NOKIA

5620 SAM
SERVICE AWARE MANAGER

14.0 R15

Planning Guide

3HE-10698-AAAN-TQZZA

Issue 1

June 2021

Legal notice

Nokia is committed to diversity and inclusion. We are continuously reviewing our customer documentation and consulting with standards bodies to ensure that terminology is inclusive and aligned with the industry. Our future customer documentation will be updated accordingly.

Contents

About this document

Purpose

This document consolidates the technical information related to the deployment of the Nokia 5620 SAM Release 14.0 product. This document does not focus on the functionality offered by 5620 SAM Release 14.0 but instead presents the reader with pre-installation information required to plan a successful deployment.

The *5620 SAM Planning Guide* is not a comprehensive list of technologies supported or not supported by 5620 SAM or the platforms hosting it. The Nokia NSM Product Group should be consulted for clarification when uncertainty exists.

The *5620 SAM Planning Guide* details the following aspects of the Nokia 5620 SAM product:

- Product deployment overview
- Supported operating systems specifications
- Hardware platform requirements
- Network requirements
- Scaling guidelines
- Workstation configuration
- Firewall information

Intended audience

This document is intended for network engineers, planners and IT staff who are familiar with the functionality of the 5620 SAM and are planning a product deployment.

Document changes

This section highlights the key differences between this release of the *5620 SAM Planning Guide* and the *5620 SAM Planning Guide*, Release 13.0.

Minor differences between the documents, such as updating release version references, are not listed.

- Updated minimum RAM requirement for collocated and SAM Server
- Added client support on Mac OS
- Added Auxiliary PCMD Collector information
- Removed port 8005
- Added OpenStack support
- Updated VMware configuration requirements
- Added port and firewall information for the 5620 SAM Auxiliary Database and 5620 SAM Analytics Server
- Added port 7879 to the Cflowd Auxiliary Collector and updated firewall rules from the Cflowd Auxiliary Collector and SAM Server
- Added client support on Windows 10

- Added Femto Auxiliary

Document support

Customer documentation and product support URLs:

- Customer Documentation Welcome Page
- Technical support

How to comment

Documentation feedback

1 Product deployment overview

1.1 Overview

1.1.1 Purpose

This chapter provides an overview of the 5620 SAM product architecture and deployment.

1.1.2 Contents

1.2 5620 SAM architecture

1.2.1 5620 SAM architecture

Seven types of platforms can be present in a 5620 SAM deployment:

- 5620 SAM GUI Client workstation(s)
- 5620 SAM GUI Client Delegate workstation(s)
- 5620 SAM Server
- 5620 SAM Auxiliary (Statistics Collector, Call Trace Collector, Cflowd Collector, PCMD Collector, femto)
- 5620 SAM Auxiliary Database
- 5620 SAM Database
- 5620 SAM Analytics Server

5620 SAM supports co-location of the 5620 SAM Server and 5620 SAM Database software on a single workstation or VM.

5620 SAM also supports a distributed deployment, whereby the 5620 SAM Server and the 5620 SAM Database software components are installed on two different workstations or VMs.

A 5620 SAM Auxiliary can be configured for statistics collection, call trace collection, cflowd statistics collection, PCMD collection, or bulkCM file creation but can only be configured to perform one of these functions.

5620 SAM supports the distribution of statistics collection. Statistics collection with a 5620 SAM Auxiliary uses either the 5620 SAM Database or the 5620 SAM Auxiliary Database for statistics record storage.

The 5620 SAM Auxiliary Database is deployed in a cluster of a minimum of three servers or VMs and when used with the 5620 SAM Auxiliary Statistics Collector, can be used to collect higher rates of accounting, performance, and application assurance accounting statistics and to increase retention of accounting and performance statistics. The 5620 SAM Auxiliary Database can only be used when statistics collection is performed with the 5620 SAM Auxiliary Statistics Collector. The server BIOS CPU frequency scaling must be disabled on any platform hosting the 5620 SAM Auxiliary Database.

The 5620 SAM Analytics Server is deployed on a separate workstation or VM and is used in conjunction with the Auxiliary Database Cluster to generate custom generated analytics reports based upon application assurance or cflowd statistics.

5620 SAM supports redundancy of the 5620 SAM Server, 5620 SAM Database, 5620 SAM Auxiliary Collector, and 5620 SAM Analytics Server workstations. The 5620 SAM Auxiliary Statistics Collector supports 3+1 redundancy.

The 5620 SAM Auxiliary Database is deployed in a cluster of at least three separate instances and can tolerate a single server failure with no data loss.

A 5620 SAM Auxiliary Statistics Collector must be installed on an independent workstation or VM and can only be configured in a 5620 SAM distributed deployment.

A 5620 SAM Auxiliary Call Trace Collector must be installed on an independent workstation or VM to collect the call trace information from WMM/vMM network elements. Up to two active 5620 SAM Auxiliary Call Trace Collector workstations can be installed to scale the collection of call trace information. Each active 5620 SAM Auxiliary Call Trace Collector workstation can be assigned to a redundant workstation. Call trace information is synchronized between the redundant pairs. The 5620 SAM Auxiliary Call Trace Collector workstations can be configured in either a 5620 SAM distributed or collocated deployment.

A 5620 SAM Auxiliary Cflowd Collector must be installed on an independent workstation or VM to collect cflowd flow records from the network. The 5620 SAM Auxiliary Cflowd Collector does not use a traditional redundancy model. Instead, the 7750s can be configured to send cflowd flows to multiple 5620 SAM Cflowd Auxiliaries. The 5620 SAM Auxiliary Cflowd Collector workstations can be configured in either a 5620 SAM distributed or collocated deployment.

A 5620 SAM Auxiliary PCMD Collector must be installed on an independent workstation or VM to collect PCMD data streams from the network. The 5620 SAM Auxiliary PCMD Collector workstations can be configured in either a 5620 SAM distributed or collocated deployment and is supported in a redundant configuration.

A 5620 SAM Femto Auxiliary must be installed on an independent workstation to offload bulkCM file generation in networks containing more that 800,000 MS HC access points. The 5620 SAM Femto Auxiliary is supported in a redundant configuration.

More details on redundancy in 5620 SAM can be found in 1.4 “Redundancy architecture” (p. 17).

5620 SAM supports IPv4 and IPv6 connectivity between the 5620 SAM Server/Auxiliary to the managed network except for the 5620 SAM Auxiliary Cflowd Collector which cannot collect cflowd flows from an IPv6 managed 7750. Connectivity between the 5620 SAM components fully supports IPv4.

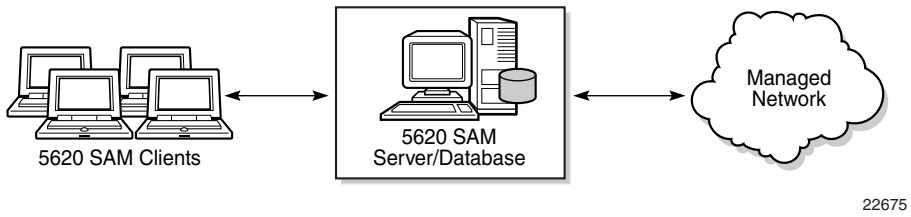
Connectivity between 5620 SAM components supports IPv6 with certain restrictions where the following is not supported:

- 5620 SAM deployments that include the management of 1830 PSS / OCS, 9500 MPR, 9471 WMM, DSC, eNodeBs, Small Cell Access Points / Gateways
- 5620 SAM deployments integrated with 5670 RAM
- 5620 SAM deployments with 5620 SAM Auxiliary Cflowd Collectors
- 5620 SAM deployments with 5620 SAM Auxiliary Database Clusters or 5620 SAM Analytics Server
- 5620 SAM deployments with 5620 SAM Auxiliary PCMD Collectors
- 5620 SAM deployments with the 3GPP OSS interface
- EMS integration with 5620 SAM
- 5620 SAM deployments using SAML SSO
- Dual Stack between SAM components, including clients
- 5620 SAM Clients on Apple Mac OS

A network element can only be managed by one 5620 SAM standalone or redundant deployment. Having multiple 5620 SAM deployments managing the same network element is not supported, and will cause unexpected behavior.

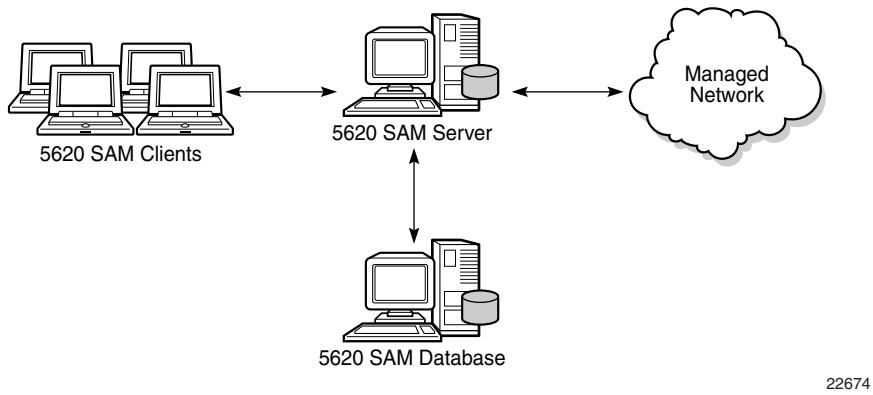
The following illustrates a typical deployment of 5620 SAM in standalone mode when the 5620 SAM Server and 5620 SAM Database functions are collocated.

Figure 1-1 5620 SAM standalone deployment - collocated SAM Server/Database configuration



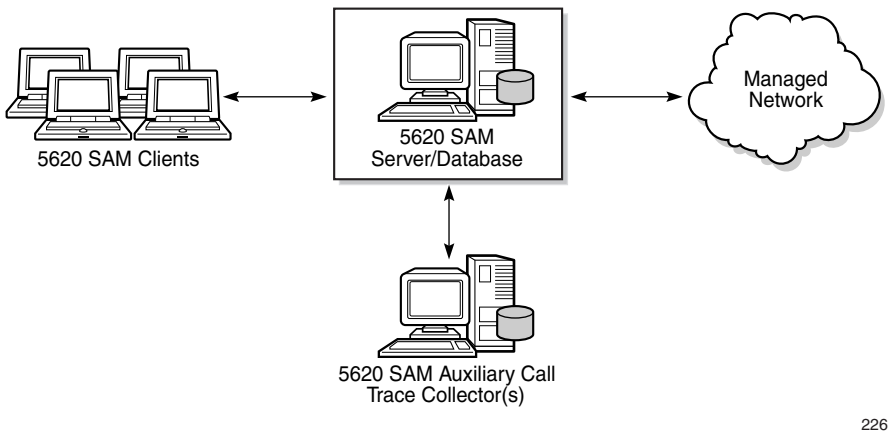
The following illustrates a typical deployment of 5620 SAM in standalone mode when the 5620 SAM Server and 5620 SAM Database functions are not collocated.

Figure 1-2 5620 SAM standalone deployment – distributed 5620 SAM Server and 5620 SAM Database configuration.



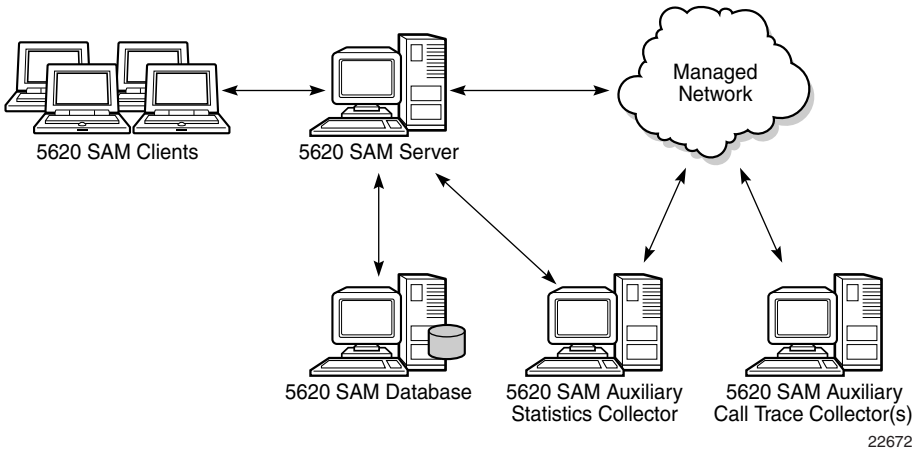
The following illustrates a typical deployment of 5620 SAM in standalone mode when the 5620 SAM Server and 5620 SAM Database functions are collocated and a 5620 SAM Auxiliary Call Trace Collector is used. The 5620 SAM Auxiliary Statistics Collector is not supported in this configuration.

Figure 1-3 5620 SAM standalone deployment – collocated 5620 SAM Server and 5620 SAM Database configuration and 5620 SAM Auxiliary Call Trace Collector



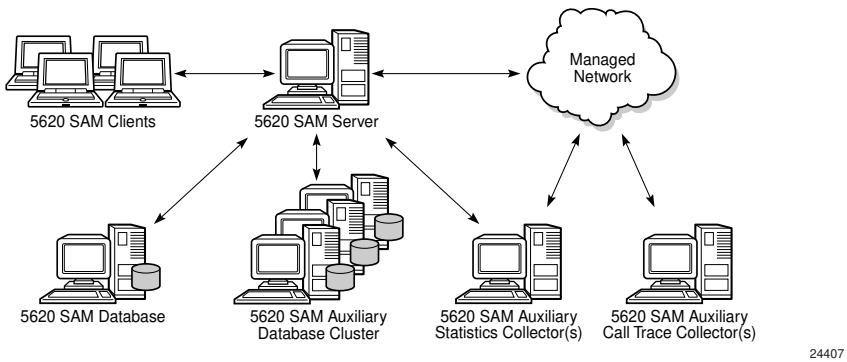
The following illustrates a typical deployment of 5620 SAM in standalone mode when the 5620 SAM Server and 5620 SAM Database functions are in a distributed configuration and 5620 SAM Auxiliary Collectors are used. In this configuration there can be up to three active 5620 SAM Auxiliary Statistics Collectors or it could be configured redundant, and there can be one or two 5620 SAM Auxiliary Call Trace Collectors collecting call trace data from the network.

Figure 1-4 5620 SAM standalone deployment - distributed 5620 SAM Server and 5620 SAM Database configuration and 5620 SAM Auxiliary Collectors



The following illustrates a deployment of 5620 SAM in standalone mode when the 5620 SAM Server and 5620 SAM Database functions are in a distributed deployment and 5620 SAM Auxiliary Collectors are installed with statistics collection using the 5620 SAM Auxiliary Database. In this configuration, there can be up to three preferred 5620 SAM Auxiliary Statistics Collectors or it could be configured redundant as n+1. There can be one or two 5620 SAM Auxiliary Call Trace Collectors collecting call trace data from the network with redundancy of the 5620 SAM Call Trace Collector supported. The 5620 SAM Auxiliary Database must always be installed in a cluster of at least three instances.

Figure 1-5 5620 SAM standalone deployment - distributed 5620 SAM Server and 5620 SAM Database configuration and 5620 SAM Auxiliary Collectors with statistics collection using the 5620 SAM Auxiliary Database



For bare metal installations, the 5620 SAM Server, 5620 SAM Auxiliary Collector, 5620 SAM Auxiliary Database, 5620 SAM Analytics Server, and 5620 SAM Database are supported on

specific Intel x86 based HP workstations and for some configuration, specific Nokia AirFrame servers are also supported. In a redundant configuration, the workstation architecture of the redundant pair must match along with the physical hardware resources. The CPU type of the server must match as well.

The 5620 SAM Client and Client Delegate software may be installed on workstations running different operating systems from the 5620 SAM Server, 5620 SAM Auxiliary, 5620 SAM Auxiliary Database, 5620 SAM Analytics Server, and 5620 SAM Database. The 5620 SAM Client can be installed on RHEL Server x86-64, RHEL Server x86, Windows, or Mac OS where the 5620 SAM Client Delegate can be installed on RHEL Server x86-64, or Windows Server 2008R2 and Server 2012. Refer to Chapter 2, “Operating systems specifications” for Operating System specifics.

All 5620 SAM workstations in the 5620 SAM management complex must maintain consistent and accurate time. It is recommended that NTP be used to accomplish this requirement.

1.2.2 5620 SAM Auxiliary Statistics Collector

This type of 5620 SAM Auxiliary collects and processes performance, accounting, application assurance and performance management statistics along with OAM PM test results. This option enables customers to reduce the load of statistics collection from the 5620 SAM Server while allowing for increased statistics collection capabilities. A 5620 SAM Auxiliary Statistics Collector workstation should be used when statistics collection is expected to exceed the capacity of the 5620 SAM Server. Refer to Chapter 3, “Platform requirements” for scalability details of the 5620 SAM Server and dimensioning of the 5620 SAM Auxiliary Statistics Collector workstation.

The 5620 SAM Auxiliary Statistics Collector can be configured as Preferred, Reserved, or Remote for a given 5620 SAM Server (Active or Standby). This allows for a redundant 5620 SAM Auxiliary Statistics Collector configuration. Statistics collection using the SAM Database allows only one 5620 SAM Auxiliary Statistics Collector to collect statistics at any given time. When collecting statistics using the 5620 SAM Auxiliary Database or using logToFile only, up to three 5620 SAM Auxiliary Statistics Collectors can collect statistics concurrently. Information on the redundancy model of the 5620 SAM Auxiliary Statistics Collector can be found in 1.4 “Redundancy architecture” (p. 17) .

The 5620 SAM Server and the 5620 SAM Auxiliary Statistics Collector must maintain consistent and accurate time. It is encouraged to use an NTP service to achieve this. An alarm will be raised if the times are not within 30 seconds. Variations in time can cause the system to stop collecting statistics prematurely.

In networks where 5620 SAM Auxiliary Statistics Collector workstations are not configured, the 5620 SAM Server handles the statistics collection. In networks where the 5620 SAM Auxiliary Statistics Collector is configured, the 5620 SAM Server will never collect statistics – regardless of the availability of the 5620 SAM Auxiliary Statistics Collector workstations. At least one 5620 SAM Auxiliary Statistics Collector workstation must be available for statistics collection to occur.

The 5620 SAM Auxiliary Statistics Collector is only supported with a distributed 5620 SAM Server and 5620 SAM Database.

For collection of performance management statistics from eNodeB network elements, NTP should be used to synchronize the network element and the 5620 SAM Server and 5620 SAM Auxiliary Statistics Collector to ensure the statistics are successfully retrieved.

1.2.3 5620 SAM Auxiliary Call Trace Collector

This type of 5620 SAM Auxiliary collects call trace files from WMM and VMM network elements.

Up to two 5620 SAM Auxiliary Call Trace Collectors can be configured to collect call trace information in 5620 SAM, and each of those collectors can be configured to be redundant. Each 5620 SAM Auxiliary Call Trace Collector is installed on a separate workstation. Each 5620 SAM Auxiliary Call Trace Collector is configured as a preferred for the 5620 SAM Active Server and as a reserved for the 5620 SAM Standby Server. This allows for a redundant 5620 SAM Auxiliary Call Trace Collector configuration. Only one of the workstations in the 5620 SAM Auxiliary Call Trace Collector redundant pair will collect the call trace information from the network elements at any given time and the call trace information is synchronized between the Preferred and Reserved pair of workstations. Information on the redundancy model of the 5620 SAM Auxiliary Call Trace Collector can be found in 1.4 “Redundancy architecture” (p. 17) .

The 5620 SAM Auxiliary Call Trace Collector is supported with both a collocated 5620 SAM Server and 5620 SAM Database or distributed 5620 SAM Server and 5620 SAM Database.

The 5620 SAM Auxiliary Call Trace Collector workstation must maintain consistent and accurate time. It is encouraged to use an NTP service to achieve this. An alarm will be raised if the times are not within 30 seconds.

1.2.4 5620 SAM Auxiliary Cflowd Collector

This type of 5620 SAM Auxiliary collects cflowd flow data from 7750 network elements.

The 5620 SAM Auxiliary Cflowd Collector operates in a standalone mode generating IPDR files for the 7750 managed network elements that are configured to send cflowd flow data to it where each 7750 can be configured to send cflowd flow data to multiple 5620 SAM Auxiliary Cflowd Collectors. Each 5620 SAM Auxiliary Cflowd Collector will generate IPDR files for the cflowd data it is sent, resulting in duplicate data being sent to the target file server.

The 5620 SAM Auxiliary Cflowd Collector is supported with both a collocated 5620 SAM Server and 5620 SAM Database or distributed 5620 SAM Server and 5620 SAM Database.

The 5620 SAM Auxiliary Cflowd Collector workstation must maintain consistent and accurate time. It is encouraged to use an NTP service to achieve this.

1.2.5 5620 SAM Auxiliary PCMD Collector

The 5620 SAM Auxiliary PCMD Collector collects PCMD data from the SGW/PGW network elements that are configured to stream per call measurement data to it. The 5620 SAM Auxiliary PCMD Collector generates CSV files from the PCMD data, that can be sent to a third party application for post processing.

The 5620 SAM Auxiliary PCMD Collector is supported with both a collocated 5620 SAM Server and 5620 SAM Database or distributed 5620 SAM Server and 5620 SAM Database.

The 5620 SAM Auxiliary PCMD Collector workstation must maintain consistent and accurate time. It is encouraged to use an NTP service to achieve this.

1.2.6 5620 SAM Femto Auxiliary

The 5620 SAM Femto Auxiliary is used to offload bulkCM file generation from the 5620 SAM Server. This is required for networks that will manage greater than 800,000 MS HC access points.

The 5620 SAM Femto Auxiliary is supported with both a collocated 5620 SAM Server and 5620 SAM Database or distributed 5620 SAM Server and 5620 SAM Database although to support 800,000 HC access points, a distributed 5620 SAM configuration is required.

The 5620 SAM Auxiliary PCMD Collector workstation must maintain consistent and accurate time. It is encouraged to use an NTP service to achieve this.

1.2.7 5620 SAM Client Delegate

This option enables customers to launch multiple 5620 SAM GUI Clients from a single Windows Server 2008R2, Windows 2012(R2), or RHEL Server x86-64 workstation. For RHEL Server x86-64 installations, these GUI clients can be displayed using the X11 protocol to other RHEL desktops or native X displays. For Windows Server 2008R2 installations, these GUI clients can be displayed using Windows Remote Desktop. Displaying GUI clients to computers running X-emulation software is not currently supported.

The Client Delegate platform provides an option to consolidate multiple installations of the 5620 SAM GUI Client on a single workstation. Individual 5620 SAM Clients can be installed on the Client Delegate. The 5620 SAM Client also supports the ability for multiple users to share a single installation; however, each user must run the client with a unique UNIX id.

Information on dimensioning the 5620 SAM Client Delegate platform is given in 3.4 “Minimum platform requirements” (p. 34) .

1.3 5620 SAM key technologies

1.3.1 Overview

This section describes the key technologies used to support 5620 SAM features.

1.3.2 Java Virtual Machine

The 5620 SAM Server, 5620 SAM Auxiliary, 5620 SAM Database, and 5620 SAM Client applications use Java technology. The installation packages contain a Java Virtual Machine which is installed with the software. This is a dedicated Java Virtual Machine and does not conflict with other Java Virtual Machines which may be installed on the same workstation.

