



**5620 SAM
SERVICE AWARE MANAGER
14.0 R1**

System Administrator Guide

3HE-10705-AAAA-TQZZA

Issue 1

March 2016

Legal notice

Nokia is a registered trademark of Nokia Corporation. Other products and company names mentioned herein may be trademarks or tradenames of their respective owners.

The information presented is subject to change without notice. No responsibility is assumed for inaccuracies contained herein.

© 2016 Nokia. All rights reserved.

Contents

About this document	12
Part I: 5620 SAM System Administrator overview	13
1 Safety information	15
1.1 Structure of safety statements.....	15
2 5620 SAM System Administrator Guide overview	17
2.1 Overview.....	17
2.2 5620 SAM System Administrator Guide overview.....	17
2.3 5620 SAM system administrator tasks and information map.....	19
2.4 Administrator tasks for application management.....	21
Part II: 5620 SAM security management	23
3 5620 SAM user security	25
3.1 Overview.....	25
5620 SAM user security	27
3.2 Overview.....	27
3.3 User account and group management.....	28
3.4 User activity logging.....	33
3.5 Sample span rule configuration.....	37
3.6 Remote 5620 SAM user access.....	38
3.7 Sample 5620 SAM user authentication configuration.....	41
5620 SAM user security procedures	45
3.8 Workflow to configure and manage 5620 SAM user security.....	45
3.9 To reserve an admin account login.....	48
3.10 To create a scope of command role.....	49
3.11 To create a scope of command profile.....	50
3.12 To create a span of control.....	51
3.13 To create a span of control profile.....	52
3.14 To create a span rule.....	53
3.15 To create a 5620 SAM user group.....	54
3.16 To add or remove workspaces for a user group.....	55
3.17 To create a 5620 SAM user account.....	56

3.18	To copy a 5620 SAM user account.....	58
3.19	To configure global user account, password	58
3.20	To configure the GUI client inactivity timeout	59
3.21	To configure the minimum allowable user name length	60
3.22	To configure authentication failure actions	60
3.23	To configure suspended account actions	61
3.24	To configure automated E-mail notification	61
3.25	To list inactive user accounts.....	62
3.26	To suspend or reinstate a 5620 SAM user account.....	63
3.27	To administratively change the password of a 5620 SAM user	63
3.28	To force a 5620 SAM user password change.....	64
3.29	To change the password of the current 5620 SAM user	65
3.30	To export the local tab preferences of one or more users	66
3.31	To assign local tab preferences to users	67
3.32	To send a broadcast message to 5620 SAM GUI users	68
3.33	To view and manage active 5620 SAM client sessions.....	68
3.34	To disconnect a 5620 SAM-O JMS client connection or remove a durable subscription	69
3.35	To view the user activity log.....	70
3.36	To view the user activity associated with an object	72
3.37	To create a proprietary 5620 SAM login statement	73
3.38	To change the maximum number of concurrent 5620 SAM admin user sessions	73
3.39	To configure the number of allowed client sessions for a client delegate server.....	75
3.40	To enable secure access for remote LDAP users	76
3.41	To enable remote user authorization via RADIUS.....	77
3.42	To enable remote user authorization via TACACS+	79
3.43	To configure 5620 SAM remote user authentication	81
3.44	To change the 5620 SAM Task Manager settings	83
3.45	To export all workspaces and local tab preferences.....	85
3.46	To import workspaces and local tab preferences	86
4	NE user and device security	89
4.1	Overview	89
	NE user and device security	91
4.2	Overview	91
4.3	RADIUS, TACACS+, and LDAP	92
4.4	CPM filters and traffic management	93

4.5	DoS protection.....	94
4.6	DDoS protection	95
4.7	IP security.....	97
4.8	7705 SAR-H firewalls	97
	NE user and device security procedures.....	99
4.9	Workflow to manage NE user and device security	99
4.10	To configure a MAF	101
4.11	To configure a CPM filter	103
4.12	To configure an NE DoS protection policy.....	105
4.13	To view NE DoS protection violations.....	106
4.14	To configure an NE DDoS protection policy	107
4.15	To configure a site user profile.....	110
4.16	To configure a user account on a managed device	111
4.17	To configure a password policy	112
4.18	To configure an NE RADIUS authentication policy.....	113
4.19	To configure an NE TACACS+ authentication policy	114
4.20	To configure an OmniSwitch RADIUS, TACACS+, or LDAP security authentication policy	116
4.21	To configure device system security settings	117
4.22	To configure and manage PKI site security on an NE	120
4.23	To configure a PKI certificate authority profile	123
4.24	To create a file transmission profile	124
4.25	To perform CMPv2 actions	125
4.26	To distribute a license key to all 7705 SAR-H nodes.....	128
4.27	To configure a 7705 SAR-H NE firewall	129
4.28	To configure an NE management access firewall on a 7705 SAR-H	131
4.29	To configure an NE CPM firewall on the 7705 SAR-H	133
4.30	To delete a security policy	134
4.31	To manually unlock a user account	135
4.32	To clear the password history of a user on a managed device	136
4.33	To clear collected statistics on a CPM filter	137
4.34	To manage OCSP cache entries on an NE	138
5	TCP enhanced authentication.....	141
5.1	Overview	141
5.2	TCP enhanced authentication	141
5.3	Workflow to configure TCP enhanced authentication for NEs.....	143

5.4	To configure a global TCP key chain	144
5.5	To distribute global key chains to NEs.....	145
5.6	To verify the distribution of a global key chain to NEs	147
5.7	To identify differences between a global and local key chain policy or two local key chains	147
Part III: 5620 SAM advanced configuration		149
6	5620 SAM component configuration	151
6.1	Overview	151
5620 SAM component configuration		153
6.2	Overview	153
6.3	Changing 5620 SAM default text fields and ID ranges.....	153
6.4	5620 SAM license management	159
6.5	Workflow to configure 5620 SAM components	160
Software and license configuration procedures		163
6.6	To view the 5620 SAM license information.....	163
6.7	To export the 5620 SAM license information to a file	164
6.8	To update the 5620 SAM license in a standalone deployment.....	164
6.9	To update the 5620 SAM license in a redundant deployment	165
6.10	To list the backed-up 5620 SAM license files	168
6.11	To change the default 5620 SAM license expiry notification date	169
System components configuration procedures		171
6.12	To modify the base configuration of all GUI clients	171
6.13	To configure the display of multiple 5620 SAM systems as client GUI login options	172
6.14	To change the default user file locations on a client delegate server	174
6.15	To change the IP address or hostname of a 5620 SAM system component.....	175
6.16	To enable 5620 SAM database backup file synchronization	176
6.17	To modify the default time period of statistics displayed by the Statistics Manager search filters.....	178
6.18	To modify the default time period of statistics displayed on object properties forms.....	179
6.19	To create or configure a format policy	180
6.20	To create or configure a range policy	182
Network management configuration procedures		185
6.21	To configure automatic device configuration backup file removal	185
6.22	To enable alarm reporting to identify duplicate NE system IP addresses	186
6.23	To enable dynamic system IP address updates for 7705 SAR nodes.....	188
6.24	To enable LSP on-demand resynchronization.....	189
6.25	To enable debug configuration file reloading on an NE for mirror services	191

6.26	To configure throttle rates for subscriber trap events	193
6.27	To configure the windowing trap delayer option for subscriber table resyncs	193
6.28	To create a default SNMPv2 OmniSwitch user on a 5620 SAM system	196
	System preferences configuration procedures	198
6.29	To configure 5620 SAM system preferences.....	198
7	5620 SAM database management	205
7.1	Overview	205
	5620 SAM database management	207
7.2	Overview	207
7.3	5620 SAM database	207
7.4	Auxiliary database	208
	5620 SAM database management procedures	209
7.5	Workflow for 5620 SAM database management.....	209
7.6	To view the 5620 SAM database properties	211
7.7	To view the auxiliary database status using the client GUI	212
7.8	To view the auxiliary database status using a CLI.....	213
7.9	To configure the allowed number of Oracle database login attempts.....	214
7.10	To configure Oracle database error monitoring	217
7.11	To configure a size constraint policy.....	217
7.12	To configure an ageout constraint policy	219
7.13	To create a database file policy to manage database log or core dump files.....	221
7.14	To configure the statistics data retention period for the 5620 SAM database	222
7.15	To perform an immediate 5620 SAM database backup using the GUI	223
7.16	To perform an immediate 5620 SAM database backup using a CLI	225
7.17	To back up an auxiliary database	227
7.18	To schedule 5620 SAM database backups	228
7.19	To schedule auxiliary database backups.....	229
7.20	To unlock the Oracle database user account	230
8	5620 SAM system redundancy	233
8.1	Overview	233
	5620 SAM system redundancy	234
8.2	Overview	234
8.3	5620 SAM system redundancy models.....	234
8.4	Redundancy functions.....	240
8.5	Redundancy failure scenarios	247

5620 SAM system redundancy procedures	253
8.6 Workflow to perform 5620 SAM system redundancy functions	253
8.7 To view the 5620 SAM system redundancy status	254
8.8 To view the 5620 SAM auxiliary server status	257
8.9 To perform a server activity switch	259
8.10 To configure 5620 SAM database switchover behavior	260
8.11 To perform a 5620 SAM database switchover using the 5620 SAM client GUI	261
8.12 To perform a 5620 SAM database switchover using a CLI script	262
8.13 To restore analytics server operation after a 5620 SAM database failover or switchover	263
8.14 To enable or disable automatic database realignment	265
8.15 To reinitiate a redundant database using the 5620 SAM client GUI	268
8.16 To reinitiate a redundant database using a CLI script	269
8.17 To configure an IPDR file transfer policy	270
Part IV: 5620 SAM routine maintenance	273
9 5620 SAM routine maintenance overview	275
9.1 Overview	275
9.2 Routine maintenance overview	275
9.3 Routine maintenance guidelines	276
9.4 Obtaining technical assistance	276
9.5 Routine maintenance checklist	277
10 5620 SAM maintenance base measures	281
10.1 Overview	281
Maintenance base measures	282
10.2 Base measures overview	282
10.3 Base measures guidelines	282
10.4 Platform base measures	283
10.5 Inventory base measures	286
10.6 Performance and scalability base measures	286
10.7 Reachability base measures	288
11 Daily maintenance	291
11.1 Overview	291
Daily maintenance information	292
11.2 Viewing and filtering alarms	292
11.3 Backing up the 5620 SAM database and components	292

11.4	Collecting and storing 5620 SAM log and configuration files	293
	Daily maintenance procedures	294
11.5	To monitor incoming alarms	294
11.6	To verify 5620 SAM database information.....	295
11.7	To back up the 5620 SAM log and configuration files	296
12	Weekly maintenance	299
12.1	Overview	299
	Weekly maintenance information	300
12.2	Collecting device hardware inventory data.....	300
12.3	Checking scheduled device backups	300
12.4	5620 SAM database audit log management	300
	Weekly maintenance procedures	301
12.5	To check for performance monitoring statistics collection	301
12.6	To gather port inventory data for a specific managed device	302
12.7	To test a 5620 SAM database restore	304
12.8	To check scheduled device backup status	308
12.9	To reduce the number of Oracle audit logs	309
13	Monthly maintenance	311
13.1	Overview.....	311
	Monthly maintenance information	312
13.2	Performing main server and database redundancy switches.....	312
13.3	Checking the 5620 SAM platform performance	312
13.4	Checking Windows client platform performance	312
13.5	Checking LAN TCP/IP connections between network-management domain elements.....	313
13.6	Generating and storing a user account list.....	313
13.7	Verifying documentation and support contact list updates	313
13.8	Setting the time and date	313
	Monthly maintenance procedures	315
13.9	To measure 5620 SAM platform performance.....	315
13.10	To check Windows client station performance	317
13.11	To check network management connections	319
13.12	To generate and store user account data.....	321
13.13	To check for documentation and support updates.....	322

14 As required maintenance	325
14.1 Overview	325
5620 SAM platform modification	328
14.2 Modifying the platform of a 5620 SAM component	328
14.3 To reconfigure a 5620 SAM main server after a platform modification.....	328
14.4 To reconfigure a 5620 SAM database after a platform modification.....	330
14.5 To reconfigure a 5620 SAM auxiliary server after a platform modification	331
14.6 To reconfigure a Cflowd auxiliary server	332
14.7 To test 5620 SAM disk performance	333
14.8 To relink the Oracle executable files.....	336
Changing 5620 SAM passwords	338
14.9 Changing 5620 SAM user passwords	338
14.10 To change the samadmin user password.....	338
14.11 To change a database user password in a standalone 5620 SAM system	339
14.12 To change a database user password in a redundant 5620 SAM system	343
Auxiliary server administration	349
14.13 To start an auxiliary server	349
14.14 To stop an auxiliary server.....	350
Cflowd auxiliary server administration	351
14.15 To start a Cflowd auxiliary server	351
14.16 To stop a Cflowd auxiliary server.....	351
14.17 To display the Cflowd auxiliary server status.....	352
Analytics server administration	354
14.18 To start an analytics server.....	354
14.19 To stop an analytics server.....	354
Auxiliary database administration	356
14.20 To start an auxiliary database.....	356
14.21 To stop an auxiliary database	356
14.22 To change an auxiliary database user password	357
14.23 To restore an auxiliary database	358
14.24 To replace an auxiliary database station	362
14.25 To remove an auxiliary database station.....	365
Backing up and restoring NE configuration files	368
14.26 General information.....	368
14.27 To back up the NE configuration files	368

14.28 To restore the NE configuration files	369
Restoring and re-instantiating the 5620 SAM database	370
14.29 General information.....	370
14.30 To restore the database in a standalone 5620 SAM system	371
14.31 To restore the primary database in a redundant 5620 SAM system	376
14.32 To reinitiate a 5620 SAM database using a client GUI	385
14.33 To reinitiate a 5620 SAM database using a CLI	386
5620 SAM database export and import	388
14.34 To export a 5620 SAM database	388
14.35 To import a 5620 SAM database	392
Clearing inactive residential subscriber instances from the 5620 SAM database	398
14.36 General information.....	398
14.37 To delete the inactive residential subscriber instances	398
Listing customer service information	401
14.38 General information.....	401
14.39 To save a list of service information	401
Checking for duplicate service or resource names	403
14.40 General information.....	403
14.41 To check for duplicate port descriptions	403
Configuring the OLC state of equipment or services	405
14.42 General information.....	405
14.43 Setting the OLC state	406
14.44 To view the OLC state of equipment or services	407
14.45 To view the scheduling of OLC state changes of equipment or services	407
14.46 To change the OLC state of equipment or services	408
14.47 To view or change the OLC state from the alarm window	409
14.48 To add the OLC state to a template using the GUI builder.....	410
Part V: Appendices	411
A Scope of command roles and permissions	413
A.1 Overview	413
A.2 Predefined scope of command profiles and roles	413
A.3 Permissions assignable to 5620 SAM scope of command roles.....	416
A.4 Permissions access for scope of command roles	453

About this document

Purpose

The *5620 SAM System Administrator Guide* provides information about 5620 SAM system management, and is intended for a user assigned with an Administrator scope of command role. The guide describes functions that include the following:

- 5620 SAM system and user security management tasks
- 5620 SAM advanced configuration tasks
- 5620 SAM routine maintenance tasks to maintain hardware and system integrity and efficiencies

Safety information

For your safety, this document contains safety statements. Safety statements are given at points where risks of damage to personnel, equipment, and operation may exist. Failure to follow the directions in a safety statement may result in serious consequences.

Document support

Customer documentation and product support URLs:

- [Customer Documentation Welcome Page](#)
- [Technical support](#)

How to comment

[Documentation feedback](#)

Part I: 5620 SAM System Administrator overview

Overview

Purpose

This part provides information about the system administrator role and the tasks described in this guide.

Contents

Chapter 1, Safety information	15
Chapter 2, 5620 SAM System Administrator Guide overview	17

1 Safety information

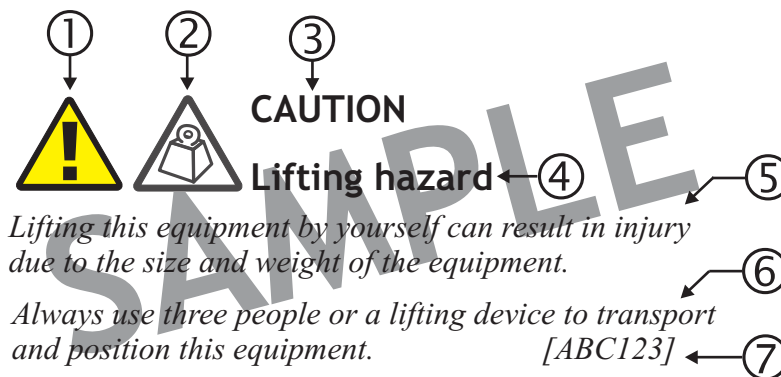
1.1 Structure of safety statements

1.1.1 Overview

This topic describes the components of safety statements that appear in this document.

1.1.2 General structure

Safety statements include the following structural elements:



Item	Structure element	Purpose
1	Safety alert symbol	Indicates the potential for personal injury (optional)
2	Safety symbol	Indicates hazard type (optional)
3	Signal word	Indicates the severity of the hazard
4	Hazard type	Describes the source of the risk of damage or injury
5	Safety message	Consequences if protective measures fail
6	Avoidance message	Protective measures to take to avoid the hazard
7	Identifier	The reference ID of the safety statement (optional)

1.1.3 Signal words

The signal words identify the hazard severity levels as follows:

Signal word	Meaning
DANGER	Indicates an extremely hazardous situation which, if not avoided, will result in death or serious injury.
WARNING	Indicates a hazardous situation which, if not avoided, could result in death or serious injury.
CAUTION	Indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.
NOTICE	Indicates a hazardous situation not related to personal injury.

2 5620 SAM System Administrator Guide overview

2.1 Overview

2.1.1 Purpose

This chapter describes the system administrator roles and tasks documented in this guide.

2.1.2 Contents

2.2	5620 SAM System Administrator Guide overview	17
2.3	5620 SAM system administrator tasks and information map	19
2.4	Administrator tasks for application management	21

2.2 5620 SAM System Administrator Guide overview

2.2.1 5620 SAM system administrator tasks

The *5620 SAM System Administrator Guide* describes the tasks that are typically performed by a user with an Administrator scope of command role. Information in this guide includes:

- 5620 SAM security management tasks including:
 - planning and implementing the user security measures required to protect all 5620 SAM data, software, and hardware and monitor the system/network for any security threats.
 - setting up all required 5620 SAM user accounts and user groups with the required scope of command roles and span of control permissions and the ongoing monitoring and management of those accounts.
 - providing security support information for accessing and securing managed devices in your network.
 - configuration and management requirements for TCP enhanced authentication for NEs based on the MD5 encryption mechanism.
- advanced configuration tasks including:
 - configuring, maintaining, and administering the 5620 SAM operational environment including software licenses, system components, network functions, and system preferences.

- performing the required tasks to establish and maintain 5620 SAM system redundancy; and as required, monitor/perform any maintenance activity switching or switchovers.
- using the 5620 SAM Database Manager to configure and monitor the 5620 SAM database.
- routine maintenance tasks to maintain hardware and system integrity and efficiencies including:
 - collecting baseline information to evaluate the activity and performance of the 5620 SAM and the various network components.
 - performing daily, weekly, monthly and supplemental routine maintenance on the 5620 SAM such as maintaining data backups and disaster recovery operations.



Note: This guide concentrates the majority of system administrator tasks into a single guide but some tasks are documented in other separate guides. See [2.3 “5620 SAM system administrator tasks and information map” \(p. 19\)](#) for a detailed listing of all system administrator tasks or information contained in this guide and other 5620 SAM customer documentation.

2.2.2 5620 SAM system administrator role

The 5620 SAM system administrator, in a typical network, would be the individual with a 5620 SAM administrative role given the responsibility for:

- performing the initial installation and setup of the 5620 SAM
- performing 5620 SAM startup and shutdown procedures
- planning and implementation of the user security measures required to protect all 5620 SAM data, software, and hardware
- setting up all required 5620 SAM user accounts with the required scope of command roles and span of control permissions and monitor the system/network for any security threats
- configuring, maintaining, and administering the 5620 SAM environment including computer hardware, software, and management network
- performing data backups and disaster recovery operations
- performing the required tasks to establish and maintain 5620 SAM system redundancy; and as required, monitor/perform any maintenance activity switching or switchovers
- monitoring the performance of the 5620 SAM to ensuring it operates and functions within set operational guidelines
- performing daily, weekly, monthly and supplementary routine maintenance on the 5620 SAM
- diagnosing any system-related alarm activity and solving unique problems identified by service and network operators
- diagnosing and troubleshooting platform, service, and connectivity problems using the 5620 SAM diagnostic tools
- integrating the 5620 SAM and other products

2.3 5620 SAM system administrator tasks and information map

2.3.1 Documentation reference

The following table provides a high-level navigation aid to help you locate specific system administrator tasks or information contained in this guide and other 5620 SAM customer documentation.

Table 1 5620 SAM system administrator task or information location

Task or information	Information location
Installation and upgrades	
Provides 5620 SAM and 5650 CPAM system deployment requirements and restrictions, and procedures for the following: <ul style="list-style-type: none"> • 5620 SAM and 5650 CPAM software installation, upgrade, and uninstallation for a standalone or redundant system • conversion from a standalone to a redundant system • system conversion from IPv4 to IPv6 inter-component communication • enabling SSL inter-component communication • system configuration for Small Cell management 	5620 SAM 5650 CPAM Installation and Upgrade Guide
Security management	
Provides information to help you access the requirements for user access to the 5620 SAM functional areas and configure and manage the following 5620 SAM user security functions and elements: <ul style="list-style-type: none"> • creating and managing user groups which 5620 SAM users are assigned to • creating and managing 5620 SAM user accounts • monitoring and managing active client sessions • configuring or managing 5620 SAM security functions • deleting 5620 SAM security elements that are no longer required 	Chapter 3, “5620 SAM user security”
Provides security support information for accessing managed devices, including the following: <ul style="list-style-type: none"> • create and manage users, profiles and passwords for access to NEs • configure RADIUS, TACACS+ or LDAP authentication to control access to the managed devices using 5620 SAM user accounts • configure device system security through CPM traffic filtering and management • configure DoS protection to protect NEs from high incoming packet rates that characterize DoS attacks 	Chapter 4, “NE user and device security”
Describes the configuration and management requirements for TCP enhanced authentication for NEs based on the MD5 encryption mechanism	Chapter 5, “TCP enhanced authentication”

Table 1 5620 SAM system administrator task or information location (continued)

Task or information	Information location
Provides a listing of the permissions, access levels, and descriptions of all pre-defined scope of command roles and profiles	Appendix Appendix A, "Scope of command roles and permissions"
Advanced configuration	
Describes how to configure the following: <ul style="list-style-type: none"> • 5620 SAM software and licences • 5620 SAM system components • Network management functions • System preferences 	Chapter 6, "5620 SAM component configuration"
Describes how to use the 5620 SAM Database Manager to perform the following: <ul style="list-style-type: none"> • view the 5620 SAM database properties • configure statistics data retention criteria • manage 5620 SAM database log storage • perform 5620 SAM database backups and restores • schedule regular database backups • configure error monitoring for increased security • troubleshoot 5620 SAM database problems 	Chapter 7, "5620 SAM database management"
Describes how to perform the following redundancy tasks using the 5620 SAM GUI, or scripts on a 5620 SAM main server: <ul style="list-style-type: none"> • Check the 5620 SAM server and database redundancy status. • Perform a manual activity switch from the primary to standby server. • Enable or disable automatic 5620 SAM database realignment. • Reinstantiate the former primary database as the standby database when an automatic or manual activity switch occurs. 	Chapter 8, "5620 SAM system redundancy"
Routine maintenance	
Provides an overview of all 5620 SAM routine maintenance tasks and their suggested application.	Chapter 9, "5620 SAM routine maintenance overview"
Provides a list of baseline information to collect for 5620 SAM applications to evaluate the performance of activity and performance of network components.	Chapter 10, "5620 SAM maintenance base measures"
Describes the daily, weekly, monthly, and as-required routine maintenance activities for 5620 SAM-managed networks and the 5620 SAM platform.	Chapter 11, "Daily maintenance" (daily) Chapter 12, "Weekly maintenance" (weekly) Chapter 13, "Monthly maintenance" (monthly) Chapter 14, "As required maintenance" (as-required)

Table 1 5620 SAM system administrator task or information location (continued)

Task or information	Information location
Troubleshooting	
Provides task-based procedures and user documentation to: <ul style="list-style-type: none"> • help resolve issues in the managed and management networks • identify the root cause and plan corrective action for: <ul style="list-style-type: none"> — alarm conditions on a network object or customer service — problems on customer services without associated alarms • list problem scenarios, possible solutions, and tools to help check: <ul style="list-style-type: none"> — network management LAN — network management platform — 5620 SAM GUI and OSS clients — 5620 SAM servers — 5620 SAM databases 	<i>5620 SAM Troubleshooting Guide</i>
Diagnosing alarms	
Provides a description of all alarms supported on the 5620 SAM, the raising and clearing conditions of each alarm, and the remedial action to fix the problem. Of interest to system administrators are alarms that require sysadmin access to solve such as database alarms or user authentication failure alarms.	<i>5620 SAM Alarm Reference</i>
Integration tasks	
Provides the procedures for 5620 SAM integration with other products.	<i>5620 SAM Integration Guide</i>

2.4 Administrator tasks for application management

2.4.1 *New Applications Guide*

The administration of browser-based 5620 SAM applications, such as domain-specific configurations and user security settings, is now described in a dedicated *5620 SAM Applications Guide*. See 5620 SAM applications administration in that guide for more information.

Part II: 5620 SAM security management

Overview

Purpose

This part provides information about configuring user and device security.

Contents

Chapter 3, 5620 SAM user security	25
Chapter 4, NE user and device security	89
Chapter 5, TCP enhanced authentication	141

3 5620 SAM user security

3.1 Overview

3.1.1 Purpose

This chapter describes user security mechanisms and procedures.

3.1.2 Contents

5620 SAM user security	27
3.2 Overview	27
3.3 User account and group management	28
3.4 User activity logging	33
3.5 Sample span rule configuration	37
3.6 Remote 5620 SAM user access	38
3.7 Sample 5620 SAM user authentication configuration	41
5620 SAM user security procedures	45
3.8 Workflow to configure and manage 5620 SAM user security	45
3.9 To reserve an admin account login	48
3.10 To create a scope of command role	49
3.11 To create a scope of command profile	50
3.12 To create a span of control	51
3.13 To create a span of control profile	52
3.14 To create a span rule	53
3.15 To create a 5620 SAM user group	54
3.16 To add or remove workspaces for a user group	55
3.17 To create a 5620 SAM user account	56
3.18 To copy a 5620 SAM user account	58
3.19 To configure global user account, password	58
3.20 To configure the GUI client inactivity timeout	59

3.21	To configure the minimum allowable user name length	60
3.22	To configure authentication failure actions	60
3.23	To configure suspended account actions	61
3.24	To configure automated E-mail notification	61
3.25	To list inactive user accounts	62
3.26	To suspend or reinstate a 5620 SAM user account	63
3.27	To administratively change the password of a 5620 SAM user	63
3.28	To force a 5620 SAM user password change	64
3.29	To change the password of the current 5620 SAM user	65
3.30	To export the local tab preferences of one or more users	66
3.31	To assign local tab preferences to users	67
3.32	To send a broadcast message to 5620 SAM GUI users	68
3.33	To view and manage active 5620 SAM client sessions	68
3.34	To disconnect a 5620 SAM-O JMS client connection or remove a durable subscription	69
3.35	To view the user activity log	70
3.36	To view the user activity associated with an object	72
3.37	To create a proprietary 5620 SAM login statement	73
3.38	To change the maximum number of concurrent 5620 SAM admin user sessions	73
3.39	To configure the number of allowed client sessions for a client delegate server	75
3.40	To enable secure access for remote LDAP users	76
3.41	To enable remote user authorization via RADIUS	77
3.42	To enable remote user authorization via TACACS+	79
3.43	To configure 5620 SAM remote user authentication	81
3.44	To change the 5620 SAM Task Manager settings	83
3.45	To export all workspaces and local tab preferences	85
3.46	To import workspaces and local tab preferences	86

5620 SAM user security

3.2 Overview

3.2.1 User security mechanisms

This chapter describes the 5620 SAM user security mechanisms for providing and restricting access to various objects and functions. 5620 SAM user security includes the following:

- user group and account management, which involves the following elements:
 - “[Scope of command roles](#)” (p. 29) — contains the roles that define the level of user control in 5620 SAM functional areas such as the read, create, update, and delete access permissions
 - “[Scope of command profiles](#)” (p. 30) — contains the appropriate scope of command role for the types of tasks to be performed
 - [3.3.5 “Span of control”](#) (p. 30) — list of objects to which a user has access
 - “[Span of control profiles](#)” (p. 32) — contains the required spans that allow user-group access to one or more 5620 SAM objects
 - “[Span rules](#)” (p. 32) — instructs the 5620 SAM to add new services to other spans in addition to the Default Service span
- global security parameters such as password expiry periods, the allowed number of login attempts, and any automated security E-mail notifications.
- managing user-group workspaces, which are customized configurations of 5620 SAM GUI elements; see the “5620 SAM custom workspaces” chapter of the *5620 SAM User Guide* for comprehensive workspace information
- monitoring and managing active client sessions
- remote user access via LDAP, RADIUS, and TACACS+ authentication
- deleting 5620 SAM security elements that are no longer required, such as inactive user accounts or user groups.
- configuring task monitoring parameters and monitoring the progress of operational tasks:
 - all write operations that are performed from the 5620 SAM GUI; for example, when you click Apply or OK
 - all write operations that are performed using the OSSI
 - some read operations; for example, when you click Resync or Collect All



Note: See Appendix [Appendix A](#), “[Scope of command roles and permissions](#)” for a list of the permissions, access levels, and descriptions of all predefined scope of command roles and profiles.

3.3 User account and group management

3.3.1 Overview



CAUTION

Service Disruption

Because the 5620 SAM cannot obtain an authentication secret value from an NE, it is recommended that you use only the 5620 SAM to configure a shared authentication secret on an NE.

If you configure a shared authentication secret on a managed NE using another interface, for example, a CLI, the 5620 SAM cannot synchronize the security policy with the NE.

You can create 5620 SAM user accounts and user groups to:

- provide GUI or OSS access to the 5620 SAM functional areas that match specific operator requirements
- restrict access to functions or objects based on operator expertise or authority

Users have view access, read-write access, or no access to 5620 SAM objects and functions based on:

- the user group to which they belong
- the scope of command profile assigned to the user group

The 5620 SAM user account called admin is created during 5620 SAM installation. The admin account is assigned the administrator scope of command role and a span of control profile that has Edit Access assigned to each default span.



Note: To restrict user access to top-level 5620 SAM functions such as 5620 SAM and NE security management, the following guidelines are recommended:

- Assign the administrator scope of command role to a minimal number of 5620 SAM user accounts.
- Assign each 5620 SAM user to a user group that has the minimum privileges for performing the required tasks.

3.3.2 General 5620 SAM security management rules

The following general rules apply to 5620 SAM user and group security management:

- Only database space limits the number of accounts and groups that can be created.
- A user cannot belong to more than one user group.
- Only one session per user account can be open at the same time on a client station.
- A scope of command profile allows user-group access to one or more 5620 SAM functional areas.

- A span of control profile allows user-group access to one or more 5620 SAM managed objects.
- A user group is associated with only one scope of command profile that can contain multiple scope of command roles.
- A user group is associated with only one span of control profile that can contain multiple spans.
- The assigned user privileges determine the following for a GUI user:
 - the available 5620 SAM menu options
 - the parameters on object property forms that are configurable
- By default, a user group is assigned access to all 5620 SAM objects.
- A user acquires span of control access rights from the associated user group.
- When you modify a user group, and a user in the group has an open client session, client actions may fail for the user. To put the new user group permissions into effect, the user must close the current client session and open a new session.
- You can modify but not delete a span of control profile that is assigned to a group.

3.3.3 Password management

A 5620 SAM user password must observe the following constraints:

- It must be 8 to 100 characters.
- It must contain at least three of the following character types:
 - lowercase
 - uppercase
 - special ()?~!@#\$%* _ +
 - numeric
- It cannot be the user account name, in forward or reverse order.
- It cannot include more than three consecutive instances of the same character.
- It must change according to a configurable schedule, to prevent account lockout.
- It cannot be reused as a new password for the same user account.

3.3.4 Scope of command

A scope of command, which defines the actions that a user is allowed to perform, is a collection of configurable roles, which are sets of permissions. A scope of command profile contains one or more roles, and the profile is subsequently applied to a user group. Each user in the group acquires the access rights specified in the scope of command profile.

Scope of command roles

A scope of command role specifies the read, create, update, and delete access permissions for a 5620 SAM object type or package. You can create custom roles by assigning specific access permissions to different 5620 SAM functional areas. The functional areas are organized in packages, methods, and classes. See Appendix

[Appendix A, "Scope of command roles and permissions"](#) for a list of all access permissions that can be assigned to a scope of command role.



Note: When you enable the Create permission for a 5620 SAM package, method, or class, the Update permission is automatically enabled.

When you enable the Update permission for a 5620 SAM package, method, or class, the Create permission is not automatically enabled.

You can create an original scope of command role, or copy an existing role and modify the role permissions to create a role. The 5620 SAM has several predefined scope of command roles. See [Appendix A, "Scope of command roles and permissions"](#) for a list of the permissions, access levels, and descriptions of all pre-defined scope of command roles and profiles.



Note: When you create a scope of command role, you must enable create, update /execute, and delete access to allow the modification of a class or package.

Scope of command profiles

A scope of command profile contains one or more scope of command roles, and is assigned to a user group. Each user in the group acquires the permissions from the scope of command roles in the profile.

3.3.5 Span of control

The span of control for a user is a list of the objects over which the user has control, for example, a group of NEs or services. You can create an original span, or copy an existing span and modify the list of associated objects to create a new span. The objects that are in a span, or that can be added to a span, are called span objects.

The 5620 SAM has several pre-defined spans. Each new 5620 SAM object, for example, a discovered NE, is added to the corresponding pre-defined span. [Table 2, "pre-defined spans of control" \(p. 30\)](#) lists the pre-defined 5620 SAM spans and the type of span objects in each.



Note: You cannot modify or delete a pre-defined span.

Table 2 pre-defined spans of control

Span	Included objects
Default Topology Group Span	Topology groups
Default Router Span	Managed NEs
Default Script Span	CLI and XML API scripts, service templates, tunnel templates, and auto-provision profiles

Table 2 pre-defined spans of control (continued)

Span	Included objects
Default Test Suite Span	Test suites
Default Group Span	Ring groups and VLAN groups
Default Bulk Operation Span	Bulk operations
Default Service Span	Services
Default Customer Span	Customers

Spans are specified in span of control profiles that are associated with user groups. A user can create a 5620 SAM object only when the pre-defined span for the object type is in the span of control profile. For example, if you do not have the Default Group Span in your span of control profile, you cannot create a ring group.

NEs are added automatically to a span when the parent topology group, ring group, or VLAN group is in a span. An object that is automatically added to a span cannot be removed from the span, but an explicitly added object can be removed.



Note: A user can view or configure a point-to-point connection only when each endpoint of the connection is in the user span of control. For example, when the endpoints of an LSP path are in different spans, you need view or configuration privileges in each span in order to view or configure the LSP path.

When you create a span, you can drag and drop NEs and topology groups into the span contents list.

Each user can control which objects the 5620 SAM displays in maps, lists, and navigation trees, based on the user span of control. The User Preferences form contains a parameter that globally specifies whether the Edit Access span objects of the user appear by default. Objects that are not in a View Access span of the user are not displayed, regardless of the user preference. See “To filter using span of control” in the *5620 SAM User Guide* for information about configuring the user span of control display preference.

In a list form, you can override the global display preference using the Span On parameter. The associated advanced filter form contains a selector for filtering the search results based on the span of control. See the *5620 SAM User Guide* for information about configuring span of control filters.

Span of control profiles



CAUTION

Service Disruption

It is recommended that you consider the effects of combining customer, service, and NE spans in a span of control profile.

For example, a user can modify a service only when the service, customer, and participating NEs are in one or more Edit Access spans of the user, and none of the objects is in a Blocked Edit or Blocked View span.

A span of control profile is a collection of one or more spans that is assigned to a user group. When you create a profile, each span in the profile is assigned one of the following access types:

- View Access—The user can view the span objects, unless the scope of command permissions deny read access.
- Edit Access—The user can modify the span objects, unless the scope of command permissions deny access.
- Blocked Edit—The user can view but not modify the span objects, regardless of the scope of command permissions.
- Blocked View—The user cannot view or modify the span objects, regardless of the scope of command permissions.

Blocked Edit and Blocked View spans restrict access to a subset of the objects in another span in the same profile. For example, when multiple span of control profiles each contain the Default Service Span, you can add a customer-specific Blocked View or Blocked Edit span to each profile so that the user group associated with a profile can view or configure only the services of specific customers.

A Blocked Edit or Blocked View span takes precedence over other spans. For example, when a user has an Edit Access span that contains all services and a Blocked View span that contains Customer A and Customer B, the user cannot view or configure the services that belong to Customer A and Customer B.

To ensure that span conflicts do not interfere with network troubleshooting, the 5620 SAM allows a user to execute tests on NEs and service sites that are not in an Edit Access span of the user. However, activities such as policy distribution, software upgrades, and statistics collection can be performed only by a user with Edit Access spans that contain the target objects.

Span rules

By default, the 5620 SAM automatically adds a new service to the Default Service span. Using an OSS or GUI client, you can create policies called span rules that add new services to other spans in addition to the Default Service span.

A span rule is associated with a format or range policy, and applies to the users and user groups that are specified in the format or range policy. You can associate multiple range policies with one user and service type, which enables the automatic addition of a new service to a specific span based on the service ID specified when the service is created.

When you create a span rule, you must specify one of the following to indicate which spans receive the services that the user creates:

- the Edit Access spans of each user associated with the format or range policy
- each span that is explicitly named in the rule

The span rules associated with a format or range policy take effect for new services only when the format or range policy is administratively enabled and has a valid configuration that includes at least one user or user group.

See [3.5 “Sample span rule configuration” \(p. 37\)](#) for a sample span rule configuration and implementation.

3.4 User activity logging

3.4.1 Log records

The 5620 SAM logs each GUI and OSS user action, such as a system access attempt or the configuration of an object, in the 5620 SAM database. The following table lists the information in a user activity log record.

Table 3 User activity log record information

Field name	Description
Time	Time of activity
Session Type	Type of session, which is GUI, JMS, or OSS
Session ID	Client session identifier
Session IP Address	Client IP address
Session Time	Client session start time
Server IP Address	IP address of 5620 SAM main server that reports the activity
Type	General activity type, which is Deployment, Operation, or Save
Sub Type	Specific activity type, which is Creation, Deletion, Modification, or name of the invoked method
Username	5620 SAM username
Site Name	Name of affected NE, if applicable
Site ID	IP address of affected NE, if applicable

Table 3 User activity log record information (continued)

Field name	Description
Object Name	Name of affected object
Object ID	Fully qualified name of affected object
Object Type	Type of affected object
State	Activity status, which is Failure, Success, or Timeout
Request ID	Identifier assigned to the request, which is unique to a session
Additional Info	Information such as old and new parameter values after a modification
XML	5620 SAM object class descriptor, if applicable, and activity details in XML request format

To view general user activity log entries in the GUI, or retrieve the entries using the 5620 SAM-O, you require a 5620 SAM user account that has the Administrator or 5620 SAM Management and Operations scope of command role.



Note: Viewing or retrieving LI user activity entries requires the Lawful Intercept Management role, and is restricted to the entries of users in the same LI user group.

The logged activity types are the following:

- Operation—a request for the 5620 SAM
- Deployment—a change that is deployed to an NE
- Save—a change to a 5620 SAM database object

Each user activity creates an Operation log entry. If the activity results in an NE configuration change, a Deployment entry is logged. If the deployed information differs from the information that the 5620 SAM saves to the database, a Save entry is logged. If appropriate, a log entry contains the activity details in XML format.

The following table lists the user activity types and describes the associated sub types.

Table 4 User activity types

Type	Sub Type	sub type description
Deployment	Creation	NE object creation
	Deletion	NE object deletion
	Modification	NE object modification
Operation	<i>method</i>	Name of invoked method

Table 4 User activity types (continued)

Type	Sub Type	sub type description
Save	Creation	5620 SAM database object creation
	Deletion	5620 SAM database object deletion
	Modification	5620 SAM database object modification

The User Activity form displays a filterable list of the logged user activities, and a filterable list of the logged client and server session activities. Client session activities include connection, disconnection, and access violation. Server session activities include startup and shutdown. The properties form of a client connection log record lists the activities performed by the user during the client session.

The 5620 SAM GUI allows direct navigation between the following objects:

- activity record and the associated session record
- activity record and the activity target object
- object properties form and the associated user activity list form
- 5620 SAM Task Manager task and the associated user activity list form
- session record and the associated user activity list form

The User Activity form lists the recent user session and activity entries; older entries are purged according to configurable storage criteria. See [6.29 “To configure 5620 SAM system preferences” \(p. 198\)](#) for information about configuring the user activity log retention criteria using the System Preferences form.

To archive user activity log entries before they are purged from the 5620 SAM database, an OSS client can use a time-based filter to retrieve entries from the sysact package using the find and findToFile methods. See the *5620 SAM-O XML Reference* for information about using the find and findToFile methods.

User activity logging is a valuable troubleshooting function. For example, if a port unexpectedly fails, you can quickly determine whether misconfiguration is the cause by doing one of the following:

- opening the port properties form and clicking User Activity to view the recent user activity associated with the port
- opening the User Activity form, filtering the list by object type or name, and then verifying the associated user activities



Note: Script execution is logged, but the actions that a script performs are not.

See “Troubleshooting using the 5620 SAM user activity log overview” in the *5620 SAM Troubleshooting Guide* for more information.

The following conditions and restrictions apply to user activity logging.

- A Deployment activity typically does not have an associated Save activity for the following reasons:
 - A Deployment activity takes place only after a successful Save activity, so a Deployment implies a Save.
 - A Save activity typically contains the same information as the associated Deployment activity.
- When a high-level object such as an NE is deleted, one aggregate activity record is created, rather than multiple NE child object activity records.
- The XML text in a log entry is limited to 4000 characters. If an activity generates more than 4000 characters of XML text, the text is truncated, and the truncation is indicated on the log entry form.

3.4.2 Client session control

Each 5620 SAM GUI client, 5620 SAM-O JMS client, or XML API request creates a 5620 SAM client session. You can view a list of the active 5620 SAM client sessions on the Sessions tab of the 5620 SAM User Security - Security Management form. Using this form, an admin user, or a user with an assigned security scope of command role, can also terminate one or more 5620 SAM GUI client sessions. When a 5620 SAM GUI client session is terminated in this manner, each client application receives a warning message and the connection is closed by the 5620 SAM server after a short delay. See [3.33 “To view and manage active 5620 SAM client sessions” \(p. 68\)](#) for more information.

Messaging connections

A list of active 5620 SAM GUI connections and 5620 SAM-O JMS connections can be viewed on the Messaging Connections tab of the 5620 SAM User Security - Security Management form. Using this form, an admin user, or a user with an assigned security scope of command role, can terminate one or more connections. When a 5620 SAM-O client connection is terminated, a notification is sent to the 5620 SAM-O client, but the admin user must also remove the 5620 SAM-O JMS client connection so that the server stops storing JMS messages for the session. See [3.34 “To disconnect a 5620 SAM-O JMS client connection or remove a durable subscription” \(p. 69\)](#) for more information.

Client delegate sessions

The threshold for the number of 5620 SAM client sessions allowed on a client delegate server is configurable using the 5620 SAM GUI. When a user tries to open a client session that exceeds the threshold, the client delegate server opens the session, displays a warning message to the user, and generates an alarm. The threshold-crossing function can help to balance the session load across multiple client delegate servers. You need the Update user permission on the Server package to configure the threshold. See [3.39 “To configure the number of allowed client sessions for a client delegate server” \(p. 75\)](#) for more information.

3.5 Sample span rule configuration

3.5.1 Workflow

This section describes the configuration of a policy that instructs the 5620 SAM to automatically add each service created for a specific customer to an Edit Access span associated with the creator of the service. Only the service administrator for the customer can create or edit the specific customer services. In contrast, a typical service user can only view the specific customer services. The following table describes the tasks to configure a span rule.

Table 5 Sample span rule configuration

Task	Description
1. Create a span that contains the existing customer services.	<ul style="list-style-type: none"> Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. Choose Create→Span on the Span of Control tab. Specify a span name for the customer services. Use the Contents tab to specify the customer X services.
2. Create a span of control profile for the service administrator.	<ul style="list-style-type: none"> Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. Choose Create→Profile on the Span of Control tab. Add the Default Service Span as a View Access span to the span of control profile, which allows the user to create a service. Add the customer services span as an Edit Access span to the span of control profile.
3. Create a range policy for each service type that the service administrator for the customer can create. In the sample, the services are IES and VPRN.	<ul style="list-style-type: none"> Choose Administration→Format and Range from the 5620 SAM main menu. Choose Create→Range Policy. Specify IES Service as the Object Type. Specify Service ID as the Property Name. Configure a range. Click Add on the Users tab to assign the policy to the service administrator. Choose Create→Range Policy. Specify VPRN Service as the Object Type. Specify Service ID as the Property Name. Configure a range. Click Add on the Users tab to assign the policy to the service administrator.
4. Create a span rule that contains the customer span.	<ul style="list-style-type: none"> Choose Administration→Span Rules from the 5620 SAM main menu. Specify a name for the customer span rule. Set the Created In parameter to All listed spans. Add the customer span on the Spans tab.

After the span rule is created, the service administrator creates a new VPRN service for the customer. The 5620 SAM uses the VPRN range policy to automatically configure the service ID, and applies the associated customer span rule when the service is saved. As

a result, the service is added to the customer span and to the Default Service Span. The service administrator has Edit Access to the customer span, and, therefore, can modify the service, as required.

3.6 Remote 5620 SAM user access

3.6.1 Overview

In addition to local account management, 5620 SAM user authentication and authorization can be accomplished via remote servers. 5620 SAM supports the following remote user access protocols:

- LDAP or LDAPS
- RADIUS
- TACACS+



Note: It is recommended that you use LDAP Secure, or LDAPS, in a live deployment. LDAPS user authentication is supported only in a 5620 SAM system that is secured using SSL, and requires additional configuration, as described in [3.40 “To enable secure access for remote LDAP users” \(p. 76\)](#).

See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for information about enabling SSL in a 5620 SAM system.

You can configure 5620 SAM access for users that log on through a third-party server in a corporate network. For example, a person who does not have a 5620 SAM user account can log in to the 5620 SAM using their corporate credentials. The 5620 SAM forwards the credentials to a remote authentication server, and grants or denies access to the user based on the remote server response.

If a remote authentication server is configured to authorize users, the remote server also sends the name of a user group in a successful authentication response. If the 5620 SAM has a user group with the same name, the user is assigned to the group and granted access based on the group properties. Otherwise, the user is assigned to a default external user group.

When a remote session terminates, the associated 5620 SAM user account remains, and the user application preferences such as filters apply to subsequent sessions.

Successful remote authentication for an OSS user requires that the remote server and the 5620 SAM use the same password format. The OSS users can log in using a clear-text or MD5-hashed password, if the remote server supports MD5 password hashing. See “Secure communication” in the *5620 SAM XML OSS Interface Developer Guide* for more information.

You use the 5620 SAM Remote Authentication Manager to configure the protocols and define the authentication order for users. For example, if you specify an order of RADIUS, LDAP, local, the 5620 SAM tries to authenticate each remote user via RADIUS;

if the RADIUS servers are unavailable, the 5620 SAM tries LDAP, and upon failure tries to match the user credentials to a local 5620 SAM account.

[3.43 “To configure 5620 SAM remote user authentication” \(p. 81\)](#) describes how to configure the general remote access properties, such as the authentication types, the authentication order, and the remote servers.

3.6.2 Assigning remote users to 5620 SAM user groups

User authorization is the assignment of a user to a user group after successful user authentication. By default, the 5620 SAM assigns a remote user to a default user group, if one is specified. Optionally, you can configure the 5620 SAM to assign a group specified by a remote server. If no default group is specified, and remote group assignment is not configured, the authorization fails and the user is denied access.

After a remote server authenticates a user, if the name of the user group sent by the remote server matches a 5620 SAM user group name, the 5620 SAM creates a user account for the login session and grants the appropriate access rights. Otherwise, authorization fails and the 5620 SAM denies user access.

RADIUS or TACACS+ user authorization

In order for a remote RADIUS or TACACS+ server to assign a 5620 SAM user group, you must preconfigure the 5620 SAM and the remote server. See [3.41 “To enable remote user authorization via RADIUS” \(p. 77\)](#) for information about enabling authorization for RADIUS users, and [3.42 “To enable remote user authorization via TACACS+” \(p. 79\)](#) for information about enabling authorization for TACACS+ users.



Note: A RADIUS authentication success message that is sent to the 5620 SAM contains the user group name.

For TACACS+, authentication must succeed before an authorization message containing the user group name is sent to the 5620 SAM.

If an LDAP user password is MD5-hashed, only local user authorization is supported.

LDAP user authorization

For each LDAP server that you specify using the 5620 SAM Remote Authentication Manager, you can include LDAP group lookup criteria. The group name that the LDAP server returns in an authentication success message must match an existing 5620 SAM group name.



Note: If an LDAP user password is MD5-hashed, only local user authorization is supported.

3.6.3 One-time password use

For increased security, a GUI user can provide an authentication token to an LDAP, RADIUS or TACACS+ server that is validated only once. You can enable one-time password use during 5620 SAM remote authentication policy configuration, as described in [3.43 “To configure 5620 SAM remote user authentication” \(p. 81\)](#) .



Note: The one-time password function is not available to OSS clients.

To change the one-time password setting in a remote authentication policy, you require a scope of command that has Update/Execute access to the srrmmtauth package.

After a communication failure between a GUI client and a 5620 SAM main server when one-time password use is in effect, the GUI client is unable to obtain authentication using the cached credentials from the previous login attempt. When this occurs, the client prompts the user to log in to the remote authentication server again, but does not automatically close the GUI, in order to preserve the current view until the user is authenticated.

3.6.4 Combined local and remote authentication

A 5620 SAM operator can integrate an existing LDAP, RADIUS, or TACACS+ user account with a 5620 SAM user account by creating a 5620 SAM user account that has the same name as the remote account. A 5620 SAM user who authenticates remotely can then log in to the 5620 SAM using their remote credentials, if the password observes the 5620 SAM password constraints described in this chapter.

A 5620 SAM user name can be 1 to 80 characters long, which is sufficient for most combined authentication scenarios.



Note: If a RADIUS or TACACS+ server is configured to perform user authorization, the 5620 SAM requires a user group from the remote server, and the following conditions apply:

- The user group sent by the remote server must exist in the 5620 SAM.
- If a 5620 SAM user account is associated with a local user group and configured to use remote authentication, the local user group is replaced by the specified remote user group.

For example, a user named jane has the following accounts:

- a remote RADIUS account called jane and the password accessforjane
- a local 5620 SAM account called jane and the password LetJane1In!

When jane is authenticated by RADIUS, she gains access to the 5620 SAM by typing in jane and accessforjane. If the RADIUS server is down, jane is authenticated locally by the 5620 SAM after typing jane and LetJane1In!.

3.7 Sample 5620 SAM user authentication configuration

3.7.1 Use case

Figure 1, “Sample 5620 SAM user and user group authentication” (p. 40) shows an example of how 5620 SAM user and user group authentication is performed.

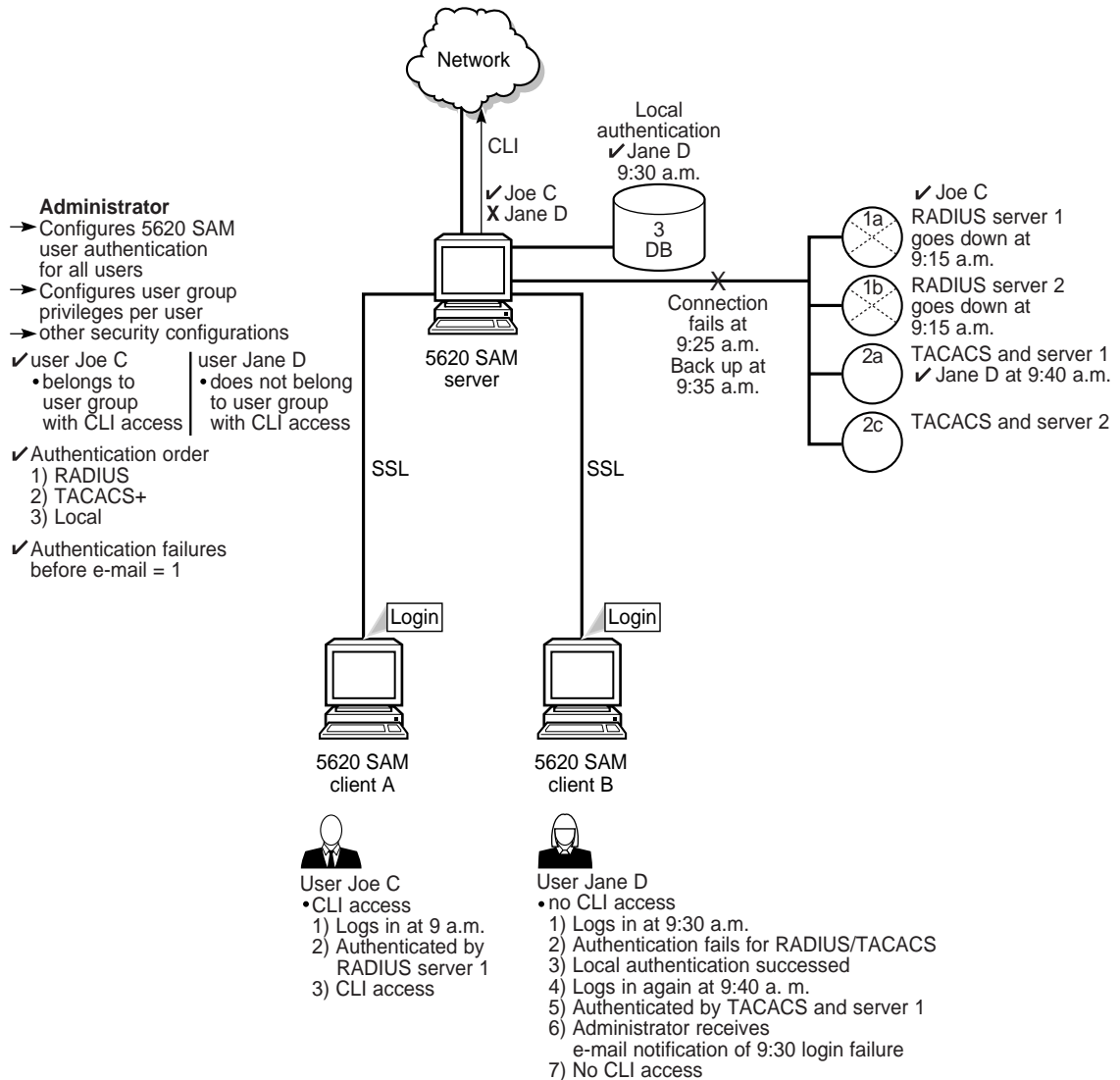


Note: RADIUS and TACACS+ authentication servers support multiple users. If the 5620 SAM cannot reach the first authentication server, the 5620 SAM sequentially attempts the user authentication using the remaining authentication servers.

If user authentication fails against the first authentication server in a sequence, for example, because of an incorrect password, there is no attempt to authenticate the user against the next authentication server in the sequence.

The 5620 SAM session log records unsuccessful user authentication attempts for known and unknown users. A user that is defined on an external AAA server but not in the 5620 SAM.

Figure 1 Sample 5620 SAM user and user group authentication



17770

The following table lists the high-level tasks required to configure this sample.

Table 6 Sample 5620 SAM user authentication configuration

Task	Description
Pre-configurations	Ensure correct RADIUS or TACACS+ server configuration, according to your company requirements. PAP authentication is supported for RADIUS and TACACS+. The 5620 SAM server must be able to communicate with the authentication servers to validate users. All configuration tasks should be done with admin access. The 5620 SAM server IP address must be configured as the client of the RADIUS or TACACS+ server. The secret keys must match on the 5620 SAM server and the RADIUS or TACACS+ server.
1. Configure the remote authentication order for all users	Choose Administration→Security→5620 SAM Remote User Authentication from the 5620 SAM main menu. Set the authentication order parameters to the following, and then specify the RADIUS and TACACS+ servers on the RADIUS and TACACS tabs. <ul style="list-style-type: none"> • Authentication Order 1—radius • Authentication Order 2—tacplus • Authentication Order 3—local
2. Create scope of command profiles	Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. Create a CLI scope of command profile and assign the default CLI management role to the profile. Create at least one scope of command profile that does not allow CLI access by assigning the <i>default</i> scope of command role, which has no access permissions to CLI management.
3. Create and configure user groups	Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. Create a CLI user group and at least one user group that does not allow CLI access. Assign the scope of command profile with CLI management access to the CLI user group. Assign the scope of command profile without CLI management access to the user group without CLI access. Authorization is done using user groups, so each user must belong to a user group with a local account on the 5620 SAM server.
4. Create and configure user accounts	You can create local users on the 5620 SAM by performing the following steps, or define remote users using RADIUS and TACACS+. The local users are available when RADIUS or TACACS+ authentication is not available. Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. Create users. Assign the appropriate user group to each user: one with CLI access and one without CLI access.
5. Configure notification	Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. Configure the authentication failure action parameters, including the parameters that allow the E-mail account of the administrator to be notified after login failure.

Consider the following:

- The 5620 SAM server acts as a network access server. A network access server is considered a client of a remote access server.
- The sequence of activity between the 5620 SAM server, which is the authentication client, and the remote server, which is the authentication server, is the following:
 - client requests authentication

- server replies to authentication request
- client requests logout and authentication stops
- When the remote authentication servers are down and local authentication is used, the user must log in using 5620 SAM credentials, as described in [3.6.4 “Combined local and remote authentication”](#) (p. 40) .

5620 SAM user security procedures

3.8 Workflow to configure and manage 5620 SAM user security

3.8.1 Process

- 1 _____
Assess the requirements for user access to the different 5620 SAM functional areas and develop a strategy for implementing user security. See [3.3 “User account and group management” \(p. 28\)](#) for more information.
- 2 _____
Reserve a client GUI session for the admin user to ensure that the admin user can always log in; see [3.9 “To reserve an admin account login” \(p. 48\)](#) .
- 3 _____
Create scope of command roles or modify the default role to meet your operational requirements; see [3.10 “To create a scope of command role” \(p. 49\)](#) .
- 4 _____
Create scope of command profiles that contain the appropriate scope of command roles for the types of tasks to be performed; see [3.11 “To create a scope of command profile” \(p. 50\)](#) .
- 5 _____
Create spans or modify the default span to meet your operational requirements. Add 5620 SAM managed objects to the spans; see [3.12 “To create a span of control” \(p. 51\)](#) .
- 6 _____
Create span of control profiles that contain the required spans; see [3.13 “To create a span of control profile” \(p. 52\)](#) .
- 7 _____
Create span rules, as required, to automatically assign new services to spans other than the Default Service Span; see [3.14 “To create a span rule” \(p. 53\)](#) .
- 8 _____
Manage user group security requirements, as required.

- Create or modify user groups and assign scope of command and span of control profiles to each group, as required; see [3.15 “To create a 5620 SAM user group” \(p. 54\)](#) .
- Add workspaces to user groups; see [3.16 “To add or remove workspaces for a user group” \(p. 55\)](#) .

9

Create, modify, or copy user accounts for performing the tasks that are associated with each user group; see [3.17 “To create a 5620 SAM user account” \(p. 56\)](#) and [3.18 “To copy a 5620 SAM user account” \(p. 58\)](#) .

10

Configure global user account parameters, as required.

- user-account expiry periods, password criteria, and a GUI inactivity timeout; see [3.19 “To configure global user account, password” \(p. 58\)](#) and [3.20 “To configure the GUI client inactivity timeout” \(p. 59\)](#) .
- minimum username length; see [3.21 “To configure the minimum allowable user name length” \(p. 60\)](#) .
- allowed number of authentication attempts; see [3.22 “To configure authentication failure actions” \(p. 60\)](#) .
- suspended account actions; see [3.23 “To configure suspended account actions” \(p. 61\)](#) .
- automated E-mail notification; see [3.24 “To configure automated E-mail notification” \(p. 61\)](#) .

11

Configure global user activity logging, as required; see [6.29 “To configure 5620 SAM system preferences” \(p. 198\)](#) .

12

Enable and configure 5620 SAM access for remote users, if required.

1. Configure authorization for remote users in which either the 5620 SAM or the remote authentication server associates the user with a user group:
 - for LDAP: [3.40 “To enable secure access for remote LDAP users” \(p. 76\)](#)
 - for RADIUS: [3.41 “To enable remote user authorization via RADIUS” \(p. 77\)](#)
 - for TACACS+: [3.42 “To enable remote user authorization via TACACS+” \(p. 79\)](#)
2. Configure the general remote-access parameters, and specify LDAP, RADIUS, and TACACS+ servers, as required; see [3.43 “To configure 5620 SAM remote user authentication” \(p. 81\)](#) .

13

Manage user accounts, as required.

- List inactive user accounts; see [3.25 “To list inactive user accounts”](#) (p. 62) .
- Suspend or reinstate user accounts; see [3.26 “To suspend or reinstate a 5620 SAM user account”](#) (p. 63) .
- Manage passwords.
 - As administrator, change the password of a specified 5620 SAM user account; see [3.27 “To administratively change the password of a 5620 SAM user”](#) (p. 63) .
 - Force a specified 5620 SAM user to change the account password during the next login attempt; see [3.28 “To force a 5620 SAM user password change”](#) (p. 64) .
 - Change the account password of the current user; see [3.29 “To change the password of the current 5620 SAM user”](#) (p. 65) .
- Export user tab preferences; see [3.30 “To export the local tab preferences of one or more users”](#) (p. 66) .
- Assign user tab preferences; see [3.31 “To assign local tab preferences to users”](#) (p. 67) .

14

Monitor and manage the active client sessions, as required.

- Broadcast a message to one or more 5620 SAM GUI users; see [3.32 “To send a broadcast message to 5620 SAM GUI users”](#) (p. 68) .
- List and optionally close GUI client sessions; see [3.33 “To view and manage active 5620 SAM client sessions”](#) (p. 68) .
- List and optionally close OSS client sessions; see [3.34 “To disconnect a 5620 SAM-O JMS client connection or remove a durable subscription”](#) (p. 69) .
- View the 5620 SAM user activity logs to monitor GUI and OSS user activity; see [3.35 “To view the user activity log”](#) (p. 70) and [3.36 “To view the user activity associated with an object”](#) (p. 72) .

15

Configure or manage the following 5620 SAM security functions, as required:

- Create a proprietary client GUI login screen; see [3.37 “To create a proprietary 5620 SAM login statement”](#) (p. 73) .
- Change the maximum number of concurrent 5620 SAM admin user sessions; see [3.38 “To change the maximum number of concurrent 5620 SAM admin user sessions”](#) (p. 73) .
- Limit the number of client sessions that the 5620 SAM accepts from one or more client delegate servers; see [3.39 “To configure the number of allowed client sessions for a client delegate server”](#) (p. 75) .

16

Change the default parameter setting for the Task Manager, as required; see [3.44 “To change the 5620 SAM Task Manager settings”](#) (p. 83) .

See “To monitor the 5620 SAM Task Manager” in the *5620 SAM User Guide* for more information on monitoring operational tasks.

17

Export or import all workspaces and tab preferences, as required.

- Export all workspaces and tab preferences; see [3.45 “To export all workspaces and local tab preferences” \(p. 85\)](#) .
- Import all workspaces and tab preferences, import workspaces only, or import tabs only; see [3.46 “To import workspaces and local tab preferences” \(p. 86\)](#) .

3.9 To reserve an admin account login

3.9.1 Purpose

You can reserve one client GUI session from the maximum number of sessions allowed by the license key, for admin users only. This allows an administrator to manage the existing client GUI sessions. You must have an account with an assigned security scope of command role to perform this procedure.

3.9.2 Steps

1

Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.

2

Configure the Reserve Administrator Login parameter.

3

Save your changes and close the form.

-
- 4 _____
Log in as required.

END OF STEPS _____

3.10 To create a scope of command role

3.10.1 Purpose

You can create a set of user permissions that define an operator role and apply one or more scope of command roles to a user group using a scope of command profile. You must have an account with an assigned security scope of command role to perform this procedure.



Note: You cannot delete a pre-defined scope of command role.

You cannot delete a scope of command role that is assigned to a scope of command profile when the scope of command profile is assigned to a user group that contains users.

Refer to [Appendix A, "Scope of command roles and permissions"](#) for a complete list of command profiles, roles, and permission information.

3.10.2 Steps

- 1 _____
Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.
- 2 _____
Click on the Scope of Command tab.
- 3 _____
Click Create and choose Role. The Role (Create) form opens.
- 4 _____
Configure the required parameters.
- 5 _____
Configure the permissions for the scope of command role:
 1. Click on the Permissions tab. A list of the 5620 SAM packages, classes, and methods is displayed.

Note:

When you enable the Create permission for a 5620 SAM package, method, or class, the Update/Execute permission is automatically enabled.

When you enable the Update/Execute permission for a 5620 SAM package, method, or class, the Create permission is not automatically enabled.

2. Select the required access permissions, which are displayed in the list column headings, for each package, class, or method that you need to assign to the scope of command role.

6

Save your changes and close the form.

END OF STEPS

3.11 To create a scope of command profile

3.11.1 Steps

1

Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.

2

Click on the Scope of Command tab.

3

Click Create and choose Profile. The Scope of Command Profile (Create) form opens.

4

Configure the required parameters.

5

Assign one or more scope of command roles to the profile:

1. Click on the Roles tab and click Add. The Select Role - Role form opens.
2. Select one or more roles and click OK.

Note:

You cannot delete a scope of command profile that is assigned to a user group that contains users.

6 _____

Save your changes and close the form.

END OF STEPS _____

3.12 To create a span of control

3.12.1 Purpose

You can specify a set of 5620 SAM objects in a span of control and the type of user access available for the objects. You can apply one or more spans to a user group using a span of control profile. You must have an account with an assigned security scope of command role to perform this procedure.



Note: You cannot delete a span of control that is assigned to a user group that contains users.

3.12.2 Steps

1 _____

Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.

2 _____

Click on the Span of Control tab.

3 _____

Click Create and choose Span. The Span (Create) form opens.

4 _____

Configure the required parameters.

5 _____

Add one or more objects for user access:

1. Click on the Contents tab.
2. Click Add and choose an object type. The Select (*object_type*) form opens.
3. Select one or more objects and click OK.

-
- 6 _____
Save your changes and close the form.

END OF STEPS _____

3.13 To create a span of control profile

3.13.1 Steps

- 1 _____
Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.
- 2 _____
Click on the Span of Control tab.
- 3 _____
Click Create and choose Profile. The Span of Control Profile (Create) form opens.
- 4 _____
Configure the required parameters.
- 5 _____
Assign one or more spans to the profile:
1. Click on the Spans tab. The predefined spans are listed.
 2. Click Add and choose an access type. The Select *access_type* Spans form opens.
 3. Select one or more spans in the list and click OK.

Note:

You cannot delete a span of control profile that is assigned to a user group that contains users.

6

Save your changes and close the form.

END OF STEPS

3.14 To create a span rule

3.14.1 Purpose

A span rule is a policy that specifies to which span of control profiles, in addition to the Default Service Span, a newly created service is automatically assigned. You must have an account with an assigned security scope of command role to perform this procedure.

