Oracle® Diameter Signalling Router (DSR)

Security Guide

7.1.1

[Part Number]

January 22, 2016

ORACLE

Contents

This document provides guidelines and recommendations for configuring the Oracle Communications Diameter Signalling Router (DSR) to enhance the security posture of the system. The recommendations herein are optional and should be considered along with your organizations approved security strategies. Additional configuration changes that are not included herein are not recommended and may hinder the product's operation or Oracle's capability to provide appropriate support.

1.1 Audience

This Guide is intended for administrators responsible for product and network security.

1.2 Related Documentation

For more information see the following documents in Oracle Communications Diameter Signalling Router documentation set.

[1] E-63628, Operation, Administration, and Maintenance (OAM) Guide

[2] E-53474, Alarms, KPIs, and Measurements Reference

[3] E-63630, DSR Administration Guide

[4] E-53488, DSR 7.1.x Base Hardware and Software Installation Procedure

[5] E-60310, DSR 7.1.x Upgrade Procedure

2. DSR Security Overview

This chapter provides an overview of Oracle Diameter Signalling Router (DSR) security.

2.1 Accessing the DSR system

There are three ways a user can access the DSR System.

i. Web browser GUI – The client access to the TOE GUI for remote administration requires a web browser supporting a TLS 1.1 enabled session to the TOE. Officially IE is the only supported web browser, and both cookies and java script must be enabled. When user access the DSR system via GUI interface the below screen is presented. The screen will provide username and password fields to enter the user credentials, and click on “Log In” button to log in to DSR GUI.

Figure 1: DSR Login Page

The successful login to the GUI will be indicated by display of the DSR home page as shown below. To logout, the user can select with the mouse the upper-right link labelled “Logout”.

Figure 2: DSR Home Page

ii. CLI via SSH client - Normal login access is remote through network connections. The client access to the command line interface (CLI) is with a SSH capable client such as PUTTY, SecureCRT or similar using the default administrative login account (admusr). SSH login is supported on the management interface. To logout, the user can enter the command “logout” and press the enter key.

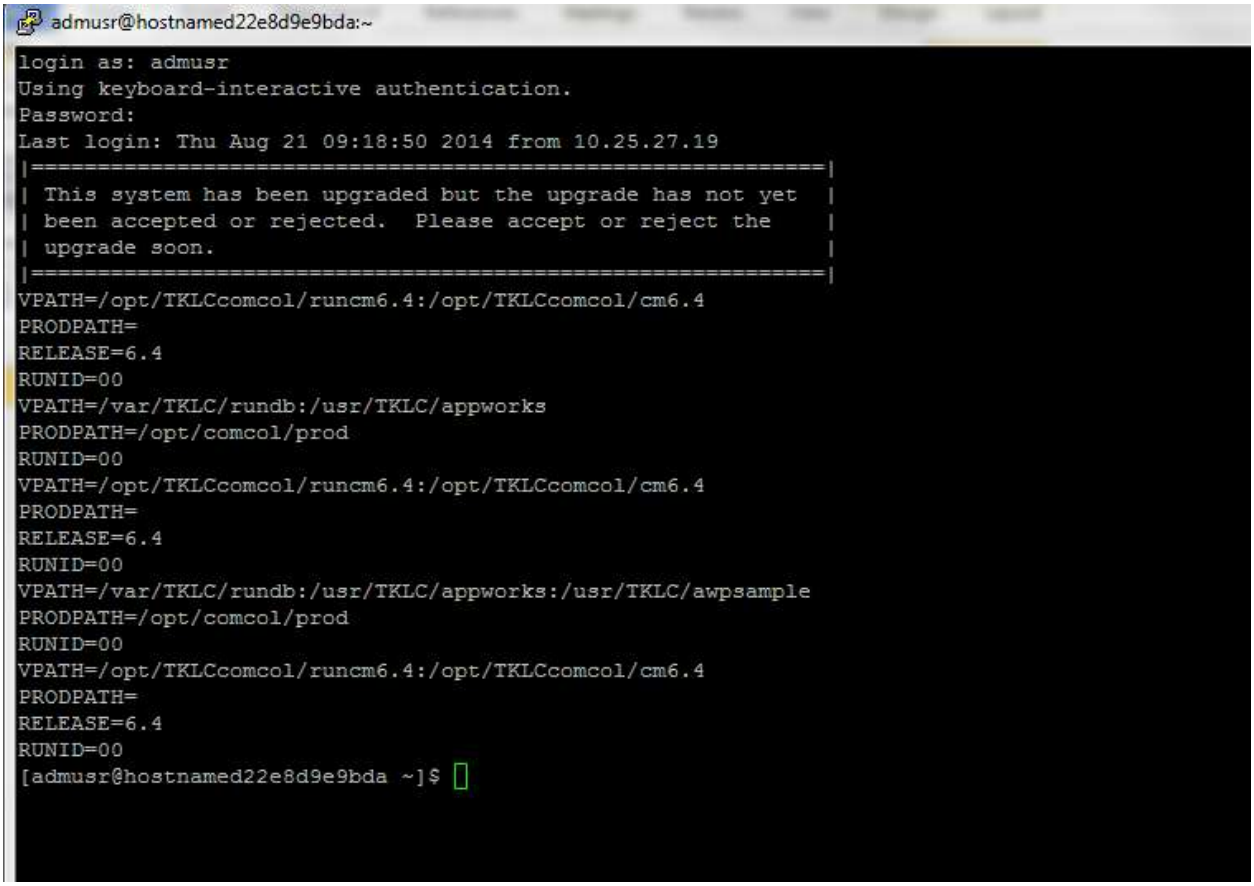


Figure 3: CLI Login Screen

iii. Local access is supported by a hardware connection of a monitor and a key board. The local access supports CLI only.
The successful login is indicated by a display of a command line prompt containing userid @host name followed by a $ prompt.