5620 SAM uses Java Virtual Machine version 8 from Oracle.

1.3.3 Oracle Database

The 5620 SAM Database embeds an installation of Oracle 12c Release 1 Enterprise Edition, which is installed with the 5620 SAM Database. This database is used to store information about the managed network. The installation of Oracle is customized for use with the 5620 SAM application and must be dedicated to 5620 SAM. 5620 SAM database redundancy uses Oracle DataGuard, and is configured in maximum performance mode.

Nokia will not support any configuration deviations from the Oracle installation as performed by the 5620 SAM Database installation package, as it represents a 5620 SAM License Agreement Violation. Modifying the Oracle installation can impact system performance, stability and upgrades. Customer support agreements may be violated.

The Oracle Database is embedded with the 5620 SAM Product and because of this; Oracle requires all licenses to be purchased from Nokia. This applies to customers with Oracle Site licenses as well. The SAM Database licensing is based on the number of physical CPU Cores installed in the dedicated SAM database or a co-located configuration or the number of vCPUs allocated to the SAM Database or a collocated configuration.

Oracle's official support position for running Oracle Database 12c, embedded within 5620 SAM, on VMware hosted virtual environments is described in Oracle Support Note 249212.1. Oracle will only provide support for issues that either are known to occur on the native Operating System, or can be demonstrated not to be as a result of running on VMware. In addition, VMware has a public statement committing to assist with resolving Oracle Database issues. Nokia will work with Oracle and VMware to resolve any 5620 SAM DB issues but due to the lack of official Oracle support, problem resolution times may be impacted in some cases. Customers should be aware of and must accept this risk when choosing to run 5620 SAM in a VMware virtualized environment.

Oracle's official support position for running Oracle Database 12c, embedded within 5620 SAM, on RHEL KVM hosted virtual environments is that Oracle does not certify any of their products in this environment. Nokia will work with Oracle and Red Hat to resolve any 5620 SAM DB issues but due to the lack of Oracle support, problem resolution times may be impacted in some cases. Customers should be aware of and must accept this risk when choosing to run 5620 SAM in a RHEL KVM virtualized environment.

1.4 Redundancy architecture

1.4.1 Overview

Redundancy between 5620 SAM Server and Database applications is used to ensure visibility of the managed network is maintained when one of the following failure scenarios occur:

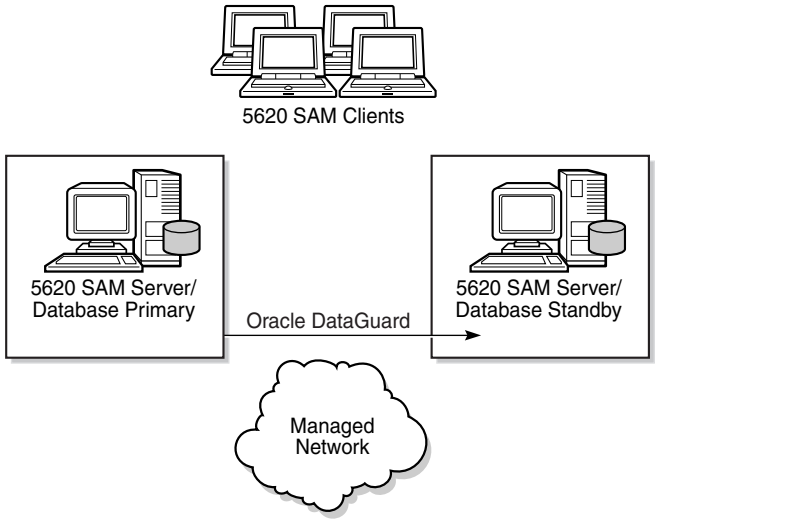
- Loss of physical network connectivity between 5620 SAM Server and/or 5620 SAM Database and the managed network
- Hardware failure on workstation hosting the 5620 SAM Server and/or 5620 SAM Database software component

5620 SAM supports redundancy of the 5620 SAM Server and 5620 SAM Database components in the following configurations:

- 5620 SAM Server and 5620 SAM Database collocated configuration
- 5620 SAM Server and 5620 SAM Database distributed configuration

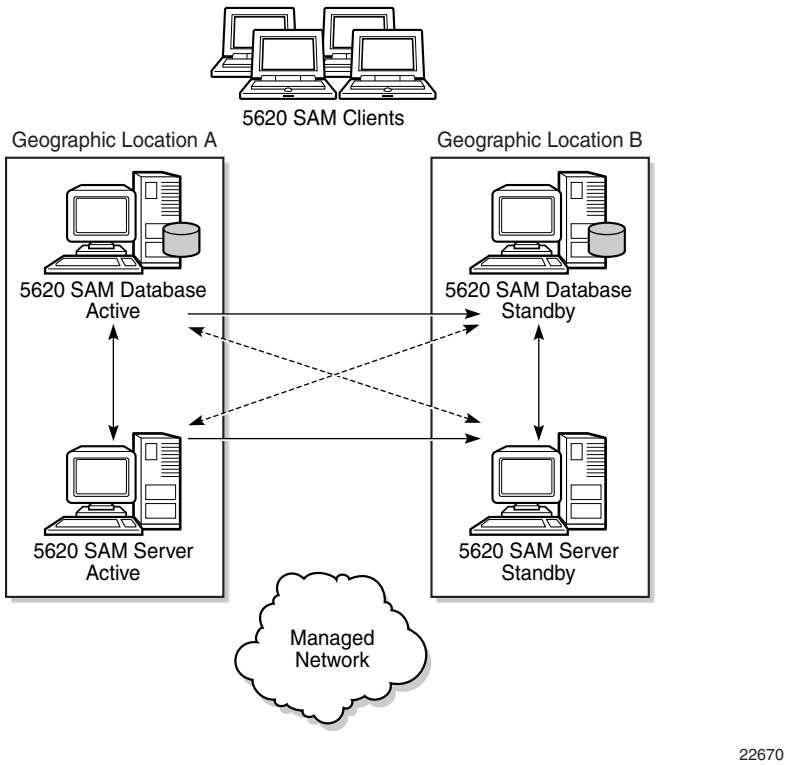
The following illustrates a 5620 SAM redundant installation when the 5620 SAM Server and 5620 SAM Database components are installed in a collocated configuration.

Figure 1-6 5620 SAM collocated Server/Database redundancy deployment



The following illustrates a 5620 SAM redundant installation when the 5620 SAM Server and 5620 SAM Database components are located on different workstations.

Figure 1-7 5620 SAM distributed Server/Database redundancy deployment in a geographically redundant setup.



1.4.2 Redundancy and 5620 SAM Auxiliary workstations

In customer networks where the statistics collection requirements exceed the scalability capabilities of a 5620 SAM Server, the 5620 SAM Auxiliary Statistics Collector can be used. As with other high availability components, 5620 SAM Auxiliary Statistics Collector can be configured to be redundant. When collecting statistics using the 5620 SAM Database, each 5620 SAM Server can be configured to have one preferred and one reserved 5620 SAM Auxiliary Statistics Collector. When collecting statistics using the 5620 SAM Auxiliary Database or using logToFile only, each 5620 SAM Server can be configured with up to three preferred and one reserved 5620 SAM Auxiliary Statistics Collector.

When Call Trace information is being collected from WMM and VMM network elements in customer networks, a 5620 SAM Auxiliary Call Trace Collector must be used. The 5620 SAM Auxiliary Call Trace Collector can be installed in a redundant pair. Up to two 5620 SAM Auxiliary Call Trace Collector redundant pairs can be installed.

In customer networks where cflowd flow data is being collected from 7750 network elements, a 5620 SAM Auxiliary Cflowd Collector must be used. The 5620 SAM Auxiliary Cflowd Collector can only be installed in a standalone configuration. To achieve data redundancy, 7750s can be configured to forward cflowd flow data to multiple 5620 SAM Auxiliary Cflowd Auxiliaries.

The collection of per call measurement data from SGW/PGW network elements, a 5620 SAM Auxiliary PCMD Collector must be used. The 5620 SAM Auxiliary PCMD Collector can be installed in a standalone or redundant configuration. Data collected by the 5620 SAM Auxiliary PCMD Collector is not replicated to the redundant collector.

The generation of bulkCM files by the 5620 SAM Femto Auxiliary is required if more than 800,000 MS HC access points are managed. The 5620 SAM Femto Auxiliary can be installed in a standalone or redundant configuration. Data generated by the 5620 SAM Femto Auxiliary is not replicated to the redundant server.

In Figure 1-8, “5620 SAM distributed Server/Database redundant deployment with redundant 5620 SAM Auxiliaries that crosses geographic boundaries” (p. 21) there are 5620 SAM Auxiliary Collectors configured. In the example where redundancy is geographic, there can be up to four 5620 SAM Auxiliary Statistics Collectors and up to two 5620 SAM Auxiliary Call Trace Collector workstations configured in each geographic location. The Preferred/Reserved/Remote role of the 5620 SAM Auxiliary Statistics Collector is dependent and configured on the 5620 SAM Server that is active. When there are more than one active Auxiliary Statistics Collector, local redundancy (Preferred/Reserved) of the Auxiliary Statistics Collector must be used in conjunction with geographic redundancy, where the same number of Auxiliary Statistics Collectors will be deployed in each geographic site. The 5620 SAM Auxiliary Statistics Collectors in the opposite geographic location are configured to be Remote. In this scenario, if one of the 5620 SAM Auxiliary Statistics Collectors for the active 5620 SAM Server were no longer available, the active 5620 SAM Server would use the reserved 5620 SAM Auxiliary Statistics Collector in the same geographic location to collect statistics. Figure 1-9, “5620 SAM distributed Server/Database redundant deployment with redundant 5620 SAM Auxiliaries using the 5620 SAM Auxiliary Database for statistics collection” (p. 22) shows the same redundant configuration but with statistics collection using the 5620 SAM Auxiliary Database. Latency between geographic sites must be less than 200 ms.

Figure 1-8 5620 SAM distributed Server/Database redundant deployment with redundant 5620 SAM Auxiliaries that crosses geographic boundaries

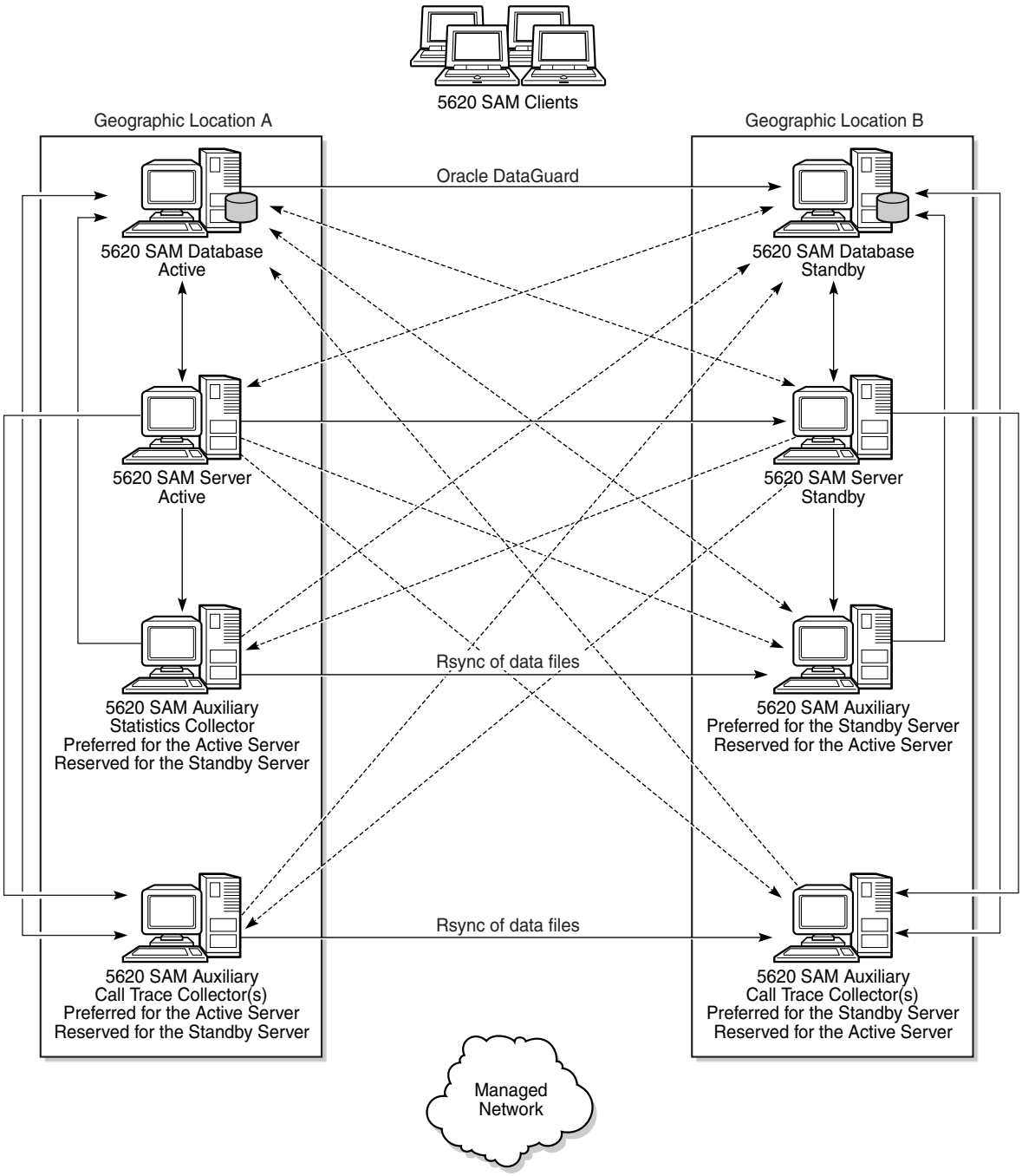
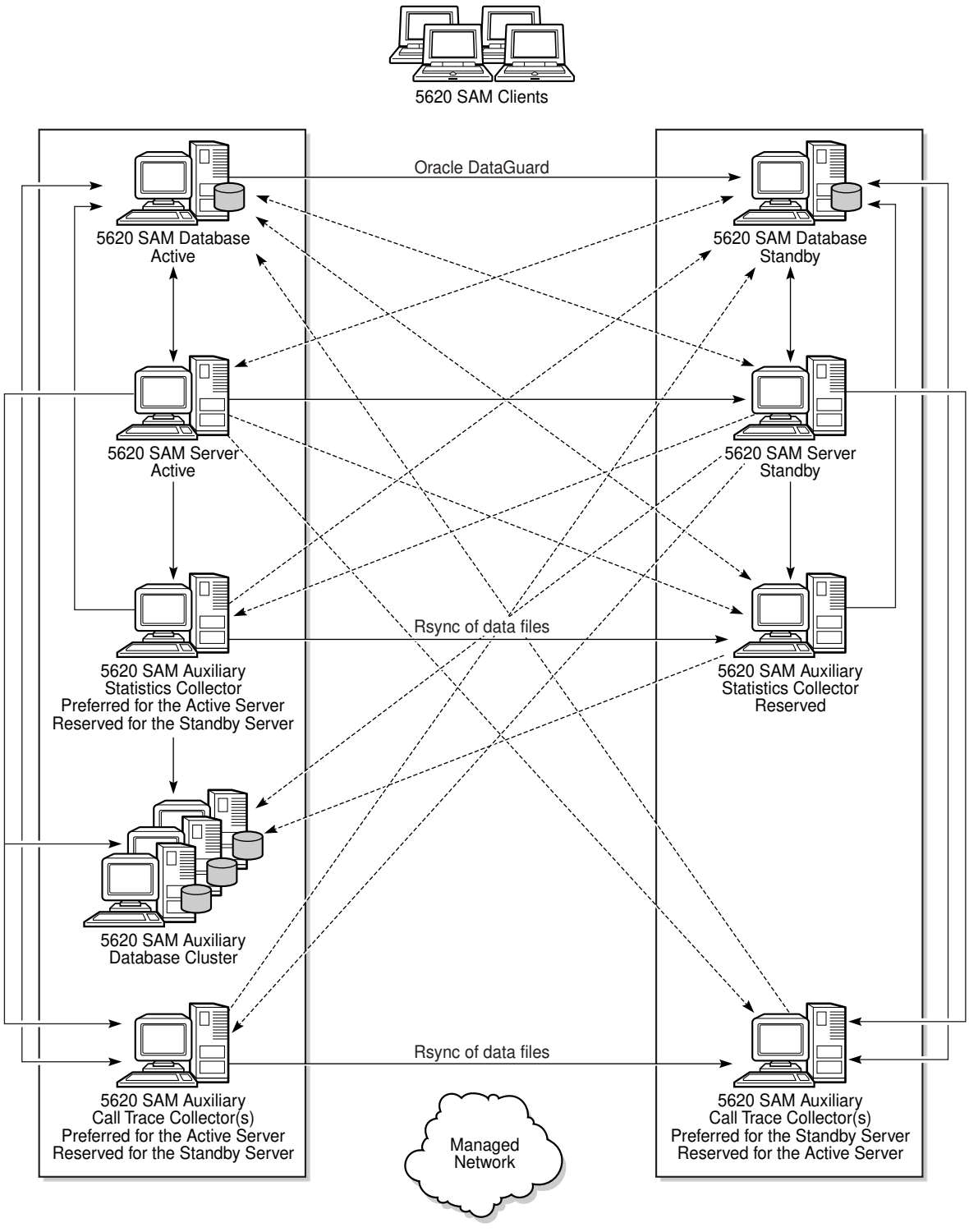


Figure 1-9 5620 SAM distributed Server/Database redundant deployment with redundant 5620 SAM Auxiliaries using the 5620 SAM Auxiliary Database for statistics collection



Further information about 5620 SAM redundancy can be found in the *5620 SAM User Guide*

1.5 Redundancy deployment considerations for 5620 SAM

1.5.1 Overview

When deploying 5620 SAM in a redundant configuration, the following items should be considered.

It is a best practice to keep the 5620 SAM Server, 5620 SAM Database, and 5620 SAM Auxiliary Collectors in the same geographic site to avoid the impact of network latency. When the 5620 SAM Database or 5620 SAM Server switches sites, the 5620 SAM auto-align functionality will ensure the SAM Server, and 5620 SAM Auxiliary Collectors are all aligned in the same geographic location. If the auto-align functionality is not enabled, a manual switch of the workstations is desirable.

1.5.2 Redundancy with collocated 5620 SAM Server/Database

Requirements:

- The operating systems installed on the primary and standby 5620 SAM Server/Database must be of the same versions and at the same patch levels.
- The layout and partitioning of the disks containing the 5620 SAM software, the Oracle software and the database data must be identical on the active and standby 5620 SAM Server/Database.
- The machine which will be initially used as the active 5620 SAM Server/Database must be installed or upgraded before the machine that will initially be used as the standby.
- The workstations hosting the 5620 SAM software should be connected in a way to prevent a single physical failure from isolating the two workstations from each other.
- Workstations running the 5620 SAM Server/Database software must be configured to perform name service database lookups on the local workstation before reverting to a name service database located on the network such as NIS, NIS+, or DNS. A root user must inspect and modify the /etc/nsswitch.conf file to ensure that files is the first entry specified for each database listed in the file.

1.5.3 Redundancy with distributed 5620 SAM Server and 5620 SAM Database

Requirements:

- The operating systems installed on the primary and standby 5620 SAM Server as well as the primary and standby 5620 SAM Database must be of the same versions and at the same patch levels.
- The layout and partitioning of the disks containing the 5620 SAM software, the Oracle software and the database data must be identical on the primary and standby 5620 SAM Database.
- The machines which are intended to be used as primary 5620 SAM Server and 5620 SAM Database should be installed on the same LAN as one another with high quality network connectivity.

- The machines which are intended to be used as standby 5620 SAM Server and standby 5620 SAM Database should be installed on the same LAN as one another with high quality network connectivity.
- The pair of workstations to be used as active 5620 SAM Server and 5620 SAM Database should be connected to the pair of workstations to be used as standby 5620 SAM Server and 5620 SAM Database in a way that will prevent a single physical failure from isolating the two workstation pairs from each other.
- Workstations running the 5620 SAM Server and 5620 SAM Database software must be configured to perform name service database lookups on the local workstation before reverting to a name service database located on the network such as NIS, NIS+, or DNS. A root user must inspect and modify the /etc/nsswitch.conf file to ensure that *files* is the first entry specified for each database listed in the file.

1.5.4 Redundancy with distributed 5620 SAM Server and 5620 SAM Database and 5620 SAM Auxiliary Collectors

In addition to the rules stated above for distributed 5620 SAM Server and 5620 SAM Database, the following rules apply:

- The operating systems installed on the 5620 SAM Auxiliary Collectors must be of the same versions and patch levels as the 5620 SAM Server and 5620 SAM Database workstations.
- If collecting statistics using the 5620 SAM Auxiliary Database, the operating systems installed on the 5620 SAM Auxiliary Database workstations must be of the same versions and patch levels as the 5620 SAM Server, 5620 SAM Database, and 5620 SAM Auxiliary Statistics Collector workstations.
- 5620 SAM Auxiliary Collectors are intended to be on the same high availability network as the 5620 SAM Server and 5620 SAM Database. 5620 SAM Auxiliary Statistics, Call Trace, and PCMD Collectors and Femto Auxiliaries are intended to be geographically collocated with the Active and Standby locations of the 5620 SAM Server and 5620 SAM Database. The 5620 SAM Auxiliary Cflowd Collector typically resides in the managed network, closer to the network elements.
- When using more than one Active 5620 SAM Auxiliary Statistics Collector in a geographic (greater than 1ms latency) configuration, the Active and Reserved Collectors for a give SAM Server must reside in the same geographic site. The Auxiliary Statistics Collectors in the opposite geographic site would be configured as Remote.
- Workstations running the 5620 SAM Auxiliary Collector software must be configured to perform name service database lookups on the local workstation before reverting to a name service database located on the network such as NIS, NIS+, or DNS. A root user must inspect and modify the */etc/nsswitch.conf* file to ensure that *files* is the first entry specified for each database listed in the file.

2 Operating systems specifications

2.1 Overview

2.1.1 Purpose

This chapter describes the OS requirements for the 5620 SAM.

2.1.2 Contents

2.2 Operating systems specifications

2.2.1 Red Hat Enterprise Linux (RHEL)

5620 SAM is supported on Red Hat Enterprise Linux 7, Server Edition x86-64 for the 5620 SAM Server, 5620 SAM Auxiliary Collector, 5620 SAM Auxiliary Database, 5620 SAM Analytics Server, 5620 SAM Database, 5620 SAM Client Delegate, and 5620 SAM Client. The 5620 SAM Client is also supported on Red Hat Enterprise Linux 7, Server Edition x86. Previous releases or other variants of Red Hat and other Linux variants are not supported.

5620 SAM Release 14.0 R15 supports the following base RHEL versions:

- RHEL Server 7(x86-64 / x86) - Update 8 (7.8)
- RHEL Server 7(x86-64 / x86) - Update 9 (7.9)

The Red Hat Linux support of 5620 SAM is applicable to specific x86 Intel platforms provided by HP and Nokia only, for bare metal installations, where some systems may require specific updates of the RHEL operating system. See Red Hat's Hardware Certification list on their website. 5620 SAM does not necessarily support all functionality provided in RHEL 7(for example SELinux).

5620 SAM supports the use of the RHEL Logical Volume Manager (LVM) on all server types except for the 5620 SAM Auxiliary Database. The support of LVM is limited to the resizing of logical volumes only. To ensure that disk throughput and latency of the resized volume remains consistent, the procedure Adding LVM disk space, in the System Administrator Guide, must be followed.