See [3.5 “Sample span rule configuration” \(p. 37\)](#) for a sample span rule configuration and implementation.

3.14.2 Steps

1

Using an account with an assigned security scope of command role, choose Administration→Span Rules from the 5620 SAM main menu. The Span Rules form opens.

2

Click Create. The Service Creation Span Rule (Create) form opens.

3

Configure the required parameters.

4

Associate one or more spans with the rule:

1. Click on the Spans tab and click Add. The Select Span(s) form opens.
2. Select one or more spans in the list and click OK.

5

Associate one or more format or range policies with the rule:

1. Click on the Format and Range Policies tab and click Add. The Select Format or Range Policies form opens.
2. Select one or more policies in the list and click OK.


-
- 6 _____
Save your changes and close the form.

END OF STEPS _____

3.15 To create a 5620 SAM user group

3.15.1 Steps

- 1 _____
Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.
- 2 _____
Click on the User Groups tab and click Create. The User Group (Create) form opens.
- 3 _____
Configure the required parameters.
- 4 _____
If the user group is for OSS users or remote GUI users, configure the required parameters in the Remote Users panel.
- 5 _____
Select a scope of command profile in the Scope of Command panel.
- 6 _____
Select a span of control profile in the Span of Control panel.
- 7 _____
If you are modifying a user group, click on the Format and Range Policies tab. The Select Format or Range Policies form opens.
- 8 _____
Select one or more policies and click OK.

 **Note:** When you change the scope of command or span of control profiles of a group, the permissions of each user in the group are altered immediately when you click OK.
You cannot delete a user group that contains users.

9 _____

Save your changes and close the form.

10 _____

If an active client GUI session is affected by the user group modification, restart the GUI client.

END OF STEPS _____

3.16 To add or remove workspaces for a user group

3.16.1 Steps

1 _____

Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.

2 _____

Click on the User Groups tab.

3 _____

Click Create or choose a user group and click Properties. The User Group (Create|Edit) form opens.

4 _____

Configure the Allow Mandatory Workspaces Only parameter in the Mandatory Workspaces panel:

a. Select the Allow Mandatory Workspaces Only check box.



Note: If you select the Allow Mandatory Workspaces Only check box, the Add button on the User Preferences→Workspaces form is dimmed and the user cannot change the list of workspaces on their User Preferences form. Any existing user-defined workspaces in the User Preferences form are deleted when the Allow Mandatory Workspaces Only check box is selected. The user can change the order that the workspaces appear in the workspace selector and set any workspace as the default workspace.

b. Deselect the Allow Mandatory Workspaces Only check box.



Note: The user can add additional workspaces to their workspace selector by clicking Add in the User Preferences form. See “5620 SAM GUI custom workspace procedures” in the *5620 SAM User Guide* for more information.

The user can change the order that the workspaces appear in the workspace selector and set any workspace as the default workspace.

5

Add mandatory workspaces to a specific user group:

1. Click Add. The Add Workspace form opens.
2. Choose a workspace from the list and click OK. The Add Workspace form closes.

Note:

All mandatory workspaces that are added to the user group by the Administrator appear in the User Preferences→Workspaces form and in the workspace selector drop-down for each user in the user group and cannot be deleted.

6

To remove a workspace from the user group, choose a workspace in the Mandatory Workspaces panel and click Delete.

7

Click Move Up or Move Down to move the workspaces up or down. The workspace at the top of the list is the default workspace.



Note: You need a minimum of one workspace in the User Group. If the last user workspace is deleted, the users default workspace in the User Preferences form is replaced by the user group default workspace.

8

Save your changes and close the form.

END OF STEPS

3.17 To create a 5620 SAM user account



Note: If you want to delete a 5620 SAM user account, schedules associated with the user account are deleted only if the schedule is not associated with a scheduled task.

3.17.1 Steps

1

Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.

2 _____

Click on the Users tab and click Create. The User (Create) form opens.

3 _____

Configure the required parameters.

4 _____

Click Select and choose a user group.

5 _____

If required, test the validity of the user E-mail address by clicking Test E-mail beside the E-mail Address parameter.



Note: Before you test the validity of the user E-mail address, ensure that the outgoing SMTP E-mail server and E-mail test message are configured. See [3.24 "To configure automated E-mail notification" \(p. 61\)](#) for information about configuring the outgoing E-mail server and test message.

6 _____

Configure the parameters in the Password panel.

7 _____

Configure the Non-Web Maximum Sessions Allowed parameter.

8 _____

Configure an OSS user account:

1. Configure the required parameters in the OSS Session panel.
2. To apply a GUI alarm filter to alarm information requests from the OSS user, click Select in the OSS Session panel and choose an alarm filter.

9 _____

Configure the required parameters in the Client IP Address panel.

10 _____

Save your changes and close the form.

END OF STEPS _____

3.18 To copy a 5620 SAM user account

3.18.1 Steps

1 _____

Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.

2 _____

Click on the Users tab.

3 _____

Choose a user and click Properties. The User *type_of_user*, Group *user_group* (Edit) form opens.

4 _____

Click Copy. A User (Create) form opens for the second user.

5 _____

Configure the required parameters. You must change the User Name parameter and configure the User Password and Confirm Password parameters.

6 _____

Save your changes and close the form.

END OF STEPS _____

3.19 To configure global user account, password

3.19.1 Steps

1 _____

Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.

2

Configure the Password Reuse Cycle and Password History Duration (days) parameters.

3

Configure the required parameters in the Expiry Periods panel.



Note: If you set any of the parameters to 0, the corresponding expiry period check is disabled.

You can specify how long an account can remain dormant before the account is locked using the Account Expiry (days) parameter.

When a user attempts to log in with an expired password, the user account is suspended. When a user updates their password, the password expiry period is reset, and the new password again expires when the Password Expiry (days) parameter value is reached.

4

Save your changes and close the form.

END OF STEPS

3.20 To configure the GUI client inactivity timeout

3.20.1 Steps

1

Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.

2

Change the GUI inactivity check for all 5620 SAM GUI users.

1. Configure the Non-Web Client Timeout (minutes) parameter.
2. Click Apply.

3

Change the GUI inactivity check for all users in a user group:

1. Click on the User Groups tab. A list of user groups is displayed.
2. Choose a user group from the list and click Properties. The User Group *name* (Edit) form opens.
3. Enable the Non-Web Override Global Timeout parameter.
4. Configure the Non-Web Client Timeout (minutes) parameter.

4 _____

Save your changes and close the form.

END OF STEPS _____

3.21 To configure the minimum allowable user name length

3.21.1 Steps

1 _____

Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.

2 _____

In the User Name panel, check the Enable box.

3 _____

Configure the Minimum User Name Length Allowed parameter.

4 _____

Save your changes and close the form.

END OF STEPS _____

3.22 To configure authentication failure actions

3.22.1 Purpose

You can specify an authentication message or a lockout for a user account that exceeds the configured number of login authentication attempts. Only non-admin accounts can be locked out. Admin accounts always have access.

3.22.2 Steps

1 _____

Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.

2 _____

Click on the E-mail tab and configure the required parameters in the Authentication Failure Actions panel.

If you set the Attempts before lockout parameter to 0, the lockout function is disabled.

3 _____

Save your changes and close the form.

END OF STEPS _____

3.23 To configure suspended account actions

3.23.1 Steps

1 _____

Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.

2 _____

Click on the E-mail tab.

3 _____

Configure the parameters in the Suspended Account Actions panel.

4 _____

Save your changes and close the form.

END OF STEPS _____

3.24 To configure automated E-mail notification

3.24.1 Purpose

You can configure the 5620 SAM to automatically send E-mail messages to users and administrators; for example, when locking out a user account that exceeds the allowed number of authentication attempts.

3.24.2 Steps

- 1 _____
Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.
- 2 _____
Click on the E-mail tab.
- 3 _____
Configure the required parameters in the Outgoing E-mail Server SMTP panel.
- 4 _____
Configure the Test Message parameter.
- 5 _____
Save your changes and close the form.

END OF STEPS _____

3.25 To list inactive user accounts

3.25.1 Steps

- 1 _____
Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.
- 2 _____
Click on the Users tab.
- 3 _____
Click Inactive User Search and perform one of the following:
 - a. Choose ≥ 90 Days.
 - b. Choose ≥ 180 Days.
 - c. Specify another period:
 1. Choose Custom User Inactivity Period. The Custom User Inactivity Period form opens.
 2. Configure the User inactive greater than or equal to parameter.

User accounts that have been inactive for a number of days that are greater than or equal to the specified value are listed on the 5620 SAM User Security - Security Management (Edit) form.

- 4 _____
Save your changes and close the form.

END OF STEPS _____

3.26 To suspend or reinstate a 5620 SAM user account

3.26.1 Steps

- 1 _____
Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.
- 2 _____
Click on the Users tab.
- 3 _____
Select a user account and click Properties. The User *type_of_user* (Edit) form opens.
- 4 _____
Configure the User State parameter to suspend or reinstate the user account.
- 5 _____
Save your changes and close the form.

END OF STEPS _____

3.27 To administratively change the password of a 5620 SAM user

3.27.1 Purpose

The system administrator uses the Security Management form to maintain user accounts. The user can change their password in a separate form. If a user forgets their password, the system administrator can change the password and inform the user of the new password.

When a user attempts to log in with an expired password, the user account is suspended. When a user updates their password, the password expiry period is reset, and the new password again expires when the Password Expiry (days) parameter value is reached.

3.27.2 Steps

- 1 _____
Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.
- 2 _____
Click on the Users tab.
- 3 _____
Select a user and click Properties. The User *type_of_user* (Edit) form opens.
- 4 _____
Configure the User Password parameter and the Confirm Password parameter.
- 5 _____
Save your changes and close the form.

END OF STEPS _____

3.28 To force a 5620 SAM user password change

3.28.1 Purpose

You can force a specific 5620 SAM user to change the user password during the next login attempt.

The next time the user logs in to the 5620 SAM, the 5620 SAM prompts the user to change the password. After the user changes the password, the Password Change Required check box returns to the default of unchecked.



Note: This change does not affect the current user session.

3.28.2 Steps

- 1 _____
Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.

- 2 _____
Click on the Users tab.
- 3 _____
Choose a user and click Properties. The User *type_of_user* (Edit) form opens.
- 4 _____
Enable the Password Change Required check box to request a password change for the user.
- 5 _____
Save your changes and close the form.

END OF STEPS _____

3.29 To change the password of the current 5620 SAM user



Note: When a user attempts to log in with an expired password, the user account is suspended.

When a user updates a password, the password expiry period is reset.

3.29.1 Steps

- 1 _____
Choose Administration→Security→Change Password from the 5620 SAM main menu. The Password Change form opens.
- 2 _____
Verify that the Login Name matches your user account name.
- 3 _____
Configure the required password parameters.

- 4 _____
Save your changes and close the form.

END OF STEPS _____

3.30 To export the local tab preferences of one or more users

3.30.1 Purpose

You can export the local tab preferences of single or multiple users to a specified directory. You can reuse these saved tab preferences settings by importing them later.

The exported settings are the local tab preferences saved for the selected users, not the custom tab preferences saved in a workspace. See “Tab preferences” in the 5620 SAM User Guide.

3.30.2 Steps

- 1 _____
Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.
- 2 _____
Click on the Users tab.
- 3 _____
Choose one or more users from the list.
- 4 _____
Click Tab Preferences and choose Export to export the selected user’s local tab preferences to a specified directory. The Export Directory window opens.
- 5 _____
Specify the export directory, or create a directory or folder, and click OK. The selected user’s local tab preferences are exported to the specified directory.

6 _____
Close the form.

END OF STEPS _____

3.31 To assign local tab preferences to users

3.31.1 Steps

1 _____
Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.

2 _____
Click on the Users tab.

3 _____
Choose one or more users from the list.

4 _____
Click Tab Preferences and choose Assign to assign the tab preferences from the specified directory to the selected users. The Import Directory window opens. To export local tab preferences to a specified directory, see [3.30 “To export the local tab preferences of one or more users” \(p. 66\)](#) .

5 _____
Navigate to the directory from which you need to assign a tab preference.



Note: Only a single user’s tab preferences can be in the specified directory or an error message appears.

6 _____
Click Open and click Yes. The assigned tab preferences overwrite the local tab preferences of the selected users.
All affected users who currently have a client session opened, other than the client session where the assign has been initiated, will receive a system-generated text message informing them that their local tab preferences have been changed and they should restart their 5620 SAM client or risk losing the changes.
The user can click on the reply button to reply to the message.

7 _____
Close the forms.

END OF STEPS _____

3.32 To send a broadcast message to 5620 SAM GUI users

3.32.1 Steps

1 _____
Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.

2 _____
Click on the Sessions tab.

3 _____
Select the required client session and click Text Message. The Text Message form opens.

4 _____
Enter a message in the Text Message form and click Send.

5 _____
Close the form.

END OF STEPS _____

3.33 To view and manage active 5620 SAM client sessions

3.33.1 Steps


1 _____
Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.

2 _____
Click on the Sessions tab.

3 _____
Specify a filter to create a filtered list of GUI or 5620 SAM-O JMS client sessions and click Search. The active client sessions are listed.

4 _____
Review the session information.

5 _____
To close a GUI client session, select a session in the list and click Close Session.

 **Note:** Closing a 5620 SAM-O session has additional dependencies; see [3.34 "To disconnect a 5620 SAM-O JMS client connection or remove a durable subscription" \(p. 68\)](#) for more information.

6 _____
Close the form.

END OF STEPS _____

3.34 To disconnect a 5620 SAM-O JMS client connection or remove a durable subscription

3.34.1 Steps

1 _____
Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.

2 _____
Click on the Messaging Connections tab.

3 _____
Specify a filter and click Search. A list of active 5620 SAM-O client connections opens.

4 _____
Select a connection in the list and perform one of the following:
a. Click Close Connection to shut down the client connection.
b. Click Remove Connection to shut down the client connection and remove the durable subscription.

5

Click Yes. The action is performed.

If you choose Close Connection, the connection is terminated, but the 5620 SAM server continues to store JMS messages for the session.

If you choose Remove Connection, the 5620 SAM server stops storing the JMS messages for the session.

i **Note:** When you remove a durable subscription, the OSS client can still attempt to connect to the 5620 SAM-O. You can prevent an OSS client from attempting to connect by suspending the OSS user account. See [3.26 “To suspend or reinstate a 5620 SAM user account” \(p. 63\)](#) for more information.

6

Close the form.

END OF STEPS

3.35 To view the user activity log

3.35.1 Purpose

You can view user activity log entries associated with the following:

- a user
- a client session



Note: Viewing user activity records other than LI activity records requires a user account with an assigned Administrator or 5620 SAM Management and Operations scope of command role.

Viewing LI user activity records requires a user account with an assigned Lawful Interception Management scope of command role. The scope is restricted to the records of users in the same LI user group.

3.35.2 Steps

1

Choose Administration→Security→User Activity from the 5620 SAM main menu. The 5620 SAM User Activity form opens.

2

Perform one of the following:

- a. View the activities performed during a specific client session:

1. Configure the filter criteria, if required, and click Search. A list of session entries is displayed.

Note:

Only client session entries with a State value of Connected contain activity entries.

2. Select the required session entry and click Properties. The Session form opens.
 3. Click on the Activity tab.
 4. Configure the filter criteria, if required, and click Search. A list of activity entries is displayed.
- b. View the activities of a specific user:
1. Click on the Activity tab.
 2. Specify the required username as the Username filter criterion and click Search. A list of user-specific entries is displayed.

3

Select an entry in the list and click Properties. The Activity form opens.

4

Review the general information, which matches the columnar information on the User Activity list form.

5

Depending on the activity Type and Sub Type, the Additional Info panel contains detailed activity information. If required, expand the panel to review the information. The following information is listed:

- **Type Operation, all Sub Types:**

- left pane—object hierarchy in tree form; each object is selectable

- right pane—properties and values of selected object in left pane

The Actions property, which is highlighted in yellow for an object creation or modification activity, has values that represent the actions associated with the activity, such as create and modify.

- **Type Deployment or Save, Sub Type Modification:**

- Property Name column—list of modified parameters

- New Value column—the parameter value set during the activity

- Old Value column—the previous parameter value

6

If required, expand the XML panel to display more information about the activity. The panel displays the following information:

- Full Class Name—the 5620 SAM class descriptor of the affected object type

- Additional Info—the activity details in the form of an XML request

i **Note:** The displayed Additional Info text is limited to 4000 characters. If an activity generates more than 4000 characters of XML text, for example, access interface creation, the Additional Info panel of the log entry contains a “truncated” object, and the XML text contains a closing <truncated/> tag.

7

To navigate directly to the object of the activity, click View Object. The object properties form opens.

i **Note:** The View Object button is dimmed when there is no object associated with the activity, for example, a user login or logout operation.

8

View the activity information and close the form.

END OF STEPS

3.36 To view the user activity associated with an object

3.36.1 Steps

1

Open the required object properties form.

2

Click User Activity. The Activity form opens.

i **Note:** The User Activity function is available only for objects that exist in the 5620 SAM database. For example, the function is not available on the User Preferences form, because the settings on the form are saved in the client or client delegate file system.

3 _____

Review the activity entries as described in [3.35 “To view the user activity log”](#) (p. 70) and close the form.

END OF STEPS _____

3.37 To create a proprietary 5620 SAM login statement

3.37.1 Steps

1 _____

Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.

2 _____

Configure the security statement parameters.

The Statement parameter text is displayed on the login form during each subsequent client GUI login attempt.

3 _____

Save your changes and close the form.

END OF STEPS _____

3.38 To change the maximum number of concurrent 5620 SAM admin user sessions

3.38.1 Steps

1 _____

Log in to the main server station as the samadmin user.

2 _____

Navigate to the /opt/5620sam/server/nms/config directory.

3 _____

Create a backup copy of the nms-server.xml file.

4



CAUTION

Service Disruption

Contact technical support before you attempt to modify the `nms-server.xml` file.

Modifying the `nms-server.xml` file can have serious consequences that can include service disruption.

Open the `nms-server.xml` file using a plain-text editor.

5

Locate the following XML tag:

```
<samsession
```

This section of the file contains the maximum number of admin sessions that can be configured.

```
max5620SAMAdminSessions="value"
```

where *value* is the max number of allowed admin user sessions.

6

Save and close the `nms-server.xml` file.

7

Open a console window.

8

Navigate to the `/opt/5620sam/server/nms/bin` directory.

9

Enter the following at the prompt:

```
bash$ ./nmserver.bash read_config ↵
```

The main server reads the `nms-server.xml` file and the number of sessions defined.

10

Log out of the main server and close the open console windows.

END OF STEPS

3.39 To configure the number of allowed client sessions for a client delegate server



Note: The 5620 SAM continues to accept new client sessions from a client delegate server after the allowed number of sessions is reached. The maximum number of sessions is used as a guide for balancing the client session load among multiple client delegate servers.

3.39.1 Steps

1

Using an account with Update permission on the Server package, choose Administration→System Information from the 5620 SAM main menu. The System Information form opens.

2

Click on the Client Delegate Servers tab.

3

Select a client delegate server and click Properties. The Client Delegate Server (Edit) form opens.

4

Configure the Maximum UI Sessions parameter.

5

Save your changes and close the form.

END OF STEPS

3.40 To enable secure access for remote LDAP users



CAUTION

Service Disruption

Performing the procedure requires a restart of each main server in the 5620 SAM system, which is service-affecting.

You must perform the procedure only during a scheduled maintenance period.



Note: SSL must be enabled in the 5620 SAM system, as described in the *5620 SAM | 5650 CPAM Installation and Upgrade Guide*.

The remote LDAP server must be operational and accessible to the 5620 SAM system when you perform the procedure.

In a redundant 5620 SAM system, you must perform the procedure first on the standby main server.

3.40.1 Steps

1

Log in as the samadmin user on the main server station.

2

Open a console window.

3

Navigate to the /opt/5620sam/server/nms/bin directory.

4

Enter the following to import the LDAP server SSL certificate to the 5620 SAM keystore:

```
bash$ ./nmserver.bash add_to_keystore IP_addressport ↵
```

where

IP_address is the remote LDAP server IP address

port is the required LDAP server port

The script prompts you for the keystore alias.

5

Press ↵ to accept the default.

The script prompts you for the keystore password.

6

Enter the keystore password that you specified when you enabled SSL in the 5620 SAM system.

The 5620 SAM imports the certificate to the keystore.

7

Restart the main server.



Note: When you restart the primary main server in a redundant system, a server activity switch occurs, and the standby main server assumes the primary role.

1. Enter the following:

```
bash$ ./nmserver.bash force_restart ↵
```

2. If you are restarting the standby main server in a redundant system, enter the following to display the server status:

```
bash$ ./nmserver.bash -s nms_status ↵
```

The command returns server status information.

Do not proceed to the next step until the command returns the following, which means that the main server is completely started.

```
-- SAM Server is UP
```

8

Close the console window.

END OF STEPS

3.41 To enable remote user authorization via RADIUS

3.41.1 Steps



Note: You must perform [Step 1](#) to [Step 8](#) on each main server in the 5620 SAM system.

Enable RADIUS remote authorization in 5620 SAM

1

Log in to the main server station as the samadmin user.

2 _____
Open a console window.

3 _____
Navigate to the `/opt/5620sam/server/nms/config` directory.

4 _____
Open the `SamJaasLogin.config` file using a plain-text editor such as `vi`.

5 _____
Locate the `RADIUSLogin` section of the file and set the `samvsa` parameter to `true`, as shown in Code [Figure 2, “SamJaasLogin.config file, RADIUS parameters” \(p. 77\)](#) :

Figure 2 SamJaasLogin.config file, RADIUS parameters

```
RADIUSLogin
{
com.timetra.nms.server.jaas.provider.radius.auth.Radius-
JaasLoginModule REQUIRED
    debug=false
    samvsa=true
    ;
};
```

6 _____
Save and close the file.

7 _____
Perform one of the following.

- a. On a standalone main server, or the primary main server in a redundant system, enter the following:

```
bash$ /opt/5620sam/server/nms/bin/nmsserver.bash read_config
↵
```

- b. On the standby main server in a redundant system, enter the following:

```
bash$ /opt/5620sam/server/nms/bin/nmsserver.bash force_
restart ↵
```

The main server puts the configuration changes into effect.

8 _____
Close the console window.

Configure remote RADIUS server

9

Copy the RADIUS dictionary section in Code [Figure 3](#), “5620 SAM RADIUS dictionary entry” (p. 78) to the RADIUS dictionary file on the RADIUS server.



Note: The vendor ID must be 123.

Figure 3 5620 SAM RADIUS dictionary entry

```
VENDOR          Nokia          123
BEGIN-VENDOR
ATTRIBUTE       Sam-security-group-name 3      group_name
END-VENDOR          Nokia
```

10

Change *group_name* in the entry to the name of a valid 5620 SAM user group.

11

As the RADIUS server administrator, add the Sam-security-group-name VSA to the RADIUS user profile, as shown in the following:

```
Sam-security-group-name="5620_SAM_user_group"
```

where *5620_SAM_user_group* is the name of a valid 5620 SAM user group

END OF STEPS

3.42 To enable remote user authorization via TACACS+

3.42.1 Steps



Note: You must perform [Step 1](#) to [Step 8](#) on each main server in the 5620 SAM system.

Enable TACACS+ remote authorization in 5620 SAM

1

Log in to the main server station as the samadmin user.

2

Open a console window.

3

Navigate to the /opt/5620sam/server/nms/config directory.

4

 Open the SamJaasLogin.config file using a plain-text editor such as vi.

5

 Locate the TACACSLogin section of the file and set the samvsa parameter to true, as shown in Code [Figure 4, "SamJaasLogin.config file, TACACS+ parameters" \(p. 79\)](#) :

Figure 4 SamJaasLogin.config file, TACACS+ parameters

```
TACACSLogin
{
    com.timetra.nms.server.jaas.provider.tacacs.auth.
    TacacsPlusJaasLoginModule REQUIRED
    debug=false
    samvsa=true
    ;
};
```

6

 Save and close the file.

7

 Perform one of the following.

- a. On a standalone main server, or the primary main server in a redundant system, enter the following:

```
bash$ /opt/5620sam/server/nms/bin/nmserver.bash read_config
↵
```

- b. On the standby main server in a redundant system, enter the following:

```
bash$ /opt/5620sam/server/nms/bin/nmserver.bash force_
restart ↵
```

8

 Close the console window.

Configure remote TACACS+ server

9

 As the TACACS+ server administrator, add the user group VSA to the TACACS+ user profile, as shown in the following:


```
service=sam-app{
  sam-security-group="5620_SAM_user_group"
}
```

where *5620_SAM_user_group* is the name of a valid 5620 SAM user group

END OF STEPS


3.43 To configure 5620 SAM remote user authentication

3.43.1 Steps

Assign default external user group

- 1

Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.
- 2

Select a user group in the Default External User Group panel.
 **Note:** Do not select a user group that has the Apply Local Authentication Only parameter enabled, or remote login attempts fail.
- 3

Save your changes and close the form.

Configure remote servers

- 4

Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM Remote User Authentication from the 5620 SAM main menu. The Remote Authentication Manager (Edit) form opens.
- 5

Configure the parameters.
- 6

Configure one or more RADIUS authentication servers, as required.
 1. Click on the RADIUS tab and click Create. The SAM RADIUS Authentication Server (Create) form opens.
 2. Configure the required parameters.

3. Save your changes.

7

Configure one or more TACACS+ authentication servers, as required.

1. Click on the TACACS tab and click Create. The SAM TACACS+ Authentication Server (Create) form opens.
2. Configure the required parameters.
3. Save your changes.

8

Configure one or more LDAP authentication servers, as required.

1. Click on the LDAP tab and click Create. The LDAP Authentication Server (Create) form opens.
2. Configure the general parameters.

Note:

The ID value that you specify defines the server priority. For example, if multiple servers are specified, the 5620 SAM attempts user authentication using the server that has the lowest ID value first. If the server is unavailable, the 5620 SAM attempts to connect to the other specified servers, in sequence, by ID.

3. Configure the parameters in the Lookup Credentials panel, if the LDAP server does not allow anonymous lookups.

The Bind DN parameter specifies the LDAP attribute set that identifies a user who is authorized to perform LDAP lookups; the Bind DN password is the password of the user.

4. Configure the parameters in the User Lookup Settings panel.

The Base DN parameter specifies the LDAP context for username and password lookup; for example, ou=People,dc=MyCompany,dc=org.

The Base Filter parameter specifies a filter for the username query. The parameter format is the following:

(attribute={USERNAME})

where

attribute is the LDAP attribute that contains the username

The 5620 SAM replaces {USERNAME} with the username provided during a login attempt; for example, (cn={USERNAME}) maps the "cn" LDAP attribute to the username.

5. If the LDAP server has user role information and is to provide the name of a user group, configure the parameters in the Group Lookup Settings panel.

Note:

The user group name that an LDAP server provides must match the name of a valid 5620 SAM user group; otherwise, an authenticated user is assigned to the default external user group.

The Group DN parameter specifies the LDAP context for group lookup; for example:

```
ou=Roles,dc=MyCompany,dc=org
```

The Group Filter parameter format is one of the following:

- **simple; the 5620 SAM replaces {1} with the DN of the user LDAP record**
(*attribute*={1})

where *attribute* is the LDAP attribute that contains the DN

- **compound; the 5620 SAM replaces {USERNAME} with the username provided during a login attempt**
(*&(any_attribute=string)(user_attribute={USERNAME})*)

where

any_attribute is an LDAP attribute

string is the attribute value to match

user_attribute is the LDAP attribute that contains the username

The Attribute ID parameter specifies one of the following:

- the LDAP attribute name that maps to a 5620 SAM group name
- the DN of the query context, if the Attribute is DN? parameter is selected; the “name” attribute in the record maps to a 5620 SAM group name

6. Save your changes.

9

Close the Remote Authentication Manager (Edit) form.

END OF STEPS

3.44 To change the 5620 SAM Task Manager settings



Note: The Task Manager is operational with the default values.

3.44.1 Steps

1

Log in to the 5620 SAM main server station as the samadmin user.

2

Open a console window.

3 _____
Navigate to the `/opt/5620sam/server/nms/config` directory.

4 _____

 **CAUTION**
Service Disruption

Contact technical support before you attempt to modify the `nms-server.xml` file.

Modifying the `nms-server.xml` file can have serious consequences that can include service disruption.

Open the `nms-server.xml` file using a plain-text editor such as `vi`.

5 _____

Find and configure the required parameters:

- `maxNumRetainedTasks`
- `numTasksToPurgeWhenFull`
- `successfulTasksPurgeInterval`
- `failedTasksPurgeInterval`

6 _____

Save and close the `nms-server.xml` file.

7 _____

Navigate to the `/opt/5620sam/server/nms/bin` directory.

8 _____

Enter the following to restart the main server:

```
bash$ ./nmserver.bash force_restart ↵
```

The main server restarts, and the configuration change takes effect.

9 _____

Modify the client configuration, if required.

1. Log in to a 5620 SAM single-user client or client delegate server station.

Note:

If you log in to a RHEL client delegate server station, you must log in as the `samadmin` user.

If you log in to a single-user client station, you must log in as the user who installed the client, or as a local administrator.

2. Open a console window.
3. Navigate to the client configuration directory, typically `/opt/5620sam/client/nms/config` on RHEL, and `C:\5620sam\client\nms\config` on Windows.
4. Open the `nms-client.xml` file using a text editor.
5. Configure the `autoRefreshInterval` parameter.
6. Save and close the `nms-client.xml` file.
7. Repeat [Step 7](#) and [Step 8](#) to restart the main server.

10

Close the console windows and form. See the *5620 SAM User Guide* to monitor the Task Manager.

END OF STEPS

3.45 To export all workspaces and local tab preferences

3.45.1 Steps

1

Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.

2

Click Settings and choose Export All. The Export Directory window opens.

3

Specify the export directory, or create a directory or folder, and click Save. All the workspaces and local tab preferences are exported to the specified directory. If the directory exists, a dialog box appears.

4

Click Yes to overwrite all the workspaces and local tab preferences saved in the existing directory.

5 _____
Close the form.

END OF STEPS _____

3.46 To import workspaces and local tab preferences

3.46.1 Steps

1 _____
Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.

2 _____
Click Settings and choose Import. The Import Directory window opens.

3 _____
Click on the drop-down menu and choose one of the following:

- a. Import All (default)—to import all the workspaces and local tab preferences.
If you choose this option, you can click on the Overwrite Existing Workspace(s) check box to allow overwriting of existing workspaces.
- b. Import Workspaces Only—to import only workspaces from the specified directory.
If you choose this option, you can click on the Overwrite Existing Workspace(s) check box to allow overwriting of existing workspaces.
- c. Import Tabs Only—to import only local tab preferences from the specified directory.

4 _____
Click Open. A confirmation dialog box displays the number of workspaces and local tab preferences that will be imported from the specified directory.

5 _____
Click Yes.
All users who have their local tab preferences changed and currently have a client session opened, other than the client session where the import has been initiated, will receive a system-generated text message informing them that their local tab preferences have been changed and they should restart their 5620 SAM client or risk losing the changes.
The user can click on the reply button to reply to the message.

For all users who have their current workspace changed and currently have a client session opened, the workspace selector displays Workspace Out of Sync. Select the current workspace from the workspace selector drop-down menu to apply the modified settings.

6 _____

Close the form.

END OF STEPS _____

4 NE user and device security

4.1 Overview

4.1.1 Purpose

This chapter describes procedures for configuring NE user and device security.

4.1.2 Contents

NE user and device security	91
4.2 Overview	91
4.3 RADIUS, TACACS+, and LDAP	92
4.4 CPM filters and traffic management	93
4.5 DoS protection	94
4.6 DDoS protection	95
4.7 IP security	97
4.8 7705 SAR-H firewalls	97
NE user and device security procedures	99
4.9 Workflow to manage NE user and device security	99
4.10 To configure a MAF	101
4.11 To configure a CPM filter	103
4.12 To configure an NE DoS protection policy	105
4.13 To view NE DoS protection violations	106
4.14 To configure an NE DDoS protection policy	107
4.15 To configure a site user profile	110
4.16 To configure a user account on a managed device	111
4.17 To configure a password policy	112
4.18 To configure an NE RADIUS authentication policy	113
4.19 To configure an NE TACACS+ authentication policy	114
4.20 To configure an OmniSwitch RADIUS, TACACS+, or LDAP security authentication policy	116

4.21	To configure device system security settings	117
4.22	To configure and manage PKI site security on an NE	120
4.23	To configure a PKI certificate authority profile	123
4.24	To create a file transmission profile	124
4.25	To perform CMPv2 actions	125
4.26	To distribute a license key to all 7705 SAR-H nodes	128
4.27	To configure a 7705 SAR-H NE firewall	129
4.28	To configure an NE management access firewall on a 7705 SAR-H	131
4.29	To configure an NE CPM firewall on the 7705 SAR-H	133
4.30	To delete a security policy	134
4.31	To manually unlock a user account	135
4.32	To clear the password history of a user on a managed device	136
4.33	To clear collected statistics on a CPM filter	137
4.34	To manage OCSP cache entries on an NE	138

NE user and device security

4.2 Overview

4.2.1 Access management



CAUTION

Service Disruption

The 5620 SAM cannot obtain a secret value from an NE during resynchronization. It is recommended that you use only the 5620 SAM to configure a shared authentication secret.

Do not configure a shared authentication secret directly on a managed NE using another interface, for example, a CLI, or the 5620 SAM cannot synchronize the security policy with the NE.

You can use the 5620 SAM to configure security for managed-device access that includes the following:

- device user accounts, profiles, and passwords
- RADIUS, TACACS+, and LDAP authentication for 5620 SAM user accounts
- MAFs
- CPM filters
- DoS protection
- DDoS protection
- X.509 authentication

4.2.2 General rules

A 5620 SAM site user profile specifies which CLI commands or command groups are permitted or denied on a managed device. A profile can be associated with multiple 5620 SAM user accounts, and each user account can have up to eight associated profiles.

The following general rules apply to 5620 SAM security management for devices.

- The authentication settings on a device override any settings distributed by the 5620 SAM. For example, if you use the 5620 SAM to configure a user account with SHA authentication, and then distribute the account to a device that uses MD5 authentication, the account authentication type changes to MD5.
- MAFs and CPM filters must be manually distributed to a managed device.
- An operator can limit the type of managed device access per user, for example, allowing FTP access, but denying console, Telnet, and SNMP access.
- A user profile is independent of a user account, and is not in effect until associated with a user account.

4.3 RADIUS, TACACS+, and LDAP

4.3.1 Overview

RADIUS is an access server AAA protocol. The protocol provides a standardized method of exchanging information between a RADIUS client, which is located on a device and managed by the 5620 SAM, and a RADIUS server, which is located externally from the device and the 5620 SAM.

RADIUS provides an extra layer of login security. The RADIUS client relays user account information to the RADIUS server, which authenticates the user and returns user privilege information. The information defines the device access of the user. For example, a user may not be allowed to FTP information to or from the device.

You can create device user accounts as a backup to RADIUS, TACACS+, or LDAP authentication. In the event that a RADIUS, TACACS+, or LDAP function fails, the device user account provides device access.

TACACS+ and LDAP provide functions that are similar to RADIUS.



Note: The 5620 SAM checks for reachability to a TACACS+ server using UDP port 49 to prevent long timeout issues. However, all subsequent communication with the server uses TCP port 49.

See the appropriate RADIUS, TACACS+, or LDAP documentation for information about authentication server installation, configuration, and management.

For TACACS+ users, you can specify the following in a user template that is read by the global TACACS+ policy:

- the type of permitted device access, for example, console, FTP, or both
- a home directory
- a login script to execute

4.3.2 Combined local and remote authentication

An organization may have an established TACACS+ or RADIUS authentication configuration. You can add 5620 SAM client GUI user accounts to an existing TACACS+ or RADIUS user base for local authentication by a 5620 SAM server.

Consider the following:

- You can create a 5620 SAM user account that matches a TACACS+, RADIUS, or LDAP user account. For example, if the RADIUS user account is Jane, you can create a 5620 SAM user Jane.
- A 5620 SAM user name can be 1 to 80 characters, which is flexible enough to match most remote authentication user accounts.
- A 5620 SAM user that is authenticated remotely can log in to the 5620 SAM using the

RADIUS, TACACS+, or LDAP password.

- For local 5620 SAM user authentication, the account password must meet the 5620 SAM password requirements.

For example, for a user called Jane:

- The RADIUS user name is Jane, and the password is accessforjane.
- The 5620 SAM user name is Jane and password is !LetJane1In.

When Jane is authenticated by RADIUS, she can log in to the 5620 SAM client by typing in Jane and accessforjane. If the RADIUS server was down, and she could not be authenticated remotely, to be authenticated locally Jane must log in to the 5620 SAM client by typing jane and !LetJane1In.

4.4 CPM filters and traffic management

4.4.1 Overview

Device CPMs provide dedicated traffic management and queuing hardware to protect the control plane. You can use CPM filters to specify which types of traffic to accept or deny, and to allocate and rate-limit the shaping queues for traffic directed to the CPMs.



Note: The 7705 SAR does not support Queue filters or MAC CPM IP filters.

There is no partial distribution of CPM IP filter policies to a 7705 SAR. When you distribute a CPM IP Filter policy to a 7705 SAR, every entry, property, and value in the policy must be supported by the NE, or the policy distribution to the 7705 SAR is blocked.

4.4.2 Supported management functions

The 5620 SAM supports the following CPM traffic management functions:

- traffic classification using CPM filters
 - Packets going to the CPM are first classified by the IOM into forwarding classes before recognition by the CPM hardware. You can use CPM filters to further classify the packets using L3/L4 information, for example, destination IP, DSCP value, and TCP SYN/ACK.
- queue allocation
 - Queues 1 — 8 are the default queues. They cannot be modified or deleted. Unclassified traffic is directed to the default queues.
 - Queues 9 — 32 are reserved for future use.
 - Queues 33 — 2000 are available for allocation.
 - Queues 2001 — 8000 are used for per-peer queuing.
- queue configuration
 - PIR
 - CIR

- CBS
- MBS

4.5 DoS protection

4.5.1 Overview

The 5620 SAM supports the use of DoS protection on network and access interfaces. To protect NEs from the high incoming packet rates that characterize DoS attacks, you can use the 5620 SAM to configure DoS protection for the following scenarios:

- the arrival of unprovisioned link-layer protocol packets that are received from CE devices in the core network
- the arrival of excessive subscriber control-plane packets on L2 or L3 access interfaces in aggregation networks
- the arrival of excessive Ethernet CFM frames on L2 and L3 access interfaces, SAPs, and SDP bindings, based on a combination of CFM OpCode and MEG-level values

DoS protection limits the number of packets that are received each second, and optionally logs a violation notification if a policy limit is exceeded. You can use the NE System Security form to view the violations for a specific NE.

4.5.2 DoS protection in the core network

DoS protection in the core network limits the number of link-layer protocol packets that each network interface on an NE accepts for protocols that are not enabled on the interface. The interface drops the excessive packets before they are queued or processed by the CPU.

You can configure global DoS protection on an NE using the NE System Security form. DoS protection controls the following for unprovisioned link-layer protocols:

- the packet arrival rate per source on each network interface
- the overall packet arrival rate per source on the NE
- whether an NE sends a notification trap if a policy limit is exceeded

An NE that supports DoS protection automatically applies default DoS protection parameters to each network and access interface. These defaults limit only the overall packet arrival rate and apply to all of the interfaces on the NE.

4.5.3 DoS protection policies in aggregation networks

In a subscriber aggregation network, an NE typically receives few control-plane packets from a specific subscriber. If one or more subscribers generate excessive control-plane traffic, DoS protection policies can help to ensure that NEs do not become overburdened by these unwanted packets.

You can configure DoS protection policies to control the following on network interfaces, VPLS L2 access interfaces, and IES and VPRN L3 access interfaces:

- the control-plane packet arrival rate per subscriber host
- the overall control-plane packet arrival rate for the interface
- whether an NE sends a notification trap if a policy limit is exceeded

An NE that supports DoS protection automatically assigns a default DoS protection policy to each network and access interface. This default policy limits only the overall packet arrival rate for the interface, and cannot be deleted or modified.

See [4.12 “To configure an NE DoS protection policy” \(p. 105\)](#) for information about creating or modifying a DoS protection policy and assigning the policy to one or more NEs. See the appropriate service chapter for information about applying DoS protection policies to interfaces.

4.6 DDoS protection

4.6.1 Overview

DDoS protection extends DoS protection by controlling traffic destined for IOM or CPM CPUs on a per-SAP, per-protocol basis. A DDoS protection policy isolates protocols from each other and, at the same time, isolates subscribers so that attacks or misconfigurations affect only the source SAP or protocol.

Policers are used to enforce a traffic rate-limiting function. Rate limiting is configurable in packets per second or kb/s. Configurable burst tolerance allows extra full handshake attempts, as required by some protocols.

When a policer determines that a packet is non-conformant, it discards the packet or marks it as low-priority. Low-priority traffic is more likely to be discarded at a downstream queueing point if there is protocol congestion. Traffic marking is also useful for routing protocols, where an operator may need to offer all packets to the CPU, and only discard packets if the CPU cannot keep up. A policer can be mapped to one or more traffic protocols.

The following types of policer can be configured in a DDoS protection policy:

- static policers, which permanently instantiate enforcement policers on SAPs
- local monitoring policers, which dynamically instantiate enforcement policers on SAPs

A DDoS protection policy can be applied to a capture SAP or to an MSAP. A DDoS protection policy that is assigned to a capture SAP typically has higher traffic rate limiting values than a policy that is assigned to an MSAP.

A DDoS protection policy can be applied to the following objects:

- base router network interface other than a system or loopback interface

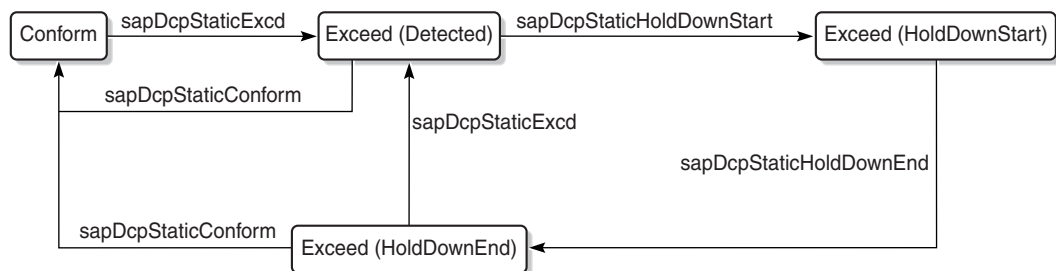
- VPRN network interface a loopback interface
- VPRN L3 access interface
- VPRN group interface SAP
- IES L3 access interface
- IES group interface SAP
- VPLS L2 access interface
- I-VPLS I-L2 access interface
- MVPLS L2 access interface
- I-MVPLS I-L2 access interface
- VLL E-Pipe L2 access interface
- VLL I-Pipe L2 access interface

4.6.2 DDoS alarm handling

The alarm messages generated by DDoS protection policies are presented in a unique manner. Instead of a new alarm message being generated in the Alarm Window every time a DDoS alarm event occurs for a given object, a single alarm message is generated and updated periodically as the object generates new DDoS alarm events. If an Alarm Information window is opened for an alarm message, the Additional Text field displays the updated alarm information.

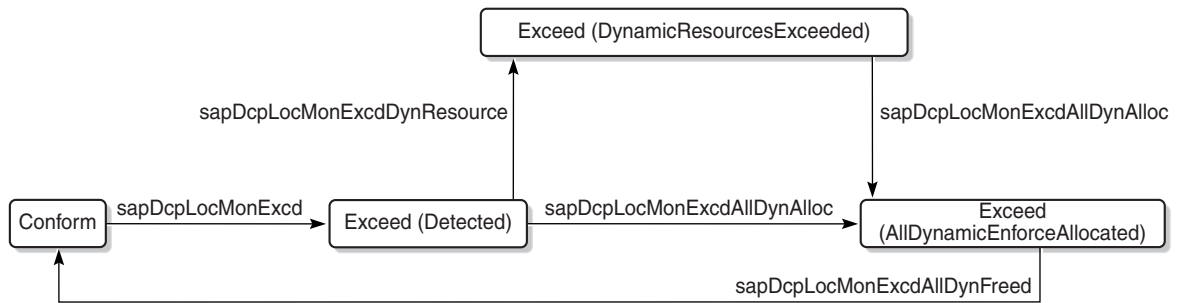
The operator can view dynamically updated alarm information, and avoid the generation of excessive numbers of individual DDoS alarm messages. [Figure 5, “Static policer alarm message sequence” \(p. 96\)](#) shows the alarm message sequence for a static policer. [Figure 6, “Local monitoring policer alarm message sequence” \(p. 97\)](#) shows the alarm message sequence for local monitoring policer. [Figure 7, “Dynamic policer alarm message sequence” \(p. 97\)](#) shows the alarm sequence for a dynamic policer. In each sequence, the alarm clears when the policer returns to the Conform state.

Figure 5 Static policer alarm message sequence



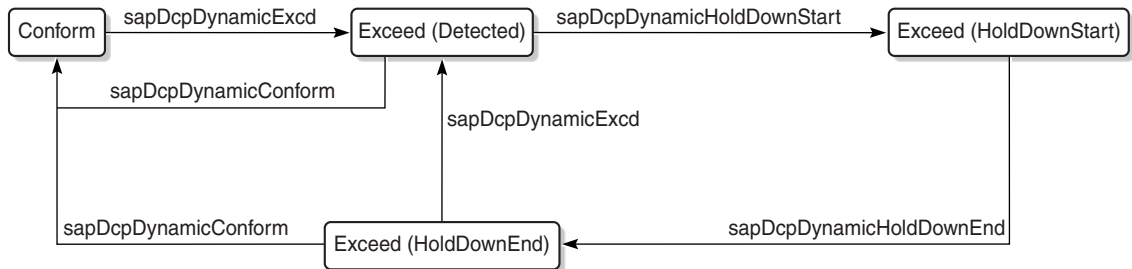
23498

Figure 6 Local monitoring policer alarm message sequence



23499

Figure 7 Dynamic policer alarm message sequence



23528

4.7 IP security

4.7.1 Overview

The 5620 SAM supports the IPsec MDA, which provides IP security support including tunneling and encryption functions. See the device security documentation for more information about configuring IP security.

4.8 7705 SAR-H firewalls

4.8.1 Overview

The 5620 SAM supports the firewall function on a Release 5.0 7705 SAR-H. Using the 5620 SAM, you can configure firewall policies, view the firewall status and display the firewall faults. The 5620 SAM supports the configuration of an individual NE instance or a policy that applies to multiple NEs. See [4.27 "To configure a 7705 SAR-H NE firewall" \(p. 129\)](#) for more information.



Note: Release 6.0 and later 7705 SAR-H devices do not support the firewall function.

4.8.2 Configuring a 7705 SAR-H firewall on a management or CPM interface

The 5620 SAM supports two interfaces to manage the control traffic on a Release 5.0 7705 SAR-H, for example, OSPF, BGP, RSVP-TE, LDP, and SNMP. These management interfaces allow zone definition entries to be applied to the firewall. The two interfaces are:

- the device management interface, which is the physical management Ethernet port on the main chassis; see [4.28 “To configure an NE management access firewall on a 7705 SAR-H ” \(p. 131\)](#) for configuration information

For the NE management access firewall interface on the management port, there is always only one set of zone rules applied to control traffic that arrives on the interface. The management zone rules are applied if configured on ingress to the firewall. If the control packets pass, they are sent to the CPM without any further egress rules applied.

- the device CPM interface, which is the in-band management interface; see [4.29 “To configure an NE CPM firewall on the 7705 SAR-H” \(p. 133\)](#) for configuration information

For the NE CPM firewall management interface, control traffic that is intended for the CPM has ingress and egress zone rules applied. When the control traffic ingresses the 7705 SAR-H on a source interface such as a SAP, spoke SDP, or network interface, the zone rules associated with the interface are applied to the firewall. If management zone rules are configured on the NE CPM firewall, the rules are applied to packets on egress from the firewall before processing by the CPM.

NE user and device security procedures

4.9 Workflow to manage NE user and device security

4.9.1 Process

- 1 _____
Specify the type of authentication keys used on the device; for example, SHA or MD5, as part of the device discovery. See “To commission a device for 5620 SAM management” in the *5620 SAM User Guide* for more information.
- 2 _____
As required, create and manage 5620 SAM user profiles and accounts. See [Chapter 3, “5620 SAM user security”](#) .
- 3 _____
Create a MAF for each device; see [4.10 “To configure a MAF” \(p. 101\)](#) .
- 4 _____
Create filter policies for device CPM modules; see [4.11 “To configure a CPM filter” \(p. 103\)](#) .
- 5 _____
Create NE DoS protection policies, as required to control the amount of subscriber-based control-plane traffic that the NE interfaces receive; see [4.12 “To configure an NE DoS protection policy” \(p. 105\)](#) .
- 6 _____
View NE DoS protection violations, as required; see [4.13 “To view NE DoS protection violations” \(p. 106\)](#) .
- 7 _____
Create NE DDoS protection policies, as required to isolate protocols from each other and isolate subscribers so that attacks or misconfigurations affect only the source SAP or protocol; see [4.14 “To configure an NE DDoS protection policy” \(p. 107\)](#) .
- 8 _____
Create site user profiles based on job classifications and the access needed to the managed devices; see [4.15 “To configure a site user profile” \(p. 110\)](#) .

- 9 _____
Create individual site user accounts based on the configured profiles; see [4.16 “To configure a user account on a managed device”](#) (p. 111) .

- 10 _____
Specify password policies for access to managed devices and users; see [4.17 “To configure a password policy”](#) (p. 112) .

- 11 _____
Create RADIUS, TACACS+, or LDAP access or security policies for user authentication on the managed device; see [4.18 “To configure an NE RADIUS authentication policy”](#) (p. 113) , [4.19 “To configure an NE TACACS+ authentication policy”](#) (p. 114) , or [4.20 “To configure an OmniSwitch RADIUS, TACACS+, or LDAP security authentication policy”](#) (p. 116) .

- 12 _____
View or configure the system security settings on managed NEs; see [4.21 “To configure device system security settings”](#) (p. 117) .

- 13 _____
As required, configure X.509 authentication or a PKI certificate authority profile; see [4.22 “To configure and manage PKI site security on an NE”](#) (p. 120) or [4.23 “To configure a PKI certificate authority profile”](#) (p. 123) .

- 14 _____
Perform PKI CMPv2 actions, as required, to obtain or assign keys from a CA; see [4.25 “To perform CMPv2 actions”](#) (p. 125) .

- 15 _____
Distribute a license key to all 7705 SAR-H nodes; see [4.26 “To distribute a license key to all 7705 SAR-H nodes”](#) (p. 128) .

- 16 _____
Configure an NE firewall on the 7705 SAR-H using the firewall manager; see [4.27 “To configure a 7705 SAR-H NE firewall”](#) (p. 129) .

- 17 _____
Configure an NE management access firewall on the 7705 SAR-H using the firewall manager; see [4.28 “To configure an NE management access firewall on a 7705 SAR-H ”](#) (p. 131) .

18 Configure an NE CPM firewall on the 7705 SAR-H using the firewall manager; see [4.29 “To configure an NE CPM firewall on the 7705 SAR-H” \(p. 133\)](#) .

19 Perform the following NE system security tasks, as required:

- Delete security policies; see [4.30 “To delete a security policy” \(p. 134\)](#) .
- Unlock user accounts that are locked due to failed login attempts; see [4.31 “To manually unlock a user account” \(p. 135\)](#) .
- Clear the password history for a user on a managed object; see [4.32 “To clear the password history of a user on a managed device” \(p. 136\)](#) .
- Perform CPMv2 certificate administration actions; see [4.25 “To perform CMPv2 actions” \(p. 125\)](#) .
- Clear collected statistics information on a CPM filter; see [4.33 “To clear collected statistics on a CPM filter” \(p. 137\)](#) .
- Clear OCSP cache entries on an NE; see [4.34 “To manage OCSP cache entries on an NE” \(p. 138\)](#) .

4.10 To configure a MAF



Note: To perform this procedure, you require an account with an assigned administrator scope of command role to the sitesec package, or a scope of command role with write access permission to the sitesec package.

4.10.1 Steps

1 Choose Administration→Security→NE Management Access Filters from the 5620 SAM main menu. The NE Management Access Filter form opens.

2 Click Create or choose a policy and click Properties. The Site Management Access Filter (Create|Edit) form opens.

3 Configure the general parameters.

4 Configure the required parameters in the IPv4, IPv6, and MAC panels.

5



CAUTION

Service Disruption

When you set the Action parameter to deny, you cannot distribute the MAF to an NE. You must set the parameter to permit, manually distribute the MAF as required, and then set the parameter to deny in each local MAF instance.

To configure an IPv4 or IPv6 entry, perform the following steps.

1. Click on the IPv4 Entries or IPv6 Entries tab.
2. Click Create or choose an entry and click Properties. The Site MAF Match Entry (Create|Edit) form opens.
3. Configure the required parameters.
4. Save your changes and close the form.

6

Repeat [Step 5](#) to configure an additional IPv4 or IPv6 entry, if required.

7

To configure a MAC entry, perform the following steps.

1. Click on the MAC Entries tab.
2. Click Create or choose an entry and click Properties. The Site MAC Match Entry (Create|Edit) form opens.
3. Configure the required parameters.
4. Click on the Filter Properties tab and configure the required parameters.

If you set the Frame Type parameter to e802dot2LLC, configure the parameters in the Match Criteria - DSAP SSAP panel.

If you set the Frame Type parameter to e802dot2SNAP, configure the parameters in the Match Criteria - SNAP panel.

If you set the Frame Type parameter to Ethernet II, configure the Ether Type parameter.

5. Save your changes and close the form.

8

Repeat [Step 7](#) to configure an additional MAC entry, if required.

9

Click Apply to save the changes.

10 _____

Distribute the MAF to NEs, as required.

11 _____

Close the open forms.

END OF STEPS _____

4.11 To configure a CPM filter



Note: To perform this procedure, you require an account with an assigned administrator scope of command role to the sitesec package, or a scope of command role with write access permission to the sitesec package.

The 7705 SAR does not support queue or MAC CPM filters.

4.11.1 Steps

1 _____

Choose Administration→Security→NE CPM Filter from the 5620 SAM main menu. The NE CPM Filter form opens.

2 _____

Click Create or choose a policy and click Properties. The CPM Filter (Create|Edit) form opens.

3 _____

Configure the required parameters.

4 _____

To configure an IPv4 filter entry, perform the following steps.

1. Click on the IPv4 Entries tab.
2. Click Create or choose an entry and click Properties. The CPM IP Filter Entry (Create|Edit) form opens.
3. Configure the required parameters.
4. Click Select to assign a Log ID to the CPM filter entry.
See the *5620 SAM User Guide* for information on configuring a Filter Log policy that employs this Log ID.
5. Click on the Filter Properties tab.
6. Configure the required parameters.
7. Save your changes and close the form.

5

Repeat [Step 4](#) to configure an additional IPv4 entry, if required.

6

To configure an IPv6 filter entry, perform the following steps.

1. Click on the IPv6 Entries tab.
2. Click Create or choose an entry and click Properties. The CPM IPv6 Filter Entry (Create|Edit) form opens.
3. Configure the required parameters.
4. Click Select to assign a Log ID to the CPM filter entry.
See the *5620 SAM User Guide* for information on configuring a Filter Log policy that employs this Log ID.
5. Click on the Filter Properties tab.
6. Configure the required parameters.
7. Save your changes and close the form.

7

Repeat [Step 6](#) to configure an additional IPv6 entry, if required.

8

To configure a MAC entry, perform the following steps.

1. Click Create or choose an entry and click Properties. The CPM MAC Filter Entry (Create|Edit) form opens.
2. Configure the required parameters.
3. Click Select to assign a Log ID to the CPM filter entry.
See the *5620 SAM User Guide* for information on configuring a Filter Log policy that employs this Log ID.
4. Click on the Filter Properties tab and configure the required parameters.
If you set the Frame Type parameter to e802dot2LLC, configure the parameters in the Match Criteria - DSAP SSAP panel.
If you set the Frame Type parameter to e802dot2SNAP, configure the parameters in the Match Criteria - SNAP panel.
If you set the Frame Type parameter to Ethernet II, configure the Ether Type parameter.
5. Save your changes and close the form.

9

Repeat [Step 8](#) to configure an additional MAC entry, if required.

10

To configure a queue entry, perform the following steps.

1. Click on the Queues tab.
2. Click Create or choose an entry and click Properties. The CPM Filter Queue Entry (Create|Edit) form opens.
3. Configure the required parameters.
4. Click on the CIR/PIR and Burst Size tab and configure the required parameters.
Ensure that the Committed Burst Size (KB) parameter value is lower than the Maximum Burst Size (KB) parameter value.
5. Save your changes and close the form.

11

Repeat [Step 10](#) to configure an additional queue entry, if required.

12

Click Apply to save the changes.

13

Distribute the filter to NEs, as required.

14

Close the open forms.

END OF STEPS

4.12 To configure an NE DoS protection policy



Note: To perform this procedure, you require an account with an assigned administrator scope of command role to the sitesec package, or a scope of command role with write access permission to the sitesec package.

4.12.1 Steps

1

Choose Administration→Security→NE DoS Protection from the 5620 SAM main menu. The NE DoS Protection form opens.

2

Click Create or choose a policy and click Properties. The NE DoS Protection (Create|Edit) form opens.

-
- 3 _____
Configure the required parameters.

 - 4 _____
Perform the following steps to configure CFM frame-rate limiting, if required.
 1. Click on the CFM Rate Limiting tab.
 2. Click Create. The CfmRateLimiting (Create) form opens.
 3. Configure the required parameters:
 4. Click Add in the Op Code Set panel. The Select Property form opens.
Note:
You must specify at least one Op Code value.
 5. Choose one or more Op Codes in the list and click OK.
 6. Save your changes and close the form.

 - 5 _____
Click Apply to save the changes.

 - 6 _____
Distribute the policy to NEs, as required.

 - 7 _____
Close the open forms.
- END OF STEPS _____

4.13 To view NE DoS protection violations

4.13.1 Steps

- 1 _____
Choose Administration→Security→NE System Security from the 5620 SAM main menu. The Select Site form opens.

- 2 _____
Choose a managed device in the list and click OK. The NE System Security (Edit) form opens.

- 3 _____
Click on the NE DoS Protection tab.

4

Perform one of the following to view a specific violation type.

- a. Click on the Per MAC Source Violations tab to view a list of the violations associated with subscriber hosts according to MAC address.
- b. Click on the Per IP Source Violations tab to view a list of the violations associated with subscriber hosts according to IP address.
- c. Click on the Link Specific Port Violations tab to view a list of the violations at the port level. The following kinds of violations are listed:
 - violations that exceed the Link Rate Limit (pps) parameter value specified for the NE
 - violations that exceed the Port Overall Rate Limit (pps) parameter value specified for the NE.
- d. Click on the Network Interface Violations tab to view a list of the violations for network interfaces that exceed the Overall Rate Limit (pps) parameter value specified in an associated NE DoS protection policy.
- e. Click on the SAP Violations tab to view a list of the violations for SAPs that exceed the Overall Rate Limit (pps) parameter value specified in an associated NE DoS protection policy.

5

Repeat [Step 4](#) as required to view another violation type.

6

Close the NE System Security (Edit) form.

END OF STEPS

4.14 To configure an NE DDoS protection policy

4.14.1 Steps

1

Choose Administration→Security→NE DDoS Protection from the 5620 SAM main menu. The NE DDoS Protection form opens.

2

Click Create or choose a policy and click Properties. The DDoS Protection Policy (Create|Edit) form opens.

3

Configure the required parameters.

4

To configure a static policer, perform the following steps.

1. Click on the Static Policers tab.
2. Click Create or choose an entry and click Properties. The Static Policer (Create|Edit) form opens.
3. Configure the required parameters.
4. If the Rate Type parameter is set to Kbps, configure the Rate Limit (Kb/s) and Buffer Space (Bytes) parameters in the Kbps panel. You can specify a default value for these parameters by selecting the Default check box.
5. If the Rate Type parameter is set to Packets, configure the Rate Limit (packets), Time Limit (seconds), and Initial Delay (packets) parameters in the Packets panel. You can specify a default value for the Rate Limit (packets) parameter by selecting the Default check box.
6. Configure the Exceed Action parameter. If you set this parameter to Discard or Low Priority, configure the Hold Down Duration (seconds) parameter.
7. Click OK. The Static Policer form closes.

5

Repeat [Step 4](#) to configure an additional static policer, if required.

6

To configure a local monitoring policer, perform the following steps.

1. Click on the Local Monitoring Policer tab.
2. Click Create or choose an entry and click Properties. The Local Monitoring Policer (Create|Edit) form opens.
3. Configure the required parameters.
4. If the Rate Type parameter is set to Kbps, configure the Rate Limit (Kb/s) and Buffer Space (Bytes) parameters in the Kbps panel. You can specify a default value for these parameters by selecting the Default check box.
5. If the Rate Type parameter is set to Packets, configure the Rate Limit (packets), Time Limit (seconds), and Initial Delay (packets) parameters in the Packets panel. You can specify a default value for the Rate Limit (packets) parameter by selecting the Default check box.
6. Configure the Exceed Action parameter.
7. Click OK. The Local Monitoring Policer form closes.

7

Repeat [Step 6](#) to configure an additional local monitoring policer, if required.

8

To configure protocol mappings for static policers and local monitoring policers, perform the following steps.

1. Click on the Protocols tab.
2. Click Create or select an entry and click Properties. The Protocols (Create|Edit) form opens.
3. Configure the required parameters.
4. Select a policer in the Enforcement panel.

Note:

If the Type parameter is set to Static, you must choose a static policer. If the Type parameter is set to Dynamic, you must choose a local monitoring policer. However, if the Type parameter is set to Dynamic and the Local Monitoring Bypass parameter is enabled, you cannot specify a local monitoring policer.

5. If the Rate Type parameter is set to Kbps, configure the Rate Limit (Kb/s) and Buffer Space (Bytes) parameters in the Kbps panel. You can specify a default value for these parameters by selecting the Default check box.
6. If the Rate Type parameter is set to Packets, configure the Rate Limit (packets), Interval (seconds), and Initial Delay (packets) parameters in the Packets panel. You can specify a default value for the Rate Limit (packets) parameter by selecting the Default check box.
7. Configure the Exceed Action parameter. If you set this parameter to Discard or Low Priority, configure the Hold Down Duration (seconds) parameter.
8. Save your changes and close the form.

9

Repeat [Step 8](#) to configure an additional protocol, if required.

10

Click Apply to save the changes.

11

Distribute the policy to NEs, as required.

-
- 12 _____
Close the open forms.

END OF STEPS _____

4.15 To configure a site user profile



Note: To perform this procedure, you require an account with an assigned administrator scope of command role to the sitesec package, or a scope of command role with write access permission to the sitesec package.

4.15.1 Steps

- 1 _____
Choose Administration→Security→NE User Profiles from the 5620 SAM main menu. The NE User Profiles form opens.

- 2 _____
Click Create or choose a profile and click Properties. The Site User Profile (Create|Edit) form opens.

- 3 _____
Configure the required parameters.



Note: You require LI user privileges to configure the LI Profile parameter.

- 4 _____
Perform the following steps.
1. Click on the Entries tab.
 2. Click Create or choose an entry and click Properties. The Site User Profile Match Entry (Create|Edit) form opens.
 3. Configure the required parameters.
The Match String parameter value is a CLI command prefix that defines the scope of the user profile. For example, when you set the match string to “config” and specify the deny action, the user profile cannot use any CLI commands that begin with the word “config”.
 4. Save your changes and close the form.

- 5 _____
Repeat [Step 4](#) to configure an additional match entry, if required.

6 _____

Click Apply to save the changes.

7 _____

Distribute the profile to NEs, as required.

8 _____

Close the open forms.

END OF STEPS _____

4.16 To configure a user account on a managed device



Note: To perform this procedure, you require an account with an assigned administrator scope of command role to the sitesec package, or a scope of command role with write access permission to the sitesec package.

4.16.1 Steps

1 _____

Choose Administration→Security→NE User Configuration from the 5620 SAM main menu. The NE User Configuration form opens.

2 _____

Click Create or choose a user and click Properties. The NE User (Create|Edit) form opens.

3 _____

Configure the required parameters.



Note: The SNMP option of the Access parameter is not valid for NEs that are managed using SNMPv2.

4 _____

If the Console option of the Access parameter is selected, perform the following steps to specify one or more site user profiles for the user account.

1. Click on the Console Profiles tab.
2. Use the Select buttons to specify up to eight profiles

5

When an SNMPv3 user account and group exist on a managed device, you can configure the user authentication parameters. To configure the parameters, perform the following steps.

i **Note:** If MD5 or SHA authentication and DES privacy is used, ensure that the keys are on the device and associated with the SNMPv3 user group.

1. Click on the SNMPv3 tab.
2. Configure the required parameters.

6

To specify an RSA key for use by SFTP on a 7750 MG, perform the following steps.

i **Note:** Only the 7750 MG supports RSA key configuration.

1. Click on the RSA Key tab.
2. Click Create. The RSA Key (Create) form opens.
3. Configure the parameters.
4. Save your changes and close the form.

7

Click Apply to save the changes.

8

Distribute the account to NEs, as required.

9

Close the open forms.

END OF STEPS

4.17 To configure a password policy



Note: To perform this procedure, you require an account with an assigned administrator scope of command role to the sitesec package, or a scope of command role with write access permission to the sitesec package.

4.17.1 Steps

1

Choose Administration→Security→NE Password Policy from the 5620 SAM main menu. The NE Password Policy form opens.

- 2 _____
Click Create or choose an entry and click Properties. The Site Password Policy (Create|Edit) form opens.
- 3 _____
Configure the required parameters.
- 4 _____
Specify the types and order of password authentication to be used to verify the user account password using the Authentication Order 1 through 3 parameters. Set the order from the most preferred authentication method to the least preferred.
- 5 _____
Configure the password complexity rules using the parameters in the Complexity Rules panel.
- 6 _____
Click Apply to save the changes.
- 7 _____
Distribute the policy to NEs, as required.
- 8 _____
Close the open forms.

END OF STEPS _____


4.18 To configure an NE RADIUS authentication policy




Note: See the appropriate RADIUS documentation for information about configuring a RADIUS server.

4.18.1 Steps

- 1 _____
Choose Administration→Security→NE RADIUS Authentication from the 5620 SAM main menu. The NE RADIUS Authentication form opens.
- 2 _____
Click Create or choose an entry and click Properties. The Site RADIUS Policy (Create|Edit) form opens.

- 3 _____
Configure the required parameters.
 - 4 _____
Click on the Servers tab.
 - 5 _____
Perform the following steps to specify a RADIUS server.
 1. Click Create or choose an entry and click Properties. The Site RADIUS Server (Create | Edit) form opens.
 2. Configure the required parameters.
 3. Save your changes and close the form.
 - 6 _____
Repeat [Step 5](#) to specify an additional RADIUS server, if required.
 **Note:** You can specify up to five RADIUS servers.
 - 7 _____
Click Apply to save the changes.
 - 8 _____
Distribute the policy to NEs, as required.
 - 9 _____
Close the open forms.
- END OF STEPS _____

4.19 To configure an NE TACACS+ authentication policy

 **Note:** See the appropriate TACACS+ documentation for more information about configuring TACACS+ servers.

4.19.1 Steps

- 1 _____
Choose Administration→Security→NE TACACS+ Authentication from the 5620 SAM main menu. The NE TACACS+ Authentication form opens.

2 _____

Click Create or choose an entry and click Properties. The Site TACACS+ Policy (Create|Edit) form opens.

3 _____

Configure the required parameters.

The Use Privilege Map parameter is configurable when the Enable Authorization parameter is set to true.

4 _____

Click on the Privilege Level Map tab.

5 _____

Click Create. The Privilege Level Map (Create) form opens.

6 _____

Configure the Privilege Level parameter.

7 _____

Choose a user profile.