There is no requirement to add additional users, but adding users is supported.

Figure 4: Picture of Front of the Blades showing local terminal connection in the upper left for each blade

Figure 5 - Custom terminal key board connector cable

Figure 6 - Picture showing custom cable connection for terminal key board

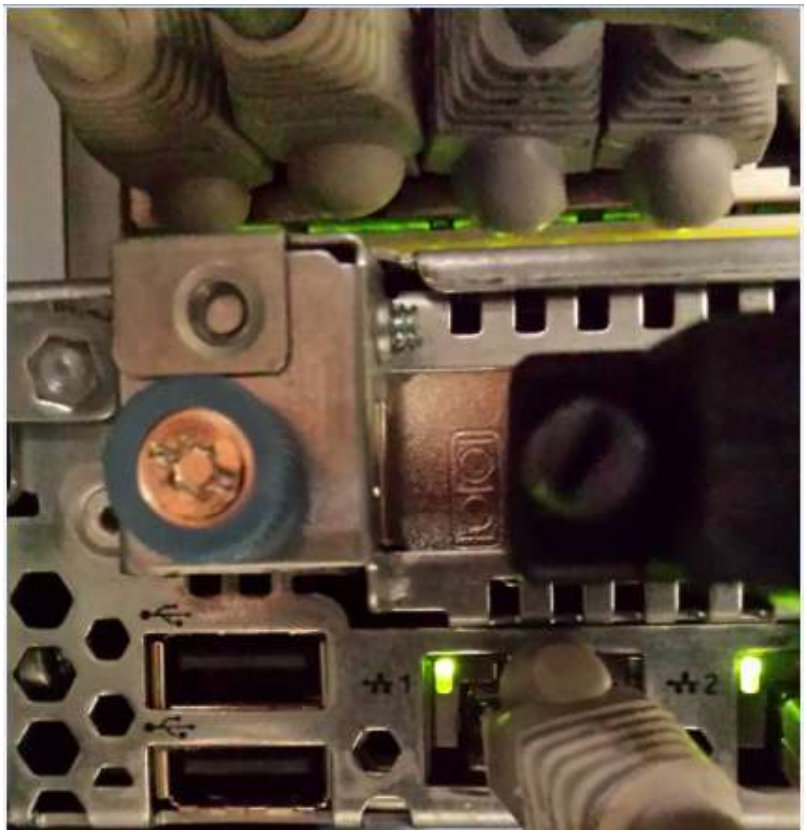


Figure 7 - USB connection for keyboard connection to Rack Mount Server

Figure 8 - Terminal Video connection on Rack Mount Server

2.2 Basic Security Considerations

The following principles are fundamental to using any application securely:

- **Keep software up to date.** This includes the latest product release and any patches that apply to it. Consult with your Oracle support team to plan for DSR software upgrades.
- **Limit privileges as much as possible.** Users should be given only the access necessary to perform their work. User privileges should be reviewed periodically to determine relevance to current work requirements.
- **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.
- **Learn about and use the DSR security features.** See Chapter 3 "Implementing DSR Security" 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" Web site:

  http://www.oracle.com/technetwork/topics/security/alerts-086861.html

2.3 Overview of DSR Security

The DSR is developed with security in mind and is delivered with a standard configuration that includes Linux operating system security hardening best practices. These practices include the following security objectives;

- Attack Surface Reduction
- Attack Surface Hardening
- Vulnerability Mitigation

2.4 Recommended Deployment Configurations

The DSR is deployed in carrier's and service provider's core networks and provides critical signalling routing functionality for 4G, LTE and IMS networks. The solution is based on Linux servers and is highly scalable to accommodate a wide range of capacities to address networks of various sizes. A DSR node is comprised of a suite of servers and related Ethernet switches that create a cluster of servers operating as a single Network Element. It is assumed that firewalls are established to isolate the core network elements from the internet and from partner networks. See figure Figure 9, Generic DSR Deployment Model for a generic model of the deployment strategy.

In addition to the firewalls mentioned above, the DSR system provides additional security capabilities including Access Control Lists (ACL) functionality at the demarcation switch, VLAN or physical separation of administrative and signalling traffic, and IP Tables functionality at the servers for local firewalling.