The RHEL operating system must be installed in 64-bit mode where the 5620 SAM Server, 5620 SAM Auxiliary Collector, 5620 SAM Auxiliary Database, 5620 SAM Analytics Server, 5620 SAM Database, or 5620 SAM Client Delegate software will be installed. 32-bit mode is supported for the 5620 SAM Client only.

The 5620 SAM Server, 5620 SAM Auxiliary Collector, 5620 SAM Auxiliary Database, 5620 SAM Analytics Server, 5620 SAM Client Delegate, and 5620 SAM Database workstation RHEL operating system must be installed in English.

Red Hat support must be purchased for all platforms running RHEL Server with 5620 SAM. It is strongly recommended to purchase a support package from Red Hat that provides 24x7 support.

Nokia recommends the installation of any OS, driver, or firmware updates that the hardware vendor advises for RHEL.

With the exception of 5620 SAM documented Operating System parameter changes, all other settings must be left at the RHEL default configuration.

2.2.2 Microsoft Windows

The Windows operating system is only supported for 5620 SAM Clients and 5620 SAM Client Delegate Servers. The table below summarizes Microsoft Windows support.

Table 2-1 Windows operating system support summary

Microsoft Windows Version	5620 SAM Client	5620 SAM Client Delegate Server
Windows 7 Professional	Supported	Not-supported
Windows 8 / 8.1 Enterprise	Supported (64-bit)	Not-supported
Windows 10 Professional	Supported	Not-supported
Windows Server 2008R2	Supported	Supported
Windows Server 2012	Supported	Supported

When installing the 5620 SAM Client on Windows, ensure that there is sufficient disk space as identified in the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for the software.

2.2.3 Apple Mac OS

The Mac OS operating system is only supported for 5620 SAM Clients when used with Mac OS X Yosemite.

2.2.4 Operating system summary

The following table summarizes the supported configurations for each of the Operating Systems supported by 5620 SAM.

Table 2-2 5620 SAM operating system support summary

5620 SAM application	RHEL 7 Server x86-64	RHEL 7 Server x86	Microsoft Windows	Mac OS
5620 SAM Server	Supported	Not-supported	Not supported	Not supported
5620 SAM Database	Supported	Not-supported	Not-supported	Not supported
Collocated 5620 SAM Server/Database	Supported	Not-supported	Not supported	Not supported
5620 SAM Client	Supported	Supported	Supported	Supported
5620 SAM Auxiliary	Supported	Not-supported	Not supported	Not supported

Table 2-2 5620 SAM operating system support summary (continued)

5620 SAM application	RHEL 7 Server x86-64	RHEL 7 Server x86	Microsoft Windows	Mac OS
5620 SAM Auxiliary Database	Supported	Not-supported	Not supported	Not supported
5620 SAM Analytics Server	Supported	Not-supported	Not supported	Not supported
5620 SAM Client Delegate	Supported	Not-supported	Supported	Not supported

2.3 5620 SAM Client or Client Delegate software requirements

2.3.1 5620 SAM Client or Client Delegate software requirements

5620 SAM clients can be launched, installed and uninstalled through a web browser (Web Launch, Install and Uninstall). To use this functionality, each client platform must have a system JRE (Java Runtime Environment) installed. The 5620 SAM web browser installer/launcher requires Oracle Java version 8. update 192 or greater for the system JRE on all Windows, RHEL, and Mac OS platforms. The system JRE needs to be already installed on the client platform. The system JRE is only used for the SAM client web browser installer/launcher, it is not required for installing, launching or running the 5620 SAM client when the web browser launch is not used.

5620 SAM applications are supported on the following web browsers:

- Microsoft Internet Explorer 11
- Latest version of Mozilla Firefox
- Latest version of Google Chrome
- Latest version of Safari

Additional Internet browsers and older versions may function with 5620 SAM applications but are not supported by Nokia.

The NEtO element manager that is cross launched from the 5620 SAM Client UI requires binding to a specific system port on a 5620 SAM Client and therefore a Client Delegate can only support a single NEtO instance running amongst all clients connected to a Client Delegate at any time.

To consolidate 5620 SAM Client UIs to a single server when using the NEtO element manager, a virtualized solution should be used instead, with each 5620 SAM Client residing in a separate VM.

3 Platform requirements

3.1 Overview

3.1.1 Purpose

This section defines the platform requirements for successfully running the 5620 SAM application. Following these platform guidelines is necessary to ensure the 5620 SAM application performs adequately.

3.1.2 Contents

3.2 Hardware platform requirements overview

3.2.1 Hardware platform requirements overview

For all bare metal installations, Nokia requires the use of supported HP or Nokia AirFrame Intel based x86 workstations running RHEL.

For optimal disk I/O performance, the read and write caches must be enabled for each disk / volume. Specific HBA controllers may be required for certain platforms to ensure that the read and write caches can be enabled. The server vendor should be consulted to determine the correct HBA controller to allow the creation of the correct number of volumes and enable the read and write caches.

Redundant installations of 5620 SAM requires matching workstations for the active and inactive platforms. It is acceptable to have different platforms for the Server, Database, and auxiliaries but their redundant platform must be the same.

Applications that are not sanctioned by Nokia should not be running on any of the 5620 SAM server, auxiliary or database workstations. Nokia reserves the right to remove any application from workstations running 5620 SAM components that are suspected of causing issues.

The hardware platforms do not support running applications that are not specifically identified for that platform. For instance, a 5620 SAM client is not supported on the hardware platform for a

distributed or collocated 5620 SAM Server as there is a significant memory requirement for the 5620 SAM client that will impact the behavior of the 5620 SAM Server platform.

In exceptional circumstances, a single 5620 SAM GUI Client can be temporarily run from a 5620 SAM Server, provided that a minimum of 24 GB RAM is installed on the 5620 SAM Server in a distributed configuration, and 32 GB RAM is installed on the 5620 SAM Server/Database in a collocated configuration.

5620 SAM supports the use of the Operating System SNMP agent for monitoring platform availability and system resources. The number of OIDs retrieved must not exceed 100 per minute to ensure 5620 SAM is not negatively impacted.

3.3 Hardware platform and resource requirements using Virtualization

3.3.1 Hardware platform and resource requirements using Virtualization

Virtualization is supported using VMware vSphere ESXi, RHEL KVM, and OpenStack. All other forms of virtualization or virtualization products are not supported.

For installations of the 5620 SAM Server, 5620 SAM Database, and 5620 SAM Auxiliary Collector on a Guest Operating System of a virtualized installation, the Guest Operating System must be a 5620 SAM supported version of RHEL 7 Server x86-64. For installations of the 5620 SAM Client and 5620 SAM Client Delegate on a Guest Operating System of a virtualized installation, the Guest Operating System can be either a 5620 SAM supported version of RHEL 7 Server or Windows.

Defined CPU and Memory resources must be reserved and dedicated to the individual Guest OSs and cannot be shared or oversubscribed. Additional hardware resources should be reserved for use by the host hypervisor installation to ensure that the resources assigned to the Guest OSs is not impacted. Disk and Network resources should be managed appropriately to ensure that other Guest OSs on the same physical server do not negatively impact the operation of 5620 SAM.

Virtualized installations of 5620 SAM are server vendor agnostic but must meet specific hardware criteria and performance targets to be used with 5620 SAM. Server class hardware must be used, not desktops. Processor support is limited to Intel and AMD based x86 CPUs with a minimum CPU core speed of 2.4GHz (unless otherwise specified), from the following microarchitechtures and variants:

- Intel Westmere E7-xxxx, X56xx, and E56xx
- Intel Sandy Bridge E5-26xx, and E5-46xx
- Intel Ivy Bridge E5-26xx v2, and E5-46xx v2
- Intel Ivy Bridge E7-28xx v2, E7-48xx v2, and E7-88xx v2
- Intel Haswell E5-26xx v3, E5-46xx v3, and E7-88xx v3
- Intel Broadwell E5-26xx v4, E5-46xx v4, and E7-88xx v4
- AMD Opteron 63xx

For best performance, storage should be either internal disks (10K or 15K RPM SAS), Fiber Channel attached storage (array or SAN) with dedicated Fiber Channel connections between hosts and Storage Arrays, or 10Gb iSCSI using non-shared infrastructure. All storage must meet the performance metrics provided with 5620 SAM Platform Sizing Responses. Performance must meet the documented requirements for both throughput and latency.

Nokia support personnel must be provided with the details of the provisioned Virtual Machine. These details can either be provided through read-only access to the hypervisor or must be available to Nokia support when requested. Failure to provide these details could impact support of 5620 SAM.

3.3.2 VMware Virtualization

5620 SAM supports using VMware vSphere ESXi 5.0, 5.1, 5.5, and 6.0 only, on x86 based servers natively supported by ESXi. VMware's Hardware Compatibility List (HCL) should be consulted to determine specific hardware support. Not all features offered by ESXi are supported when using 5620 SAM. For example, Memory Compression, or Distributed Resource Scheduler (DRS) are not supported. Nokia should be contacted to determine if a specific ESXi feature is supported with a 5620 SAM installation.

Defined CPU and Memory resources must be reserved and dedicated to the individual Guest OSs and cannot be shared or oversubscribed. Provisioned CPU resources must be based upon CPU cores and not threads. If threaded CPUs are used, the number of vCPUs required should be multiplied by the number of threads per physical CPU core and assigned to the Virtual Machine.

Virtual Machine Version 8,9, or 10 must be used. The disk must be "Thick Provisioned" with "Eager Zero" set. The SCSI controller must be set to "VMware Paravirtual" and the Disk Provisioning must be "Thick Provision Eager Zero". The Network Adapter must be "VMXNET 3". See the following table for additional Virtual Machine setting requirements.

Table 3-1 VMware Virtual Machine Settings

Resource Type	Parameter	Setting
CPU	Shares	Set to High
	Reservation	Must be set to 1/2 the number of vCPUs * the CPU frequency. For example, on a 2.4GHz 8 vCPU configuration, the reservation must be set to (1/2*8*2400) 9600MHz
	Limit	check box checked for Unlimited
Advanced CPU	Hyperthreaded Core Sharing Mod	Set to None.
	Scheduling Affinity 5620 SAM Auxiliary Database only	Specify the cores that correspond to the socket that the VM is using. For example, on an 8–core socket with hyper-threading, specify 0–15 for the first socket, 16–31 for the second socket,...
Memory	Shares	set to High
	Reservation	slider set to the size of the memory allocated to the VM
	Limit	check box checked for Unlimited
Advanced Memory	NUMA Memory Affinity	No affinity
	Use Memory from nodes 5620 SAM Auxiliary Database only	Select the socket that the VM will be using. For example, if 0–15 was selected for the first socket, specify 0.

Table 3-1 VMware Virtual Machine Settings (continued)

Resource Type	Parameter	Setting
Disk	Shares	set to High
	Limit - IOPs	set to Unlimited

NTP should not be configured on both the hypervisor and the Guest OSs. Either the Guest OS should use NTP to sync the time or the hypervisor should and the Guest OS should be time synced to the hypervisor using VMtools.

3.3.3 VMware Features

The following VMware features have been tested with 5620 SAM. To ensure 5620 SAM stability and compatibility, the following recommendations should be noted for each feature:

vMotion

- Always follow VMware best practices
- Testing was performed with dedicated 10Gb connections between all hosts
- Not supported with the 5620 SAM Auxiliary Database

High Availability

- Always follow VMware best practices
- Do not use Application Monitoring
- Use Host or VM Monitoring only
- Enable 5620 SAM database alignment feature to keep active servers in same Data Center

Snapshots

- Always follow VMware best practices
- Do not include memory snapshots
- Always reboot all 5620 SAM Virtual Machines after reverting to snapshots
- 5620 SAM performance can be degraded by as much as 30% when a snapshot exists and therefore 5620 SAM performance and stability is not guaranteed
- Snapshots should be kept for the least amount of time possible
- Snapshot deletion can take many hours and will pause the VM several times
- SAM Database failover will occur when VMs are reverted to snapshots, requiring a re-instantiation of the Standby Database

3.3.4 KVM Virtualization

5620 SAM supports using RHEL 6.3 through 6.7 KVM using QEMU version 0.12.1.2 and RHEL 7.2 KVM using QEMU version 1.5.3 and 2.3.0 only, on x86 based servers natively supported by KVM. RHEL's Hardware Compatibility List (HCL) should be consulted to determine specific hardware support. Not all features offered by KVM are supported when using 5620 SAM. For example, Live Migration, Snapshots, or High Availability are not supported. Nokia should be contacted to determine if a specific KVM feature is supported with a 5620 SAM installation.

Defined CPU and Memory resources must be reserved and dedicated to the individual Guest OSs and cannot be shared or oversubscribed. Provisioned CPU resources must be based upon CPU cores and not threads. If threaded CPUs are used, the number of vCPUs required should be multiplied by the number of threads per physical CPU core and assigned to the Virtual Machine.

The Disk Controller type must be set to “virtio”, the storage format must be configured as “raw”, cache mode set to “none”, the I/O mode set to “native”, and the I/O scheduler set to “deadline”. The NIC device model must be “virtio”. The hypervisor type must be set to “kvm”.

3.3.5 OpenStack

5620 SAM supports deployment in an OpenStack environment using Red Hat OpenStack Platform release 8. While a 5620 SAM installation may function in other OpenStack environments, the 5620 SAM Product Group makes no commitment to make 5620 SAM compatible with a customer's alternate OpenStack environment.

To ensure 5620 SAM stability and compatibility with OpenStack, the following recommendations should be noted:

Hypervisor

- KVM is the only hypervisor supported within an OpenStack environment. See the preceding section for supported versions.

CPU and Memory resources

- Defined CPU and Memory resources must be reserved and dedicated to the individual Guest OSs and cannot be shared or oversubscribed. The OpenStack Nova configuration for cpu_ allocation_ratio and ram_allocation_ratio must both be set to 1.0 on either the control node or each individual compute node where a VM hosting 5620 SAM could reside.

Hyperthreading

- Hyper-threaded CPU usage must be consistent across all compute nodes. If there are CPUs that do not support hyper-threading, hyper-threading must be disabled on all compute nodes, at the hardware level, where 5620 SAM components could be deployed.

CPU Pinning

- CPU pinning is not recommended as it restricts the use of OpenStack migration

Availability zones / affinity / placement:

- Nokia does not provide recommendations on configuring OpenStack for VM placement.

Migration

- Only Regular migration is supported. Live migration is not supported.

Networking

- Basic Neutron functionality using Open vSwitch with the ML2 plugin can be used in a 5620 SAM

deployment. OpenStack floating IP address functionality can be used on specific interfaces used by 5620 SAM that support the use of NAT. This would require a Neutron router using the neutron L3 agent.

Storage

- All storage must meet the performance metrics provided with 5620 SAM Platform Responses. Performance must meet the documented requirements for both throughput and latency.

VM Storage

- VM storage must be persistent block (Cinder) storage and not ephemeral. For each VM to be deployed, a bootable Cinder volume must be created. The size of the volume is indicated in the 5620 SAM Platform sizing response.

Flavors

- Flavors should be created for each “Station Type” indicated in the 5620 SAM Platform Sizing Response.

Firewalls

- Firewalls can be enabled using OpenStack Security Groups or on the VMs using firewalld. If firewalld is used, an OpenStack Security Group that allows all incoming and outgoing traffic should be used.

3.4 Minimum platform requirements

3.4.1 Minimum hardware platform requirements

The following tables specify the minimum hardware platform requirements necessary to successfully operate the 5620 SAM application in a bare metal configuration.

The minimum platform requirements also represent the smallest configurations suitable for lab evaluations and demonstrations of the 5620 SAM product.

3.4.2 Bare Metal hardware configuration

Table 3-2 5620 SAM bare metal minimum collocated platforms

For networks not exceeding: • 675 MDAs • 1000 GNEs • 5 simultaneous 5620 SAM Clients (GUI or OSS) • 3,000 elemental STM tests every 15 minutes • 50,000 performance or 100,000 accounting statistics records every 15 minutes • 50,000 TCAs	
5620 SAM application	x86 architecture
5620 SAM Server and Database (Collocated)	4* x86 CPU Cores, minimum 2.4GHz 32 GB RAM minimum. 4 SAS 10K RPM disk drives of at least 146 GB in size is required for performance and storage capacity

Table 3-3 5620 SAM bare metal minimum distributed platforms

For networks not exceeding: • 1875 MDAs • Maximum of 5,000 GNEs • 5 simultaneous 5620 SAM Clients (GUI or OSS) • 6,000 elemental STM tests every 15 minutes • 150,000 performance or 200,000 accounting statistics records every 15 minutes • 150,000 TCAs OR • 1275 MDAs • Maximum of 5,000 GNEs • 25 simultaneous 5620 SAM Clients (GUI or OSS) • 6,000 elemental STM tests every 15 minutes • 150,000 performance or 200,000 accounting statistics records every 15 minutes • 150,000 TCAs	
5620 SAM application	x86 architecture
5620 SAM Server	4* x86 CPU Cores, minimum 2.4GHz 32 GB RAM minimum. 2 SAS 10K RPM disk drives of at least 146 GB each in size
5620 SAM Database	4* x86 CPU Cores, minimum 2.4GHz 32 GB RAM minimum 4 SAS 10K RPM disk drives of at least 146 GB in size is required for performance and storage capacity

3.4.3 Minimum hardware platform and resource requirements

The following four tables list the minimum hardware platform requirements for deployments of 5620 SAM using VMware vSphere ESXi or RHEL KVM.

The minimum collocated x86 platforms will deliver acceptable performance in situations in small network which are expected to be relatively static. If the rate of changes in the network or if the rate of transactions through the OSS application(s) are expected to exceed a few changes per second, the collocated minimum platform specified below will not be sufficient to deliver adequate performance. In that case, the distributed minimum platform is recommended.

Red Hat support must be purchased for all platforms running RHEL Server with 5620 SAM. It is strongly recommended to purchase a support package from Red Hat that provides 24x7 support.

3.4.4 Virtual Machine RHEL resource requirements

Table 3-4 5620 SAM Virtual Machine minimum collocated configuration

For networks not exceeding: • 675 MDAs • 1000 GNEs • 5 simultaneous 5620 SAM Clients (GUI or OSS) • 3,000 elemental STM tests every 15 minutes • 50,000 performance or 100,000 accounting statistics records every 15 minutes • 50,000 TCAs	
5620 SAM application	VM Guest H/W Resource Requirements
5620 SAM Server and Database (Collocated)	4 * x86 CPU Cores (8 vCPUs), minimum 2.4GHz 32 GB RAM minimum 600GB disk space I/O requirements found in 3.8 “Storage considerations” (p. 44)

Table 3-5 5620 SAM virtual machine minimum distributed resource requirements

For networks not exceeding: • 1875 MDAs • Maximum of 5,000 GNEs • 5 simultaneous 5620 SAM Clients (GUI or OSS) • 6,000 elemental STM tests every 15 minutes • 150,000 performance or 200,000 accounting statistics records every 15 minutes • 150,000 TCAs OR • 1275 MDAs • Maximum of 5,000 GNEs • 25 simultaneous 5620 SAM Clients (GUI or OSS) • 6,000 elemental STM tests every 15 minutes • 150,000 performance or 200,000 accounting statistics records every 15 minutes • 150,000 TCAs	
5620 SAM application	x86 architecture
5620 SAM Server	4* x86 CPU Cores, minimum 2.4GHz 32 GB RAM minimum. 500 GB disk space I/O throughput and latency as provided in the 5620 SAM sizing response
5620 SAM Database	4* x86 CPU Cores, minimum 2.4GHz 32 GB RAM minimum. 1000 GB disk space I/O throughput and latency as provided in the 5620 SAM sizing response

The minimum resource requirements above are also applicable in situations where the 5620 SAM application is installed in a redundant configuration.

3.4.5 Scaling limits for collocated configurations

Collocated configurations have been capped at the maximums described in the following table. Higher numbers may be achievable, but Nokia will only support the stated maximums. In the event that higher number of simultaneous 5620 SAM Clients is desired, the number of equivalent MDAs can be reduced. Note that all stated maximums may not be achievable simultaneously.

Table 3-6 Scaling limits for collocated configurations

Scaling parameter	Maximum
Number of MDAs	1,875
Number of Simultaneous 5620 SAM Clients (GUI or OSS)	5
Number of SAPs	600,000
Number of OAM tests per 10 minute interval	1,000

Table 3-6 Scaling limits for collocated configurations (continued)

Scaling parameter	Maximum
Performance Statistics per 15 minute interval	50,000
Accounting statistics per 15 minute interval	200,000
TCAs	50,000

3.4.6 Minimum platform requirements for 5620 SAM Auxiliary

Table 3-7 5620 SAM Auxiliary platforms - Bare Metal

Architecture	Supported 5620 SAM Auxiliary type	Configuration
HP x86	Statistics Collector	4 * x86 CPU Cores, minimum 2.4GHz 8 GB RAM minimum. 16GB RAM is recommended. 4 SAS 10K RPM disk drives of at least 146GB each in size (RAID 0)
HP x86	Call Trace Collector	4* x86 CPU Cores, minimum 2.4GHz 16 GB RAM minimum. 4 SAS 10K RPM disk drives of at least 146 GB each in size (RAID 0)
HP x86	Cflowd Collector	12 * x86 CPU Cores, minimum 2.4GHz 32 GB RAM minimum. 2 SAS 10K RPM disk drives of at least 146 GB each in size (RAID 0)
HP x86	PCMD Collector	12 * x86 CPU Cores, minimum 2.6GHz 64 GB RAM minimum. 2 SAS 10K RPM disk drives of at least 300GB each in size (RAID 1) + 6 SAS 10K RPM disk drives of at least 300GB each in size (RAID 0) Minimum of two 1Gb network interfaces. One dedicated to PCMD data collection.
HP x86	Femto	16 * x86 CPU Cores, minimum 2.4GHz 64 GB RAM minimum. 4 SAS 10K RPM disk drives of at least 300GB each in size (RAID 0)

Table 3-8 5620 SAM Auxiliary platforms - VM

Architecture	Supported 5620 SAM Auxiliary type	Configuration
VMware/KVM	Statistics Collector	4* x86 CPU Cores (8 vCPUs), minimum 2.4GHz 8 GB RAM minimum. 16GB RAM is recommended. 500 GB disk space I/O throughput and latency as provided in 5620 SAM Sizing response
VMware/KVM	Call Trace Collector	4* x86 CPU Cores (8 vCPUs), minimum 2.4GHz 16 GB RAM minimum. 600 GB disk space I/O throughput and latency as provided in 5620 SAM Sizing response

Table 3-8 5620 SAM Auxiliary platforms - VM (continued)

Architecture	Supported 5620 SAM Auxiliary type	Configuration
VMware/KVM	Cflowd Collector	12* x86 CPU Cores (24 vCPUs), minimum 2.4GHz 32 GB RAM minimum. 300 GB disk space I/O throughput and latency as provided in 5620 SAM Sizing response
VMware/KVM	PCMD Collector	12 * x86 CPU Cores, minimum 2.6GHz 64 GB RAM minimum. 1,800 GB disk space Dedicated network interface for PCMD data collection. I/O throughput and latency as provided in 5620 SAM Sizing response

When a 5620 SAM Statistics Auxiliary is used, the 5620 SAM Database is required to have a minimum 16 GB RAM to accommodate the additional Oracle database sessions.