8 _____

Click on the Servers tab.

9 _____

Perform the following steps to specify a TACACS+ server.

1. Click Create or choose an entry and click Properties. The Site TACACS+ Server (Create | Edit) form opens.
2. Configure the required parameters.
3. Save your changes and close the form.

10 _____

Repeat [Step 9](#) to specify an additional TACACS+ server, if required.



Note: You can specify up to five TACACS+ servers.

11 _____

Click Apply to save the changes.

12 _____
Distribute the policy to NEs, as required.

13 _____
Close the open forms.

END OF STEPS _____

4.20 To configure an OmniSwitch RADIUS, TACACS+, or LDAP security authentication policy

4.20.1 Steps

1 _____
Choose Administration→Security→NE AOS Security Authentication from the 5620 SAM main menu. The NE AOS Security Authentication form opens.

2 _____
Click Create or choose an entry and click Properties. The Site AOS Security Policy (Create|Edit) form opens.

3 _____
Configure the required parameters.

4 _____
Click Apply to save the changes.

5 _____
Distribute the policy to NEs, as required.

-
- 6 _____
Close the open forms.


END OF STEPS _____

4.21 To configure device system security settings


4.21.1 Steps

- 1 _____
Choose Administration→Security→NE System Security from the 5620 SAM main menu. The Select Site form opens.

- 2 _____
Select a managed device and click OK. The NE System Security (Edit) form opens.

 **Note:** Items that appear on the NE System Security (Edit) form are device-dependent. Not all configuration form tabs and parameters in this procedure apply to all devices.

- 3 _____
To configure the FTP, Telnet, or SSH server parameters, click on the Servers Configuration tab.

 **Note:** The 7705 SAR may become temporarily unreachable when enabling SSH and starting the SSH server on the device.

- 4 _____
To configure allowed SSH ciphers, perform the following.
1. Click on the Servers Configuration tab, then on the SSH Cipher List tab.
 2. Click Create in the Client tab. The SSH Client Cipher List (Create) form opens.
 3. Configure the required parameters.
 4. Save and close the form.
 5. Click on the Server tab and click Create. The SSH Server Cipher List (Create) form opens.
 6. Configure the required parameters.
 7. Save and close the form.

- 5 _____
To configure the CPM hardware queueing for BGP or T-LDP peers, click on the CPM Per-Peer-Queueing tab.

6 _____
To configure user profiles, click on the System User Template tab. Otherwise, go to [Step 19](#) .

The default System User radius_default and tacplus_default templates are listed.

7 _____
Select the appropriate default template and click Properties. The System User Template (Edit) form opens.

8 _____
Configure the required parameters.

9 _____
If you intend to use the default Template Profile, go to [Step 19](#) .

10 _____
Click Select in the Template Profile panel to choose a template profile.

11 _____
If you choose the administrative template, go to [Step 19](#) .

12 _____
Click Create. The Site User Profile (Create) form opens.

13 _____
Configure the required parameters.

14 _____
Click on the Entries tab.

15 _____
Perform the following steps.

1. Click Create. The Site User Profile Match Entry (Create) form opens.
2. Configure the required parameters.
The Match String parameter value is a CLI command prefix that defines the scope of the user profile. For example, when you set the match string to “config” and specify the deny action, the user profile cannot use any CLI commands that begin with the word “config”.

16 _____

Repeat [Step 15](#) to specify an additional match entry, if required.

17 _____

Save your changes and close the form.

18 _____

Close the System User Template (Edit) form.

19 _____

To configure global DoS protection, click on the NE DoS Protection tab.

20 _____

Configure the required parameters.



Note: PIM in an MVPN on the egress DR does not switch traffic from the (*,G) to the (S,G) tree if protocol protection is enabled, and if PIM is not enabled on the ingress network interface. Enable the Block PIM Tunneled parameter to enable extraction and processing of PIM packets that arrive from a tunnel, for example, an MPLS or GRE tunnel, on a network interface.

21 _____

Click on the following child tabs, as required, to view the DoS violations.

- Per MAC Source Violations
- Per IP Source Violations
- Link Specific Port Violations
- Network Interface Violations
- SAP Violations
- SDP Violations

22 _____

Click on the VPRN Network Exceptions tab to configure rate limits for VPRN network exceptions.

23 _____

Configure the required parameters.

24 _____

Save your changes and close the NE System Security (Edit) form.

25

Close the NE System Security form.

END OF STEPS

4.22 To configure and manage PKI site security on an NE

4.22.1 Purpose

Perform this procedure to create the required DSA or RSA keypair and CA request on an NE to enable PKI security between peers, and to manage keys, certificates, and CRLs.

PKI encryption is required for functions such as IPsec, which use X.509 certificate-based authentication. The following devices support PKI encryption:

- 7450 ESS
- 7750 MG
- 7750 SR

4.22.2 Steps

1

Choose Administration→Security→NE PKI Authentication→Site Public Key Infrastructure from the 5620 SAM main menu. The Select Site form opens.

2

Choose a managed NE and click OK. The Site Security Public Key Infrastructure (Edit) form opens.

3

Configure the required parameters.

4

Click Apply to save the changes.

5

Perform the following steps to generate a PKI keypair that is stored in a file on an NE compact flash drive.

1. Choose Admin Certificate→Generate Keypair from the More Actions button menu. The Admin Certificate Generate Keypair form opens.
2. Configure the required parameters.
3. Click Execute. The keypair is generated and stored.
4. Close the form.

6

Perform the following steps to generate local PKCS#10 certificate request on a local compact flash drive.

1. Choose Admin Certificate→Generate Local Certificate Request from the More Actions button menu. The Admin Certificate Generate Local Certificate Request form opens.
2. Configure the required parameters.
3. Click Execute. The local request is generated.
4. Close the form.

7

If you want the certificate signed by a CA, FTP the request file to the CA and use the CA-signed certificate in the following steps.

8

Perform the following steps to convert the certificate file to the required format for the NE.

1. Choose Admin Certificate→Import File from the More Actions button menu. The Admin Certificate Import File form opens.
2. Configure the required parameters.
3. Click Execute. The file is imported.
4. Close the form.

9

To convert a certificate, keypair, or CRL file on the NE to another format, perform the following steps.

1. Choose Admin Certificate→Export File from the More Actions button menu. The Admin Certificate Export File form opens.
2. Configure the required parameters.
3. Click Execute. The file is exported.
4. Close the form.

10

To display the content of a certificate, keypair, or CRL file in plain text, perform the following steps.

1. Choose Admin Certificate→Display File from the More Actions button menu. The Admin Certificate Display File form opens.
2. Configure the required parameters.

Note:

If you are displaying key file content, only the Key Size and Key Type are displayed.

You must configure the Password parameter if the file uses PKCS#12 encryption.

3. Click Execute. The file content is displayed.
4. Close the form.

11

To reload a certificate or keypair file from a local compact flash drive, perform the following steps.

1. Choose Admin Certificate→Reload File from the More Actions button menu. The Admin Certificate Reload File form opens.
2. Configure the required parameters.
3. Click Execute. The file content is reloaded.
4. Close the form.

12

To clear the OCSP cache, perform the following steps.

1. Choose Admin Certificate→Clear OCSP Cache from the More Actions button menu. The Admin Certificate Clear OCSP Cache form opens.
2. Configure the required parameters.
3. Click Execute. The file content is reloaded.
4. Close the form.

13

To import a Secure ND RSA keypair, perform the following.

1. Choose Admin Certificate→Secure ND Import from the More Actions button menu. The Admin Certificate Secure ND Import form opens.
2. Configure the required parameters.
3. Click Execute. The keypair is imported.
4. Close the form.

14

To export the Secure ND RSA keypair, perform the following.

1. Choose Admin Certificate→Secure ND Export from the More Actions button menu. The Admin Certificate Secure ND Export form opens.
2. Click Execute. The keypair is exported.
3. Close the form.

15 _____
To perform CMP2 actions, see [4.25 “To perform CMPv2 actions” \(p. 125\)](#) .

16 _____
Close the Site Security Public Key Infrastructure (Edit) form.

END OF STEPS _____

4.23 To configure a PKI certificate authority profile

4.23.1 Steps


1 _____
Choose Administration→Security→NE PKI Authentication→PKI Certificate Authority Profiles from the 5620 SAM main menu. The PKI Certificate Authority Profiles form opens.

2 _____
Click Create. The Certificate Authority Profile (Create) form opens.

3 _____
Configure the required parameters.

4 _____
Click on the CMPv2 tab and configure the required parameters.

5 _____
To create a CMP key, perform the following steps.

 **Note:** A key that is created locally on an NE, for example, using a CLI, is not sent to the 5620 SAM, and is displayed on the Certificate Authority Profile form as N/A. Any N/A keys on an NE must be deleted before the profile can be distributed to the NE.

1. Click Create. The CMP Key List (Create) form opens.
2. Configure the parameters.
3. Save your changes and close the form.

6 _____
To configure automatic CRL file download, perform the following.

1. Click on the Auto CRL Update tab and click Create. The Auto CRL Update form opens.

2. Configure the required parameters.
3. To specify a URL for the CRL file, click on the Create button in the URL entries panel and configure the parameters in the CRL URL Entry form. See [4.24 “To create a file transmission profile” \(p. 123\)](#) for information about creating a file transmission profile to use with the CRL URL entry.
4. Save your changes and close the form.

7

Click Apply to save your changes.

8

Distribute the policy to NEs, as required.

9

Close the open forms.

END OF STEPS

4.24 To create a file transmission profile

4.24.1 Purpose

Follow this procedure to create a file transmission profile for use with a CRL URL entry when configuring a PKI certificate authority profile to use automatic CRL file download.

4.24.2 Steps

1

Choose Policies→ISA Policies→File Transmission Profile from the 5620 SAM main menu. The File Transmission Profile form opens.

2

Configure the required parameters.

3

Save your changes and close the form.

END OF STEPS

4.25 To perform CMPv2 actions

4.25.1 Purpose

CMP is a protocol that runs between a CA (Certificate Authority) and an end entity to provide certificate management functions, using HTTP as transport protocol to communicate to the CA.

4.25.2 Steps

1

Choose Administration→Security→NE PKI Authentication→Site Public Key Infrastructure from the 5620 SAM main menu. The Select Site form opens.

2

Choose an NE in the list and click OK. The Site Security Public Key Infrastructure (Edit) form opens.

3

Click Admin Certificate and choose Perform CMPv2 Actions. The Admin Certificate form opens.

4

Perform one of the following to configure the CA Profile Name parameter.

- a. Select a CA profile.
- b. Enter the profile name.

CMPv2 actions

5

Select a CMPv2 action from the drop-down menu beside the Type parameter in the Action panel. The following table lists the available CMPv2 actions. You can view the status of the last CMPv2 action performed on this site in the Last Action Status panel.

Table 7 CMPv2 actions

Action	See step
4.25.2 "Initial Registration" (p. 126)	Step 6
4.25.2 "Certificate Request" (p. 126)	Step 10
4.25.2 "Key Update" (p. 127)	Step 14
4.25.2 "Poll" (p. 127)	Step 18
4.25.2 "Clear Request" (p. 127)	Step 20
4.25.2 "Abort Request" (p. 128)	Step 22
4.25.2 "Manually Update CRL files" (p. 128)	Step 24

Initial Registration

6 _____

Configure the required parameters in the Action panel.

7 _____

Perform one of the following:

- a. To perform an initial registration using a password, configure the required parameters in the Protection Algorithm - using Password panel.
- b. To perform an initial registration using a certificate, configure the required parameters in the Protection Algorithm - using Certificate panel.

8 _____

Click Apply to perform the action.

9 _____

Go to [Step 26](#) .

Certificate Request

10 _____

Configure the required parameters in the Action panel.

11 _____

Configure the required parameters in the Protection Algorithm - using Certificate panel.

12 _____

Click Apply to perform the action.

13 _____

Go to [Step 26](#) .

Key Update

14 _____

Configure the required parameters in the Action panel.

15 _____

Configure the required parameters in the Protection Algorithm - using Certificate panel.

16 _____

Click Apply to perform the action.

17 _____

Go to [Step 26](#) .

Poll

18 _____

Click Apply to send the poll request.

19 _____

Go to [Step 26](#) .

Clear Request

20 _____

Click Apply to send the clear request.

21 _____

Go to [Step 26](#) .

Abort Request

22 _____
Click Apply to send the abort request.

23 _____
Go to [Step 26](#) .

Manually Update CRL files

24 _____
Configure the Certificate Authority Profile parameter.

25 _____
Click on the Execute button to send the update request.

26 _____
Close the open forms.

END OF STEPS _____

4.26 To distribute a license key to all 7705 SAR-H nodes

4.26.1 Steps

1 _____
Choose Administration→Security→NE Firewall→Default NE Firewall from the 5620 SAM main menu. The Firewall - Default (Edit) form opens.

2 _____
Choose one or more system IDs from the list and click Distribute Key.

3 _____
The Distribute License Key dialog box opens.

4 _____
Enter the license key to be distributed.

5



CAUTION

Service Disruption

You must click OK to complete license distribution.

Changes are applied immediately when you click OK.

Click OK to distribute the license key to all nodes.

6

The Firewall - Default (Edit) form opens.

7

Click OK to close the form.

END OF STEPS

4.27 To configure a 7705 SAR-H NE firewall



Note: The NE firewall function is supported only on a Release 5.0 or later 7705 SAR-H.

4.27.1 Steps

1

Choose Administration→Security→NE Firewall→Default NE Firewall from the 5620 SAM main menu. The Firewall - Default (Edit) form opens.

2

Select a site and click Properties. The Firewall Site (Edit) form opens.

3

Configure the required parameters.

4

In the Firewall Site on the navigation tree, choose one of the following to create a new policy on the site:

- a. Right-click on Zones and choose Create Zone.
- b. Right-click on Rule Sets and choose Create Rule Set.
- c. Right-click on Service Groups and choose Create Service Group.

d. Right-click on Host Groups and choose Create Host Group.

5

In the Firewall Site on the navigation tree, choose one of the following to add a firewall policy on the site:

- a. To add a zone, right-click on Zones and choose Add.
- b. To add a rule set, right-click on Rule Sets and choose Add.
- c. To add a service group, right-click on Service Groups and choose Add.
- d. To add a host group, right-click on Host Groups and choose Add.

6

The Select Global Policies - Firewall Site - Default, Site form opens.

7

Click Search to display a list of policies.

8

Choose a policy from the list and click OK to add the policy to the existing site.

9

To delete a firewall policy right-click on one of the following and choose Delete:

- a. Zone
- b. Rule Set
- c. Service Group
- d. Host Group



Note: Policies can be deleted in the following order:

- Zone
 - Rule Set
 - Host Group or Service Group
- Host Group or Service Group policies cannot be deleted if rule sets are associated with them.
- Rule set policies cannot be deleted if they are associated with zones.
- Zone policies cannot be deleted if they are associated with SAP, SDP, MGMT, or CPM interfaces.

10

Click OK to close the Firewall Site (Edit) form.

11 _____

The Firewall - Default (Edit) form opens.

12 _____

The Network Interfaces, SAPs and SDPs tabs display the firewall instances associated with the zone.

13 _____

To add a firewall entry for the network interfaces, SAPs or SDPs:

1. Choose a Site Id from the list.
2. Click on Add Firewall Entry.
3. The Firewall Interface Entry, Firewall SAP Entry, or the Firewall SDP Entry (Create) form opens.
4. Configure the required parameters.
5. Click Select, the Select Zone form opens.
6. Choose a zone from the list and click OK.
7. Click OK in the Firewall Interface Entry, Firewall SAP Entry, or the Firewall SDP Entry (Create) form.
8. The Firewall - Default (Edit) form opens.

14 _____

To view the Firewall Properties from the Network Interfaces, SAPs and SDPs tabs, choose a Site Id and click Properties.

15 _____

Click OK to close the Firewall - Default (Edit) form.

END OF STEPS _____

4.28 To configure an NE management access firewall on a 7705 SAR-H



CAUTION

Service Disruption

If the zone entry using the Management Access Firewall on the 7705 SAR-H is not properly configured, the essential communication channel between 5620 SAM and the NE could be terminated.

It is advisable to check before turning up the Management Access Firewall that protocols such as UDP, ICMP, SSH, TFTP, FTP, TELNET, SCP, and NTP are not blocked.



Note: The NE management access firewall function is supported only on a Release 5.0 or later 7705 SAR-H.

You cannot attach a zone containing a ruleset that has a firewall log with destination as syslog to the management access firewall.

4.28.1 Steps

- 1 _____
Choose Administration→Security→NE Firewall→NE Management Access Firewall from the 5620 SAM main menu. The NE Management Access Firewall form opens.
- 2 _____
Perform one of the following:
 - a. To create a firewall, click Create. The Management Access Firewall (Create) form opens.
 - b. To modify a firewall, click Search to display a list of firewall entries. Choose an entry from the filtered list and click Properties. The Management Access Firewall (Edit) form opens.
- 3 _____
Configure the required parameters.
- 4 _____
Create one or more firewall entries.
 1. Click on the Firewall Entries tab.
 2. Click Create. The Firewall Entry (Create) form opens.
 3. Configure the required parameters.
 4. Click Select and choose a zone.
 5. Select the IP Operator check box from the IP Address panel on the Firewall Entry (Create) form.
 6. Choose one of the following from the IP Operator drop-down menu and enter the range, if required:
 - EQUAL
 - RANGE
 7. Save and close the form.
- 5 _____
Save and close the form.

6 Select the newly created NE Management Access Firewall policy and click Properties.

7 The Management Access Firewall form opens. The Configuration Mode parameter in the Policy Configuration panel is in the Draft state. Release the policy and distribute the policy as required.

1. Click Switch Mode. A confirmation dialog box opens.
2. Click Yes to confirm the action. The Configuration Mode changes to Released, and the policy is distributed to the NEs.

END OF STEPS

4.29 To configure an NE CPM firewall on the 7705 SAR-H



Note: The NE CPM firewall function is supported only on a Release 5.0 or later 7705 SAR-H.

4.29.1 Steps

1 Choose Administration→Security→NE Firewall→NE CPM Firewall from the 5620 SAM main menu. The NE CPM Firewall form opens.

2 Perform one of the following:

- a. To create a firewall, click Create. The NE CPM Firewall (Create) form opens.
- b. To modify a firewall, click on search to display a list of firewall entries. Choose an entry from the filtered list and click Properties. The NE CPM Firewall (Edit) form opens.

3 Configure the required parameters.

4 Create one or more firewall entries.

1. Click on the Firewall Entries tab.
2. Click Create. The Firewall Entry (Create) form opens.
3. Configure the required parameters.
4. Click Select, the Select Zone form opens.

5. Choose a zone from the list and click OK.
6. Select the IP Operator check box from the IP Address panel on the Firewall Entry (Create) form.
7. Choose one of the following from the IP Operator drop-down menu and enter the range, if required:
 - EQUAL
 - RANGE
8. Save and close the form.

5 _____
Save and close the form.

6 _____
Choose the newly created NE CPM Firewall policy and click Properties.

7 _____
The NE CPM Firewall form opens. The Configuration Mode parameter in the Policy Configuration panel is in the Draft state. Release the policy and distribute the policy as required.

1. Click Switch Mode. A confirmation dialog box opens.
2. Click Yes to confirm the action. The Configuration Mode changes to Released, and the policy is distributed to the NEs.

END OF STEPS _____

4.30 To delete a security policy



Note: When you delete site management access filter policies in which the Action parameter is set to deny, ensure that you modify the policy to set the parameter to permit before it is deleted, otherwise, the 5620 SAM may be isolated.

You cannot remove a site management access filter if the filter administrative state is up and the default action of the filter is set to deny or deny host unreachable.

If you attempt to delete an OmniSwitch RADIUS or TACACS+ security policy that is applied to an authentication service, the 5620 SAM generates a deployment error. You must use the OmniSwitch CLI to delete the policy from the authentication service before you can delete the policy from the 5620 SAM.

4.30.1 Steps

- 1 _____
- Choose the appropriate policy from one of the following.
- a. The Administration→Security→*option* 5620 SAM main menu

b. The Policies→AAA Policies→*option* 5620 SAM main menu

The appropriate form opens.

2 _____

Set the filter criteria, if applicable.

3 _____

Click Search. A policy list opens.

4 _____

Choose a policy from the list.

5 _____

Click Delete.

6 _____

Click Yes. The policy is deleted.

END OF STEPS _____

4.31 To manually unlock a user account

4.31.1 Steps

1 _____

From the 5620 SAM main menu, choose Administration→Security→NE User Configuration. The NE User Configuration form opens.

2 _____

Click Search. A list of user accounts appears.

3 _____

Perform one of the following:

a. To unlock a 5620 SAM user, choose a user and click Unlock User. The user account is unlocked.

b. To unlock the local definition of a user on an NE, perform the following:

1. Choose a user account and click Properties. The NE User form opens.

2. Click on the Local Definitions tab.

3. Click Search. A list of NEs with local definitions for the user appears.

-
4. Choose an NE and click Unlock User. The user account on the selected NE is unlocked.
 5. Close the NE User form.

4 _____
Close the NE User Configuration form.

END OF STEPS _____

4.32 To clear the password history of a user on a managed device

4.32.1 Steps

- 1 _____
Choose Administration→Security→NE User Configuration from the 5620 SAM main menu. The NE User Configuration form opens.
- 2 _____
Configure the filters and click Search. A list of configured users appears.
- 3 _____
Select a user and click Properties. The NE User (Edit) form opens.
- 4 _____
Click on the Local Definitions tab. A list of sites with local definitions for the selected user appears.
- 5 _____
Select one or more sites and click Clear Password History. A dialog box appears.
- 6 _____
Click Yes to confirm the operation. The password history for the selected user at the specified sites is cleared.

7

Click OK. The NE User (Edit) form closes.

END OF STEPS

4.33 To clear collected statistics on a CPM filter

4.33.1 Steps

1

From the 5620 SAM main menu, choose Administration→Security→NE CPM Filter. The CPM Filter form appears.

2

Click Search. A list of CPM filters appears.

3

Choose a CPM filter and click Properties. The CPM Filter (Edit) form appears.

4

Click on the Local Definitions tab.

5

Configure the filters and click Search. A list of CPM filter local definitions appears.

6

Choose a local definition and click Properties. The CPM Filter Local Policy form appears.

7

Click on the IPv4 Entries, IPv6 Entries, MAC Entries or Queues tab, depending on the type of statistic you need to clear.

8

Configure the filters and click Search. A list of filter entries appears.

9

Perform one of the following:

- a. To clear specific entries, choose the entries you need to clear and click Clear Statistics on Entry.

-
- b. To clear all entries, choose an entry and click Clear Statistics on All Entries. This button is not available in the Queues tab.

10

To view the status of all clear requests, perform the following:

1. Click on the Clear Statistics Status tab.
2. Configure the filters, and click Search. A list of clear requests appears.
3. Choose a clear request and click Properties. The status of the clear request appears.

11

Close the CPM Filter Local Policy, CPM Filter (Edit) and CPM Filter forms.

END OF STEPS

4.34 To manage OCSP cache entries on an NE

4.34.1 Steps

1

Choose Administration→Security→NE PKI Authentication→Site Public Key Infrastructure from the 5620 SAM main menu. The Select Site form opens.

2

Choose a managed device in the list and click OK. The Site Security Public Key Infrastructure (Edit) form opens.

3

Click on the OCSP Cache Entries tab.

4

Click Search. A list of OCSP cache entries for the site opens.

5

To clear cache entries, perform the following.

1. Click Admin Certificate and choose Clear OCSP Cache. The Admin Certificate Clear OCSP Cache form opens.
2. Enter the Entry ID number of the cache entry you need to clear in the Entry ID parameter. To clear all entries, leave the parameter blank.
3. Click Execute. The results of the clear operation appear in the results panel.
4. Click Close. The Admin Certificate Clear OCSP Cache form closes.

6

Click OK or Cancel. The Site Security Public Key Infrastructure (Edit) form closes.

END OF STEPS

5 TCP enhanced authentication

5.1 Overview

5.1.1 Purpose

This chapter describes TCP enhanced authentication keys

5.1.2 Contents

5.2	TCP enhanced authentication	141
5.3	Workflow to configure TCP enhanced authentication for NEs	143
5.4	To configure a global TCP key chain	144
5.5	To distribute global key chains to NEs	145
5.6	To verify the distribution of a global key chain to NEs	147
5.7	To identify differences between a global and local key chain policy or two local key chains	147

5.2 TCP enhanced authentication

5.2.1 Overview



CAUTION

Service Disruption

It is recommended that you use only the 5620 SAM to create keys and key chains. Do not create a key or key chain directly on a managed NE using another interface, for example, a CLI. The 5620 SAM cannot obtain a TCP key secret value from an NE during resynchronization, so it cannot specify the key for use on another NE.

If a local NE key chain and the associated global 5620 SAM key chain differ after a resynchronization, the 5620 SAM generates an alarm.

This chapter describes the 5620 SAM support of TCP enhanced authentication for NEs based on the MD5 encryption mechanism described in RFC2385. 5620 SAM TCP enhanced authentication allows the use of powerful algorithms for authenticating routing messages.

The 5620 SAM uses a TCP extension to enhance BGP and LDP security. TCP enhanced authentication is used for applications that require secure administrative access at both ends of a TCP connection. TCP peers update authentication keys during the lifetime of a connection.

A 5620 SAM operator with administrative privileges can create, delete, modify, and distribute TCP enhanced authentication components, and can perform an audit of a local key chain to compare it with the associated global key chain or other local key chains. The 5620 SAM TCP enhanced authentication components are called keys and key chains.

Global key chains are created in Draft mode. This allows operators to verify that the key chain is correctly configured before they distribute it to the network elements. When the key chain is approved for distribution, you can change the global key chain to Released mode, which also distributes the key chain to existing local definitions. The 5620 SAM saves the latest released version of the global key chain.

5.2.2 TCP keys and key chains

A key is a data structure that is used to authenticate TCP segments. One or more keys can be associated with a TCP connection. Each key contains an identifier, a shared secret, an algorithm identifier, and information that specifies when the key is valid for authenticating the inbound and outbound segments.

A key chain is a list of up to 64 keys that is associated with a TCP connection. Each key within a key chain contains an identifier that is unique within the key chain. You can use the 5620 SAM to distribute a global key chain to multiple NEs and assign a key to multiple BGP or LDP instances.

The 5620 SAM treats global and local key chain management as it does policy management; depending on the distribution mode configuration of a local key chain, when you modify a global key chain using the 5620 SAM, all local instances can be updated to ensure that all instances of the key chain in the network are synchronized. See “Policies overview” in the *5620 SAM User Guide* for information about global and local policy instances, policy distribution and distribution modes, and local policy audits.

When the 5620 SAM attempts to synchronize the keys in a global key chain with the keys on an NE, the NE does not return the secret key value. After a key chain is deployed to an NE, the shared secret and the encryption algorithm cannot be modified. You can delete a key chain or key only when it is not in use by a protocol.

You can specify whether an NE uses a TCP key for sending packets, receiving packets, or both. Using keys that are configured for both, or send-receive, is general good practice because communication between NEs cannot be affected by assigning the wrong key type.

There are two classes of TCP keys:

- Active
- Eligible

Active keys

A key set contains one active key. An active key is a key that TCP uses to generate authentication information for outbound segments. You cannot delete the active key in a keychain.

Eligible keys

Each set of keys, called a key chain, contains zero or more eligible keys. An eligible key is a key that TCP uses to authenticate inbound segments.

5.3 Workflow to configure TCP enhanced authentication for NEs

5.3.1 Process

- 1 _____
Create a global key chain that contains at least one key; see [5.4 “To configure a global TCP key chain” \(p. 144\)](#) .
- 2 _____
Distribute the key chain to the NEs; see [5.5 “To distribute global key chains to NEs” \(p. 145\)](#) .
- 3 _____
Verify the distribution of a global key chain to the NEs; see [5.6 “To verify the distribution of a global key chain to NEs” \(p. 147\)](#) .
- 4 _____
Assign the key chain to a routing protocol, such as BGP or LDP.
- 5 _____
If required, identify the differences between a global and local policy or two local key chains; see [5.7 “To identify differences between a global and local key chain policy or two local key chains” \(p. 147\)](#) .

5.4 To configure a global TCP key chain

5.4.1 Steps

- 1 _____
Choose Administration→Security→TCP KeyChains from the 5620 SAM main menu. The TCP KeyChains form opens.
- 2 _____
Click Create or choose a key chain and click Properties. The KeyChain Create|Edit form opens.
- 3 _____
Configure the required parameters.
- 4 _____
Click on the KeyChain Key tab.
- 5 _____
Click Create or choose a key chain key and click Properties. The KeyChain Key Create|Edit form opens.
- 6 _____



CAUTION

Service Disruption

You must ensure bidirectional communication between NEs.

It is recommended that you choose the Send-receive option for the Key Direction parameter.

Configure the required parameters.

The End Time parameter is configurable only if the Key Direction parameter is set to Receive.



Note: The 5620 SAM generates a random default value for the Key parameter. For greater security, it is recommended that you accept this value rather than manually enter a value. You cannot subsequently delete a TCP key chain or TCP key when the Admin State parameter for the key chain or key is set to In Service.

7

Save and close the forms.

END OF STEPS

5.5 To distribute global key chains to NEs

5.5.1 Purpose

Perform the following procedure to distribute one or more global TCP key chains to one or more NEs. When you distribute a global key chain, a local key chain using the Sync With Global distribution mode allows the NE to receive the key chain.



CAUTION

Service Disruption

Releasing, distributing, or deleting a TCP keychain or TCP key can be service-affecting. Ensure that you understand the implications of these operations before you proceed.

5.5.2 Steps

1

Choose Administration→Security→TCP KeyChains from the 5620 SAM main menu. The TCP KeyChains form opens.

2

Verify that none of the key chains in the list that you want to distribute are in Draft configuration mode and go to [Step 4](#) . Otherwise go to [Step 3](#) .

3



WARNING

Equipment Damage

Verify the local definitions before releasing a global key chain.

When you release a global key chain, the key chain is distributed to existing local definitions.

When a key chain is in Draft configuration mode, the Distribute button is disabled and the key chain cannot be distributed to an NE. You must first release the key chain for distribution.

To release a key chain:

1. Select the key chain entry and click Properties. The Key Chain (Edit) form opens.
2. Click Switch Mode to acknowledge the Configuration Mode change. The Release form opens.
3. Select the required NEs for release by moving the appropriate row entries from the Available Objects panel to the Selected Objects panel.
Refer to the Policies chapter in the *5620 SAM User Guide* for more information on policy distribution.
4. Click on the Distribute button to release the key chain locally to devices.
5. Click Close. The Release form closes and the configuration mode of the key chain is changed to Released.
6. Close the Key Chain (Edit) form.

4

To distribute a key chain:

i **Note:** Local definitions of key chains that use the Local Edit Only distribution mode do not allow their NEs to receive the distribution of a global key chain. You must set the distribution mode of a local key chain to Sync With Global if you need the associated NE to receive the distribution of a global key chain.

1. Select one or more key chains and click Distribute. The Distribute - KeyChain form opens.
2. Select the required NEs by moving the appropriate row entries from the Available Objects panel to the Selected Objects panel.
3. Click Distribute. The 5620 SAM distributes the key chains to the NEs.
4. Close the Distribute - KeyChain form. The TCP KeyChains form reappears.

5

To configure the distribution mode of a local definition:

1. Click Switch Distribution Mode. The Switch Distribution Mode form opens.
2. Choose Sync With Global, Local Edit Only, or All from the drop-down menu. Only the sites that are configured with the selected distribution mode are listed.
3. Choose one or more entries in the Available Local Policies panel and click on the right arrow. The chosen entries move to the Selected Local Policies panel.
4. Depending on the current distribution mode of the chosen entries, perform one of the following:
 - Click Sync With Global.
 - Click Local Edit Only.The distribution mode of the selected entries changes accordingly.
5. Close the Distribution Mode form.

-
- 6 _____
Close the TCP KeyChains form.

END OF STEPS _____

5.6 To verify the distribution of a global key chain to NEs

5.6.1 Steps

- 1 _____
Choose Administration→Security→TCP KeyChains from the 5620 SAM main menu. The TCP KeyChains form opens.
- 2 _____
Select a key chain and click Properties. The KeyChain (Edit) form opens.
- 3 _____
Click on the Local Definitions tab. The NEs that have a local instance of the key chain are displayed in a list.
- 4 _____
View the list of NEs to confirm that the key chain is distributed to the required NEs.
- 5 _____
Close the forms.

END OF STEPS _____

5.7 To identify differences between a global and local key chain policy or two local key chains


5.7.1 Steps

- 1 _____
Choose Administration→Security→TCP KeyChains from the 5620 SAM main menu. The TCP KeyChains form opens.
- 2 _____
Choose Local from the Policy scope menu to select a local NE. The Select a Network Element form opens.

3 _____
Select an NE and click OK. The NE IP address is displayed in the Local Node IP Address field.

4 _____
Choose the local key chain that you need to compare with another key chain and click Properties. The KeyChain (Edit) form opens.

5 _____
Click Local Audit On. The Local Audit form opens.

 **Note:** You can cancel the local audit at any time by clicking Local Audit Off on the KeyChain (Edit) form.
The 5620 SAM does not identify differences between the Begin Time and End Time properties of key chains.

6 _____
Perform one of the following from the Policy scope menu:

- a. Choose Global and go to [Step 7](#) .
- b. Choose Local to choose an NE. The Select a Network Element form opens.
 1. Select an NE and click OK. The NE IP address is displayed in the Local Node IP Address field.
 2. Go to [Step 7](#) .

7 _____
Click OK. The Local Audit form closes and the appropriate global|local policy opens for comparison.

8 _____
View the differences between the key chains by clicking on the tabs that are highlighted with an arrow icon to indicate that differences exist on the forms. An arrow icon beside a property indicates that the property is modified. In lists, new entries are highlighted in pink and modified entries are highlighted in purple.

9 _____
Close the forms.

END OF STEPS _____

Part III: 5620 SAM advanced configuration

Overview

Purpose

This part provides information about 5620 SAM components, database, and system redundancy.

Contents

Chapter 6, 5620 SAM component configuration	151
Chapter 7, 5620 SAM database management	205
Chapter 8, 5620 SAM system redundancy	233

6 5620 SAM component configuration

6.1 Overview

6.1.1 Purpose

This chapter describes configuration and management procedures for 5620 SAM components.

6.1.2 Contents

5620 SAM component configuration	153
6.2 Overview	153
6.3 Changing 5620 SAM default text fields and ID ranges	153
6.4 5620 SAM license management	159
6.5 Workflow to configure 5620 SAM components	160
Software and license configuration procedures	163
6.6 To view the 5620 SAM license information	163
6.7 To export the 5620 SAM license information to a file	164
6.8 To update the 5620 SAM license in a standalone deployment	164
6.9 To update the 5620 SAM license in a redundant deployment	165
6.10 To list the backed-up 5620 SAM license files	168
6.11 To change the default 5620 SAM license expiry notification date	169
System components configuration procedures	171
6.12 To modify the base configuration of all GUI clients	171
6.13 To configure the display of multiple 5620 SAM systems as client GUI login options	172
6.14 To change the default user file locations on a client delegate server	174
6.15 To change the IP address or hostname of a 5620 SAM system component	175
6.16 To enable 5620 SAM database backup file synchronization	176
6.17 To modify the default time period of statistics displayed by the Statistics Manager search filters	178

6.18	To modify the default time period of statistics displayed on object properties forms	179
6.19	To create or configure a format policy	180
6.20	To create or configure a range policy	182
	Network management configuration procedures	185
6.21	To configure automatic device configuration backup file removal	185
6.22	To enable alarm reporting to identify duplicate NE system IP addresses	186
6.23	To enable dynamic system IP address updates for 7705 SAR nodes	188
6.24	To enable LSP on-demand resynchronization	189
6.25	To enable debug configuration file reloading on an NE for mirror services	191
6.26	To configure throttle rates for subscriber trap events	193
6.27	To configure the windowing trap delayer option for subscriber table resyncs	193
6.28	To create a default SNMPv2 OmniSwitch user on a 5620 SAM system	196
	System preferences configuration procedures	198
6.29	To configure 5620 SAM system preferences	198

5620 SAM component configuration

6.2 Overview

6.2.1 Post-installation

The 5620 SAM may require a configuration change after it is installed to meet your specific operational requirements. The procedures in this chapter change the default system-wide behavior of 5620 SAM settings or functional preferences. The procedures in this chapter describe how to perform configuration changes on the following 5620 SAM components:

- 5620 SAM software and licenses
- system components
- network management functions
- global 5620 SAM alarm settings
- system preferences



Note: You can use the 5620 SAM auto-client update function to reconfigure multiple GUI clients using one central configuration. See “Automated client installation, upgrade, and configuration” in the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for operational information about the function, and [6.12 “To modify the base configuration of all GUI clients” \(p. 171\)](#) for information about using the function to update multiple clients.

6.3 Changing 5620 SAM default text fields and ID ranges

6.3.1 Overview

You can create format and range policies to change the default number and format of characters used for text fields and the ID ranges used in the 5620 SAM GUI.

6.3.2 Format and range policies

Format policies manage how services, policies, LSPs, and L2 and L3 access interfaces are named and described. Range policies manage the ID numbers that are assigned to services, policies, LSPs, and L2 and L3 access interfaces. For example, you can configure a range policy to specify a range of 200 and 499 for all IDs for a service. You can configure a format policy to specify that service names do not exceed 10 characters. The object creation form indicates when a range or format policy is in effect for an object.

Format and range policies are not distributed to NEs. The format and range policies apply only to GUI creation of services, policies, LSPs, and L2 and L3 access interfaces. You cannot configure format and range policies when the services, LSPs, and L2 and L3 access interfaces are created using templates. However, the 5620 SAM allows an

operator to use preconfigured examples of LSPs and services that have format and range policies applied to them. The examples can be used to create a template. For information about creating templates from a preconfigured example, see “Format and range policies configuration of services and LSPs using templates” in the *5620 SAM Scripts and Templates Developer Guide*.

See [6.19 “To create or configure a format policy” \(p. 180\)](#) for information about configuring a format policy. See [6.20 “To create or configure a range policy” \(p. 182\)](#) for information about configuring a range policy.

The following table lists the objects and associated parameters that can be managed using format and range policies.

Table 8 Format and Range policy objects and associated parameters

Object name	Format policy parameter	Range policy parameter
B-VPLS Service Site	Description, Name	—
Bypass-only LSP	Description, Name	ID
Customer	—	ID
Dynamic LSP	Description, Name	ID
I-VPLS Service Site	Description, Name	—
IES Group Interface	Description, Name	Interface ID
IES L3 Access Interface	Description, Name	Interface ID, Outer Encapsulation Value
IES Service	Description, Service Name	Service ID
IES Service Access Point	Description, Name	Outer Encapsulation Value
IES Service Site	Description, Name	—
IES Subscriber Interface	Description, Name	Interface ID
IP Mirror Interface	—	Interface ID
MVPLS B-L2 Access Interface	Description	Outer Encapsulation Value
MVPLS I-L2 Access Interface	Description	Outer Encapsulation Value
MVPLS L2 Access Interface	Description	Outer Encapsulation Value
MVPLS Service	Description, Service Name	Service ID
Mirror L2 Access Interface	—	Outer Encapsulation Value
MVPLS Service B-Site	Description, Name	—
MVPLS Service I-Site	Description, Name	—

Table 8 Format and Range policy objects and associated parameters (continued)

Object name	Format policy parameter	Range policy parameter
MVPLS Service Site	Description, Name	—
Mirror Service	Description, Service Name	Service ID
Mirror Service Site	Description, Name	—
Redundant Interface	—	Interface ID
Spoke SDP Binding	—	VC ID
Static LSP	Description, Name	ID
Tunnel	Description, Name	ID
VLAN L2 Access Interface	Description	—
VLAN Service	Description, Service Name	Service ID
VLAN Service Access Point	Description, Name	—
VLAN Service Site	Description, Name	—
VLL Apipe Service	Description, Service Name	Service ID
VLL Apipe Service Site	Description, Name	—
VLL Cpipe Service	Description, Service Name	Service ID
VLL Cpipe Site	Description, Name	—
VLL Epipe Service	Description, Service Name	Service ID
VLL Epipe Service Site	Description, Name	—
VLL Fpipe Service	Description, Service Name	Service ID
VLL Fpipe Service Site	Description, Name	—
VLL Ipipe L2 Access Interface	Description	Outer Encapsulation Value
VLL Ipipe Service	Description	Service ID
VLL Ipipe Site	Description, Name	—
VLL L2 Access Interface	Description	Outer Encapsulation Value
VPLS B-L2 Access Interface	Description	Outer Encapsulation Value
VPLS I-L2 Access Interface	Description	Outer Encapsulation Value
VPLS L2 Access Interface	Description	Outer Encapsulation Value
VPLS L2 Management Interface	—	Interface ID
VPLS Service	Description, Service Name	Service ID

Table 8 Format and Range policy objects and associated parameters (continued)

Object name	Format policy parameter	Range policy parameter
VPLS Service Site	Description, Name	—
VPRN Group Interface	Description, Name	Interface ID
VPRN L3 Access Interface	Description, Name	Interface ID, Outer Encapsulation Value
VPRN Service	Description, Service Name	Service ID
VPRN Service Access Point	Description, Name	Outer Encapsulation Value
VPRN Service Site	Description, Name	—
VPRN Subscriber Interface	Description, Name	Interface ID

The following table lists the policies that support format and range policies.

Table 9 Format and Range policy objects and associated parameters for policies

Policy	Format policy	Range policy
Access Ingress QoS	Description, Displayed Name	ID
Access Egress QoS	Description, Displayed Name	ID
ATM QoS policy	Description, Displayed Name	ID
Egress Queue Group template	Description, Displayed Name	—
7705 SAR Fabric Profile	Description, Displayed Name	ID
Policer Control policy	Description, Displayed Name	—
HSMDA Pool policy	Description, Displayed Name	—
HSMDA Scheduler policy	Description, Displayed Name	—
HSMDA WRED Slope policy	Description, Displayed Name	—
Ingress Queue Group template	Description, Displayed Name	—
MCFR Egress QoS Profile	Description	Profile ID
MCFR Ingress QoS Profile	Description	Profile ID
MLPPP Egress QoS Profile	Description	Profile ID
MLPPP Ingress QoS Profile	Description	Profile ID
Named Buffer Pool policy	Description, Name	—
Network policy	Description, Displayed Name	ID

Table 9 Format and Range policy objects and associated parameters for policies (continued)

Policy	Format policy	Range policy
Network Queue	Description, Name	—
Port Scheduler policy	Description, Displayed Name	—
Sap Access Ingress for 7210	Description, Displayed Name	ID
Network Policy for 7210	Description, Displayed Name	NW Mgr ID, Policy Id
Network Queue for 7210	Description, Name	—
Port Access Egress for 7210	Description, Displayed Name	ID
Port Scheduler for 7210	Description, Displayed Name	—
Slope Policy for 7210	Description, Displayed Name	—
Scheduler policy	Description, Displayed Name	—
WRED Slope policy	Description, Displayed Name	—
ACL IP filter	Description, Displayed Name	Filter ID
ACL IPv6 filter	Description, Displayed Name	Filter ID
ACL MAC filter	Description, Displayed Name	Filter ID
ANCP policy	Displayed Name	—
Host Tracking policy	Description, Displayed Name	—
MSAP policy	Description, Displayed Name	—
PPPoE policy	Description, Displayed Name	—
SLA Profile	Description, Displayed Name	—
Subscriber Explicit Map Entry	Description, Displayed Name	—
Subscriber Identification policy	Description, Displayed Name	—
Subscriber Profile	Description, Displayed Name	—
AA Application filter	—	Entry ID
Egress Multicast Group	Description, Displayed Name	—
Multicast Package	Description, Displayed Name	ID
Multicast CAC	Description, Name	—
Multicast PathMgmt BW policy	Description, Name	—

Table 9 Format and Range policy objects and associated parameters for policies (continued)

Policy	Format policy	Range policy
Multicast PathMgmt Info policy	Description, Name	—
AS Path	Description, AS Path Name	—
Community	Description, Community Name	—
Community Member	Community Member	—
Damping	Damping Name	—
Prefix List	Description, Prefix List Name	—
Statement	Description, Statement Name	—
Service L3 Routing	Export Target IP Address, Import Target IP Address, Target IP Address	Export Target AS Value, Export Target AS Value (4Byte), Export Target Community Value, Export Target Extended Community Value, Export Target AS Value, Import Target AS Value (4Byte), Import Target Community Value, Import Target Extended Community Value, Target AS Value, Target AS Value (4Byte), Target Community Value, Target Extended Community Value,
MPLS Administrative Groups	Displayed Name	Value
Static Configuration for SRLGs	Displayed Name	—
Shared Risk Link Group Static Config	Displayed Name	Value
Accounting policy	Description, Displayed Name	ID
File policy	Description, Displayed Name	ID
Maintenance Domain	Description, Name	MD Mgr ID
Network Address Translation policy	Description, Displayed Name	—
PAE 802_1x policy	Description, Displayed Name	—

Table 9 Format and Range policy objects and associated parameters for policies (continued)

Policy	Format policy	Range policy
RADIUS Based Accounting	Description, Displayed Name	—
RMON	Description, Displayed Name	—
Time of Day Suite	Description, Name	—
Time Range	Description, Name	—
VRRP policy	Description, Displayed Name	ID, Service ID

6.4 5620 SAM license management

6.4.1 Overview

You can view the 5620 SAM license information by choosing Help→5620 SAM License Information from the 5620 SAM main menu. The 5620 SAM License form lists the following, which you can export to a text file, if required.

- basic information, such as the software release, license type and the system ID of the main server associated with the license
- licensed 5620 SAM software options
- consumed and remaining equipment license points
- number of allowed operator positions

You can view the license consumption information for an NE from the Inventory tab of the NE properties form. The tab lists the license information for cards, blades, chassis, and other equipment specific to the NE. See “Inventory Management Overview” in the *5620 SAM User Guide* for more information.

The Manage Equipment form displays license consumption information specific to a type of equipment, for example, a physical card.



Note: When the 5620 SAM license capacity is reached, the 5620 SAM does not discover new equipment.

To enable the options or equipment capacity specified in a new license, you must import the license file on each 5620 SAM main server, as described in [6.8 “To update the 5620 SAM license in a standalone deployment” \(p. 164\)](#) and [6.9 “To update the 5620 SAM license in a redundant deployment” \(p. 165\)](#). If required, you can uncompress a license file and view the contained license information, which is in XML format.

6.5 Workflow to configure 5620 SAM components

6.5.1 Process

1

As required, manage the 5620 SAM software and license configuration.

- a. View the 5620 SAM license information, such as the equipment license capacity and the installed 5620 SAM options; see [6.6 “To view the 5620 SAM license information” \(p. 163\)](#) .
- b. Export the 5620 SAM license information to a file; see [6.7 “To export the 5620 SAM license information to a file” \(p. 164\)](#) .
- c. Update the 5620 SAM license. For a standalone deployment, see [6.8 “To update the 5620 SAM license in a standalone deployment” \(p. 164\)](#) . For a redundant deployment, see [6.9 “To update the 5620 SAM license in a redundant deployment” \(p. 165\)](#) .
- d. View a list of the backup copies of 5620 SAM license files; see [6.10 “To list the backed-up 5620 SAM license files” \(p. 168\)](#) .
- e. Change the 5620 SAM license expiry notification date; see [6.11 “To change the default 5620 SAM license expiry notification date” \(p. 169\)](#) .

2

As required, configure 5620 SAM system components.

- a. Modify the base configuration of each 5620 SAM GUI client that connects to the 5620 SAM; see [6.12 “To modify the base configuration of all GUI clients” \(p. 171\)](#) .
- b. Display multiple server login options on a 5620 SAM client GUI to allow you to connect to an alternate 5620 SAM server; see [6.13 “To configure the display of multiple 5620 SAM systems as client GUI login options” \(p. 172\)](#) .
- c. Customize the default file location of 5620 SAM client delegate server files such as the user-defined GUI preference, script results files, and client log files; see [6.14 “To change the default user file locations on a client delegate server” \(p. 174\)](#) .
- d. Change the IP address or hostname of a 5620 SAM component, for example, a server or database; see [6.15 “To change the IP address or hostname of a 5620 SAM system component” \(p. 175\)](#) .
- e. Enable 5620 SAM database backup file synchronization; see [6.16 “To enable 5620 SAM database backup file synchronization” \(p. 176\)](#) .
- f. Modify the default time period of the statistics displayed by the 5620 SAM Statistics Manager search filters; see [6.17 “To modify the default time period of statistics displayed by the Statistics Manager search filters” \(p. 178\)](#) .
- g. Modify the default time period of the statistics displayed on the Statistics tab on

object properties forms; see [6.18 “To modify the default time period of statistics displayed on object properties forms”](#) (p. 179) .

- h. Create format policies to manage how services, policies, LSPs, L2 and L3 access interfaces are named and described; see [6.19 “To create or configure a format policy”](#) (p. 180) .
- i. Create range policies to manage the ID numbers that are assigned to services, policies, LSPs, L2 and L3 access interfaces; see [6.20 “To create or configure a range policy”](#) (p. 182) .

3

As required, configure 5620 SAM network management functions.

- a. Configure the 5620 SAM to automatically remove the configuration backup files for a device when the device is unmanaged; see [6.21 “To configure automatic device configuration backup file removal”](#) (p. 185) .
- b. Enable alarm reporting to identify duplicate NE system IP addresses; see [6.22 “To enable alarm reporting to identify duplicate NE system IP addresses”](#) (p. 186) .
- c. Enable LSP on-demand resynchronization to disable scheduled resynchronization for some LSP objects; see [6.24 “To enable LSP on-demand resynchronization”](#) (p. 189) .
- d. Reload the debug configuration file after an NE restarts to ensure mirror services in a managed network resume operation after a reboot or a CPM activity switch; see [6.25 “To enable debug configuration file reloading on an NE for mirror services”](#) (p. 191) .
- e. Configure throttle rates for residential subscriber create and delete event traps on the 7750 SR; see [6.26 “To configure throttle rates for subscriber trap events”](#) (p. 193) .
- f. Configure the windowing trap delayer option to provide an enhanced method to resync the subscriber table in the event of a trap drop from an NE; see [6.27 “To configure the windowing trap delayer option for subscriber table resyncs”](#) (p. 193) .
- g. Create a default SNMPv2 OmniSwitch user on a 5620 SAM system; see [6.28 “To create a default SNMPv2 OmniSwitch user on a 5620 SAM system”](#) (p. 196) .

4

As required, customize the global 5620 SAM alarm settings to meet specific operational requirements, for example:

- severity, clearing, and deletion criteria
- history logging

See “Alarm management” in the *5620 SAM User Guide* for detailed information about the global alarm settings that can be customized.

5

As required, customize or change the 5620 SAM system preferences to meet operational requirements; see [6.29 “To configure 5620 SAM system preferences” \(p. 198\)](#) .

Software and license configuration procedures

6.6 To view the 5620 SAM license information

6.6.1 Steps

1

To view the 5620 SAM license information in the client GUI:



Note: You can also list equipment license information for one NE or the entire network using the 5620 SAM Equipment Manager; see the “Inventory management” chapter of the *5620 SAM User Guide*.



Note: The Equipment Manager does not display 1830 PSS GMPLS NE license information. See the *5620 SAM Optical User Guide* for information about viewing and managing 1830 PSS GMPLS NE licenses

1. Choose Help→5620 SAM License Information from the 5620 SAM main menu. The 5620 SAM License (Edit) form opens.
2. View the license information in the following panels:
 - License Information—basic license and system information
 - Options—the optional 5620 SAM functions that are enabled
 - Licensed Limits—the number of consumed and remaining license points for capacity-based licensing objects such as equipment
3. A highlighted entry in the Licensed Limits panel is alarmed, and may indicate that the license capacity is approaching or has reached the license limit. To view the current alarms against an entry, double-click on the entry and click on the Faults tab of the form that opens.
4. Close the open forms, as required.

2



CAUTION

Service Disruption

A 5620 SAM license file is digitally signed. If you rename or modify the license XML file, the 5620 SAM rejects the license.

Do not rename or modify the XML file inside a compressed license file.

To verify the contents of a 5620 SAM license file, for example, if you are unsure which file contains a specific license option or number of license points:



Note: A license file does not include an object that has a licensed quantity of zero.

1. Uncompress the license zip file.
2. View the contents of the contained XML file.
3. Close the file.

END OF STEPS

6.7 To export the 5620 SAM license information to a file

6.7.1 Steps

1

Choose Help→5620 SAM License Information from the 5620 SAM main menu. The 5620 SAM License (Edit) form opens.

2

Click Export License information to file. A Save as form opens.

3

Specify a name, location, and format for the file that is to contain the license information.

4

Click Save. The license information is saved in the specified file.

5

Close the form.

END OF STEPS

6.8 To update the 5620 SAM license in a standalone deployment

6.8.1 Steps

1

Log in to the main server station as the samadmin user.

2

Open a console window.

3

Navigate to the `/opt/5620sam/server/nms/bin` directory.

4

Enter the following:

```
bash$ ./nmserver.bash import_license license_file ↵
```

where *license_file* is the absolute file path of the 5620 SAM license zip file

The following prompt is displayed:

```
Detected a 5620 SAM license key. Do you want to proceed? (YES/no):
```

5

Enter the following:

```
YES ↵
```

The main server reads the license file, copies the license file to a backup location, and displays the following status information:

```
Importing 5620 SAM license key...
Original license key file has been backed up to /opt/5620sam/server/
timestamp/SAMLicense.zip
Done.
```

where *timestamp* is a directory name in the following format: `yyyy.mm.dd-hh.mm.ss`

6

Close the console window.

Verify new license information

7

Perform [6.6 “To view the 5620 SAM license information” \(p. 163\)](#) to verify the imported license information.

8

If a license parameter is incorrect, contact technical support for assistance.

END OF STEPS

6.9 To update the 5620 SAM license in a redundant deployment



Note: The license files that you import to the primary and standby main servers must contain identical license quantity and option values.



Note: To reduce the risk of importing mismatched licenses, it is recommended that you obtain one license file that contains the system ID of each main server, and then import the same file on each main server.



Note: The primary and standby main server licenses must be synchronized to ensure correct 5620 SAM operation in the event of a server activity switch. The main servers compare license values after a system reconfiguration. If a difference is detected, the 5620 SAM raises an alarm that clears when the licenses are synchronized.

6.9.1 Steps

Update license on primary main server

1

Open a client GUI to monitor the 5620 SAM during the license update.

2

Log in to the primary main server station as the samadmin user.

3

Open a console window.

4

Navigate to the `/opt/5620sam/server/nms/bin` directory.

5

Enter the following:

```
bash$ ./nmserver.bash import_license license_file ↵
where license_file is the absolute file path of the 5620 SAM license zip file
The following prompt is displayed:
```

```
Detected a 5620 SAM license key. Do you want to proceed? (YES/no):
```

6

Enter the following:

```
YES ↵
```

The primary main server reads the license file, copies the license file to a backup location, and displays the following status information:

```
Importing 5620 SAM license key...
Original license key file has been backed up to /opt/5620sam/server/
timestamp/SAMLICENSE.zip
Done.
```

where *timestamp* is a directory name in the following format: yyyy.mm.dd-hh.mm.ss

i **Note:** Importing the new license on the primary main server creates a license mismatch with the standby main server. As a result, the 5620 SAM generates an alarm. The alarm clears automatically after you import the new license on the standby main server.

7

Close the console window.

Update license on standby main server

8

Log in to the standby main server station as the samadmin user.

9

Open a console window.

10

Navigate to the /opt/5620sam/server/nms/bin directory.

11

Enter the following:

```
bash$ ./nmsserver.bash import_license license_file ↵
where license_file is the absolute file path of the 5620 SAM license zip file
The following prompt is displayed:
```

```
Detected a 5620 SAM license key. Do you want to proceed? (YES/no):
```

12

Enter the following:

```
YES ↵
```

The standby main server reads the license file, copies the license file to a backup location, and displays the following status information:

```
Importing 5620 SAM license key...
Original license key file has been backed up to /opt/5620sam/server/
timestamp/SAMLicense.zip
Done.
```

where *timestamp* is a directory name in the following format: yyyy.mm.dd-hh.mm.ss

-
- 13** _____
Ensure that the license mismatch alarm clears automatically. If it does not, contact technical support.

Verify new license information

- 14** _____
Perform [6.6 “To view the 5620 SAM license information” \(p. 163\)](#) to verify the imported license information.

- 15** _____
If a license parameter is incorrect, contact technical support.

END OF STEPS _____

6.10 To list the backed-up 5620 SAM license files

6.10.1 Purpose

When you import a 5620 SAM license, the 5620 SAM creates a backup copy of the existing license file. The following steps describe how to list the 5620 SAM license files.

6.10.2 Steps

- 1** _____
Log in to the main server station as the samadmin user.

- 2** _____
Open a console window.

- 3** _____
Navigate to the /opt/5620sam/server/nms/bin directory.

- 4** _____
Enter the following:

```
bash$ ./nmserver.bash import_license ↵
```


The command lists the files, as shown below:

The following backed up license key files have been detected on the system.

```
/opt/5620sam/server/timestamp1/SAMLlicense.zip
/opt/5620sam/server/timestamp2/SAMLlicense.zip
```

```
.
```

where *timestamp1* and *timestamp2* are directory names in the following format:
yyyy.mm.dd-hh.mm.ss

5 _____

Close the console window.

END OF STEPS _____

6.11 To change the default 5620 SAM license expiry notification date

6.11.1 Purpose

The 5620 SAM raises a daily warning alarm as the expiry date of the 5620 SAM license approaches. By default, the first alarm is raised seven days before the expiry date. Perform this procedure to change the default 5620 SAM license expiry notification date.



CAUTION

Service Disruption

Modifying the nms-server.xml file can have serious consequences that can include service disruption.

Contact technical support before you attempt to modify the nms-server.xml file.

6.11.2 Steps

1 _____

Log in to the main server station as the samadmin user.

2 _____

Navigate to the /opt/5620sam/server/nms/config directory.

3 _____

Create a backup copy of the nms-server.xml file.

4 _____

Open the nms-server.xml file using a plain-text editor such as vi.

5 _____

Locate the following XML tag in the nms-server.xml file:

```
<license  
  timedLicenseExpiryCount="value"
```

where *value* is the number of days prior to timed license expiry.

6 _____

Modify the value to the required number of days to be notified before expiry.

7 _____

Save and close the nms-server.xml file.

8 _____

Open a console window.

9 _____

Navigate to the /opt/5620sam/server/nms/bin directory.

10 _____

Enter the following:

```
bash$ ./nmsserver.bash read_config ↵
```

The main server reads the nms-server.xml file and the time period is updated.

END OF STEPS _____

System components configuration procedures

6.12 To modify the base configuration of all GUI clients



Note: You can exclude a specific 5620 SAM client from a global configuration change by using a command line option when you open the client GUI.

Do not use this procedure to configure SSL for 5620 SAM clients. Use the appropriate SSL configuration procedures in the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* to configure SSL.

6.12.1 Steps

1

Log in to the 5620 SAM main server station as the samadmin user.

2

Modify the appropriate client configuration file in the `/opt/5620sam/server/nms/config/clientDeploy` directory. For example, update the `nms-client.xml` file with a new client log location.

3

Open a console window.

4

Enter the following to enable an update notification for clients that connect to the server and to prepare the client configuration files for download.

```
bash$ /opt/5620sam/server/nms/bin/nmsdeploytool.bash deploy ↵
```

5

Perform one of the following on each single-user GUI client and client delegate server station.



Note: When you perform this step on a client delegate server station, you affect each GUI client that connects through the client delegate server.

- a. Update the client configuration by restarting the client GUI. The client automatically backs up the current configuration and applies the configuration change.



Note: On a RHEL client delegate server station, you must start the client software as the root user, or the configuration update fails.

On RHEL, the client configuration backup is stored in the *path/nms/configBackup* directory, where *path* is the client installation location, typically */opt/5620sam/client*.

On Windows, the client configuration backup is stored in the *path\nms\configBackup* directory, where *path* is the client installation location, typically *C:\5620sam\client*.

- b. Retain the current client configuration when the client GUI starts by specifying the startup option that disables the auto-client update function. See “5620 SAM GUI opening and closing procedures” in the *5620 SAM User Guide* for information about 5620 SAM client startup options.

i **Note:** Specifying a client startup option affects only the current GUI session. To ensure that the client configuration is not updated automatically during a subsequent session, you must open the session using the startup option that disables the auto-client update.

END OF STEPS

6.13 To configure the display of multiple 5620 SAM systems as client GUI login options



Note: You cannot configure a client delegate server to display multiple server options on the client login form. If you need client connections to multiple 5620 SAM main servers through a client delegate server, you must install one client delegate server software instance for each main server.

The 5620 SAM auto-client update function overrides the *nms-client.xml* configuration changes that are specified in this procedure. If the *nms-client.xml* file on a main server changes, it overwrites the local client copy the next time the client connects to the server, unless a client startup option is used to prevent it. For information about using client startup options, see the “Procedures for opening and closing the GUI” in the *5620 SAM User Guide*.

It is recommended that you use the 5620 SAM auto-client update function described in [Chapter 6, “5620 SAM component configuration”](#) to modify the 5620 SAM client configuration.

6.13.1 Steps

1

Click on Application→Exit to close the 5620 SAM client GUI, if it is open. The client GUI closes.

2

Navigate to the client configuration directory, typically */opt/5620sam/client/nms/config* on RHEL, and *C:\5620sam\client\nms\config* on Windows.

3

Open the nms-client.xml file using a text editor.

4

Find the lines starting with <j2ee> and <systemMode>. By default, the IP address and port information of the standalone or redundant servers, as configured during installation, are displayed.

5

For each standalone main server or redundant main server pair you need displayed on the client GUI login form, perform the following:

1. Copy the entire <j2ee> and <systemMode> sections of the file.
2. Paste the <j2ee> and <systemMode> sections after the previous section.
3. Modify the ejbServer IP address to the IP address or hostname of the server you need displayed during client GUI login.
4. Modify the nameOne (for standalone) or nameOne and nameTwo (for redundant) parameters to indicate the domain name and hostname of the server, for easier identification by operators. This name does not have to be the hostname of the server domain. In some cases, the name may be the same for the active and standby server in a redundant server domain. The name is not automatically derived from a host lookup.

Note:

Common hostname restrictions apply to the nameOne and nameTwo fields. You cannot use the following special characters:

- !
- #
- \$
- %
- &
- (
-)
- +

5. Save the changes and close the file.

-
- 6 _____
- Log in to the client GUI. The new server options are displayed in the Server drop-down menu.

END OF STEPS _____

6.14 To change the default user file locations on a client delegate server

6.14.1 Purpose

Perform this procedure to configure the default location of one or more of the following on a 5620 SAM client delegate server:

- user preference files that contain the following information:
 - saved table layouts
 - preferences saved using Application→User Preferences
- script result files

6.14.2 Steps

- 1 _____
- Close each 5620 SAM GUI client that connects through the client delegate server by choosing Application→Exit from the 5620 SAM main menu.
- 2 _____
- Log in to the client delegate server station as the samadmin user.
- 3 _____
- Open a console window.
- 4 _____
- Navigate to the client configuration directory, typically /opt/5620sam/client/nms/config on RHEL, and C:\5620sam\client\nms\config on Windows.
- 5 _____
- Open the nms-client.xml file using a plain-text editor.
- 6 _____
- To change the default GUI preferences and table layout file location, insert the following line directly above the </configuration> line at the end of the file:

```
<guiPreferences path="new_file_location" />
```

where *new_file_location* is the new default GUI table layout and GUI preferences location

i **Note:** The specified location can be an absolute file path or a file path relative to *install_dir/nms*, where *install_dir* is the client installation location.

7

To change the default script result file location, insert the following line directly above the `</configuration>` line at the end of the file:

```
<cache directoryName="new_file_location" />
```

where *new_file_location* is the new default script result file location

i **Note:** The specified location can be an absolute file path or a file path relative to *install_dir/nms*, where *install_dir* is the client installation location.

8

Save and close the `nms-client.xml` file. Subsequent 5620 SAM client sessions on the client delegate server use the new file location.

END OF STEPS

6.15 To change the IP address or hostname of a 5620 SAM system component

6.15.1 Purpose

Changing the IP address or hostname of one or more 5620 SAM components in a standalone or redundant system may be required, for example, when the management network topology changes.

Typically, an IP address or hostname change on a 5620 SAM component requires a series of component uninstallation and re-installation activities, depending on the scope of the change. The requirements of such an operation depend on the management network topology and other considerations, so must be co-ordinated and performed only under the guidance of technical support.



CAUTION

Service Disruption

Changing an IP address or hostname in a 5620 SAM system is a complex operation that requires careful planning and organization, and depending on the type of change required, may involve a brief network management outage.

Do not attempt to modify the network configuration of a 5620 SAM component without assistance from technical support.

6.15.2 Steps

1

Collect the following information:

- the hostname of each main server, auxiliary server, client delegate server, and 5620 SAM database station in the 5620 SAM system
- the current IP address of each interface that is used by the main servers, auxiliary servers, client delegate servers, and 5620 SAM databases
- configuration information for mechanisms in the management network that affect addressing, such as NAT
- the new IP addresses and hostnames of the components

2

Contact technical support to schedule a maintenance period for the network configuration change.

END OF STEPS

6.16 To enable 5620 SAM database backup file synchronization

6.16.1 Purpose

Perform this procedure to enable the main servers in a redundant 5620 SAM system to synchronize the 5620 SAM database backup file sets. After a database backup, if database backup file synchronization is enabled, the 5620 SAM automatically copies the database backup file set to the standby database station.



Note: This procedure applies only to a redundant 5620 SAM deployment.



Note: Before you perform this procedure, you must ensure that there is sufficient network bandwidth between the 5620 SAM database stations for a database copy operation. See the *5620 SAM Planning Guide* for information about the bandwidth requirements of database backup file synchronization.



Note: You must perform this procedure first on the standby main server station, and then on the primary main server station.

6.16.2 Steps

1 _____
Log in to the main server station as the root user.

2 _____
Open a console window.

3 _____
Enter the following:
`# samconfig -m main ↵`
The following is displayed:
Start processing command line inputs...
<main>

4 _____
Enter the following:
<main> `configure redundancy database backup-sync ↵`
The prompt changes to <main configure redundancy database>.

5 _____
Enter the following:
<main configure redundancy database> `exit ↵`
The prompt changes to <main>.

6 _____
Enter the following:
<main> `apply ↵`
The configuration change is applied.

7 _____
Enter the following:
<main> `exit ↵`
The samconfig utility closes.

8

Enter the following to switch to the samadmin user:

```
# su - samadmin ↵
```

9

Navigate to the /opt/5620sam/server/nms/bin directory.

10

Enter the following:

```
bash$ ./nmserver.bash read_config ↵
```

The main server puts the configuration change into effect. The 5620 SAM automatically copies subsequent 5620 SAM database backup file sets from the primary database station to the standby database station.

END OF STEPS

6.17 To modify the default time period of statistics displayed by the Statistics Manager search filters

6.17.1 Purpose

By default, the 5620 SAM Statistics Manager limits search results to statistics records collected during the past hour. Perform this procedure to modify the default time period of the statistics displayed by the 5620 SAM Statistics Manager search filters.



CAUTION

Service Disruption

Consider possible service disruptions before modifying the statistics default time period.

Changing the default time period for the 5620 SAM Statistics Manager search filters can affect the performance of the 5620 SAM.

6.17.2 Steps

1

Choose Application→Exit to close the 5620 SAM client GUI, if it is open. The 5620 SAM client GUI closes.

2

Navigate to the client configuration directory, typically /opt/5620sam/client/nms /config on RHEL, and C:\5620sam\client\nms\config on Windows.

3 _____

Open the nms-client.xml file using a text editor.

4 _____

Locate the XML tag:

```
<statistics
```

5 _____

Edit the following line to read:

```
browserDefaultHour="value"
```

where *value* is the default number of hours for the Past <number_of_hours> filter.