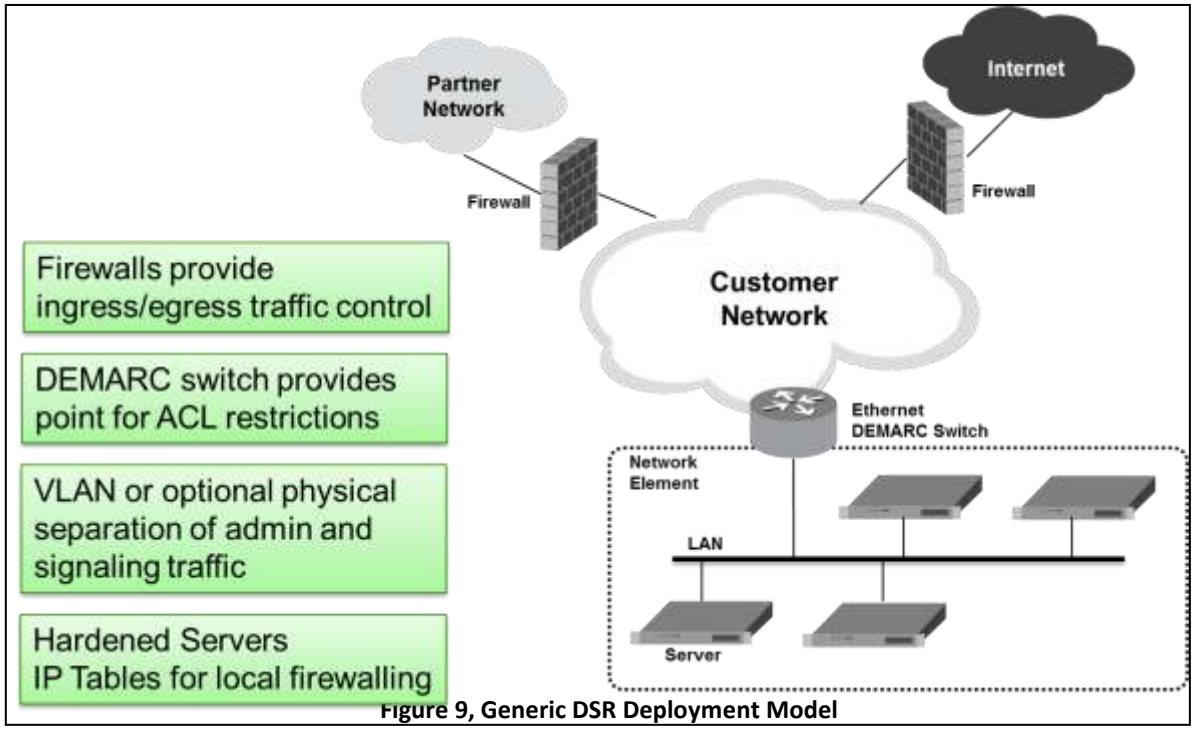


Figure 9, Generic DSR Deployment Model

3. Implementing DSR Security

This chapter explains security related configuration settings that may be applied to the DSR.

3.1 Standard Features

This section explains the security features of the Oracle Diameter Signalling Router (DSR) available to the Administrative User through the application Graphical User Interface (GUI) using a compatible web browser.

3.1.1 User Administration

There is a pre-defined user and group that are delivered with the system for setting up the groups and users by the customer.

User	Group	Description
guiadmin	**admin**	Full access (read/write privileges) to all functions including administration functions.

The **User Administration** page enables the administrator to perform functions such as adding, modifying, enabling or deleting user accounts. Each user that is allowed access to the user interface is assigned a unique **Username.** This username and associated password must be provided during login. After three consecutive, unsuccessful login attempts, a user account is disabled. The number of failed login attempts before an account is disabled is a value that is configured through **Administrations> Options.**

Each user is also assigned to a group. A user must have user/group administrative privileges to view or make changes to user accounts or groups.

For more details on user administration, see page 12 in [1] E-63628, Operation, Administration, and Maintenance (OAM) Guide.

3.1.1.1 Establishing Groups and Group Privileges

Each user is assigned to a group. Permissions to a set of functions are assigned to the group. The permissions determine the functions and restrictions for the users belonging to the group. The “Groups Administration” page enables you to create, modify and delete user groups.

The permissions in this page are grouped into the below sections.

a. Global Action Permissions
b. Administration Permissions
c. Configuration Permissions
d. Alarms & Events Permissions
e. Security Log Permissions
f. Status & Manage Permissions
g. Measurements Permissions
h. IPFE Configuration Permissions
i. Communication Agent Configuration Permissions
j. Communication Agent Maintenance Permissions
k. Diameter Configuration Permissions

For more details on the permissions available for the above groups please see the section **Group Administration,** page 19, in [1] E-63628, Operation, Administration, and Maintenance (OAM) Guide.

For non-administrative users, a group with restricted access is essential. To prevent non-administrative users from setting up new users and groups, be sure User and Group in the Administration Permissions section are unchecked.

Permissions:

Resource	View	Insert	Edit	Delete	Manage
Global Action Permissions	☐	☐	☐	☐	☐
Administration Permissions	☐	☐	☐	☐	☐
General Options	☐		☐		
Users	☐	☐	☐	☐	☐
Groups	☐	☐	☐	☐	
Sessions	☐			☐	
Certificate Management	☐	☐	☐	☐	
Authorized IPs	☐	☐	☐	☐	
SFTP Users	☐	☐	☐	☐	
Software Versions	☐				
ISO Deployment	☐		☐		☐
Software Upgrade	☐		☐		☐
Remote LDAP Authentication	☐	☐	☐	☐	
Remote SNMP Trapping	☐		☐		
Remote Export Server	☐	☐	☐	☐	☐
DNS Configuration	☐		☐		
Licenses	☐	☐			

3.1.1.2 Creating Users and assigning to Groups

Prior to adding a User, determine which user group the user should be assigned based on their operational role. The group assignment determines the functions that a user may access. A user must have user/group administrative privileges to view or make changes to user accounts or groups. The administrative user can set up or change user accounts and groups, enable or disable user accounts, set password expiration intervals, and change user passwords.

The Insert User page displays the following elements.

Element	Data Input
Username	String (5 – 16 characters)
Group	Provisioned Groups(Default: admin)
Authentication Options	Check box format, Remote Authentication / Local Authentication
Access Allowed	Check box format
NE Filter	Check box format
NE Filter Preset	Default: All
Maximum Concurrent Logins	Range 0-50, Default:1
Session Inactivity Limit	Range: 0-120, Default:120
Comment	Range 0 -64 characters

For more details on these elements please refer page 12 in [1] E-63628, Operation, Administration, and Maintenance (OAM) Guide.