3.4.7 Minimum platform requirements for 5620 SAM Auxiliary Database

Table 3-9 5620 SAM Auxiliary Database platform

Architecture	Configuration (for each node of the Auxiliary Database cluster [1])
HP x86	12* x86 CPU Cores, minimum 2.6GHz 128 GB RAM minimum. 2 SAS 10K RPM disk drives of at least 300GB each in size (RAID 1) + 12 SAS 10K RPM disk drives of at least 600GB each in size (RAID 1+0) Minimum of two 1Gb network interfaces. One dedicated to inter-cluster communication.
VMware/KVM	12* x86 CPU Cores (24 vCPUs), minimum 2.6GHz 128 GB RAM minimum. Dedicated network interface for inter-cluster communication only. SAN usage is not supported, must use locally attached disks

Notes:

1. Minimum of three nodes required in the cluster.

3.4.8 Minimum platform requirements for 5620 SAM Analytics Server

Table 3-10 5620 SAM Analytics Server platform

Architecture	Configuration
HP x86	4 * x86 CPU Cores, minimum 2.4GHz 24 GB RAM minimum. 1 SAS 10K RPM disk drive of at least 300GB in size (live network) 1 SAS 10K RPM disk drive of at least 146GB in size (lab)

Table 3-10 5620 SAM Analytics Server platform (continued)

Architecture	Configuration
VMware/KVM	4 * x86 CPU Cores (8 vCPUs), minimum 2.4GHz 24 GB RAM minimum. 200 GB disk space I/O throughput and latency as provided in the 5620 SAM Sizing response

3.4.9 Platform requirements for 5620 SAM Client Delegate workstations

5620 SAM allows multiple GUI clients to be installed on a single HP x86 workstation running RHEL 7 Server x86-64, or specific versions of Windows. This option enables customers to launch multiple 5620 SAM GUI Clients from a single workstation. These GUI clients can be displayed using a Citrix Client/Server, or additionally in the case of RHEL, the X11 protocol to other desktops, or native X displays.

The Client Delegate platform provides an option to consolidate multiple installations of the 5620 SAM GUI Client on a single workstation or the option of installing one instance of the 5620 SAM GUI client run by many users (with unique Operating System accounts). Regardless of the method of the client installation, the platform requirements per client are the same.

Additional memory for each 5620 SAM Client will be required for management of the network elements described in 5.16 “GNE, Nokia OmniSwitch, 9471 WMM, eNodeB, and DSC considerations” (p. 68) or for a Web Browser if SAM Supervisor is to be used.

Management of certain network elements may include the cross-launch of additional software that may not be compatible with certain operating systems. The information in Table 3-13, “Element Manager operating system support summary” (p. 42) lists these element managers and their operating system support. The documentation of these element managers should be consulted to determine current operating system support.

The 5620 SAM Client Delegate configuration is only supported for HP x86 workstations running RHEL Server x86-64, or specific versions of Windows. Additionally, the 5620 SAM Client Delegate installation is supported on a Guest Operating System of a VMware vSphere ESXi or RHEL KVM installation. The Guest OS must be one of those supported for GUI Clients found in 2.2 “Operating systems specifications” (p. 25) . Table 3-11, “Minimum 5620 SAM Client Delegate resource requirements” (p. 40) describes resource requirements for this type of workstation.

Table 3-11 Minimum 5620 SAM Client Delegate resource requirements

Architecture	Configuration
HP x86	4* x86 CPU Cores, minimum 2.0GHz 16 GB RAM minimum, 24 GB for networks with greater than 15,000 NEs 1 SAS 10K RPM disk drives, 146GB in size
VMware/KVM	4* x86 CPU Cores (8 vCPUs), minimum 2.0GHz 16 GB RAM minimum, 24 GB for networks with greater than 15,000 NEs 70 GB disk space

The configurations in the preceding table will support up to 15 GUI Clients. Additional GUI Clients can be hosted on the same platform provided that the appropriate additional resources found in Table 3-12, “Additional Client 5620 SAM Client Delegate resource requirements” (p. 40) are added to the platform.

Table 3-12 Additional Client 5620 SAM Client Delegate resource requirements

Architecture	Additional resources per client
HP x86	1/4 * x86 CPU Core, minimum 2.0GHz 1 GB RAM, 1.5 GB for networks with greater than 15,000 NEs 1 GB Disk Space
VMware/KVM	1/4 CPU Core (1/2 vCPU), minimum 2.0GHz 1 GB RAM, 1.5 GB for networks with greater than 15.000 NEs 1 GB Disk Space

For situations where more than 60 simultaneous GUI sessions are required, Nokia recommends deploying multiple 5620 SAM Client Delegates.

Displaying GUI clients to computers running X-emulation software is not currently supported. In cases where the GUI client is to be displayed to a PC computer running Windows, Nokia supports installing the GUI client directly on the PC.

5620 SAM supports using Citrix for remote display of 5620 SAM Clients. Supporting Citrix on the delegate platform will require extra system resources that will need to be added to those that are required by the 5620 SAM delegate. Refer to Citrix documentation to determine the additional Citrix resource requirements.

The following Citrix software has been tested with the Windows Client Delegate :

- Windows 2008R2 — Citrix Server - XenApp Version 6.5
- Windows 2012R2 — Citrix Server - XenApp Version 7.6
- Windows 7 — Citrix Client - Receiver Version 3.4.0.29577

The following Citrix software has been tested with the RHEL Client Delegate:

- Citrix Server - XenApp Presentation Server 4.0 with Feature Pack 1 and Patch PSE400SOLX066 for Solaris x86
- Citrix Client - Version 8.50.117422 for Solaris x86
- Citrix Client - Receiver Version 3.4.0.29577 for Windows 7

3.5 5620 SAM-O 3GPP Interface

3.5.1 5620 SAM-O 3GPP Interface

5620 SAM-O 3GPP Interface is used by management systems that need to access 5620 SAM information collected from mobile networks.

5620 SAM-O 3GPP Interface requires a separate JVM to be installed on the 5620 SAM Server, and is only supported on 5620 SAM Servers with a minimum 32 GB RAM in a distributed configuration or 5620 SAM Server/Databases with a minimum 48 GB RAM in a collocated configuration.

3.6 5620 SAM GUI Client platform requirements

3.6.1 5620 SAM GUI Client platform requirements

Nokia recommends 1 GB of dedicated RAM – regardless of the operating system. In cases where other applications are running on the same platform as the 5620 SAM Client, it is important to ensure 1 GB RAM is available to the 5620 SAM Client.

Additional memory for each 5620 SAM Client will be required for management of the network elements described in 5.16 “GNE, Nokia OmniSwitch, 9471 WMM, eNodeB, and DSC considerations” (p. 68) or for a Web Browser if 5620 SAM applications are to be used.

Management of certain network elements may include the cross-launch of additional software that may not be compatible with certain operating systems. The information in the following table lists these element managers and their operating system support. The documentation of these element managers should be consulted to determine current operating system support.

All platforms used to display 5620 SAM Applications must have a WebGL compatible video card and the corresponding drivers installed.

Table 3-13 Element Manager operating system support summary

Element Manager	Node Type	RHEL 7 Server Support	Microsoft Windows Support
NEM	eNodeB	Supported	Supported
NEtO	9500 MPR	Not-supported	Supported
MI	9471 WMM	Not-supported	Supported
PSS - WebUI	1830 PSS	Supported	Supported

The following table provides the minimum requirement for the hardware that will host 5620 SAM GUI client software. Additional memory and disk resources will be required by the Operating System.

Table 3-14 5620 SAM GUI hardware platform requirements

5620 SAM GUI Client hardware platform requirements	
RHEL platforms	Microsoft Windows
1 CPU @ 2GHz or higher 1 GB RAM dedicated to 5620 SAM Client, 1.5 GB for networks with greater than 15,000 NEs 1 GB available disk space 1280*1024 Display resolution for java GUI 1280*720@72ppi Display resolution for 5620 SAM applications (minimum) 1920*1080@72ppi Display resolution for 5620 SAM applications (recommended) Example platform: DL380 G7	1 CPU @ 2 GHz or higher 1 GB RAM dedicated to 5620 SAM Client, 1.5 GB for networks with greater than 15,000 NEs 1 GB available disk space 1280*1024 Display resolution for java GUI 1280*720@72ppi Display resolution for 5620 SAM applications (minimum) 1920*1080@72ppi Display resolution for 5620 SAM applications (recommended)

A 5620 SAM GUI client installation is supported on a Guest Operating System of a VMware vSphere ESXi or RHEL KVM installation. The Guest OS must be one of those supported for GUI Clients found in 2.2 “Operating systems specifications” (p. 25) .

The following table provides the dedicated 5620 SAM resource requirements for each Guest OS running under VMware vSphere ESXi or RHEL KVM that will be used to host the 5620 SAM Client GUI. This does not include the specific operating system resource requirements which are in addition to the hardware resources listed below. CPU and Memory resources must be reserved and dedicated to the individual Guest OSs and cannot be shared or oversubscribed. Disk and Network resources should be managed appropriately to ensure that other Guest OSs on the same physical server do not negatively impact the operation of the 5620 SAM GUI Client.

Table 3-15 Virtualized 5620 SAM GUI resource requirements

Virtual Machine resource requirements	
RHEL Guest OS resources	Microsoft Windows Guest OS resources
1 CPU Core @ 2GHz or higher 1 GB dedicated RAM, 1.5 GB for networks with greater than 15,000 NEs 1 GB available disk space 1280*1024 Display resolution for java GUI 1280*720@72ppi Display resolution for 5620 SAM applications (minimum) 1920*1080@72ppi Display resolution for 5620 SAM applications (recommended)	1 CPU Core @ 2 GHz or higher 1 GB dedicated RAM, 1.5 GB for networks with greater than 15,000 NEs 1 GB available disk space 1280*1024 Display resolution for java GUI 1280*720@72ppi Display resolution for 5620 SAM applications (minimum) 1920*1080@72ppi Display resolution for 5620 SAM applications (recommended)

3.7 Determining platform requirements for larger networks

3.7.1 Determining platform requirements for larger networks

5620 SAM may require larger workstations in order to successfully manage networks that exceed any of the dimensions supported by the minimum hardware platforms. In order to determine workstation requirements to successfully manage larger networks, the following information is required:

- Expected number and types of Network Elements to be managed
- Expected number of MDAs in the network to be managed
- Expected number of services and SAPs in the network to be managed
- Expected number of Dynamic LSPs to be deployed in the network
- Maximum expected number of 5620 SAM Clients (GUI) simultaneously monitoring the network
- Expected number of OSS applications that will connect as clients to the 5620 SAM-O interface
- Expected number of subscribers, specifically for triple-play network deployments
- Expected statistics collection and retention
- Expected number of STM tests
- Expected number of managed GNEs
- Whether 5620 SAM redundancy is to be utilized

- Whether NEBS compliance is required
- Whether CPAM is required
- Whether RAID 1 is required

The information above must then be sent to an Nokia representative who can provide the required hardware specifications.

Ensure that any projected growth in the network is taken into account when specifying the expected network dimensioning attributes. For existing 5620 SAM systems, the user may determine the number of MDAs deployed in the network using the help button on the 5620 SAM GUI. It is also possible to determine the number of statistics being handled by the system by looking at the 5620 SAM GUI's "Statistics Collection" information window. Select the "Tools", then "Statistics", then "Server Performance Statistics" Menu. List the "Statistics Collection" objects. From this list window, check the "Scheduled Polling Stats Processed Periodic" and the "Accounting Stats Processed Periodic" columns for the performance and accounting statistics that your system is currently processing within the time interval defined by the collection policy (15 minutes by default).

3.8 Storage considerations

3.8.1 Storage considerations

This section provides information on configuring workstations that will host 5620 SAM software.

Specific partition sizes and configuration procedures are available in the *5620 SAM | 5650 CPAM Installation and Upgrade Guide*.

When using the RHEL Server OS, ext4 is the required file system for all application specific mount points. No other file systems are supported with 5620 SAM. OS specific mount points can be either xfs or ext4 as the file system. Windows based client must use a local file system for client files. Network based file systems, including Samba, are not supported.

While Nokia identifies areas of the disk that are not specifically required for 5620 SAM and are partitionable for customer use, workstation resources are expected to be dedicated for 5620 SAM. As such, these "Remainder" portions of the disks should only be used for static storage purposes. Consideration should also be made to the expected growth of the network. If the "Remainder" is not to be used, then it should not be created.

For all network sizes, Nokia requires the use of at least four disks on workstations running the 5620 SAM Database. This disk configuration allows for better performance by distributing the database onto multiple disks. Customized disk configurations may be required for larger network deployments or where large scale statistics collection is required. Request a formal platform sizing for further details. NAS disk configurations are not supported.

Disk configurations for workstations running the 5620 SAM Database with less than four physical disks greatly limits the 5620 SAM system performance, managed-network size, and data storage capacity, and is therefore only supported for lab trials.

Refer to "Scaling guidelines for statistics collection" (p. 77) for statistics collection recommendations.

In 5620 SAM upgrade scenarios, previous disk configurations may still be valid.

3.8.2 Using RAID technologies

In bare metal deployments, Nokia requires the use of RAID 0 (striping) provided by a hardware based RAID controller. Software based RAID 0 is not supported. Nokia will provide disk layout and configuration details for customers requiring a Storage Array or layouts not specified in the *5620 SAM | 5650 CPAM Installation and Upgrade Guide*. The increased disk I/O performance offered by RAID 0 is required for all 5620 SAM deployments. The *5620 SAM | 5650 CPAM Installation and Upgrade Guide* provides details of these configurations. A RAID 0 stripe size of 512 Kbytes is required for optimal 5620 SAM disk performance. If a platform does not support a stripe size of 512 Kbytes, choose the next largest stripe size, for example, 256 Kbytes. Specifying a smaller or larger stripe size may result in degraded performance that compromises 5620 SAM network management.

Nokia supports the use of RAID 1 (Mirroring). Deployments requiring increased resiliency are encouraged to use 5620 SAM platform redundancy. If RAID 1 is required, a platform providing hardware RAID 1 and that has sufficient number of disk to meet the increased disk requirements must be selected.

To reduce the chance of data loss or application down time, Nokia recommends the use of RAID 1, in a RAID 1+0 configuration.

Note: Nokia is not responsible for installation, administration or recovery of RAID on a 5620 SAM platform.

3.8.3 Using SAN storage

Nokia supports the use of SAN storage. SAN connectivity must consist of 4Gb or faster optical connections or 10Gb iSCSI connections. It is recommended that these connections are dedicated connections between the hosts and storage arrays. The SAN must be available to 5620 SAM without interruption in a low latency environment.

5620 SAM Platform Sizing responses will provide the required performance targets when using 5620 SAM with a SAN. Note that certain mount points may not be required due to deployment options. Refer to the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for required mount points based upon the type of 5620 SAM workstations deployed. The 5620 SAM Auxiliary Database is not supported with a SAN where directly attached disks are required to meet the high I/O requirements.

Note: Nokia is not responsible for installation, administration or recovery of SANs on a 5620 SAM platform.

3.8.4 Virtualization I/O requirements

When using 5620 SAM on a Guest Operating System of a hosted Virtualized installation, specific storage requirements must be met. For optimal performance, storage should be either internal disks (10K or 15K RPM SAS), Fiber Channel attached storage (array or SAN) with dedicated Fiber Channel connections between hosts and Storage Arrays, or 10Gb iSCSI using non-shared infrastructure. All storage must meet the performance metrics provided with 5620 SAM Platform Sizing Responses. Storage I/O shares must be set to “High” and IOPs set to “Unlimited” for best performance and low latency. The 5620 SAM Auxiliary Database is not supported on a SAN where direct attached storage is required. Therefore, in a virtual environment, the storage requirement must be met using direct attached disks.

Refer to Table 3-16, “Minimum collocated throughput and latency” (p. 45) for the minimum required throughput and latency for a collocated 5620 SAM configuration. Higher scale networks and distributed configurations may require alternate throughput and latency targets that will be provided with the 5620 SAM Platform Sizing response that is required for every 5620 SAM deployment.

5620 SAM includes a benchmarking utility to be used for determining the throughput and latency of the storage device to be used with the virtual server hosting 5620 SAM. The utility is installed with a 5620 SAM Server in the /opt/5620sam/server/nms/bin/unsupported/5620_SAM_IOTest directory and is called 5620_SAM_IOTest.pl. If 5620 SAM has not yet been installed, the utility can be obtained from Nokia or from the 5620 SAM software package.

Executing the utility with the -h flag will present the user with a help menu, explaining different options and presenting execution examples. Each mount point must be tested and must meet the throughput and latency requirements for the specific deployment. These throughput and latency requirements must be obtained from Nokia as they are specific to each deployment. The throughput and latency targets must be met, irrespective of any other activity on the underlying storage device and the targets must be achievable concurrently. For this reason, it is important to understand the underlying storage configuration to ensure that the output of the benchmarking utility is interpreted correctly. For example, each of the listed targets may be achievable using a single 10K RPM SAS disk but concurrently, the listed targets would not be achievable using the same single 10K RPM SAS disk. The performance of 5620 SAM would be degraded using this configuration.

Table 3-16 Minimum collocated throughput and latency

Mount Point	Read (MB/s)	Write (MB/s)	Latency (ms)
/opt/5620sam	37	15	< 1.0
/opt/5620sam/server/xml_output	37	15	< 1.0
/opt/5620sam/dbbackup	14	21	< 1.0
/opt/5620sam/samdb/tablespace	158	8	< 1.0
/opt/5620sam/server/nms/log	1	1	< 1.0
/opt/5620sam/samdb/archivelog	14	38	< 1.0
/opt/5620sam/nebackup	6	6	< 1.0

The *5620 SAM | 5650 CPAM Installation and Upgrade Guide* should be consulted for recommended partition sizes.

4 NE maintenance

4.1 Overview

4.1.1 Purpose

This chapter describes how to display the current state of and maintain the network elements managed by the 5620 SAM.

4.1.2 Contents

4.2 Mechanism to maintain current state of network elements

4.2.1 Mechanism to maintain current state of network elements

5620 SAM uses several mechanisms to maintain and display the current state of the network elements it manages. These mechanisms can include:

- IP connectivity (ping) verification
- SNMP connectivity verification
- SNMP traps
- SNMP trap sequence verification
- Scheduled SNMP MIB polling

These mechanisms are built into the Nokia 7950, 7750, 7450, 7710, 7210, and 7705 Network Elements and the 5620 SAM network element interaction layers.

4.3 IP connectivity (ping) verification

4.3.1 IP connectivity (ping) verification

5620 SAM can be configured to ping all network elements at a configurable interval to monitor IP connectivity. If the network element is unreachable, an alarm will be raised against the network element. Details of the alarm are the following:

- Severity: Critical
- Type: communicationsAlarm
- Name: StandbyCPMManagementConnectionDown, OutOfBandManagementConnectionDown or InBandManagementConnectionDown
- Cause: managementConnectionDown.

Ping verification is disabled by default. IP connectivity checks using ping must be scheduled through the default policy.

4.4 SNMP connectivity verification

4.4.1 SNMP connectivity verification

5620 SAM performs an SNMP communication check every 4 minutes. If 5620 SAM can not communicate via SNMP with a network element, 5620 SAM will raise a communications alarm against that network element. 5620 SAM will also color the network element red on the map to indicate the communication problem. 5620 SAM will clear the alarm and color the network element as green once 5620 SAM detects SNMP connectivity to the network is re-established. Details of the alarm are the following:

- Severity: Major
- Type: communicationsAlarm
- Name: SnmpReachabilityProblem
- Cause: SnmpReachabilityTestFailed

This behavior occurs by default and is not configurable.

4.5 SNMP traps

4.5.1 SNMP traps

5620 SAM listens to SNMP traps to receive changes from the network elements. 5620 SAM configures the trap log ID on each network element when it is first discovered. The network element then uses that trap log ID to send all configuration changes and updates to 5620 SAM. 5620 SAM will react to the traps it receives and make appropriate changes to the database, alarms and related object as required.

4.6 SNMP trap sequence verification

4.6.1 SNMP trap sequence verification

5620 SAM retrieves the last trap sequence number sent from all network elements at a configurable interval. This interval is configurable on a per resource group basis. Resource groups allow the user to configure the communications behavior of a group of network elements. By default, the core resource group includes all network elements, and verifies the trap sequence number every 4 minutes. 5620 SAM compares that sequence number with the sequence number of the last trap it received from that network element. If they do not match, 5620 SAM will request only the missing traps from the network element. If at any point 5620 SAM realizes that it is missing more than 200 traps from a network element, or if the network element no longer has the missed trap, SAM will request a full resynchronization on that network element rather than just request the missing traps.

This behavior occurs by default and is not configurable.

4.7 Scheduled SNMP MIB polling

4.7.1 Scheduled SNMP MIB polling

5620 SAM can poll all data SNMP MIBs from the network elements at a configurable interval. Starting in 5620 SAM Release 7.0 R1, the Polling Policy is disabled by default. This behavior is configurable via the Polling tab of the Network Elements properties form.

4.8 Network outages

4.8.1 Network outages

When an Nokia 7x50-based network element loses visibility of the 5620 SAM Network Manager, it is unable to send traps to the network manager, and the traps are queued on the network element. 4.6 “SNMP trap sequence verification” (p. 49) describes 5620 SAM behavior with regards to trap handling. When a network outage occurs, the network element configuration in 5620 SAM will be made consistent with the network element, but any event notifications, such as SNMP traps, that occurred during the network outage will not have been processed. This will cause intermediate state change alarms to not be reflected in 5620 SAM during the network outage.

5 Network requirements

5.1 Overview

5.1.1 Purpose

This chapter defines the network requirements for the 5620 SAM systems, network elements, and OSS systems.

5.1.2 Contents

5.2 Network requirements

5.2.1 Network requirements

The network interconnecting the 5620 SAM systems, network elements, and OSS systems is of significant importance to the effective management of the network. The following sections describe the requirements for the network links between 5620 SAM workstations and the connection to the network being managed. Nokia recommends that sufficient bandwidth be made available to the 5620 SAM workstations within the Data Communication Network.

For SNMP management of Nokia network elements, all network segments that carry SAM management traffic must allow the successful transmission of 9216 byte SNMP packets. The *5620 SAM Troubleshooting Guide* contains more information on packet fragmentation issues.

Be sure to include the tables with the bandwidth required for statistics collection in the total bandwidth required between the 5620 SAM workstations, as they are in separate tables.

The tables do not specify the underlying infrastructure required to support these bandwidth requirements.

See Chapter 8, “Deploying the 5620 SAM with multiple network interfaces/IP addresses” for information on configuring the 5620 SAM workstations with multiple interfaces.

5.3 Connectivity to the network elements

5.3.1 Connectivity to the network elements

5620 SAM supports both IPv4 and IPv6 connectivity to network elements. The following network elements may be managed by 5620 SAM using IPv6:

- 7950
- 7750
- 7450
- 7710
- 7705
- 7210
- eNodeB
- 9471 WMM (vMM)
- 9500 MPR
- Multi Standard Enterprise and Home Cell Access Points

Cflowd flow data can only be retrieved from network elements with IPv4 connectivity. Call Trace data can only be retrieved from WMM/vMM network elements with IPv4 connectivity.

5620 SAM supports the use of multiple interfaces for network element management communication. If a network element uses both an in-band and out-of-band address for management, these interfaces must reside on the same server interface.