6 _____

Save the changes and close the file.

7 _____

Open a new 5620 SAM client and login. The new value is displayed on the Statistics Manager form.

END OF STEPS _____

6.18 To modify the default time period of statistics displayed on object properties forms

6.18.1 Purpose

By default, the 5620 SAM displays the statistics records collected during the past hour on the Statistics tab on object properties forms. Perform this procedure to modify the default time period of the statistics displayed on the Statistics tab of an object properties form.



CAUTION

Service Disruption

Consider possible service disruptions before modifying the statistics default time period.

Changing the default time period for the 5620 SAM Statistics Manager search filters can affect the performance of the 5620 SAM.

6.18.2 Steps

- 1 _____
Choose Application→Exit to close the 5620 SAM client GUI, if it is open. The 5620 SAM client GUI closes.
- 2 _____
Navigate to the client configuration directory, typically `/opt/5620sam/client/nms/config` on RHEL, and `C:\5620sam\client\nms\config` on Windows.
- 3 _____
Open the `nms-client.xml` file using a text editor.
- 4 _____
Locate the following XML tag:

`<statistics`
- 5 _____
Edit the following line to read:

`tabDefaultHour="value"`
where *value* is the default number of hours for the Past `<number_of_hours>` filter.
- 6 _____
Save the changes and close the file.
- 7 _____
Open a new 5620 SAM client and login. The new value is displayed on the Statistics tab of the object properties form.

END OF STEPS _____

6.19 To create or configure a format policy

6.19.1 Steps

- 1 _____
Choose Administration→Format and Range Policies from the 5620 SAM main menu. The Format and Range Polices form opens.


2 Expand Format/Range (Property Rules) and choose Format Policy (Property Rules) from the Select Object Type drop-down menu.

3 Click Create or choose a format policy and click Properties. The Format Policy (Create | Edit) form opens.

4 Configure the required parameters.

5 Select an object and property for which you need to apply the name format policy in the Property panel.

6 Click on the Users tab.

 **Note:** Only users and user groups that are assigned to this policy are affected by the policy. You can apply one or more format policies to a user or user group. See [Chapter 3, “5620 SAM user security”](#) for more information about creating users and user groups.


7 Click Add. The Select User form opens with a list of users.

8 Select one or more users in the list and click OK. The Format Policy form is refreshed with the selected users.

9 Click on the User Groups tab.

10 Click Add. The Select Group form opens with a list of user groups.

11 Choose one or more user groups in the list and click OK. The Format Policy (Create | Edit) form is refreshed with the selected user groups.

-
- 12** Click on the Text Block Formats tab to further define the format of the text. For example, an operator can classify a group of services with a similar name. The operator can also create a tool tip text to describe the purpose of the parameter.
-
- 13** Click Move Up or Move Down to change the sequence of the text blocks in the text string.
-
- 14** Click Create and perform one of the following:
- Choose Auto-Filled Parameter. The Auto-Filled Parameter (Create) form opens.
 - Choose Masked Text Parameter. The Formatted Text (Create) form opens.
 - Choose Number Range Parameter. The Number Range (Create) form opens.
 - Choose Text Parameter. The Text (Create) form opens.
-
- 15** Configure the required parameters.
- The Min. Length and Max. Length parameters are not configurable when the Read Only parameter is enabled.
-
- 16** Save your changes and close the forms.
-  **Note:** After a format policy is applied to a service, a drop-down menu is displayed beside the object field during object creation, to indicate that a format policy is in effect. When there is only one matching policy, the drop-down menu is dimmed. When there are multiple matching policies, the drop-down menu is used to choose a policy. The sequence of the policies in the drop-down menu is based on the value of the Priority parameter.

END OF STEPS

6.20 To create or configure a range policy

6.20.1 Steps

-
- 1** Choose Administration→Format and Range Policies from the 5620 SAM main menu. The Format and Range Polices form opens.

2 _____
Expand Format/Range (Property Rules) and choose Range Policy (Property Rules) from the Select Object Type drop-down menu.

3 _____
Click Create or choose a range policy and click Properties. The Range Policy (Create | Edit) form opens.


4 _____
Configure the required parameters.

5 _____
Select an object and property for which you need to apply the range policy in the Property panel.

6 _____
Configure the parameters in the Range panel.

7 _____
Configure the parameters in the Auto Assignment panel.

8 _____
Click on the Users tab.

 **Note:** Only users and user groups that are assigned to this policy are affected by the policy. You can apply one or more range policies to a user or user group. See [Chapter 3, "5620 SAM user security"](#) for more information about creating users and user groups.

9 _____
Click Add. The Select User form opens with a list of users.


10 _____
Choose one or more users in the list and click OK. The Range Policy form is refreshed with the users.

11 _____
Click on the User Groups tab.

12 _____
Click Add. The Select Group form opens with a list of user groups.

13 _____
Choose one or more user groups in the list and click OK. The Range Policy form is refreshed with the user groups.

14 _____
Click OK and close the forms.

 **Note:** After a range policy is applied to a service, a drop-down menu is displayed beside the object field during object creation, to indicate that a range policy is in effect. When there is only one matching policy, the drop-down menu is dimmed. When there are multiple matching policies, the drop-down menu is used to choose a policy. The sequence of the policies in the drop-down menu is based on the value of the Priority parameter.

END OF STEPS _____

Network management configuration procedures

6.21 To configure automatic device configuration backup file removal

6.21.1 Purpose

Configure the 5620 SAM to automatically remove the configuration backup files for a device when the device is unmanaged.



CAUTION

Service Disruption

This procedure requires a restart of the 5620 SAM server.

A server restart can be service-affecting.

6.21.2 Steps

1 _____

Navigate to the `/opt/5620sam/server/nms/config` directory.

2 _____

Create a backup copy of the `nms-server.xml` file.

3 _____



CAUTION

Service Disruption

Modifying the `nms-server.xml` file can have serious consequences that can include service disruption.

Contact technical support before you attempt to modify the `nms-server.xml` file.

Open the `nms-server.xml` file using a plain-text editor.

4 _____

Search for the following XML tag:

```
</configuration>
```

5 _____

Enter the following line above the `</configuration>` tag:

```
<nodeBackups removeBackupOnDelete="true"/>
```

6

Save and close the nms-server.xml file.

7

Open a console window.

8

Navigate to the /opt/5620sam/server/nms/bin directory.

9

**CAUTION****Service Disruption**

Restarting a 5620 SAM server is service-affecting.

Ensure that you perform this step only during a scheduled maintenance window.

Enter the following at the console prompt to restart the 5620 SAM server:

```
bash$ ./nmserver.bash force_restart ↵
```

10

The 5620 SAM main server restarts. The 5620 SAM deletes the configuration backup files of NEs that are subsequently unmanaged.

END OF STEPS

6.22 To enable alarm reporting to identify duplicate NE system IP addresses

6.22.1 Purpose

Perform this procedure to enable the 5620 SAM to verify the uniqueness of NE system IP addresses. When verification is enabled, the 5620 SAM generates an alarm when an NE reports a system IP address that is in use by another NE.

6.22.2 Steps

1

Log in to the main server station as the samadmin user.

2 _____
Open a console window.

3 _____
Navigate to the /opt/5620sam/server/nms/config directory.

4 _____



CAUTION

Service Disruption

Modifying the nms-server.xml file can have serious consequences that can include service disruption.

Contact technical support before you attempt to modify the nms-server.xml file.

Open the nms-server.xml file using a plain-text editor.

5 _____
Locate the following tag that marks the beginning of the SNMP section:

```
<snmp
```

6 _____
Add the following before the end of the SNMP section, ensuring that there is a space between the last character and the section end, which is marked by a /> tag:
verifyNodeIdentity="1"

7 _____
Save and close the nms-server.xml file.

8 _____
Navigate to the /opt/5620sam/server/nms/bin directory.

9 _____
Enter the following:
bash\$./nmsserver.bash read_config ↵

The main server reads the `nms-server.xml` file and alarm reporting for duplicate NE system IP addresses is enabled.

END OF STEPS

6.23 To enable dynamic system IP address updates for 7705 SAR nodes

6.23.1 Purpose

Perform this procedure to allow the 5620 SAM to react automatically when the IP address of a 7705 SAR node changes (for example, if it acquires a new address through DHCP). 7705 SAR nodes are instead uniquely identified in the network using a System ID parameter. Before enabling this feature, please consider the following:

- The System ID for each 7705 SAR node must be unique, or the 5620 SAM may update SDPs to point to the incorrect node. You can configure the system ID parameter through CLI.
- 7705 SAR nodes in the network should be unmanaged before performing this procedure.

6.23.2 Steps

1

Log in to the main server station as the `samadmin` user.

2

Open a console window.

3

Navigate to the `/opt/5620sam/server/nms/config` directory.

4



CAUTION

Service Disruption

Modifying the `nms-server.xml` file can have serious consequences that can include service disruption.

Contact technical support before you attempt to modify the `nms-server.xml` file.

Open the `nms-server.xml` file using a plain-text editor.

5

Locate the following tag and related parameters:

```
<SARSysIPAddrChange
    enabled="false"
    ipRange="224.224.0.0"
    prefix="24" />
```

6

Change the value of the enabled parameter to “true”.

7

Save and close the nms-server.xml file.

8

Navigate to the /opt/5620sam/server/nms/bin directory.

9

Enter the following:

```
bash$ ./nmserver.bash read_config ↵
```

The main server reads the nms-server.xml file and alarm reporting for duplicate NE system IP addresses is enabled.

END OF STEPS

6.24 To enable LSP on-demand resynchronization

6.24.1 Purpose

By default, the LSP on-demand resynchronization functionality is disabled. When you enable LSP on-demand resynchronization, the 5620 SAM scheduled resynchronization is then disabled for some LSP objects. See “LSP on-demand resynchronization” in the *5620 SAM User Guide* for information about which LSP objects do not support on-demand resynchronization.



CAUTION

Service Disruption

Modifying the nms-server.xml file can have serious consequences that can include service disruption.

Contact technical support before you attempt to modify the nms-server.xml file.

6.24.2 Steps

- 1 _____
Log in to the main server station as the samadmin user.
- 2 _____
Navigate to the /opt/5620sam/server/nms/config directory .
- 3 _____
Create a backup copy of the nms-server.xml file.
- 4 _____
Open the nms-server.xml file using a plain-text editor.
- 5 _____
Locate the following line:

`<lspOnDemand overrideEnabled="false" />`
- 6 _____
Change "false" to "true".
- 7 _____
Save and close the nms-server.xml file.
- 8 _____
Navigate to the /opt/5620sam/server/nms/bin directory.
- 9 _____
Enter the following:

`bash$./nmsserver.bash read_config ↵`

The main server reads the `nms-server.xml` file and enables LSP on-demand resynchronization.

END OF STEPS

6.25 To enable debug configuration file reloading on an NE for mirror services

6.25.1 Purpose

Perform this procedure to ensure that managed NEs reload the debug configuration file after an NE restart. This ensures that the mirror services in the managed network resume operation after a reboot or a CPM activity switch on the NE that hosts the mirror service. By default, debug configuration file reloading is disabled.



CAUTION

Service Disruption

This procedure requires a 5620 SAM main server restart.

A server restart can be service-affecting.

6.25.2 Steps

1 _____

Log in to the main server station as the `samadmin` user.

2 _____

Open a console window.

3 _____

Navigate to the `/opt/5620sam/server/nms/config` directory.

4 _____



CAUTION

Service Disruption

Modifying the `nms-server.xml` file can have serious consequences that can include service disruption.

Contact technical support before you attempt to modify the `nms-server.xml` file.

Open the `nms-server.xml` file using a plain-text editor.

5

Locate the following XML tag:

```
<serviceMirror
```

6


Specify the NE location of the debug configuration file. For example:

```
<serviceMirror  
  debugFilename=""  
  reloadDelay="10"  
>
```

where

reloadDelay specifies the time, in seconds, to wait before a reload request is sent

debugFilename specifies the location of the file on an NE, for example, cf3:
/ServiceMirror.dbg

 **Note:** The debugFilename value must be the name of the debug configuration file on the NEs that host mirror services.

7

Save and close the nms-server.xml file.

8

Navigate to the /opt/5620sam/server/nms/bin directory.

9



CAUTION

Service Disruption

Restarting a 5620 SAM main server is service-affecting.

Ensure that you perform this step only during a scheduled maintenance window.

Enter the following to restart the main server:

```
bash$ ./nmserver.bash force_restart ↵
```

The main server restarts.

10 _____

If required, create a device backup policy to ensure that device configurations are not lost in the event of an NE failure.

END OF STEPS _____

6.26 To configure throttle rates for subscriber trap events

6.26.1 Purpose

The throttle rate defines the number of events that can be received during a specified interval before the NE stops sending individual traps. Configure throttle rates for residential subscriber create and delete event traps on the 7750 SR.

6.26.2 Steps

1 _____

On the equipment tree, right-click on the NE for which you want to configure trap event throttle rates and choose Properties. The Network Element (Edit) form opens.

2 _____

Click Event Throttling. The ESM Trap Throttle form opens.

3 _____

Disable the Default check box and configure the required parameters.

4 _____

Click Execute. The Detailed Status/Error message field displays status information about the throttle rate change.

5 _____

Close the forms.

END OF STEPS _____

6.27 To configure the windowing trap delayer option for subscriber table resyncs

6.27.1 Purpose

Configure the windowing trap delayer option to provide an enhanced method to resync the subscriber table in the event of a trap drop from an NE.

Configurable hold-off options prevent subscriber table resyncs for a minimum specified duration after a trap drop is received from the NE, and until a specified time window has elapsed with no additional trap drops received from the NE. Additionally, a maximum hold-off time is specified to prevent excessive periods during which the 5620 SAM is out of sync with the NE. The windowing trap delayer configuration reduces the number of subscriber table resync events while providing a reasonable in-sync state with the NE.

The windowing trap delayer option is configured in `nms-server.xml` file. It only affects `tmnxTrapDropped` traps which are related to `tmnxSubscriberCreated`, `tmnxSubscriberDeleted` or `tmnxSubscriberRenamed` traps. When the windowing trap delayer option is disabled, `tmnxTrapDropped` traps are delayed using the default trap delayer function.

6.27.2 Steps

- 1 _____
Log in to the main server station as the `samadmin` user.
- 2 _____
Navigate to the `/opt/5620sam/server/nms/config` directory.
- 3 _____
Create a backup copy of the `nms-server.xml` file.
- 4 _____



CAUTION

Service Disruption

Modifying the `nms-server.xml` file can have serious consequences that can include service disruption.

Contact technical support before you attempt to modify the `nms-server.xml` file.

Open the `nms-server.xml` file using a text editor.

- 5 _____
Locate the following XML tag:

```
<snmp
```

This section of the file contains the 5620 SAM SNMP information.

6

Add the following before the end of the SNMP section, ensuring that there is a space between the last character and the section end, which is marked by a `</>` tag:

```
<windowingTrapDelayer enabled="true" checkInterval="10"
windowLength="30" maxHoldOff="60"/>
```

```
/snmp>
```

where *windowingTrapDelayer enabled* (boolean) sets the windowing trap delayer option as enabled or disabled. The default is true.

checkInterval is the minimum interval after a trap drop is received, during which subscriber table resyncs are prevented. The range is 5 to 30 seconds. The default is 10 seconds.

windowLength is a sliding time interval after a trap drop is received, during which no additional trap drops can be received before subscriber table resyncs are allowed. The range is 5 to 60 seconds. The default is 30 seconds.

maxHoldOff is the absolute maximum hold-off time, after which subscriber table resyncs are allowed. The range is 5 to 1800 seconds. The default is 60 seconds.

The *checkInterval* value must be less than the *windowLength* value, which must be less than the *maxHoldOff* value.

7

Save and close the `nms-server.xml` file.

8

Navigate to the `/opt/5620sam/server/nms/bin` directory.

9

Enter the following:

```
bash$ ./nmserver.bash read_config ↵
```

The main server reads the nms-server.xml file and the window trap delayer function is enabled.

END OF STEPS

6.28 To create a default SNMPv2 OmniSwitch user on a 5620 SAM system



CAUTION

Service Disruption

Modifying the nms-server.xml file can have serious consequences that can include service disruption.

Contact technical support before you attempt to modify the nms-server.xml file.

6.28.1 Steps

1

Log in to the main server station as the samadmin user.

2

Navigate to the /opt/5620sam/server/nms/config directory.

3

Create a backup copy of the nms-server.xml file.

4

Open the nms-server.xml file using a plain-text editor.

5

Locate the following XML tag:

```
<snmp
```

This section of the file contains the 5620 SAM SNMP information.

6

Add the following before the end of the SNMP section, ensuring that there is a space between the last character and the section end, which is marked by a /> tag:

```
snmpV2UserName="user_name"
```

where *user_name* is a user name that is configured on the switch

The SNMP section should read as follows:

```
<snmp
    ip="server_IP_address"
    port="port_number"
    trapLogId="log_ID"
    snmpV2UserName="user_name" />
```

7

Save and close the nms-server.xml file.

8

Navigate to the /opt/5620sam/server/nms/bin directory.

9

Enter the following:

```
bash$ ./nmserver.bash read_config ↵
```

The main server reads the nms-server.xml file and the new SNMPv2 user name is enabled.

END OF STEPS

System preferences configuration procedures

6.29 To configure 5620 SAM system preferences



CAUTION

Service Disruption

Changing a system preference parameter value may adversely affect the 5620 SAM service or function.

Do not change a parameter value from the default without contacting technical support.



Note: You need a user account with the Administrator scope of command role to perform this procedure.

6.29.1 Steps

1

Choose Administration→System preferences from the 5620 SAM main menu. The System Preferences form opens.

The following table lists the settings and functions that can be configured using the System Preferences form, and the location of additional information if applicable. System preferences are listed by the functional tabs on the System Preferences form.

Table 10 5620 SAM system preferences functions or settings

Function or setting	Additionally see
General tab	

Table 10 5620 SAM system preferences functions or settings (continued)

Function or setting	Additionally see
<p>Allows you to configure the default behavior for displaying tabs on 5620 SAM configuration forms including:</p> <ul style="list-style-type: none"> • Pre-hiding some tabs on forms (default) • Showing all tabs on forms • Initially show all tabs on forms 	<p><i>5620 SAM User Guide</i></p>
<p>The NE display threshold for Equipment Group parameter specifies the number of NEs to display when an equipment group is expanded in the navigation tree.</p> <p>Equipment groups can contain up to 2000 NEs. The 5620 SAM client can display NEs in the navigation tree up to a limit of 500 NEs per group. This limit is not configurable, and is not affected by the NE display threshold for Equipment Group parameter.</p> <p>You can set the NE display threshold for Equipment Group parameter to accomplish any of the following:</p> <ul style="list-style-type: none"> • To display all the NEs in equipment groups (when groups contains no more than 500 NEs), set the parameter to the maximum value of 500 (the default). • To display a small number of NEs per equipment group, set the parameter to a low value. The minimum setting is 2. You can use the NE list form to access and manage the NEs in the group, and you can show additional NEs in the tree if required. See “To manage NEs in equipment groups on the navigation tree” in the <i>5620 SAM User Guide</i>. • To allow the display of enough NEs to meet your typical requirements while also allowing additional NEs to show in the tree if necessary, set the parameter to a value in the middle of the range. This is useful if you have more than 500 NEs in a group. For example, if the parameter is set to 300, then 300 of the NEs in the group are displayed in the tree. You can select and display up to 200 additional NEs in that group before the limit of 500 is reached. Select the additional NEs to show in the tree from the NE list form for the group; see “To manage NEs in equipment groups on the navigation tree” in the <i>5620 SAM User Guide</i>. <p>You must close and re-open the 5620 SAM client for changes to the NE display threshold for Equipment Group parameter to take effect. The change is propagated to all clients for a 5620 SAM server, but only after the clients are closed and re-opened.</p>	
<p>Allows you to configure the default behavior for the Save to File option to export CSV files using UTF-8 with BOM (byte order mark) encoding.</p>	
<p>Services tab</p>	

Table 10 5620 SAM system preferences functions or settings (continued)

Function or setting	Additionally see
<p>Allows you to configure the default behavior for the following Services-related functions:</p> <ul style="list-style-type: none"> • For Composite Services: <ul style="list-style-type: none"> — Allow or suppress the auto discovery of Spoke, CCAG, SCP, or RVPLS connectors. — Enable or disable the use of VRF Route Target connections. — Enable or disable the auto discovery of composite services or if service alarms are aggregated for them. • Specify the maximum of sites that can be moved from one service to another when reducing the overall size of a particular service; the default is 25. • Specify the default priority of a service when creating a service; the default is set to Low. • Allow or suppress VPRN SNMP Community string warnings and alarms. • Allow or suppress the automatic removal of an empty service. • Enable or disable the use of multi-segment tunnel selection functionality. • Specify if CAC is enabled or disabled for a service. • Specify if a site name and description of the should be added when a service is created. • Allow or suppress Route Target Reservation alarms. • Enable or disable if a service or service site can be deleted if the service or service site has any child objects such as SAPs, SDP bindings, policies, or any other objects related to the service CLI hierarchy. When enabled, you must first delete all child objects before the service or service site can be deleted. This preference only applies to services or service site associated with SROS-based devices. • Specify if a Service Name should be added to the Site Name when sites are added to a service. 	<p><i>5620 SAM User Guide</i></p>
TCA tab	
<p>Allows you to configure the default behavior associated with configuring TCA policies such as specifying the maximum TCA alarm limit, the TCA alarm reset synchronization time or reset interval, and the default TCA alarm severity.</p>	<p><i>5620 SAM User Guide</i></p>
Statistics tab	
<p>Allows you to configure the default behavior associated when exporting statistics files on a 5620 SAM server such as specifying the default log file retention time (applies to accounting and performance statistics) or log file rollover time (applies to performance statistics).</p>	<p><i>5620 SAM Statistics Management Guide</i></p>
<p>Allows you to enable or disable the storage of performance or accounting statistics in the 5620 SAM database; when database storage is disabled for a statistics type, the statistics data is retained only temporarily on a main or auxiliary server and must be retrieved using the registerLogToFile OSS method</p>	<p><i>5620 SAM Statistics Management Guide</i></p>
<p>Allows you to configure the number of JMS client connection checks when exporting statistics files on a 5620 SAM server that are performed before a registerLogToFile request is automatically de-registered.</p>	<p><i>5620 SAM XML OSS Interface Developer Guide</i></p>

Table 10 5620 SAM system preferences functions or settings (continued)

Function or setting	Additionally see
Bin Alarm tab	
Allows you to configure the maximum Bin Alarm limit, reset synchronization time, reset interval, and alarm severity.	<i>5620 SAM User Guide</i>
Test Manager tab	
Allows you to configure the default retention time for dB test results and target test results and log files performed with the Service Test Manager and which test results are stored.	<i>5620 SAM User Guide</i>
User Activity tab	
Allows you to configure how much user activity log information is stored in the 5620 SAM database before it purges information and the retention period.	Chapter 7, "5620 SAM database management"
OLC tab	
<p>Allows you to configure the default behavior associated with OLC state of an object that is undergoing commissioning or maintenance. You can configure the following:</p> <ul style="list-style-type: none"> • Enable or disable if the OLC state is automatically set to maintenance when the following actions occur: <ul style="list-style-type: none"> — When the Administrative state is down. — If the status of the parent object is set to administratively down. — If the affecting object administrative state is down. • For scheduled objects set to the maintenance mode, if alarm information should be created prior to an OLC revert and the lead time of the alarm notification before reverting. Three OLC time options can be configured for each object. <p>Additionally, the following applies to this system preference configuration:</p> <ul style="list-style-type: none"> • If the Enable Automatic OLC State change parameter is enabled, a Shut Down action will set the object's state to Maintenance and a Turn Up action will set the object's state to In Service. This state change is also applied to any child objects. • The Enable Automatic OLC State change parameter applies only to objects which support the OLC state. It does not apply to routing objects. 	"Configuring the OLC state of equipment or services" (p. 405)
Policies tab	

Table 10 5620 SAM system preferences functions or settings (continued)

Function or setting	Additionally see
<p>Allows you to display or hide the policy names on policy configuration forms for the following:</p> <ul style="list-style-type: none"> • Access ingress and access egress policies • ACL IP, ACL IPv6, and ACL MAC policy filters 	<p><i>5620 SAM User Guide</i></p>
<p>Allow you to set a restriction in the distribution mode for certain types of local policies that will permit local editing only. Additionally, the following applies to this system preference configuration:</p> <ul style="list-style-type: none"> • Policy types supported by this system preference include Access Ingress, Access Egress, Network QoS, ACL MAC, ACL IPv4, and ACL IPv6. • When creating any of these policies, if you set the Scope parameter to exclusive, the 5620 SAM will set the distribution mode to local edit. • The 5620 SAM will not allow policies with the Scope parameter set to exclusive to be assigned or used more than once. • If you attempt to set the Policy Distribution Mode to Sync With Global while the Scope attribute is configured as exclusive, an error message will result. 	
<p>Allow you to specify that for policy changes made using CLI, to switch the distribution mode for certain types of local policies to Local Edit Only, as opposed to the default Sync with Global mode.</p>	
<p>Allows you to configure the automatic distribution of a global policy to applicable NEs once the policy is released.</p>	
<p>Allows you to configure the maximum number of scheduled audit results stored for a local policy.</p>	
<p>Allows you to enable or disable if all zones are re-synchronized from the node as local edit only. If you disable the Discover Security Zone in Local Edit Only parameter, all zones re-synchronized from the node are set to Sync With Global.</p> <ul style="list-style-type: none"> • The Discover Security Zone in Local Edit Only parameter is only supported on the 7705 SAR-8 with CSMv2, 7705 SAR-8v2 with CSMv2, 7705 SAR-18, 7705 SAR-H, 7705 SAR-Hc, and 7705 SAR-Wx variants, Release 6.1 R1 or later. 	
<p>Custom NE Properties tab</p>	
<p>Allows you to configure if custom property labels and values are used to identify an NE, for example, the location and site name that differs from the actual NE site name. These properties cannot be configured on the NE. Additionally, the following applies to this system preference configuration:</p> <ul style="list-style-type: none"> • If custom property labels are not configured, the default labels are used. • NE custom properties support the extended character set including multi-byte characters. • Custom property labels and values are displayed in the following locations: <ul style="list-style-type: none"> — NE Properties form — NE List form 	<p>—</p>

Table 10 5620 SAM system preferences functions or settings (continued)

Function or setting	Additionally see
ESM tab	
<p>Allows you to configure the default behavior associated with the on-demand retrieval of residential subscriber-related information from NEs such as:</p> <ul style="list-style-type: none"> • The tracked subscriber retrieval timeout interval • The subscriber host retrieval timeout interval • The maximum number of residential subscriber instances returned via OSS • If managed route information should be collected • If QoS override information should be collected • If SLAAC host addresses should be collected • If access loop encapsulations should be collected • If BGP peer information should be collected 	<i>5620 SAM User Guide</i>
WMM tab	
<p>Allows you to configure the default behavior for the following 5620 SAM LTE ePC functions:</p> <ul style="list-style-type: none"> • Enable or disable the automatic creation of physical links by the 5620 SAM between SRS and MME 9471 WMMs. • The time-to-live time interval for PM statistics on WMM nodes. • Enable or disable automatic PM file retrieval on discovery or manage to automatically collect any PM files that were missed during an out-of-service software upgrade. • Set the timeout value for on-demand EPS peers queries. 	<i>5620 SAM LTE RAN User Guide</i>
MPR tab	
<p>Allows or denies user-access to configure 9500 MPR devices using a Local Craft Terminal (LCT). This prevents multi-write access sessions on 9500 MPR devices. You can also enable or disable if the 5620 SAM receives LAC alarms from the nodes.</p>	<i>5620 SAM 9500 MPR User Guide</i>
Application Assurance tab	
<p>Allows you to configure the default behavior for the following 5620 SAM AA functions:</p> <ul style="list-style-type: none"> • The database persisted transit IP address retrieval time interval • The database persisted transit prefix address retrieval time interval • The maximum number of database transit subscribers returned via OSS 	<i>5620 SAM User Guide</i>
NFV tab	
<p>Allows you to configure automatic healing and automatic scale-out for the VMM and VMG. You can enable the functions and configure timers to limit the frequency at which automatic scale-out or healing is attempted.</p>	<i>5620 SAM NFV Solutions Guide</i>

2

Configure the required parameters. Information about system preferences parameters is available in the *5620 SAM User Guide* appendix, and in the online help Parameter Search Tool.

3 _____

As required, click on the appropriate tab to configure another system preference.

4 _____

Click OK to save and close the form.

END OF STEPS _____

7 5620 SAM database management

7.1 Overview

7.1.1 Purpose

This chapter describes procedures and mechanisms for 5620 SAM database management.

7.1.2 Contents

5620 SAM database management	207
7.2 Overview	207
7.3 5620 SAM database	207
7.4 Auxiliary database	208
5620 SAM database management procedures	209
7.5 Workflow for 5620 SAM database management	209
7.6 To view the 5620 SAM database properties	211
7.7 To view the auxiliary database status using the client GUI	212
7.8 To view the auxiliary database status using a CLI	213
7.9 To configure the allowed number of Oracle database login attempts	214
7.10 To configure Oracle database error monitoring	217
7.11 To configure a size constraint policy	217
7.12 To configure an ageout constraint policy	219
7.13 To create a database file policy to manage database log or core dump files	221
7.14 To configure the statistics data retention period for the 5620 SAM database	222
7.15 To perform an immediate 5620 SAM database backup using the GUI	223
7.16 To perform an immediate 5620 SAM database backup using a CLI	225
7.17 To back up an auxiliary database	227
7.18 To schedule 5620 SAM database backups	228

7.19 To schedule auxiliary database backups	229
7.20 To unlock the Oracle database user account	230

5620 SAM database management

7.2 Overview

7.2.1 References

The 5620 SAM uses the following databases to store network data such as object configurations, device backups, and statistics:

- 5620 SAM database
- auxiliary database

See the following documents for more information:

- *5620 SAM Planning Guide*—platform and network requirements
- *5620 SAM | 5650 CPAM Installation and Upgrade Guide*—deployment information
- *5620 SAM Troubleshooting Guide*—troubleshooting information
- *5620 SAM Alarm Reference*—alarm descriptions, raising and clearing conditions, and remedial actions

7.3 5620 SAM database

7.3.1 Description

A 5620 SAM system requires a central database for persistent storage. The database can be on the same station as a 5620 SAM main server, or on a separate station. A redundant 5620 SAM deployment has two databases that are synchronized in a primary-standby configuration to limit data loss in the event of a failure.

You can manage the following database functions and parameters:

- security
- statistics data retention
- data synchronization
- backups and restores
- historical record retention
- object ageout
- log storage
- error monitoring
- alarm handling

7.3.2 5620 SAM database safeguards

In addition to the protection of system redundancy, the 5620 SAM has mechanisms that raise alarms for the following:

- database disk and tablespace capacity issues
- redundancy events, misconfiguration, and failures
- database backup misconfiguration and failures
- archive log management actions and failures
- internal errors that may represent a security risk

- size constraint and ageout constraint policy violations

7.4 Auxiliary database

7.4.1 Description

A 5620 SAM auxiliary database is an optional, distributed database that reduces the 5620 SAM database processing load for demanding operations such as statistics collection. An auxiliary database is deployed as a cluster of separate stations. Load balancing and data replication among the stations provide high performance and robust fault tolerance.

You can use the 5620 SAM client GUI to perform the following operations:

- View the status of each auxiliary database station in the cluster.
- Perform manual and scheduled database backups.

7.4.2 Auxiliary database safeguards

The 5620 SAM monitors each station in an auxiliary database cluster and raises alarms for the following events:

- station unavailability
- cluster unavailability

5620 SAM database management procedures

7.5 Workflow for 5620 SAM database management

7.5.1 Process

Viewing database properties and status

- 1 _____
Display the 5620 SAM database properties; see [7.6 “To view the 5620 SAM database properties”](#) (p. 211) .
- 2 _____
Display the auxiliary database properties; see [7.7 “To view the auxiliary database status using the client GUI”](#) (p. 212) and [7.8 “To view the auxiliary database status using a CLI”](#) (p. 213).

Configuring database operation and security

- 3 _____
As a security precaution, configure the number of failed Oracle database user login attempts that the 5620 SAM allows before a user is locked out; see [7.9 “To configure the allowed number of Oracle database login attempts”](#) (p. 214) .
- 4 _____
Configure how the 5620 SAM responds to Oracle database errors; see [7.10 “To configure Oracle database error monitoring”](#) (p. 217) .
- 5 _____
Configure size constraint policies to regulate the number of records retained in the 5620 SAM database; see [7.11 “To configure a size constraint policy”](#) (p. 217) .
- 6 _____
Configure ageout constraint policies to define a configurable ageout time for a specific object type in the 5620 SAM database; see [7.12 “To configure an ageout constraint policy”](#) (p. 219) .
- 7 _____
Manage 5620 SAM database disk usage by configuring policies to manage the file size and number of archive log and core dump files; see [7.13 “To create a database file policy to manage database log or core dump files”](#) (p. 221) .

-
- 8 _____
Configure the statistics data retention period for the 5620 SAM database; see [7.14 “To configure the statistics data retention period for the 5620 SAM database”](#) (p. 222) .

Backup, restore, and general maintenance

- 9 _____
Perform an immediate full or partial 5620 SAM database backup; see [7.15 “To perform an immediate 5620 SAM database backup using the GUI”](#) (p. 223) or [7.16 “To perform an immediate 5620 SAM database backup using a CLI”](#) (p. 225) .
- 10 _____
Schedule a regular 5620 SAM database backup; see [7.18 “To schedule 5620 SAM database backups”](#) (p. 228) .
- 11 _____
Back up an auxiliary database; see [7.17 “To back up an auxiliary database”](#) (p. 227) .
- 12 _____
Schedule regular auxiliary database backups; see [7.19 “To schedule auxiliary database backups”](#) (p. 229) .
- 13 _____
Restore the 5620 SAM database in a standalone or redundant system; see [14.30 “To restore the database in a standalone 5620 SAM system”](#) (p. 371).
- 14 _____
Restore an auxiliary database; see [14.23 “To restore an auxiliary database”](#) (p. 358)
- 15 _____
Test the 5620 SAM database restore function to ensure that 5620 SAM database backups are viable in the event of a failure; see [12.7 “To test a 5620 SAM database restore”](#) (p. 304) .
- 16 _____
Verify the synchronization of NE and 5620 SAM database information; see [11.6 “To verify 5620 SAM database information”](#) (p. 295) .

Incidental tasks

17

As required, unlock the Oracle database user account due to multiple login failures; see [7.20 “To unlock the Oracle database user account”](#) (p. 230) .

18

Manage 5620 SAM database redundancy in a redundant system:

- Perform a 5620 SAM database switchover; see [8.10 “To configure 5620 SAM database switchover behavior”](#) (p. 260) , [8.11 “To perform a 5620 SAM database switchover using the 5620 SAM client GUI”](#) (p. 261) , or [8.12 “To perform a 5620 SAM database switchover using a CLI script”](#) (p. 262) .
- Enable or disable automatic database realignment on a main server; see [8.14 “To enable or disable automatic database realignment”](#) (p. 265) .
- Re-establish redundancy after a database activity switch or similar maintenance activity; see [8.15 “To instantiate a redundant database using the 5620 SAM client GUI”](#) (p. 268) and [8.16 “To instantiate a redundant database using a CLI script”](#) (p. 269) .

19

Troubleshoot 5620 SAM database problems such as corruption, failure, disk space shortage, or performance degradation. See the *5620 SAM Troubleshooting Guide*.

7.6 To view the 5620 SAM database properties

7.6.1 Steps

1

Choose Administration→Database from the 5620 SAM main menu. The Database Manager (Edit) form opens and displays information that includes the following:

- Database Name—created during 5620 SAM installation
- Instance Name—created during 5620 SAM installation
- Listener Port—the port on the main server for database communication
- DBID—the Oracle database ID, sometimes called the SID
- Creation Time—the database creation time
- Version—the Oracle version identifier
- IP Address—the database IP address that the main and auxiliary servers use
- Host Name—the database station hostname
- Open Mode—specifies the type of database access
- Archive Log Mode—specifies whether to archive the database log files; configured during database installation
- Protection Mode—the database protection mode, which cannot be changed

-
- 2 _____
View the information.
 - 3 _____
Close the Database Manager (Edit) form.

END OF STEPS _____

7.7 To view the auxiliary database status using the client GUI

7.7.1 Purpose

Perform this procedure to display information about an auxiliary database in the 5620 SAM client GUI.

7.7.2 Steps

- 1 _____
Choose Administration→Database from the 5620 SAM main menu. The Database Manager form opens.
- 2 _____
Click on the Auxiliary Database Cluster tab. The auxiliary database clusters are listed.
- 3 _____
Select a cluster and click Properties. The Auxiliary Database Cluster (View) form opens.
- 4 _____
Click on the Auxiliary Databases tab. The auxiliary database stations in the cluster are listed.
- 5 _____
Select an auxiliary database station and click Properties. The Auxiliary Database (View) form opens.
- 6 _____
View the State and Connectivity State indicators. During normal operation, the indicators display:
 - State—Up
 - Connectivity State—Online

If the indicators display different values, contact technical support for assistance.

7

Close the open forms.

END OF STEPS

7.8 To view the auxiliary database status using a CLI

7.8.1 Purpose

Perform this procedure to display auxiliary database information in a CLI window on a main server station or on an auxiliary database station.

7.8.2 Steps

1

To display the status on a main server station:

1. Log in to a main server station as the samadmin user.
2. Open a console window.
3. Enter the following:

```
bash$ /opt/5620sam/server/nms/bin/nmsserver.bash -s
nms_status ↵
```

The command generates output that includes the following:

```
-- Auxiliary Database Information
   -- Auxiliary Database Enabled: Yes
-- Auxiliary Database Servers Information
   -- Auxiliary Database Server: 198.51.100.1
      Auxiliary Database Server Status: Up
      Auxiliary Database Server Connectivity Status:
ONLINE
   -- Auxiliary Database Server: 198.51.100.2
      Auxiliary Database Server Status: Up
      Auxiliary Database Server Connectivity Status:
ONLINE
   -- Auxiliary Database Server: 198.51.100.3
      Auxiliary Database Server Status: Up
      Auxiliary Database Server Connectivity Status:
ONLINE
```

4. View the Auxiliary Database Server Status and Database Connectivity Status of each station in the cluster. If each is not Up and ONLINE, contact technical support for assistance.

2

To display the status on an auxiliary database station:

1. Log on to an auxiliary database station as the root user.
2. Open a console window.
3. Enter the following:

```
# /opt/5620sam/samauxdb/bin/auxdbAdmin.sh describe ↵
```

The command generates output similar to the following:

```
Copyright (c) 2000-20XX Noka. All rights reserved
Database status
DB      | Host          | State
-----+-----+-----
samdb  | 10.1.2.70    | UP
samdb  | 10.1.2.71    | UP
samdb  | 10.1.2.72    | UP
Database description:
Database: samdb
Database Log:
/opt/5620sam/auxdb/catalog/samdb/dbLog, /opt/5620sam/auxdb/catalog/samdb
Hosts: 10.1.2.70,10.1.2.71,10.1.2.72
Restart Policy: ksafe
Port: 5433
Catalog Directory:
/opt/5620sam/auxdb/catalog/samdb/v_samdb_node0001_catalog
Hosts in cluster:
10.1.2.70,10.1.2.71,10.1.2.72
```

4. View the database status. If the status of each station in the cluster is not UP, contact technical support for assistance.

3

Close the console window.

END OF STEPS

7.9 To configure the allowed number of Oracle database login attempts

7.9.1 Purpose

As a security precaution, you can configure the allowed number of Oracle database user login attempts before the user account is locked because of failed attempts. See [7.20 “To unlock the Oracle database user account” \(p. 230\)](#) for information about how to reset the Oracle database user account.



Note: In a redundant deployment, you must perform this procedure on the primary database station. After you perform the procedure, the primary database automatically copies the configuration change to the standby database.

The configuration changes that you make in this procedure are not affected by subsequent database upgrades.

7.9.2 Steps

1 _____

Log in to the 5620 SAM database station as the Oracle management user.

2 _____

Open a console window.

3 _____

Enter the following:

```
bash$ path/install/config/samdb/SAMDb_security.sh ↵
```

where *path* is the 5620 SAM database installation location, typically /opt/5620sam/samdb

The following prompt is displayed:

```
Enter the password for the "sys" user (terminal echo is off):
```

4 _____

Enter the Oracle SYS user password and press ↵.

The following prompt is displayed:

```
Accept value? [y/n/q] (y):
```

5 _____

Perform one of the following.

a. Press ↵ to confirm that the supplied password is correct.

The following prompt is displayed:

```
Please select one of the following options:
```

- 1) Setting failed login attempts
- 2) Unlock database user
- 0) Exit

```
Please enter(1,2 or 0):
```

b. Press n ↵ if you have incorrectly entered the password; return to [Step 4](#) .

6

To specify the allowed number of login failures, perform the following steps.

1. Enter 1 ↵.

The following prompt is displayed:

```
Please select one of the following options:  
  1) Setting the number of failed login attempts  
  2) Remove the number of failed login attempts setting  
(no checking)  
  0) Exit  
Please enter(1,2 or 0):
```

2. Enter 1 ↵.

The following prompt is displayed:

```
This value will be use for setting the number of failed  
login attempts before locking the database user account.  
Please enter value for number of failed login attempts(20  
to 1000) (30):
```

3. Perform one of the following.
 - Accept the default of 30. Press ↵.
 - Specify a value between 20 and 1000, and then press ↵.

The following messages are displayed:

```
About to change the Oracle database user settings  
Completed changing the Oracle database user settings
```

4. Go to [Step 8](#) .

7

To remove the allowed number of failed login attempts, enter 2 ↵.

The following messages are displayed, and the 5620 SAM no longer locks the Oracle database user account after multiple login failures.

```
About to change the Oracle database user settings  
Completed changing the Oracle database user settings
```


8 _____

Close the console window.

END OF STEPS _____

7.10 To configure Oracle database error monitoring

7.10.1 Purpose

You can configure how the 5620 SAM handles Oracle database errors to provide monitoring information that may help with troubleshooting or the detection of security violations such as SQL injection attacks. When database error monitoring is enabled, the 5620 SAM raises an alarm when the Oracle software reports an error, for example, an invalid SQL statement.

7.10.2 Steps

1 _____

Choose Administration→Database from the 5620 SAM main menu. The Database Manager (Edit) form opens.

2 _____

To enable database error monitoring, select the Enable Database Error Monitoring parameter.

3 _____

To disable database error monitoring, deselect the Enable Database Error Monitoring parameter.

4 _____

Save your changes and close the form.

END OF STEPS _____

7.11 To configure a size constraint policy

7.11.1 Purpose

Size constraint policies regulate the number of historical records that the 5620 SAM database retains before they are purged. The scheduling of tasks through the 5620 SAM can generate a large volume of archived result information if left unchecked. Size constraint policies control the volume of information stored by defining thresholds for various record classes. When the number of records for a specific class or group of

classes reaches a threshold specified in the policy, the 5620 SAM deletes a specified number of the oldest objects that are associated with the class or group of classes.

7.11.2 Steps

- 1 _____
Choose Administration→Constraint Policies→Size Constraint Policies from the 5620 SAM main menu. The Size Constraint Policies form opens.
- 2 _____
Click Create or choose a policy and click Properties. The Size Constraint Policy (Create | Edit) form opens.

i **Note:** The 5620 SAM is preconfigured with the following default size constraint policies for various record classes:
 - Script Management Results
 - Clear Requests
 - CPAM Protocol Data
 - Work Order Import Logs
 - LTE User Stats Query Output Snapshots
- 3 _____
Configure the general policy parameters.
- 4 _____
Click on the Constrained Packages tab.
- 5 _____
Right-click on the Size Constraint Policy icon and choose Select Packages.
- 6 _____
Choose a size constraint package and click OK. The package appears in the navigation tree under the Size Constraint policy. Go to [Step 7](#) if the package selected supports a sub-class package, for example, the dhcp package supports three sub-class packages. Otherwise, go to [Step 9](#) .
- 7 _____
Right-click on the package icon and choose Select Classes. The Select Size Constrained Classes form opens.
- 8 _____
Choose a sub-class package and click OK to Save your changes and close the form.

 9

Close the Size Constraint Policy (Create|Edit) form.

 END OF STEPS

7.12 To configure an ageout constraint policy

7.12.1 Purpose

An ageout constraint policy defines the database ageout period for a specific object type. When the age of an object reaches the ageout value, the 5620 SAM deletes the object from the database.

The 5620 SAM supports ageout constraint policies to define the period of time the database retains persisted virtual network objects. These policies are the dctr policies listed below. See the *VSAP User Guide* for more information about virtual network object persistence in data center networks.

The 5620 SAM has the following preconfigured ageout constraint policies:

- ressubscr.ResidentialSubscriberInstance—residential subscriber instance Residential subscriber instances on an NE become inactive when the subscriber is deleted from the NE. The accumulation of inactive residential subscriber instances can be particularly rapid during operations such as Wi-Fi offload.
- aapolicy.DbInfoTransitSubscriber—AA transit subscriber
- dynsvc.DynSvcActivityEntry—dynamic service activity logs
- dctr.GatewayVirtualPort
- dctr.VirtualMachine
- dctr.VirtualPort
- dctr.VirtualSwitch
- dctr.VplsVirtualSite
- dctr.VprnVirtualSite
- dctr.VrsGVirtualSwitch
- dctr.VrgVirtualSwitch

7.12.2 Steps

 1

Choose Administration→Constraint Policies→Ageout Constraint Policies from the 5620 SAM main menu. The Ageout Constraint Policies form opens.

 2

Select a policy and click Properties. The Ageout Constraint Policy form opens.

3

Review the Object Count information in the Status panel. The information refers to the most recent object deletion, and can help you define the appropriate ageout time and deletion interval values for the policy.

4

Configure the parameters.

 **Note:** The default Qualified Ageout Time for non-DC object types is:

- 24 hours, if the 5670 RAM is not enabled
- 1464 hours, if the 5670 RAM is enabled

The default value does not change when the 5670 RAM is enabled using a different method, in which case the value must be changed manually to enable optimum 5620 SAM and 5670 RAM interoperation.

The Qualified Ageout Time defaults are guidelines. Consider the following when setting the Qualified Ageout Time:

- A small value can prevent excessive database table growth.
- The value must be great enough to allow sufficient time to upload the database records to a third-party application.

5

Save your changes and close the form.

6

CAUTION


Service Disruption

Contact technical support before you attempt to modify a 5620 SAM configuration file.

Modifying a 5620 SAM configuration file can have serious consequences that may include service disruption.

If required, edit the ageout constraint policy configuration file to modify the following parameters in the Deletion Interval panel:

- Synchronization Time—shown as ageoutSyncTime in the configuration file
- Interval (hours)—shown as ageoutInterval in the configuration file

 **Note:** If the 5620 SAM is deployed in a redundant configuration, you must perform the following steps on each main server in the deployment.

1. Log in to the main server station as the samadmin user.
2. Open a console window.
3. Navigate to the /opt/5620sam/server/nms/config directory.

4. Open the AgeoutConstraint.xml file using a plain-text editor.

5. Locate the following tag shown in the following code:

```
<ageout>
```

6. Locate the object class section that you need to modify; the following code shows the residential subscriber instance object class as an example.

Deletion interval parameters

```
<ageout>
  <class name="ressubscr.ResidentialSubscriberInstance"
    ageoutSyncTime="00:00"
    ageoutInterval="1">
  </class>
</ageout>
```

7. Modify the ageoutSyncTime and ageoutInterval values, as required.

8. Save and close the AgeoutConstraint.xml file.

9. Navigate to the /opt/5620sam/server/nms/bin directory.

10. Enter one of the following, depending on the main server you are configuring:

- On a standalone main server, or the primary main server in a redundant deployment:

```
bash$ ./nmsserver.bash read_config ↵
```

- On the standby main server in a redundant deployment:

```
bash$ ./nmsserver.bash force_restart ↵
```

The 5620 SAM puts the configuration change into effect.

11. Log out of the main server station.

END OF STEPS

7.13 To create a database file policy to manage database log or core dump files

7.13.1 Purpose

You can create database file policies to manage the file size and number of archives for stored alert, listener, trace, audit, and core dump files. When the size and number of files are left unbounded, excessive database disk capacity is consumed.

Database trace, alert, and audit log files are compressed and stored in the alert log directory. Database listener log files are stored in the listener log directory.



Note: For historical or troubleshooting purposes, recommends that you archive the 5620 SAM database log files on a regular basis.

7.13.2 Steps

- 1 _____
Choose Administration→Database from the 5620 SAM main menu. The Database Manager (Edit) form opens.
- 2 _____
Click on the File Policies tab.
- 3 _____
Click Database File Policies or choose a default policy and click Properties. The Database File Policies Create | Edit) form opens. If you selected a default policy, go to [Step 5](#) .
- 4 _____
Click Create.
- 5 _____
Configure the required general file policy parameters and Purge Details panel parameters.
- 6 _____
Click OK to save your changes and close the form.
- 7 _____
If required, click Select to apply the new purge details to a default policy.
- 8 _____
Save your changes and close the Database Manager (Edit) form.

END OF STEPS _____

7.14 To configure the statistics data retention period for the 5620 SAM database

7.14.1 Steps

- 1 _____
Choose Administration→Database from the 5620 SAM main menu. The Database Manager (Edit) form opens.

2

**CAUTION****Service Disruption**

Configuring the parameter can affect 5620 SAM system performance.

Consult technical support before you configure the parameter.

Configure the Accounting Statistic Data Retention Period (Days) parameter.

3

Save your changes and close the Database Manager (Edit) form.

END OF STEPS

7.15 To perform an immediate 5620 SAM database backup using the GUI

7.15.1 Purpose

Perform this procedure to initiate an on-demand 5620 SAM database backup using the client GUI. You can perform a full backup, which includes the entire database, or a partial backup, which excludes accounting statistics data.

**CAUTION****Service Disruption**

The disk partition that is to contain the database backup must have sufficient space for the database backup file set, or system performance may be compromised.

Ensure that the backup directory is at least five times as large as the expected database backup size. For more information, contact technical support or see the 5620 SAM Planning Guide.



Note: The 5620 SAM backs up the Oracle encryption wallet during a database backup, and restores the wallet during a database restore. In a redundant deployment, the 5620 SAM automatically replicates the encryption wallet from the primary to the standby database after the standby database reinstantiation.



Note: During a database backup, the performance of GUI or OSS operations may be affected. It is recommended that you perform a database backup only during a period of low 5620 SAM activity.

7.15.2 Steps

1 _____
Choose Administration→Database from the 5620 SAM main menu. The Database Manager form opens.

2 _____
Click on the Backup tab.

3 _____



CAUTION

Data Loss

Before the 5620 SAM performs a database backup, it deletes the contents of the specified backup directory.

Ensure that the backup directory that you specify in this step does not contain files that you need to retain.



CAUTION

Data Loss

The Manual Backup Directory value must not include the 5620 SAM database installation directory, or data loss may occur.

Ensure that the directory path does not include /opt/5620sam/samdb.

Configure the following parameters:

i **Note:** The Oracle management user requires read and write permissions on the backup directory that you specify.

- Manual Backup Directory
- Enable Backup File Compression

4 _____
Perform one of the following.

- a. Click Partial Backup.
- b. Click Full Backup.

5 _____
Click Yes. The full or partial backup operation begins, and the Backup State indicator reads In Progress.

Depending on the database size, a backup may require several hours to complete.

6

If required, monitor the Backup Status information, which includes the following:

- Scheduled Backup—whether scheduled backup is configured
- Backup State—state of current backup operation; dynamically updated
- Next Scheduled Backup Time—time of next scheduled backup
- Last Successful Backup Time—completion time of latest successful backup
- Last Successful Backup Type—type of latest successful backup
- Last Attempted Backup Time—when latest attempted backup began
- Last Attempted Backup Type—type of latest attempted backup
- Directory of the Last Successful Backup—location of latest successful backup
- Host Name of the Last Successful Backup—hostname of station that performed latest successful backup

7

Close the Database Manager (Edit) form.

END OF STEPS

7.16 To perform an immediate 5620 SAM database backup using a CLI



CAUTION

Service Disruption

The disk partition that is to contain the database backup must have sufficient space for the database backup file set, or system performance may be compromised.

Ensure that the backup directory is at least five times as large as the expected database backup size. For more information, contact technical support or see the 5620 SAM Planning Guide.



Note: You can perform only a full backup using a CLI script. To perform a partial backup, see [7.15 “To perform an immediate 5620 SAM database backup using the GUI” \(p. 223\)](#).



Note: The 5620 SAM backs up the Oracle encryption wallet during a database backup, and restores the wallet during a database restore. In a redundant deployment, the 5620 SAM automatically replicates the encryption wallet from the primary to the standby database after the standby database reinstatement.



Note: During a database backup, the performance of GUI or OSS operations may be affected. It is recommended that you perform a database backup only during a period of low 5620 SAM activity.

7.16.1 Steps

1 _____
Log in as the Oracle management user on the database station.



Note: In a redundant 5620 SAM system, you must log in to the primary database station.

2 _____
Open a console window.

3 _____



CAUTION

Data Loss

Before the 5620 SAM performs a database backup, it deletes the contents of the specified backup directory.

Ensure that the backup directory that you specify in this step does not contain files that you need to retain.



CAUTION

Data Loss

The 5620 SAM database backup directory path must not include the 5620 SAM database installation directory, or data loss may occur.

Ensure that the directory path does not include /opt/5620sam/samdb.

Enter the following to begin the database backup:



Note: The Oracle management user requires read and write permissions on the backup directory that you specify.

```
bash$ /opt/5620sam/samdb/install/config/samdb/SAMbackup.sh  
backup_directory ↵
```

where *backup_directory* is the directory that is to contain the database backup file set

Depending on the database size, a backup may require several hours to complete.

4 _____

When the backup is complete, close the console window.

END OF STEPS _____

7.17 To back up an auxiliary database

7.17.1 Steps

1 _____

Choose Administration→Database from the 5620 SAM main menu. The Database Manager form opens.

2 _____

Click on the Auxiliary Database Backups tab.

3 _____



CAUTION

Service Disruption

Consider the directory path when you configure the Backup Location parameter.

You must specify the absolute path of a directory in a partition other than the partition that contains the database data.

Configure the Backup Location parameter.

4 _____

Click Backup All Databases. A confirmation form opens.

5 _____

Click OK. The backup process begins, and the Latest Backup State indicator displays In Progress; the backup is complete when the indicator displays Success.

6

When the backup is complete, close the Database Manager form.

END OF STEPS

7.18 To schedule 5620 SAM database backups



CAUTION

Service Disruption

The disk partition that is to contain the database backup must have sufficient space for the database backup file set, or system performance may be compromised.

Ensure that the backup directory is at least five times as large as the expected database backup size. For more information, contact technical support or see the 5620 SAM Planning Guide.



CAUTION

Service Disruption

A 5620 SAM database backup consumes considerable system resources.

Ensure that you specify a backup schedule of reasonable frequency. for example, daily.



Note: The 5620 SAM backs up the Oracle encryption wallet during a database backup, and restores the wallet during a database restore. In a redundant deployment, the 5620 SAM automatically replicates the encryption wallet from the primary to the standby database after the standby database reinstatement.



Note: During a database backup, the performance of GUI or OSS operations may be affected. It is recommended that you schedule the database backup to occur during a period of low 5620 SAM activity.

7.18.1 Steps

1


Choose Administration→Database from the 5620 SAM menu. The Database Manager form (Edit) opens.

2

Click on the Backup tab.

3

Configure the required parameters in the Backup Schedule panel.

 **Note:** You must select the Schedule Enabled parameter.

4




CAUTION


Data Loss

Before the 5620 SAM performs a database backup, it deletes the contents of the specified backup directory.

Ensure that the backup directory that you specify in this step does not contain files that you need to retain.

Configure the Scheduled Backup Directory parameter in the Backup Setting panel. The value that you specify is the database station directory in which to save the backup file sets. Each file set is stored in a subdirectory named backupset n , where n is a sequential number; the highest possible value is the Number to Keep parameter value.

 **Note:** The Oracle management user requires read and write permissions on the Scheduled Backup Directory.

 **Note:** The Scheduled Backup Directory must be a directory on the local file system.

5

Close the Database Manager form.

6

After each scheduled database backup completes, move the database backup file set to another station for safekeeping.

END OF STEPS

7.19 To schedule auxiliary database backups

7.19.1 Steps

1

Choose Administration→Database from the 5620 SAM menu. The Database Manager form (Edit) opens.

2

Click on the Auxiliary Database Backups tab.

3 _____
Select the Run Scheduled Backups parameter.

4 _____



CAUTION

Service Disruption

Consider the directory path when you configure the Backup Location parameter.

You must specify the absolute path of a directory in a partition other than the partition that contains the database data.

Configure the remaining parameters.

5 _____

Click OK to save your changes and close the form.

END OF STEPS _____

7.20 To unlock the Oracle database user account

7.20.1 Purpose

Perform this procedure to unlock the Oracle database user account after the user account is locked out because of multiple login failures. See [7.9 “To configure the allowed number of Oracle database login attempts” \(p. 214\)](#) for information about how to configure the allowed number of Oracle database user login attempts.

7.20.2 Steps

1 _____
Log in to the 5620 SAM database station as the Oracle management user.

2 _____
Open a console window.

3 _____
Enter the following:

```
bash$ /opt/5620sam/samdb/install/config/samdb/SAMDb_
security.sh ↵
```

The following prompt is displayed:

Enter the password for the "sys" user (terminal echo is off):

4 _____

Enter the Oracle SYS user password and press ↵.

The following prompt is displayed:

```
Accept value? [y/n/q] (y):
```

5 _____

Perform one of the following.

a. Press ↵ to confirm that the supplied password is correct.

The following prompt is displayed:

```
Please select one of the following options:
```

```
 1) Setting failed login attempts
```

```
 2) Unlock database user
```

```
 0) Exit
```

```
Please enter(1,2 or 0):
```

b. Press n ↵ if you have incorrectly entered the password; return to [Step 4](#) .

6 _____

Enter 2 ↵.

The following messages are displayed, and the Oracle database user account is unlocked.

```
About to unlock the database user username
```

```
Completed unlocking the database user username
```

where *username* is the Oracle database username

7 _____

Close the console window.

END OF STEPS _____

8 5620 SAM system redundancy

8.1 Overview

8.1.1 Purpose

This chapter describes the workflow to set up system redundancy.

8.1.2 Contents

5620 SAM system redundancy	234
8.2 Overview	234
8.3 5620 SAM system redundancy models	234
8.4 Redundancy functions	240
8.5 Redundancy failure scenarios	247
5620 SAM system redundancy procedures	253
8.6 Workflow to perform 5620 SAM system redundancy functions	253
8.7 To view the 5620 SAM system redundancy status	254
8.8 To view the 5620 SAM auxiliary server status	257
8.9 To perform a server activity switch	259
8.10 To configure 5620 SAM database switchover behavior	260
8.11 To perform a 5620 SAM database switchover using the 5620 SAM client GUI	261
8.12 To perform a 5620 SAM database switchover using a CLI script	262
8.13 To restore analytics server operation after a 5620 SAM database failover or switchover	263
8.14 To enable or disable automatic database realignment	265
8.15 To reinstantiate a redundant database using the 5620 SAM client GUI	268
8.16 To reinstantiate a redundant database using a CLI script	269
8.17 To configure an IPDR file transfer policy	270

5620 SAM system redundancy

8.2 Overview

8.2.1 Redundancy functions

5620 SAM system redundancy is initially configured during 5620 SAM installation. You use the 5620 SAM GUI, or scripts on a 5620 SAM main server, to perform the following redundancy functions:

- Check the 5620 SAM redundant server and database status.
- Perform a manual activity switch from the primary to the standby main server.
- Enable or disable automatic database realignment.
- Reinstantiate the former primary database as the standby database when an automatic or manual activity switch occurs and verify its status.

You can configure the following redundancy parameters to specify how a 5620 SAM system manages a loss of connection to the managed NEs; contact technical support for more information:

- the number of elapsed seconds that constitute a loss of connectivity
- how often a main server refreshes the list of managed NEs
- the minimum number of NEs that must respond to a connectivity check

8.3 5620 SAM system redundancy models

8.3.1 Overview



CAUTION

Service Disruption

It is recommended that you deploy the primary server and database in the same geographical location and LAN.

This results in increased 5620 SAM system performance and fault tolerance.

You can deploy a 5620 SAM system in a redundant configuration to provide greater fault tolerance by ensuring that there is no single point of software failure in the 5620 SAM management network. A redundant 5620 SAM deployment consists of the following components:

- primary and standby 5620 SAM main servers
- primary and standby 5620 SAM databases

The current state of a component defines the primary or standby role of the component. The primary main server actively manages the network and the primary database is

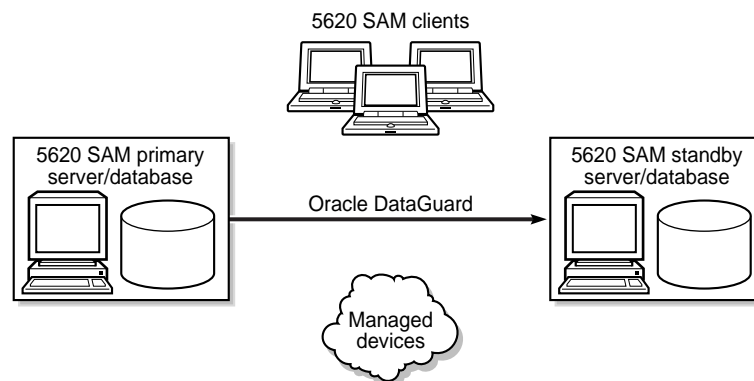
open in read/write mode. When a standby component detects a primary component failure, it automatically changes roles from standby to primary. You can also change the role of a component using the 5620 SAM client GUI or a CLI script.

The 5620 SAM supports collocated and distributed system redundancy. A collocated system requires two stations that each host a main server and database. A distributed system requires four stations that each host a main server or database. Each main server and database is logically independent, regardless of the deployment type.

The primary and standby main servers communicate with the redundant databases and periodically verify server redundancy. If the standby server fails to reach the primary server within 60s, the standby server becomes a primary server. See [8.5 “Redundancy failure scenarios” \(p. 247\)](#) for information about various 5620 SAM redundancy failure scenarios.

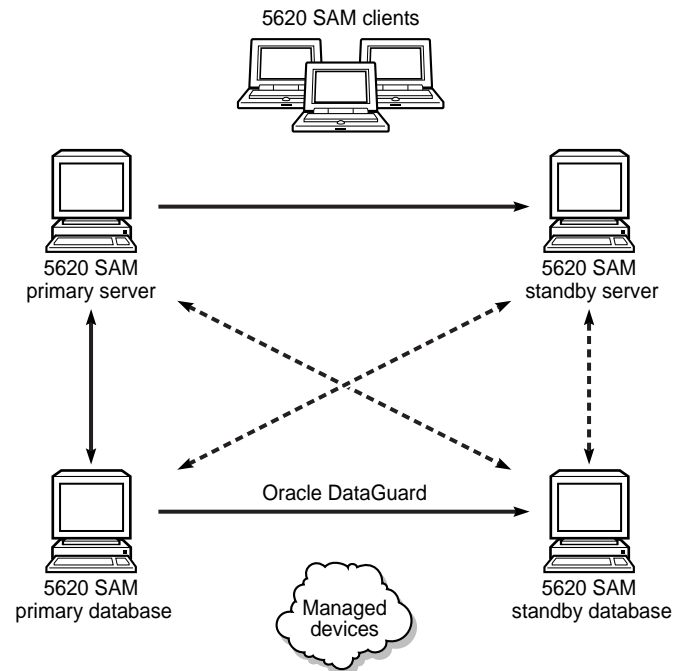
A 5620 SAM database uses the Oracle DataGuard function to maintain redundancy. During a redundant 5620 SAM installation or upgrade, the Oracle DataGuard synchronization level is set to real-time apply, which ensures that the primary and standby databases are synchronized.

Figure 8 Collocated redundant 5620 SAM deployment



17896

Figure 9 Distributed redundant 5620 SAM deployment



17897

A main server role change is called a server activity switch. An automatic database role change is called a failover; a manual database role change is called a switchover.



Note: After a database failover or switchover in a 5620 SAM system that includes a 5620 SAM analytics server, you must reconfigure the analytics server to communicate with the new primary database, as described in [8.13 “To restore analytics server operation after a 5620 SAM database failover or switchover”](#) (p. 263).

A typical redundant 5620 SAM deployment has a primary server and database in a geographically separate facility from the standby server and database facility. To ensure that the primary components are in the same LAN after an activity switch or failover, you can configure automatic database realignment during a main server installation or upgrade. See [8.4.6 “Automatic database realignment”](#) (p. 244) for more information.

The 5620 SAM GUI clients always communicate with the current primary server. After a server activity switch, the GUI clients automatically connect to the new primary server, which is the former standby server. The 5620 SAM OSS clients also communicate with the current primary server, but after a server activity switch, the OSS clients do not automatically connect to the new primary server.

The following general conditions apply to 5620 SAM system redundancy:

- The main servers and databases must each be redundant. For example, you cannot have redundant servers and a standalone database.
- The network that contains a redundant 5620 SAM system must meet the latency and bandwidth requirements described in the *5620 SAM Planning Guide*.

Note:

To provide hardware fault tolerance in addition to software redundancy, it is recommended that you use redundant physical links between the primary and standby servers and databases to ensure there is no single point of network or hardware failure.

- The server and database stations require the same OS version and patch level.
- The server stations require identical disk layouts and partitioning.
- The database stations require identical disk layouts and partitioning.
- The following users can perform manual server activity switches or database switchovers:
 - the samadmin user on a main server station
 - a client GUI user with update or execute permissions on the following classes:
 - db.DatabaseManager.switchover
 - db.DatabaseManager.reinstantiateStandby
 - a GUI client user with the admin scope of command role

8.3.2 Auxiliary server redundancy

5620 SAM auxiliary servers are optional servers that extend the network management processing engine by distributing server functions among multiple stations. A 5620 SAM main server controls task scheduling and sends task requests to auxiliary servers. Each auxiliary server is installed on a separate station, and responds to processing requests only from the current primary main server in a redundant system.

When an auxiliary server cannot connect to the primary main server or database, it re-initializes and continues trying to connect until it succeeds or, in the case of a database failover, until the main server directs it to the peer database.

After startup, an auxiliary server waits for initialization information from a main server. An auxiliary server restarts if it does not receive all required initialization information within five minutes.



Note: 5620 SAM system performance may degrade when a main server loses contact with a number of auxiliary servers that exceeds the number of Preferred auxiliary servers in the server cluster.

When an auxiliary server fails to respond to a primary main server, the main server tries repeatedly to establish communication before it generates an alarm. The alarm clears when the communication is re-established.

Auxiliary server types

The auxiliary servers in a 5620 SAM system are specified in each main server configuration, which includes the address of each auxiliary server in the system, and the auxiliary server type, which is one of the following:

- Preferred—processes requests under normal conditions
- Reserved—processes requests when a Preferred auxiliary server is unavailable
- Remote Standby—unused by the main server; processes requests only from the peer main server, and only when the peer main server is operating as the primary main server

If a Preferred auxiliary server is unresponsive, the main server directs the requests to another Preferred auxiliary server, if available, or to a Reserved auxiliary server. When the unresponsive Preferred auxiliary server returns to service, the main server reverts to the Preferred auxiliary server and stops sending requests to any Reserved auxiliary server that had assumed the Preferred workload.

An auxiliary server that is specified as a Remote Standby auxiliary server is a Preferred or Reserved auxiliary server of the peer main server. The Remote Standby designation of an auxiliary server in a main server configuration ensures that the main server does not use the auxiliary server under any circumstances. Such a configuration may be required when the network latency between the primary and standby server clusters is high, for example, when the 5620 SAM system is geographically dispersed.