User administration page let users to perform the below actions.

- Add a New User
- View User Account Information
- Update User Account Information
- Delete a User
- Enable / Disable a User Account
- Changing a User's Assigned Group
- Generate a User Report
- Change Password

For the details on how to perform these actions, please refer *pages 13- 19* in [1] E-63628, Operation, Administration, and Maintenance (OAM) Guide.

3.1.2 User Authentication

Users are authenticated using either login credentials or Single Sign-On. See **Passwords** section under **Administration** in OAM guide for more details on password setup. See **Single Sign-On Administration** in [1]E-63628, Operation, Administration, and Maintenance (OAM) Guide for details on single sign-on setup.

3.1.2.1 Local Password Management

3.1.2.1.1 Changing Default Passwords for DSR Administrative account

The System Installation procedure will create the default accounts listed below:

- GUI "**guiadmin**"
- CLI "**root**"
- CLI "**admusr**"

The System installation procedure will also convey the passwords for the above accounts. As a security measure, these passwords must be changed.

For changing the default password of "guiadmin" account, See [1]E-63628, Operation, Administration, and Maintenance (OAM) Guide page 17 on "Passwords".

For changing the default passwords of CLI account, please see the section "3.2.3 Changing Default Passwords" under non-standard configurations.

3.1.2.1.2 Setting up Password Complexity

A valid password must contain from 8 to 16 characters. A password must contain at least three of the four types of characters: numerics, lower case letters, upper case letters, or special characters (! @ # $ % ^ & * ? ~). A password cannot be the same as the Username or contain the Username in any part of the password (for example, Username=jsmith and password=$@jsmithJS would be invalid). A password cannot be the inverse of the Username (for example, Username=jsmith and password=$@htimsj would be invalid). By default, a user cannot reuse any of the last three passwords. This feature can be configured with the required setting for the "MaxPasswordHistory" field in the "Administration → General Options" page.

3.1.2.1.3 Setting up Password Aging Parameters

Password expiration is enforced the first time a user logs in to the user interface. During initial user account setup, the administrative user grants the user a temporary password. When the user attempts to log in for the first time, the software forces the user to change the password. The user is redirected to a page that requires the user to enter the old password and then enter a new, valid password twice.

The user interface provides two forms of password expiration. The password expiration can be forced when a new user logs in for the first time with a temporary password granted by

the administrator. The administrative user can configure password expiration on a system-wide basis. By default, password expiration occurs after 90 days.

See the section **Passwords** for detailed steps on setting up password aging in [1] E-63628, Operation, Administration, and Maintenance (OAM) Guide page 17.

3.1.2.1.4 Restrict Concurrent GUI Logins

The **Insert User** page has "Maximum Concurrent Logins" field; the value in this field indicates the maximum concurrent Logins per user per server. This feature cannot be enabled for users belonging to Admin group. The range in this field can vary from 0 to 50.

User Administration page has "Concurrent Logins Allowed" field. And the value in this field is the concurrent number of logins allowed.

3.1.2.2 External Authentication

Users can be authenticated remotely where an external LDAP server is used to perform authentication.

3.1.2.2.1 LDAP Authentication

The system provides the feature to configure, update or delete LDAP authentication servers. This feature is available under **Remote Servers** option. If multiple LDAP servers are configured, the first available server in the list is used to perform authentication. Secondary servers are only used if the first server is unavailable.

The below are the elements to configure LDAP server.

a. Hostname

b. Account Domain Name

c. Account Domain Name Short

d. Port

e. Base DN

f. Password

g. Account Filter Format

h. Account Canonical Form

i. Referrals

j. Bind Requires DN

See page 54 in [1]E-63628, Operation, Administration, and Maintenance (OAM) Guide for more details.

3.1.2.3 System Single Sign-On

Single Sign-On allows the user to log into multiple servers within a zone by using a shared certificate among the subject servers within the zone. Once a user has successfully authenticated with any system in the SSO domain, the user can access other systems in the SSO zone without the need to re-enter authentication credentials. When two zones in the SSO domain exchange certificates, a trusted relationship is established between the zones, as well as between all systems grouped into the zone expanding the authenticated login capability to servers in both zones. For details on configuring single sign-on zones please see [1]E-63628, Operation, Administration, and Maintenance (OAM) Guide, page 35.

3.1.3 Login and Welcome Banner Customization

When logged in to the DSR GUI as administrator user, the Options page under Administration enables the administrative user to view a list of global options.

The **LoginMessage** field is the configurable portion of login message seen on the login screen. The admin user can enter the message in this field as required. Similarly **WelcomeMessage** field can be used by admin user to enter the message seen after successful login.

3.1.4 SNMP Configuration

The application has an interface to retrieve KPIs and alarms from a remote location using the industry-standard Simple Network Management Protocol (SNMP) interface. Only the active Network OAM&P server allows SNMP administration. For more details see page 57 on **SNMP Trapping** in OAM guide.

The Active Network OAM&P server provides a single interface to SNMP data for the entire network and individual servers interface directly with SNMP managers. The application sends SNMP traps to SNMP Managers that are registered to receive traps. IP addresses and authorization information can be viewed and changed using the **SNMP Trapping** page.

For SNMP to be enabled, at least one Manager must be set up. The system allows configuring up to 5 different Managers to receive SNMP traps and send requests. These could be either a valid IPv4 address or a valid hostname. IP address is a numeric identifier comprised of four 8-bit octets separated by periods. The first octet must be between 1 – 255 and last 3 octets must be between 0-255. Hostname must be unique and case-insensitive, max. 20 – Character string. Valid characters are alphanumeric and minus sign. Must start with an alphanumeric and end with an alphanumeric.