5.4 Bandwidth requirements for collocated 5620 SAM installations

5.4.1 Bandwidth requirements for collocated 5620 SAM installations

The following table lists the bandwidth requirements for the connections between the components of a 5620 SAM Collocated installation. It is a good practice to measure the bandwidth utilization between the various components to determine a suitable bandwidth. There are a number of factors that could require an increase above our bandwidth utilization recommendations, including: GUI activity, OSS activity, network events, number of network elements being managed.

Table 5-1 5620 SAM collocated Server/Database bandwidth requirements

Available bandwidth required from primary 5620 SAM Server/Database workstation	Recommended bandwidth: excluding statistics bandwidth requirements
5620 SAM Client (GUI)	1 Mbps
5620 SAM-O Client (The bandwidth will depend on the OSS application)	1 Mbps
Between primary and standby 5620 SAM Server/Database workstation NOTE: When network element database backup synchronization is enabled, the bandwidth requirement between the 5620 SAM Servers will vary significantly depending on the size of the network element backup file sizes.	5-10 Mbps (sustained) 16-26 Mbps (during re-instantiation or database backup synchronization)

5.5 Bandwidth requirements for distributed 5620 SAM installations

5.5.1 Bandwidth requirements for distributed 5620 SAM installations

The following tables list the requirements for the connections between the components of a 5620 SAM Distributed installation. It is a good practice to measure the bandwidth utilization between the various components to determine a suitable bandwidth. There are a number of factors that could require an increase above our bandwidth utilization recommendations – including: GUI activity, OSS activity, network events, number of network elements being managed.

Table 5-2 5620 SAM distributed Server/Database bandwidth requirements

Available bandwidth requirements for 5620 SAM	Recommended bandwidth: excluding statistics and call trace bandwidth requirements
5620 SAM Server to a 5620 SAM Database NOTE: This depends on GUI changes and lists, # of changes occurring in the network, and network objects managed.	5 to 10 Mbps (3 Mbps minimum)
5620 SAM Server to a 5620 SAM Client	1 Mbps
5620 SAM Server to a 5620 SAM-O Client (The bandwidth will depend on the OSS application)	1 Mbps

Table 5-2 5620 SAM distributed Server/Database bandwidth requirements (continued)

Available bandwidth requirements for 5620 SAM	Recommended bandwidth: excluding statistics and call trace bandwidth requirements
Between a primary and a standby 5620 SAM Server NOTE: When network element database backup synchronization is enabled, the bandwidth requirement between the 5620 SAM Servers will vary significantly depending on the size of the network element backup file sizes.	1 Mbps
5620 SAM Server to a 5620 SAM Auxiliary Statistics Collector	1 Mbps
Between primary and standby 5620 SAM Databases NOTE: The higher bandwidth is required to handle re-instantiation and is also required immediately after a database backup when database backup synchronization is enabled.	6 Mbps (sustained) 15-25 Mbps (during re-instantiation or database backup synchronization) 3 Mbps (minimum)

Table 5-3 Additional bandwidth requirements for file accounting STM results collection

Bandwidth requirements for installations collecting file accounting STM results using the logToFile method only	Increased Bandwidth per 50,000 file accounting STM records
5620 SAM Server to a 5620 SAM-O Client if using registerLogToFile NOTE: a higher bandwidth may be desirable	3.5 Mbps
5620 SAM Server to 5620 SAM Database workstation	1.5 Mbps
Between the 5620 SAM Database workstations – required for sufficient bandwidth for database re-instantiations NOTE: The higher bandwidth is required to handle re-instantiation during STM collection	2 Mbps (sustained) 12 Mbps (during re-instantiation or database backup synchronization)

Table 5-4 Additional bandwidth requirements for management of Small Cell Access Points

Bandwidth requirements for installations managing Small Cell Access Points	Required Bandwidth
5620 SAM Server to the Motive Home Device Manager NOTE: a higher bandwidth may be desirable	20 Mbps

5.5.2 Additional bandwidth requirements for statistics collection

The size of the network and the number of statistics that are collected will impact the recommended bandwidth between the following workstations:

- 5620 SAM Auxiliary Statistics Collector and 5620 SAM Database
- Active and Inactive 5620 SAM Database workstations

The following tables should be used to determine how much additional bandwidth will be required between the 5620 SAM workstations when statistics collection is added to the system. The bandwidths of connections not listed do not change dramatically with the addition of statistics.

The registerLogToFile method of retrieving statistics can be compressed or uncompressed. Using the compressed option will require additional CPU requirements on the workstation that is collecting the statistics (either 5620 SAM Server or 5620 SAM Auxiliary Statistics Collector). In this case, the bandwidth required will be reduced.

Table 5-5 Additional bandwidth requirements for accounting statistics collection

Bandwidth requirements for installations collecting accounting statistics.	Additional bandwidth per 200,000 accounting statistics records
5620 SAM Server to a 5620 SAM-O Client if using findToFile. OR 5620 SAM Server to 5620 SAM-O Client if using an uncompressed registerLogToFile (5620 SAM Auxiliary Statistics Collector is NOT installed). OR 5620 SAM Auxiliary Statistics Collector to 5620 SAM-O Client if using an uncompressed registerLogToFile.	3.5 Mbps
5620 SAM Server to 5620 SAM Database workstation if the 5620 SAM Server is collecting the statistics OR 5620 SAM Auxiliary Statistics Collector to 5620 SAM Database workstation if the 5620 SAM Auxiliary Statistics Collector is collecting the statistics	2.2 Mbps
Between the 5620 SAM Database workstations NOTE: The higher bandwidth is required to handle re-instantiation during statistics collection NOTE: Not required if accounting statistics are not stored in the 5620 SAM Database (logToFile only)	3.2 Mbps (sustained) 18 Mbps (during re-instantiation or database backup synchronization)

Table 5-6 Additional bandwidth requirements for application assurance statistics collection

Bandwidth requirements for installations collecting accounting statistics.	Additional bandwidth per 200,000 applications assurance objects configured for collection
5620 SAM Server to 5670 RAM (5620 SAM Auxiliary Statistics Collector is NOT installed). OR 5620 SAM Auxiliary Statistics Collector to 5670 RAM	4.6 Mbps
5620 SAM Server to 5620 SAM Database workstation if the 5620 SAM Server is collecting the statistics OR 5620 SAM Auxiliary Statistics Collector to 5620 SAM Database workstation if the 5620 SAM Auxiliary Statistics Collector is collecting the statistics	3.1 Mbps
Between the 5620 SAM Database workstations NOTE: The higher bandwidth is required to handle re-instantiation during statistics collection	4.2 Mbps (sustained) 20 Mbps (during re-instantiation or database backup synchronization)

Table 5-7 Additional bandwidth requirements for performance and optical performance management statistics collection

Bandwidth requirements for installations collecting performance and optical performance management statistics.	Increased Bandwidth per 200,000 performance and optical performance management statistics records
5620 SAM Server to a 5620 SAM-O Client if using findToFile OR 5620 SAM Server to 5620 SAM-O Client if using an uncompressed registerLogToFile (5620 SAM Auxiliary Statistics Collector is NOT installed). OR 5620 SAM Auxiliary Statistics Collector to 5620 SAM-O Client if using an uncompressed registerLogToFile. NOTE: a higher bandwidth may be desirable	3.5 Mbps
5620 SAM Server to 5620 SAM Database workstation SUM the following bandwidths: If the 5620 SAM Server is collecting the statistics:(5620 SAM Auxiliary Statistics Collector is NOT installed) If the 5620 SAM-O Client is using findToFile to collect all statistics data	5.4 Mbps 5.4 Mbps
5620 SAM Auxiliary Statistics Collector to 5620 SAM Database workstation if the 5620 SAM Auxiliary Statistics Collector is collecting the statistics	5.4 Mbps
Between the 5620 SAM Database workstations – required for sufficient bandwidth for database re-instantiations NOTE: The higher bandwidth is required to handle re-instantiation during statistics collection NOTE: Not required if performance and optical performance management statistics are not stored in the 5620 SAM Database (logToFile only)	14.4 Mbps (sustained) 72 Mbps (during re-instantiation or database backup synchronization)

Table 5-8 Additional bandwidth requirements for LTE performance management statistics collection

Bandwidth requirements for installations collecting LTE performance management statistics.	Increased Bandwidth per 200,000 LTE performance management statistics records
Between a primary and a standby 5620 SAM Server: If the 5620 SAM Server is collecting the statistics:(5620 SAM Auxiliary Statistics Collector is NOT installed)	1.0 Mbps
Between a preferred and a reserved 5620 SAM Auxiliary Statistics Collector if the 5620 SAM Auxiliary Statistics Collector is collecting the statistics	1.0 Mbps

When a 5620 SAM Auxiliary Statistics Collector is installed to collect statistics using the 5620 SAM Database, the bandwidth requirements between two geographic locations will need to reflect the state where a 5620 SAM Auxiliary Statistics Collector in geographic location A may send information to the active 5620 SAM Server in geographic location B which will - in turn – send information back to the 5620 SAM Database in geographic location A. For this reason, the bandwidth between geographic location A and B must be the sum of the bandwidth requirements between the 5620 SAM Auxiliary Statistics Collector to 5620 SAM Server and 5620 SAM Server to

5620 SAM Database. It is also a best practice to ensure that the 5620 SAM Auxiliary Statistics Collector, 5620 SAM Server, and 5620 SAM Database are all collocated in the same geographic site.

5.5.3 5620 SAM Auxiliary Call Trace Collectors

When a 5620 SAM Auxiliary Call Trace Collector is installed, there are a number of bandwidth requirements listed below. Any bandwidths not listed are not impacted significantly by call trace data collection.

To handle the redundant pairs appropriately, the bandwidth requirements between two geographic locations will need to reflect the state where a 5620 SAM Auxiliary Call Trace Collector in geographic location A may need to provide information to the 5620 SAM-O Client in geographic location B. The synchronization of call trace and debug trace files will be impacted by the number client application ftp sessions retrieving call trace and debug trace files. To minimize this impact, it is recommended to limit the number of ftp sessions.

Table 5-9 Additional bandwidth requirements for call trace collection

Bandwidth requirements for installations with call trace collection	Bandwidth usage characterization
5620 SAM Server to a 5620 SAM-O Client	Low bandwidth OSS requests and responses
5620 SAM-O Client to 5620 SAM Auxiliary Call Trace Collector workstation NOTE: a higher bandwidth may be desirable	Higher bandwidth to retrieve via FTP the call trace files from the 5620 SAM Auxiliary
5620 SAM Auxiliary Call Trace Collector Preferred workstation to it's Reserved redundant pair. NOTE: a higher bandwidth may be desirable	Higher bandwidth to ensure timely synchronization of call trace files

5.5.4 5620 SAM Auxiliary Database Cluster

When a 5620 SAM Auxiliary Database Cluster is part of a 5620 SAM deployment, there are a number of bandwidth requirements listed below. Any bandwidths not listed are not impacted significantly by the use of the 5620 SAM Auxiliary Database for statistics collection.

The 5620 SAM Auxiliary Database Server requires a minimum of two network interfaces; one for communication to the 5620 SAM management complex and one for internal data communication between each of the 5620 SAM Auxiliary Database servers in the cluster. The interface for internal data communication needs to be dedicated with a minimum interface speed of 1Gbps and part of a private network.

Table 5-10 Additional bandwidth requirements for 5620 SAM Auxiliary Database

Bandwidth requirements for installations with 5620 SAM Auxiliary Database	Bandwidth usage characterization
5620 SAM Auxiliary Statistics Collector to 5620 SAM Auxiliary Database cluster	Higher bandwidth to write statistics data into the 5620 SAM Auxiliary Database cluster
5620 Analytics Server to 5620 SAM Auxiliary Database cluster NOTE: a higher bandwidth may be desirable	Higher bandwidth to generate reports based upon raw and aggregated data

Table 5-10 Additional bandwidth requirements for 5620 SAM Auxiliary Database (continued)

Bandwidth requirements for installations with 5620 SAM Auxiliary Database	Bandwidth usage characterization
5620 SAM Auxiliary Database to 5620 SAM Auxiliary Database	High — must use a dedicated, minimum 1Gbps interface

5.6 Bandwidth requirements for 5620 SAM GUI Clients

5.6.1 Bandwidth requirements for 5620 SAM GUI Clients

The bandwidth specifications provided above for 5620 SAM GUI Clients are based on the fact that information about changes in the network is forwarded to the 5620 SAM GUI Clients. The 5620 SAM Client updates information visible to the user based on recent changes in the network.

A few examples of network changes which will be reported to 5620 SAM include status changes of physical equipment, status changes of Layer 2 or Layer 3 interfaces, configuration of network elements, provisioning of new equipment or services, status changes in services or any attributes thereof, configuration changes of routing protocols and several others.

In situations where the frequency of changes sent to the 5620 SAM GUI is significant and exceeds the bandwidth specification, the performance of the 5620 SAM Client will degrade, and there is a possibility that the connection to the server will be dropped. A 5620 SAM GUI restart will be required to reconnect to the server to receive change notifications.

5.7 Bandwidth requirements for displaying 5620 SAM GUI Clients on X displays

5.7.1 Bandwidth requirements for displaying 5620 SAM GUI Clients on X displays

5620 SAM GUI Clients can be displayed remotely on terminals using the X11 protocol for graphical displays. In these cases, it is important to ensure the bandwidth availability between the workstation running the 5620 SAM Client and the host displaying the 5620 SAM Client be at least 1024 Kbps. Also, it is important to ensure the round-trip network latency between these two hosts is quite low (20-30ms). To achieve acceptable performance on bandwidth limited links, X-compression should be used by using the ssh -XC command. If not using compression, it is recommended that the minimum bandwidth be higher than 1024 Kbps. Situations where the available bandwidth is lower or the network latency is higher will result in poor usability of the 5620 SAM GUI Client. A bandwidth of 1024 Kbps will impact GUI start time and will not meet the published time of 30s.

Extra bandwidth may be required to support the network elements described in 5.16 “GNE, Nokia OmniSwitch, 9471 WMM, eNodeB, and DSC considerations” (p. 68)

Note that 5620 SAM GUI Client startup may be impacted when using minimum bandwidth links.

5.8 Bandwidth requirements for 5620 SAM-O OSS Clients

5.8.1 Bandwidth requirements for 5620 SAM-O OSS Clients

There are two main factors affecting the bandwidth requirements between the 5620 SAM Server and a 5620 SAM-O OSS Client:

- Design and behavior of the application using the 5620 SAM-O OSS
- Rate of changes in the network

Applications which listen to network changes via the JMS interface provided by 5620 SAM-O or applications which retrieve large pieces of information via 5620 SAM-O, such as statistics information or network inventory information, will require access to dedicated bandwidth from the machine hosting the application to the 5620 SAM Server according to the tables above. Applications which do not require real time event and alarm notification may operate with acceptable performance when the bandwidth between the machine hosting the application and the 5620 SAM Server is less than the quantity specified in the tables above.

It is a best practice to minimize event and alarm notifications using a JMS filter to reduce bandwidth requirements and the possible effects of network latency.

In an environment where network changes are infrequent, it is possible to successfully operate an application using the 5620 SAM-O when the bandwidth between the machine hosting this application and the 5620 SAM Server is less than the quantity specified in the tables above, possibly as little as 128 kbps. However, in situations where the frequency of network changes increases, the performance or responsiveness of the application will degrade.

5.9 Bandwidth requirements for the 5620 SAM Auxiliary Statistics Collector workstation

5.9.1 Bandwidth requirements for the 5620 SAM Auxiliary Statistics Collector workstation

The main factors impacting communication to and from the 5620 SAM Auxiliary Statistics Collector workstation are:

- Number of performance statistics being collected. The 5620 SAM Server needs to tell the 5620 SAM Auxiliary Statistics Collector which statistics to collect every interval.
- Number of statistics collected from the network elements.
- Number of statistics written to the 5620 SAM Database.

The more performance statistics are collected, the more significant the bandwidth utilization between the 5620 SAM Server and the 5620 SAM Auxiliary Statistics Collector. Similarly, this will require more significant bandwidth utilization between the 5620 SAM Auxiliary Statistics Collector and the 5620 SAM Database workstations. The bandwidth requirements are not dependent on network activity.

5.10 Bandwidth requirements for the 5620 SAM Call Trace Collector workstation

5.10.1 Bandwidth requirements for the 5620 SAM Call Trace Collector workstation

The main factors impacting communication to and from the 5620 SAM Auxiliary Call Trace Collector workstation are:

- Number of WMMs where Call Traces are enabled.
- Size of files being retrieved by the 5620 SAM OSS client requesting the Call Trace.

The more call traces that are enabled, the higher the bandwidth requirement from the WMM network elements to the 5620 SAM Auxiliary Call Trace Collector. Enable and Disable messages are sent to the 5620 SAM Auxiliary Call Trace Collector from the 5620 SAM Server. 5620 SAM OSS Clients can ask the 5620 SAM Server for the list of 5620 SAM Call Trace Collector workstations, and ftp connect directly to the 5620 SAM Auxiliary Call Trace Collector to retrieve the call trace log files.

5.11 Bandwidth requirements for the 5620 SAM Auxiliary Cflowd Collector workstation

5.11.1 Bandwidth requirements for the 5620 SAM Auxiliary Cflowd Collector workstation

The main factors impacting communication to and from the 5620 SAM Auxiliary Cflowd Collector workstation are:

- Size of the SAM managed network for the network extraction
- Size of generated IPDR files
- Number of 7750 flows sending cflowd records

Table 5-11 Additional bandwidth requirements for Cflowd Auxiliary.

Bandwidth requirements for 5620 SAM Cflowd Auxiliary	Bandwidth usage characterization
5620 SAM Server to a 5620 Cflowd Auxiliary This is for Network Snapshot Transfer (FTP/SFTP) By default this operation should only occur weekly if the SAM Server and 5620 SAM Cflowd Auxiliary Server remain in sync. The amount of bandwidth required is dependent on network size.	Bandwidth requirement will depend upon network size, which determines the network extraction file size, and the desired time complete the file transfer from the SAM Server to the Cflowd Auxiliary
7750 SR(s) to 5620 SAM Cflowd Auxiliary In the case of Redundant 5620 SAM Cflowd Auxiliary Servers the amount of dedicated bandwidth is required for each Cflowd Auxiliary.	40 Mbps per 20,000 flows per second

Table 5-11 Additional bandwidth requirements for Cflowd Auxiliary. (continued)

Bandwidth requirements for 5620 SAM Cflowd Auxiliary	Bandwidth usage characterization
5620 SAM Cflowd Auxiliary to IPDR file storage server Approximate amount of Stats per a 1 MB IPDR Stats File: 2,560 TCP PERF statistics (all counters) or, 3,174 RTP statistics (all counters) or, 9,318 Comprehensive statistics (all counters) or 9,830 Volume statistics (all counters) In the case of Redundant 5620 SAM Cflowd Auxiliary Servers, the amount of dedicated bandwidth calculated on the right is for each 5620 SAM Cflowd Auxiliary Server to the workstation where IPDR files are being transferred.	Use the information on the left to calculate the amount of data generated for the expected Statistics. Use this to calculate the time to transfer at a given bandwidth. The total time must be less than 50% of collection interval. For example – if 1GB of IPDR files are expected per interval, and the collection interval is 5min, a 45 Mbps connection will take 3min,2sec to transfer. This is more than 50% and a larger network connection is required.

5.12 Bandwidth requirements for the 5620 SAM PCMD Collector workstation

5.12.1 Bandwidth requirements for the 5620 SAM PCMD Collector workstation

The main factors impacting communication to and from the 5620 SAM Auxiliary PCMD Collector workstation are:

- Number of bearers.
- Number of and size of events per bearer.
- Size of files being retrieved by the 5620 SAM OSS client requesting the PCMD files.

On average, each bearer will generate 100 events per hour where each event is approximately 250 bytes in size.

5.13 5620 SAM bandwidth requirements for communicating with network elements

5.13.1 5620 SAM bandwidth requirements for communicating with network elements

In order to effectively manage the network, 5620 SAM must have access to sufficient bandwidth between the 5620 SAM Server(s), 5620 SAM Auxiliary(s) and the network elements.

This bandwidth will be used to carry the management traffic between 5620 SAM and the network element. The following table describes the bandwidth requirements for a particular network element.

Table 5-12 5620 SAM Server to network bandwidth requirements

Number of MDAs/CMAs/XMAs	Network element Example	Bandwidth requirement from 5620 SAM Server(s) to the network element
2	7450 ESS-1	200 kbps
N/A	OmniSwitch 6250, 6400, 6450, 6850, 6855, 9000 Series	300 kbps

Table 5-12 5620 SAM Server to network bandwidth requirements (continued)

Number of MDAs/CMAs/XMAs	Network element Example	Bandwidth requirement from 5620 SAM Server(s) to the network element
N/A	OmniSwitch 6900, 6860E, 10K	400 kbps
N/A	9500 MPR	200 kbps
10	7450 ESS-7 (fully loaded)	1 Mbps
8	7705 SAR (fully loaded)	200 kbps – 400 kbps
20	7750 SR-12 (fully loaded)	2 Mbps
18	7750 SR-12E (fully loaded)	2 Mbps
6	7950 XRS	2-4 Mbps
12	7750 SR-c12 (fully loaded)	600 kbps
1	7210 SAS-E, 7210 SAS-M, 7210 SAS-K	200-300 kbps
1	7210 SAS-D, 7210 SAS-X, 7210 SAS-T, 7210 SAS-R, 7210 SAS-Mxp, 7210 SAS-Sx	500-600 kbps
N/A	7701 CPAA	250 kbps
N/A	9471 WMM / vMM	200 kbps
N/A	DSC	200 kbps
N/A	Macro Cell eNodeB (3 Cell)	600 kbps
N/A	1830 PSS / OCS	600-800 kbps
N/A	1830 VWM OSU	400 kbps
N/A	Small Cell Gateway	600-800 kbps
N/A	Small Cell Access Point	3.5 Mbps (per 1,000 APs)

5.13.2 Details on the bandwidth requirements

The recommended bandwidth described above is a conservative figure that is meant to ensure that the performance of 5620 SAM and its ability to manage successfully each network element will not be affected by unusual network conditions.

Specifically, the bandwidth recommendation ensures that 5620 SAM can fully discover (or resynchronize) all of the objects contained in the network element, within a reasonable amount of time, usually no more than a few minutes for a densely populated network element.

The following are the main operations that result in significant amounts of information being exchanged between 5620 SAM and the network elements. These factors are therefore the principal contributors to the bandwidth requirements.

- Network Element Discovery: Upon first discovery of the network element, a significant amount of data is exchanged between 5620 SAM and the network element.
- SNMP traps: SNMP traps do not result directly in significant data being sent from the network element to the 5620 SAM. Several of the SNMP traps however do not contain all of the information required for 5620 SAM to completely represent the new status of the network

element. As a result, 5620 SAM will subsequently perform a poll of a certain number of the SNMP MIBs to obtain the required information from the network element. Consequently, SNMP traps do result in a certain quantity of data and therefore cause bandwidth utilization. The exact quantity of bandwidth utilized will vary based on the number and the type of trap that is sent from the network element. In the worst case however, this bandwidth utilization will be less than that utilized during a network element discovery.