Alternatively, if all main and auxiliary servers are in the same physical facility and the network latency between components is not a concern, no Remote Standby designation is required, and you can apply the Preferred and Reserved designations based on your requirements. For example, you may choose to configure a Preferred auxiliary server of one main server as the Reserved auxiliary server of the peer main server, and a Reserved auxiliary server as the Preferred of the peer main server.

8.3.3 IPDR file transfer redundancy

The 5620 SAM can forward AA accounting and AA Cflowd statistics in IPDR format to redundant destinations for retrieval by OSS applications. Additionally, you can use multiple Cflowd auxiliary servers to collect AA Cflowd statistics from NEs and forward the data to the redundant targets. Such a configuration provides a high degree of fault tolerance in the event of a 5620 SAM component failure.

AA accounting statistics collection

The 5620 SAM sends the collected AA accounting statistics files to the target servers specified in an IPDR file transfer policy. An IPDR file transfer policy also specifies the file transfer type and user credentials, and the destination directory on the server. See [8.17 “To configure an IPDR file transfer policy” \(p. 270\)](#) for IPDR file transfer policy configuration information.

Each file is transferred as it is closed. A file that cannot be transferred is retained by the server, which logs an error. A file that cannot be created or is corrupted is stored in a directory named “bad” below the specified destination directory on the server.

After you configure the IPDR file transfer policy, the main or auxiliary server that collects AA accounting statistics forwards the statistics files to the primary transfer target named in the policy. If the server is unable to perform a file transfer, for example, because of an unreachable target, invalid user credentials, or a disk-capacity issue, the main or auxiliary server attempts to transfer the files to the alternate target, if one is specified in the policy.

AA Cflowd statistics collection

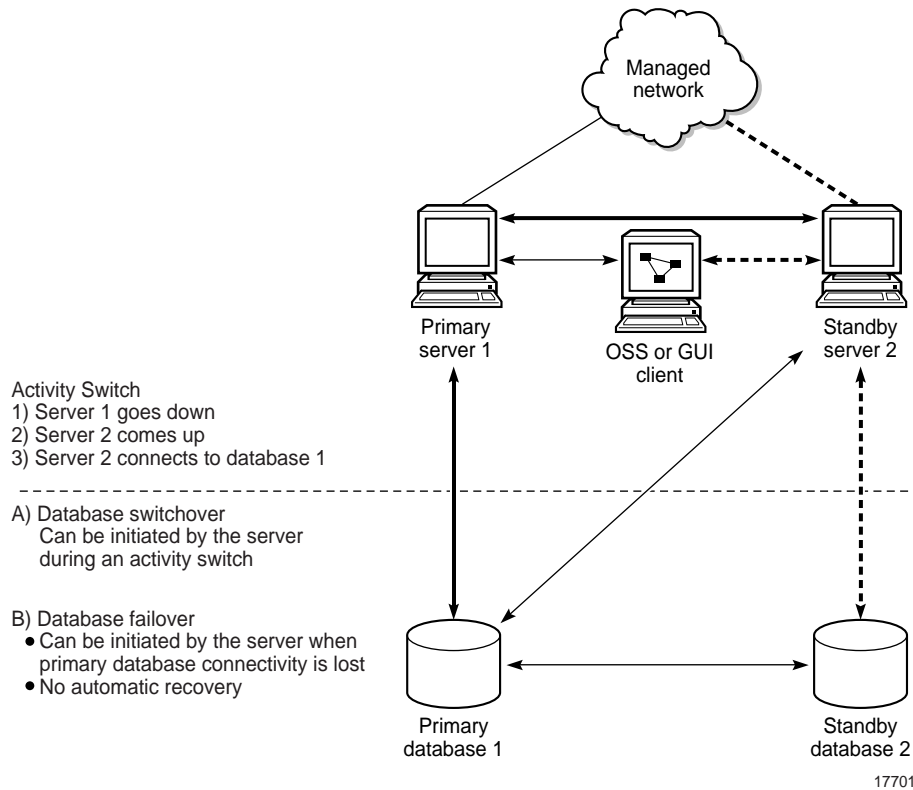
If a 5620 SAM system includes Cflowd auxiliary servers, each server transfers the AA Cflowd statistics files to the targets configured in the server web UI. When two targets are configured, an OSS can retrieve the files from either target. If the OSS finds that files are absent from a target, or the target is unreachable, the OSS can retrieve the files from the other target. See the “Flow statistics collection” chapter of the *5620 SAM Statistics Management Guide* for configuration information.

To ensure minimal data loss in the event of a Cflowd auxiliary server or file-transfer target failure, you can deploy two Cflowd auxiliary servers to retrieve the AA Cflowd statistics from one group of NEs. To facilitate the configuration of redundant Cflowd auxiliary servers, you can copy the collection configuration of one Cflowd auxiliary server to another, as described in the “Flow statistics collection” chapter of the *5620 SAM Statistics Management Guide*.

8.4 Redundancy functions

8.4.1 Overview

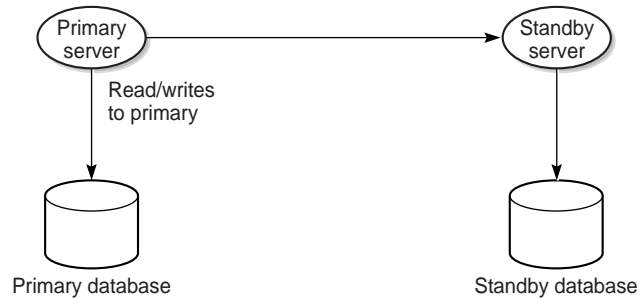
Figure 10 5620 SAM redundancy role-change functions



8.4.2 Server activity switches

The standby server initiates an automatic server activity switch when it cannot communicate with the primary server. A 5620 SAM administrator performs a manual server activity switch, which is typically a planned server maintenance or test operation. For security reasons, you cannot use a 5620 SAM GUI or OSS client to perform a server activity switch.

Figure 11 Server and database roles before server activity switch



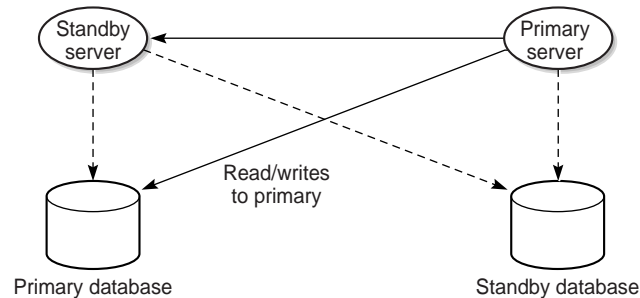
17840

During a server activity switch, a main server does not process SNMP traps, attempt to synchronize NEs, or collect statistics. Auxiliary servers process outstanding requests during an activity switch, but do not communicate with a main server.

The following occurs during a server activity switch:

- The primary server raises alarms about the event.
- Each GUI client receives notification of the activity switch and displays a message about the server unavailability during the activity switch.

Figure 12 Server and database roles after server activity switch



17893

The following occur after a server activity switch:

- If automatic database realignment is enabled, the new primary server performs a database switchover.
- The GUI clients communicate with the new primary server and display the current redundancy status.
- The OSS clients must connect to the new primary server.
- The new primary server establishes communication and synchronizes information with the 5620 SAM auxiliary servers.
- The auxiliary servers exchange information with the new primary server; no auxiliary servers exchange information with the former primary server.

- The Preferred or Reserved state of each auxiliary server changes, depending on the configuration of the new primary server.
- The new primary server attempts to redeploy the client requests that the former primary server did not complete before the activity switch.

8.4.3 Database switchovers

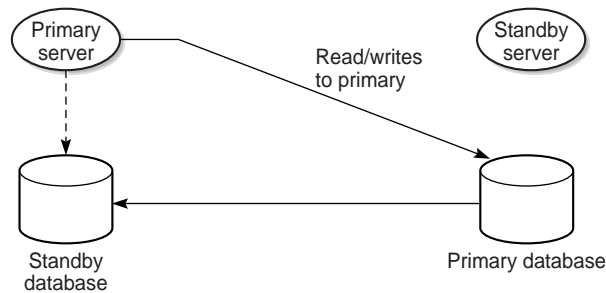
A 5620 SAM administrator directs a main server to initiate a database switchover.

Figure 13 Server and database roles before database switchover



17826

Figure 14 Server and database roles after database switchover



17891

The following occurs after a successful database switchover:

- The primary server connects to the new primary database.
- Archive logging begins on the new primary database.
- The primary server directs each auxiliary server to use the new primary database.

When a database switchover fails, the primary and standby database roles do not change. No automatic database realignment occurs as a result of a switchover.

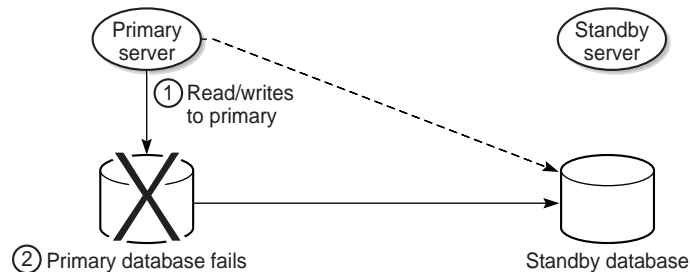
8.4.4 Database failovers

The 5620 SAM database failover function is enabled by default. A failover occurs when a main server cannot communicate with the primary database, but can communicate with the standby database and the managed NEs. When this happens, the main server directs the standby database to become the primary database.

A database failover occurs only if the following conditions are true.

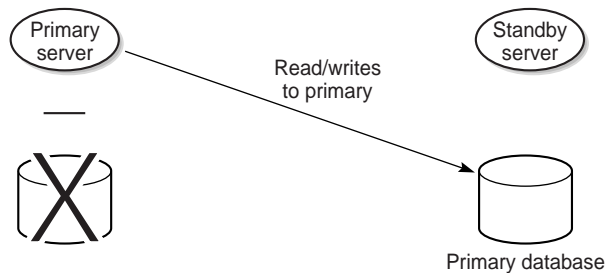
- The standby database is configured, operational, and reachable.
- The main server can communicate with the managed NEs.

Figure 15 Server and database roles before database failover



17827

Figure 16 Server and database roles after database failover



17890

When a database failover fails, the primary server tries again to communicate with the primary database. If the primary database remains unavailable, the primary server tries again to initiate a failover.

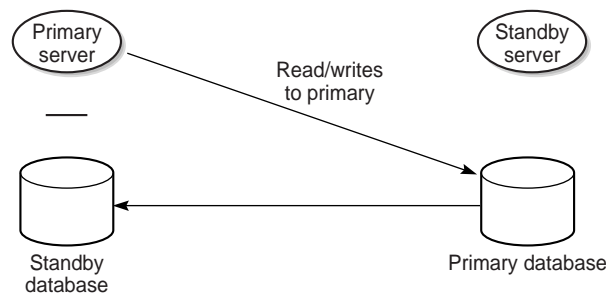


Note: After a successful failover, database redundancy is not available. See [8.4.5 “Re-establishing database redundancy” \(p. 244\)](#) in this section.

8.4.5 Re-establishing database redundancy

After a failover, the former primary database is no longer part of the redundant configuration. To re-establish database redundancy, you must re-instantiate the former primary database as the new standby database. You can do this only when the failed database station is restored to full operation and has a functional proxy port. See [8.15 “To re-instantiate a redundant database using the 5620 SAM client GUI” \(p. 268\)](#) and [8.16 “To re-instantiate a redundant database using a CLI script” \(p. 269\)](#) for information about how to re-instantiate a database.

Figure 17 Server and database roles after database re-instantiation



18562

Automatic database re-instantiation

You can configure the 5620 SAM to automatically re-instantiate the former primary database as the new standby database. Automatic database re-instantiation occurs only in the event of a database failover. When the function is enabled, the 5620 SAM attempts an automatic re-instantiation every 60 minutes by default. You can enable automatic database re-instantiation during a 5620 SAM main server installation or upgrade. See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for information about enabling and configuring automatic database re-instantiation.

8.4.6 Automatic database realignment

In a redundant 5620 SAM system that is geographically dispersed, the primary server and database may be in separate LANs or WANs after an activity switch or failover. The network latency that this introduces can affect 5620 SAM system performance. Automatic database realignment is an optional mechanism that attempts to ensure that each main server uses the local database.

The database with which a main server tries to align itself is called the preferred database of the main server. An operator enables automatic database realignment and specifies the preferred database during 5620 SAM server installation, or during server configuration after installation.



Note: For automatic database alignment to work, you must enable it and specify a preferred database on each main server in a redundant 5620 SAM system.

When a primary server starts, it verifies that the primary database is the preferred database. If the primary database is not the preferred database, the server performs a database switchover to reverse the primary and standby database roles. If the switchover is successful, the main servers and databases in the 5620 SAM system are aligned. If the switchover fails, each database reverts to the former role, and the main server generates an alarm about the failed switchover.

When you perform a database switchover and automatic database realignment is enabled, the primary server does not attempt database realignment. A switchover is a manual operation that is considered to be a purposeful act.

Performing a server activity switch when automatic database realignment is enabled triggers a database switchover.

8.4.7 Redundancy function summary

Table 11 5620 SAM server redundancy functions

Function	Notes
<p>Automatic server activity switch</p> <p>An automatic activity switch occurs when the primary server cannot communicate with the standby server, and involves the following sequence of events.</p> <ul style="list-style-type: none"> • The standby server cannot communicate with the primary server within 60 seconds, or the primary server cannot communicate with the managed network. • The standby server performs an activity switch to become the new primary server. The activity switch occurs only if the standby server can communicate with the managed network. • If automatic database realignment is enabled, the new primary server attempts a database switchover. • The new primary server connects to the primary database and manages the network. • The new primary server and the auxiliary servers synchronize the outstanding request information. 	<p>When the primary server detects a standby server communication failure, each GUI client receives notification of the failure.</p> <p>During an activity switch, each client GUI displays a main server status message.</p> <p>During an activity switch, a main server does not process SNMP traps from the network, and no NE re-synchronizations occur. The auxiliary servers continue to process outstanding requests, and synchronize the request information with the new primary server after the activity switch.</p>
<p>Manual server activity switch</p> <p>A manual activity switch is typically performed for maintenance or testing during a scheduled period of low activity, and involves the following sequence of events.</p> <ul style="list-style-type: none"> • A 5620 SAM administrator initiates the activity switch on the primary server. • The standby server performs an activity switch to become the new primary server. • The new primary server connects to the primary database and manages the network. • The new primary server and the auxiliary servers synchronize the request information. • If automatic database realignment is enabled, the new primary server attempts a database switchover. 	<p>When the communication failure is resolved, each GUI client receives notification that redundancy is restored.</p>

Table 12 5620 SAM database redundancy functions

Function	Notes
<p>Database switchover</p> <p>A database switchover is a manual operation that reverses the primary and standby database roles, for example, for primary database maintenance, or to realign database roles with database stations after a server activity switch.</p> <p>A switchover can occur only when the primary and standby databases are functioning correctly and can communicate with each other.</p> <p>A database switchover involves the following sequence of events.</p> <ul style="list-style-type: none"> • A 5620 SAM administrator initiates the switchover on a primary or standby server. • The main server asks each auxiliary server to release all database connections. The switchover fails if all database connections are not released within 15 minutes. • The main server directs the standby database to become the primary database. • The main server fully synchronizes information with the new primary database. <p>See 8.11 "To perform a 5620 SAM database switchover using the 5620 SAM client GUI" (p. 261) for information about performing a database switchover.</p>	<p>No automatic database realignment occurs after a database switchover.</p>
<p>Database failover</p> <p>A database failover is an automatic operation that changes the standby database into a primary database when the original primary database is unreachable, for example, because of a power disruption on the primary database station.</p> <p>A database failover involves the following sequence of events.</p> <ul style="list-style-type: none"> • No main server can communicate with the primary database within a period that is 2 min by default. • The currently active main server directs the standby database to become the primary database. • If automatic database realignment is enabled and the primary server and database are not aligned, the primary server performs an activity switch. • The primary server directs each auxiliary server to connect to the new primary database. • The main server restarts after a failover. 	<p>When the primary server detects a communication failure with the primary or standby database, the GUI clients are informed that the database is not reachable.</p> <p>After the cause of the communication failure is resolved, the GUI clients are notified that the database is reachable.</p> <p>After a failover, you must reinitiate the former primary database as the new standby database. Database redundancy is not restored until reinitiation is complete.</p> <p>The 5620 SAM attempts to automatically reinitiate the former primary database when automatic database reinitiation is enabled.</p>

Table 12 5620 SAM database redundancy functions (continued)

Function	Notes
<p>Re-establishing database redundancy</p> <p>Re-establishing database redundancy after a database failure requires database instantiation to replicate the current primary database as the standby database.</p> <p>After a failover, the former primary database is not available for redundancy until an operator or the automatic database instantiation function re-instantiates it as the new standby database.</p> <p>See 8.15 “To instantiate a redundant database using the 5620 SAM client GUI” (p. 268) and 8.16 “To instantiate a redundant database using a CLI script” (p. 269) for information about re-establishing database redundancy after a failover.</p>	<p>The following conditions must be met before you can re-establish database redundancy.</p> <ul style="list-style-type: none"> • The failover completes successfully. • The station that contains the primary database is operational. • The former primary database proxy port is configured and in service.

8.5 Redundancy failure scenarios

8.5.1 Overview

The following describe the 5620 SAM actions in response to various types of redundancy failures.

- **Primary server loses contact with primary database**

If the standby server can communicate with the primary database and the managed NEs, the primary server performs a server activity switch. No database failover occurs.

If automatic database realignment is enabled, the new primary server performs a database switchover.

- **Primary server loses contact with managed NEs**

If the standby server can communicate with the primary database and the managed NEs, the primary server performs a server activity switch.

If automatic database realignment is enabled, the new primary server performs a database switchover.

- **Primary server loses contact with primary database and managed NEs**

If the standby server can communicate with the primary database and the managed NEs, the primary server performs a server activity switch. No database failover occurs.

If automatic database realignment is enabled, the new primary server performs a database switchover.

- **Primary server loses contact with primary database, managed NEs, and standby server**

The standby server activates to become the new primary server, and if automatic database realignment is enabled, initiates a database switchover.

- **Both servers lose contact with primary database**

The primary server initiates a database failover, and if automatic database realignment is enabled, also initiates a server activity switch.

- **Both servers lose contact, primary server and database can communicate**

The primary server and database remain the primary server and database. The 5620 SAM raises an alarm about the server communication failure.

- **Both servers lose contact with managed NEs**

If the primary and standby servers can each communicate with the preferred database, no server activity switch or database failover occurs. The 5620 SAM raises a reachability alarm against each NE in the network.

- **Both servers lose contact with primary database and managed NEs**

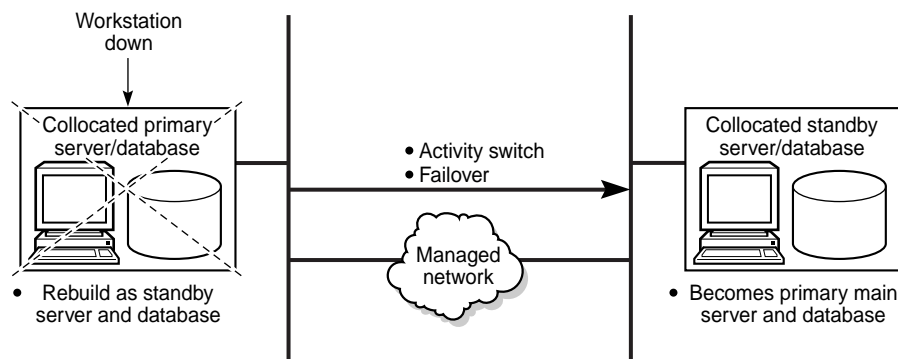
If the primary and standby servers can communicate with each other, no server activity switch or database failover occurs. However, the 5620 SAM system is unavailable; manual intervention such as a database failover is required.

- **Both servers fail, primary database isolated, standby database operational**

When both servers return to operation, the servers cannot connect to the primary database. Because the state of the standby database is unknown, no database failover occurs; manual intervention such as a database switchover is required.

8.5.2 Collocated system, primary station unreachable

Figure 18 Primary server and database station down, collocated system



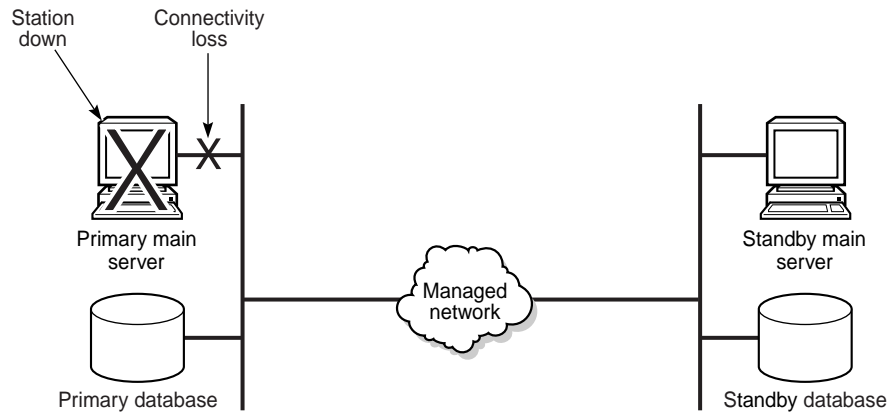
24116

The following occur when the primary station becomes unresponsive:

- The standby server and database become the primary server and database.
- Redundancy is restored when the former primary station returns to service as the standby station.

8.5.3 Distributed system, primary server unreachable

Figure 19 Primary server unreachable, distributed system



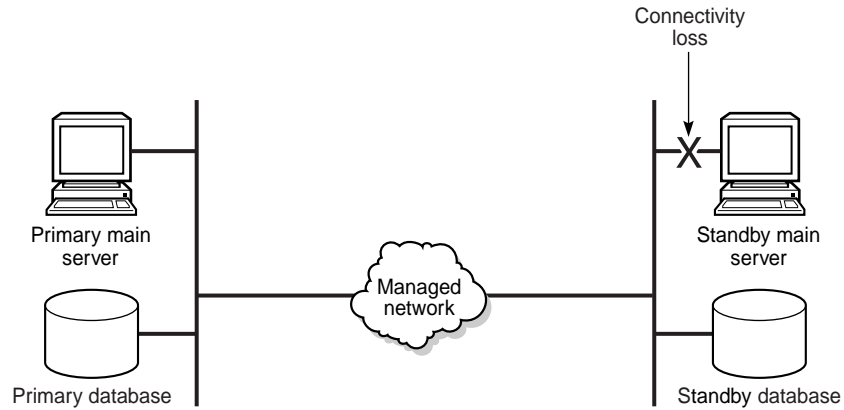
24117

The following occur when the primary station becomes unresponsive:

- The standby server detects the connectivity loss and becomes the primary server.
- The new primary server raises alarms about the unavailability of the former standby server and about the activity switch.
- If automatic database realignment is enabled, the new primary server initiates a database switchover.
- When connectivity is restored, the former primary server assumes the standby server role.

8.5.4 Distributed system, standby server unreachable

Figure 20 Standby server unreachable, distributed system



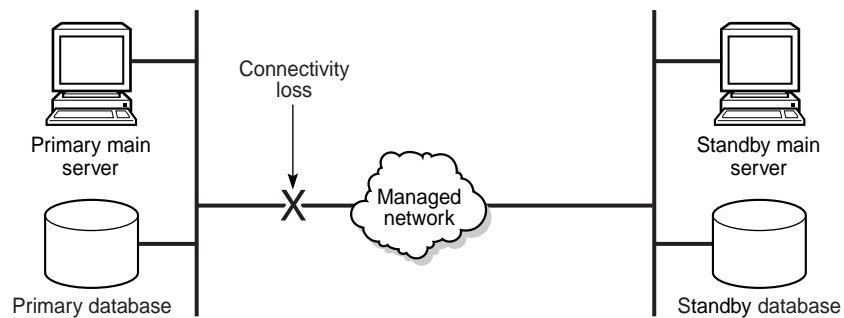
24118

The following occur when the standby station becomes unresponsive:

- The standby server interprets the primary server unresponsiveness as a primary server failure, so attempts to assume the primary server role.
- The primary server generates an alarm to indicate that the standby server is down.
- When the reachability is restored, the standby server resumes the standby role and the alarm clears.

8.5.5 Distributed system, managed network unreachable by primary side

Figure 21 Network failure on primary side, distributed system



24119

The following occur after the connectivity loss is detected:

- The initial primary server continues to operate as a primary server.

- The initial primary server generates an alarm about the standby server unavailability, and a reachability alarm against each NE in the network.
- Each GUI client displays the standby server status as Down.
- The standby server becomes a primary server.

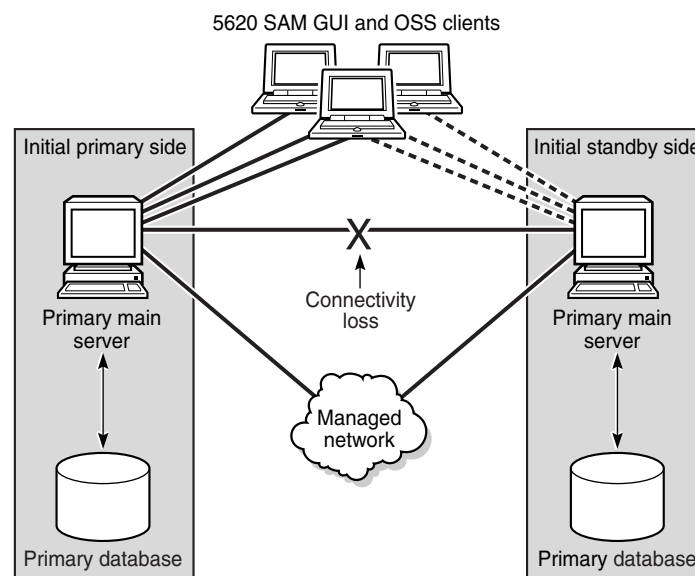


Note: You can eliminate a single point of hardware or network failure by using redundant interfaces and redundant physical network paths. See the *5620 SAM Planning Guide* for more information.

8.5.6 Split complex

A split complex is a scenario in which both servers in a collocated or distributed 5620 SAM system lose contact, but each server can communicate with the preferred database, as shown in the following figure.

Figure 22 Split complex, collocated or distributed system



24120

The following occur after the connectivity loss is detected:

- The initial primary server and database roles do not change; the initial primary server continues to manage the network. The client sessions are not interrupted.
- The primary server raises an alarm about the communication failure.
- The standby server and database switch roles to become a second primary server and database.
- New clients connect to the initial primary server; however, if a client explicitly tries to connect to the second primary server, a session is established.
- When the servers regain contact:

-
- If the network disruption also isolates one server from the managed NEs, the other server and database remain the primary.
 - Otherwise, the server that has currently held the primary role for longer remains the primary, and the other server and database assume the standby role,

5620 SAM system redundancy procedures

8.6 Workflow to perform 5620 SAM system redundancy functions

8.6.1 Process

1

Configure redundancy during 5620 SAM component installation. See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide*.

2

As required, perform manual activity switch and switchover.

a. For 5620 SAM main servers:

1. View the status of the primary and secondary servers to verify the redundancy status is Up; see [8.7 “To view the 5620 SAM system redundancy status” \(p. 254\)](#).
2. If required, verify the redundancy status of the 5620 SAM auxiliary server; see [8.8 “To view the 5620 SAM auxiliary server status” \(p. 257\)](#).
3. Perform a manual activity switch to reverse the roles of the primary and standby servers; see [8.9 “To perform a server activity switch” \(p. 259\)](#).
4. Validate the updated redundancy status; see [8.7 “To view the 5620 SAM system redundancy status” \(p. 254\)](#).

b. For 5620 SAM database servers:

1. View the redundancy status of the primary and secondary database servers to verify the redundancy status is Up; see [8.7 “To view the 5620 SAM system redundancy status” \(p. 254\)](#).
2. As required, specify the behavior of how database switchovers are executed; see [8.10 “To configure 5620 SAM database switchover behavior” \(p. 260\)](#).
3. As required, perform a database switchover; see [8.11 “To perform a 5620 SAM database switchover using the 5620 SAM client GUI” \(p. 261\)](#) or [8.12 “To perform a 5620 SAM database switchover using a CLI script” \(p. 262\)](#).
4. As required, enable or disable automatic database realignment; see [8.14 “To enable or disable automatic database realignment” \(p. 265\)](#).
5. Validate the updated redundancy status; see [8.7 “To view the 5620 SAM system redundancy status” \(p. 254\)](#).

3

After a failover, re-establish redundancy between the standby and primary databases; see [8.15 “To reinitiate a redundant database using the 5620 SAM client GUI”](#) (p. 268) or [8.16 “To reinitiate a redundant database using a CLI script”](#) (p. 269) .

4

If the 5620 SAM system includes an analytics server, perform [8.13 “To restore analytics server operation after a 5620 SAM database failover or switchover”](#) (p. 263) to reconfigure the analytics server.

8.7 To view the 5620 SAM system redundancy status

8.7.1 Steps

1

View the Standby Server, Primary DB and Standby DB status indicators in the 5620 SAM client GUI task bar. Each indicator should display Up.

2

Choose Administration→System Information. The System Information form opens.

3

View the general redundancy information:

- Domain Name—the 5620 SAM domain name specified at installation
- Redundancy Enabled—selected if redundancy is enabled
- Realignment Enabled—selected if automatic database realignment is enabled; displayed only if the 5620 SAM system is redundant
- Auto Standby Re-instantiation Enabled
- Realignment Status—Aligned or Not Aligned

4

View the following information in the Primary Server panel:

- Host Name—the host name of the primary or standalone main server
- Preferred DB—the preferred database of the main server
- Status—Unknown, Down, or Up

5

View the following information in the Primary Database Server panel:

- Instance Name—the name of the primary database instance, also called a SID

-
- IP Address—the IP address that each main or auxiliary server uses to reach the primary database
 - Host Name—the host name of the primary database, or of the database in a standalone 5620 SAM system

6

If the 5620 SAM system is redundant, view the following information in the Standby Server panel:

- Host Name—the host name of the standby main server
- Status—Unknown, Down, or Up

7

If the 5620 SAM system is redundant, view the following information in the Standby Database Server panel:

- Instance Name—the name of the standby database instance, also called a SID
- IP Address—the IP address that each main or auxiliary server uses to reach the standby database
- Host Name—the host name of the standby database

8

Click Properties to display additional information about the primary or standby 5620 SAM main server. The Main Server (Edit) properties form opens.

9

View the following general main-server information:

- Host Name—the host name of the primary main server
- Server Type—Main
- Resource Managed—selected if the main server is included in 5620 SAM resource management

10

View the following information in the Client Communication panel:

- Private IP Address—the IP address that the main server uses as the source address for communication with the 5620 SAM GUI and OSS clients through a NAT router
- Public IP Address—the IP address that the 5620 SAM GUI and OSS clients use to reach the main server through a NAT router



Note: The Private IP Address and Public IP Address display 0.0.0.0 when the 5620 SAM clients and the main server use host names, rather than IP addresses, for communication.

The Private IP Address and Public IP Address display the same IP address when NAT is not used between the main server and clients.

11

View the following information in the Redundant Server Communication panel:

- Private IP Address—the IP address that the main server uses as the source address for communication with the standby main server through a NAT router
- Public IP Address—the IP address that the standby main server uses to reach the primary main server through a NAT router
- Peer Public IP Address—the IP address that the standby main server uses to reach the main server

 **Note:** The Private IP Address and Public IP Address display the same IP address when NAT is not used between the primary and standby main servers.

12


View the following information in the Redundancy Database State panel:

- Switchover State—whether switchover in progress, and operational state
- Last Attempted Switchover Time—time of previous switchover attempt
- Failover State—whether failover in progress, and operational state
- Last Attempted Failover Time—time of previous failover attempt
- Standby Re-instantiation State—whether re-instantiation is in progress, and operational state
- Last Attempted Standby Re-instantiation Time—time of previous standby re-instantiation attempt
- Number of Archive Logs To be Applied—number of archive logs that remain to be applied on standby database
- Estimated Time to Apply Archive Logs (seconds)—system time estimate for application of archive logs on standby database

13

View the following information in the Auxiliary Server Communication panel:

- Private IP Address—the IP address that the main server uses as the source address for communication with the auxiliary servers through a NAT router
- Public IP Address—the IP address that the auxiliary servers use to reach the primary main server

 **Note:** The Private IP Address and Public IP Address display the same IP address when NAT is not used between the main server and the auxiliary servers.

14

View the following information in the Main Server Communication panel:

- Server Public IP Address—the IP address that the auxiliary server uses to communicate with the main server

-
- 15** _____
Close the Main Server properties form. The System Information form reappears.
- 16** _____
Click Database to view more detailed database information, if required. See [Chapter 7, "5620 SAM database management"](#) for information about the 5620 SAM database.
- 17** _____
Click on the Faults tab to view alarm information, if required.
- 18** _____
Close the form.
- END OF STEPS** _____

8.8 To view the 5620 SAM auxiliary server status

8.8.1 Steps

- 1** _____
Choose Administration→System Information. The System Information form opens.
- 2** _____
Click on the Auxiliary Servers tab.
- 3** _____
Review the list of auxiliary servers.
- 4** _____
Select an auxiliary server in the list and click Properties. The properties form for the auxiliary server opens.
- 5** _____
Review the auxiliary server information, which includes the following:
- Host Name—the host name of the auxiliary server
 - Port Number—identifies the port that the auxiliary server uses to communicate with each main server and database
 - Auxiliary Server Type—Reserved or Preferred
 - Server Status—Unknown, Down, Up or Unused

-
- Resource Managed—selected if the auxiliary server is included in 5620 SAM resource management
 - Public IP address—the IP address that the main servers use to reach the auxiliary server

6

Perform one of the following:

- a. View the following main server information for a redundant 5620 SAM system:
 - Server 1 Public IP address—the IP address that the auxiliary server uses to communicate with the primary or standby main server
 - Server 2 Public IP address—the IP address that the auxiliary server uses to communicate with the primary or standby main server
- b. View the following main server information for a standalone 5620 SAM system:
 - Server Public IP address—the IP address that the auxiliary server uses to communicate with the main server

7

Click on the Auxiliary Services tab.

8

Review the list of auxiliary services.

9

Review the information for each auxiliary service, which includes the following:

- Service Name—the type of service, for example, statistics collection
- Selected—indicates whether this auxiliary server is currently used by a main server to process requests
- IP Address—the IPv4 address that the managed NEs use to reach the auxiliary server
- IPv6 Address—the IPv6 address that the managed 9500 MPR NEs use to reach the auxiliary server
- Host Name—the host name of this auxiliary server
- Auxiliary Server Type—Reserved or Preferred

10

Close the Auxiliary Services form.

11

Click on the Faults tab to view alarm information, if required.

12

Close the form.

END OF STEPS

8.9 To perform a server activity switch

8.9.1 Purpose

Perform this procedure to reverse the primary and standby roles of the main servers in a redundant 5620 SAM system. Consider the following before you perform a server activity switch.

- Each client GUI receives notification of a server activity switch.
- During a server activity switch, a main server does not process SNMP traps, attempt to synchronize NEs, or collect statistics.
- During a server activity switch, auxiliary servers process outstanding requests, but do not communicate with a main server.
- After a server activity switch, the new primary main server deploys outstanding configuration changes to NEs, establishes communication with the auxiliary servers, and synchronizes information with the auxiliary servers.
- A manual activity switch stops and starts the former primary main server. Server redundancy is unavailable until the former primary main server is fully initialized as the new standby main server.

8.9.2 Steps

1

Log in to the primary main server station as the samadmin user.

2

Open a console window.

3

Enter the following at the CLI prompt:

```
bash$ /opt/5620sam/server/nms/bin/nmsserver.bash force_restart
↵
```

The server activity switch begins. The primary main server restarts as the standby main server, and the former standby main server becomes the new primary main server.

4

Close the console window.

5 _____
Clear alarms, as required. The activity switch alarms must be cleared manually.

6 _____
Verify that the GUI and OSS clients can connect to the new primary main server.

END OF STEPS _____

8.10 To configure 5620 SAM database switchover behavior

8.10.1 Purpose

Perform this procedure on a redundant 5620 SAM system to specify how database switchovers are executed. A database switchover occurs immediately upon request unless a database query is in progress, in which case the 5620 SAM does the following:

- if session interruption is enabled, waits a specified period before forcing the switchover
- if session interruption is disabled, the switchover does not occur and the Switchover State is Failed

8.10.2 Steps

1 _____
Choose Administration→Database from the 5620 SAM main menu. The Database Manager (Edit) form opens.

2 _____
Configure the required parameters:

- DB Session wait time (minutes)
- Interrupt Read sessions after time out
- Interrupt Write sessions after time out

3

Save your changes and close the form.

END OF STEPS

8.11 To perform a 5620 SAM database switchover using the 5620 SAM client GUI

8.11.1 Purpose

Perform this procedure to use the 5620 SAM client GUI to switch the primary and standby database roles. Before you perform the procedure, ensure that you understand the following implications of a switchover.

- The primary and standby database roles are reversed.
- The primary main server connects to the new primary database.
- Archive logging begins on the new primary database.
- The primary main server directs each auxiliary server to connect to the new primary database.



CAUTION

Service Disruption

The execution of a database switchover depends on how the database switchover behavior is configured.

It is recommended that you review [8.10 "To configure 5620 SAM database switchover behavior" \(p. 260\)](#) before you attempt to perform this procedure to verify the current database switchover configuration.

8.11.2 Steps

1


Log in to the client GUI as a 5620 SAM user with the admin scope of command role.

2

Choose Administration→System Information from the 5620 SAM main menu. The System Information form opens.

3

Click Switchover and respond to the dialog box prompt.

 **Note:** The Switchover option is disabled when the correct switchover conditions are not in place, for example, when a switchover or failover is in progress.

4 _____
Click Yes. The 5620 SAM server performs the database switchover.

5 _____
Close the form.

END OF STEPS _____

8.12 To perform a 5620 SAM database switchover using a CLI script

8.12.1 Purpose

Perform this procedure to use a CLI script to switch the primary and standby database roles. Before you perform the procedure, ensure that you understand the following implications of a switchover.

- The primary and standby database roles are reversed.
- The primary main server connects to the new primary database.
- Archive logging begins on the new primary database.
- The primary main server directs each auxiliary server to connect to the new primary database.



CAUTION

Service Disruption

The execution of a database switchover depends on how the database switchover behavior is configured.

It is recommended that you review [8.10 "To configure 5620 SAM database switchover behavior" \(p. 260\)](#) before you attempt to perform this procedure to verify the current database switchover configuration.

8.12.2 Steps

1 _____
Log in to the primary main server station as the samadmin user.

2 _____
Open a console window.

3

Enter the following at the CLI prompt:

```
bash$ /opt/5620sam/server/switchoverdb.bash username password
↵
```

where *username* and *password* are the login credentials of a 5620 SAM user with the required privilege level and scope of command

The script displays the following confirmation message:

```
The standby database will become the new primary database,
and the old primary will become the new standby.
Do you want to proceed? (YES/no) :
```

4

Enter the following to initiate the switchover:

```
YES ↵
```

The 5620 SAM server initiates a database switchover. Progress is indicated by a rolling display of dots in the console window. The database switchover is complete when the CLI prompt reappears.

5

Close the console window when the database switchover is complete.

END OF STEPS

8.13 To restore analytics server operation after a 5620 SAM database failover or switchover

8.13.1 Steps

After a 5620 SAM database failover or switchover, you must manually reconfigure a 5620 SAM analytics server to communicate with the new primary 5620 SAM database. Otherwise, the 5620 SAM Analytics application cannot function.

1

Log in to the 5620 SAM analytics server as the samadmin user.

2

Open the following file using a plain-text editor such as vi:

```
/opt/5620sam/tomcat/webapps/jasperserver-pro/META-INF/context.xml
```

3

Locate the section that begins with the following tag:

```
<Resource name="jdbc/jasperserver"
```

4

Edit the following line in the section to read:

```
url="jdbc:oracle:thin:@IP_address:port:instance_name"
```

where

IP_address is the IP address of the new primary database

port is the port on the new primary database station that the analytics server uses to reach the database

instance_name is the instance name of the new primary database

5

Save and close the file.

6

Open the following file using a plain-text editor such as vi:

```
/opt/5620sam/analytics/config/install.config
```

7

Locate the section that begins with the following tag:

```
#Oracle DB (Repo and JNDI) details
```

8

Edit the following line in the section to read:

```
dbName=instance_name
```

where

instance_name is the instance name of the new primary database

9

Save and close the file.

10

Open a console window.

11

Enter the following to stop the analytics server:

```
bash$ /opt/5620sam/analytics/bin/AnalyticsAdmin.sh stop ↵
```

The following message is displayed:

```
Stopping 5620 SAM Analytics Server
```


When the analytics server is completely stopped, the following message is displayed:

```
5620 SAM Analytics Server is not running
```

12

When the analytics server is completely stopped, enter the following to start the analytics server:

```
bash$ /opt/5620sam/analytics/bin/AnalyticsAdmin.sh start ↵
```

The following message is displayed:

```
Starting 5620 SAM Analytics Server
```

When the analytics server is completely started, the following message is displayed.

```
5620 SAM Analytics Server successfully started!
```

The analytics server now communicates with the new primary 5620 SAM database.

13

Close the console window.

END OF STEPS

8.14 To enable or disable automatic database realignment



CAUTION

Service Disruption

This procedure requires a primary 5620 SAM main server restart, which is service-affecting.

Ensure that you perform this procedure only during a scheduled maintenance period.



Note: This procedure applies only to redundant 5620 SAM deployments.

8.14.1 Steps

1

Perform [Step 4](#) to [Step 14](#) on the standby main server station.

2

Perform [Step 4](#) to [Step 14](#) on the primary main server station.



Note: When you stop the primary main server, a switchover to the standby main server occurs.

3Go to [Step 15](#).**4**

Log in to the main server as the samadmin user.

5

Stop the main server.

1. Enter the following:

```
bash$ cd /opt/5620sam/server/nms/bin ↵
```

2. Enter the following:

```
bash$ ./nmserver.bash stop ↵
```

3. Enter the following:

```
bash$ ./nmserver.bash appserver_status ↵
```

4. The main server is stopped when the command in [Step 5 3](#) returns the following text string:

```
Application Server is stopped
```

If the command returns anything other than the above text string, wait five minutes and repeat [Step 5 3](#) . Do not proceed unless the console displays the above text.

6

Enter the following to switch to the root user:

```
bash$ su - ↵
```

7

Enter the following:

```
# samconfig -m main ↵
```

The following is displayed:

```
Start processing command line inputs...
```

```
<main>
```

8

Perform one of the following:

a. Enable database alignment; perform the following steps.

1. Enter the following:

```
<main> configure redundancy database alignment ↵
```

Database alignment is enabled, and the prompt changes to `<main configure redundancy database>`.

2. Enter the following:

```
<main configure redundancy database> prefer-instance  
instance ↵
```

where *instance* is the database instance with which the main server is to align, typically the database instance on the same side of the management LAN

- b. Disable database alignment; perform the following steps.

1. Enter the following:

```
<main> configure redundancy database no alignment ↵
```

Database alignment is disabled, and the prompt changes to `<main configure redundancy database>`.

9

Enter the following:

```
<main configure redundancy database> exit ↵
```

The prompt changes to `<main>`.

10

Enter the following:

```
<main> apply ↵
```

The configuration change is applied.

11

Enter the following:

```
<main> exit ↵
```

The samconfig utility closes.

12

Enter the following to switch back to the samadmin user:

```
# exit ↵
```

13

Start the main server.

1. Enter the following:

```
bash$ cd /opt/5620sam/server/nms/bin ↵
```

2. Enter the following:

```
bash$ ./nmserver.bash start ↵
```

3. Enter the following:

```
bash$ /opt/5620sam/server/nms/bin/nmserver.bash -s  
nms_status ↵
```

The command returns server status information.

The main server is completely started when the command returns one of the following lines of output:

- on a primary main server:
-- Primary Server is UP
- on a standby main server:
-- Standby Server is UP

4. If the command output indicates that the server is not completely started, wait five minutes and then return to [Step 13 3](#).

Do not proceed to the next step until the server is completely started.

14

Log out of the main server station.

15

If required, perform [8.9 “To perform a server activity switch” \(p. 259\)](#) to perform a server activity switch to revert the primary and standby main servers to their initial roles.

END OF STEPS

8.15 To reinitiate a redundant database using the 5620 SAM client GUI

8.15.1 Purpose

Perform this procedure to re-establish redundancy after a database failover or similar maintenance activity. This procedure re-instantiates the former primary database as the new standby database.

When automatic database reinitiation is enabled, a failed manual re-instantiation attempt does not affect the re-instantiation timer. If a manual reinitiation is successful, the 5620 SAM does not attempt a subsequent re-instantiation.

Before you attempt to perform this procedure, the following conditions must be true:

- The primary database proxy and the standby database proxy are in contact with the primary 5620 SAM server.
- The database listener is operating.

8.15.2 Steps

- 1 _____
Log in to the client GUI as a user with the 5620 SAM admin scope of command role.
- 2 _____
Choose Administration→System Information from the 5620 SAM main menu. The System Information form opens.
- 3 _____
Verify the database redundancy status matches the following:
 - Failover State: Successful
 - Switchover State: Not Attempted
- 4 _____
Click Re-Instantiate Standby, and click Yes. The database re-instantiation begins.
The client GUI status bar and the System Information form display the re-instantiation status. The Standby Re-instantiation State changes from In Progress to Success when re-instantiation is complete. The Last Attempted Standby Re-instantiation Time displays the start time of the current re-instantiation.
- 5 _____
Close the form when the re-instantiation is complete.

END OF STEPS _____

8.16 To re-instantiate a redundant database using a CLI script

8.16.1 Purpose

Perform this procedure to re-establish redundancy after a database failover or similar maintenance activity. This procedure re-instantiates the former primary database as the new standby database. Before you start, the following conditions must be true:

- The primary database proxy and the standby database proxy are in contact with the 5620 SAM server.
- The database listener is operating.

8.16.2 Steps

- 1 _____
Log in to the primary main server station as the samadmin user.

-
- 2 _____
Open a console window.
- 3 _____
Navigate to the `/opt/5620sam/server/nms/bin` directory.
- 4 _____
Enter the following:

```
bash$ ./reinstantiatedb.bash -u username -p password ↵
```

where
username is the user name of a 5620 SAM client account with the required privilege level and scope of command
password is the password for the user account
The script displays the following confirmation message:

```
This action will rebuild the standby database.  
Do you want to proceed? (YES/no) :
```
- 5 _____
Enter the following to begin the reinstantiation:

```
YES ↵
```

The 5620 SAM server begins to reinstantiate the former primary database as the standby database. Progress is indicated by a rolling display of dots in the console window. Database reinstantiation is complete when the CLI prompt reappears.
- 6 _____
Close the console window when the reinstantiation is complete.
- END OF STEPS _____

8.17 To configure an IPDR file transfer policy

8.17.1 Steps

- 1 _____
Choose Tools→Statistics→IPDR transfer policies from the 5620 SAM main menu. The IPDR File Transfer Policy form opens.
- 2 _____
Select the default policy and click Properties. The IPDR File Transfer Policy form (Edit) opens.

3 _____


Select the Enabled parameter.


4 _____

Configure the File Transfer Protocol parameter.

5 _____


Configure the parameters in the Transfer Target panel to specify the target IP address or hostname, port, file-transfer user credentials, and the directory on the target in which to store the transferred statistics files.


 **Note:** The directory that you specify must be an absolute path on the target host, and must currently exist on the target host.

 **Note:** You must ensure that the specified user has read and write access to the target file server directory that you specify.

6 _____

Configure the parameters in the Alternate Transfer Target panel to specify a redundant transfer target, if required.

 **Note:** The directory that you specify must be an absolute path on the target host, and must currently exist on the target host.

 **Note:** You must ensure that the specified user has read and write access to the alternate target file server directory that you specify.

7 _____

Click OK to save your changes and close the form.

END OF STEPS _____

Part IV: 5620 SAM routine maintenance

Overview

Purpose

This part provides information about 5620 SAM maintenance.

Contents

Chapter 9, 5620 SAM routine maintenance overview	275
Chapter 10, 5620 SAM maintenance base measures	281
Chapter 11, Daily maintenance	291
Chapter 12, Weekly maintenance	299
Chapter 13, Monthly maintenance	311
Chapter 14, As required maintenance	325

9 5620 SAM routine maintenance overview

9.1 Overview

9.1.1 Purpose

This chapter describes routine maintenance information.

9.1.2 Contents

9.2	Routine maintenance overview	275
9.3	Routine maintenance guidelines	276
9.4	Obtaining technical assistance	276
9.5	Routine maintenance checklist	277

9.2 Routine maintenance overview

9.2.1 General information

The 5620 SAM maintenance tasks and procedures are intended for NOC operations or other engineering operational staff that are responsible for developing and implementing maintenance procedures in 5620 SAM-managed IP/MPLS networks.

The 5620 SAM maintenance tasks and procedures are categorized by the frequency they are performed or on an as required basis. The implementation of a regular maintenance schedule is recommended in order to:

- prevent downtime caused by software, platform, or network failure
- enable maximum 5620 SAM system performance

The appropriate maintenance frequency depends on the network conditions of the individual service provider or operation. Tailor the suggested maintenance actions and frequency to the unique needs of your network.

Table 13 Maintenance information

For information about	See chapter
Performance maintenance baselines	Chapter 10, "5620 SAM maintenance base measures"
Daily maintenance tasks	Chapter 11, "Daily maintenance"

Table 13 Maintenance information (continued)

For information about	See chapter
Weekly maintenance tasks	Chapter 12, “Weekly maintenance”
Monthly maintenance tasks	Chapter 13, “Monthly maintenance”
As required maintenance tasks	Chapter 14, “As required maintenance”

9.3 Routine maintenance guidelines

9.3.1 General information

Use these guidelines as a basis for developing new or enhancing existing maintenance procedures and workflows that are used in the NOC. These guidelines do not provide a complete list of the features and functionality of the 5620 SAM. The guide includes a high-level view of maintenance actions based on frequency, suggests baseline measures to ensure performance tracking, and describes how to use 5620 SAM and OS utilities to check the performance.

See the other documentation, as described in [2.3 “5620 SAM system administrator tasks and information map” \(p. 19\)](#) , to supplement the development of individualized maintenance procedures for your network.

9.4 Obtaining technical assistance

9.4.1 General information

Collect the information listed in [Table 14, “Required technical-support Information” \(p. 276\)](#) before you contact technical support. The list of support contacts is available at the following URL:

[Technical support](#)

Table 14 Required technical-support Information

Information type	Description
Issue description	<ul style="list-style-type: none"> • recent 5620 SAM GUI or OSS operations • screen captures or text versions of error or information messages • actions performed in response to the issue

Table 14 Required technical-support Information (continued)

Information type	Description
Platform and software specifications	<ul style="list-style-type: none"> • 5620 SAM software release ID • OS release and patch level • hardware information such as the following: <ul style="list-style-type: none"> — CPU type — number of CPUs — disk sizes, partition layouts, and RAID configuration — amount of RAM
OS and 5620 SAM system logs	<p>You can run the following script to collect the log files required by technical support:</p> <ul style="list-style-type: none"> • On a main server station: <code>/opt/5620sam/server/nms/bin/getDebugFiles.bash</code> • On an auxiliary server station: <code>/opt/5620sam/auxserver/nms/bin/getDebugFiles.bash</code> <p>See the <i>5620 SAM Troubleshooting Guide</i> for information about using the script.</p>

9.5 Routine maintenance checklist

9.5.1 Preventive maintenance tasks

Table 15 Recommended 5620 SAM preventive maintenance tasks

✓	Maintenance task	Purpose
Daily maintenance tasks		
	“Daily maintenance information” (p. 292)	Check the type and characteristics of the alarms, and to resolve the network problems caused by the alarms.
	“Daily maintenance procedures” (p. 294)	Ensure consistency between the 5620 SAM database and managed NE configurations.
	11.3 “Backing up the 5620 SAM database and components” (p. 292)	Prevent the loss of network data.
	11.4 “Collecting and storing 5620 SAM log and configuration files” (p. 293)	Record historical system activities and current configuration settings.
	11.3.1 “Overview” (p. 292)	Back up an entire platform to ensure that all data can be restored.
Weekly maintenance tasks		
	12.5 “To check for performance monitoring statistics collection” (p. 301)	Ensure that there is sufficient capacity to process and store network statistics.

Table 15 Recommended 5620 SAM preventive maintenance tasks (continued)

✓	Maintenance task	Purpose
	12.6 “To gather port inventory data for a specific managed device” (p. 302)	Collect inventory information for future baseline checks and post processing of equipment trends and use.
	12.7 “To test a 5620 SAM database restore” (p. 304)	Ensure that 5620 SAM database backups are viable in the event that a restore is required.
	12.8 “To check scheduled device backup status” (p. 308)	Ensure that managed device configuration backups are stored and collected correctly if a restore is required.
	12.9 “To reduce the number of Oracle audit logs” (p. 309)	Ensure that the logs do not use excessive disk space.
Monthly maintenance tasks		
	“Monthly maintenance information” (p. 312)	Perform regular main server and 5620 SAM database activity switches to ensure that 5620 SAM system redundancy functions correctly and responsively.
	13.3 “Checking the 5620 SAM platform performance” (p. 312)	Compare RHEL platform performance over time to check for degradation.
	13.4 “Checking Windows client platform performance” (p. 312)	Compare Windows platform performance over time to check for degradation.
	13.5 “Checking LAN TCP/IP connections between network-management domain elements” (p. 313)	Test connectivity between 5620 SAM components.
	13.6 “Generating and storing a user account list” (p. 313)	Keep up-to-date records of staff and their assigned user accounts.
	13.7 “Verifying documentation and support contact list updates” (p. 313)	Check for product updates and new load information.
	13.8 “Setting the time and date” (p. 313)	Keep network devices and the NMS domain on the same clock.
As required maintenance tasks		
	“5620 SAM platform modification” (p. 328)	As required, modify the 5620 SAM main server, auxiliary server or database platform to add or remove a CPU, install another NIC type, or increase or decrease the amount of RAM.
	“Changing 5620 SAM passwords” (p. 338)	For greater security, it is recommended that you regularly change the 5620 SAM database user and Oracle SYS user passwords.
	“Auxiliary server administration” (p. 349)	Stop and restart a 5620 SAM auxiliary server when it requires maintenance.
	“Cflowd auxiliary server administration” (p. 351)	Stop and restart a Cflowd auxiliary server when it requires maintenance and to display its status.

Table 15 Recommended 5620 SAM preventive maintenance tasks (continued)

✓	Maintenance task	Purpose
	"Backing up and restoring NE configuration files" (p. 368)	It is recommended that you back up the files each time you back up the 5620 SAM database, and restore the files during a 5620 SAM database restore.
	"Restoring and re-instantiating the 5620 SAM database" (p. 370)	Restore a 5620 SAM database using a previously created database backup.
	"Restoring and re-instantiating the 5620 SAM database" (p. 370)	Restore a standalone 5620 SAM database using a backup copy of the database.
	"Clearing inactive residential subscriber instances from the 5620 SAM database" (p. 398)	Periodically run a script to clear out the accumulation of inactive residential subscriber instance records from the 5620 SAM database
	"Listing customer service information" (p. 401)	Generate and export a list of services or service objects that handles customer traffic for analysis purposes.
	"Checking for duplicate service or resource names" (p. 403)	Check for duplicate names to ensure naming conventions are followed.
	"Configuring the OLC state of equipment or services" (p. 405)	To limit the numbers of alarms displayed on the 5620 SAM, configure the OLC state of equipment, services, or schedules to specify whether the object is in maintenance or in-service mode.

10 5620 SAM maintenance base measures

10.1 Overview

10.1.1 Purpose

This chapter describes the maintenance base measures used to evaluate the activity and performance of network components.

10.1.2 Contents

Maintenance base measures	282
10.2 Base measures overview	282
10.3 Base measures guidelines	282
10.4 Platform base measures	283
10.5 Inventory base measures	286
10.6 Performance and scalability base measures	286
10.7 Reachability base measures	288

Maintenance base measures

10.2 Base measures overview

10.2.1 General information

Maintenance base measures can be used by NOC operations or engineering staff that are responsible for maintenance issues to evaluate the activity and performance of network components, for example, client GUI response times when listing equipment.

The data from a series of base measures can be used, over time, to track performance trends. For example, if there are reports that client GUI response times for listing equipment degrades over time, you can use the base measures to determine how much performance has degraded. The procedures in this guide can help narrow the search for the cause of performance degradation.

You should:

- determine the types of base measures that should be implemented for your network
- record base measures data
- create and regularly perform the tasks necessary to gather and compare base measures over time

This chapter provides base measure information for:

- platform—to ensure system sizes are tracked
- performance and scalability—to categorize system limitations as a baseline against NMS response times
- inventory counts—to generate inventory lists for storage and post-processing
- reachability—to ensure that customer services are available

10.3 Base measures guidelines

10.3.1 Overview

Base measures can be affected by issues that are beyond the scope of this guide, including:

- network topology design
- NOC or operations area LAN design

The 5620 SAM service test manager (STM) provides the ability to group OAM diagnostic tests into test suites that you can run as scheduled tasks. You can customize a test suite to your network topology and execute the test suite to establish baseline performance information. You can retain the test suite, modify it to accommodate network topology changes, and execute the test suite to establish new base measures as required. Scheduled execution of the test suite and regular review of the results may reveal

deviations from the baseline. See the *5620 SAM User Guide* for information about using the STM and creating scheduled tasks.

10.4 Platform base measures

10.4.1 Overview

You can use 5620 SAM base measures to:

- record the details of the platform configuration
- track network-specific growth to provide a delta for performance measures, for example, how long it takes to list 1000 ports on the current station compared to 10 000 ports on the same station, or on a smaller or larger station

Table 16 Platform base data

Application	Platform information
Windows	
5620 SAM client GUI	RAM: CPU (quantity, type, speed): OS version and patch level: Disk space: Monitor: Graphics card:
Windows	
Additional 5620 SAM client GUI	RAM: CPU (quantity, type, speed): OS version and patch level: Disk space: Monitor: Graphics card:
Additional 5620 SAM client GUI	RAM: CPU (quantity, type, speed): OS version and patch level: Disk space: Monitor: Graphics card:
RHEL	

Table 16 Platform base data (continued)

Application	Platform information
5620 SAM main server 1	RAM: CPU (quantity, type, speed): OS version and patch level: Swap space: Disk partition sizes:
5620 SAM database 1	RAM: CPU (quantity, type, speed): OS version and patch level: Swap space: Disk partition sizes:
5620 SAM main server 2	RAM: CPU (quantity, type, speed): OS version and patch level: Swap space: Disk slices:
5620 SAM database 2	RAM: CPU (quantity, type, speed): OS version and patch level: Swap space: Database disk file systems: Disk slice sizes:
5620 SAM preferred auxiliary server 1	RAM: CPU (quantity, type, speed): OS version and patch level: Swap space: Disk slice sizes:
5620 SAM preferred auxiliary server 2	RAM: CPU (quantity, type, speed): OS version and patch level: Swap space: Disk slice sizes:

Table 16 Platform base data (continued)

Application	Platform information
5620 SAM reserved auxiliary server 1	RAM: CPU (quantity, type, speed): OS version and patch level: Swap space: Disk slice sizes:
5620 SAM reserved auxiliary server 2	RAM: CPU (quantity, type, speed): OS version and patch level: Swap space: Disk slice sizes:
5620 SAM client GUI	RAM: CPU (quantity, type, speed): OS version and patch level: Swap space: Disk slices: Monitor: Graphics card:
Additional 5620 SAM client GUI	RAM: CPU (quantity, type, speed): OS version and patch level: Swap space: Disk slices: Monitor: Graphics card:
Additional 5620 SAM client GUI	RAM: CPU (quantity, type, speed): OS version and patch level: Swap space: Disk slices: Monitor: Graphics card:

10.5 Inventory base measures

10.5.1 Overview

You can use inventory base measures to:

- create lists of network objects for future processing
- track network-specific growth to provide a delta for any performance measures, for example, how long it takes 5 versus 15 client GUIs to list 1000 ports

Use the following sequence to create inventory base measures, for example, for access ports. You can modify the sequence to create additional inventory base measures for other objects.

1. Determine the type of object data for which you need to create inventory records, for example, access ports.
2. List the ports of all managed network devices using the client GUI manage equipment window or create an XML OSS request to generate the list.
3. Format the inventory for future processing, based on your inventory processing applications.
4. Generate the inventory data, using the same listing and filtering criteria, on a weekly or monthly basis, as necessary to track changes to the network.

When new devices are added to the network on a regular basis, increase the inventory frequency.

5. Use the generated list to record the current inventory of network objects and as a baseline measure of performance.

For example, baseline the time required to generate a client GUI list of 1000 access ports.

When an access port list is later generated, record the time required to generate the list using 2000 ports. Ideally, it takes twice as long to list twice as many ports; if the ratio of listing time to number of ports is highly nonlinear, there may be scalability issues that require investigation.

10.6 Performance and scalability base measures

10.6.1 Overview

You can use the following 5620 SAM performance and scalability base measures to:

- record the system limit numbers and compare to the measurement data collected in your network
- track network-specific growth to provide a delta for any performance measures on similarly-sized platforms, for example, how long it takes to discover 10 new devices versus 20 new devices
- quantify user perceptions of performance

Table 17 Scalability base measures

Type of base measure	System limits	Expected response time	Network base measure response time	Additional information
Total devices managed	See the appropriate <i>5620 SAM Release Description</i> and <i>5620 SAM Planning Guide</i> for information about release-specific system limits.	The client GUI is operational XX seconds after launching.		The time to open icons in the Equipment navigation tree increases depending on the number of configured MDAs.
Total services		<ul style="list-style-type: none"> • XML OSS configuration of 300 VLL services in X min • XML OSS configuration of 100 VPLS services with 3 sites and one SAP in 5 min 		The complexity of the service configuration affects response time. For example, adding additional SAPs to a VPLS increases provisioning time.
Outstanding alarms		The client GUI is able to retrieve and display XX 000 alarms in the dynamic alarm list during startup.		—
Client GUIs for each server		—		Open a configuration form using the client GUI in X amount of time. Measure X against a constant platform size over time
Device discovery		Discover one additional device with an IP address in the X.X.X.1 to 255 range in less than 1 min.		—

10.6.2 Performance base measures

For networks, commonly available tools such as ping, which measures round trip time using ICMP, can be used to determine quantities such as packet loss and round trip delay. See the ping command information in this guide, and the *5620 SAM Troubleshooting Guide*, for more information about performing the commands.

- Packet loss is defined as the fraction of packets sent from a measurement agent to a test point for which the measurement agent does not receive an acknowledgement from the test point. Acknowledgements that do not arrive within a pre-defined round trip delay at the measurement agent are considered lost.

- Round trip delay is defined as the interval between the time a measurement agent application sends a packet to a test point and the time it receives acknowledgement that the packet was received by the test point.

You can baseline the packet loss results and round trip delay times for specific NMS LAN and network scenarios. Record those results for future baselines against regularly run packet loss and round trip delay tests.

10.7 Reachability base measures

10.7.1 Overview

System reachability is important in business-critical applications. Service reachability components are:

- Can the customer reach the service? (reachability)
- If so, is the service available for customer use? (service availability)
- If not, how frequently and how long do service outages last? (service outage duration)

The types of measures and baselines necessary to ensure reachability and availability are network-dependent, and vary depending on the topology of the network, the networking technologies used to move data, and the types of equipment used.

10.7.2 Reachability

A test point is reachable from a testing measurement agent when the agent can send packets to the test point and receive a response from the test point that the packet was received. The ping test and the OAM diagnostics using the 5620 SAM or device CLI can test reachability. The results from these tests should be recorded to create a measurement baseline.

These tests can be performed when you troubleshoot a customer service, or when you perform SLA tests before you enable a customer service.

10.7.3 Service availability

The network between a measurement agent and a test point is considered available at a given time when the measured packet loss rate and the round trip delays are both below pre-defined thresholds. The threshold values are dependent on network topology. The ping test and the OAM diagnostics using the 5620 SAM or CLI to a device can test service availability. The results from these tests should be recorded to create a measurement baseline.

10.7.4 Service outage duration

The duration of an outage is defined as the difference between the time a service becomes unavailable and the time it is restored. Time between outages is defined as the difference between the start times of two consecutive outages. Troubleshooters that resolve customer problems, or the data generated to resolve SLAs, can provide the baseline metrics to measure outages, and the time between outages. Record the information to create a measurement baseline.

11 Daily maintenance

11.1 Overview

11.1.1 Purpose

This chapter describes daily maintenance information and procedures for monitoring alarms, backing up the 5620 SAM database, and collecting and storing log and configuration files.

11.1.2 Contents

Daily maintenance information	292
11.2 Viewing and filtering alarms	292
11.3 Backing up the 5620 SAM database and components	292
11.4 Collecting and storing 5620 SAM log and configuration files	293
Daily maintenance procedures	294
11.5 To monitor incoming alarms	294
11.6 To verify 5620 SAM database information	295
11.7 To back up the 5620 SAM log and configuration files	296

Daily maintenance information

11.2 Viewing and filtering alarms

11.2.1 Overview

In large networks where the 5620 SAM is constantly interacting with a busy network, many alarms are raised. You should review alarms on a daily basis to check the type and characteristics of the alarms, and to resolve the network problems caused by the alarms. You should immediately correct physical equipment failure alarms or network device alarms.

You can create search filters to identify alarms for a specific site or service, and view up to six filtered alarm lists to monitor network wide issues.

You can also analyze the alarm history log on an as required basis to determine whether there are any chronic or prolonged failures, or trends. See “To review historical alarm records” in the *5620 SAM User Guide* for more information.



Note: If your NOC is organized to feed alarm streams from multiple vendor equipment to a third-party OSS, you should verify that all alarms are correctly logged by the OSS and then remove the alarms from the 5620 SAM GUI.

Daily maintenance operations that are performed on NEs can cause a large number of alarms to be raised in the 5620 SAM. The OLC state of an object shows whether the object is in service or in maintenance mode. You can filter alarms generated for objects with a particular OLC state. See [“Configuring the OLC state of equipment or services” \(p. 405\)](#).

11.3 Backing up the 5620 SAM database and components

11.3.1 Overview

It is strongly recommended that you frequently back up the 5620 SAM database to prevent network data loss in the event of a failure. Other reasons for performing a database backup include the following:

- To move a database from one station to another
- To set aside a clean copy of the database before performing a system upgrade
- As a preventive measure before making a major change to the network

You can use the 5620 SAM client GUI or a CLI script to perform an immediate backup, and can use the GUI to schedule regular backups. See [Chapter 7, “5620 SAM database management”](#) for information about configuring and performing database backups.

It is recommended that you perform a daily backup of the file system on each 5620 SAM station to enable the component restoration in the event of a catastrophic failure.

11.4 Collecting and storing 5620 SAM log and configuration files

11.4.1 Overview

When a 5620 SAM system runs for long periods with significant activity, the number of generated log files can consume a large amount of disk space. You must ensure that the contents of the 5620 SAM log directories are backed up on a regular basis to maintain a system activity record and to save disk space. It is also recommended that you back up the 5620 SAM configuration files



Note: You must contact technical support to modify the 5620 SAM log storage parameters.

Daily maintenance procedures

11.5 To monitor incoming alarms

11.5.1 Process

The dynamic alarm list allows you to monitor all incoming network and network management domain alarms.

11.5.2 Steps

- 1 _____
If required, choose Application→Alarm Window to enable the display of correlated alarms in the alarm window.
- 2 _____
Ensure that the Alarm Table tab in the Alarm Window at the bottom of the 5620 SAM client GUI is selected.
- 3 _____
If required, configure the filter criteria to limit the range of alarms displayed or to identify alarms for a specific site or service.
- 4 _____
Right-click on an alarm entry row.
The contextual alarm menu appears.
- 5 _____



CAUTION

Service Disruption

Handle the alarms according to your company alarm policies

You cannot recover a deleted alarm unless you store alarms in the alarm history log.

