundancy, for example, RAID 10 or 0+1.
- Geographical spread of servers over several locations to prevent a service outage in event of a catastrophic failure at a site. Make sure the network requirements, as described in the installation guide, are also followed for inter-site connectivity.
- The implementation of Oracle Disaster Recovery solution can provide an extra layer of security. For information on how to setup such a solution, see Oracle *Database Backup and Recovery User's Guide*.
- Activation of database logs.

Access Control Mechanism

Rejection Levels

To prevent overload of the systems coming from the external network, connection rejection levels can be set. The rejection level on the interfaces will reject all new incoming traffic on the specified interface.

Interfaces also need to be considered with network details such as IP addresses, ports, and point codes required to connect the user or network element to the product. The technical and operational guides provide more information on how to configure traffic rejection levels and network parameters.

The kernel settings are a deeper layer of protection for your systems. See *Advanced Control Services Technical Guide* for a collection of kernel settings and *Installation Guide* for example values.

Configuring and Using Authentication

Introduction

This topic explains how to configure the authentication mechanism.

Command Line

The database implementation for Convergent Charging Controller uses Oracle Solaris command line authentication to enable users to connect to systems.

The operating system permits the database to use information it maintains to authenticate users. This has the following benefits:

- Once authenticated by the operating system, users can connect to the Oracle systems more conveniently, without specifying a user name or password. For example, an operating-system-authenticated user can invoke SQL*Plus and skip the user name and password prompts by entering the following:

  ```
  SQLPLUS /
  ```
- With control over user authentication centralized in the operating system, the Oracle database does not need to store or manage user passwords, though it still maintains user names in the database.

- Audit trails in the database and operating system can use the same user names.

For more information on this subject, see *Oracle Database 2 Day + Security Guide*.

GUI Access

For all screens that can be started independently (VPN, CCP, ACS, SMS), usernames and passwords are setup by the master user through the Service Management System GUI.

When logging on, these passwords are encrypted before sending over the network to the SMS.

Configuring and Using Access Control

Authorization Systems

This section explains the authorization system used to control access to data, resources and processes for Convergent Charging Controller users.

The Convergent Charging Controller system administrator can set the resource limits for each user through the GUI. Defining roles and creating the appropriate user templates for them on the system is advised. More information on this topic and on how to set this up is available can be found in these guides:

- *Service Management System User's Guide*
- *Advanced Control Services Technical Guide*

It is important when setting up a new MNVO Telco ACS customer in a MVNE that the following configuration options are considered:

- Create a ‘Termination Number Range Rule’ for this new Telco ACS customer.   See *Advanced Control Services User's Guide*.
- To select **Own Range** in the **Termination Number Range Rules** frame of the ACS New Customer screen, refer to *Advanced Control Services User's Guide*.
- Never grant level 7 access.

For network access by a non-administrator, it is recommended that you:

- Work with a VPN connection.
- Connect on the external IP address defined for each server.

More details about the configuration of network ports for the product can be found on **Oracle Support.** This information can be used to restrict network traffic rules and control access to the network to a specific subset of known network connections.

Another layer of network security can be achieved by separating the different network domains, which can be achieved by using a number of virtual LANs, designed to carry very specific traffic such as:

- Management
- Billing
- Internal
- Signaling
- Cluster Inter-connect

It is advised, for performance reasons, that cluster inter-connect is separated from the other networks.

Configuring and Using Security Audit

About Middleware

Convergent Charging Controller is based on Oracle Database middleware. The security audit capabilities of this middleware are utilized to provide the ability to audit Convergent Charging Controller at the system level.

For more information on database audit, refer to *Oracle Database Security Guide* for information on guidelines for auditing.

You can enable the User Audit features to get more visibility of the security status of the system, which will allow you to take remedial action if required.

Security Considerations for Developers

Developer Information

This section provides information useful to developers using the Oracle Communications Convergent Charging Controller Software Development Kit and PI programming options.   For more information, see *Oracle Communications Convergent Charging Controller SDK Developer’s Guide* and *Oracle Communications Convergent Charging Controller Provisioning Interface User's & Technical Guide*.

- General vulnerabilities such as buffer overflow, error exceptions, and SQL injections must be prevented and/or correctly processed.   Guidelines for secure coding can be found at:

  The CERT C++ Secure Coding Standard available at the CERT website: https://www.cert.org/
- Oracle Multithreaded Programming Guide when using Oracle T series hardware

Through the SDK, new database tables can be created. For secure setup and usage of database tables, see *Oracle Database Security Guide*.

Appendix A

Secure Deployment Checklist

Checklist

The following security checklist includes guidelines that help secure your database:

- Install only what is required.
- Lock and expire default user accounts.
- Enforce password management.
- Enable data dictionary protection.
- Practice the principles of least privilege:
  - Grant necessary privileges only.
  - Revoke unnecessary privileges from the PUBLIC user group.
  - Restrict permissions on run-time facilities.
- Enforce access controls effectively and authenticate clients stringently.
- Restrict network access:
  - Use a firewall.
  - Never poke a hole through a firewall.
  - Protect the Oracle listener.
  - Monitor listener activity.
  - Monitor who accesses your systems.
  - Check network IP addresses.
  - Encrypt network traffic.
  - Harden the operating system.
- Apply all security patches and workarounds.
- Contact Oracle Security Products if you come across vulnerability in Oracle Database.

Refer to the security checklist in *Oracle Database Security Guide*.