- SNMP polling: It is possible to configure 5620 SAM to poll the SNMP MIBs on the network elements at various intervals. By default, 5620 SAM will perform a complete poll of the SNMP MIBs every 24 hours on non-SR–OS based network elements. During the polling cycle, the amount of data transferred between 5620 SAM and the network element is equivalent to the amount of data transferred during the network element discovery.
- Statistics collection: It is possible to configure 5620 SAM to poll the SNMP MIBs on the network elements that contain performance statistics information. During the polling cycle, the amount of data transferred between 5620 SAM and the network element is less than the amount of data transferred during the network element discovery. With the configuration of a 5620 SAM Auxiliary Statistics Collector, the communication from and to the network elements will be distributed between the 5620 SAM Server and a 5620 SAM Auxiliary Statistics Collector.
- Network element backup: It is possible to configure 5620 SAM to request a backup of the network element at specified interval. During the NE backup cycle, the amount of data transferred between 5620 SAM and the network element is less than half of the amount of data transferred during the network element discovery.
- Provisioning of services and deployment of configuration changes: When network elements are configured or when services are provisioned via the 5620 SAM GUI or via application using the 5620 SAM-O interface, a small quantity of network bandwidth is utilized. The amount of data transferred is significantly less than during the network element discovery.
- Initiation and collection of STM tests and their results: When STM tests are initiated, the 5620 SAM Server sends individual requests per elemental test to the network elements. Once the test is complete, the network elements report back using a trap. The 5620 SAM server then requests the information from the network element, and stores it in the database. This can result in a significant increase in network traffic to the network elements.
- Software Downloads: The infrequent downloading of network element software loads is not included in the bandwidth levels stated in Table 5-12, “5620 SAM Server to network bandwidth requirements” (p. 61) . Bandwidth requirements will depend upon the size of the network element software load and the desired amount of time to successfully transfer the file to the NE.

For some network elements, management of the NE includes methods other than standard MIB/SNMP management – for example web-based tools. These network elements may require additional bandwidth above the bandwidth levels stated in Table 5-12, “5620 SAM Server to network bandwidth requirements” (p. 61) .

5.13.3 Possible consequences of insufficient bandwidth

In situations where there is less than the recommended bandwidth between the 5620 SAM and the network element, the following are possible consequences:

- The length of time required to perform a network element discovery will increase
- The length of time required to perform a SNMP poll of the network element will increase

- The length of time required to retrieve statistics from the network element will increase
- The proportion of SNMP traps that will not reach 5620 SAM because of congestion will increase. This is significant since 5620 SAM will detect it has missed traps from the network element and will result in 5620 SAM performing additional SNMP polling to retrieve the missing information. This will result in additional data being transferred, which will increase the bandwidth requirements, possibly exacerbating the situation.

5.13.4 Determining total bandwidth requirements for 5620 SAM-managed networks

The amount of bandwidth required for each of the network elements should be obtained from Table 5-12, “5620 SAM Server to network bandwidth requirements” (p. 61) .

The total amount of bandwidth that is required for 5620 SAM to manage the complete network will vary based on the topology of the infrastructure that is used to carry the management traffic. From 5620 SAM’s perspective, there must be sufficient bandwidth (as per Table 5-12, “5620 SAM Server to network bandwidth requirements” (p. 61)) between itself and each of the network elements that is under management.

In cases where the management traffic is carried over physical point-to-point links between the 5620 SAM Server and 5620 SAM Auxiliary network and each of the network elements, sufficient bandwidth must be reserved on the physical links. The 5620 SAM Server complex can simultaneously communicate to several NEs for the following functions:

- NE Discovery, NE Resync, Resyncing for Trap Processing
- NE Backups, NE Software Downloading, and sending configurations to NEs
- Collecting Performance Statistics
- Collecting Accounting Statistics
- Initiating STM Tests on NEs
- Retrieve STM Test Results - also via FTP
- NE Reachability checks and NE trap gap checks

Rarely are all of the above performed simultaneously so it is recommended to assume for link aggregation points that SAM can communicate with a minimum of 20-30 NEs simultaneously – this can increase to 60-70 NEs on a 16 CPU core 5620 SAM Server workstation. For Networks of over 1,000 NEs or where a SAM Auxiliary Statistics Collector is being used, that number should be increased by 20-30 NEs. Higher bandwidth maybe required under special cases where above average data is attempted to be transferred between SAM and the network elements. For example, large statistics files, NE backups, or software images.

5.14 Network latency considerations

5.14.1 Network latency considerations

Network latency can potentially impact the performance of the 5620 SAM workstations. The following are known impacts of latency between the various 5620 SAM workstations:

- 5620 SAM Server to 5620 SAM Clients (GUI/OSS): event notification rates of network changes

- 5620 SAM Auxiliary Statistics Collector to the network elements: ftp connection for statistics collection and SNMP stats collection
- 5620 SAM Server to the network elements: resync times, provisioning, ftp connections for statistics and network element backups, trap handling, and SNMP stats collection (See "Scaling guidelines for statistics collection" (p. 77) for more information on latency impact on SNMP stats collection)
- 5620 SAM Server and 5620 SAM Auxiliary Collector to 5620 SAM Database: 5620 SAM performance is sensitive to latency in this area. The round trip latency between the active 5620 SAM components (Server, Database, Auxiliary) must be no longer than 1 ms., otherwise overall 5620 SAM performance will be significantly impacted. The 5620 SAM Auxiliary Database can tolerate up to 200 ms of latency between it and the rest of the 5620 SAM management complex.

Since SNMP communication to a single Network Element is synchronous, the impact of latency is directly related to the number of SNMP gets and responses. Operations to a Network Element with a round trip latency of 50 ms will have the network transmission time increase by ten times compared to a Network Element with a round trip latency of only 5 ms. For example, is a specific operation required 5620 SAM to send 1,000 SNMP gets to a single Network Element, 5620 SAM will spend a total of 5 seconds sending and receiving packets when the round trip latency to the network element if 5 ms. The time that 5620 SAM spends sending and receiving the same packets would increase to 50 seconds if the round trip latency were increased to 50 ms.

Network Element re-sync can be especially sensitive to latency as the number of packets exchanged can number in the hundreds of thousands. For example, if a re-sync consists of the exchange of 100,000 packets (50,000 gets and 50,000 replies), 50 ms of round trip latency would add almost 42 minutes to the overall re-sync time and 100 ms of round trip latency would add almost 84 minutes to the overall re-sync time.

As of SAM 12.0R1, a proprietary mechanism is used to discover and resync specific node types and versions, that can dramatically reduce resync and discovery times to network elements with high network latency. TCP Streaming is supported on the following Network Element types with a release of 11.0R5 or later:

- 7950 XRS
- 7750 SR
- 7450 ESS
- 7710 SPR

5.14.2 Common geographical location of 5620 SAM workstations

It is ideal to ensure that all 5620 SAM workstations and the 5620 SAM OSS clients are collocated within a geographical site on a high availability network to avoid the impact of network latency.

In cases where geographic redundancy is configured, all active 5620 SAM workstations (5620 SAM Server, 5620 SAM Auxiliary, and 5620 SAM Database) should be located within a geographical site on a high availability network to avoid the impact of network latency. When a 5620 SAM workstation (server, auxiliary, or database) switchover or failover occurs, manual intervention may be required to align the workstations on the same geographical site to minimize the performance impact of network latency. This task can be automated by enabling the DB Alignment feature within 5620 SAM.

5.14.3 Optimizing throughput between 5620 SAM workstations

In high-speed, high-latency networks the TCP socket buffer size controls the maximum network throughput that can be achieved. If the TCP socket buffer is too small it will limit the network throughput, despite the fact that the available bandwidth might support much higher transfer rates.

Adjusting the TCP socket buffer size to achieve optimal network throughput may be necessary if the network bandwidth is more than 10Mbps and roundtrip latency is higher than 25ms.

The optimal TCP socket buffer size is the bandwidth delay product (BDP). The bandwidth delay product is a combination of the network bandwidth and the latency, or round-trip time (RTT); basically, it is the maximum amount of data that can be in transit on the network at any given time.

For example, given a 20Mbps network with a RTT of 40ms the optimal TCP socket buffer size would be computed as follows:

```
BDP = 20 Mbps * 40ms = 20,000,000 bps * .04s = 800,000 bits / 8 = 100,000 bytes socket
buffer size = BDP  = 100,000 bytes
```

The RHEL documentation should be consulted to determine how to modify the TCP socket buffer size and ensure that the change is persistent.

It is important to note that increasing the TCP socket buffer size directly affects the amount of system memory consumed by each socket. When tuning the TCP socket buffer size at the operating system level, it is imperative to ensure the current amount of system memory can support the expected number of network connections with the new buffer size.

5.14.4 Additional 5620 SAM Database throughput optimizations

In addition to the optimizations above, the 5620 SAM Database workstation requires changes to the sqlnet.ora and listener.ora files that are contained in the oracle/network/admin directory. The lines with the SEND_BUF_SIZE and RECV_BUF_SIZE should be uncommented (delete the “#” character), and set to 3 times the BDP value calculated above. The database should be shutdown when this change is made.

5.15 Network reliability considerations

5.15.1 Network reliability considerations

This section describes network reliability considerations.

5.15.2 Reliability between 5620 SAM components

The 5620 SAM requires reliable network communications between all the SAM Components:

- 5620 SAM Servers
- 5620 SAM Databases
- 5620 SAM Auxiliaries
- 5620 SAM Auxiliary Databases
- 5620 SAM Analytics Server
- 5620 SAM GUI Clients and 5620 SAM Client Delegate Server

- 5620 SAM OSS Clients

The performance and operation of 5620 SAM can be significantly impacted if there is any measurable packet loss between the 5620 SAM workstations. Significant packet loss can cause 5620 SAM reliability issues.

Nokia supports the deployment of 5620 SAM using the RHEL IP Bonding feature. The support for IP Bonding is intended only to provide network interface redundancy configured in active-backup mode for IP Bonding. All other modes of IP Bonding are not supported. RHEL documentation should be consulted on how to configure IP Bonding.

5.15.3 5620 SAM Server to NE network reliability

The 5620 SAM Server requires reliable network connectivity between the 5620 SAM Server/ Auxiliary to the managed network elements. The mediation layer in 5620 SAM is designed to recover from lost packets between the 5620 SAM Server and the network elements; however, these mechanisms come with a cost to performance. Any measurable packet loss will degrade performance of 5620 SAM's ability to manage the Network Elements. The loss of packets between SAM and NE will have an impact on (but not limited to):

- Any SNMP operations to the network elements:
- SNMP Trap processing performance
- Provisioning performance
- Provisioning failures
- Performance statistics collection (possibly to the point where statistics collection will be incomplete)
- STM test operation (initiating test and collecting results retrieval)
- NE discovery and resync performance
- NE discovery and resync failures
- scheduled polling for reachability checks
- Accounting Statistics retrieval (possibly to the point where statistics collection will be incomplete)
- CLI session operation
- NE backup retrieval and software download performance

The following example highlights the significant impact of lost packets. It only considers the SNMP communication times with one network element. With the default mediation policy configured with an SNMP retry time-out of 10 seconds, and an average round trip latency of 50 ms between 5620 SAM Server and the network element, 5620 SAM will spend a total of 25 seconds sending and receiving 1000 packets (500 SNMP gets and 500 SNMP responses). With a 0.1% packet loss (1 packet out of the 1,000) the 5620 SAM Server will wait for the retry time-out (10 seconds) to expire before retransmitting. This will cause the time to complete the 500 SNMP gets to increase by 10 seconds – for a total of 35 seconds of communication time, or an increase of 40% over the time with no packet loss. With 0.5% packet loss, the 500 SNMP gets would increase by 50 seconds – for a total of 75 seconds to complete or an increase of 200%.

5.16 GNE, Nokia OmniSwitch, 9471 WMM, eNodeB, and DSC considerations

5.16.1 GNE, Nokia OmniSwitch, 9471 WMM, eNodeB, and DSC considerations

5620 SAM Clients support the web-based WebView functionality on OmniSwitch family of switches which requires direct network connectivity to the Network Element from the 5620 SAM Client.

5620 SAM Clients support web-based clients on Generic Network Elements (GNEs) but require direct network connectivity between the 5620 SAM Client and GNE.

The DSC and 9471 WMM are treated as network elements within 5620 SAM.

The DSC is managed via a web interface that is run through the browser that is installed on the 5620 SAM Client workstation or 5620 SAM Delegate workstation. It requires a direct connection from the 5620 SAM Client to the DSC. As such, unique firewall rules are required. There are also increased memory requirements on the 5620 SAM Client and/or 5620 SAM Delegate workstations for the Web Browser.

The 9471 WMM requires two management tools to be configured: the MME MI tool, and the Client. Their management includes communication directly from the 5620 SAM Client to the 9471 WMM platforms.

The eNodeB NEM is installed along with the 5620 SAM Client and communicates with the eNodeB elements in the network through a UDP proxy configured on the 5620 SAM Server, eliminating the need for direct communication between the network elements and the 5620 SAM Client. NEM runs within a separate JVM requiring additional memory resources on the 5620 SAM Client workstation. Please consult the NEM User Guide for up-to-date memory requirements for NEM.

9500 MPR support includes the use of NEtO for specific management functions for these Network Element types. NEtO is a separate application that is installed along with the 5620 SAM Client and launched through the 5620 SAM Client UI. Please consult the 9500 MPR Documentation Suite for current memory requirements that are in addition to the 5620 SAM Client memory requirements. The 9500MPR also uses a web interface for management.

6 Scaling

6.1 Overview

6.1.1 Purpose

This chapter provides general information about platform scalability for the 5620 SAM.

6.1.2 Contents

Scaling guidelines

6.2 Scalability limits

6.2.1 Scalability limits

Table 6-1, “5620 SAM Release 14.0 R15 scalability limits” (p. 70) represents the scalability limits for Release 14.0 R15. Note that:

- These limits require particular hardware specifications and a specific deployment architecture.
- Scale limits for all network elements assume a maximum sustained trap rate of 100 traps/second for the entire network. 5620 SAM’s Trap processing rate depends on many factors including trap type, NE type, NE configuration, NE and network latency, network reliability as well as the size and speed of the servers hosting the 5620 SAM application. 5620 SAM scalability testing runs at a sustained trap rate exceeding 100 trap/s for the largest deployment and server configurations.

Chapter 3, “Platform requirements” contains information on identifying the correct platform for a particular network configuration. To achieve these scale limits, a distributed 5620 SAM configuration is required, and may also require a 5620 SAM Auxiliary Statistics Collector and a storage array for the 5620 SAM database workstation.

Consult Nokia personnel to ensure you have the correct platform and configuration for your network size.

Table 6-1 5620 SAM Release 14.0 R15 scalability limits

Attribute of managed network	Scaling Limit
Maximum number of managed MDAs	60,000
Maximum number of Network Elements	50,000
Maximum number of GNEs [1]	50,000
Maximum number of managed services	4,000,000
Maximum number of optical transport services	20,000
Maximum number of SAPs	12,000,000
Maximum number of simultaneous 5620 SAM GUI sessions	250
Maximum number of simultaneous web UI client sessions	50–250 (see 5620 SAM Applications Guide for details)
Maximum number of simultaneous active 5620 SAM-O HTTP applications	30
Maximum number of simultaneous active 5620 SAM-O JMS applications	20
Maximum number of outstanding alarms	50,000
Maximum number of outstanding alarms - Distributed Configuration	250,000

Table 6-1 5620 SAM Release 14.0 R15 scalability limits (continued)

Attribute of managed network	Scaling Limit
Maximum number of Alarms	9,600,000
Maximum number of TCAs	250,000
Maximum number of monitored services in the Service Supervision application	1,000,000
Maximum number of VMs (VSAP)	25,000
Maximum number of vPorts (VSAP)	25,000

Notes:

1. The number of interfaces on a GNE and the traps that may arise from them is the key factor determining the number of GNE devices that can be managed. As GNE devices are expected to be access devices the sizing is based on an average of 10 interfaces of interest on each device (10 x 50,000 = 500,000 interfaces). Processing of traps from interface types that are not of interest can be turned off in 5620 SAM. Under high trap load, 5620 SAM may drop traps

   5620 SAM uses the number of MDAs as the fundamental unit of network dimensioning. To determine the current or eventual size of a network, the number of deployed or expected MDAs, as opposed to the capacity of each router, must be calculated.

Table 6-2 Network element maximums and equivalency

Network element Type	Maximum number of network elements supported	MDA equivalency
7750, 7450, 7710	50,000	1 MDA = 1 MDA [1] [2]
7705	50,000	50,000
7210	50,000	50,000
OMNISwitch 6250, 6400, 6450, 6850, 6855 (each shelf in the stackable chassis)	50,000	50,000
OMNISwitch 6860E	800	800
OMNISwitch 6900	800	800
OMNISwitch 9600, 9700, 9700E, 9800, 9800E (each NI)	1,000	1,000
OMNISwitch 10K (each NI)	400	400
9471 WMM,	80	[3]
DSC	64	[3]
9500 MPR	15,000	15,000
9412 LTE / 9926 LTE eNodeB	15,000	1 Cell = 1 MDA (max 72,000 cells)
9763 LTE MCI / 9764 LTE MCO eNodeB	25,000	25,000

Table 6-2 Network element maximums and equivalency (continued)

Network element Type	Maximum number of network elements supported	MDA equivalency
9962 Multi-standard Enterprise Cell AP	50,000	N/A
9362 3G Enterprise Cell AP	100,000	N/A
9361 3G Home Cell / 9961 MS Home Cell AP	1,000,000	N/A
9363 3G MCI / 9364 3G MCO / 9764 WCDMA MCO AP	100,000	N/A
9966 MS Gateway	100	N/A
1830 PSS	10,000	[4]
1830 PSS OCS	300	[5]
1830 VWM OSU	2,000	[6]
VSC	1	N/A

Notes:

1. The IMM card has an MDA equivalency of 2 MDAs per card.
2. The CMA card has an MDA equivalency of 1 MDA per card.
3. The DSC and the 9471 WMM have an MDA equivalency of 1 MDA per blade.
4. The1830 PSS Card Slot has an MDA equivalency of 1/4 MDA per card, to a maximum MDA equivalency of 35,000
5. The1830 PSS OCS Card Slot has an MDA equivalency of 1/10 MDA per card, to a maximum MDA equivalency of 1,920
6. The 1830 VWM OSU Card Slot has an MDA equivalency of 1/4 MDA per card to a maximum MDA equivalency of 25,000

6.3 5620 SAM Performance Targets

6.3.1 5620 SAM Performance Targets

Table 6-3, “5620 SAM Release 14.0 Performance Targets” (p. 73) represents the performance targets 5620 SAM. Factors that may result in fluctuations of these targets include:

- 5620 SAM Server and 5620 SAM Database system resources
- network activity
- user/OSS activity
- database activity
- network size
- latency

Table 6-3 5620 SAM Release 14.0 Performance Targets

Performance item description	Target
5620 SAM Client GUI performance	
Time to launch a 5620 SAM Client GUI	~30 seconds
Time to launch a 5620 SAM Client GUI configuration form	~2 seconds
Time to save a 5620 SAM Client GUI configuration form	~2 seconds
5620 SAM Server performance	
Time to restart the 5620 SAM Server when managing the maximum number of devices	~30 minutes
Estimated time to resynchronize one new router in domain	<20 minutes (subject to size of new router)
5620 SAM DB Backup (without Statistics)	Up to 60 minutes (subject to network size)
5620 SAM DB Restore	~75 minutes
5620 SAM Server activity switch	<45 minutes
5620 SAM DB switchover (by invoking through the GUI)	<45 minutes
5620 SAM DB failover	<45 minutes until complete recovery, including 5620 SAM Server restart
Recovery of standby 5620 SAM Database after failover	<75 minutes
5620 SAM-O performance	
Number of services created per day by an OSS workflow for VLL Service type	Up to 25K per day (24 hours)
Average time to create 1 VLL service	~3.0 seconds
Average time to create 1 VPLS service (3 sites, 1 SAP/site)	~4.5 seconds
Average time to create 1 VPLS service (6 sites, 1 SAP/site, 30 circuits fully meshed)	~10 seconds
Average time to configure 100 VPLS services on 3 sites using one SAP	~16 minutes
Average time to add 1 IES interface to an existing service	~1.5 seconds
Average time to create 1 static route on a 7750 SR	~0.6 seconds
Average time to create 1 MAC ACL filter	~0.8 seconds
Average time to create 1 GRE SDP	~0.75 seconds
Average time to create 1 MPLS SDP	~1.0 seconds
Average time to create 1 MPLS path	~0.8 seconds
Upgrade Performance	
5620 SAM Client Upgrade	<10 minutes
5620 SAM complex upgrade (server, database, auxiliaries) [1]	<6 hours

Table 6-3 5620 SAM Release 14.0 Performance Targets (continued)

Performance item description	Target
5620 SAM upgrade maximum visibility outage with 5620 SAM redundant system [2]	<15 minutes

Notes:

1. The target includes the installation of the software on the existing servers and 5620 SAM database conversion. Operating System installation/upgrades, patching, pre/post-upgrade testing and file transfers are excluded from the target.
2. Provided proper planning and parallel execution procedures were followed.

Scaling guidelines for 5620 SAM OSS Clients

6.4 OSS client limits

6.4.1 OSS client limits

There can be a maximum of 20 5620 SAM OSS-JMS Clients. Greater than 10 5620 SAM OSS-JMS Clients requires a SAM Server with a minimum of 16 CPU Cores.

The number of 5620 SAM OSS-HTTP Clients supported by a 5620 SAM Server workstation is 2 times the number of CPU cores with at least 10 and at most 30 clients supported.

The 3GPP interface can support up to 3 notification clients and 3 action/request clients.

The maximum number of concurrent findToFile operations supported is 5.

6.5 5620 SAM OSS Clients using JMS

6.5.1 5620 SAM OSS Clients using JMS

As of 5620 SAM 9.0R5, OSS Clients using JMS durable connections have a maximum message rate comparable to non-durable clients.

Network latency between the 5620 SAM Server and a 5620 SAM OSS Client will reduce the JMS message rate. For durable JMS clients, the *Duplicate OK* method will allow for a higher message rate than the *Auto Acknowledge* method. Refer to the *5620 SAM-O OSS Interface Developer Guide* for more information.

5620 SAM is also able to deliver hundreds of messages per second to a non-durable 5620 SAM OSS client.

Table 6-4 JMS durable messaging rates

JMS messaging	Roundtrip latency from the OSS Client to the 5620 SAM Server		
	0ms	20ms	40ms
Durable connection with Auto-acknowledge (messages/s) [1]	1000	690	383
Durable connection with Duplicates-OK (messages/s) [1]	1000	815	418

Notes:

1. Messaging rates will be lower if using SSL.

6.6 5620 SAM 3GPP OSS Client

6.6.1 5620 SAM 3GPP OSS Client

5620 SAM 3GPP OSS Clients connect to the 3GPP CORBA interface provided on the 5620 SAM Server. Network latency between the 5620 SAM Server and a 5620 SAM 3GPP OSS Client will reduce the message rate.

Table 6-5 3GPP OSS JMS messaging rates

CORBA messaging	Roundtrip latency from the OSS Client to the 5620 SAM Server		
	0ms	20ms	40ms
3GPP OSS connection (messages/s)	74	68	53

Scaling guidelines for statistics collection

6.7 Statistics collection

6.7.1 Statistics collection

5620 SAM provides the ability to collect statistics information from the network elements. This section provides guidelines that can be used to determine the extent to which Statistics Collection can be retrieved from the network.