The **Enabled Versions** field in this page lets user to pick the specific version of SNMP. The traps can be enabled or disabled collectively or independently from individual servers, by checking the traps enabled check box in this page.

The **SNMP Trapping** page provides the below functionalities.

- Add an SNMP Manager
- View SNMP settings
- Updating SNMP settings
- Delete SNMP manager

For more details on these actions please refer to [1]E-63628, Operation, Administration, and Maintenance (OAM) Guide *pages 61-62.*

3.1.4.1 Selecting Versions

Enabled Versions field in this page lets user to pick the specific version of SNMP. Options are

- SNMPv2c: Allows SNMP service only to managers with SNMPv2c authentication.
- SNMPv3: Allows SNMP service only to managers with SNMPv3 authentication.
- SNMPv2c and SNMPv3: Allows SNMP service to managers with either SNMPv2c or SNMPv3 authentication. This is the default option.

The recommended option is SNMPv3 for secure operation.

3.1.4.2 Community Names / Strings

When the SNMPv2c is enabled in the **Enabled Versions** the SNMPV2c Community Name is a required field. This is the configured Community Name. This string can be optionally changed. The maximum length of Community Name (String) is 31 characters.

3.1.5 Authorized IPs

IP addresses that have permission to access the GUI can be added or deleted on the Authorized IPs page. If a connection is attempted from an IP address that does not have permission to access the GUI, a notification appears on the GUI. This feature cannot be enabled until the IP address of the client is added to the authorized IP address table. You must add the IP address of your own client to the list of authorized IPs first before you enable this feature.

Enabling Authorized IPs functionality prevents unauthorized IP addresses from accessing GUI. See [1] E-63628, Operation, Administration, and Maintenance (OAM) Guide, page 40 for more details on how to enable this feature under Authorized IPs section.

3.1.6 Enabling IPsec

Internet Protocol Security (IPsec) provides network layer security protocols used for authentication, encryption, payload compression, and key exchange. IPsec provides Host-to-Host encrypted connections or Network-to-Network packet tunnelling.

Network traffic between two end-points is encrypted and decrypted by authenticated hosts at the end-points, using a shared private key. The shared private key forms a Security Association that can be automatically changed by Security Policies based on traffic volume, expiry time, or other criteria.

IPsec will work for both IPv4 and IPv6. DSR IPsec uses the Encapsulating Security Payload (ESP) protocol for encryption and authentication. ESP also provides authentication of the encrypted packets to prevent attacks by ensuring the packet is from the correct source.

Internet Key Exchange (IKE) is used to exchange secure keys to set up IPsec security associations. See [3] E-63630, DSR Administration Guide, page 101 for more details on how to enable IPsec under the chapter IPsec.

3.1.7 Certificate Management

The Certificate Management feature allows the user to configure digital security certificates for securing DSR web sessions, user authentication thru secure LDAP over TLS, and secure Single Sign-On authentication across a defined zone of DSR servers. The feature supports certificates based on host name or fully qualified host name.

This feature allows users to build certificate signing requests (CSRs) for signing by a known certificate authority and imported into the DSR. This feature lets the user generate a Certificate Report of individual or all defined certificates.

For details on Certificate Management feature see Certificate Management chapter in [1]E-63628, Operation, Administration, and Maintenance (OAM) Guide page 35.

3.1.8 SFTP Administration

The DSR supports SFTP sessions with external servers for transfer of various files from the DSR. The authentication process requires a digital certificate for authenticating the sessions.

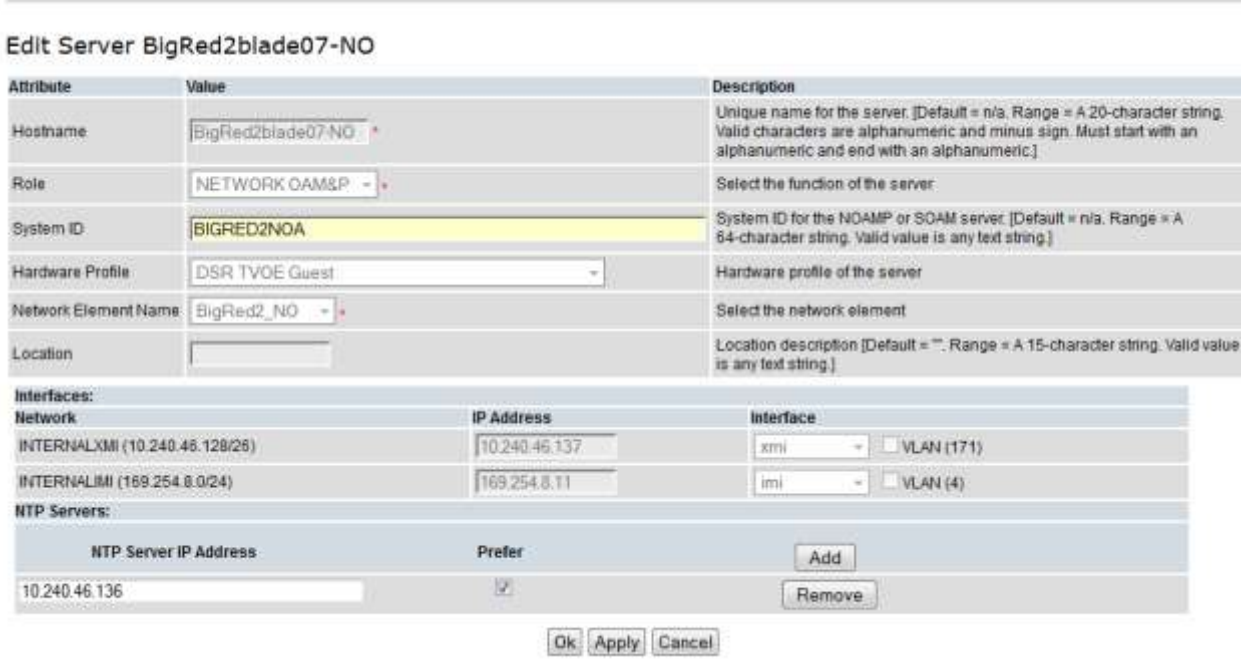
The transfer of files is driven from the external server. Please see SFTP Users Administration in [1] E-63628, Operation, Administration, and Maintenance (OAM) Guide, page 42.