For example, to acknowledge an alarm and then delete the alarm:

1. Choose Acknowledge Alarm(s).
The Alarm Acknowledgment form appears.
2. Modify the Severity and Urgency parameters, as required.
3. In the Acknowledgment Text parameter, enter data about the alarm, according to your company alarm policies.

4. Click OK.
5. Confirm the action.
The Ack column in the alarm row indicates that the alarm is acknowledged.
6. Right-click on the alarm entry row.
The contextual alarm menu appears.
7. Choose Delete Alarm(s) from the contextual menu to delete the alarm.

Note:

It is recommended that you save all deleted alarms to the alarm history log. You can specify when alarms are logged using the Alarm History DB Behavior panel in the Alarm Setting window. See “To configure alarm history database management behavior” in the *5620 SAM User Guide* for more information.

8. Confirm the action. The alarm is deleted.

END OF STEPS

11.6 To verify 5620 SAM database information

11.6.1 Steps

Monitor device synchronization to confirm that the 5620 SAM database information is maintaining synchronization with the NE configuration information.

1

Check for deployment failures. Deployment failures indicate that communication with a managed NE is failing.

1. Choose Administration→NE Maintenance→Deployment from the 5620 SAM main menu. The Deployment form opens.
2. Click Search to display the latest information.
When no failed deployments are listed, deployment problems are not causing a synchronization issue.
3. If deployments are listed, view the state of a deployment in the State column. The possible deployment states include:
 - Canceled
 - Deployed
 - Failed (Configuration). Failure occurred because the configuration could not be applied to the specified objects.
 - Failed (Internal Error). Failure occurred due to general error conditions. The state is intended for all other possible errors.
 - Failed (Partial). Failure occurred at deployment and some of the configuration may have been sent to the network.

- Failed (Resource Unavailable). Failure occurred because one of the resources required to apply the configuration is not in the 5620 SAM database.
 - Not Deployed
 - Pending
 - Postponed
4. Identify the source of the deployment problem. For example, for a Failed configuration state, ensure the configuration was performed correctly on the client GUI.

2

If you determine that there is a deployment problem and the problem is unrelated to the 5620 SAM or device configuration, use your company IT policies to check the LAN for connectivity and transmission problems, such as collisions and CRC errors.

END OF STEPS

11.7 To back up the 5620 SAM log and configuration files

11.7.1 Process

Perform this procedure to save a copy of the 5620 SAM installation log and configuration files for later analysis in the event of a failure.



Note: During a system restart, 5620 SAM log files are backed up to directories that are named using a timestamp. A component that runs for a long time can generate multiple log files. Before you restart a 5620 SAM component, ensure that there is sufficient disk space to store the backed-up log files.

11.7.2 Steps

1

Collect the installation log files from the /tmp directory on a RHEL station, or from the C:\5620sam directory on a Windows client station. The installation log files are named 5620_SAM_utility_stderr.txt and 5620_SAM_utility_stdout.txt.

where *utility* is the 5620 SAM installer type, for example, dbconfig or Server_Install

2

Collect the following 5620 SAM database, server, JMS server, and client log files, as required.

1. Collect the database dbconfig.properties file, which contains database configuration setting information, from the *installation_directory*/config directory on each 5620 SAM database station.

2. Collect the `nms-server.xml` file, which contains server configuration setting information, from the `installation_directory/nms/config` directory on each main server station.
3. Collect the log files from the `installation_directory/nms/log` directory. There may be many log files in this directory, depending on how long the 5620 SAM software is running.

When a 5620 SAM log file reaches a predetermined size, the 5620 SAM closes, compresses, and renames the file by including a sequence number and a timestamp. The following is an example of the filename format:

`EmsServer.#.timestamp.log`

where

`#` is a sequence number; the sequence begins at 0

`timestamp` is the time of closure, in the following format: `YYYY-MM-DD_hh-mm-ss`

4. Collect the `nms-auxserver.xml` file, which contains server configuration settings, from the `installation_directory/nms/config` directory on each auxiliary server.
5. Collect the `installation_directory/nms/config/nms-client.xml` file from each client station. This file contains the client configuration settings. Rename each file to indicate the client GUI station from which it is copied.

3

Transfer the log files to a secure location that is not in the network management domain.

END OF STEPS

12 Weekly maintenance

12.1 Overview

12.1.1 Purpose

This chapter describes weekly maintenance information and procedures.

12.1.2 Contents

Weekly maintenance information	300
12.2 Collecting device hardware inventory data	300
12.3 Checking scheduled device backups	300
12.4 5620 SAM database audit log management	300
Weekly maintenance procedures	301
12.5 To check for performance monitoring statistics collection	301
12.6 To gather port inventory data for a specific managed device	302
12.7 To test a 5620 SAM database restore	304
12.8 To check scheduled device backup status	308
12.9 To reduce the number of Oracle audit logs	309

Weekly maintenance information

12.2 Collecting device hardware inventory data

12.2.1 Overview

You can collect device hardware inventory data to:

- create a list of managed device objects, for example, access ports that are available as SAPs
- save for future processing and inventory tracking
- compare the current and historical lists to identify trends and capacity changes
- record the time required to gather inventory data as a base measure

See the inventory chapter in the *5620 SAM User Guide* for more information about generating specific types of inventory reports.

12.3 Checking scheduled device backups

12.3.1 Overview

When the 5620 SAM performs a device configuration backup, the 5620 SAM FTPs the following files from the NE:

- bof.cfg
- primary-config file specified in bof.cfg
- index file, which is the primary-config file with an .ndx extension

Before you schedule a backup, you must:

- have a 5620 SAM user account with an assigned admin scope of command role or a scope of command role with write access to the mediation package.
- have a user account with FTP access on the managed device.
- ensure the BOF persist parameter is set by typing the command: <show bof>. The parameter should be set to <persist on>.

12.4 5620 SAM database audit log management

12.4.1 Overview

As part of the 5620 SAM database security, audit log files are automatically created to track database session creation activities. The 5620 SAM does not automatically remove the files. You must monitor the directory that contains the audit log files to ensure that the files do not consume excessive disk space.

Weekly maintenance procedures

12.5 To check for performance monitoring statistics collection

12.5.1 Process

Use the performance monitoring statistic log records to determine whether performance statistics are collected within the scheduled interval using the client GUI.

1 _____

Choose Tools→Statistics→Statistics Manager from the 5620 SAM main menu. The Statistics Manager form opens.

2 _____

Set the Statistics Type parameter to Statistics Record to retrieve a list of historical data for the type of logged statistics.

3 _____

Choose a type of statistics to collect. For example, to check interface statistics for managed devices, choose Interface Additional Stats (Physical Equipment).

4 _____

Perform one of the following:

- a. To collect statistics for the past hour, click Search. Go to [Step 6](#).
- b. To collect statistics based on a set of user-defined criteria, choose No Filter.

5 _____

Configure the filter criteria and click Search.



Note: You must specify a filter to limit the number of log records to less than 15 000; otherwise, a problem encountered form appears.

6 _____

Review the data for the selected statistic.

1. Click on the Monitored Object or Monitored Object Name headings to sort the historical statistics records by type of object.
2. Review the Time Captured heading for one or more objects.

Verify that the time captured intervals match the intervals set for the object or the statistic logging class, as specified in the *5620 SAM User Guide*.

If the time captured intervals are not sufficient, there will be gaps in the historical record.

7

If there are gaps in the historical record, check the mediation policy to ensure that:

- polling is enabled and administratively up
- the polling interval for a specific MIB or MIB entry is sufficient for collecting the required statistics

i **Note:** Each row that represents a log record shows the Suspect column. When a check mark is present for an interval, there may have been a problem with collection during that interval.

8

Record the data for the selected device and type of statistics. Use this data as a base measurement to verify that statistics data was collected correctly over the scheduled interval.

END OF STEPS

12.6 To gather port inventory data for a specific managed device

12.6.1 Process

For most inventory lists you can:

- generate an inventory of the listed data
- reorganize the information from most important to least important
- remove columns of data
- sort rows in ascending or descending order

12.6.2 Steps

1

Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2

Choose a Network Element (Network) and click Search. The list form displays the results of the inventory search.

3

Choose an NE from the list and click Properties. The Network Element (Edit) form opens.

4

Click on the Inventory tab and choose Port (Physical Equipment). The list form displays the results of the inventory search for the selected device.

5

Generate a list based on the inventory collection or comparison that you plan to make. For example, to compare weekly lists of access ports, generate a filter to list only access ports.

6

Record the amount of time required to generate the inventory list for future base measure comparisons.

7

To show or hide columns of access port information:

1. Right-click on a column heading and choose Column Display.
2. Select Administrative State in the Displayed on Table column and click the left arrow to move the Administrative State to the Available for Table column.
3. Click Apply. The Administrative State column of data is removed from the access port list.

8

To save the list of access ports:

1. Right-click on a column heading and choose Save To File. The Save form opens.
2. Enter a filename; for example, *access_device123_dateoflistgeneration*.
3. Click Files of Type to specify the file type.
4. Browse to choose a location in which to save the file.
5. Click Save. The file is saved to the specified location with the appropriate file extension.

9

To save the table preferences for future use:

1. Right-click on a column heading and choose Save Table Preferences.
2. Click OK to confirm.

The table preferences for the list form and user are saved. For example, when you choose another device, and click on the Ports tab and the Physical Ports tab, the Administrative State heading is not displayed. However, when you click on the SONET Channels tab, the Administrative State heading appears.

10

Move the file to another station, as required, for inventory analysis or post-processing.

END OF STEPS

12.7 To test a 5620 SAM database restore



CAUTION

Service Disruption

Using a station that has connectivity to the managed network or other 5620 SAM components may cause a service disruption.

Ensure that you perform the procedure only on an isolated station.

12.7.1 Steps

It is strongly recommended that you regularly test a recent database backup to ensure that you can use the backup file to restore the 5620 SAM database in the event of a failure.

1

Generate comparison points for the 5620 SAM database, for example, the number of managed devices and cards, by creating an inventory of information, as described in the *5620 SAM User Guide*. This information is used to compare against the restored database information in a test environment to check the validity of the database backup.

2

Ensure that the test station has the same system configuration as the actual database station, for example, partitioning, OS version, and OS patch level.

3

Obtain a recent 5620 SAM database backup.

4

Log in to the test station as the root user.

5

Open a console window.

6 Shut down any running 5620 SAM software on the test station.

7 Copy the database backup file set to the test station.

i **Note:** The path to the backup file set must be the same as the path to the file set at creation time.

8 Copy the following files for the existing 5620 SAM release to an empty directory on the test station:

- samjre-SAM_R_r_revision-Pp.x86_64.rpm
- samconfig-SAM_R_r_revision-Pp.x86_64.rpm
- samoracle-SAM_R_r_revision-Pp.x86_64.rpm
- samdb-SAM_R_r_revision-Pp.x86_64.rpm
- OracleSw_PreInstall.sh

9 Navigate to the directory that contains the 5620 SAM installation files.

10 Enter the following:

```
# ./OracleSw_PreInstall.sh ↵
```

i **Note:** A default value is displayed in brackets []. To accept the default, press ↵. The following prompt is displayed:

```
Please select between the following option:
1) NEW INSTALL, DB RESTORE, OR DB RECONFIGURATION OF 5620 SAM
2) UPGRADE OF 5620 SAM
3) EXIT
Please enter(1,2 or 3):
```

11 Enter 1. The following prompt is displayed:

```
Enter the Oracle dba group name [group]:
```

12 Enter the group name from the existing database deployment. The following messages and prompt are displayed:

```
Creating group group if it does not exist ...
done
```

```
Enter the Oracle user name [user]:
```

13

Enter the username from the existing database deployment.

The following messages and prompt are displayed:

```
Oracle user [user] new home directory will be [/opt/5620sam/
oracle12r1].
Checking or Creating the Oracle user home directory /opt/5620sam/
oracle12r1...
Checking user user...
Adding user...
Changing ownership of the directory /opt/5620sam/oracle12r1 to
user:group.
About to unlock the UNIX user [user]
Unlocking password for user user.
passwd: Success
Unlocking the UNIX user [user] completed
```

```
Please assign a password to the UNIX user user ..
New Password:
```

14

Enter the password from the existing database deployment.

The following prompt is displayed:

```
Re-enter new Password:
```

15

Re-enter the password. The following message is displayed if the password change is successful:

```
passwd: password successfully changed for user
```

The following message and prompt are displayed:

```
Specify whether a 5620 SAM server will be installed on this workstation.
The database memory requirements will be adjusted to account for the additional load.
```

```
Will the database co-exist with a 5620 SAM server on this workstation [Yes/No]:
```

16

Enter Yes or No, as required, based on the existing 5620 SAM deployment.

Messages like the following are displayed as the script execution completes:

```
INFO: About to set kernel parameters in /etc/sysctl.conf...
INFO: Completed setting kernel parameters in /etc/sysctl.conf...
INFO: About to change the current values of the kernel parameters
INFO: Completed changing the current values of the kernel parameters
INFO: About to set ulimit parameters in /etc/security/limits.conf...
INFO: Completed setting ulimit parameters in /etc/security/limits.conf...
INFO: Completed running Oracle Pre-Install Tasks
```

17

Enter the following:

```
# yum install samjre* samconfig* samoracle* samdb* ↵
```

The yum utility resolves any package dependencies, and displays the following prompt:

```
Total size: nn G
Installed size: nn G
Is this ok [y/N]:
```

18

Enter y. The following is displayed, along with the installation status as the package is installed.

```
Downloading Packages:
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
```

The package installation is complete when the following is displayed:

```
Complete!
```

19

Enter the following:

```
# /opt/5620sam/samdb/install/bin/samrestoreDb.sh path ↵
```

where *path* is the absolute path of the database backup file set

The database restore begins, and messages are displayed as the restore progresses.

The following is displayed when the restore is complete:

```
DONE
```

20

Review the comparison points of the restored database with the actual database, as generated in [Step 1](#) . If the databases are the same, the backup and restore operation is successful.

END OF STEPS

12.8 To check scheduled device backup status

12.8.1 Steps

1

Choose Administration→NE Maintenance→Backup/Restore from the 5620 SAM main menu. The Backup/Restore form opens.

2

Click on the Backup/Restore Status tab. The managed devices are listed and backup and restore status information is displayed.

3

Select a device and click Properties. The NE Backup/Restore Status form opens.

4

View the information in the Backup Status panel. A Backup State other than Successful may indicate a communication problem or a backup policy configuration error.

5

Ensure that the device configuration file and the associated index file are saved on the device and available for backup. Click on the Configuration Saves tab, and ensure that the Config Save State indicator reads Success.

See the appropriate device operating-system documentation for more information.

6

Click on the Backups tab to view a list of backup operations that are currently in progress. A backup operation disappears from the list after it completes.

7

Click on the Faults tab to view additional troubleshooting information.

8

Close the NE Backup/Restore Status form.

9 _____

Use the information obtained from the NE Backup/Restore Status form to check the backup policy configuration, if required. Click on the Backup/Restore Policy tab.

10 _____

Select the backup policy for the device and click Properties. The Backup Policy (Edit) form opens.

11 _____

Ensure that the policy is assigned to the device.

1. Click on the Backup/Restore Policy Assignment tab. The Backup Policy - Filter form opens.
2. Configure the policy filter criteria and click OK. The Backup Policy - Filter form closes.
3. Move the device to the Assigned Sites list if it is not there by selecting the site from the Unassigned Sites list and clicking on the right-arrow.
4. Save your changes and close the form.

12 _____

Click on the General tab on the Backup Policy (Edit) form.

13 _____

Select the Enable Backup check box.

14 _____

Modify the other parameters, if required.

15 _____

Save your changes and close the form.

END OF STEPS _____

12.9 To reduce the number of Oracle audit logs

12.9.1 Steps

1 _____

Log in to the 5620 SAM database station as the Oracle management user.

2 _____

Navigate to the /opt/5620sam/oracle12r1/rdbms/audit directory.

3

Archive and delete the files, as required. If the number of audit files increases quickly, you may need to perform this procedure more frequently.

END OF STEPS

13 Monthly maintenance

13.1 Overview

13.1.1 Purpose

This chapter describes monthly maintenance information and procedures.

13.1.2 Contents

Monthly maintenance information	312
13.2 Performing main server and database redundancy switches	312
13.3 Checking the 5620 SAM platform performance	312
13.4 Checking Windows client platform performance	312
13.5 Checking LAN TCP/IP connections between network-management domain elements	313
13.6 Generating and storing a user account list	313
13.7 Verifying documentation and support contact list updates	313
13.8 Setting the time and date	313
Monthly maintenance procedures	315
13.9 To measure 5620 SAM platform performance	315
13.10 To check Windows client station performance	317
13.11 To check network management connections	319
13.12 To generate and store user account data	321
13.13 To check for documentation and support updates	322

Monthly maintenance information

13.2 Performing main server and database redundancy switches

13.2.1 Overview

In a redundant 5620 SAM system, performing regular main server and database redundancy tests is important for the following reasons:

- to ensure that 5620 SAM server and database redundancy functions correctly and responsively
- to identify conditions that may interfere with a 5620 SAM upgrade



Note: It is strongly recommended that you perform a main server activity switch and a database switchover monthly, or at least quarterly, if a monthly test is not possible. See [Chapter 8, “5620 SAM system redundancy”](#) for information about performing a server activity switch or database switchover. Contact technical support for further assistance.

13.3 Checking the 5620 SAM platform performance

13.3.1 Overview

Use the following procedure to test the 5620 SAM platform performance and to record base measures. You can compare performance monthly to:

- collect base measure information related to platform performance
- ensure that there is no degradation in performance

If the performance degrades, collect the necessary logs and performance data and contact technical support. See the *5620 SAM Troubleshooting Guide* for information about 5620 SAM log collection.

13.4 Checking Windows client platform performance

13.4.1 Overview

You can compare Windows client station performance monthly to:

- collect base measure information related to platform performance
- ensure that there is no degradation in performance

13.5 Checking LAN TCP/IP connections between network-management domain elements

13.5.1 Overview

Use the ping and traceroute functions each month to check LAN TCP/IP connectivity between 5620 SAM components. Contact your IT department if there seems to be a communication problem between components.

13.6 Generating and storing a user account list

13.6.1 Overview

System administrators should keep a record of 5620 SAM users to:

- associate staff names with user accounts
- provide account information to TAC or Support staff as required for support to log in
- review user account privileges

13.7 Verifying documentation and support contact list updates

13.7.1 Overview

Use the [Customer Documentation Welcome Page](#) website as the source for 5620 SAM technical information and updates to:

- check for changes to TAC, Support, and Call Centre information
- find additional product updates, updated user documentation, and documentation generated for specific situations, such as Network Application Notes, Technical Notes, Product Change Notifications, and Field Notices

You should also regularly check your 5620 SAM platform vendor websites for information about OS patches, updates, and other software and hardware issues.

13.8 Setting the time and date

13.8.1 Overview

You can use a variety of time synchronization and network time protocol tools, depending on network design needs, including:

- ntpd, xntpd, or rdate, for network management domain devices
- the clock function on a Windows station
- SNTP, for devices in the managed network

It is strongly recommended that you maintain time synchronization between network devices. See the appropriate OS documentation for more information about using time and date synchronization protocols.



Note: Timing between the 5620 SAM main servers and GUI clients must be synchronized.

Monthly maintenance procedures

13.9 To measure 5620 SAM platform performance

13.9.1 Steps

1 _____

Log into the main server, auxiliary server, or 5620 SAM database station as the root user.

2 _____

Open a command window.

3 _____

Enter the following to check CPU usage per process:

```
# top ↵
```

Depending on your system configuration, approximately the top 20 processes are displayed.

4 _____

Review the output.

The top 5620 SAM process listed under the CPU column should be the Java process. However, the Java process should not consume the majority of CPU cycles compared to previous base measures. Some database processes may also take CPU time, depending on the system load.

5 _____

Record the data for future performance comparison.

6 _____

Press CTRL-C to stop the command.

7 _____

Use the mpstat command to review the activities performed by the CPU.

1. Enter the following:

```
# mpstat time ↵
```

where *time* is the interval, in seconds, between CPU polls; a value between 10 and 60 is recommended

2. **mpstat output example**

```

CPU      %usr   %nice   %sys %iowait  %irq    %soft  %steal %guest  %idle
all      0.25   0.00    0.17  0.00    0.00   0.00   0.00   0.00   99.58
    
```

mpstat field descriptions

Field	Description (events per second unless noted)
CPU	Processor number; the keyword all indicates that statistics are calculated as averages among all processors
%usr	Percentage of CPU utilization at the user application level
%nice	Percentage of CPU utilization at the user level with nice priority
%sys	Percentage of CPU utilization at the system level; does not include time spent servicing hardware and software interrupts
%iowait	Percentage of CPU idle time during which the system had an outstanding disk I/O request
%irq	Percentage of CPU time spent servicing hardware interrupts
%soft	Percentage of CPU time spent servicing software interrupts
%steal	Percentage of time spent in involuntary wait by the virtual CPU or CPUs during hypervisor servicing of another virtual processor
%guest	Percentage of CPU time spent running a virtual processor
%idle	Percentage of CPU idle time without an outstanding disk I/O request

3. Record the data for future base measure comparisons of station performance. Look for differences in the output of the data for similar loads on each station. Such differences indicate performance degradation.
4. Press CTRL-C to stop the command.

8

Use the iostat command to collect disk read and write data for determining whether there is a disk bottleneck.

1. Type:

```
iostat -x time ↵
```

where *time* is the time period, in seconds, during which you need to collect data; a starting value of 2 is recommended

2. Review the command output; an example is shown below, and the following table describes each field::

iostat output example

```
Device: tps Blk_read/s Blk_wrtn/s Blk_read Blk_wrtn
sdb      0.01      0.04      6.63      11573      181015
sda      2.94      58.78      261.      56      16040031      71372946
```

iostat field descriptions

Field	Description
device	Name of the device
tps	Transfers per second
Blk_read/s	Block reads per second
Blk_wrtn/s	Block writes per second
Blk_read	Total blocks read
Blk_wrtn	Total blocks written

- Record the data for future comparison of platform performance. Look for differences in the output of the data for similar loads on each station, which indicate performance degradation.
- Press CTRL-C to stop the iostat command.

9

Use the netstat command to check for network interface performance issues.

- Type:

```
netstat -i time ↵
```

where *time* is the time period, in seconds, over which you need to collect data; a starting value of 5 is recommended

- Review the netstat output.

END OF STEPS

13.10 To check Windows client station performance**13.10.1 Steps****1**

Open a command window on the client station.

2

Enter the following at the command prompt:

```
ping station_name ↵
```

where *station_name* is the IP address or hostname, if DNS is used, of the main server to which you need to test connectivity

3

Review the ping output for round-trip delays or lost packets. Resolve any connectivity issues that cause delays or dropped packets. Store ping round-trip delay or lost-packet data as a performance base measure for the station. You can use the data for future performance comparisons.

4

Choose Start→Run from the Windows menu bar. The Run form opens.

5

Enter the following in the Open field:

taskmgr ↵

The Windows Task Manager form opens. It provides details about the programs and processes that run on the station. If you are connected to a LAN, you can also view the network status and check network performance. Depending on the NOC work environment and shared computer usage policy, you can also view additional information about other users.

6

Check performance using the appropriate Task Manager tab.

a. Click on the Processes tab. A list of processes appears.

Organize the processes according to CPU usage. The name of each 5620 SAM process begins with 5620SAM. The CPU usage percentage for each 5620 SAM process should fall within your IT specifications or the established performance base measures.

b. Click on the Performance tab. The CPU and page file usage charts appear.

The memory and page-file usage percentages should fall within your IT specifications or the established performance base measures.

c. Click on the Networking tab. The Local Area Connection chart appears.

Network utilization greater than 10 or 20 percent may indicate collisions or other LAN problems that could affect performance in the network management domain.

7

Choose File→Exit Task Manager to close the form.

8

Open a console window.

9

Type:

`tracert station_name ↵`

where *station_name* is the IP address or hostname of the main server to which you need to test connectivity

The tracert command provides details about network connectivity.

10

Review the tracert data, including:

- number of hops required to reach the main server
- average time between hops

Record the data for future base measure comparison. For example, when the number of hops between a client GUI and main server increases over time, traffic takes longer to travel between them, which can degrade performance.

11

Check regularly for advisories related to the OS. If updates or patches are required, contact technical support for information about potential effects on the 5620 SAM.

END OF STEPS

13.11 To check network management connections

13.11.1 Steps

1

Open a console window on the station.

2

Ping the hostname of another station in the network management domain by entering the following:

`ping station_name ↵`

where *station_name* is the IP address or hostname of the other station

3

Review the output. The following is an example of ping output:

```
PING station_name: 56 data bytes
64 bytes from station_name (station_IP_address): icmp_seq=0, time=1.
ms
64 bytes from station_name (station_IP_address): icmp_seq=1, time=0.
ms
64 bytes from station_name (station_IP_address): icmp_seq=2, time=0.
ms
----station_name PING Statistics----
3 packets transmitted, 3 packets received, 0% packet loss
round-trip (ms) min/avg/max = 0/0/1
```

LAN congestion may be a problem if packets are received out of order, are dropped, or take too long to complete the round trip.

4

Store the output for future base measure comparison.

Compare the output over time to ensure that changes in the data are not caused by deteriorating LAN conditions.

5

Check the routing information.

1. Open a console window on the station.
2. Enter one of the following traceroute commands to determine the path taken to a destination by an ICMP echo request message:
 - `tracert` ↵ on a Windows station
 - `tracert` ↵ on a Windows station

The list of near-side interfaces in the path between a source host and a destination device is displayed. The near-side interfaces are the interfaces closest to the source host.

6

Store the output as a record for future base measure comparisons. Compare routes over time to ensure that there is optimal connectivity.

7

To check the routing tables for the platform:

1. Open a console window on the station.
2. To view the active routes for the platform, type:

```
netstat -rn ↵
```

The following information is displayed:

- network destination and gateway IP addresses
- gateway used to reach the network destination
- IP address of the interface on which communication occurs

- metric value of the route

8 _____

Store the output as a record for future base measure comparison. Compare routes over time to ensure that there is optimal connectivity.

END OF STEPS _____

13.12 To generate and store user account data

13.12.1 Steps

1 _____

As admin user, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The User Security -- Security Management (Edit) form opens.

2 _____

Click on the Users tab.

3 _____

Click Search without setting any filtering. The complete list of user accounts appears.

4 _____

Organize the list of users. For example, to organize the list by the type of group that the user belongs to, click on the User Group column heading. The user accounts are listed alphabetically by user group.

5 _____

Save the list of user accounts.

1. Right-click on the user name list heading and choose Save To File. The Save form opens.
2. Enter a name for the user account list, for example, NOCabc_useraccounts_yearmonthday.
3. Click on the Files of Type pull-down menu to specify the file type.
4. Browse to choose a location in which to save the file.
5. Click Save. The file is saved to the selected location in the specified format with the appropriate extension.

-
- 6 _____
Move the account list to a secure location. Store the latest version of the list and keep existing versions of the list for historical purposes.

END OF STEPS _____


13.13 To check for documentation and support updates



Note: You need a Support Documentation Service account to view customer documentation. Contact your account representative for more information.

13.13.1 Steps

- 1 _____
Log in to <https://www.alcatel-lucent.com/support>.
- 2 _____
Enter your login user name and password when prompted.
- 3 _____
Click on the Support Documentation Service link.
- 4 _____
Narrow the documentation search to 5620 SAM.
 1. Set the Select a product category field to Network Management.
The Select a product field list is updated.
 2. Set the Select a product field to 5620 SAM.
 3. Set the Select a type field to the type of information you are looking for, for example:
 - All types to view all applicable documentation for the product
 - Installation for a list of installation guides, sorted by date and release
 - Product Manual for list of guides, such as the *5620 SAM User Guide*, sorted by date and release
 - Release Description for a list of release descriptions that describe release information, such as feature overviews, supported platforms, and scalability considerations
 - Release Notice for a list of release notices that describe load information, such as outstanding and closed problem lists, and restrictions to functionality
- 5 _____
Click Search. The list of documents appears.

 **Note:** You can also use the enhanced search feature to search for 5620 SAM updates between specified dates. Alternatively, you can configure your user profile to automatically notify you of new 5620 SAM user information.

6

Download the documents.

7

Check for TAC, Call Center, or Support updates:

1. Click on the Support link.
2. Click on the Global Support link.
3. Click on the Carrier/Service Provider link.
4. Click on the link to the global technical support organization that supports your organization.
5. Check the contact information for your regional Customer Service or Call Center.

END OF STEPS

14 As required maintenance

14.1 Overview

14.1.1 Purpose

This chapter describes the 5620 SAM maintenance activities that are performed occasionally as required.

14.1.2 Contents

5620 SAM platform modification	328
14.2 Modifying the platform of a 5620 SAM component	328
14.3 To reconfigure a 5620 SAM main server after a platform modification	328
14.4 To reconfigure a 5620 SAM database after a platform modification	330
14.5 To reconfigure a 5620 SAM auxiliary server after a platform modification	331
14.6 To reconfigure a Cflowd auxiliary server	332
14.7 To test 5620 SAM disk performance	333
14.8 To relink the Oracle executable files	336
Changing 5620 SAM passwords	338
14.9 Changing 5620 SAM user passwords	338
14.10 To change the samadmin user password	338
14.11 To change a database user password in a standalone 5620 SAM system	339
14.12 To change a database user password in a redundant 5620 SAM system	343
Auxiliary server administration	349
14.13 To start an auxiliary server	349
14.14 To stop an auxiliary server	350
Cflowd auxiliary server administration	351
14.15 To start a Cflowd auxiliary server	351
14.16 To stop a Cflowd auxiliary server	351
14.17 To display the Cflowd auxiliary server status	352

Analytics server administration	354
14.18 To start an analytics server	354
14.19 To stop an analytics server	354
Auxiliary database administration	356
14.20 To start an auxiliary database	356
14.21 To stop an auxiliary database	356
14.22 To change an auxiliary database user password	357
14.23 To restore an auxiliary database	358
14.24 To replace an auxiliary database station	362
14.25 To remove an auxiliary database station	365
Backing up and restoring NE configuration files	368
14.26 General information	368
14.27 To back up the NE configuration files	368
14.28 To restore the NE configuration files	369
Restoring and re-instantiating the 5620 SAM database	370
14.29 General information	370
14.30 To restore the database in a standalone 5620 SAM system	371
14.31 To restore the primary database in a redundant 5620 SAM system	376
14.32 To reconstitute a 5620 SAM database using a client GUI	385
14.33 To reconstitute a 5620 SAM database using a CLI	386
5620 SAM database export and import	388
14.34 To export a 5620 SAM database	388
14.35 To import a 5620 SAM database	392
Clearing inactive residential subscriber instances from the 5620 SAM database	398
14.36 General information	398
14.37 To delete the inactive residential subscriber instances	398
Listing customer service information	401
14.38 General information	401
14.39 To save a list of service information	401

Checking for duplicate service or resource names	403
14.40 General information	403
14.41 To check for duplicate port descriptions	403
Configuring the OLC state of equipment or services	405
14.42 General information	405
14.43 Setting the OLC state	406
14.44 To view the OLC state of equipment or services	407
14.45 To view the scheduling of OLC state changes of equipment or services	407
14.46 To change the OLC state of equipment or services	408
14.47 To view or change the OLC state from the alarm window	409
14.48 To add the OLC state to a template using the GUI builder	410

5620 SAM platform modification

14.2 Modifying the platform of a 5620 SAM component

14.2.1 General information



CAUTION

Service Disruption

To avoid a network management outage, it is strongly recommended that you contact 5620 SAM technical support before you modify the platform of a 5620 SAM component.

A 5620 SAM component may require reconfiguration or another type of action in response to a change in the available platform resources.

Table 18 5620 SAM platform modification requirements

Modification type	Component and required action			
	Main server	5620 SAM database	Auxiliary server	Cflowd auxiliary server
Number of CPUs	14.3 "To reconfigure a 5620 SAM main server after a platform modification" (p. 328)	14.4 "To reconfigure a 5620 SAM database after a platform modification" (p. 330)	14.5 "To reconfigure a 5620 SAM auxiliary server after a platform modification" (p. 331)	14.6 "To reconfigure a Cflowd auxiliary server" (p. 332)
Amount of RAM				
NIC type				
LVM disk space	14.7 "To test 5620 SAM disk performance" (p. 333) , before increasing disk space			
OS patch or upgrade	—	14.8 "To relink the Oracle executable files" (p. 336)	—	—

14.3 To reconfigure a 5620 SAM main server after a platform modification

14.3.1 Purpose

Perform this procedure to update the main server configuration after a change in the available platform resources.

**CAUTION****Service Disruption**

This procedure requires a main server restart, which is service-affecting.

Ensure that you perform the procedure only during a scheduled maintenance period.



Note: You require root and samadmin user privileges on the main server station.

14.3.2 Steps

1 _____

Log in to the main server station as the samadmin user.

2 _____

Open a console window.

3 _____

Stop the main server:

1. Enter the following:

```
bash$ cd /opt/5620sam/server/nms/bin ↵
```

2. Enter the following:

```
bash$ ./nmserver.bash force_stop ↵
```

3. Enter the following to display the main server status:

```
bash$ ./nmserver.bash appserver_status ↵
```

The command displays a status message.

4. The main server is stopped when the following is displayed:

```
Application Server is stopped
```

If the command displays a different message, repeat [Step 3 3](#) . Do not proceed until the server is stopped.

4 _____

Enter the following to switch to the root user:

```
bash$ su - ↵
```

5 _____

Enter the following to reboot the station:

```
# init 6 ↵
```

The station reboots, and the platform change takes effect.

6 _____
Close the console window.

END OF STEPS _____

14.4 To reconfigure a 5620 SAM database after a platform modification

14.4.1 Purpose

Perform this procedure to update the 5620 SAM database configuration after a change in the available platform resources.



CAUTION

Service Disruption

This procedure requires a 5620 SAM database restart, which is service-affecting. Ensure that you perform the procedure only during a scheduled maintenance period.



Note: You require root user privileges on the 5620 SAM database station:

14.4.2 Steps

1 _____
Log in as the root user on the 5620 SAM database station.

2 _____
Open a console window.

3 _____
Enter the following to reboot the database station:
`# init 6 ↵`

The station reboots, and the platform change takes effect.

END OF STEPS

14.5 To reconfigure a 5620 SAM auxiliary server after a platform modification

14.5.1 Purpose

Perform this procedure to update the auxiliary server configuration after a change in the available platform resources.



CAUTION

Service Disruption

This procedure requires a restart of the auxiliary server, which is service-affecting.

Ensure that you perform the procedure only during a scheduled maintenance period.



Note: You require root and samadmin user privileges on the auxiliary server station.

14.5.2 Steps

1 _____

Log in as the samadmin user on the auxiliary server station.

2 _____

Open a console window.

3 _____

Stop the auxiliary server:

1. Enter the following:

```
bash$ cd /opt/5620sam/auxserver/nms/bin ↵
```

2. Enter the following:

```
bash$ ./auxnmserver.bash auxforce_stop ↵
```

3. Enter the following to display the auxiliary server status:

```
bash$ ./auxnmserver.bash auxappserver_status ↵
```

The command displays a status message.

4. The auxiliary server is stopped when the following is displayed:

```
Auxiliary Server is stopped
```

If the command displays a different message, repeat [Step 3 3](#) . Do not proceed until the server is stopped.

4 _____

Enter the following command to switch to the root user:

```
bash$ su - ↵
```

5 _____

Enter the following:

```
# init 6 ↵
```

The station reboots, and the platform change takes effect.

END OF STEPS _____

14.6 To reconfigure a Cflowd auxiliary server

14.6.1 Purpose

Perform this procedure to update the Cflowd auxiliary server configuration after a change in the available platform resources.



CAUTION

Service Disruption

This procedure requires a restart of the Cflowd auxiliary server, which is service-affecting.

You must perform the procedure only during a scheduled maintenance period.



Note: You require root user privileges on the Cflowd auxiliary server station.

14.6.2 Steps

1 _____

Log on to the Cflowd auxiliary server as the root user.

2 _____

Open a console window.

3 _____

Enter the following:

```
# cd /opt/5620sam/dcp-R_rRn/bin ↵
```

where R_rRn is the software release identifier

4

Enter the following to stop the Cflowd auxiliary server:

```
# ./dcpctl.sh stop ↵
```

The following messages are displayed.

```
Stopping 5620 SAM DCP server...
5620 SAM DCP server is stopped successfully
```

5

Enter the following:

```
# ./dcpctl.sh reconfig ↵
```

The script lists the configuration files that are updated.

6

Enter the following to start the Cflowd auxiliary server:

```
# ./dcpctl.sh start ↵
```

The following messages are displayed.

```
Starting 5620 SAM DCP server...date time org.xnio.Xnio <clinit>
INFO: XNIO Version n.n.n.GA-redhat-n
date time org.xnio.nio.NioXnio <clinit>
INFO: XNIO NIO Implementation Version n.n.n.GA-redhat-n
date time org.jboss.remoting3.EndpointImpl <clinit>
INFO: JBoss Remoting version n.n.n.Final-redhat-n
5620 SAM DCP server is started successfully
```

7

Close the console window.

END OF STEPS

14.7 To test 5620 SAM disk performance

14.7.1 Purpose

Before you add disk capacity to a component that uses the RHEL LVM function, you must ensure that the disk throughput and latency values of a new volume are within tolerance, which is defined as being within 10% of the values for the current volume.

Perform this procedure to check the performance of a 5620 SAM disk partition.

**CAUTION****Service Disruption**

Performing this procedure requires stopping one or more 5620 SAM components.

You must perform this procedure only during a scheduled maintenance period.

14.7.2 Steps**1**

Perform one of the following:

a. Perform the following steps to shut down a 5620 SAM main server.

1. Log in to the main server station as the samadmin user.
2. Open a console window.
3. Navigate to the /opt/5620sam/server/nms/bin directory.
4. Enter the following:

```
bash$ ./nmsserver.bash force_stop ↵
```

5. Enter the following to display the server status:

```
bash$ ./nmsserver.bash appserver_status ↵
```

The command returns a status message.

6. The main server is stopped when the command returns the following status message:

```
Application Server is stopped
```

If the command returns a different message, repeat 5 . Do not proceed until the server is stopped.

b. Perform the following steps to shut down a 5620 SAM auxiliary server.

1. Log in to the auxiliary server station as the samadmin user.
2. Open a console window.
3. Navigate to the /opt/5620sam/auxserver/nms/bin directory.
4. Enter the following:

```
bash$ ./auxnmsserver.bash auxforce_stop ↵
```

5. Enter the following to display the auxiliary server status:

```
bash$ ./auxnmsserver.bash auxappserver_status ↵
```

The command returns a status message.

6. The auxiliary server is stopped when the command returns the following status message:

```
Auxiliary Server is stopped
```

If the command returns a different message, repeat 5 . Do not proceed until the server is stopped.

c. Perform the following steps to shut down a 5620 SAM database.

1. Log in to the 5620 SAM database station as the root user.
2. Open a console window.
3. Enter the following:

```
# cd /etc/rc3.d ↵
```

4. Enter the following to stop the Oracle proxy:

```
# ./S965620SAMOracleProxyWrapper stop ↵
```

Do not proceed until the command returns the following:

```
Done
```

5. Enter the following to stop the 5620 SAM database:

```
# ./S95db5620sam stop ↵
```

Do not proceed until the command returns the following:

```
Done
```

2

If you are performing the test on a main or auxiliary server station, enter the following to switch to the root user:

```
bash$ su - ↵
```

3

Perform one of the following to run the disk performance utility.

a. On a main server station, enter the following:

```
# /opt/5620sam/server/nms/bin/unsupported/5620_SAM_IOTest/  
5620_SAM_IOTest.pl -d target ↵
```

b. On an auxiliary server station, enter the following:

```
# /opt/5620sam/auxserver/nms/bin/unsupported/5620_SAM_  
IOTest/5620_SAM_IOTest.pl -d target ↵
```

c. On a 5620 SAM database station, enter the following:

```
# /opt/5620sam/samdb/install/tools/unsupported/5620_SAM_  
IOTest/5620_SAM_IOTest.pl -d target ↵
```

where *target* is the disk partition to test

4

Record the utility output.

- 5 _____
Increase the disk space of the target disk partition, as required.
 - 6 _____
Repeat [Step 3](#) to [Step 5](#) , as required.
 - 7 _____
Compare the two Read, Write, and Latency values for the partition. If the values differ by more than 10%, contact the 5620 SAM Platform Team through your account representative.
 - 8 _____
Close the console window.
- END OF STEPS _____

14.8 To relink the Oracle executable files

14.8.1 Purpose

Perform this procedure to relink the Oracle executable files on a 5620 SAM database station after you apply an OS patch, or after an OS upgrade.



CAUTION

Service Disruption

This procedure requires a restart of the 5620 SAM database, which is service-affecting.

You must perform the procedure only during a scheduled maintenance period.



Note: You require Oracle management user privileges on the 5620 SAM database station.

14.8.2 Steps

- 1 _____
Log in to the 5620 SAM database station as the Oracle management user.
- 2 _____
Open a console window.

3

Enter the following:

```
bash$ /opt/5620sam/instance_name/install/config/database_name/  
relinkOracle.sh ↵
```

where *instance_name* is the name of the 5620 SAM database instance, for example, samdb1

The script relinks the Oracle executable files.

4

When the script execution is complete, enter the following to reboot the database station:

```
# init 6 ↵
```

The station reboots, and the 5620 SAM database initializes.

END OF STEPS

Changing 5620 SAM passwords

14.9 Changing 5620 SAM user passwords

14.9.1 General information

For increased security, it is recommended that you regularly change the passwords of the user accounts on 5620 SAM components. [14.10 “To change the samadmin user password” \(p. 338\)](#) describes how to change the samadmin user password. [14.11 “To change a database user password in a standalone 5620 SAM system” \(p. 339\)](#) and [14.12 “To change a database user password in a redundant 5620 SAM system” \(p. 343\)](#) describe how to change a 5620 SAM database password.

14.10 To change the samadmin user password

14.10.1 Purpose

Perform this procedure to change the password of the samadmin user in a standalone or redundant 5620 SAM system.



CAUTION

Service Disruption

If you perform this procedure, you must update the samadmin password in each backup/restore and software upgrade policy that requires the password, or the associated operation fails.

Changing the samadmin user password affects the following policy-based operations, if the associated policy includes the samadmin user credentials:

- eNodeB backups, restores, and software upgrades
- Small Cell backups, restores, and software upgrades

You must change the samadmin password on each of the following stations, and must set each password to the same value:

- main server
- auxiliary server
- client delegate server

14.10.2 Steps

1

Log in to the component station as the root user.

2 _____
Open a console window.

3 _____
Enter the following:
passwd samadmin ↵
The following prompt is displayed:

New Password:

4 _____
Enter the new password and press ↵.
The following prompt is displayed:

Confirm New Password:

5 _____
Enter the new password again and press ↵. The password is changed.
Record the new password and store it in a secure location.

6 _____
Close the console window.

7 _____
Log out of the component station.

END OF STEPS _____

14.11 To change a database user password in a standalone 5620 SAM system

14.11.1 Purpose

Perform this procedure to change the password of a user associated with the 5620 SAM database or the auxiliary database in a standalone 5620 SAM system.

**CAUTION****Service Disruption**

The procedure requires a restart of the 5620 SAM main server, which is service-affecting.

It is strongly recommended that you perform this procedure only during a scheduled maintenance period.



Note: Before you perform the procedure, you must ensure that each 5620 SAM main server, auxiliary server, and database is running and operational.

You can use the procedure to change only one user password at a time. To change multiple user passwords, you must perform the procedure multiple times.

When you change a password on one station, the 5620 SAM automatically updates the password on all other 5620 SAM stations.



Note: The 5620 SAM synchronizes the samauxdb password of an auxiliary database with the SYS password of the 5620 SAM database . When you change the SYS password, the samauxdb password is set to the same value.



Note: The 5620 SAM synchronizes the samuser password of an auxiliary database with the samuser password of the 5620 SAM database . When you change the samuser password of the 5620 SAM database, the samuser password of the auxiliary database is set to the same value.

14.11.2 Steps

1 _____

Log in to the main server station as the samadmin user.

2 _____

Open a console window and navigate to the /opt/5620sam/server/nms/bin directory.

3 _____

Enter the following:

```
bash$ ./nmserver.bash passwd ↵
```

The script prompts you for the current SYS user password.

4 _____

Enter the password. The script validates the password, and then displays a list of user names like the following:

```

SAM Database Users:
- sys
- database_user_name (installation default is samuser)
Other Database Users:
- sqltexplain
- appqossys
- outln
- dip
- system
- exit

```

5

Enter a user name. The script prompts you for a password.

6

Enter the new password, which must:

- Be between 4 and 30 characters long
- Contain at least three of the following:
 - lower-case alphabetic character
 - upper-case alphabetic character
 - numeric character
 - special character, which is one of the following:
 - # \$ _
- Not contain four or more of the same character type in sequence
- Not be the same as the user name or the reverse user name
- Not contain a space character
- Differ by at least four characters from the current password

If the password is valid, the script prompts you to retype the password.

7

Enter the new password again. The following prompt is displayed:

```

WARNING: Changing passwords may cause instability to the 5620 SAM
server as well as the Oracle proxy on the database server.
Do you want to proceed (yes/no)?:

```

8

Enter yes ↵. The script displays status messages and then exits. If the status indicates a password change failure, contact technical support.

9

Record the password in a secure location.

10

Perform the following steps.

1. Log in to the 5620 SAM database station as the root user.
2. Open a console window.
3. Enter the following to stop the database proxy:

```
# /etc/rc3.d/S965620SAMOracleProxyWrapper stop ↵
```

Do not proceed until the command returns the following:

```
Done
```

4. Enter the following to start the database proxy:

```
# /etc/rc3.d/S965620SAMOracleProxyWrapper start ↵
```

Do not proceed until the command returns the following:

```
Done
```

5. Close the console window.
6. Log out of the database station.

11

Perform the following steps.

1. Navigate to the `/opt/5620sam/server/nms/bin` directory on the main server station.
2. Enter the following to restart the main server:

```
bash$ ./nmserver.bash force_restart ↵
```

3. Enter the following to display the server status:

```
bash$ ./nmserver.bash -s nms_status ↵
```

The command returns server status information.

If the main server is not completely started, the first line of status information is the following:

```
Main Server is not ready...
```

The main server is completely started when the command returns the following:

```
-- SAM Server is UP
```

12

Close the console windows.

13

Log out of the main server station.

END OF STEPS

14.12 To change a database user password in a redundant 5620 SAM system

14.12.1 Purpose

Perform this procedure to change the password of a user associated with the 5620 SAM database or the auxiliary database in a redundant 5620 SAM system.



CAUTION

Service Disruption

The procedure requires a restart of each 5620 SAM main server, which is service-affecting.

Perform the procedure only during a scheduled maintenance period.



Note: Before you perform the procedure, you must ensure that each 5620 SAM main server, auxiliary server, and database is running and operational.

You can use the procedure to change only one user password at a time. To change multiple user passwords, you must perform the procedure multiple times.

When you change a password on one station, the 5620 SAM automatically updates the password on all other 5620 SAM stations.



Note: The 5620 SAM synchronizes the samauxdb password of an auxiliary database with the SYS password of the 5620 SAM database . When you change the SYS password, the samauxdb password is set to the same value.



Note: The 5620 SAM synchronizes the samuser password of an auxiliary database with the samuser password of the 5620 SAM database . When you change the samuser password of the 5620 SAM database, the samuser password of the auxiliary database is set to the same value.

14.12.2 Steps

1

Log in to the primary main server station as the samadmin user.

2

Open a console window.

3**CAUTION****Service Disruption**

Contact technical support before you attempt to modify the `nms-server.xml` file.

Modifying the `nms-server.xml` file can have serious consequences that can include service disruption.

If you are changing the SYS user or 5620 SAM database user password, perform the following steps.

1. Navigate to the `/opt/5620sam/server/nms/config` directory.
2. Open the `nms-server.xml` file using a plain-text editor such as `vi`.
3. Locate the following parameter entry:

```
dbAutoFailOver=value
```

4. Record the parameter setting.
5. Edit the entry to read:

```
dbAutoFailOver="no"
```

6. Save and close the `nms-server.xml` file.

4

Navigate to the `/opt/5620sam/server/nms/bin` directory.

5

Enter the following:

```
bash$ ./nmserver.bash passwd ↵
```

The script prompts you for the current SYS user password.

6

Enter the password. The script validates the password, and then displays a list of user names like the following

```
SAM Database Users:
- sys
- database_user_name (installation default is samuser)
Other Database Users:
- sqltxplain
- appqossys
- outln
- dip
- system
- exit
```

7

Enter a user name. The script prompts you for a password.

8

Enter the new password, which must:

- Be between 4 and 30 characters long
- Contain at least three of the following:
 - lower-case alphabetic character
 - upper-case alphabetic character
 - numeric character
 - special character, which is one of the following:

\$ _

- Not contain four or more of the same character type in sequence
- Not be the same as the user name or the reverse user name
- Not contain a space character
- Differ by at least four characters from the current password

If the password is valid, the script prompts you to retype the password.

9

Enter the new password again. The following prompt is displayed:

```
WARNING: Changing passwords may cause instability to the 5620 SAM
server as well as the Oracle proxy on the database server.
Do you want to proceed (yes/no)?:
```

10

Enter yes ↵. The script displays status messages and then exits. If the status indicates a password change failure, contact technical support.

11

Record the password in a secure location.

12

If you are changing a password other than the SYS or database user password, go to [Step 16](#).

13

Perform the following steps on each 5620 SAM database station.

1. Log in to the database station as the root user.
2. Enter the following to stop the database proxy:

```
# /etc/rc3.d/S965620SAMOracleProxyWrapper stop ↵
```

Do not proceed until the command returns the following:

Done

3. Enter the following to start the database proxy:

```
# /etc/rc3.d/S965620SAMOracleProxyWrapper start ↵
```

Do not proceed until the command returns the following:

Done

4. Close the console window.
5. Log out of the database station.

14

Perform the following steps.

1. Log in to the standby main server station as the samadmin user.
2. Navigate to the /opt/5620sam/server/nms/bin directory.

3. Enter the following to stop the main server:

```
bash$ ./nmserver.bash force_stop ↵
```

The standby main server stops.

4. Enter the following to display the server status:

```
bash$ ./nmserver.bash appserver_status ↵
```

The main server is stopped when the command returns the following:

```
Application Server is stopped
```

If the command returns a different message, wait five minutes and repeat the step. Do not proceed until the main server is stopped.

5. On the primary main server station, enter the following:

```
bash$ ./nmserver.bash force_restart ↵
```

The primary main server restarts.

6. Enter the following to display the server status:

```
bash$ ./nmserver.bash -s nms_status ↵
```

The command returns server status information.

If the main server is not completely started, the first line of status information is the following:

```
Main Server is not ready...
```

The main server is completely started when the command returns the following:

```
-- Primary Server is UP
```

If the command output indicates that the server is not completely started, wait five minutes and then repeat the step. Do not proceed until the server is completely started.

7. On the standby main server, enter the following to start the main server:

```
bash$ ./nmserver.bash start ↵
```

The standby main server starts.

8. Enter the following to check the server status:

```
bash$ ./nmserver.bash -s nms_status ↵
```

The command returns server status information. The main server is completely started when the command returns the following line of output:

```
-- Standby Server is UP
```

9. Close the console window.
10. Log out of the standby main server station.

15



CAUTION

Service Disruption

Modifying the nms-server.xml file can have serious consequences that can include service disruption.

Contact technical support before you attempt to modify the file.

If the dbAutoFailOver value recorded in [Step 3](#) is yes, perform the following steps:

1. Navigate to the /opt/5620sam/server/nms/config directory on the primary main server station.
2. Open the nms-server.xml file using a plain-text editor such as vi.
3. Locate the following parameter entry:

```
dbAutoFailOver="no"
```

4. Edit the entry to read:

```
dbAutoFailOver="yes"
```

5. Save and close the nms-server.xml file.
6. Navigate to the /opt/5620sam/server/nms/bin directory.
7. Enter the following:

```
bash$ ./nmserver.bash read_config ↵
```

16

Close the open console windows.

17 _____
Log out of the primary main server station.

END OF STEPS _____

Auxiliary server administration

14.13 To start an auxiliary server

14.13.1 Steps

- 1 _____
Choose Administration→System Information from the 5620 SAM main menu. The System Information form opens.
- 2 _____
Click on the Auxiliary Servers tab.
- 3 _____
Select the auxiliary server and click Properties. The Auxiliary Server (Edit) form opens.
- 4 _____
Set the Operation Mode parameter to In Service.
- 5 _____
Click OK to commit the change and close the form.
- 6 _____
Close the System Information form.
- 7 _____
Log on to the auxiliary server station as the samadmin user.
- 8 _____
Open a console window.
- 9 _____
Enter the following:

```
bash$ /opt/5620sam/auxserver/nms/bin/auxnmserver.  
bash auxstart ↵
```


The auxiliary server starts. The initialization may require twenty minutes or more.

10 _____
Close the console window.

END OF STEPS _____

14.14 To stop an auxiliary server



CAUTION

Service Disruption

Performing this procedure may be service-affecting.

Ensure that you perform this procedure only during a scheduled maintenance period.

14.14.1 Steps

1 _____
Choose Administration→System Information from the 5620 SAM main menu. The System Information form opens.

2 _____
Click on the Auxiliary Servers tab.

3 _____
Select the auxiliary server and click Properties. The Auxiliary Server (Edit) form opens.

4 _____
Set the Operation Mode parameter to In Maintenance Mode.

5 _____
Click OK to commit the change and close the form.
The auxiliary server stops.

6 _____
Close the System Information form.

END OF STEPS _____

Cflowd auxiliary server administration

14.15 To start a Cflowd auxiliary server

14.15.1 Steps

1 _____

Log in to the Cflowd auxiliary server station as the root user.

2 _____

Open a console window.

3 _____

Enter the following to start the server:

```
# /opt/5620sam/dcp-R_rRn/bin/dcpctl.sh start ↵
```

where *R_rRn* is the software release identifier

The server starts, and the following messages are displayed:

```
Starting 5620 SAM DCP server...date time org.xnio.Xnio <clinit>
INFO: XNIO Version n.n.n.GA-redhat-n
date time org.xnio.nio.NioXnio <clinit>
INFO: XNIO NIO Implementation Version n.n.n.GA-redhat-n
date time org.jboss.remoting3.EndpointImpl <clinit>
INFO: JBoss Remoting version n.n.n.Final-redhat-n
5620 SAM DCP server is started successfully
```

4 _____

Close the console window.

END OF STEPS _____

14.16 To stop a Cflowd auxiliary server

14.16.1 Steps

1 _____

Log in to the Cflowd auxiliary server station as the root user.

2 _____

Open a console window.

3

Enter the following:

```
# /opt/5620sam/dcp-R_rRn/bin/dcpctl.sh stop ↵
```

where *R_rRn* is the software release identifier

The server stops, and the following messages are displayed:

```
Stopping 5620 SAM DCP server...
5620 SAM DCP server is stopped successfully
```

4

Close the console window.

END OF STEPS

14.17 To display the Cflowd auxiliary server status

14.17.1 Steps

1

Log in to the Cflowd auxiliary server station as the root user.

2

Open a console window.

3

Enter the following:

```
# /opt/5620sam/dcp-R_rRn/bin/dcpctl.sh status ↵
```

where *R_rRn* is the software release identifier

The following is displayed if the server is functioning normally:

```
#####
Status report at date time
Checking 5620 SAM DCP server status...
date time org.xnio.nio.NioXnio <clinit>
INFO: XNIO Version n.n.n.GA-redhat-n
date time org.xnio.nio.NioXnio <clinit>
INFO: XNIO NIO Implementation Version n.n.n.GA-redhat-n
date time org.jboss.remoting3.EndpointImpl <clinit>
INFO: JBoss Remoting version n.n.n.Final-redhat-n
5620 SAM DCP server is started successfully
JBoss Status: UP
DCP Operational Status: UP
DCP Admin Status: ENABLED
#####
```


- 4** _____
Close the console window.

END OF STEPS _____

Analytics server administration

14.18 To start an analytics server

14.18.1 Purpose

Perform this procedure to start the 5620 SAM analytics server software.

1 _____

Log in to the 5620 SAM analytics server as the samadmin user.

2 _____

Open a console window.

3 _____

Enter the following:

```
bash$ /opt/5620sam/analytics/bin/AnalyticsAdmin.sh start ↵
```

The following message is displayed:

```
Starting 5620 SAM Analytics Server
```

When the analytics server is completely started, the following message is displayed.

```
5620 SAM Analytics Server successfully started!
```

4 _____

Close the console window.

END OF STEPS _____

14.19 To stop an analytics server

14.19.1 Purpose

Perform this procedure to stop the 5620 SAM analytics server software.

1 _____

Log in to the 5620 SAM analytics server as the samadmin user.

2 _____

Open a console window.

3

Enter the following:

```
bash$ /opt/5620sam/analytics/bin/AnalyticsAdmin.sh stop ↵
```

The following message is displayed:

```
Stopping 5620 SAM Analytics Server
```

When the analytics server is completely stopped, the following message is displayed:

```
5620 SAM Analytics Server is not running
```

4

Close the console window.

END OF STEPS

Auxiliary database administration

14.20 To start an auxiliary database

14.20.1 Purpose

Perform this procedure to start the auxiliary database software, for example, if the auxiliary database fails to start after a power disruption.

1 _____

Log in to an auxiliary database station as the samauxdb user.

2 _____

Enter the following:

```
# /opt/5620sam/samauxdb/bin/auxdbAdmin.sh start ↵
```

You are prompted for the database user password.

3 _____

Enter the password. The auxiliary database starts.

END OF STEPS _____

14.21 To stop an auxiliary database

14.21.1 Purpose

Perform this procedure to stop the auxiliary database software, for example, for maintenance purposes.

1 _____

Log in to an auxiliary database station as the samauxdb user.

2 _____

Enter the following:

```
# /opt/5620sam/samauxdb/bin/auxdbAdmin.sh stop ↵
```

You are prompted for the database user password.

3

Enter the password. The auxiliary database stops.

END OF STEPS

14.22 To change an auxiliary database user password

14.22.1 Purpose



Note: The 5620 SAM automatically synchronizes an auxiliary database password with the password of the corresponding 5620 SAM database user. To change an auxiliary database password, you must change the corresponding 5620 SAM database password.

1

To change the samauxdb password in a standalone 5620 SAM system, perform [14.11 “To change a database user password in a standalone 5620 SAM system” \(p. 339\)](#) and specify the SYS password.

2

To change the samauxdb password in a redundant 5620 SAM system, perform [14.12 “To change a database user password in a redundant 5620 SAM system” \(p. 343\)](#) and specify the SYS password.

3

To change the samuser password in a standalone 5620 SAM system, perform [14.11 “To change a database user password in a standalone 5620 SAM system” \(p. 339\)](#) and specify the samuser password.

4

To change the samuser password in a redundant 5620 SAM system, perform [14.12 “To change a database user password in a redundant 5620 SAM system”](#) (p. 343) and specify the samuser password.

END OF STEPS

14.23 To restore an auxiliary database

14.23.1 Purpose



CAUTION

Service disruption

Restoring an auxiliary database requires a shutdown of the 5620 SAM system and causes a network management outage.

Ensure that you perform this procedure only during a scheduled maintenance period.

Perform this procedure to restore an auxiliary database in a 5620 SAM system using a database backup.

1

If the 5620 SAM system is redundant, stop the standby main server and the associated auxiliary servers.

1. Perform [14.14 “To stop an auxiliary server”](#) (p. 350) to stop each Preferred and Reserved auxiliary server of the standby main server.
2. Log in to the standby main server as the samadmin user.
3. Open a console window.
4. Enter the following:

```
bash$ cd /opt/5620sam/server/nms/bin ↵
```

5. Enter the following to stop the main server:

```
bash$ ./nmserver.bash stop ↵
```

6. Enter the following to display the main server status:

```
bash$ ./nmserver.bash appserver_status ↵
```

The command displays a status message.

7. The main server is stopped when the following is displayed:

```
Application Server is stopped
```

If the command displays a different message, wait five minutes and return to [Step 1 6](#). Do not proceed until the server is stopped.

2

Stop the standalone or primary main server and the associated auxiliary servers.

1. Perform [14.14 “To stop an auxiliary server” \(p. 350\)](#) to stop each Preferred and Reserved auxiliary server of the primary or standalone main server.
2. Log in to the main server station as the samadmin user.
3. Open a console window.
4. Enter the following:

```
bash$ cd /opt/5620sam/server/nms/bin ↵
```

5. Enter the following to stop the main server:

```
bash$ ./nmserver.bash stop ↵
```

6. Enter the following to display the main server status:

```
bash$ ./nmserver.bash appserver_status ↵
```

The command displays a status message.

7. The main server is stopped when the following is displayed:

```
Application Server is stopped
```

If the command displays a different message, wait five minutes and return to [Step 2 6](#). Do not proceed until the server is stopped.

3

Perform the auxiliary database installation procedure in the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* on each auxiliary database station in the cluster.

4

Stop the auxiliary database; perform [14.21 “To stop an auxiliary database” \(p. 356\)](#).

5

If the backup files to restore are not in the original backup location on each auxiliary database station, you must copy the files to the original backup location on each station.

1. If you know the original backup location, go to [Step 5 6](#).
2. Open the following text file in for viewing:

```
path/AuxDbBackUp/samAuxDbBackup_restore.conf
```

where *path* is the current location of the backup file set

3. Locate the [Mapping] section, which contains one line like the following for each auxiliary server station:

```
v_samdb_node0001 = IP_address:path/AuxDbBackUp
```

The *path* is the original backup location.

4. Record the original backup location.

5. Close the `samAuxDbBackup_restore.conf` file.
6. Copy the `AuxDbBackUp` directory contents from the current backup location to the `AuxDbBackUp` directory in the original backup location on each auxiliary database station.
7. As the root user, enter the following commands on each auxiliary database station:

```
# chown -R samauxdb path ↵
# chmod -R 777 path ↵
```

where *path* is the absolute path of the original backup location

6

Enter the following on one of the stations in the auxiliary database cluster to switch to the `samauxdb` user:

```
# su - samauxdb ↵.
```

7

Perform one of the following:

- a. To restore the latest backup, enter the following:

```
bash$ vbr.py -task restore -config-file path/AuxDbBackUp/
samAuxDbBackup_restore.conf ↵
```

where *path* is the original backup directory

- b. To restore a backup other than the latest, enter the following:

```
bash$ vbr.py -task restore -config-file path/AuxDbBackUp/
samAuxDbBackup_restore.conf --archive=restore_point ↵
```

where

path is the original backup directory

restore_point is the timestamp that follows the word “archive” in the name of the directory that contains the backup set

The restore operation begins. The following messages and a progress indicator are displayed:

```
Preparing...
Found Database port: port
Copying...
[=====
```

8

When the restore is complete, the progress indicator reaches 100% and the following messages are displayed:

```
[=====] 100%
All child processes terminated successfully.
restore done!
```

9

Enter the following to start the auxiliary database:

```
bash$ /opt/5620sam/samauxdb/bin/auxdbAdmin.sh start ↵
```

10

Start the standalone or primary main server and associated auxiliary servers.

1. Log in to the main server station as the samadmin user.
2. Open a console window.
3. Enter the following:

```
bash$ cd /opt/5620sam/server/nms/bin ↵
```

4. Enter the following to start the main server:

```
bash$ ./nmsserver.bash start ↵
```

5. Enter the following to display the main server status:

```
bash$ ./nmsserver.bash appserver_status ↵
```

The command displays a status message.

6. The main server is started when the following is displayed:

```
Application Server process is running. See nms_status for
more detail.
```

If the command displays a different message, wait five minutes and return to [Step 10 5](#). Do not proceed until the server is stopped.

7. Perform [14.13 “To start an auxiliary server” \(p. 349\)](#) to start each Preferred and Reserved auxiliary server of the primary or standalone main server.

11

If the 5620 SAM system is redundant, start the standby main server and associated auxiliary servers.

1. Log in to the standby main server as the samadmin user.
2. Open a console window.
3. Enter the following:

```
bash$ cd /opt/5620sam/server/nms/bin ↵
```

4. Enter the following to start the main server:

```
bash$ ./nmsserver.bash start ↵
```

5. Enter the following to display the main server status:

```
bash$ ./nmsserver.bash appserver_status ↵
```

The command displays a status message.

6. The main server is started when the following is displayed:

```
Application Server process is running. See nms_status for
more detail.
```

If the command displays a different message, wait five minutes and return to [Step 11 5](#). Do not proceed until the server is started.

7. Perform [14.13 “To start an auxiliary server” \(p. 349\)](#) to start each Preferred and Reserved auxiliary server of the standby main server.

END OF STEPS

14.24 To replace an auxiliary database station

14.24.1 Purpose

Perform this procedure to replace an auxiliary database station with a station that has the same IP address, for example, after a hardware failure.

1

Log in to the replacement auxiliary database station as the root user.

2

Open a console window.

3

Navigate to the directory that contains the auxiliary database software.

4

Enter the following:

```
# ./VerticaSw_PreInstall.sh ↵
```

The script displays output similar to the following:

```
INFO: About to set kernel parameters in /etc/sysctl.conf...
```

```
INFO: Completed setting kernel parameters in /etc/sysctl.
conf...
```

```
INFO: About to change the current values of the kernel
parameters...
```

```
INFO: Completed changing the current values of the kernel
parameters...
```

```
INFO: About to set ulimit parameters in /etc/security/limits.conf...
```

```
INFO: Completed setting ulimit parameters in /etc/security/limits.conf...
```

```
Checking Vertica DBA group samauxdb...
```

```
Adding Vertica DBA group samauxdb...
```

```
Checking Vertica user samauxdb...
```

```
Adding Vertica user samauxdb...
```

```
Changing ownership of the directory /opt/5620sam/samauxdb to samauxdb:samauxdb.
```

```
Adding samauxdb to sudoers file.
```

```
Changing ownership of /opt/5620sam/auxdb files.
```

```
INFO: About to add setting to /etc/rc.d/rc.local...
```

```
INFO: Completed adding setting to /etc/rc.d/rc.local...
```

5

If the script instructs you to perform a restart, perform the following steps.

1. Enter the following:

```
# init 6 ↵
```

The station restarts.

2. Log in to the station as the root user.
3. Open a console window.
4. Navigate to the directory that contains the auxiliary database software.

6

Enter the following commands in sequence:

```
# yum install samjre-SAM_R_r_revision-Pp.x86_64.rpm ↵
```

```
# yum install vertica-V.w.x-y.x86_64.RHEL5.rpm ↵
```

```
# yum install samauxdb-SAM_R_r_revision-Pp.x86_64.rpm ↵
```

where

R_r is the 5620 SAM release identifier, in the form MAJOR_minor

revision is the 5620 SAM revision identifier, such as R1, R3, or another descriptor

p is the patch level

V.w.x-y is a version number

After you enter a command, the yum utility resolves any dependencies and displays the following prompt:

```
Total size: nn G
```

```
Installed size: nn G
```

```
Is this ok [y/N]:
```

7

Enter `y ↵`. The following is displayed, along with the installation status as the package is installed.

```
Downloading Packages:
```

```
Running rpm_check_debug
```

```
Running Transaction Test
```

```
Transaction Test Succeeded
```

```
Running Transaction
```

The package installation is complete when the following is displayed:

```
Complete!
```

8

Return to [Step 6](#) as required to enter the next command in the sequence.

9

Perform the following steps on each auxiliary database station.

1. Log in to the station as the root user.

2. Open a console window.

3. Enter the following:

```
# rm -f ~root/.ssh/known_hosts ↵
```

4. Enter the following:

```
# rm -f ~samauxdb/.ssh/known_hosts ↵
```

10

Log in to an existing station in the cluster as the root user.