6.7.2 Statistics collection definitions

Performance statistics: These statistics are associated with various network objects such as ports, interfaces, channels and network elements (routers). These statistics are retrieved by 5620 SAM using SNMP polling according to the MIB policies that are configured by the user.

Accounting statistics: These statistics are associated with Services, Subscribers, and Network Interfaces and contain data that can be used for accounting, billing and SLA management purposes. These statistics are collected on the 7x50 and retrieved by 5620 SAM via a file that is transferred via ftp/sftp.

Application Assurance Accounting statistics: These statistics are associated with Subscribers, SAPs, and spoke SDP bindings and contain data related to traffic flows that can be used for QoS and traffic management, and application aware reporting. These statistics are collected on the 7x50 ISA cards and retrieved by 5620 SAM via a file that is transferred via ftp/sftp.

Statistics Item: An individual statistics counter, such as RxOctets or TxFrames.

Statistics Record: A collection of statistics items which is retrieved from the router and stored in the 5620 SAM database as an atomic operations. In the various statistics forms on the 5620 SAM GUI Client, a statistics record appears to the user as a single row which contains the collection or retrieval timestamp and a set of individual statistics items. In the case of performance statistics, a statistics record corresponds to a row in the MIB table.

6.7.3 Determining the number of statistics records that will be collected

Statistics can be collected and processed by the 5620 SAM Server or by the 5620 SAM Auxiliary Statistics Collector for dedicated statistics handling. The 5620 SAM Auxiliary Statistics Collector provides a dedicated workstation for statistics collection. The following sections should be used to determine the maximum performance and accounting statistics for different hardware setups.

6.7.4 Performance statistics

Refer to the *5620 SAM Statistics Management Guide* to find the steps required to configure 5620 SAM to retrieve and process performance statistics. Note that two steps are required to enable the collection of performance statistics from the network. First, a policy is defined which specifies a set of polling periods for various MIBs. Second, the policy is applied to a number of network elements.

In general, enabling the statistics collection of a MIB will result in one statistics record being collected, at the specified polling period, for each network object to which the MIB applies.

For example, consider a policy is created with only the rtr.L2AccessDhcpRelayCfgStats MIB enabled for collection at 15-minute intervals. That policy is assigned to only two network elements which each contain 500 L2 Access Interfaces. As a result of this action, 5620 SAM will collect 1,000 statistics records from the network every 15 minutes.

The quantity of resources which are allocated to the retrieval and processing of performance statistics does not depend significantly on the number of CPU Cores available to the 5620 SAM Server or Auxiliary Statistics collector software. The tables below show the maximum number of performance statistics that can be retrieved and processed by the 5620 SAM server and the 5620 SAM Auxiliary Statistics Collector every 15 minutes.

Table 6-6 Maximum number of performance statistics records processed by a 5620 SAM Server

Number of CPU cores on 5620 SAM Server workstations	Maximum number of performance statistics records per 15-minute interval	
	Collocated configuration	Distributed configuration
4 or greater	50,000	150,000

Table 6-7 Maximum number of performance statistics records processed by a 5620 SAM Statistics Auxiliary

Number of Active Auxiliary Statistics Collectors	Maximum number of performance statistics records per 15-minute interval			
	Statistics collection with SAM Database		Statistics collection with Auxiliary Database	logTofile only
	8 CPU Cores, 16GB RAM	12 CPU Cores, 24GB RAM	12 CPU Cores, 32GB RAM	12 CPU Cores, 24GB RAM
1	500,000	2,000,000	2,000,000	2,000,000
2	500,000	2,000,000	4,000,000	4,000,000
3	500,000	2,000,000	4,000,000	4,000,000

To compute the number of CPU cores available on the workstation, the following command can be used:

```
# dmidecode | grep "Core Count" | /usr/bin/awk '{SUM += $3} END {print SUM}'
```

In situations where 5620 SAM is asked to collect more performance statistics than it can process in the specified polling period, the *PollerDeadlineMissed* alarms will start appearing. These alarms indicate to the user that the polling mechanisms within 5620 SAM cannot retrieve the requested information within the specified polling period. Should this situation arise, the polling period for statistics should be increased or the number of objects that are applied to Statistics Poller Policies should be reduced.

6.7.5 Performance statistics collection and network latency

5620 SAM collection of performance statistics from a single network element may be limited due to the round trip delay caused by network and network element latency. 5620 SAM collects performance statistics records using SNMP. One record is collected at a time to limit the load on the network element. Therefore, round trip latency will directly impact the maximum number of performance statistics records collected. As an example, if the round trip latency is 100ms, and we target a completion time of 66% of the collection interval (to allow for processing variances and

other system impacts), the maximum number of performance statistics records that can be collected from one network element in a 15 minute interval would be 6000 records (66% of 900 seconds divided by 100 ms latency).

6.7.6 Accounting statistics

Refer to the *5620 SAM Statistics Management Guide* to find the steps required to configure 5620 SAM to retrieve and process accounting statistics.

The quantity of resources which are allocated to the retrieval and processing of accounting statistics within the 5620 SAM Server or Auxiliary Statistics collector are set at the installation time and depend on the number of CPU Core available to the 5620 SAM Server or Auxiliary Statistics collector software. The number of CPU Cores available to the server depends on the number of CPU Cores on the workstation and whether the 5620 SAM Database software is collocated with the 5620 SAM Server software on the same workstation.

An accounting statistic record is the statistic for one queue for one SAP. For example, if 2 ingress and 2 egress queues are configured per SAP, the “Combined Ingress/Egress” statistic represents 4 5620 SAM accounting statistic records.

It is recommended that the Accounting Policy Interval and the File Policy Interval be aligned to the same period. Misalignment of the policy periods can cause 5620 SAM resource contention for both performance and accounting statistics processing.

The following tables provide the maximum number of accounting statistics records that can be retrieved and processed by the 5620 SAM Server or 5620 SAM Auxiliary Statistics Collector in various situations.

To reach the peak accounting statistics collection from the 5620 SAM Auxiliary Statistics Collector workstation, the 5620 SAM Database workstation requires a customized configuration that can be obtained from Nokia personnel.

Table 6-8 Maximum number of accounting statistics records processed by a 5620 SAM Server workstation

Number of CPU cores on 5620 SAM Server workstations	Maximum number of accounting statistics records per 15-minute interval	
	Collocated configuration	Distributed configuration
4	100,000	200,000
8 or greater	200,000	400,000

Table 6-9 Maximum number of accounting statistics records processed by a 5620 SAM Statistics Auxiliary

Number of Active Auxiliary Statistics Collectors	Maximum number of accounting statistics records per 15-minute interval			
	Statistics collection with SAM Database		Statistics collection with Auxiliary Database	logToFile only
	8 CPU Cores, 16GB RAM	12 CPU Cores, 24GB RAM	12 CPU Cores, 32GB RAM	12 CPU Cores, 24GB RAM
1	10,000,000	10,000,000	20,000,000	20,000,000
2	10,000,000	10,000,000	40,000,000	40,000,000
3	10,000,000	10,000,000	60,000,000	60,000,000

To compute the number of CPU cores available on the workstation, the following command can be used:

```
# dmidecode | grep "Core Count" | /usr/bin/awk '{SUM += $3} END {print SUM}'
```

In situations where 5620 SAM is asked to collect more accounting statistics records than it can process in the specified retrieval period, the extra statistics will not be retrieved from the network.

There are two methods to export accounting and performance statistics from 5620 SAM; registerLogToFile, and findToFile. The registerLogToFile method is the preferred method and is required for situations where more than 400,000 accounting statistics records are retrieved in 15 minutes or 500,000 performance statistics are retrieved in 15 minutes.

6.7.7 Application Assurance Accounting statistics

Refer to the *5620 SAM Statistics Management Guide* to find the steps required to configure 5620 SAM to retrieve and process application assurance accounting statistics.

The quantity of resources which are allocated to the retrieval and processing of application assurance accounting statistics within the 5620 SAM Server are set at the installation time and depend on the number of CPUs available to the 5620 SAM Server software. The number of CPUs available to the 5620 SAM Server depends on the number of CPUs on the workstation and whether the 5620 SAM Database software is collocated with the 5620 SAM Server software on the same workstation.

Scaling of Application Assurance collection is related to the number of objects configured for collection as opposed to the number of records collected per interval.

The following tables provide the maximum number of application assurance objects that can be configured for collection by the 5620 SAM Server or 5620 SAM Auxiliary Statistics Collector in various situations.

Table 6-10 Maximum number of application assurance accounting objects configured for collection by a 5620 SAM Server workstation

Number of CPU cores on 5620 SAM Server workstations	Maximum number of application assurance accounting objects configured for collection per 15-minute interval	
	Collocated configuration	Distributed configuration
4	50,000	100,000
8 or greater	100,000	200,000

Table 6-11 Maximum number of application assurance accounting objects configured for collection by a 5620 SAM Statistics Auxiliary

Number of Active Auxiliary Statistics Collectors	Maximum number of application assurance accounting objects configured for collection per 15-minute interval		
	Statistics collection with SAM Database		Statistics Collection with Auxiliary Database
	8 CPU Cores, 16GB RAM	12 CPU Cores, 24GB RAM	12 CPU Cores, 32GB RAM
1	5,000,000	7,500,000	5,000,000
2	5,000,000	15,000,000	10,000,000
3	5,000,000	15,000,000	20,000,000

To compute the number of CPU cores available on the workstation, the following command can be used:

```
# dmidecode | grep "Core Count" | /usr/bin/awk '{SUM += $3} END {print SUM}'
```

In situations where 5620 SAM is asked to collect more application assurance accounting records than it can process in the specified retrieval period, the extra statistics will not be retrieved from the network.

6.7.8 Exporting performance and accounting statistics records

There are two methods to export accounting and performance statistics from 5620 SAM; registerLogToFile, and findToFile. The registerLogToFile method is the preferred method and is required for situations where more than 400,000 accounting statistics records are retrieved in 15 minutes or 500,000 performance statistics are retrieved in 15 minutes. This recommendation also minimizes collection latency and reduces system load.

6.7.9 5620 SAM Database hardware platform requirements

To collect large numbers of statistics using the SAM Database, there are RAM and storage I/O requirements for the 5620 SAM Database workstation. The table below highlights these requirements.

Table 6-12 5620 SAM Database workstation hardware requirements for a distributed configuration

Maximum number of simultaneous statistics records per 15-minute interval			5620 SAM Auxiliary Statistics Collec-tor(s)	Requires the following 5620 SAM Database workstation setup
Accounting statistics records	Application Assurance accounting objects configured for collection	Performance statistics records		
400,000	0	0	No	4 CPU cores, minimum 2.4GHz 4 disks (RAID 0) 12 GB RAM
0	200,000	0		
0	0	150,000		
800,000	0	0	Yes	4 CPU cores, minimum 2.4GHz 4 disks (RAID 0) 16 GB RAM
0	400,000	0		
0	0	200,000		
10,000,000	0	500,000	Yes	8 CPU cores, minimum 2.4GHz 6 disks (RAID 0) 32 GB RAM
0	5,000,000	500,000		
10,000,000	5,000,000	2,000,000	Yes	12 CPU cores, minimum 2.4GHz 6 disks (RAID 0) 64 GB RAM
0	15,000,000	0		

6.7.10 Simultaneous collection of performance, applications assurance accounting and accounting statistics records

5620 SAM can collect performance, application assurance, and accounting statistics records simultaneously. However, it is important to consider that enabling the collection of one type of statistics will reduce the capability of 5620 SAM to collect and process the other type of statistics. It is therefore not possible to achieve the maximum stated limits for performance, application assurance, and accounting statistics records simultaneously, in certain configurations. Table 6-12, “5620 SAM Database workstation hardware requirements for a distributed configuration” (p. 82) shows an example of simultaneous collection.

6.7.11 Determining the number of performance and accounting statistics records being collected by 5620 SAM

To ensure the number of performance and accounting statistics records that 5620 SAM is asked to collect and process every 15 minutes remains below the stated scalability guidelines, it is important to carefully assess the impact of creating and assigning statistics policies. Review the number of objects that are assigned to statistics policies and ensure the polling and retrieval periods are set such that the numbers will remain below the stated guidelines.

Using SAM Server Performance Statistics, 5620 SAM can assist in determining how many polled and accounting statistics are being collected.

5620 SAM performance can be adversely affected by increasing the number of historical statistics entries recorded by the 5620 SAM. 5620 SAM system impacts include increased time listing log records from the GUI and OSS clients, increased Oracle tablespaces, and increased database backups times.

6.7.12 Statistics record retention

The table below shows the different retention rates that are achievable depending upon the collection rate and statistic type.

Table 6-13 Maximum statistics interval retention - SAM Database

Statistics Type	Total Number of statistics records to be stored in the Database	Maximum number of retention intervals
Performance	<40M	672
	>40M	96
Accounting	<40M	672
	>40M	16

Table 6-14 Maximum statistics interval retention - Auxiliary Database

Statistics Type	Total Number of statistics records to be stored in the Database	Maximum number of retention intervals
Performance	<5,376M	35,040
	>5,376M	1,344
Accounting	<80,640M	35,040
	>80,640M	1,344

When using the logToFile method only, for collection, the maximum retention of data on the file system is 600 minutes (10 hours).

Scaling guidelines for scheduled tests (STM)

6.8 Scaling guidelines for scheduled tests (STM)

6.8.1 Scaling guidelines for scheduled tests (STM)

5620 SAM provides the ability to generate, manage and schedule STM tests within the network. This section provides guidelines that can be used to determine the extent to which STM tests can be scheduled and launched within a network.

There are a number of factors which will influence 5620 SAM's ability to concurrently manage and schedule a large number of tests. 5620 SAM keeps track of how many tests are running concurrently. This is to limit the initiation of the tests, and the processing of the results without interfering with the system's other functions.

To understand the STM guidelines, the following terminology is required:

Elemental Test: An OAM test to be sent to a router such as an LSP ping

Elemental Test Result: An OAM test result received from a network element

Accounting file Test: An OAM test that is initiated in the default manner, however, the test results are retrieved from the network element via FTP on a periodic basis.

Test Policy: A definition or configuration that tells 5620 SAM the specifics about how to generate a test. A test policy can contain multiple test definitions. The policies are used by test suites.

Test Suite: A collection of elemental tests that can be assigned to a specific schedule. There are three defined sections in which tests can be placed within a test suite: First run, Generated and Last run. The tests are executed in order by these sections. It is possible to configure the execution order of tests within the First Run and Last Run sections to be parallel or sequential. The tests in the Generated position are run by the system as concurrently as possible. If the Generated section contains tests from several different test definitions, then all the tests belonging to one definition will be executed before the tests of the next definition begin. Within a definition, the system will attempt to execute the tests as concurrently as possible. This is important to note, as a test suite containing a large number of tests in the Generated section (or in the First Run/Last Run sections set to parallel) may tax the system. Part of the increased stress placed on the system by concurrent tests is a result of the need for the system to use greater amounts of resources in order to initiate, wait for and process many tests concurrently. As well, tests that result in a large amount data to be returned from the routers will place increased demands on the 5620 SAM.

Schedule: A start time that can have a test suite or test suites assigned to it to produce scheduled tasks. When the schedule's start time is reached, the suite or suites assigned to it will commence. The schedule may be set to continuously repeat after a configurable period of time.

Scheduled Task: An instance of a test suite assigned to a schedule

Non -NE Schedulable STM Tests: 5620 SAM provides the ability to execute and process results for non NE schedulable tests. Non NE schedulable tests are elemental tests which are not persistently defined on network elements; rather, these tests are defined/configured from 5620 SAM per test execution. Elemental test results from non-NE schedulable tests are always regular (SNMP mediated) and share the same scale limits/considerations as regular scheduled STM tests.

Table 6-15 Maximum number of STM elemental test results

5620 SAM platform	Maximum regular STM elemental test results (SNMP mediated schedulable/ non-NE schedulable) in a 15 minute period	Maximum accounting file STM elemental test results in a 15 minute period with results stored in the SAM Database or SAM Database and using logToFile	Maximum accounting file STM elemental test results in a 15 minute period using logToFile only
Distributed 5620 SAM Configuration with minimum 8 CPU Core 5620 SAM Server	15,000	1,500,000 [1]	1,500,000 [1]
Distributed 5620 SAM Configuration NOTE: It may be possible to achieve higher numbers depending on the 5620 SAM Server activity and hardware platform	6,000	22,500	60,000
Minimum Supported Collocated 5620 SAM configuration NOTE: It may be possible to achieve higher numbers depending on the 5620 SAM Server activity and hardware platform	3,000	1,500	15,000

Notes:

1. may require a dedicated disk or striped disks for the xml_output partition

6.8.2 Guidelines for maximizing STM test execution:

By default, 5620 SAM will only allow test suites with a combined weight of 80,000 to execute concurrently. The test suite weights are identified in the 5620 SAM GUI's Test Suites List window. Running too many tests that start at the same time will cause the system to exceed the previously mentioned limit, and the test will be skipped. Ensuring the successful execution of as many STM tests as possible requires planning the schedules, the contents, and the configuration of the test suites. The following guidelines will assist in maximizing the number of tests that can be executed on your system:

- When configuring Tests or Test Policies, do not configure more packets (probes) than necessary, as they increase the weight of the Test Suite.
- Test Suite's with a smaller weight will typically complete more quickly, and allow other test suites to execute concurrently. The weight of the test suite is determined by the number of tests in the test suite, and the number of probes that are executed by each test. See Table 6-16, "OAM test weight" (p. 86) for test weight per test type.
- Assign the time-out of the test suite in such a way that if one of the test results has not been received it can be considered missed or failed without stopping other test suites from executing.
- Rather than scheduling a Test Suite to execute all tests on one network element, tests should be executed on multiple network elements to allow for concurrent handling of the tests on the network elements. This will allow the test suite results to be received from the network element and processed by 5620 SAM more quickly freeing up available system weight more quickly.
- Rather than scheduling a test suite to run sequentially, consider duplicating the test suite and running the test suites on alternating schedules. This allows each test suite time to complete or

time-out before the same test suite is executed again. Remember that this may cause double the system weight to be consumed until the alternate test suite has completed.

- Create test suites that contain less than 200 elemental tests. This way you can initiate the tests at different times by assigning the test suites to different schedules thereby having greater control over how many tests are initiated or in progress at any given time.
- Prioritize which tests you wish to perform by manually executing the test suite to determine how long it will take in your network. Use that duration with some added buffer time to help determine how much time to leave between schedules or repetitions of a schedule and how to configure the test suite time-out.
- A test suite time-out needs to be configured to take effect before the same test suite is scheduled to run again, or it will not execute if it does not complete before the time-out.
- 5620 SAM Database backups can impact the performance of STM tests.

Table 6-16 OAM test weight

Test Type	Weight
Regular Elemental STM Test	10 per Test Packet
Accounting File Elemental STM Test	1

6.8.3 Accounting file STM test configuration

In 5620 SAM Release 7.0 R4, the concept of accounting file collection of STM test results was introduced. This feature requires 7750 and 7450 network elements that are version 7.0 R4 and above. To take advantage of accounting file STM test execution, the test policy must be configured to be NE schedulable with “Accounting file” selected. This will produce STM tests that will be executed on the network element, while the test results are collected by the 5620 SAM Server by way of an accounting file in a similar way to accounting Statistics. Accounting file STM test results are collected by the 5620 SAM Server only.

5620 SAM supports the use of logToFile for file accounting STM results. When using this method only for results, the number of tests that can be executed per 15 minute interval is increased. Refer to Table 6-15, “Maximum number of STM elemental test results” (p. 85) for specific scaling limits. The logToFile method for file accounting STM results supports a maximum of two JMS clients.

6.8.4 Examples of STM test configuration

The following examples describe the configuration of STM tests on different network configurations.

6.8.5 Example 1

Assume there is a network with 400 LSPs and that the objective is to perform LSP pings on each LSP as frequently as possible. The following steps are to be followed:

1. Create 4 test suites each containing 100 elemental LSP ping tests
2. One at a time, execute each test suite and record the time each one took to complete. Assume that the longest time for executing one of the test suites is 5 minutes.
3. Create a schedule that is ongoing and has a frequency of 15 minutes. This doubles the time

taken for the longest test suite and ensures that the test will complete before it is executed again. Assign this schedule to the 4 test suites.

4. Monitor the test suite results to ensure that they are completing. If the tests are not completing (for example getting marked as “skipped”), then increase the frequency time value of the schedule.
5. In the above case, there are 200 elemental tests configured to be executed each 10 minutes.

6.8.6 Example 2

Assume there are eight test suites (T1, T2, T3, T4, T5, T6, T7 and T8), each containing 50 elemental tests. Assume the test suites individually take 5 minutes to run. Also, assume the objective is to schedule them so that the guideline of having less than 200 concurrently running elemental tests is respected.

The recommended approach for scheduling these tests suites is as follows:

- Test suites T1, T2, T3, T4 can be scheduled on the hour and repeat every 10 minutes
- Test suites T5, T6, T7, T8 can be scheduled on the hour + 5 minutes and repeated every 10 minutes

This will ensure no more than 200 elemental tests are scheduled to run concurrently.

6.8.7 Factors impacting the number of elemental tests that can be executed in a given time frame

The following factors can impact the number of elemental tests that can be executed during a given time frame:

- The type of tests being executed. Each type of elemental test takes varying quantities of time to complete (e.g. a simple LSP ping of an LSP that spans only two routers may take less than 2 seconds; an MTU ping could take many minutes).
- The amount of data that is generated/updated by the test within the network elements. 5620 SAM will have to obtain this information and store it in the 5620 SAM database. The quantity of data depends on the type of tests being performed and the configuration of the objects on which the tests are performed.
- The number of test suites scheduled at or around the same time
- The number of tests in a test suite
- The number of routers over which the tests are being executed. Generally, a large number of tests on a single router can be expected to take longer than the same number of tests distributed over many routers.
- A 5620 SAM Database backup may temporarily reduce the system’s ability to write test results into the database.
- The workstation used to perform the tests will dictate how many physical resources 5620 SAM can dedicate to executing elemental tests. On the minimum supported workstation (collocated 5620 SAM Server and 5620 SAM Database on a single Server), the number of concurrent tests must be limited to 3,000.

6.8.8 Possible consequences of exceeding the capacity of the system to perform tests

5620 SAM will exhibit the following symptoms if the number of scheduled tests exceeds the system's capacity.

6.8.9 Skipped Tests:

If a test suite is still in progress at the time that its Schedule triggers again, then that scheduled task will be marked as skipped and that test suite will not be attempted again until the next scheduled time.

6.8.10 Failed tests (time-out):

Tests may time-out and get marked as failed. If any of the tests take more than 15 minutes it may get purged from an internal current test list. For example, a test may be successfully sent to a router and the system does not receive any results for 15 minutes. The system marks the test as failed and purges its' expectation of receiving a result. However, later, the system could still receive the results from the router and update its result for the test to success.

6.8.11 Disk space requirements for STM test results

STM test results are stored in the tablespace DB partition. The STM database partitions start with a total size of 300MB of disk space. When the maximum number of test results is configured at 20,000,000 (maximum), the disk space requirement for the STM tests may increase by up to 80GB. A larger tablespace partition should be considered.

The maximum number of test results stored in the database reflects the sum of the aggregate results, test results, and probe results.

Running 10 tests with 1 probe each versus 1 test with 10 probes consumes the same amount of disk space.