3.2 Non-Standard Configurations

This section explains the security features of the Oracle Diameter Signalling Router (DSR) available to the Platform Administrator through the Linux Command Line Interface (CLI).

3.2.1 Configuring NTP servers

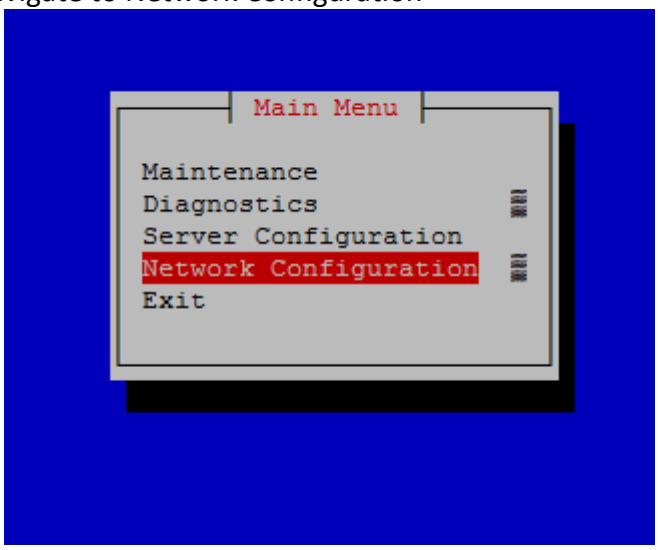
Each Server that is being added at the NOAM server under Administration → Configuration → Servers will have the option to specify the NTP Server details. The NTP Servers field will be visible after selecting a network element. The below screen shot displays a configured server with NTP server details.



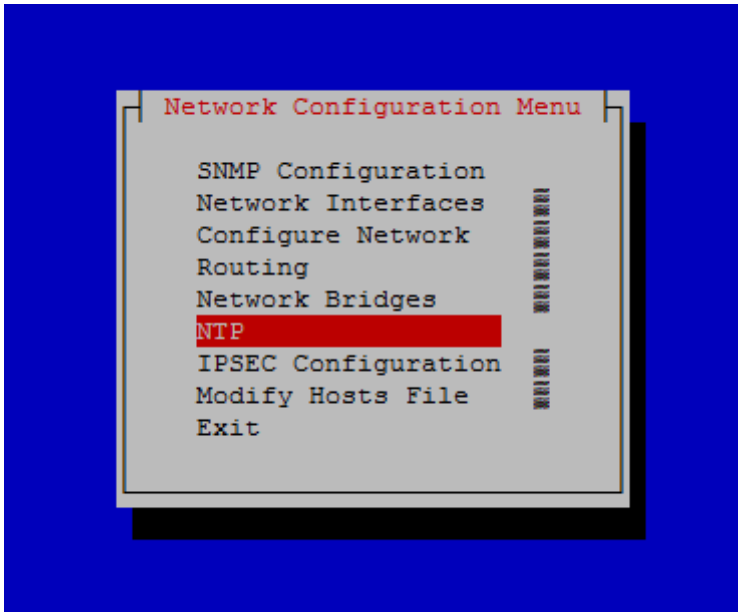
For details on adding a server see "Inserting a server" under **Servers** chapter in [1] E-63628, Operation, Administration, and Maintenance (OAM) Guide, page 80.

Configure NTP for the Host operating system hosting application guest:

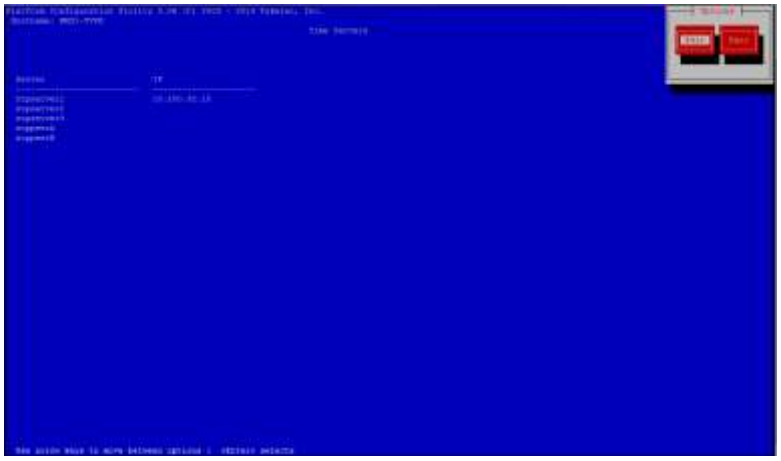
1. Login or switch user to platcfg user on the TVOE server. The platcfg main menu will be shown.
2. Navigate to Network Configuration