11

Open a console window.

12

Enter the following:

```
# /opt/5620sam/samauxdb/bin/auxdbAdmin.sh recoverNode
internal_IP ↵
```

where *internal_IP* is the IP address that the station uses to communicate with the other auxiliary database stations

13

When you are prompted for the database user password, enter the password.

14

When you are prompted for the samauxdb password, enter the password.

15

Log in to the replacement station as the root user.

16

Open a console window.

17

Enter the following:

```
# /etc/init.d/samauxdbproxy start ↵
```

The replacement auxiliary database station initializes, and the data is rebalanced among the stations in the cluster.

END OF STEPS

14.25 To remove an auxiliary database station

14.25.1 Purpose



Note: An auxiliary database cluster requires a minimum of three stations.

Perform this procedure to remove a station from an auxiliary database cluster, for example, if the auxiliary database throughput requirements decrease.

1

Log in to the auxiliary database station as the root user.

2

Open a console window.

3

Enter the following:

```
# /opt/5620sam/samauxdb/bin/auxdbAdmin.sh removeNode
internal_IP ↵
```

where *internal_IP* is the IP address that the station uses to communicate with the other stations in the cluster

The station is removed from the auxiliary database cluster.

4

If the cluster requires rebalancing after the removal of the station, you are prompted for the database user password. Perform the following steps.

i **Note:** A cluster rebalance operation may take considerable time, depending on the volume of data in the auxiliary database.

1. Enter the password.

The cluster rebalancing begins. When the rebalancing is complete, the following message is displayed:

```
Cluster rebalance completed. Press a key to continue...
```

2. Press a key to continue.

5

Perform the following steps on each main server when the rebalance operation is complete.

i **Note:** In a redundant system, you must perform the steps on the standby main server station first.

1. Log in to the main server station as the samadmin user.
2. Open a console window.
3. Enter the following to navigate to the server configuration directory:


```
bash$ cd /opt/5620sam/server/nms/config ↵
```
4. Enter the following to make a backup copy of the server configuration file:


```
bash$ cp nms-server.xml nms-server.xml.backup ↵
```
5. Open the nms-server.xml file with a plain-text editor, for example, vi.
6. Locate the section that begins with the following tag:


```
<samauxdb
```
7. Locate the following line in the section and remove the IP address of the auxiliary database station:


```
ipaddress="IP_address_1,IP_address_2...IP_address_n" />
```
8. Save and close the file.

9. If you are configuring the standby main server in a redundant system, enter the following:

```
bash$ /opt/5620sam/server/nms/bin/nmsserver.bash
force_restart ↵
```

The main server restarts.

10. If you are configuring a standalone main server, or the primary main server in a redundant system, enter the following:

```
bash$ /opt/5620sam/server/nms/bin/nmsserver.bash read_config
↵
```

The main server reads the updated configuration file and puts the change into effect.

6

Log in to one of the remaining auxiliary database stations as the root user.

7

Open the `/opt/5620sam/samauxdb/config/install.config` file using a plain-text editor such as vi.

8

Locate the following line and delete the IP address of the station that is being removed from the cluster:

```
hosts=internal_IP1,internal_IP2...internal_IPn
```

9

Locate the following line and delete the IP address entries of the station that is being removed from the cluster:

```
export_hosts=internal_IP1[export_IP1],internal_IP2[export_IP2]...internal_IPn[export_IPn]
```

10

Save and close the file.

11

Enter the following:

```
# /opt/5620sam/samauxdb/bin/auxdbAdmin.sh distributeConfig ↵
```

The updated auxiliary database configuration is distributed to the other stations in the cluster.

END OF STEPS

Backing up and restoring NE configuration files

14.26 General information

14.26.1 Overview

The 5620 SAM stores NE configuration files on a main server file system. The following procedures describe how to create a backup archive of all NE configuration files on a main server, and how to restore an NE backup archive, for example, after a main server disk failure.

14.27 To back up the NE configuration files



Note: Depending on the size and number of NE configuration files, a backup operation may take considerable time.

14.27.1 Steps

1

Log in to the standalone main server station, or the primary main server station in a redundant deployment, as the samadmin user.

2

Open a console window.

3

Enter the following:



Note: If you intend to copy and paste the command from this step into the console window, ensure that you remove the line breaks from the command text before you paste the text.

```
bash$ tar cf - --exclude='backup' /opt/5620sam/nebackup/
| gzip -c >/opt/5620sam/nebackup/backup/nebackup_`date +%Y-%
m-%d-%H-%M`.tgz ↵
```

A compressed archive file named YYYY-MM-DD-hh-mm.tgz is created in the /opt/5620sam/nebackup/backup directory, where YYYY-MM-DD-hh-mm is the file creation time.

4

When the backup operation is complete, copy the file to a secure station that is not part of the 5620 SAM system. If you lack access to such a station, and the 5620 SAM system is redundant, copy the file to the standby main server station.

5 _____
Close the console window.

END OF STEPS _____

14.28 To restore the NE configuration files



Note: Depending on the size and number of NE configuration files, a restore operation may take considerable time.

14.28.1 Steps

1 _____
Log in to the standalone or primary main server station as the samadmin user.

2 _____
Open a console window.

3 _____
Copy the appropriate NE configuration archive file to the /opt/5620sam/nebackup/backup directory.



Note: An NE configuration archive file is named using the file creation time, and has the following format:
YYYY-MM-DD-hh-mm.tgz

4 _____
Enter the following:



Note: If you intend to copy and paste the command from this step into the console window, ensure that you remove the line break from the command text before you paste the text.

```
bash$ gzip -cd /opt/5620sam/nebackup/backup/nebackup_YYYY-MM-DD-hh-mm.tgz | tar xf - -C / ↵
```

where YYYY-MM-DD-hh-mm.tgz is the name of the backup file

The NE configuration files are extracted to the /opt/5620sam/nebackup directory.

5 _____
When the restore operation is complete, close the console window.

END OF STEPS _____

Restoring and re-instantiating the 5620 SAM database

14.29 General information

14.29.1 Overview



CAUTION

Service Disruption

A 5620 SAM database restore requires a shutdown of each 5620 SAM database and main server in the 5620 SAM system, which causes a network management outage.

You must perform a database restore only during a scheduled maintenance period, and contact technical support before you attempt to restore a 5620 SAM database.

You can restore a 5620 SAM database using a backup copy.

In a redundant 5620 SAM system, you must perform one or both of the following to regain 5620 SAM database function and redundancy, depending on the failure type.

- Restore the primary 5620 SAM database.
- Reinstantiate the standby 5620 SAM database.

Both operations are required after a primary database failure. After a standby database failure, no restore operation is required, but you must reinitiate the primary database on the standby database station to restore redundancy. You can use the 5620 SAM client GUI or a CLI script to reinitiate a database.



Note: In a redundant 5620 SAM system, you can restore a 5620 SAM database backup only on a primary database station. To restore a database backup on a station other than the primary station, you must do the following on the station before you attempt the restore:

- Uninstall the 5620 SAM database, if it is installed.
- Install a primary database on the station.

In a redundant 5620 SAM system, you can reinitiate a database only on a standby database station. To reinitiate a database on a station other than the standby station, you must do the following on the station before you attempt the reinitiation:

- Uninstall the 5620 SAM database, if it is installed.
- Install a standby database on the station.

See [14.30 “To restore the database in a standalone 5620 SAM system”](#) (p. 371) for information about restoring a standalone 5620 SAM database. See [14.31 “To restore the primary database in a redundant 5620 SAM system”](#) (p. 376) for information about restoring a redundant 5620 SAM database. See [14.32 “To reinitiate a 5620 SAM database using a client GUI”](#) (p. 385) and [14.33 “To reinitiate a 5620 SAM database using a CLI”](#) (p. 386) for information about re-instantiating a primary 5620 SAM database

on a standby database station.

14.30 To restore the database in a standalone 5620 SAM system

14.30.1 Purpose

The following steps describe how to restore a standalone 5620 SAM database using a backup copy. You require the following:

- a database backup file set from the same 5620 SAM release
- the original file path of the database backup
- root user privileges on the main server and database stations
- samadmin user privileges on the main server station
- Oracle management user privileges on the main server and database stations

14.30.2 Steps

1

If the database backup file set is on the database station, copy the file set to a different station for safekeeping.

2

Perform the following steps to stop the main server.

1. Log in to the main server station as the samadmin user.
2. Open a console window.
3. Enter the following:

```
bash$ cd /opt/5620sam/server/nms/bin ↵
```

4. Enter the following to stop the main server:

```
bash$ ./nmserver.bash force_stop ↵
```

5. Enter the following to display the 5620 SAM server status:

```
bash$ ./nmserver.bash appserver_status ↵
```

The command displays a status message.

The main server is stopped when the command displays the following:

```
Application Server is stopped
```

If the command displays a different message, wait five minutes and repeat [Step 2](#)
[5](#). Do not proceed until the server is stopped.

3

Disable the automatic main server startup:

1. Enter the following to switch to the root user:

```
bash$ su - ↵
```

2. Enter the following:

```
# cd /etc/init.d ↵
```

3. Enter the following:

```
# mv 5620SAMServerWrapper inactive.5620SAMServerWrapper ↵
```

4

Enter the following to uninstall the 5620 SAM database:

```
# yum remove samdb ↵
```

The yum utility displays the following prompt:

```
Installed size: nn G
```

```
Is this ok [y/N]:
```

5

Enter y ↵. The following is displayed:

```
Downloading Packages:
```

```
Running rpm_check_debug
```

```
Running Transaction Test
```

```
Transaction Test Succeeded
```

```
Running Transaction
```

```
Uninstalling the 5620 SAM Database...
```

When the uninstallation is complete, the following is displayed:

```
Complete!
```

6

When the uninstallation is complete, enter the following to reboot the database station:

```
# init 6 ↵
```

The station reboots.

7

When the reboot is complete, log in as the root user on the database station.

8

Open a console window.

9

Remove any files that remain in the `/opt/5620sam/samdb/tablespace` and `/opt/5620sam/samdb/archivelog` directories.

10

Copy the database backup file set to the database station.



Note: The path to the backup file set must be the same as the path to the file set at creation time.

11

Navigate to the directory that contains the 5620 SAM installation files.

12

Enter the following:

```
# ./OracleSw_PreInstall.sh ↵
```

13

The following prompt is displayed:

```
Please select between the following option:
```

```
1) NEW INSTALL, DB RESTORE, OR DB RECONFIGURATION OF 5620 SAM
```

```
2) UPGRADE OF 5620 SAM
```

```
3) EXIT
```

```
Please enter(1,2 or 3):
```

```
Enter 1 ↵.
```

14

The following prompt is displayed:

```
Enter the Oracle dba group name [group]:
```

```
Press ↵ to accept the default.
```

The following message is displayed:

```
Creating group group if it does not exist ...
```

```
WARNING: Group group already exists locally.
```

The following prompt is displayed:

```
Do you want to use the existing group? [Yes/No]:
```

15

Enter Yes ↵.

The user [username] for the group [group] already exists locally.
Do you want to use the existing user? [Yes/No]:

16

Enter Yes ↵.

The following messages are displayed:

```
Checking or Creating the Oracle user home directory /opt/5620sam/oracle12r1...
Checking user username...
WARNING: Oracle user with the specified name already exists locally.
Redefining the primary group and home directory of user username ...
Changing ownership of the directory /opt/5620sam/oracle12r1 to username:group.
About to unlock the UNIX user [username]
Unlocking password for user username.
passwd: Success
Unlocking the UNIX user [username] completed
```

The following prompt is displayed:

Do you want to change the password for the user username? [Yes/No]:

Type No ↵.

The following prompt is displayed:

Specify whether a 5620 SAM server will be installed on this workstation.
The database memory requirements will be adjusted to account for the additional load.
Will the database co-exist with a 5620 SAM server on this workstation [Yes/No]:

17

Enter Yes or No, as required, and press ↵.

Messages like the following are displayed as the script execution completes:

```
INFO: About to set kernel parameters in /etc/sysctl.conf...
INFO: Completed setting kernel parameters in /etc/sysctl.conf...
INFO: About to change the current values of the kernel parameters
INFO: Completed changing the current values of the kernel parameters
INFO: About to set ulimit parameters in /etc/security/limits.conf...
INFO: Completed setting ulimit parameters in /etc/security/limits.conf...
INFO: Completed running Oracle Pre-Install Tasks
```

18

Enter the following:

yum install samdb* ↵

The yum utility resolves any package dependencies, and displays the following prompt:

```
Total size: nn G
Installed size: nn G
Is this ok [y/N]:
```

19

Enter `y` ↵. The following is displayed, along with the installation status as the package is installed.

```
Downloading Packages:
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
```

The package installation is complete when the following is displayed:

```
Complete!
```

20

Enter the following:

```
# /opt/5620sam/samdb/install/bin/samrestoreDb.sh path ↵
```

where *path* is the absolute path of the database backup file set

The database restore begins, and messages are displayed as the restore progresses.

The following is displayed when the restore is complete:

```
DONE
```

21

When the database restore is complete, enable the automatic main server startup.

1. Enter the following on the main server station:

```
# cd /etc/init.d ↵
```

2. Enter the following:

```
# mv inactive.5620SAMServerWrapper 5620SAMServerWrapper ↵
```

22

Start the main server.

1. Enter the following to switch to the samadmin user:

```
# su - samadmin ↵
```

2. Enter the following:

```
bash$ cd /opt/5620sam/server/nms/bin ↵
```

3. Enter the following:

```
bash$ ./nmserver.bash start ↵
```

The main server starts.

23

Close the open console windows, as required.

24

Perform a full network resynchronization to discover the interim changes in the managed network.

END OF STEPS

14.31 To restore the primary database in a redundant 5620 SAM system

14.31.1 Purpose

The following steps describe how to restore a 5620 SAM database using a database backup created on the same station in a redundant 5620 SAM system. The station is called the primary database station in this procedure.

To regain 5620 SAM database redundancy when the database restore is complete, you must reinitiate the restored primary database on the standby database station. See [14.32 “To reinitiate a 5620 SAM database using a client GUI” \(p. 385\)](#) and [14.33 “To reinitiate a 5620 SAM database using a CLI” \(p. 386\)](#) for information.

You require the following:

- a 5620 SAM database backup file set from the same 5620 SAM release
- the original file path of the database backup
- root user privileges on the main server and 5620 SAM database stations
- samadmin user privileges on each main server stations
- Oracle management user privileges on each 5620 SAM database stations

14.31.2 Steps

1

If the 5620 SAM database backup file set is on the primary database station, copy the file set to a different station for safekeeping.

2

Stop the standby main server.

1. Log in to the standby main server station as the samadmin user.
2. Open a console window.
3. Enter the following:

```
bash$ cd /opt/5620sam/server/nms/bin ↵
```

4. Enter the following:

```
bash$ ./nmserver.bash force_stop ↵
```

5. Enter the following to display the 5620 SAM server status:

```
bash$ ./nmserver.bash appserver_status ↵
```

The command displays a status message.

The main server is stopped when the following is displayed:

```
Application Server is stopped
```

If the command displays a different message, wait five minutes and repeat [Step 2 5](#) . Do not proceed until the server is stopped.

3

Disable the automatic standby main server startup:

1. Enter the following to switch to the root user:

```
bash$ su - ↵
```

2. Enter the following:

```
# cd /etc/init.d ↵
```

3. Enter the following:

```
# mv 5620SAMServerWrapper inactive.5620SAMServerWrapper ↵
```

4

Stop the standby 5620 SAM database:

1. Log in to the standby database station as the root user.
2. Open a console window.
3. Enter the following:

```
# cd /etc/rc3.d ↵
```

4. Enter the following to stop the Oracle proxy:

```
# ./S965620SAMOracleProxyWrapper stop ↵
```

5. Enter the following to stop the 5620 SAM database:

```
# ./S95db5620sam stop ↵
```

Do not proceed until the command displays the following:

```
Done
```

5

Stop the primary main server.

1. Log in to the primary main server station as the samadmin user.
2. Open a console window.
3. Enter the following:

```
bash$ cd /opt/5620sam/server/nms/bin ↵
```

4. Enter the following:

```
bash$ ./nmserver.bash force_stop ↵
```

5. Enter the following to display the 5620 SAM server status:

```
bash$ ./nmserver.bash appserver_status ↵
```

The command displays a status message.

The main server is stopped when the following is displayed:

```
Application Server is stopped
```

If the command displays a different message, wait five minutes and repeat [Step 2 5](#) . Do not proceed until the server is stopped.

6

Disable the automatic primary main server startup:

1. Enter the following to switch to the root user:

```
bash$ su - ↵
```

2. Enter the following:

```
# cd /etc/init.d ↵
```

3. Enter the following:

```
# mv 5620SAMServerWrapper inactive.5620SAMServerWrapper ↵
```

7

Enter the following to uninstall the primary database:

```
# yum remove samdb ↵
```

The yum utility displays the following prompt:

```
Installed size: nn G
```

```
Is this ok [y/N]:
```

8

Enter y ↵. The following is displayed:

```
Downloading Packages:
```

```
Running rpm_check_debug
```

```
Running Transaction Test
```

```
Transaction Test Succeeded
Running Transaction
Uninstalling the 5620 SAM Database...
When the uninstallation is complete, the following is displayed:
Complete!
```

9

When the uninstallation is complete, enter the following to reboot the primary database station:

```
# init 6 ↵
```

The station reboots.

10

When the reboot is complete, log in as the root user on the primary database station.

11

Open a console window.

12

Remove any files that remain in the `/opt/5620sam/samdb/tablespace` and `/opt/5620sam/samdb/archivelog` directories.

13

Copy the database backup file set to the database station.



Note: The path to the backup file set must be the same as the path to the file set at creation time.

14

Navigate to the directory that contains the 5620 SAM installation files.

15

Enter the following:

```
# ./OracleSw_PreInstall.sh ↵
```



Note: The default values displayed by the script are shown as `[default]`. To accept a default value, press `↵`. If you specify a value other than the default, you must record the value for use when the `OracleSw_PreInstall.sh` script is run during a software upgrade, or when the Oracle management user information is required by technical support.

16

The following prompt is displayed:

```
Please select between the following option:  
1) NEW INSTALL, DB RESTORE, OR DB RECONFIGURATION OF 5620 SAM  
2) UPGRADE OF 5620 SAM  
3) EXIT  
Please enter (1,2 or 3):
```

Enter 1 ↵.

17

The following prompt is displayed:

```
Enter the Oracle dba group name [default]:
```

Enter a group name and press ↵.

i **Note:** To reduce the complexity of subsequent software upgrades and technical support activities, it is recommended that you accept the default for this parameter.

The following message is displayed:

```
Creating group group if it does not exist ...
```

If you specify a new group, the following message is displayed:

```
done
```

18

If you specify an existing group, the following prompt is displayed:

```
WARNING: Group group already exists locally.  
Do you want to use the existing group? [Yes/No]:
```

Perform one of the following.

- a. Enter Yes ↵.
- b. Enter No ↵. Go to [Step 17](#) .

19

If the default user exists in the specified group, the following prompt is displayed:

```
The user [username] for the group [group] already exists locally.  
Do you want to use the existing user? [Yes/No]:
```

20

Perform one of the following.

a. Enter Yes ↵; the following messages are displayed:

```

Checking or Creating the Oracle user home directory /opt/5620sam/
oracle12r1...
Checking user username...
WARNING: Oracle user with the specified name already exists
locally.
Redefining the primary group and home directory of user username
...
Changing ownership of the directory /opt/5620sam/oracle12r1 to
username:group.
About to unlock the UNIX user [username]
Unlocking password for user username.
passwd: Success
Unlocking the UNIX user [username] completed

```

b. Enter No ↵; the following prompt is displayed:

```
Enter the Oracle user name:
```

Type a username and press ↵.

The following messages and prompt are displayed:

```

Oracle user [username] new home directory will be [/opt/5620sam/
oracle12r1].
Checking or Creating the Oracle user home directory /opt/5620sam/
oracle12r1...
Checking user username...
Adding username...
Changing ownership of the directory /opt/5620sam/oracle12r1 to
username:group.
About to unlock the UNIX user [username]
Unlocking password for user username.
passwd: Success
Unlocking the UNIX user [username] completed
Please assign a password to the UNIX user username ..
New Password:

```

21

Perform one of the following.

a. If you specify a new user in [Step 20](#) , the following prompt is displayed:

```
Please assign a password to the UNIX user username ..
```

```
New Password:
```

Perform the following steps.

1. Type a password and press ↵. The following prompt is displayed:

Re-enter new Password:

2. Retype the password and press ↵. The following message is displayed if the password update is successful:

```
passwd: password successfully changed for username
```

- b. If you specify an existing user in [Step 20](#) , the following prompt is displayed:

```
Do you want to change the password for the user username? [Yes/No]:
```

Type No ↵.

22

The following prompt is displayed:

```
Specify whether a 5620 SAM server will be installed on this
workstation.
The database memory requirements will be adjusted to account for the
additional load.
Will the database co-exist with a 5620 SAM server on this workstation
[Yes/No]:
```

Enter Yes or No, as required, and press ↵.

Messages like the following are displayed as the script execution completes:

```
INFO: About to set kernel parameters in /etc/sysctl.conf...
INFO: Completed setting kernel parameters in /etc/sysctl.conf...
INFO: About to change the current values of the kernel parameters
INFO: Completed changing the current values of the kernel parameters
INFO: About to set ulimit parameters in /etc/security/limits.conf...
INFO: Completed setting ulimit parameters in /etc/security/limits.
conf...
INFO: Completed running Oracle Pre-Install Tasks
```

23

Enter the following:

```
# yum install samb* ↵
```

The yum utility resolves any package dependencies, and displays the following prompt:

```
Total size: nn G
Installed size: nn G
Is this ok [y/N]:
```

24

Enter y ↵. The following is displayed, along with the installation status as the package is installed.

```

Downloading Packages:
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
The package installation is complete when the following is displayed:
Complete!

```

25

Enter the following:

```
# /opt/5620sam/samdb/install/bin/samrestoreDb.sh path ↵
```

where *path* is the absolute path of the database backup file set

The database restore begins, and messages are displayed as the restore progresses.

The following is displayed when the restore is complete:

```
DONE
```

26

When the database restore is complete, close the console window.

27

Start the primary main server.

1. Log in to the primary main server station as the samadmin user.

2. Enter the following:

```
bash$ cd /opt/5620sam/server/nms/bin ↵
```

3. Enter the following:

```
bash$ ./nmsserver.bash start ↵
```

4. Enter the following to check the server status:

```
bash$ ./nmsserver.bash -s nms_status ↵
```

The command returns server status information.

If the main server is not completely started, the first line of status information is the following:

```
Main Server is not ready...
```

The main server is completely started when the command returns the following:

```
-- Primary Server is UP
```

5. If the command output indicates that the server is not completely started, wait five minutes and then repeat [Step 26 4](#). Do not proceed until the server is completely started.

28

Enable the automatic primary main server startup.

1. Enter the following to switch to the root user:

```
bash$ su - ↵
```

2. Enter the following:

```
# cd /etc/init.d ↵
```

3. Enter the following:

```
# mv inactive.5620SAMServerWrapper 5620SAMServerWrapper ↵
```

29

Perform a full resynchronization of the network to discover the interim changes in the managed network.

30

Log in to the standby database station as the root user.

31

Remove any files that remain in the /opt/5620sam/samdb/tablespace and /opt/5620sam/samdb/archivelog directories.

32

Start the standby database.

1. Enter the following on the standby database station:

```
# cd /etc/rc3.d ↵
```

2. Enter the following:

```
# ./S965620SAMOracleProxyWrapper start ↵
```

3. Enter the following:

```
# ./S95db5620sam start ↵
```

Do not proceed until the following is displayed:

```
Done
```

33

Start the standby main server.

1. Enter the following on the standby main server station to switch to the samadmin user:

```
# su - samadmin ↵
```

2. Enter the following:

```
bash$ cd /opt/5620sam/server/nms/bin ↵
```


3. Enter the following:

```
bash$ ./nmserver.bash start ↵
```

4. Enter the following to check the server status:

```
bash$ ./nmserver.bash -s nms_status ↵
```

The command returns server status information.

If the main server is not completely started, the first line of status information is the following:

```
Main Server is not ready...
```

The main server is completely started when the command returns the following:

```
-- Standby Server is UP
```

5. If the command output indicates that the server is not completely started, wait five minutes and then repeat [Step 33 4](#). Do not proceed until the server is completely started.

34

Enable the automatic standby main server startup.

1. Enter the following to switch back to the root user:

```
bash$ exit ↵
```

2. Enter the following:

```
# cd /etc/init.d ↵
```

3. Enter the following:

```
# mv inactive.5620SAMServerWrapper 5620SAMServerWrapper ↵
```

35

To restore the 5620 SAM database redundancy, reinstantiate the primary database on the standby database station, as described in [14.32 “To reinstantiate a 5620 SAM database using a client GUI”](#) (p. 385) or [14.33 “To reinstantiate a 5620 SAM database using a CLI”](#) (p. 386).

END OF STEPS

14.32 To reinstantiate a 5620 SAM database using a client GUI

14.32.1 Purpose

Perform this procedure to reinstantiate a restored primary 5620 SAM database on a standby database station in a redundant 5620 SAM system using a client GUI.



Note: You require samadmin user privileges.

The 5620 SAM client GUI displays a progress indicator during the reinitiation, unlike a CLI-based reinitiation.

14.32.2 Steps

- 1 _____
Choose Administration→System Information from the 5620 SAM main menu. The System Information form opens.
- 2 _____
Click Re-Initiate Standby and confirm the action. The database reinitiation begins.

i

Note: The Re-Initiate Standby button may not display depending on your scope of command. See the *5620 SAM User Guide* for more information about scope of command.

 The client GUI status bar and the System Information form display the reinitiation status. The Standby Re-initiation State changes from In Progress to Success when reinitiation is complete. The Last Attempted Standby Re-initiation Time displays the start time of the current reinitiation.

END OF STEPS _____

14.33 To reinitiate a 5620 SAM database using a CLI

14.33.1 Purpose

Perform this procedure to reinitiate a restored 5620 SAM database on a standby database station in a redundant 5620 SAM system using CLI.



Note: The CLI script does not display a progress indicator during the reinitiation.

14.33.2 Steps

- 1 _____
Log in to the primary main server station as the samadmin user.

2 _____

Open a console window.

3 _____

Navigate to the `/opt/5620sam/server/nms/bin` directory.

4 _____

Enter the following:

```
./reinstantiatedb.bash -u username -p password ↵
```

where

username is the user name of a 5620 SAM client account that has the admin scope of command role

password is the password for the user account

The following prompt is displayed:

```
This action will rebuild the standby database.  
Do you want to proceed? (YES/no) :
```

5 _____

Enter the following case-sensitive text to begin the reinstantiation:

```
YES ↵
```

The 5620 SAM begins to reinstantiate the 5620 SAM database on the standby database station. Progress is indicated by a rolling display of dots in the console window.

6 _____

Close the console window when the reinstantiation is complete.

7 _____

Open a 5620 SAM GUI client to verify that the 5620 SAM main servers and databases are functional. The component status is displayed in the status bar.

END OF STEPS _____

5620 SAM database export and import

14.34 To export a 5620 SAM database

14.34.1 Purpose

Perform this procedure to export a 5620 SAM database to a file set.

You require the following user privileges:

- on each main server station:
 - root
 - samadmin
- on the standalone or primary database station:
 - root
 - Oracle management



CAUTION

Service Disruption

A database export operation requires a shutdown of each main server, which causes a network management outage.

You must perform this procedure only during a scheduled maintenance period.



Note: The passwords that you enter in this procedure are not displayed.

14.34.2 Steps

General preparation

1

Clear all outstanding failed deployments. See the “To view and manage failed deployments” procedure in the *5620 SAM User Guide* for information about how to clear a failed deployment.

2

Obtain the following 5620 SAM database information; in a redundant deployment, you must obtain the primary database information.

- Oracle database instance name
- Oracle database user password
- Oracle SYS user password

Stop main servers

3

Perform the following steps on each main server station to stop the main server.

i **Note:** In a redundant deployment, you must stop the standby main server first.

1. Log in to the main server station as the samadmin user:
2. Open a console window.
3. Enter the following:

```
bash$ cd /opt/5620sam/server/nms/bin ↵
```

4. Enter the following to stop the main server:

```
bash$ ./nmserver.bash stop ↵
```

5. Enter the following to display the main server status:

```
bash$ ./nmserver.bash appserver_status ↵
```

The command displays a status message.

6. The main server is stopped when the following is displayed:

```
Application Server is stopped
```

If the command displays a different message, wait five minutes and return to [Step 3 5](#) . Do not proceed until the server is stopped.

Run database export script

4

Log in to the 5620 SAM database station as the Oracle management user.

5

Open a console window.

6

If the directory that is to hold the database export file set does not exist, create the directory.

i **Note:** A 5620 SAM database export operation fails if the directory that is to contain the exported database file set does not exist.
The directory must be a directory on the local file system.

7

Enter the following:

```
bash$ /opt/5620sam/samdb/install/config/samdb/SAMDb_
exportImport.sh -e destination ↵
```

where *destination* is the absolute path of the directory that is to hold the database file set

i **Note:** To display the script usage, specify the `-h` option, as follows:
`SAMDb_exportImport.sh -h ↵`

The following prompt is displayed:

```
Using DB_INSTALL_BASE = /opt/5620sam/samdb/install
Please enter the ORACLE_SID (samdb1):
```

8

Specify the 5620 SAM database instance name and press `↵`. The following prompt is displayed:

```
Accept "instance_name" [y/n/q]? (y):
```

9

Press `↵` if the value is correct, or type `n ↵` to re-enter the value. The following messages and prompt are displayed:

```
Using ORACLE_SID = instance_name
Using ORACLE_HOME = /opt/5620sam/oracle12r1
Setting PATH to /usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/
usr/bin:/root/bin:/opt/5620sam/oracle12r1/bin
Enter the password for the "sys" user (terminal echo is off):
```

10

Enter the Oracle SYS user password and press `↵`.

The following prompt is displayed:

```
Accept value? [y/n/q] (y):
```

11

Press `↵` if you are sure that the password is entered correctly, or type `n ↵` to re-enter the value.

The following prompt is displayed:

```
Enter the password for database_user (terminal echo is off):
```

12

Enter the database user password and press `↵`.

The following prompt is displayed:

```
Accept value? [y/n/q] (y):
```

13

Press `↵` if you are sure that the password is entered correctly, or type `n ↵` to re-enter the value.

The following prompt is displayed:

Enter the export encryption password (terminal echo is off):

14

Create and record a database export encryption password. The password is required for a subsequent database import operation.



Note: The password can be of any length and use any characters.

15

Type the created password and press ↵.

The following prompt is displayed:

```
Confirm export encryption password (terminal echo is off):
```

16

Retype the password and press ↵.

The following message and prompt are displayed:

```
This tool will shutdown the db listener disconnecting any connections
to the database.
```

```
Have the SAM servers been shutdown? [y/n/q] (y):
```

17

Press ↵.

The following message and prompt are displayed:

```
To optimize the speed of the export this script will use as many CPUs
as you allow it to.
```

```
The maximum number of CPUs available are n
```

```
How many CPUs will be used for this export? (1):
```

where n is the number of CPUs that the script detects

18

Type the number of CPUs to use for the export operation, and press ↵.

The following prompt is displayed:

```
Accept value? [y/n/q] (y):
```

19

Type ↵.

The following prompt is displayed:

```
Do you want to perform an export size estimate first? [y/n/q] (y):
```

20

Press ↵ to direct the script to estimate the amount of disk space that the export requires.

The script displays an estimate of the required disk space, the available space in the partition that contains the destination directory, and the following prompt:

```
Do you have enough space? [y/n/q] (n):
```

21

Perform one of the following.

a. Confirm the space requirement and proceed with the export.

1. Type y ↵ if the partition has sufficient capacity to hold the exported file set.

The following prompt is displayed:

```
Proceed with the export? [y/n/q] (y):
```

2. Press ↵. The database export begins.

The script displays information that includes the export log filename and a series of progress indicators.

b. Press ↵ if the partition lacks sufficient capacity to hold the exported file set.

The following message is displayed and the script exits:

```
Cancelling export...
```

22

Close the open console windows, as required.

END OF STEPS

14.35 To import a 5620 SAM database

14.35.1 Purpose

Perform this procedure to import a 5620 SAM database from an exported file set.

You require the following user privileges:

- on each main server station:
 - root
 - samadmin
- on the standalone or primary database station:
 - root
 - Oracle management



CAUTION

Service Disruption

A database import operation requires a shutdown of each main server, which causes a network management outage.

You must perform this procedure only during a scheduled maintenance period.



Note: The passwords that you enter in this procedure are not displayed.

14.35.2 Steps

Stop main servers

1

Perform the following steps on each main server station to stop the main server.



Note: In a redundant deployment, you must stop the standby main server first.

1. Log in to the main server station as the samadmin user.
2. Open a console window.
3. Enter the following:

```
bash$ cd /opt/5620sam/server/nms/bin ↵
```

4. Enter the following to stop the main server:

```
bash$ ./nmserver.bash stop ↵
```

5. Enter the following to display the main server status:

```
bash$ ./nmserver.bash appserver_status ↵
```

The command displays a status message.

6. The main server is stopped when the following is displayed:

```
Application Server is stopped
```

If the command displays a different message, wait five minutes and return to [Step 1 5](#). Do not proceed until the server is stopped.

Install database

2

You can perform a 5620 SAM database import only on a station that has a newly installed 5620 SAM database.

1. If the station on which you are performing the import hosts a 5620 SAM database that is not newly installed, uninstall the database, as described in the *5620 SAM | 5650 CPAM Installation and Upgrade Guide*.

2. If the station on which you are performing the import has no 5620 SAM database installed, install a 5620 SAM database on the station, as described in the *5620 SAM | 5650 CPAM Installation and Upgrade Guide*.

Run database import script

3

Copy the exported database file set to the database station.

i **Note:** The directory to which you copy the file set must contain no other files. The Oracle management user requires read access to the database file set on the station.

4

Log in to the database station as the Oracle management user.

5

Open a console window.

6

Enter the following:

```
bash$ /opt/5620sam/samdb/install/config/samdb/SAMDb_
exportImport.sh -i source ↵
```

where *source* is the absolute path of the directory that contains the exported database file set

i **Note:** To display the script usage, specify the `-h` option, as follows:
`SAMDb_exportImport.sh -h ↵`

The following prompt is displayed:

```
Using DB_INSTALL_BASE = /opt/5620sam/samdb/install
Please enter the ORACLE_SID (samdb1):
```

7

Specify the 5620 SAM database instance name and press `↵`. The following prompt is displayed:

```
Accept "instance_name" [y/n/q]? (y):
```

8

Press `↵` if the value is correct, or type `n ↵` to re-enter the value. The following messages and prompt are displayed:

```
Using ORACLE_SID = instance_name
Using ORACLE_HOME = /opt/5620sam/oracle12r1
Setting PATH to /usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/
usr/bin:/root/bin:/opt/5620sam/oracle12r1/bin
Enter the password for the "sys" user (terminal echo is off):
```

9

Enter the Oracle SYS user password and press ↵.

The following prompt is displayed:

```
Accept value? [y/n/q] (y):
```

10

Press ↵ if you are sure that the password is entered correctly, or type n ↵ to re-enter the value.

The following prompt is displayed:

```
Enter the password for database_user (terminal echo is off):
```

11

Enter the database user password and press ↵.

The following prompt is displayed:

```
Accept value? [y/n/q] (y):
```

12

Press ↵ if you are sure that the password is entered correctly, or type n ↵ to re-enter the value.

The following prompt is displayed:

```
Enter the export encryption password (terminal echo is off):
```

13

Enter the database export encryption password created during the database export operation.

The following prompt is displayed:

```
Accept value? [y/n/q] (y):
```

14

Press ↵ if you are sure that the password is entered correctly, or type n ↵ to re-enter the value.

The following messages and prompt are displayed:

In order to optimize the speed of this import, this script needs to know how many CPUs are available on this machine and how many data files there are to import.

This machine appears to have n CPUs

Is this correct? [y/n/q] (y):

where n is the number of CPUs that the script detects

15

Type the number of CPUs to use for the export operation, and press ↵.

The following prompt is displayed:

```
Accept value? [y/n/q] (y):
```

16

Type ↵.

The following message and prompt are displayed:

```
There appears to be  $n$  data files to import
```

```
Is this correct? [y/n/q] (y):
```

where n is the number of data files found by the script

17

Press ↵ if the number of data files to import is correct.

The following message and prompt are displayed:

```
Log of import command will be written to log_file
```

```
Proceed with the import? [y/n/q] (y):
```

where *log_file* is the name of a log file that the script creates

18

Press ↵ to proceed with the database import.

The script generates messages like the following as it begins to import the 5620 SAM database.

```
Adding addition datafiles to existing tablespacesRestore wallet file
```

```
Restarting the database...
```

```
Shutting down the listener
```

```
Starting import: timestamp
```

where *timestamp* is the start time of the import operation

The script displays a series of progress indicators.

The following messages are displayed when the import operation is complete:

```
Executing recreate TI_BULK* packages body
Import done: timestamp
Starting up the listener
Here is the import log: log_file
```

where

log_file is the name of a log file that the script creates

timestamp is the start time of the import operation

19

Close the open console windows, as required.

END OF STEPS

Clearing inactive residential subscriber instances from the 5620 SAM database

14.36 General information

14.36.1 Overview

It is recommended that you periodically remove the inactive residential subscriber instance records from the 5620 SAM database. A residential subscriber instance becomes inactive when the associated subscriber is deleted from an NE. The inactive instances accumulate rapidly, for example, in a Wi-Fi offload deployment.



Note: Before you execute the script, it is recommended that you disable the GUI client timeout so that you can use the client GUI to monitor the script execution. Otherwise, if the execution takes longer than the GUI client timeout, you can monitor the script execution using the 5620 SAM user activity log.

14.37 To delete the inactive residential subscriber instances

14.37.1 Purpose

Perform this procedure to configure and execute a script that removes the inactive residential subscriber instance records from the 5620 SAM database.

14.37.2 Steps

If required, disable the GUI client timeout

- 1 _____
Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security — Security Management (Edit) form opens.
- 2 _____
Set the Client Timeout (minutes) parameter to 0, which specifies no timeout. Setting the parameter to 0 ensures that the 5620 SAM GUI client session does not close because of user inactivity while the script execution is in progress.
- 3 _____
Save your changes and close the form.


Configure a script bundle

- 4 _____
Choose Tools→Scripts from the 5620 SAM main menu. The Scripts form opens.
- 5 _____
Choose Script Bundle (Scripting) from the drop-down menu and click Search. A list of script bundles is displayed.
- 6 _____
If a subscriber instance deletion script bundle is listed, go to [Step 12](#) .
- 7 _____
Click Browse Examples. The Browse Examples of Scripts form opens.
- 8 _____
Navigate to the required bundle example. The path is Script Bundle Examples→Miscellaneous→Remove Inactive Residential Subscriber Instances Bundle.
- 9 _____
Select the bundle example and click Create Bundle. The Script Bundle (Create) form opens.
- 10 _____
Configure the Name parameter.
- 11 _____
Save your changes and close the forms.

Execute the script bundle

- 12 _____
Select the script bundle in the Scripts form and click Properties. The Script Bundle (Edit) form opens.
- 13 _____
Select Remove Residential Subscriber CTL and click Execute Script. The Execute Script form opens.

14 _____
Configure the parameter on the form to specify the number of days of inactivity that qualify a residential subscriber instance for deletion.

 **Note:** If the 5620 SAM forwards statistics or billing information to the 5670 RAM, ensure that the parameter value is greater than the billing period in days to ensure that no inactive subscriber instances are deleted before the billing occurs.

15 _____
Click Execute. The script execution begins.
While the script runs, a new item with an hourglass symbol is displayed in the navigation panel on the left side of the form. When the script execution is complete, the symbol changes to a green check mark.

16 _____
Close all forms.

17 _____
If required, restore the GUI client timeout to its original value.

END OF STEPS _____

Listing customer service information

14.38 General information

14.38.1 Overview

Record customer service information to:

- document which devices and interfaces are used to handle customer traffic
- provide raw data for post-processing customer trends and customer information

14.39 To save a list of service information

14.39.1 Steps

Generate a list of service information

1

Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2

Perform one of the following:

a. Generate a list of services in the network.

1. Specify a filter to narrow the services listed. You can filter based on service ID, customer name, or other criteria as required.
2. Order the columns of service data as required. For example, you can click on the Service Name heading to sort the services by name.

b. Generate a list of access interfaces on a service.

1. Select a service and click Properties. The service properties form opens.
2. Click on the Interfaces tab and select an interfaces tab. For example, you can click on the L3 Access Interfaces tab if it is available for the selected service type.
3. Order the columns of the interface data as required. For example, you can click on the Service Name heading to sort the access interface data based on the service name.

Save the list of service information

3

Right-click on a column header and choose Save To File. The Save form opens.

4 _____

Enter a filename and specify a file type.

5 _____

Browse to a location in which to save the file.

6 _____

Click Save. The service information is saved in the specified location.

7 _____

Close the forms.

END OF STEPS _____

Checking for duplicate service or resource names

14.40 General information

14.40.1 Overview

It is recommended that you develop standardized naming conventions before you configure network objects, in order to:

- facilitate identifying the object type
- ensure that data passed to a northbound OSS interface or southbound in a data file for processing is named consistently throughout the management domain

It is good practice to include information such as the following when creating or configuring an object using the object properties form:

- the object type; for example, VPRN
- a customer association to the object; for example, site 1.1.1.1 for XYZ Industries
- source and destination endpoint identifiers; for example, the devices at each end of an LSP
- ports and IP addresses used

You can check for duplicate names to ensure that naming conventions are followed and to help prevent confusion when you deal with customers or operations staff. [14.41 “To check for duplicate port descriptions” \(p. 403\)](#) uses ports as the objects to check for duplicate names.

14.41 To check for duplicate port descriptions

14.41.1 Purpose

Perform this procedure to check for duplicate object descriptions on all managed devices. This procedure uses ports as an example. You can also check logical entity names; for example, service or policy names. This procedure assumes that the Description parameter uniquely identifies each port.

14.41.2 Steps

- 1 _____
Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form appears.
- 2 _____
Generate a list of all ports:
 1. Choose Port (Physical Equipment) from the drop-down menu.


2. Configure the filter for the Administrative State column to display devices that are administratively up.

3

 Click on the Description heading to list ports alphabetically by description.

4

 Scan the list for duplicate names.

 **Note:** By default, ports are assigned a description based on the card type when the Description parameter is not configured.

5

 If you find a duplicate description, modify the description based on your naming conventions.

1. Select the port and click Properties. The Physical Port (Edit) form opens.
2. Configure the Description parameter to uniquely describe the port.
3. Save your changes and close the forms.

END OF STEPS

Configuring the OLC state of equipment or services

14.42 General information

14.42.1 Overview

Daily maintenance operations that are performed on NEs can cause a large number of alarms to be raised in the 5620 SAM. You can configure the OLC state on an object or service to specify whether the object is in maintenance or in-service mode to filter alarms in the alarm window.



Note: Alarms are generated for objects and services regardless of the Current OLC State parameter setting. The parameter setting is not sent to the network objects or services.

You can set the OLC state for the following objects and services:

- network elements
- power supply trays
- card slots
- daughter cards
- ports
- LAGs
- composite services
- services
- sites
- SAPs

In addition, you can specify on properties forms that the 5620 SAM reverts the OLC state to the in-service or maintenance mode after a specified time, depending on the current OLC state of the object or service. In addition, you can specify in NE discovery rules that the current OLC state reverts after the resynchronization is complete. You can specify that the 5620 SAM raises an informational alarm about the object OLC state reverting to the opposite state.

14.42.2 General information



CAUTION

Service Disruption

Changing the OLC state on an object also changes the OLC state on all of its child objects. The OLC state of the parent object will overwrite the OLC state of its children during shut down/turn up operation.

The operation may take several minutes to complete, depending on the number of objects affected. Alarms that occur before the object's OLC state is propagated may indicate incorrect OLC state.

Not all OLC state changes will be logged in the Task Manager during shut down/turn up operation.



Note: An NE shelf inherits the OLC state of the NE, and is read-only.

14.43 Setting the OLC state

14.43.1 Overview

The default value of the OLC state for NEs can be specified in the discovery rules. See the *5620 SAM User Guide* for more information about configuring the default OLC state for discovered network elements.

The OLC state default value of a child object is inherited from the parent object or service. The default value of the OLC state for composite services and services can be specified using the `nms-server.xml` file.

14.43.2 General information



CAUTION

Service Disruption

Unauthorized modification of the `nms-server.xml` file can seriously affect network management and 5620 SAM performance.

Contact technical support before you attempt to modify the file.

When the OLC state of an NE is set to the maintenance mode, all child objects such as access interfaces, card slots, daughter cards, and ports are set to maintenance mode. The sites on the NE are set to the maintenance mode.

When the OLC state of a composite service or service is set to the maintenance mode, the following related objects are changed:

- sites on which the services reside
- access interfaces (SAPs, L2 and L3 access interfaces)
- SDP Bindings (mesh, mirror and spoke bindings)

When the OLC state of a composite service or services is changed to in service, access interfaces and sites may not change to in service if they belong to equipment objects that are set to maintenance.

The OLC state of the parent object must be in service to change the OLC state of the child object. You can change the OLC state of the parent object regardless of the OLC state of the child object. However, when a child object has more than one parent object and the OLC state of one parent is set to maintenance, the child object is set to maintenance. The OLC state for a child object cannot be changed if one of the parent OLC states is set to maintenance.

You can configure the default OLC state for objects that become administratively down from the OLC tab on the System Preferences form. See [6.29 “To configure 5620 SAM system preferences” \(p. 198\)](#) .

See the *5620 SAM User Guide* for information about how to configure the OLC state for network objects, equipment objects, services, and sites.

You must add the OLC state property to manually created service templates, as described in [14.48 “To add the OLC state to a template using the GUI builder” \(p. 410\)](#) .

14.44 To view the OLC state of equipment or services

14.44.1 Steps

- 1 _____
Choose Administration→OLC from the 5620 SAM main menu. The OLC form opens.
- 2 _____
Choose a service or network object from the drop-down menu and click Search.
The form displays a list of objects based on the search criteria. The OLC state is listed in the left-most column.

END OF STEPS _____

14.45 To view the scheduling of OLC state changes of equipment or services

14.45.1 Steps

- 1 _____
Choose Administration→OLC from the 5620 SAM main menu. The OLC form opens.
- 2 _____
Click on the Schedules tab. A list of scheduled OLC state changes appears.
- 3 _____
View the following information:
 - object ID and name
 - current OLC state
 - OLC state to which the object reverts at the scheduled time
 - time when the OLC state reverts

-
- 4 _____
As required, select an entry and click Properties to view more information.

END OF STEPS _____

14.46 To change the OLC state of equipment or services



CAUTION

Service Disruption

Changing the OLC state can affect 5620 SAM performance and can take several minutes to complete.

Changing the OLC state of a parent object changes the OLC state of the child objects.

14.46.1 Steps

- 1 _____
Choose Administration→OLC from the 5620 SAM main menu. The OLC form opens.
- 2 _____
Choose a service or network object from the drop-down menu and click Search.
- 3 _____
Select an entry from the list and click OLC State→Maintenance or OLC State→In Service. You can select multiple objects at once.
The OLC state of the selected object changes in the filtered list panel.

i **Note:** You can configure the Revert OLC State parameter on the properties form for the object. The Revert OLC State parameter allows you to specify that the object automatically reverts to either the In Service mode or the Maintenance mode after a selected time, depending on the current OLC state of the object.
You can also configure the OLC state of a service or network object by configuring the OLC State parameter on the General tab of the object properties form.

- 4 _____
Close the form.

END OF STEPS _____

14.47 To view or change the OLC state from the alarm window

14.47.1 Steps

If required, create a filter

- 1 _____
Click on the filter icon in the alarm window. A filter form opens.
- 2 _____
Choose Assigned OLC State from the Attribute drop-down menu.
- 3 _____
Configure the filter form to search for alarms. See the *5620 SAM User Guide* for more information about creating search filters.

Change the OLC state of an alarm

- 4 _____
Select an alarm from the list. You can select multiple alarms at once.
- 5 _____
Right-click on the alarm and choose Assign OLC State. The OLC State Assignment form opens.
- 6 _____
Choose Maintenance or In service from the Assigned OLC State drop-down menu.

- 7 _____
Save your changes and close the form.

END OF STEPS _____

14.48 To add the OLC state to a template using the GUI builder

14.48.1 Purpose

Some service objects have an OLC state property. You cannot configure the OLC state property during the configuration of the service object. For 5620 SAM-created service templates, the OLC state property is automatically added to the template. For manually created service templates, the OLC state property is not added to the template.

Perform the following procedure to add the OLC state property to a manually created template.

14.48.2 Steps

- 1 _____
Open the GUI builder. See the *5620 SAM Scripts and Templates Developer Guide*.
- 2 _____
Create a combo box component and enter `olcState` for the Name combo box component attribute.
- 3 _____
Enter the value "maintenance" for the List combo box component attribute.
- 4 _____
Enter the value "inService" for the List combo box component attribute.
- 5 _____
Enter the value "maintenance" or "inService" for the Default combo box component attribute.
- 6 _____
Save your changes and close the forms.

END OF STEPS _____

Part V: Appendices

Overview

Purpose

This part provides information about the 5620 SAM scope of command roles and permissions.

Contents

Appendix A, Scope of command roles and permissions	413
--	-----

A Scope of command roles and permissions

A.1 Overview

A.1.1 Purpose

Appendix A describes the scope of command roles and permissions.

A.1.2 Contents

A.2 Predefined scope of command profiles and roles	413
A.3 Permissions assignable to 5620 SAM scope of command roles	416
A.4 Permissions access for scope of command roles	453

A.2 Predefined scope of command profiles and roles

A.2.1 General information

This appendix describes the predefined 5620 SAM scope of command profiles and roles, and the access permissions for each predefined role. Predefined scope of command profiles and roles cannot be deleted.

Table 19 Summary of command profiles, roles, and permission information

Table	Description
Table 20, "Predefined scope of command profiles" (p. 414)	Lists the predefined scope of command profiles, the assigned roles for each profile, and a description for each profile.
Table 21, "Predefined scope of command roles" (p. 414)	Lists the 5620 SAM predefined scope of command roles and provides a description of the user security access provided for each role.
14.3 "Permissions assignable to 5620 SAM scope of command roles" (p. 416)	Lists the permissions that can be assigned to a 5620 SAM scope of command role and a description of the permission.
14.4 "Permissions access for scope of command roles" (p. 453)	Describes the access levels that can be assigned for permissions in a scope of command role, and how to view the permission configuration of a role.

A.2.2 Predefined scope of command profiles

Table 20 Predefined scope of command profiles

Profile name	Assigned roles	Description
admin	Administrator	Default administrative scope of command profile with access to all menus accessible from the 5620 SAM GUI with the exception of LI menu functions. This profile also has no OSSI access.

A.2.3 Predefined scope of command roles

Table 21 Predefined scope of command roles

Role	Access provided
Base Read-only	Read-only to all objects except for the objects in the SAM Security and Mirror Service Management roles.
Administrator	GUI access, but no OSSI access, to all objects. Create, modify, delete, import, and export public workspaces. View private or public workspaces in the Manage Workspaces list.
User Management	5620 SAM user and group management. Create, modify, delete, import, and export public workspaces. View private or public workspaces in the Manage Workspaces list.
SAM Management and Operations	Database functions such as backup, restore, reinstantiation, and switchover. Alarm administration such as acknowledgement, clearing, and setting severity-change thresholds. General NE management functions such as discovery, deployment, mediation, polling, statistics management, and security management that includes modifying spans. Create, modify, delete, import, and export public workspaces. View private or public workspaces in the Manage Workspaces list.
Network Element Equipment Management	Physical equipment configuration and management.
Service Management	Service, service component, and service template management functions, excluding mirror-service management.
Old Service Template Management	Management of service templates deprecated; see Template Script Management in this table.
Subscriber Management	Customer and residential subscriber management.

Table 21 Predefined scope of command roles (continued)

Role	Access provided
QoS/ACL Policy Management	General QoS and ACL policy management, Ethernet service and time of day suite policy management.
Policy Management (except QoS/ACL)	Management of policies other than those in the QoS/ACL Policy Management role.
Routing Management	Routing protocol, L2 forwarding, and bandwidth management.
Tunnel Management	Service tunnel and underlying transport management.
SAM Management and Operations	Database management (Backups, Reinstantiation, and Switchovers), Alarm acknowledgement, Alarm clearing, and Severity Change Thresholds, Router administration (Scheduling, Backup Policies, Upgrade Policies, Deployment Policies, and Management Ping Policies), NE Security, LPS, and Mediation Policies, SNMP Poller/Stats Polices, Event Notification Policies, MIB Policies, SNMP Performance Statistics, SAM Performance Statistics, Statistics Plotter, Usage and Activity Records, and Span configuration.
Network Element Software Management	NE software management functions.
Fault Management	Functions such as alarm management and remote network monitoring.
Service Test Management	STM functions such as creating, running and scheduling OAM tests.
Script Management	XML API and CLI script management, excluding execution.
Script Execution	XML API and CLI script execution.
Mirror Service Management	Creation and management of mirror services and mirror-service components using the GUI.
OSS Management	Use of the OSSI.
Telnet/SSH Management	Telnet or SSH access to NEs from the GUI.
CPAM Management	Route Analysis of ISIS Topology, OSPF Topology, MPLS Topology, IP Path monitoring, LSP Monitoring, Checkpoints, and Impact Analysis Scenarios for CPAM management.
CPAM OSS PCA	Route Analysis of ISIS Topology, OSPF Topology, and MPLS Topology for CPAM routing.
CPAM Topology Simulator	Route Analysis of ISIS Topology, OSPF Topology, and MPLS Topology for CPAM Topology Simulator.
Root Cause Analysis (RCA) Object Verification	RCA functions.
Lawful Interception Management	LI configuration for mirror services, mediation policies, and NE security.
Template Script Management	Service and tunnel template script management.
Service Template Script Execution	Service template script execution.

Table 21 Predefined scope of command roles (continued)

Role	Access provided
Tunnel Template Script Execution	Tunnel template script execution.
Application Assurance (AA) Management	AA policy management.
Format and Range Policy Management	Format and range policy management, service-creation span rules.
Work Order Activation	The ability to perform CM work order activation.
Configuration Snapshot Export	The ability to perform export CM configuration snapshots.
Create and Delete Access	The ability to create and/or delete eNodeB objects via 5620 SAM-O.
Configuration Management which causes node reset	The ability to configure objects which causes a full or partial reset of the node.
EPC Operator	Read and write permission on all Evolved Packet Core classes.
eNodeB NEM Operator	The ability to launch the 9400 NEM (parameter configuration tool for the eNodeB) from the 5620 SAM client GUI.
Statistics Plotter Profile Management	Management of all Statistics Plotter profiles.
Admin Neto Launch	The ability to open the NEtO with the administration profile.
Viewer Neto Launch	The ability to open the NEtO with the viewer profile.
Default Neto Launch	The ability to open the NEtO with the null profile.
Ageout Constraint Policy Management	The ability to configure Ageout Constraint Policies.
Purge Records	The ability to purge historical records from the 5620 SAM such as statistics logs, event logs, etc.

A.3 Permissions assignable to 5620 SAM scope of command roles

A.3.1 Permissions assignable to 5620 SAM scope of command roles

Table 22 Permissions assigned to 5620 SAM scope of command roles

Package.Class.Method/Property	Description
aaa	AAA - Configurations for authentication, authorization, and accounting.
aaa.RadiusProxyInterface	RADIUS Proxy Interface - Access to Radius Proxy Interface configuration.
aaa.RadiusProxyServer	RADIUS Proxy Server - Access to Radius Proxy Server configuration.

Table 22 Permissions assigned to 5620 SAM scope of command roles (continued)

Package.Class.Method/Property	Description
aaa.RadiusServer	RADIUS Server - Access to Radius Server configuration.
aapolicy	Application Assurance - AA policies, configuration, protocol, group, filter, and profiles.
aapolicy.DbInfoTransitSubscriberManager.property_dbInfoTransIpAddrRtrvTimeOut	Db Info Transit Subscriber Manager - property_dbInfoTransIpAddrRtrvTimeOut - Service preferences can only be modified by a user with an administrator role.
aapolicy.DbInfoTransitSubscriberManager.property_dbInfoTransPrfxAddrRtrvTimeOut	Db Info Transit Subscriber Manager - property_dbInfoTransPrfxAddrRtrvTimeOut - Service preferences can only be modified by a user with an administrator role.
aapolicy.DbInfoTransitSubscriberManager.property_dbInfoTransSubscrRtrvMax	Db Info Transit Subscriber Manager - property_dbInfoTransSubscrRtrvMax - Service preferences can only be modified by a user with an administrator role.
accessuplink	Access Uplink - Configuration of 7210 Access Uplink Specifics for physical ports and LAG interfaces.
accounting	Accounting Policy - Statistics Accounting Policies.
aclfilter	ACL Filter Policy - MAC, IP, and IPv6 ACL Filters.
aclfilterli	ACL Filter LI - All configurations for mirroring of packets matching entries of Lawful intercept ACL filters to mirror destinations.
activation	Activation - Used to define, manage, and deploy work orders used in activation.
activation.Session	Activation Session - Used to manage activation sessions and activate work orders.
activation.Snapshot	Snapshot - Used to manage CM configuration snapshots.
activation.SnapshotEntity	Snapshot Entity - Used to manage snapshot entities.
activation.WebDAVSharedData	Activation. Web DAVShared Data - Ability to restrict access to CM data (CM work orders and configuration snapshots) via the WebDAV protocol.
activation.WorkOrder	Work Order - Used to manage work orders.
aengr	Access Egress Policy - Access Egress QoS Policies.
ageoutcstr	Ageout Constraint - Configurations related to Ageout Constraint.
aingr	Access Ingress Policy - Access Ingress QoS Policies.
ancp	ANCP - Access Node Control Protocol (ANCP) policy and configuration.

Table 22 Permissions assigned to 5620 SAM scope of command roles (continued)

Package.Class.Method/Property	Description
ancp.AncpLoopback	ANCP Loopback - Access to ANCP Loopback tests, ANCP Loopback test definitions, and ANCP Loopback deployed tests.
antispoof	Anti-Spoofing - Anti-Spoofing for L2/L3 Access Interfaces and Filter configuration.
aosqos	AoS QoS - Quality of Service for Application over Signaling (AoS QoS) Policy and conditions, AoS QoS configuration for Physical Port and Layer 2 Bridge.
aosredundancy	Aos-Redundancy - AOS Multichassis.
aossas	AOS SAS - OAM tests specific to AOS nodes.
aossas.CPETestGroupHead	CPE SLA Test Group - Access to CPE SLA tests, CPE SLA test definitions, and CPE SLA deployed tests.
aossas.CPETestHead	CPE SLA Test - Access to CPE SLA tests, CPE SLA test definitions, and CPE SLA deployed tests.
apipe	APipe - All contained objects are listed. Package access is not currently used.
apipe.Apipe	Apipe Service - Access to VLL ATM Pipe (Apipe) Service objects themselves.
apipe.Site	Apipe Site - Access to Apipe Sites.
aps	APS - Automatic Protection Switching (APS) Groups.
arp	ARP - ARP host and configurations on service interfaces.
atm	ATM - ATM configuration for Service interfaces and routers, ATM Connections, ILMI Link, and other ATM related objects.
atm.AtmPing	ATM Ping - Access to ATM Ping tests, ATM Ping test definitions, and ATM Ping deployed tests.
atmpolicy	ATM QoS Policy - ATM Traffic Descriptor Policy.
audit	Resource Audit - Ability to execute audits and view audit results.
autoconfig	Automatic Configuration - Auto-Config Source and Target Node Profiles.
autoconfig.AutoConfigScriptManager.method_configure	Automatic Configuration - method_configure - Ability to create/modify/delete an auto-config script.
autoconfig.AutoConfigScriptManager.method_copyContents	Automatic Configuration - method_copyContents - Ability to copy the contents of one auto-config script to new one.
bfd	BFD - Bi-Directional Forwarding Detection (BFD) can be configured on rtr.NetworkInterface, ies.L3AccessInterface, vprn.L3AccessInterface and vprn.NetworkInterface.

Table 22 Permissions assigned to 5620 SAM scope of command roles (continued)

Package.Class.Method/Property	Description
bgp	Routing Management: BGP - Border Gateway Protocol (BGP) configuration for routers, policies, peers, groups, MD5, and Confederations.
bgp.Site	BGP Site - Access to a BGP protocol site on a router.
bulk	Bulk Operations - Not currently used.
bulk.BulkChange	Bulk Change - The ability to create, modify, and/or delete bulk changes.
bulk.BulkManager.method_execute	Bulk Operations Manager - method_execute - The ability to execute bulk operations.
bulk.BulkManager.method_generateBatches	Bulk Operations Manager - method_generateBatches - The ability to generate batches for bulk operations.
bundle	Bundle - Bundle configuration for T1/E1 Multilink Group and channel members, APS, Multichassis and Service interfaces.
cac	CAC - CAC configuration for Physical Links, Physical Port and other CAC related objects.
calltrace.WebDAVSharedData	Calltrace. Web DAVShared Data - Ability to restrict access to call traces via the WebDAV protocol.
ccag	CCAG - Cross-Connect Aggregation Group (CCAG) MDA card and forwarding path configuration.
cflowd	Cflowd - CFLOWD Objects.
cflowd.NeCflowd	Cflowd Configuration - Ability to configure cflowd params for SR.
cflowd.NeCollector	Cflowd Collector Configuration - Ability to configure collector for cflowd params for SR.
clear	Clear - Clear application commands and requests.
cli	CLI - Ability to connect to open NE sessions from SAM.
cli.SSH	Cli. SSH - Ability to open an SSH Telnet session to the node from SAM.
cli.Telnet	Cli. Telnet - Ability to open a Telnet session to the node from SAM.
connprof	Connection Profile - Connection Profile configuration.
cpipe	CPipe - Access to this package is for configuring CES Interface Specifics for Cpipe specific SAPs.
cpipe.Cpipe	Cpipe Service - Access to VLL Circuit Emulation Pipe (Cpipe) Service objects themselves.

Table 22 Permissions assigned to 5620 SAM scope of command roles (continued)

Package.Class.Method/Property	Description
cpipe.Site	Cpipe Site - Access to Cpipe Sites.
crdtctrl	Credit Control - Credit Control configuration.
customproperties	Custom Properties - Custom properties configuration.
db	Database - Configuration for Size constraint policies and Database file policies.
db.AuxiliaryDatabase.method_reinstantiationDatabase	Auxiliary Database - method_reinstantiationDatabase - Ability to perform a auxiliary database instantiation.
db.AuxiliaryDatabase.method_snapshotDatabase	Auxiliary Database - method_snapshotDatabase - Ability to perform a auxiliary database snapshot.
db.DatabaseManager.method_backup	Database Manager - method_backup - Ability to perform a database backup.
db.DatabaseManager.method_reinstantiateStandby	Database Manager - method_reinstantiateStandby - Ability to re-instantiate the standby database.
db.DatabaseManager.method_snapshotAllDatabases	Database Manager - method_snapshotAllDatabases - Ability to perform a auxiliary database snapshot.
db.DatabaseManager.method_switchover	Database Manager - method_switchover - Ability to perform a database switchover.
db.SnapshotHistory.method_deleteSnapshot	Snapshot History - method_deleteSnapshot - Ability to delete a auxiliary database snapshots.
dctr	Data Center - Data Center information and configurations.
dctr.PortProfile	Port Profile - Configuration of Port Profile.
dctr.VirtualSpokeSdpBinding	Virtual Spoke SDP Binding - Access to Virtual Spoke SDP Binding configuration.
dctr.VlanRange	VLAN Range - Configuration of Vlan Entry.
dctr.VplsVirtualSite	Virtual Site VPLS - Access to VPLS eVPN-Sites on a VPLS Service.
dctr.VprnVirtualSite	Virtual Site VPRN - Access to VPLS eVPN-Sites on a VPLS Service.
dhcp	DHCP - Dynamic Host Configuration Protocol (DHCP) Server for rtr.VirtualRouter and vprn.Site.
diameter	Diameter - Access to this package is for configuring Diameter related configurations, e.g. Diameter Policy.
dns	Domain Name System - Domain Name System.
dynsvc	Dynamic Services - Dynamic Services Configuration.

Table 22 Permissions assigned to 5620 SAM scope of command roles (continued)

Package.Class.Method/Property	Description
entity	Physical Entity Management.
epipe	EPIPE - Access to this package is for configuring CES Interface Specifics and FR Interface Specifics for Epipe specific SAPs.
epipe.Epipe	Epipe Service - Access to VLL Ethernet Pipe (Epipe) Service objects themselves.
epipe.PbbMacName	PBB MAC Name - Ability to configure the MAC Name Address for a Network Element.
epipe.Site	Epipe Site - Access to Epipe Sites.
equipment	Physical Equipment - General equipment configuration.
equipment.PortPolicy	Port Policy - Access to Port Policy for 7750 nodes.
equipment.Shelf.method_rebootUpgrade	Shelf - method_rebootUpgrade - Ability to perform node reboot upgrade.
ethernetequipment	Ethernet Equipment - Ethernet Equipment configuration.
ethernetoam	Ethernet OAM - Maintenance Domains and Maintenance Entity Groups, autogeneration of the MEPs on each SAP or Binding in a Service.
ethernetoam.CcmTest	CFM Continuity Check - Access to Continuity Check tests, Continuity Check test definitions, and Continuity Check deployed tests.
ethernetoam.CcTest	Global Maintenance Entity Group - Access to Continuity Check tests, Continuity Check test definitions, and Continuity Check deployed tests.
ethernetoam.CfmDmmBin	CFM DMM Session Bin - Access to CFM DMM Test Session, CFM DMM Test Session definitions.
ethernetoam.CfmDmmSession	CFM DMM Test Session - Access to CFM DMM Test Session, CFM DMM Test Session definitions.
ethernetoam.CfmEthTest	CFM Eth Test - Access to CFM EthTests, CFM EthTest definitions, and CFM EthTest deployed tests.
ethernetoam.CfmLinkTrace	CFM Link Trace - Access to Link Trace tests, Link Trace test definitions, and Link Trace deployed tests.
ethernetoam.CfmLmmSession	CFM LMM Test Session - Access to CFM LMM Test Session, CFM LMM Test Session definitions.
ethernetoam.CfmLmTest	CFM LM Test - Access to CFM LM tests, CFM LM test definitions, and CFM LM deployed tests.

Table 22 Permissions assigned to 5620 SAM scope of command roles (continued)

Package.Class.Method/Property	Description
ethernetoam.CfmLoopback	CFM Loopback - Access to CFM Loopback tests, CFM Loopback test definitions, and CFM Loopback deployed tests.
ethernetoam.CfmOneWayDelayTest	CFM One Way Delay Test - Access to CFM One Way Delay tests, CFM One Way Delay test definitions, and CFM One Way Delay deployed tests.
ethernetoam.CfmOneWaySlm	CFM One Way SLM Test - Access to CFM One Way SLM tests, CFM One Way SLM test definitions, and CFM One Way SLM deployed tests.
ethernetoam.CfmSingleEndedLossTest	CFM Single Ended Loss Test - Access to CFM Single Ended Loss tests, CFM Single Ended Loss test definitions, and CFM Single Ended Loss deployed tests.
ethernetoam.CfmSlmSession	CFM SLM Test Session - Access to CFM SLM Test Session, CFM SLM Test Session definitions.
ethernetoam.CfmTwoWayDelayTest	CFM Two Way Delay Test - Access to CFM Two Way Delay tests, CFM Two Way Delay test definitions, and CFM Two Way Delay deployed tests.
ethernetoam.CfmTwoWaySlm	CFM Two Way SLM Test - Access to CFM Two Way SLM tests, CFM Two Way SLM test definitions, and CFM Two Way SLM deployed tests.
ethernetoam.EthSession	Ethernet Test Session - Access to Ethernet Test Session, Ethernet Test Session definitions.
ethernet-service	Ethernet Service Policy - SAP Profile and UNI Profile policies.
ethernet-tunnel	Ethernet Tunnel - Ethernet Tunnel configuration.
ethring	Ethernet Ring - Ethernet Ring Configuration.
event	events - Parent package for all event classes.
fabric-qos	Fabric QoS Policies - Fabric Profile QoS policy.
femto	FEMTO - All Femto BSR configurations and status.
femto-lte-call-profile	FemtoLteCallProfile - Femto Lte Callp Profile.
femto-lte-local-override	FemtoLteLocalOverride - Femto LTE Local Override.
femto-lte-oam-profile	FemtoLteOAMProfile - Femto Lte OAM Profile.
femto-lte-rrm-profile	FemtoLteRRMProfile - Femto Lte RRM Profile.
femto-lte-transport-profile	femtoLteTransportProfile - Femto Lte Transport Profile.
femto-perf	Femto Performance Management - Performance counter collection for NEs in Femto Network.