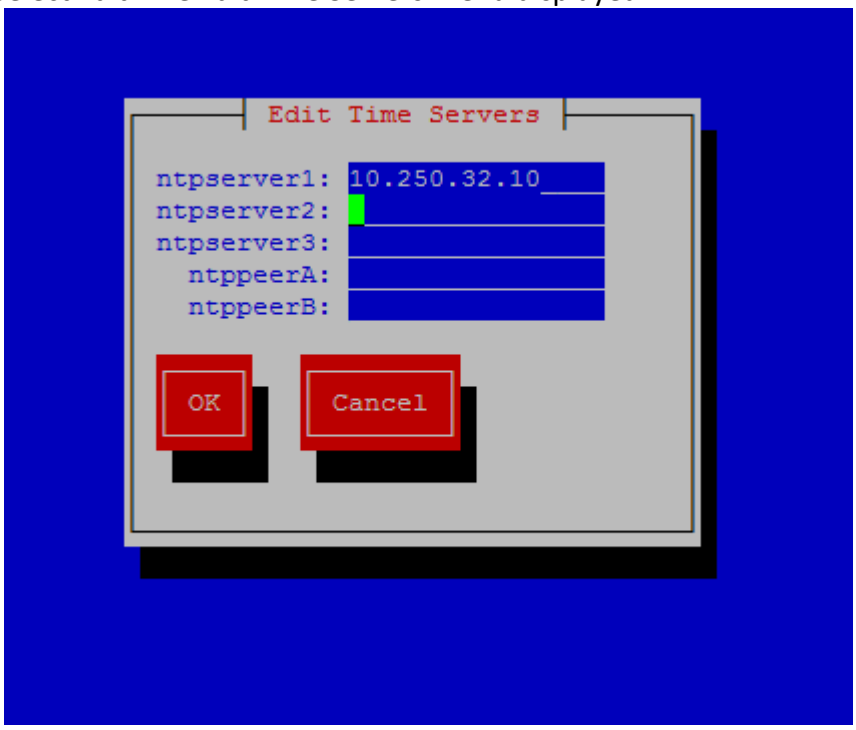
3. Choose NTP.



4. The 'Time Servers' page will now be shown, which shows the configured NTP servers and peers.



5. Select Edit. The Edit Time Servers Menu displayed.



4. Enter the NTP Server information and select “OK” and exit platcfg menu.
5. Ensure that the time is set correctly by executing the steps in the section “Setting the time” section.

3.2.1.1 Setting the time on TVOE server

At the time of DSR installation, the date and time is set on TVOE hosts as follows:

TVOE Management Server: Ensure time set correctly according to the previous procedure.

a) a Login as “admusr” and execute the below commands.

$ sudo /sbin/service ntpd stop

$ sudo /usr/sbin/ntpdate ntpserver1

$ sudo /sbin/service ntpd start

These steps will synchronize the time to the NTP server.

3.2.2 IP Tables

The “iptables” functionality inherent in the DSR Linux operating system provides a network firewall capability. For DSR, the “iptables” configuration provides network traffic isolation for the various networks in the DSR multi-server system. Use of this feature must be authorized by Oracle.

3.2.3 Changing Default Passwords

Procedure to Change Default Passwords for CLI:

1. **Log in as admusr on the source server.**

   login: <admusr> (default administrative user account)

   Password: <current admusr password> (will not display)

   [prompt] $

   [prompt] $ su - root

   Password: <current root password> (will not display)

   [prompt] #

   [prompt] # passwd root

   Changing password for user root.

   New password: <new root password> (will not display)

   Retype new password: <new root password> (will not display)

   passwd: all authentication tokens updated successfully.

   [prompt] #

2. **Change the passwords for each of the accounts being changed:**

   [prompt] # passwd <admusr>

   Changing password for user admusr.

   New password: <new admusr password> (will not display)

   Retype new password: <new admusr password> (will not display)

   passwd: all authentication tokens updated successfully.

   [prompt] #

3. **Repeat step 2 for all accounts that are being changed.**

3.2.4 Configure Password Expiry for OS Users

Use the below procedure to configure password expiry:

1. Login as root on the server

   Login: root

   Password: <current root password>

2. Show the four password security restriction menus hidden in the platcfg menu

   ```
   # platcfgadm --show Security SecPasswordRestrictions SecPasswordRestrictionsUser SecPasswordRestrictionsCommon
   ```

3. Open the platcfg menu by switching to the platcfg user

   ```
   # su – platcfg
   ```

4. Select security form the menu and hit Enter

5. Fill out the following settings:

   Maximum number of days a password may be used: 99999

6. Select OK and hit enter

7. Select exit in each of the menus until a command prompt is reached.

3.2.5 Password Length Configuration for OS Users

1. Login as admusr on the server

   Login: admusr

   Password: <current admusr password>

2. Enter the following command:

   $ sudo su - platcfg

3. Select security form the menu and hit Enter

4. From the menu select “Sec Password Restrictions” option

5. Select “Global Password Restrictions for New Users”. And in the menu displayed fill out the field “Minimum acceptable size for the new password”. Select OK and hit enter

6. Select exit in each of the menus until a command prompt is reached.

3.2.6 Configuring Session inactivity for OS users

Use the below procedure to configure password expiry:

7. Login as admusr on the server

   Login: admusr

   Password: <current admusr password>

8. Enter the following command:

   $ sudo su - platcfg

1. Select security form the menu and hit Enter
2. Select “Idle Terminal Timeout” option in the security menu and enter the desired value in minutes for the “Idle Terminal” Timeout field.
3. Select OK and hit enter
4. Select exit in each of the menus until a command prompt is reached.

3.2.7 Procedure to change Login Display Message

1. Log in as admusr on the source server.

   ```
   login: admusr

   Password: <current admusr password>
   ```

2. Create a backup copy of sshd_config

   ```
   $ cd /etc/ssh

   $ sudo cp sshd_config sshd_config.bak
   ```

3. Edit the sshd configuration file.

   ```
   $ sudo rcstool co sshd_config

   $ sudo vi sshd_config
   ```

   Uncomment and edit the following line:

   ```
   $ Banner /some/path
   ```

   To this:

   ```
   Banner /etc/ssh/sshd-banner
   ```

   Save and exit the vi session.

4. Edit the banner file.

   ```
   $ sudo vi sshd-banner
   ```

   Add and format the desired text. Save and exit the vi session

5. Restart the sshd service.

```
$ sudo service sshd restart
```

6. Test the change. Repeat steps 4 & 5 until the message is formatted correctly.

```
$ sudo ssh <current server name>
```

Verify message line feeds are formatted correctly.

```
$ exit
```

7. Check the files into rcs to preserve changes during upgrades

```
$ sudo rcstool init /etc/ssh/sshd-banner
```

```
$ sudo rcstool ci sshd_config
```

3.2.8 Forcing iLO to use Strong Encryption

Log in as an administrator on to the iLO and execute the below steps.

1. On the Administration tab: click Security from the side menu.

2. On the Encryption tab: under Encryption Enforcement Settings set the Enforce AES/3DES Encryption to enabled.

3. Click Apply. Then log out and wait 30 seconds before logging back in.

3.2.9 rsyslog setup for external logging

Procedure to enable logging to a central server from the NOAMs and SOAMs:

1. Log in as root on the server:
   login: root

   Password: <current root password>

2. Enable remote logging:
   #syslog_config --remote=<IP of remote host to log to>

3. Repeat on all necessary NOAMs and SOAMs

3.3 Ethernet Switch Considerations

This section describes security related configuration changes that could be made to the demarcation Ethernet switches.

3.3.1 SNMP Configuration in Switches

It is essential that all switches have been configured successfully using the procedures in [4]E-53488, DSR 7.1.x Base Hardware and Software Installation Procedure:

- Configure Cisco 3020 switch (netConfig) and/or
- Configure HP 6120XG switch (netConfig) and/or

- Configure Cisco 4948/4948E/4948E-F (netConfig)

Login to the server as root user and list all the configured switches using the below command.

 # netConfig --repo listDevices

Refer to application documentation to determine which switches to add/remove the community string, making a note of the DEVICE NAME of each switch. This will be used as <switch_name>.

For any given switch by switch name, display SNMP community information using the below command:

 # netConfig getSNMP --device=<switch_name>

For any given switch by switch name, display its SNMP trap information using the below command

#netConfig listSNMPNotify --device=<switch_name>

NOTE1: If the reply indicates "**Could not lock device**", enter the following command to clear the lock in order to proceed:
 # netConfig --wipe --device=<switch_name>

(reply **"y"** if prompted)

3.3.2 Configure Community Strings

a. To ADD a community string to ANY switch by switch name, use below command with appropriate switch name

#netConfig addsSNMP –device=<switch name> community=<community string> uauth=RO

b. To DELETE a community string to ANY switch by switch name, use appropriate switch name in the below command

 # netConfig deleteSNMP --device=<switch_name> community=<community_string>

3.3.3 Configure Traps

a. To ADD a trap server, use below command with appropriate switch name

#netConfig addSNMPNotify --device=<switch_name> host=<snmp_server_ip> version=2c auth=<community_string> [traplvl=not-info]

b. To DELETE a trap server, use the below command with appropriate switch name

#netConfig deleteSNMPNotify --device=<switch_name> host=<snmp_server_ip> version=2c auth=<community_string> [traplvl=not-info]

Note: traplvl=not-info in the command is needed only in case of 6120 switch. The switches 4948 or 3020 do not need this field in the above commands.

3.4 Security Logs and Alarms

The Security Log page allows you to view the historical security logs from all configured Security logs are displayed in a scrollable, optionally filterable table. The security logs can also be exported to file management area in .csv format. For more details see Security Log chapter in [1]E-63628, Operation, Administration, and Maintenance (OAM) Guide, page 126.

Application Alarms and Events are unsolicited messages used in the system for trouble notification and to communicate the status of the system to Operations Services (OS). The application merges unsolicited alarm messages and unsolicited informational messages from all servers in a network and notifies you of their occurrence. Security alarms enable a network manager to detect security events early and take corrective action to prevent degradation in the quality of service.

Alarms provide information pertaining to a system‘s operational condition that a network manager may need to act upon. Alarms can have these severities:

- Critical
- Major
- Minor
- Cleared

See chapters “Alarms and Events” and “Security Log” in [1] E-63628, Operation, Administration, and Maintenance (OAM) Guide and [2] E-53474, Alarms, KPIs, and Measurements Reference for more details.

OS level logging is captured in

- /var/log/messages - general system messages
- /var/log/secure – security related messages
- /var/log/httpd (directory) – apache webserver logging

Appendix A: Secure Deployment Checklist

{{{This appendix lists actions that need to be performed to create a secure system. }}}

The following security checklist lists guidelines to help you secure Oracle DSR and its components.

Secure Deployment Checklist

- Change default passwords
- Utilize LDAP for authentication purposes
- Utilize Authorized IP addresses feature
- Use TLS or IPSEC
- Enforce strong password management
- Restrict admin functions to the required few administrator groups
- Restrict network access by using IPTables feature
- Enforce iLO to use strong encryption