Table 22 Permissions assigned to 5620 SAM scope of command roles (continued)

Package.Class.Method/Property	Description
file	File Policy - File creation on the NE for events and accounting.
filter	Filter - Public search filters.
filterprefixlist	Filter Policy - Filter PrefixList and PortList Policies.
firewall	Firewall - All Firewall configurations.
fm	Fault Management - Alarm policies, Severity change thresholds, Alarms, Notes, and History.
fm.AlarmHistoryDatabase.method_purge	Alarm History Database - method_purge - Ability to purge the alarm history database.
fm.FaultManager	Fault Manager - Access to assign OLC state, alter severity, clear, acknowledge, and remove faults.
fm.FaultManager.method_editNote	Fault Manager - method_editNote - Ability to edit an alarm note.
fm.GlobalPolicy	Global Alarm Behavior - Access to configure the global alarm behavior.
fm.SpecificPolicy	Specific Alarm Policy - Access to configure specific alarm policies.
fpipe	FPipe - All contained objects are listed. Package access is not currently used.
fpipe.Fpipe	Fpipe Service - Access to Frame Relay Pipe (Fpipe) Service objects themselves.
fpipe.Site	Fpipe Site - Access to Fpipe Sites.
fr	Frame Relay - Frame Relay configuration for Service interfaces and routers.
generic	Generic - Generic configuration for SAM objects, deployment, and administrative state changes for DHCP and Multichassis objects, Maintenance Association End Points (MEP), and SRRP instances.
generic.GenericObject.method_collectData	Generic Object - method_collectData - Ability to collect and plot real-time statistics.
genericlog	Log Viewer - Display logs in Log Viewer.
genericne	Generic NE - Generic NE Interface and Profile configuration.
genericne.GenericNeProfileManager.method_checkFileContent	Generic NE Profiles - method_checkFileContent - Checks the descriptor installation package content for validity.
genericne.GenericNeProfileManager.method_installFile	Generic NE Profiles - method_installFile - Ability to install a descriptor driver.

Table 22 Permissions assigned to 5620 SAM scope of command roles (continued)

Package.Class.Method/Property	Description
gmpls	ASON Domain Management - GMPLS Management.
gmplsuni	GMPLS-UNI - GMPLS-UNI Configuration.
gsmp	GSMP - General Switch Management Protocol (GSMP) configuration for VPLS, MVPLS and VPRN routing instances.
hip	Horizontal Integration Protocol - Access to HIP managed Element Managers and subtending nodes.
hip.EMServer	Element Manager - Access to HIP managed Element Managers.
hip.EMSystem	EM System - Access to HIP managed EM Systems.
histcorr	Historical Correlation - Historical Correlation configuration.
hpipe	HPipe - All contained objects are listed. Package access is not currently used.
hpipe.Hpipe	Hpipe Service - Access to HPipe (Hpipe) Service objects themselves.
hpipe.Site	Hpipe Site - Access to Hpipe Sites.
icmp	ICMP - Internet Control Message Protocol (ICMP) and Domain Name System (DNS) test results.
icmp.DnsPing	DNS Ping - Access to DNS Ping tests, DNS Ping test definitions, and DNS Ping deployed tests.
icmp.IcmpPing	ICMP Ping - Access to ICMP Ping tests, ICMP Ping test definitions, and ICMP Ping deployed tests.
icmp.IcmpTrace	ICMP Trace - Access to ICMP Trace tests, ICMP Trace test definitions, and ICMP Trace deployed tests.
ies	IES - Access to this package is for configuring Group Interfaces, SAPs, MSAPs, IGMP Host Tracking on Sites and SAPs, and FR Interface Specifics for IES specific SAPs.
ies.AaInterface	IES AA Interface - Access to IES AA Interfaces.
ies.Ies	IES Service - Access to Internet Enhanced Service (IES) Service objects themselves.
ies.L3AccessInterface	IES L3 Access Interface - Access to IES L3 Access Interfaces.
ies.Site	IES Site - Access to IES Sites.
ies.SubscriberInterface	IES Subscriber Interface - Access to IES Subscriber Interfaces.
igh	IGH - Interface-Group-Handlers.

Table 22 Permissions assigned to 5620 SAM scope of command roles (continued)

Package.Class.Method/Property	Description
igmp	IGMP - Internet Group Management Protocol (IGMP) configuration for Service interfaces and routers.
igmp.Site	IGMP Site - Access to IGMP Sites.
impact.FullReset	Impact. Full Reset - Ability to configure objects which will result in a full reset of the node. Currently applies to 9412 node.
impact.PartialReset	Impact. Partial Reset - Ability to configure objects which will result in a partial reset of impacted SW/HW unit. Currently applies to 9412 node.
ipfix	IPFIX - IPFIX Policy.
ipipe	IPipe - Access to this package is for configuring IPCP on L2 Access Interfaces and FR Interface Specifics for Ipipe specific SAPs.
ipipe.Ipipe	Ipipe Service - Access to IP Interworking Pipe (Ipipe) Service objects themselves.
ipipe.L2AccessInterface	L2 Access Interface - Access to IPipe L2 Access Interfaces.
ipipe.Site	Ipipe Site - Access to Ipipe Sites.
ipsec	IP Security - IKE Policy and IPsec Transform.
isa	ISA - ISA-IPsec, ISA-MG, and ISA-AA configuration on a MDA card for IP Security, LTE, and Application Assurance.
isa.IPSecMgIlsaGroup	ISA IPSMG Group - Configuration of IPsec ISA-MG Group.
isa.IPSecMgIlsaGroupMdaAssociation	ISA-IPSMG Group MDA Association - Configuration of ISA-IPSMG Group MDA Association.
isa.MgGroupMember	ISA-MG Group Member - Configuration of ISA-MG Group Member.
isa.MgIlsaGroup	ISA-MG Group - Configuration of ISA-MG Group.
isis	Routing Management: ISIS - IS-IS configuration for Service interfaces and routers, Area, Adjacency, Neighbors, Policies and other IS-IS related objects.
l2fib	L2 FIB - Layer 2 Forwarding Information Base (FIB) configuration for Multicast and Non-Multicast.
l2fwd	L2 Forwarding - All Layer 2 Forwarding configuration for Service interfaces and routers, circuits, ports, Spanning Tree, Registration, FIB, Mac Protection, IGMP Snooping, etc.
l2tp	L2TP - L2TP configuration for Service interfaces and routers, Groups, Tunnels, PeersRPs, and other L2TP related objects.

Table 22 Permissions assigned to 5620 SAM scope of command roles (continued)

Package.Class.Method/Property	Description
l3fwd	L3 Forwarding - All Layer 3 Forwarding configuration for Service interfaces and routers, Import and Export policies, Dot1p and DSCP for VPRNs.
lag	LAG - Link Aggregation Group (LAG) configuration for Service interfaces and routers.
layer2	Layer 2 - All Layer 2 configuration: Bridges, Transparent LAN Service (TLS), and VLAN interfaces.
ldp	Routing Management: LDP - Label Distribution Protocol (LDP) configuration for Service interfaces and routers, Session, MD5 Key, Equal-Cost Multipath Routing (EMCP), Forwarding Equivalency Class (FEC), Policies, and Peers.
lldp	LLDP - Link Layer Discovery Protocol (LLDP) configuration on equipment.PhysicalPort.
lmg	LMG - All LMG configurations and status.
lmp	LMP - LMP Configuration for Sites.
localuserdb	Local User DB - DHCP or PPPoE configuration for Local User Databases on a router.
log	Statistics - Parent package for all statistics classes.
log.LogToFileManager.property_jmsRetries	Log To File Manager - property_jmsRetries - LogToFile preferences can only be modified by a user with an administrator role.
log.LogToFileManager.property_retention	Log To File Manager - property_retention - LogToFile preferences can only be modified by a user with an administrator role.
log.LogToFileManager.property_rollover	Log To File Manager - property_rollover - LogToFile preferences can only be modified by a user with an administrator role.
lps	LPS - Learned Port Security (LPS) configuration for layer2.Bridge and MAC Entries for ports.
lte	LTE - All LTE configurations and status.
lte.ApnFqdnGroupList	FQDN Group List - Configuration of FQDN Group List.
lte.ApnFqdnIpEntry	FQDN IP Entry - Configuration of FqdnGroup IP Entry.
lte.ApnPolicyRuleBase	Policy Rule Base - Configuration of Policy Rule Base.
lte.ApnTaiLaiList	TAI-LAI List Binding - Configuration of TAI-LAI List Binding.
lte.CallTraceDirectory	Call Trace Directory - Configuration of Call Trace Directory.
lte.DccaProfile	DCCA Profile - Configuration of DCCA Profile.

Table 22 Permissions assigned to 5620 SAM scope of command roles (continued)

Package.Class.Method/Property	Description
Ite.DiameterPeerListEntry	Diameter Peer List Entry - Configuration of Diameter Peer List Entry.
Ite.DiameterPeerProfile	Diameter Peer Profile - Configuration of Diameter Peer Profile.
Ite.DiameterProfile	Diameter Profile - Configuration of Diameter Profile.
Ite.DiscoveryLog	Drill Down Log - Creation of Drill Down Log.
Ite.DupRadiusAccServerGroup	Duplicate Accounting RADIUS Server Group - Configuration of Serving Gateway APN.
Ite.ENBEquipment.method_launchNEM	ENB Equipment - method_launchNEM - Ability to launch NEM.
Ite.EPSPathDiscoveredLinkComponent	EPS Path Discovery Link Component - Configuration of EPS Path Discovery Link Component.
Ite.EPSPathDiscoveryHint	EPS Path Drill Down Hint - Configuration of EPS Path Drill Down Hint.
Ite.EPSPathDiscoveryProfile	Path Drill Down Profile - Configuration of Path Drill Down Profile.
Ite.EPSPathInterfaceComponent	EPS Path Interface Component - Configuration of EPS Path Interface Component.
Ite.EPSPathLinkComponent	EPS Path Link Component - Configuration of EPS Path Link Component.
Ite.EPSPathSapComponent	EPS SAP Component - Configuration of EPS SAP Component.
Ite.EPSPathSegment	EPS Path Segment - Configuration of EPS Path Segment.
Ite.EPSPathServiceComponent	EPS Path Service Component - Configuration of EPS Path Service Component.
Ite.EPSPathSiteComponent	EPS Path Site Component - Configuration of EPS Path Site Component.
Ite.FqdnGroupProfile	FQDN Group Profile - Configuration of FQDN Group Profile.
Ite.FqdnNameEntry	FQDN Name Entry - Configuration of FQDN Name Entry.
Ite.GtpPrimaryServerListEntry	GTP Primary Server List Entry - Configuration of GTP Primary Server List Entry.
Ite.GtpPrimeServerGroupProfile	GTP Prime Server Group Profile - Configuration of GTP Prime Server Group Profile.
Ite.GtpProfile	GTP Profile - Configuration of GTP Profile.
Ite.IpPool	IP Address Pool - Configuration of IP Address Pool.
Ite.IpPoolBinding	IP Address Pool Binding - Configuration of IP Address Pool Binding.

Table 22 Permissions assigned to 5620 SAM scope of command roles (continued)

Package.Class.Method/Property	Description
Ite.IpPoolEntry	IP Address Pool Entry - Configuration of IP Address Pool Entry.
Ite.IpPoolTaiLaiBinding	TAI-LAI List IP Address Pool Binding - Configuration of TAI-LAI List IP Address Pool Binding.
Ite.LTEEquipment.method_launchQoSAnalyzer	Lte. LTEEquipment - method_launchQoSAnalyzer - Ability to launch LTE QoS Analyzer.
Ite.MobileNodeRegion	Mobile Node Region/Public Land Mobile Network (PLMN) - Configuration of Mobile Node Region.
Ite.NETCELlinkState	TCE Assignment Status of eNodeB - TCE Assignment Status of eNodeB.
Ite.PcmdProfile	PCMD Profile - Configuration of PCMD Profile.
Ite.PdnApn	PDN APN - Configuration of PDN APN.
Ite.PDNGateway	PDN Gateway - Configuration of PDN Gateway.
Ite.PdnGxReferencePoint	PDN Gx Reference Point - Configuration of Pdn Gx Reference Point.
Ite.PdnRfReferencePoint	PDN Rf Reference Point - Configuration of PGW Rf Reference Point.
Ite.PdnS5ReferencePoint	PDN S5 Reference Point - Configuration of PGW S5 Reference Point.
Ite.PdnS8ReferencePoint	PDN S8 Reference Point - Configuration of PGW S8 Reference Point.
Ite.PdnSignalling	PGW Signalling - Configuration of PGW Signalling.
Ite.PgwChargingProfile	PGW Charging Profile - Configuration of PGW Charging Profile.
Ite.PlmnListPolicy	PLMN List Profile - Configuration of PLMN List Profile.
Ite.PlmnListPolicyGroup	PLMN List Group - Configuration of PLMN List Group.
Ite.QciPolicy	QCI Policy - Configuration of QCI Policy.
Ite.QciPolicyEntry	QCI Policy Entry - Configuration of QCI Policy Entry.
Ite.RTCountersENBStatus	Real Time Counters Status for ENB - Real Time Counters Session.
Ite.RTCountersSession	Real Time Counters Session - Real Time Counters Session.
Ite.S11ReferencePoint	S11 Reference Point - Configuration of S11 Reference Point.
Ite.S1uReferencePoint	S1-u Reference Point - Configuration of S1u Reference Point.
Ite.ServingGateway	Serving Gateway - Configuration of Serving Gateway.

Table 22 Permissions assigned to 5620 SAM scope of command roles (continued)

Package.Class.Method/Property	Description
Ite.SgwApn	Serving Gateway APN - Configuration of Serving Gateway APN.
Ite.SgwChargingProfile	SGW Charging Profile - Configuration of SGW Charging Profile.
Ite.SgwRfReferencePoint	SGW Rf Reference Point - Configuration of SGW Rf Reference Point.
Ite.SgwS5ReferencePoint	SGW S5 Reference Point - Configuration of SGW S5 Reference Point.
Ite.SgwS8ReferencePoint	SGW S8 Reference Point - Configuration of SGW S8 Reference Point.
Ite.SgwSignalling	Serving Gateway Signalling - Configuration of Serving Gateway Signalling.
Ite.SubscAndEquipmentTraces	Subsc And Equipment Traces - Configuration of Call Traces.
Ite.TaiLaiListEntry	TAI-LAI List Entry - Configuration of TAI-LAI Entry.
Ite.TaiLaiListProfile	TAI-LAI List Profile - Configuration of TAI-LAI List Profile.
Ite.TrustedPeerListEntry	Trusted Peers - Configuration of Trusted Peer List Entries.
Ite.TrustedPeerListEntryUnlisted	Unlisted Peer - Configuration of Unlisted Trusted Peer List Entries.
Ite.TrustedPeerListPolicy	Trusted Peer List Policy - Configuration of Trusted Peer List Policy.
Iteanr	LTE - Access to LTE ANR profiles.
Iteepdg	LTE - All LTE configurations and status.
Iteepdg.EpdgChargingProfile	EPDG Charging Profile - Configuration of EPDG Charging Profile.
Iteepdg.IPSecProfile	IPSec Profile - Configuration of IPSec Profile.
Iteepdg.SwmAvpOptionProfile	SWm AVP Option Profile - Configuration of SWm AVP Option Profile.
Iteepdg.SwmReferencePoint	SWm Reference Point - Configuration of SWm Reference Point.
Iteepdg.SwuReferencePoint	SWu Reference Point - Configuration of SWu Reference Point.
Iteggsn	LTE - All LTE configurations and status.
Iteggsn.CdrAvpOptionProfile	CDR AVP Option Profile - Configuration of CDR AVP Option Profile.
Iteggsn.DccaRatingGroup	DCCA Rating Group - Configuration of Dcca Rating Group.
Iteggsn.GnReferencePoint	Gn Reference Point - Configuration of Gn Reference Point.

Table 22 Permissions assigned to 5620 SAM scope of command roles (continued)

Package.Class.Method/Property	Description
Iteggnsn.GpReferencePoint	Gp Reference Point - Configuration of Gp Reference Point.
Iteggnsn.GyAvpOptionProfile	Gy AVP Option Profile - Configuration of Gy AVP Option Profile.
Iteggnsn.PdnGyReferencePoint	Gy Reference Point - Configuration of Gy Reference Point.
Iteggnsn.PgwGaReferencePoint	PGW Ga Reference Point - Configuration of PGW Ga Reference Point.
Iteggnsn.SgwGaReferencePoint	SGW Ga Reference Point - Configuration of SGW Ga Reference Point.
Itegw	LTE - All LTE configurations and status.
Itegw.ApnListPolicy	APN List Profile - Configuration of APN List Profile.
Itegw.ApnListPolicyGroup	APN List Group - Configuration of APN List Group.
Itegw.DiameterPeerRedirHostEntry	Diameter Peer Redirect Host Entry - Configuration of Diameter Peer Redirect Host Entry.
Itegw.DiameterPeerSupportedHost	Diameter Peer Support Supported Host - Configuration of Diameter Peer Support Host Entry.
Itegw.PcscfGroupProfile	P-CSCF Group Profile - Configuration of P-CSCF Group Profile.
Itegw.PcscfPeerEntry	P-CSCF Peer Entry - Configuration of P-CSCF Peer Entry.
Itegw.PcscfResolvedPeerIpEntry	P-CSCF Resolved Peer Ip Entry - Configuration of P-CSCF Peer Entry.
Itegw.SCTPProfile	SCTP Profile - Configuration of SCTP Profile.
Itegw.UMTSQoSPolicy	UMTS QoS Policy - Configuration of UMTS QoS Policy.
Itehomeagent	LTE - All LTE configurations and status.
Itehomeagent.DNSRedirectServer	DNS Redirect Server - Configuration of DNS Redirect Server.
Itehomeagent.FAHAPeerList	FA-HA Peer List - Configuration of FA-HA Peer List.
Itehomeagent.MobileIpv4Profile	Mobile IPv4 Profile - Configuration of Mobile IPv4 Profile.
Itehomeagent.PiReferencePoint	Pi Reference Point - Configuration of Pi Reference Point.
Iteli	LTE LI - All LTE LI configurations and status.
Iteli.DFPeer	LTE LI Delivery Function Peer - Configuration of LTE LI Delivery Function Peer.
Iteli.DFPeerCardGroup	LTE LI Delivery Function Peer Card Group Status - Display of LTE LI Delivery Function Peer Card Status.
Iteli.InterceptionTarget	LTE LI Interception Target - Configuration of LTE LI Interception Target.

Table 22 Permissions assigned to 5620 SAM scope of command roles (continued)

Package.Class.Method/Property	Description
Iteli.LILteCfg	LTE LI Pre Configuration - Contains system Lawful Intercept Configuration for MG.
Itemme	LTE-2G3G - All LTE MME configurations.
Itemme.MmeInstance.method_abortMmeLoadBalance	WMM Instance - method_abortMmeLoadBalance - Ability to abort MME load balancing operation.
Itemme.MmeInstance.method_deployGcToNode	WMM Instance - method_deployGcToNode - Ability to deploy a GC to a node.
Itemme.MmeInstance.method_intraMmeLoadBalance	WMM Instance - method_intraMmeLoadBalance - Ability to perform intra MME load balancing operation.
Itemme.MmeInstance.method_lockMmeAggregateService	WMM Instance - method_lockMmeAggregateService - Ability to lock the MME aggregate service.
Itemme.MmeInstance.method_unlockMmeAggregateService	WMM Instance - method_unlockMmeAggregateService - Ability to unlock the MME aggregate service.
Iteperf	LTE Performance Management - All LTE configurations : SGW, PGW, eNodeB.
Itepmip	LTE - All LTE configurations and status.
Itepmip.Pmipv6Profile	PMIPv6 Profile - Configuration of PMIPv6 Profile.
Itepmip.S2aReferencePoint	S2a Reference Point - Configuration of S2a Reference Point.
Itepmip.S2bReferencePoint	S2b Reference Point - Configuration of S2b Reference Point.
Itepmip.S6bAvpOptionProfile	S6b AVP Option Profile - Configuration of S6b AVP Option Profile.
Itepmip.S6bReferencePoint	S6b Reference Point - Configuration of S6b Reference Point.
Itepolicyoptions	LTE - All LTE configurations and status.
Itepolicyoptions.AsoOptions	ASO Options Profile - Configuration of ASO Options Profile.
Itepolicyoptions.ChargingRuleUnit	Charging Rule Unit Profile - Configuration of ChargingRuleUnit Profile.
Itepolicyoptions.DhcpServerGroupProfile	DHCP Server Group Profile - Configuration of DHCP Server Group Profile.
Itepolicyoptions.DhcpSGPeerEntry	DHCP Peer Entry - Configuration of DHCP Peer Entry.
Itepolicyoptions.GxAvpOptionProfile	Gx AVP Option Profile - Configuration of Gx AVP Option Profile.
Itepolicyoptions.PolicyRule	Policy Rule Profile - Configuration of PolicyRule Profile.
Itepolicyoptions.PolicyRuleBase	Policy Rule Base Profile - Configuration of PolicyRuleBase Profile.

Table 22 Permissions assigned to 5620 SAM scope of command roles (continued)

Package.Class.Method/Property	Description
Itepolicyoptions.PolicyRuleBaseEntry	Base Policy Entry - Configuration of PolicyRuleBase Profile.
Itepolicyoptions.PolicyRuleUnit	Policy Rule Unit Profile - Configuration of PolicyRuleUnit Profile.
Itepolicyoptions.PolRuleUnitFlwDescription	Policy Rule Unit Flow Description Entry - Configuration of Flow Description Entry.
Itepolicyoptions.ServiceClassIndicator	Service Class Indicator - Configuration of ServiceClassIndicator Profile.
Itepolicyoptions.TrafficHashProfile	Traffic Hash Profile - Configuration of Traffic Hash Profile.
Itepolicyoptions.TrafficRedirectProfile	Traffic Redirect Profile - Configuration of Traffic Redirect Profile.
Itepolicyoptions.TrafficRedirectTarget	Traffic Redirect Target Entry - Configuration of Traffic Redirect Target Entry.
Itepool	LTE POOL - All LTE POOL configurations.
Itepool.MmeInstanceBinding	MME Instance Binding - Ability to configure associations between an MME Instance and an MME Pool.
Itepool.TaBinding	Tracking Area Binding - Ability to configure associations between a Tracking Area and an MME Pool.
Iteadius	LTE - All LTE configurations and status.
Iteadius.RadiusGroupProfile	RADIUS Group Profile - Configuration of Radius Group Profile.
Iteadius.RadiusPeerProfile	RADIUS Peer Profile - Configuration of RADIUS Peer Profile.
Iteadius.RadiusProfile	RADIUS Profile - Configuration of RADIUS Profile.
Ites1mme	LTES1MME - All LTE S1MME Configurations and Monitoring Status.
Itesecurity	LTE Security - All LTE configurations : SGW, PGW, Bearers, and more.
Iteservice	LTE - All LTE configurations and status.
Itesgsn	LTE - All LTE configurations and status.
Itesgsn.SgwS12ReferencePoint	S12 Reference Point - Configuration of S12 Reference Point.
Itesgsn.SgwS4ReferencePoint	S4 Reference Point - Configuration of S4 Reference Point.
Ithreshold	LTE - All LTE configurations and status.
Iteuserstats	LTE - All LTE configurations and status.
Iteuserstats.UserStatsQuery	User Stat Query - Configuration of User Stats Queries.
Iteuserstats.UserStatsQueryOutputSnapshot	User Query Output Snapshot - Configuration of User Stats Query Snapshots.

Table 22 Permissions assigned to 5620 SAM scope of command roles (continued)

Package.Class.Method/Property	Description
lteuserstats.UserStatsUserPgw	PGW User Data - Configuration of User Stats User Output.
lteuserstats.UserStatsUserSgw	SGW User Data - Configuration of User Stats User Output.
mediation	Router Admin: Policies - Router administration: Backup Policies, Upgrade Policies and Software images, Deployment Policies, and Management Ping Policies.
mirror	Mirror - All configurations for Service Mirroring.
mirror.Endpoint	Endpoint - Access to MIRROR Endpoints.
mirror.Mirror	Mirror Service - Access to Mirror Service objects themselves.
mirror.Site	Mirror Site - Access to Mirror Sites.
mld	MLD - Multicast Listener Discovery Protocol (MLD) configuration for a Service interfaces and routers.
mmepolicy	WMM Policies - Management of policies associated with 9471 WMM.
mmepolicy.MMEEmergencyNumListPolicy	WMM Emergency Number List - Configuration of Emergency Number List.
mmepolicy.MMEEmergencyNumListTblPolicy	WMM Emergency Number List Table - Configuration of Emergency Number List Table.
mmepolicy.MMEGTPProfile	WMM GTP Profile - Configuration of GTP Profile.
mmepolicy.MMESCTPProfile	WMM SCTP Profile - Configuration of SCTP Profile.
mmepolicy.WMMPfmJobEntry	WMM Performance Measurement Job Entry - Configuration of Performance Measurement Job Entry.
mmepolicy.WMMPfmJobMts	WMM Performance Measurement Job Measurements - Configuration of Performance Measurement Job Measurements.
mmepolicy.WMMPfmJobSched	WMM Performance Measurement Job Schedules - Configuration of Performance Measurement Job Measurements.
mmepolicy.WMMPfmMeasGroupName	WMM Performance Measurement Group Name - Configuration of Performance Measurement Group Name.
mmepolicy.WMMPfmMeasGroups	WMM Performance Measurement Groups - Configuration of Performance Measurement Groups.
monitor	Monitor - Subscriber Host monitoring and SAP monitoring.
monpath	Monitored Path - IP path monitoring and LSP monitoring.

Table 22 Permissions assigned to 5620 SAM scope of command roles (continued)

Package.Class.Method/Property	Description
mpls	Path/Routing Management: MPLS - Multiprotocol Label Switching (MPLS) configuration on a rtr.VirtualRouter, LSPs, Segments, Hops, Tunnels, CrossConnects, and other MPLS related objects.
mpls.LdpTreeTrace	LDP Tree Trace - Access to LDP Tree Trace tests, LDP Tree Trace test definitions, and LDP Tree Trace deployed tests.
mpls.LspPing	LSP Ping - Access to LSP Ping tests, LSP Ping test definitions, and LSP Ping deployed tests.
mpls.LspTrace	LSP Trace - Access to LSP Trace tests, LSP Trace test definitions, and LSP Trace deployed tests.
mpls.P2MPLspPing	P2MP LSP Ping - Access to P2MP LSP Ping tests, P2MP LSP Ping test definitions, and P2MP LSP Ping deployed tests.
mpls.P2MPLspTrace	P2MP LSP Trace - Access to P2MP LSP Trace tests, P2MP LSP Trace test definitions, and P2MP LSP Trace deployed tests.
mplstp	MPLS TP - MPLS TP Configuration for Sites.
mpr	9500 MPR - 9500 Microwave Packet Radio (MPR) VLAN Paths and Hops.
mpr.AI2AccessInterface	9500 MPR Apipe L2 Access Interface - Access to L2AccessInterface objects.
mpr.Apipe	9500 MPR Apipe Service - Access to vll ATM Pipe (Apipe) Service objects themselves.
mpr.Asite	9500 MPR Apipe Site - Access to the service instance objects.
mpr.Cpipe	9500 MPR Cpipe Service - Access to VLL Circuit Emulation Pipe (Cpipe) Service objects themselves.
mpr.El2AccessInterface	9500 MPR Epipe L2 Access Interface - Access to L2AccessInterface objects.
mpr.Epipe	9500 MPR Epipe Service - Access to VLL Ethernet Pipe Service objects themselves.
mpr.Esite	9500 MPR Epipe Site - Access to the service instance objects.
mpr.L2AccessInterface	9500 MPR Cpipe L2 Access Interface - Access to L2AccessInterface objects.
mpr.Site	9500 MPR Cpipe Site - Access to the service instance objects.
msappolicy	MSAP Policy - MSAP policy configuration.

Table 22 Permissions assigned to 5620 SAM scope of command roles (continued)

Package.Class.Method/Property	Description
msdp	MSDP - Multicast Source Discovery Protocol (MSDP) configuration for a rtr.VirtualRouter, MD5 Key, Peers, Policies and Source.
multicast	Multicast - Multicast Connection Admission Control (CAC) Policies and Bandwidth Policies.
multicast.CustomerVlanTag	Customer Vlan Tag - Configuration of Customer VLAN Tags for a Multicast VLAN.
multicast.MfibPing	MFIB Ping - Access to MFIB Ping tests, MFIB Ping test definitions, and MFIB Ping deployed tests.
multicast.Mrinfo	Mrinfo - Access to Mrinfo tests, Mrinfo test definitions, and Mrinfo deployed tests.
multicast.Mtrace	Mtrace - Access to Mtrace tests, Mtrace test definitions, and Mtrace deployed tests.
multicastmgr	CPAM: Multicast - All CPAM Multicast related objects: PIM Domain, VPLS Domain, Groups, and Sources.
multichassis	Multi-Chassis - Multi-Chassis configuration for a router; LAGs, Rings, Syncs, Peers, VLAN Ranges, IPsecs.
mvpls	MVPLS - All contained objects are listed. Package access is not currently used.
mvpls.BL2AccessInterface	MVPLS B-L2 Access Interface - Access to MVPLS B-L2 Access Interfaces.
mvpls.BSite	MVPLS B-Site - Access to MVPLS B-Sites.
mvpls.EvpnSite	MVPLS EVPN-Site - Access to MVPLS EVPN-Sites on a MVPLS Service.
mvpls.IL2AccessInterface	MVPLS I-L2 Access Interface - Access to MVPLS I-L2 Access Interfaces.
mvpls.ISite	MVPLS I-Site - Access to MVPLS I-Sites.
mvpls.L2AccessInterface	MVPLS L2 Access Interface - Access to MVPLS L2 Access Interfaces (except I and B).
mvpls.Mvpls	MVPLS Service - Access to Management Virtual Private LAN Service (MVPLS) Service objects themselves.
mvpls.Site	MVPLS Site - Access to MVPLS Sites (except I and B).
mvrp	MVRP - MVRP global configuration and for Interfaces(Ports and LAG's).

Table 22 Permissions assigned to 5620 SAM scope of command roles (continued)

Package.Class.Method/Property	Description
mwa	Microwave Aware - Access to MW (Microwave) Link and MW Link Members configuration for Service interfaces and routers.
nat	Network Address Translation - NAT Policy.
nat.LsnSubSession	LSN Subscriber Session - Access to NAT Package.
nat.PcpServer	Port Control Protocol Server - Access to Port Control Protocol Server configuration.
nat.PcpServerInterface	Port Control Protocol Server Interface - Access to Port Control Protocol Interface configuration.
neaudit	NE Audit Management - Ability to manage NE Audits.
nelicense	NeLicense - Apply License on the node.
netca	NE Threshold Crossing Alerts - Manage NE Threshold Crossing Alert profiles.
netw	Network - Network objects: groups and links.
netw.AdvertisedNode	Advertised Node - Control of Discovered Nodes.
netw.NeLimitHolder	NE Limits - Access to NE Limit configuration.
netw.NetworkElement	Network Element - Access to Network Elements.
netw.NetworkElement.method_executeCli	Network Element - method_executeCli - Execute a single raw CLI command on this Network Element.
netw.NetworkElement.method_executeMultiCli	Network Element - method_executeMultiCli - Execute Multiple CLI commands on this Network Element.
netw.NetworkElement.method_GUICrossLaunch	Network Element - method_GUICrossLaunch - The ability to launch LTE web-browser based tools.
netw.NetworkElement.method_NetoAdminProfileBasedLaunch	Network Element - method_NetoAdminProfileBasedLaunch - The ability to launch Neto with Admin profile.
netw.NetworkElement.method_NetoViewerProfileBasedLaunch	Network Element - method_NetoViewerProfileBasedLaunch - The ability to launch Neto with Viewer profile.
netw.NetworkElement.property_elementManagerCmd	Network Element - property_elementManagerCmd - Ability to update the 'Alternate Element Manager' command for a GNE.
netw.NodeDiscoveryControl	Node Discovery Control - Control of Discovered Nodes.
netw.Topology	Discovery Manager - Access to the Discovery Manager.
netw.Topology.method_move	Discovery Manager - method_move - Ability to move a node or group on the SAM Client GUI maps.

Table 22 Permissions assigned to 5620 SAM scope of command roles (continued)

Package.Class.Method/Property	Description
netw.UplinkBofConfiguration	Uplink Bof Configuration - Ability to configure the Uplink BOF for a 7210 node.
netw.UplinkRouteConfiguration	Uplink Route Configuration - Ability to configure the Uplink Routes for a 7210 node.
nge	NetworkGroupEncryption - Network Group Encryption configuration on 7705 router.
niegr	Network Ingress/Egress Policy - Network Policies.
nodelog	Node Log Policy - Filter Log and Sys Log Target Policies.
nqueue	Network Queue Policy - Network Queue QoS Policies.
ntp	Network Time Protocol - Network Time Protocol.
ntp.NTPBroadcast	NTP Broadcast - Ability to configure broadcast for ntp params.
ntp.NTPMulticast	NTP Multicast - Ability to configure multicast for ntp params.
olc	Object Life Cycle.
olc.OLCSchedulerManager.property_autosetMaintenanceOLCStateOnAdminDown	OLC Scheduler Manager - property_autosetMaintenanceOLCStateOnAdminDown - Service preferences can only be modified by a user with an administrator role.
olc.OLCSchedulerManager.property_createAlarmNotification	OLC Scheduler Manager - property_createAlarmNotification - OLC preferences can only be modified by a user with an administrator role.
olc.OLCSchedulerManager.property_leadTimeForNotification	OLC Scheduler Manager - property_leadTimeForNotification - OLC preferences can only be modified by a user with an administrator role.
openflow	OpenFlow - OpenFlow configuration and status on a router.
optical	Optical Management - Optical NE Specific Information.
optical.MultipointServicePath	Multipoint Service Path - Access for all Multi Point Service Paths.
optical.MultipointTransportService	Multipoint Transport Service - Access for all optical services.
optical.OCHTrail	OCH Trail - Access for all OCH trails.
optical.ODUTrail	ODU Trail - Access for all ODU trails.
optical.OMSTrail	OMS Trail - Access for all OMS trails.
optical.OTSTrail	OTS Trail - Access for all OTS trails.
optical.OTUTrail	OTU Trail - Access for all OTU trails.

Table 22 Permissions assigned to 5620 SAM scope of command roles (continued)

Package.Class.Method/Property	Description
optical.STMTrail	STM Trail - Access for all STM trails.
optical.TransportService	Optical Transport Service - Access for all optical services.
opticalacl	Optical Access Control Lists - ACL Management.
opticalequipment	Optical Management - Optical NE Specific Configuration.
opticalrouting	Optical Routing - Optical Routing Meta.
opticsperf	Optics Specifics - All 1830 PSS configurations.
ospf	Routing Management: OSPF - OSPF configuration for Service interfaces and routers, Area, Adjacency, MD5 Key, Virtual Links Neighbors, LSAs, Policies and other OSPF related objects.
ospf.Site	OSPF Site - Access to OSPF Sites.
oss	OSS - Ability to connect to the SAM Server through the OSS interface.
oth	Optical Transport Hierarchy - OTH Management.
pae802_1x	PAE 802.1x - Port Access Entity (PAE) configuration for a router and physical port; RADIUS Server Policy.
pbbvlan	PBBVLAN - Access to this package is for configuring SPB-BVLAN Service, Site, SAPs, MeshSDPs and site stats.
pbbvlan.Site	SPB Site - Access to SPB Services.
pbbvlan.VlanPBBEdge	SPB Service - Access to SPB Services.
pim	PIM - PIM configuration for Service interfaces and routers, MDT Threshold, Policies, Neighbors, Groups, RPs, Multicast CAC Level and LAG Port Down events, and other PIM related objects.
pim.Site	PIM Site - Access to PIM Sites.
policing	Policing Policy - Policer Control.
policy	Policy - Parent package for all policies; Policy Audits, Policy Export/Imports.
policy.PolicyDefinition.method_setConfigurationModeToReleased	Policy Definition - method_setConfigurationModeToReleased - Ability to set Configuration Mode to Released and distribute the global policy to the local definitions network-wide.
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	Policy Definition - method_setDistributionModeToLocalEditOnly - Ability to set Configuration Mode to Local Edit Only for local policies and ignore changes to the global policy.

Table 22 Permissions assigned to 5620 SAM scope of command roles (continued)

Package.Class.Method/Property	Description
policy.PolicyDefinition.method_ setDistributionModeToSyncWithGlobal	Policy Definition - method_ setDistributionModeToSyncWithGlobal - Ability to set Configuration Mode to Sync with Global and synchronize local policies with the most recent released global policy.
policy.PolicyNameManager.property_ autoDistributeOnRelease	Policy Name Manager - property_ autoDistributeOnRelease - Ability to set the automatic distribution of a global policy when released.
policy.PolicyNameManager.property_ localEditOnly	Policy Name Manager - property_ localEditOnly - Ability to force the distribution mode to Local Edit Only for Scope exclusive.
policy.PolicyNameManager.property_ localEditOnlyOnCLIChange	Policy Name Manager - property_ localEditOnlyOnCLIChange - Ability to switch the distribution mode to Local Edit Only on CLI changes.
policy.PolicyNameManager.property_ maxScheduledAuditResultPerLocalPolicy	Policy Name Manager - property_ maxScheduledAuditResultPerLocalPolicy - Ability to set the maximum number of audit results stored per local policy.
policy.PolicyNameManager.property_ securityZoneDiscoveredInLocalEditOnlyMode	Policy Name Manager - property_ securityZoneDiscoveredInLocalEditOnlyMode - Ability to discover security zones in Local Edit Only.
policy.PolicyNameManager.property_ showFilterDisplayName	Policy Name Manager - property_ showFilterDisplayName - Ability to show the Display Name on access ingress/egress QoS policy forms.
policy.PolicyNameManager.property_ showQoSPolicyDisplayName	Policy Name Manager - property_ showQoSPolicyDisplayName - Ability show the Display Name on ACL filter forms.
policy.PolicySyncGroupManager	Policy Sync Group Manager - Ability to configure and control policy sync group.
policytestutil	Policy Test Utility - TODO.
port.RestrictModeConfigModify	Port. Restrict Mode Config Modify - Ability to restrict Port Mode modification for Ports with dependencies.
portscheduler	Port Scheduler Policy - Port Scheduler and HSMDA Scheduler Policies.
ppp	PPP - Point-to-Point Protocol (PPP) configuration on a router.
pppoe	PPP Policy and Session - Point-to-Point Protocol over Ethernet over ATM (PPPoE/PPPoEoA/PPPoA) Policies and Sessions.
propertyrules	Property Rules - Range and Format Value Policies.
ptp	Precision Timing Protocol - Access to this package is for configuring Precision Timing Protocol.
qgroup	Queue Group Policy - Queue Group Policies.

Table 22 Permissions assigned to 5620 SAM scope of command roles (continued)

Package.Class.Method/Property	Description
qosprefixlist	QoS Policy - QoS PrefixList Policy.
qosprofile	Multilink QoS Profile - Multilink PPP QoS Profiles and Multilink Frame Relay QoS Profiles.
radioequipment	Radio Equipment - Radio Equipment configuration.
radiusaccounting	Radius Accounting - Radius Accounting Policy.
ranlicense	NE License Management - Ability to manage NE licenses.
ranradiom	eNodeB Router Admin: radio measurement - eNodeB Router administration: radio measurement.
rca	RCA - Root Cause Analysis (RCA) for verification applications (OSPF Area,ISIS Area,BGP AS,...).
rca.RcaManager.method_fixProblem	Rca Manager - method_fixProblem - Ability to fix a problem on an object.
rca.RcaManager.method_preFixProblem	Rca Manager - method_preFixProblem - Ability to determine if a problem can be fixed, and the fix impact.
redirectfilter	Redirect Filter Policy - Redirect Filters.
resiliency	HSDPA Resiliency - HSDPA Resiliency for services.
resources	SAM Resources - SAM Resource Pools as configured in the nms-server.xml file.
ressubscr	Residential Subscriber - All Residential Subscriber configuration including Connectivity Verifications (SHCV), SAPs, Packages, Hosts, QoS, and other related objects.
ressubscr.BgpPeeringPolicy	BGP Peering Policy - Access to BGP Peering Policies.
ressubscr.HostTrackingPolicy	Host Tracking Policy - Access to Host Tracking Policies.
ressubscr.IgmpPolicy	IGMP Policy - Access to IGMP Policies.
ressubscr.IpoePolicy	IPoE Session Policy - Access to IPoE Session Policies.
ressubscr.MldPolicy	MLD Policy - Access to MLD Policies.
ressubscr.ResidentialSubscriberManager.property_hostTrkSubscrRtrvTimeOut	Residential Subscriber Manager - property_hostTrkSubscrRtrvTimeOut - Service preferences can only be modified by a user with an administrator role.
ressubscr.ResidentialSubscriberManager.property_resSubscrInstRtrvMax	Residential Subscriber Manager - property_resSubscrInstRtrvMax - Service preferences can only be modified by a user with an administrator role.

Table 22 Permissions assigned to 5620 SAM scope of command roles (continued)

Package.Class.Method/Property	Description
ressubscr.ResidentialSubscriberManager.property_retrieveAcclpEncap	Residential Subscriber Manager - property_retrieveAcclpEncap - Service preferences can only be modified by a user with an administrator role.
ressubscr.ResidentialSubscriberManager.property_retrieveBgpPeerInfo	Residential Subscriber Manager - property_retrieveBgpPeerInfo - Service preferences can only be modified by a user with an administrator role.
ressubscr.ResidentialSubscriberManager.property_retrieveManagedRoutes	Residential Subscriber Manager - property_retrieveManagedRoutes - Service preferences can only be modified by a user with an administrator role.
ressubscr.ResidentialSubscriberManager.property_retrieveQoSovr	Residential Subscriber Manager - property_retrieveQoSovr - Service preferences can only be modified by a user with an administrator role.
ressubscr.ResidentialSubscriberManager.property_retrieveSlaacHostAddr	Residential Subscriber Manager - property_retrieveSlaacHostAddr - Service preferences can only be modified by a user with an administrator role.
ressubscr.ResidentialSubscriberManager.property_subscriberHostRtrvTimeOut	Residential Subscriber Manager - property_subscriberHostRtrvTimeOut - Service preferences can only be modified by a user with an administrator role.
ressubscr.SubMcastCacPolicy	Subscriber Multicast CAC Policy - Access to Subscriber Multicast CAC Policies.
rip	Routing Management: RIP - Routing Information Protocol (RIP) configuration for Service interfaces and routers, Authentication Key, Groups, Export and Import Policies.
rip.Site	RIP Site - Access to RIP Sites.
rmd	Remote Managed Device - Remote Managed Device Management.
rmon	Remote Network Monitoring - Remote Network Monitoring Alarm and Event Policies.
rollback	Rollback - All scheduled tasks; Cron Actions, OSS Commands, CLI Scripts and Schedules.
rp	Routing Policy - Policy Statements, Prefix Lists, Communities, Damping, and AS Paths.
rsvp	Routing Management: RSVP - RSVP configuration for a rtr.VirtualRouter, Authentication Keys, and Neighbors.
rtr	Routing Management: General - General rtr.VirtualRouter configurations including Neighbor Discovery, DHCP Relays, Interfaces, Peers, Address Ranges and ARP, Routes and Router Advertisement.

Table 22 Permissions assigned to 5620 SAM scope of command roles (continued)

Package.Class.Method/Property	Description
rules	Rules - Rule Repository and Sets of rules that may get invoked when a rule engine is fired.
sas	Assurance - Parent package for all tests; Service Test Manager.
sas.IPSession	IP Session - Access to IP Session, IP Test Session definitions.
sas.TestManager.property_sasNumberOfHours	Service Test Manager - property_sasNumberOfHours - These preferences can only be modified by a user with an administrator role.
sas.TestManager.property_sasRetention	Service Test Manager - property_sasRetention - LogToFile preferences can only be modified by a user with an administrator role.
sas.TestManager.property_sasRollover	Service Test Manager - property_sasRollover - LogToFile preferences can only be modified by a user with an administrator role.
sas.TWLBIn	TWAMP Light Session Bin - Access to TWAMP Light Test Session, TWAMP Light Test Session definitions.
sas.TwlReflector	TWAMP Light Reflector - Access to TWAMP Light Reflector.
sas.TWLSession	TWAMP Light Test Session - Access to TWAMP Light Test Session, TWAMP Light Test Session definitions.
saspm	SAS PM - Access to OAM Performance Monitoring Objects.
sasqos	7210 and 1830 QoS - QoS Policies for 7210 and 1830 nodes.
sasqos.QoSPool	QoS Pool - Access to QoS Pools for 7210 nodes.
schedule	Schedule - All scheduled tasks; Cron Actions, OSS Commands, CLI Scripts and Schedules.
script	Scripting - Script Management and execution of Service and Tunnel Template, OSS, and CLI scripts.
script.AbstractScript.method_configureTarget	Script - method_configureTarget - Ability to configure targets and instances.
script.AbstractScript.method_configureTargets	Script - method_configureTargets - Ability to configure targets and instances.
script.Bundle	Script Bundle - Ability to configure script bundles.
script.ControlScript	Control Script - Ability to configure control scripts.
script.ControlScriptVersion	Control Script Version - Ability to configure Control script versions.
script.HandlerBinding	Handler Script Binding - Ability to configure associations between scripts and control scripts.

Table 22 Permissions assigned to 5620 SAM scope of command roles (continued)

Package.Class.Method/Property	Description
script.InvokerBinding	Invoker Script Binding - Ability to configure associations between scripts and control scripts.
script.LargeTextTargetParameter	Large Text Target Parameter - Ability to configure target/instance large text parameters.
script.Result	Result - Ability to create script results.
script.Script	CLI Script - Ability to configure CLI scripts.
script.Script.method_createTargetScript	CLI Script - method_createTargetScript - Ability to configure targets.
script.Script.method_createTargetScripts	CLI Script - method_createTargetScripts - Ability to configure targets.
script.ScriptManager	Script Manager - Ability to configure and control scripts and script operations.
script.ScriptManager.method_configure	Script Manager - method_configure - Ability to configure scripts.
script.ScriptManager.method_copyContents	Script Manager - method_copyContents - Ability to copy scripts.
script.ScriptManager.method_exportBundle	Script Manager - method_exportBundle - Ability to export bundle.
script.ScriptManager.method_importBundle	Script Manager - method_importBundle - Ability to import bundle.
script.ScriptManager.method_importBundleSimulation	Script Manager - method_importBundleSimulation - Ability to import bundle.
script.ScriptScheduledTask	Script Scheduled Task - Ability to schedule a script.
script.TargetParameter	Target Parameter - Ability to configure target/instance parameters.
script.TargetParameterItem	Target Parameter Item - Ability to configure target/instance parameter items.
script.TargetParameterList	Target Parameter List - Ability to configure target/instance parameter lists.
script.TargetScript	Target Script - Ability to configure targets and instances.
script.TemplateBinding	Template Binding - Ability to configure associations between templates.
script.Version	Version - Ability to configure CLI script versions.
script.XmlApiConfigTemplate	Template - Ability to configure XML API templates.
script.XmlApiConfigTemplate.method_execute	Template - method_execute - Ability to create an object from a template.

Table 22 Permissions assigned to 5620 SAM scope of command roles (continued)

Package.Class.Method/Property	Description
script.XmlApiConfigTemplate.method_executeMulti	Template - method_executeMulti - Ability to create an object from a template.
script.XmlApiConfigTemplate.method_executeScript	Template - method_executeScript - Ability to create an object from a template.
script.XmlApiConfigTemplate.method_serviceTemplateExecute	Template - method_serviceTemplateExecute - Ability to execute a service template.
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	Template - method_tunnelTemplateExecute - Ability to execute a tunnel template.
script.XmlApiScript	XMLAPI Script - Ability to configure XML API scripts.
script.XmlApiVersion	XMLAPI Version - Ability to configure XML API script versions.
security	Security - SAM User security including Sessions, TCP KeyChains, and SSH2 Known Host Keys.
security.CpamLicense	CPAM License - Read-only view of the 5650 CPAM License.
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	CPAM License - method_clearRouterLimitExceedDueToMultiAdditions - Ability to clear the isRouterLimitExceedDueToMultiAdditions flag on the license.
security.CpamLicenseScenario	CPAM License Scenario - Read-only view of the 5650 CPAM Imapct Analysis Application License.
security.MediationPolicy	Mediation Policy - Access to Mediation Policies. Used in conjunction with snmp.PollerManager.
security.MessagingConnection	Messaging Connection - Ability to view messaging connections.
security.RoleBasedAccess	Security. Role Based Access - Ability to restrict online object creation and deletion to a specific role. Currently applies to 9412 node.
security.ScopeOfCommandProfile	Profile - Access to Scope of Command Profile configuration.
security.ScopeOfCommandRole	Role - Access to Scope of Command Role configuration.
security.Span	Span - Access to Span configuration. Used in conjunction with security.SpanObjectBinding.
security.SpanObjectBinding	Span Objects - Access to Span object configuration. Used in conjunction with security.Span.
security.SpanOfControlProfile	Profile - Access to Span of Control Profile configuration.
security.User	User - Access to User object configuration and password changes.
security.UserGroup	User Group - Access to UserGroup configuration.

Table 22 Permissions assigned to 5620 SAM scope of command roles (continued)

Package.Class.Method/Property	Description
securitypolicy	Security Policy - All Security configurations including security policy,profile,zone,NAT.
securityqueue	Security Queue QoS Policies - Security Queue QoS policy.
selfconfig	Self Config - Ability to configure self config objects.
server	SAM Server - SAM Servers (JMS, Main, Auxiliary Server, Auxiliary Database) as configured in the nms-server.xml file.
service	Service Management - Parent package for all services; Composite Services and Connectors and Access Policy Queue Override Policies.
service.AarpInterface	AARP Interface - Access to AARP Interface configuration between AARP.
service.CpePing	CPE Ping - Access to CPE Ping tests, CPE Ping test definitions, and CPE Ping deployed tests.
service.GneAccessInterface	GNE Service Interface - Access to GNE Service Interfaces.
service.GneSite	GNE Site - Access to GNE Sites.
service.MacPing	MAC Ping - Access to MAC Ping tests, MAC Ping test definitions, and MAC Ping deployed tests.
service.MacPopulate	MAC Populate - Access to MAC Populate tests, MAC Populate test definitions, and MAC Populate deployed tests.
service.MacPurge	MAC Purge - Access to MAC Purge tests, MAC Purge test definitions, and MAC Purge deployed tests.
service.MacTrace	MAC Trace - Access to MAC Trace tests, MAC Trace test definitions, and MAC Trace deployed tests.
service.RedundantInterface	Redundant Interface - Access to Redundant Interface configuration between SRRP instances.
service.Service.method_create	Service - method_create - Ability to create a service via the SAM Client GUI.
service.Service.method_highPriorityServiceDelete	Service - method_highPriorityServiceDelete - Ability to delete high priority Service.
service.Service.property_svcPriority	Service - property_svcPriority - Service priority can only be modified by a user with an administrator role.
service.ServiceManager.property_alarmAggregationCompositeService	Service Manager - property_alarmAggregationCompositeService - Service preferences can only be modified by a user with an administrator role.

Table 22 Permissions assigned to 5620 SAM scope of command roles (continued)

Package.Class.Method/Property	Description
service.ServiceManager.property_alarmAggregationSdp	Service Manager - property_alarmAggregationSdp - Service preferences can only be modified by a user with an administrator role.
service.ServiceManager.property_autoDiscoverCompositeSvc	Service Manager - property_autoDiscoverCompositeSvc - Service preferences can only be modified by a user with an administrator role.
service.ServiceManager.property_enableCac	Service Manager - property_enableCac - Service preferences can only be modified by a user with an administrator role.
service.ServiceManager.property_enableRTCConnection	Service Manager - property_enableRTCConnection - Service preferences can only be modified by a user with an administrator role.
service.ServiceManager.property_generateReservedRrcAlarm	Service Manager - property_generateReservedRrcAlarm - Service preferences can only be modified by a user with an administrator role.
service.ServiceManager.property_maxNumberOfMoveSites	Service Manager - property_maxNumberOfMoveSites - Service preferences can only be modified by a user with an administrator role.
service.ServiceManager.property_multiSegmentTunnelSelection	Service Manager - property_multiSegmentTunnelSelection - Service preferences can only be modified by a user with an administrator role.
service.ServiceManager.property_propagateServiceNameToSites	Service Manager - property_propagateServiceNameToSites - Service preferences can only be modified by a user with an administrator role.
service.ServiceManager.property_propagateSiteNameToService	Service Manager - property_propagateSiteNameToService - Service preferences can only be modified by a user with an administrator role.
service.ServiceManager.property_removeEmptyService	Service Manager - property_removeEmptyService - Service preferences can only be modified by a user with an administrator role.
service.ServiceManager.property_supVprnSnmpCommunityStringMsg	Service Manager - property_supVprnSnmpCommunityStringMsg - Service preferences can only be modified by a user with an administrator role.
service.ServiceManager.property_svcPriority	Service Manager - property_svcPriority - Service priority can only be modified by a user with an administrator role.
service.ServiceMemberAuditPolicyEntry	Service Membership Audit Policy Entry - Access to Service Member Audit Policy Entry to configure service membership RCA audit behavior.

Table 22 Permissions assigned to 5620 SAM scope of command roles (continued)

Package.Class.Method/Property	Description
service.SitePing	Service Site Ping - Access to Service Site Ping tests, Service Site Ping test definitions, and Service Site Ping deployed tests.
service.TemplateService.method_constructServiceTemplate	Service Template - method_constructServiceTemplate - Ability to construct a Template from a Service.
service.TemplateService.method_constructTemplatedService	Service Template - method_constructTemplatedService - Ability to construct a Service from a Template.
service.Y1564TestHeadBiDirectional	Y1564 Bi-Directional Test - Access to Y1564 Bi-Directional tests, Y1564 Bi-Directional test definitions, and Y1564 Bi-Directional deployed tests.
sflow	sFlow - SFLOW Objects.
shaperqos	Shaper QoS Policies - Shaper QoS policy.
shg	Split Horizon Group - Split Horizon Groups for VPLS services.
simulator	CPAM: Simulator - Parent package for all CPAM simulated objects; Scenarios, Sessions, Change and Action events.
simulator.SimSession	Session - Access to simulation sessions for 5650 CPAM Impact Analysis.
sitesec	NE Security - All Network Element security configuration including NE System Security, RADIUS, TACACS+ and AOS Authentication, Site Management Access and CPM Filters, DoS Protection, Password Policy, Users and Profiles.
sitesec.LocalUser	NE User - Access to NE Site User configuration.
sitesec.UserProfile	Site User Profile - Access to NE Site User Profile configuration.
sitesec.UserPublicKey	RSA Key - Public keys(SSHv2) configuration for the system users.
slaprofile	SLA Profile - SLA Profiles for QoS Policies.
slope	Slope Policy - WRED Slope, HSMDA WRED Slope, HSMDA Pool, and Named Buffer Pool Policies.
slope.QosPool	QoS Pool - Access to QoS Pools for 7450, 7750, and 7710 nodes.
snmp	SNMP - SNMP Poller Policies, Event Notification Policies, Statistics Poller Policies.
snmp.EventNotificationPolicy	Event Notification Policy - Access to Event Notification Policies.
snmp.PollerManager	Mediation - Access to Mediation Policies. Used in conjunction with security.MediationPolicy.

Table 22 Permissions assigned to 5620 SAM scope of command roles (continued)

Package.Class.Method/Property	Description
snmp.PollerManager.method_resync	Mediation - method_resync - Ability to resync a Network Element. Requires 'update' access on netw.NetworkElement.
sonet	SONET Sync - SONET Synchronization for Shelf and Processor Cards.
sonetequipment	SONET Equipment - SONET Equipment configuration.
spanrules	Span Rules - Span Rules for service creation.
spb	SPB - Access to this package is for configuring SPB site and site stats.
spb.AccessInterface	Access Interface - Access to SPB Interface of VPLS B-L2 Access Interfaces on a BVPLS Service.
spb.NetworkInterface	Network Interface - Access to SPB Network Interfaces.
spb.SpokeSdpBindingInterface	Spoke SDP Binding Interface - Access to SPB Interface of VPLS Spoke-SDP on a BVPLS Service.
squeue	Shared Queue Policy - Shared Queue Policies.
srmrmtauth	SAM Remote Authentication - Remote Authentication for SAM configuration of RADIUS, TACACS+, and LDAP authentication servers.
srpythonmgmt	Python Management - Python Management.
srrp	SRRP - Subscriber Routed Redundancy Protocol (SRRP) configuration for IES and VPRN services.
statistics	SAM Performance Statistics - SAM Performance Statistics (Memory, Alarm Rate, Snmp Traps, and Node Resyncs).
statsplot	Statistics Plotter - Statistics Plotter.
subscr	Subscriber Management - Customers configuration.
subscr.Site	Subscriber Site - Access to Subscriber Sites.
subscrauth	Subscriber Authentication - Subscriber Authentication Policy using RADIUS for DHCP sessions.
subscrxpmap	Subscriber Explicit Map - Subscriber Explicit Map Entry.
subscrident	Subscriber Identification - Subscriber Identification Policy.
subscrprofile	Subscriber Profile - Subscriber Profile, SLA Entries, Access Policy Queue Overrides and Scheduler Policy Entry Overrides.
sup	Supervision - SAM Supervision (Dashboard).

Table 22 Permissions assigned to 5620 SAM scope of command roles (continued)

Package.Class.Method/Property	Description
svq	Aggregation Scheduler - Service and Subscriber Aggregation Scheduler, Ingress and Egress Aggregation Scheduler Overrides.
svr	Service Routing - All contained objects are listed. Package access is not currently used.
svt	Service Tunnel Management - All Service Tunnel configurations including Clouds, Service Distribution Path (SDP) Bindings and Pseudo Wires.
svt.BvlanTunnel	SPB BVLAN Tunnel (SDP) - Access to vlan Tunnel (SDP) configuration.
svt.L2TPv3Tunnel	L2TPv3 Tunnel (SDP) - Access to l2tpv3 Tunnel (SDP) configuration.
svt.MeshSdpBinding	Mesh SDP Binding - Access to Mesh SDP Binding configuration.
svt.MirrorSdpBinding	Mirror SDP Binding - Access to Mirror SDP Binding configuration.
svt.MtuPing	MTU Ping - Access to MTU Ping tests, MTU Ping test definitions, and MTU Ping deployed tests.
svt.SpokeSdpBinding	Spoke SDP Binding - Access to Spoke SDP Binding configuration.
svt.Tunnel	Tunnel - Access to Tunnel (or SDP object) configuration.
svt.TunnelPing	Tunnel Ping - Access to Tunnel Ping tests, Tunnel Ping test definitions, and Tunnel Ping deployed tests.
svt.VccvPing	VCCV Ping - Access to VCCV Ping tests, VCCV Ping test definitions, and VCCV Ping deployed tests.
svt.VccvTrace	VCCV Trace - Access to VCCV Trace tests, VCCV Trace test definitions, and VCCV Trace deployed tests.
svt.VlanPBBEdgeMeshSdpBinding	PBB VLAN Mesh SDP Binding - Access to PBB VLAN Mesh SDP Binding configuration.
sw	Router Admin: Software - Router administration: Backup Files, Card Software, Upgrade schedules, and Accounting Statistics Retrieval.
sw.BackupRestoreManager.method_backup	Backup/Restore Status - method_backup - Ability to perform a Network Element backup.
sw.BackupRestoreManager.method_restore	Backup/Restore Status - method_restore - Ability to perform a Network Element restore.

Table 22 Permissions assigned to 5620 SAM scope of command roles (continued)

Package.Class.Method/Property	Description
swran	eNodeB Router Admin: Software - eNodeB Router administration: Upgrade schedules.
sysact	User Activity - User Activity.
taskmgmt	Task Management - Monitor the tasks being executed in the server.
tca	TCA Policy - Parent package for all TCA classes.
tca.TCAManager.property_maxTCAAlarmLimit	TCAManager - property_maxTCAAlarmLimit - TCA preferences can only be modified by a user with an administrator role.
tca.TCAManager.property_maxTCAAlarmResetInterval	TCAManager - property_maxTCAAlarmResetInterval - TCA preferences can only be modified by a user with an administrator role.
tdm	Optical Transport Hierarchy - TDM Management.
tdmequipment	TDM Equipment - TDM Equipment configuration.
template	Service Template - Deprecated 6.0: use XML API based configuration templates (see class script. XmlApiConfigTemplate).
tod	TOD - Time Of Day Range Policy.
todsuite	TOD Suite - Time Of Day Suite Policy for Egress and Ingress Entries.
topology	CPAM: Topology - All CPAM topology configurations including BGP, IS-IS, OSPF, CPAA, Links, Routers, Areas, Subnets, Checkpoints, and Route Alarms.
topologysim	CPAM: Simulated Topology - CPAM simulated IGP topology including Links, Routers, Areas, Subnets, and IP Paths.
trapmapper	Trap to Alarm Mapper - Trap to Alarm Mapper.
tunnelmgmt	Tunnel Management - All Tunnel related objects including Hubs, Spokes, Meshes, Chains, Rings, Two Neighbor, Class Forwarding and Rule-based Groups.
udprelay	UDP Relay - UDP Relay configuration and services for layer2.Bridge, DHCP Snooping for VLANs and Ports.
udptunnel	UDP Tunnel - Access to UDP Tunnel.
user	User Preference - SAM Client GUI preferences for Info Tables.

Table 22 Permissions assigned to 5620 SAM scope of command roles (continued)

Package.Class.Method/Property	Description
vlan	VLAN - Access to this package is for configuring TLS, MVR, Super VLAN, Customer VLAN, SAP and MSAP, Network Interfaces (Uplink Ports) and VLAN configuration for a MST Instance.
vlan.EthernetService	VLAN Ethernet Service - Access to VLAN Ethernet Services.
vlan.L2AccessInterface	VLAN Access Interface - Access to VLAN Access Interfaces.
vlan.Site	VLAN Site - Access to VLAN Sites.
vlan.Vlan	VLAN Service - Access to Virtual LAN (VLAN) Service objects themselves.
vll	VLL - All contained objects are listed. Package access is not currently used.
vll.Endpoint	Endpoint - Access to VLL Endpoints.
vll.L2AccessInterface	L2 Access Interface - Access to VLL L2 Access Interfaces (except lpipe).
vpls	VPLS - Access to this package is for configuring MLD Snooping, PIM Snooping, DHCP Relay, Multicast CAC Level and LAG Port Down events, and discovered VLAN Elements.
vpls.BL2AccessInterface	VPLS B-L2 Access Interface - Access to VPLS B-L2 Access Interfaces on a VPLS Service.
vpls.BSite	VPLS B-Site - Access to VPLS B-Sites on a VPLS Service.
vpls.Endpoint	VPLS Endpoint - Access to VPLS Endpoints on a VPLS Service.
vpls.EvpnSite	VPLS eVPN-Site - Access to VPLS eVPN-Sites on a VPLS Service.
vpls.IL2AccessInterface	VPLS I-L2 Access Interface - Access to VPLS I-L2 Access Interfaces on a VPLS Service.
vpls.ISite	VPLS I-Site - Access to VPLS I-Sites on a VPLS Service.
vpls.L2AccessInterface	VPLS L2 Access Interface - Access to VPLS L2 Access Interfaces (except I and B) on a VPLS Service.
vpls.L2ManagementInterface	VPLS L2 Management Interface - Access to VPLS L2 Management Interfaces on a VPLS Service.
vpls.Site	VPLS Site - Access to VPLS Sites (except I and B) on a VPLS Service.
vpls.Vpls	VPLS Service - Access to Virtual Private LAN Service (VPLS) Service objects themselves.

Table 22 Permissions assigned to 5620 SAM scope of command roles (continued)

Package.Class.Method/Property	Description
vprn	VPRN - Access to this package is for configuring VPRN Router Instance Sites, SNMP Community, IPsec Interfaces, Group Interfaces, SAPs, MSAPs, IGMP Host Tracking on Sites and SAPs, and FR Interface Specifics for VPRN specific SAPs.
vprn.AalInterface	VPRN AA Interface - Access to VPRN AA Interfaces.
vprn.DVRSSite	VPRN dVRS Site - Access to dVRS VPRN Sites on a VPRN service.
vprn.IPMirrorInterface	IP Mirror Interface - Access to VPRN IP Mirror Interfaces.
vprn.L3AccessInterface	VPRN L3 Access Interface - Access to VPRN L3 Access Interfaces.
vprn.Site	VPRN Site - Access to VPRN Sites.
vprn.SubscriberInterface	VPRN Subscriber Interface - Access to VPRN Subscriber Interfaces.
vprn.Vprn	VPRN Service - Access to Virtual Private Routed Network (VPRN) Service objects themselves.
vprn.VprnPing	VPRN Ping - Access to VPRN Ping tests, VPRN Ping test definitions, and VPRN Ping deployed tests.
vprn.VprnTrace	VPRN Trace - Access to VPRN Trace tests, VPRN Trace test definitions, and VPRN Trace deployed tests.
vrrp	VRRP - Virtual Router Redundancy Protocol (VRRP) configuration on rtr.NetworkInterface, IES and VPRN access interfaces, Authentication Keys, Priority Control Policies and Events.
vs	Scheduler Policy - Scheduler Policies.
webclient	WebClient - Access to the WebClient.
wlangw	WLAN Gateway - WiFi Offload.
workspace	Workspace - Ability to view workspaces, and Create/Edit/Delete private workspaces.
workspace.WorkspaceManager.method_publicControl	Workspace Manager - method_publicControl - Ability to create/edit/delete public workspaces.
wpp	WPP - Web Portal Protocol.
wpp.Site	WPP Site - Access to WPP Sites.

A.4 Permissions access for scope of command roles

A.4.1 Overview

Each predefined scope of command role has defined access levels to the available permissions based on what the role is designed to do. Permissions grant the following levels of access to an object package, class, method or property:

- Read-only—provides read access to an object class without the ability to create or delete objects.
- Read/write—provides full access to an object class that includes read, create, update/execute, and delete access.
- Read/update/execute—provides read and update/execute access to an object package or property, but does not provide delete access.
- Update/execute—provides update/execute access on class methods, and is typically combined with read access on the parent object package.
- No access.

To view the permission configuration of a scope of command role (default or custom), open the properties form of the role by performing the following steps:

1. Choose Administration→Security→5620 SAM User Security from the main menu. The 5620 SAM User Security manager opens.
2. Click on the Scope of Command tab.
3. Select Role (Security) from the drop-down menu and click Search.
4. Select the required role and click Properties. The Role (Edit) form opens.
5. Click on the Permissions tab.

The Permissions tab lists all permissions and the current access level configured on the scope of command role.