When using logToFile for accounting file STM test results, the maximum time-to-live on the disk is 24 hours. At the maximum collection rate of 1,500,000 test results per 15 minutes, the storage requirements on the 5620 SAM Server in the xml_output directory is 600GB per JMS client. The storage requirements are doubled if using the maximum number of JMS clients for file accounting STM results. The disk storage requirements can be decreased by using the compress option for logToFile but will result in increased CPU utilization on the SAM Server.

Scaling guidelines for Cflowd statistics collection

6.9 Scaling guidelines for Cflowd statistics collection

6.9.1 Scaling guidelines for Cflowd statistics collection

The table below shows the scaling limits for a 5620 SAM Cflowd Auxiliary in its ability to process cflowd flow records from the network and produce IPDR formatted files. The guidelines are divided into the 5620 SAM Cflowd Auxiliary collecting in a Residential/Mobile deployment and the 5620 SAM Cflowd Auxiliary collecting in a Business deployment.

For Residential and Mobile deployments, the only statistics types that should be in use are Volume, Comprehensive, Unknown and corresponding Special Study types. TCP and RTP are not supported in Mobile, and although the statistics types are available for Residential deployments, the use case is not, and there are no reports for this data. Additionally, even for Residential, the only reports available are for Comprehensive. Comprehensive statistics have a fixed 60min aggregation interval. Due to the amount of data generated in a Mobile deployment, Volume statistics require an aggregation interval of 60 minutes. As an alternative, Volume Special Study statistics on specific subscribers can be used. The only key factor of difference is whether or not additional counters are enabled for Comprehensive statistics.

Table 6-17 cflowd statistics scaling limits for residential and mobile deployments

5620 SAM Cflowd Auxiliary processing rate in flows per second	Counter Selection [1]	Maximum number of unique objects in memory [2]	Packet Loss per Hour [3]
100,000 FPS	Default two counters	100M Objects	<= 2%
	All counters	60M Objects	<= 1%

Notes:

1. Default: two counters. Volume: total bytes/total packets. Comp-volume: total bytes StoC/CtoS sum unknown. Only one counter exists. Vol SS: should be minuscule. All counters: Comp-volume has a total of ten counters that can be enabled.
2. Number of aggregated output requests that are sent to the server every 60 minutes. Assumes transfer has sufficient bandwidth to complete in a timely manner.
3. Packet loss may increase if communication between the 5620 SAM Cflowd Aux and target file server is interrupted.

For Business deployments, in addition to the statistics types with a small number of records; Comprehensive, Volume, Unknown, and Volume Special Study, there are also statistics types with a larger number of records; TCP Performance, and RTP (Voice/Audio/Video). The main distinction is whether or not the TCP/RTP statistics types use the default enabled counters, or if all counters have been enabled. Enabling all of the TCP/RTP counters increases the amount of memory used by the 5620 SAM Cflowd Auxiliary. Aside from the incoming FPS (Flows Per Second) that the 5620 SAM Cflowd Auxiliary can process, the other main factor putting pressure on the 5620 SAM Cflowd Auxiliary is the memory used by the number of unique objects/records (or unique routes, i.e. the # of output records the 5620 SAM Cflowd Auxiliary produces in the IPDR files) in 5620 SAM Cflowd Auxiliary memory at any one time. And finally the interval size – the smaller the aggregation

interval, the greater percentage of the next interval time will overlap with the transfer time of the previous interval – during this time the 5620 SAM Cflowd Auxiliary must store objects in memory from two different intervals. Comprehensive statistics types are fixed at 60 minute intervals.

A unique object/route for TCP/Volume records in the business context is:

SAP, App/AppGroup, Interval ID, Src Group ID, Source Interface ID, Dest Group ID, Dest Interface ID

A Volume record will also have a direction field. Volume records coming from the router to the 5620 SAM Cflowd Auxiliary will result in two output records in the IPDR files (one for each direction). For TCP, two incoming records from the 5620 SAM Cflowd Auxiliary (one for each direction) will be combined by the 5620 SAM Cflowd Auxiliary into a single output TCP record in the IPDR files.

A unique object/route for COMPREHENSIVE record in the business context is:

SAP, App/AppGroup, Interval ID, Src Group ID, Source Interface ID, Dest Group ID, Dest Interface ID

and either a hostname field, or three device identification fields.

A unique object/route for RTP is defined as:

Every single flow into the 5620 SAM Cflowd Auxiliary is a unique route and an equal number of flow records are produced in the IPDR file. The expected number of RTP records sent from 7750 SR Routers is expected to be a small percentage of the total flows (i.e. <5% total flows TCP/VOL/RTP)

Table 6-18 cflowd statistics scaling limits for Business deployments

5620 SAM Cflowd auxiliary processing rate in flows per second	Statistic types used and counters used [1]	Maximum number of unique objects in Memory [2]	Packet Loss per Hour [3]
100,000 FPS	Comprehensive/Volume/ Unknown/Vol S.S Only All Counters	60M objects	<= 1%
	TCP/TCP S.S Only: Default Counter	25M objects	<= 1%
	TCP/TCP S.S Only: All Counters	15M objects	<= 1%
	RTP Only: Default Counters	10M objects	<= 1%
	RTP Only: All Counters	3M objects	<= 1%
	Combined Comprehensive/Volume/ Unknown/TCP/RTP (including Special Study)	20M Comp/Volume/ Unknown + 5M TCP (All Cnt) + 0.5 RTP (All Cnt)	<= 1%

Notes:

1. Comprehensive/Volume/ Unknown/Volume SS: All Counters RTP/TCP/TCP S.S Counter Selection Default Counters: Leaving default enabled counters on All Counters: Enabling all available counters for given stat type. There are 40-60 total counters available for TCP and RTP types.
2. Number of aggregated output requisitions that are sent to the server every 60 seconds. Assumes transfer has sufficient bandwidth to complete in a timely manner.
3. Packet loss may increase if communication between the 5620 SAM Cflowd Aux and target file server is interrupted

Scaling guidelines for PCMD collection

6.10 Scaling guidelines for PCMD collection

6.10.1 Scaling guidelines for PCMD collection

LTE management networks support the collection of per call measurement data (PCMD) from SGW, PGW, and ePDG network elements when using the Auxiliary PCMD Collector. A single Auxiliary PCMD Collector can process up to 18 million records per minute where multiple Auxiliary PCMD Collectors can be deployed to increase overall scaling limits. The scaling limits for a single Auxiliary PCMD Collector represents approximately 10M Bearers.

7 Security

7.1 Overview

7.1.1 Purpose

This chapter provides general information about platform security for the 5620 SAM

7.1.2 Contents

7.2 Securing 5620 SAM

7.2.1 Securing 5620 SAM

Nokia recognizes the importance of deploying important software such as the 5620 SAM in secure environments and, as such, supports the use of security techniques to enhance the security of the 5620 SAM.

5620 SAM communications can be secured using SSL/TLS, SNMPv3 and HTTPS. See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for configuration information.

Nokia recommends the following steps to achieving 5620 SAM workstation security:

- Install a clean operating system environment with the minimum required packages documented in the *5620 SAM | 5650 CPAM Installation and Upgrade Guide*
- Install the latest Recommended Patch Cluster from Red Hat (available at www.redhat.com)
- If installing RHEL, disable the mDNS Service.
- Implement firewall rules for 5620 SAM to control access to ports on 5620 SAM platforms as described in 7.6 “5620 SAM and firewalls” (p. 95)

- If installing RHEL, enable the RHEL firewall filter rules lists. See 7.9 “Firewall and NAT rules” (p. 108) for more details
- Installation of 5620 SAM with a secure configuration described in 7.4 “5620 SAM software installation” (p. 94)
- Network Element connection configuration as described in 7.5 “5620 SAM network element communication” (p. 95)
- If installing RHEL, configure 5620 SAM to run at runlevel 3 as opposed to the default runlevel 5

7.3 Operating system installation for 5620 SAM workstations

7.3.1 Operating system installation for 5620 SAM workstations

Nokia supports customers applying RHEL, or Windows patches provided by Red Hat, or Microsoft which will include security fixes as well as functional fixes. If a patch is found to be incompatible with 5620 SAM, the patch may need to be removed until a solution to the incompatibility is provided by Red Hat, Microsoft, or Nokia. Consult the *Nokia 5620 SAM Release 14.0 Release Notice* documents for up-to-date information about the recommended RHEL maintenance update and patch levels.

5620 SAM is supported on RHEL installed with the list of required RHEL Packages documented in the *5620 SAM | 5650 CPAM Installation and Upgrade Guide*. SELinux is not supported.

Additional efforts to secure the system could impact 5620 SAM's operation or future upgrades of the product. Customer's should perform some level of basic testing to validate additional platform hardening does not impact 5620 SAM's operation. The 5620 SAM Product Group makes no commitment to make 5620 SAM compatible with a customer's hardening requirements.

7.4 5620 SAM software installation

7.4.1 5620 SAM software installation

Nokia recommends the following steps when installing the 5620 SAM components:

- Configure the 5620 SAM Server IP validation during the 5620 SAM Database installation to ensure that only the specified IP address can communicate with the 5620 SAM database. This is documented in the *5620 SAM | 5650 CPAM Installation and Upgrade Guide*.
- Configure SSL for secure communication between the 5620 SAM server and 5620 SAM clients (OSS and UI) as documented in the *5620 SAM | 5650 CPAM Installation and Upgrade Guide*.

Nokia recommends the configuration (as documented in the *5620 SAM User Guide*) of the following options to secure communication with the 5620 SAM Client UI and 5620 SAM Client OSS interfaces:

- Password history count
- Password expiry periods
- Client time-outs
- Security statements
- Scope of command and Span of Control

- Client IP validation

7.5 5620 SAM network element communication

7.5.1 5620 SAM network element communication

The following configurations are documented in the *5620 SAM User Guide*, and help secure communication between the network elements and 5620 SAM server installations:

- SNMPv3
- SSH for remote access to the network elements
- SCP/SFTP for secure file transfer
- NETCONF

7.6 5620 SAM and firewalls

7.6.1 5620 SAM and firewalls

A firewall can be deployed to protect the 5620 SAM server from the managed network and to protect the server from the network hosting the 5620 SAM clients. The diagrams below illustrate this and show the communications services that are required through the firewalls. Installations of 5620 SAM can make use of the built in firewall using firewalld. Standalone Firewall products must not be collocated on servers hosting 5620 SAM components. Only the built-in RHEL firewall used to enable filter rules lists can be collocated with 5620 SAM components. See 7.9 “Firewall and NAT rules” (p. 108) for more details.

Some 5620 SAM operations require idle TCP ports to remain open for longer periods of time. Therefore, customer's using a firewall that closes idle TCP connections should adjust Operating System TCP keepalives to a value that ensures that the firewall will not close sockets in use by 5620 SAM.

For some of the network elements described in 5.16 “GNE, Nokia OmniSwitch, 9471 WMM, eNodeB, and DSC considerations” (p. 68) there is a requirement for the 5620 SAM GUI client to communicate directly with the network element using specialized configuration tools.

Figure 7-1 Firewalls and 5620 SAM standalone deployments

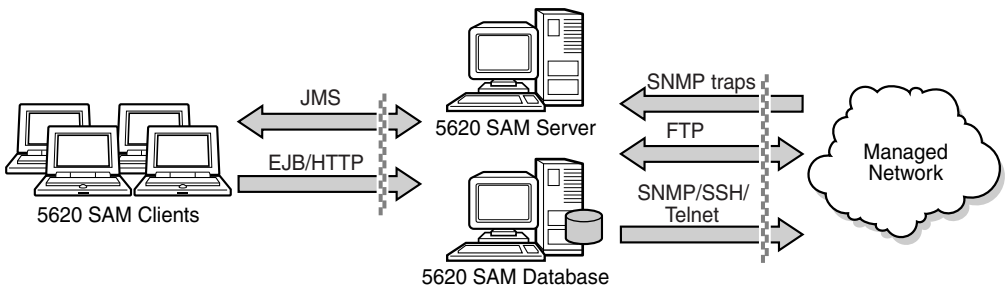
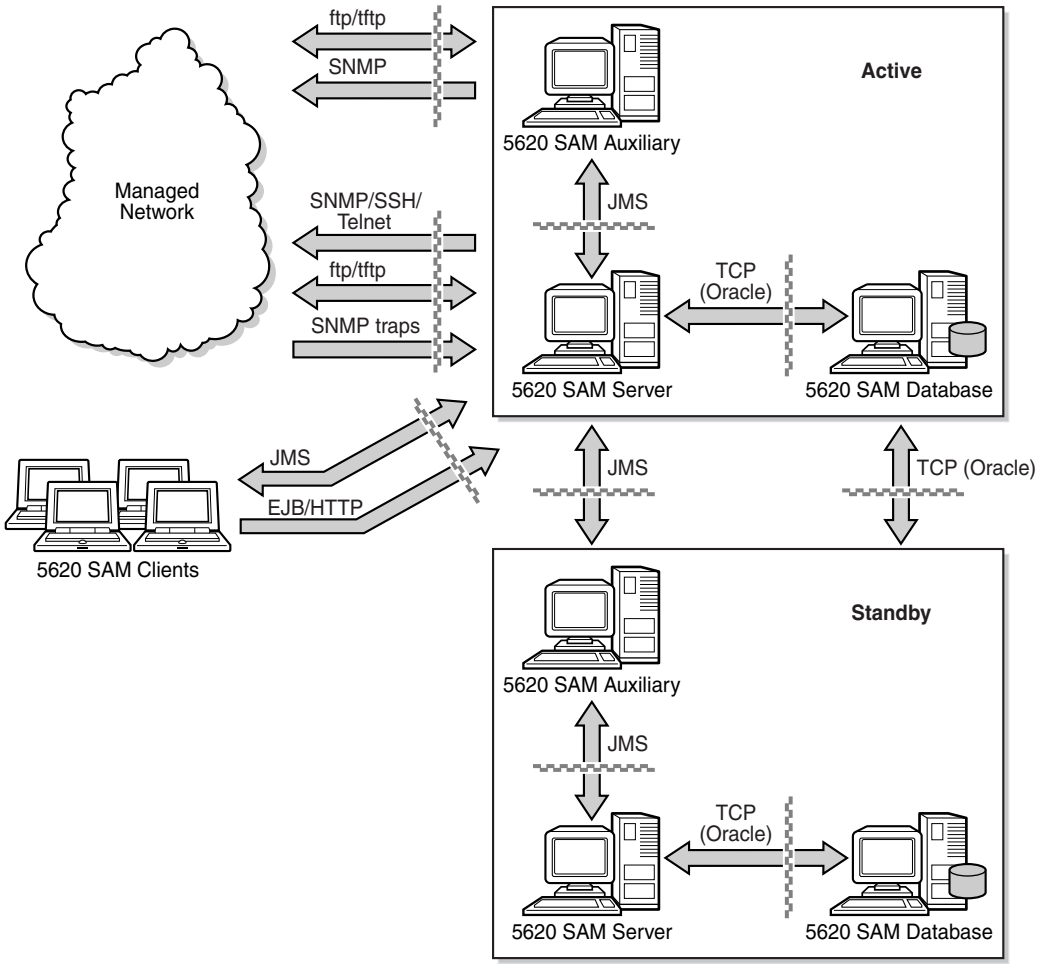


Figure 7-2 Firewalls and 5620 SAM redundant deployments



7.7 Port Information

7.7.1 Port Information

The following table describes the listening ports on the various 5620 SAM Applications.

Table 7-1 5620 SAM firewall requirements

Default port	Type	Encryption	Description
5620 SAM Server and 5620 SAM Auxiliary (Statistics, Call Trace, PCMD, and Femto)			

Table 7-1 5620 SAM firewall requirements (continued)

Default port	Type	Encryption	Description
N/A	ICMP	N/A	ICMP Ping The active 5620 SAM Server will periodically ping the 5620 SAM Delegate Server to ensure reachability.
21 Ports from 1023 - 65536	TCP	None. See SCP and SFTP as secure alternatives	FTP (Passive) This port is used to enable ftp communication from a 5620 SAM-O Client to either the 5620 SAM Server or Auxiliary. Ftp is used by the 5620 SAM-O Client to retrieve logToFile statistics or findToFile results. (See 7.8 "FTP between the 5620 SAM Server and 5620 SAM Auxiliary Statistics Collector and the managed network" (p. 107))
22	TCP	Dynamic Encryption Cipher Suite and strength as per RFC 4253	SSH/SCP/SFTP This port is used for remote access, rsync between 5620 SAM Servers, rsync between the 5620 SAM Databases, and scp/sftp to 5620 SAM OSS clients.
69	UDP	None.	TFTP This port is used to do ftp when managing 1830 PSS equipment. If there are none of these NEs in the network, this port is not required
80	TCP	None. See port 443/9400 for secure communications.	HTTP This port provides an HTTP interface for the User Documentation Server (InfoCenter) and Web Applications. Also provides a WebDav Server for snapshots and workorders.
162	UDP	Static Encryption When SNMPv3 is configured. Cipher and strength is NE dependant.	SNMP traps By default, this port on the 5620 SAM Server receives SNMP traps from the network elements. This item is specified during the installation of the server and can be changed. (Not required by the 5620 SAM Auxiliary)
443	TCP	Dynamic Encryption Encryption provided by SSL/TLS. Strong ciphers are supported. Selection of CBC and AES ciphers provided by TLS are supported.	HTTPS This port provides an HTTPS interface for the User Documentation Server (InfoCenter) and Web Applications. Also provides a WebDav Server for snapshots and workorders. This is a secure version of port 80/8400.
1095	TCP	None.	Internal system communications protocol (JBoss messaging) These ports are used by commands on the 5620 SAM Auxiliary workstation to adjust the 5620 SAM Auxiliary behaviour. (Example: adjusting log levels, shutting down the auxiliary server, etc)
1097	TCP	None.	Internal system communications protocol (JMS naming/messaging service) Used by the 5620 SAM Client (GUI and OSSI) and 5620 SAM Server and 5620 SAM Auxiliary applications to register for JMS notifications and messages. This is used to ensure that the Client, Server, and Auxiliary are aware of system events (i.e.: database changes or alarm notifications, etc)

Table 7-1 5620 SAM firewall requirements (continued)

Default port	Type	Encryption	Description
1099	TCP	None.	Internal system communications protocol (JBoss Naming Service -JNDI) This port is required to ensure the 5620 SAM GUI, OSS clients, Auxiliaries and standby SAM Server properly initialize with the active 5620 SAM Server. When initially logging into the 5620 SAM Server, 5620 SAM GUI and OSS clients use this port to find the various services that are available. This port is also used by the 5620 SAM GUI and OSS clients to register with the 5620 SAM Server to receive notification of network changes.
1998	TCP	None.	RMI Port for CNBI This is a local port to the host.
1999	TCP	None.	JNDI Port for CNBI This is a local port to the host.
3528	TCP	None.	Not used but open and listening This port can be blocked in the firewall
4273	TCP	None.	EJB3 invoker port for CNBI This is a local port to the host.
4447	TCP	Dynamic Encryption Encryption provided by SSL/TLS. Strong ciphers are supported. Selection of CBC and AES ciphers provided by TLS are supported.	JBoss messaging port for JMS
4846	TCP	None.	JBoss remoting connector port for CNBI This is a local port to the host.
5344	TCP	None.	RMI/JRMP invoker port for CNBI This is a local port to the host.
5345	TCP	None.	Pooled invoker port for CNBI This is a local port to the host.
6100-6119	UDP	None.	NEM Proxy Used to provide NEM eNodeB access from SAM Clients.
6362	UDP	None.	Neo4j database backup port This is a local port to the host.
6633	TCP	None.	OpenFlow Used to exchange openflow protocol messages with 7x50 NEs.
7474	TCP	None.	Neo4j This is a local port to the host. SAM Server only

Table 7-1 5620 SAM firewall requirements (continued)

Default port	Type	Encryption	Description
7879	TCP	Dynamic Encryption (if SSL is configured) Encryption provided by SSL/TLS. Strong ciphers are supported. Selection of CBC and AES ciphers provided by TLS are supported	RPC Layer Used for FM correlation engine to SAM Server communications. Used for CPROTO communication with the Cflowd Auxiliary
8080	TCP	None. See port 8443 for secure communications	HTTP This port provides an HTTP interface for 5620 SAM-O clients to access the 5620 SAM server.
8085	TCP	None. See port 8444 for secure communications.	HTTP This port provides an HTTP interface for 5620 SAM client. The 5620 SAM Client uses this port to verify the existence of the server.
8086	TCP	None. See port 8445 for secure communications.	HTTP This port provides an HTTP interface to the WebDav Server for WTA. This port is only required on the CallTrace Auxiliary.
8087	TCP	Dynamic Encryption Encryption provided by SSL/TLS. Strong ciphers are supported. Selection of CBC and AES ciphers provided by TLS are supported.	HTTP / HTTPS (if SSL is configured) Servlet connector used for communication between tomcat and SAM Server to handle requests with a normal processing time.
8088	TCP	Dynamic Encryption Encryption provided by SSL/TLS. Strong ciphers are supported. Selection of CBC and AES ciphers provided by TLS are supported.	HTTP / HTTPS (if SSL is configured) Webapp services such as correlation.
8089	TCP	Dynamic Encryption Encryption provided by SSL/TLS. Strong ciphers are supported. Selection of CBC and AES ciphers provided by TLS are supported.	HTTP / HTTPS (if SSL is configured) Servlet connector used for communication between tomcat and SAM Server to handle requests with a long processing time.
8400	TCP	None. See port 443/9400 for secure communications	HTTP This port provides an HTTP interface for the User Documentation Server (InfoCenter) and Web Applications. Also provides a WebDav Server for snapshots and workorders. This port re-directs to port 80.
8443	TCP	Dynamic Encryption Encryption provided by SSL/TLS. Strong ciphers are supported. Selection of CBC and AES ciphers provided by TLS are supported.	HTTPS This port provides an HTTPS (secure HTTP) interface for 5620 SAM-O clients that wish to use this protocol to access the 5620 SAM server

Table 7-1 5620 SAM firewall requirements (continued)

Default port	Type	Encryption	Description
8444	TCP	Dynamic Encryption Encryption provided by SSL/TLS. Strong ciphers are supported. Selection of CBC and AES ciphers provided by TLS are supported.	HTTPS This port provides an HTTPS (secure HTTP) interface for 5620 SAM Client. This is a secure version of port 8085. Used only if 5620 SAM Client is connecting via SSL.
8445	TCP	Dynamic Encryption Encryption provided by SSL/TLS. Strong ciphers are supported. Selection of CBC and AES ciphers provided by TLS are supported.	HTTPS This port provides an HTTPS (secure HTTP) interface to the WebDav Server for WTA. This is a secure version of port 8086. Used only if the WTA is connecting via SSL. This port is only required on the CallTrace Auxiliary.
8483	TCP	None.	JBoss RMI port for WebServices This is a local port to the host.
8889	TCP	None.	Notification port used by TAO (CORBA Notification) This is a local port to the host.
8980	TCP	None See port 9443 for secure communications.	HTTP This port provides an HTTP interface for 5620 SAM-O Clients to the WDSL 3GPP WebServices Integration Reference Points.
9010	TCP	None.	This port is used for file synchronization between redundant SAM Servers, redundant Auxiliary Collectors (Statistics and Call Trace), and between SAM Servers and SAM Femto Auxiliaries.
9400	TCP	Dynamic Encryption Encryption provided by SSL/TLS. Strong ciphers are supported. Selection of CBC and AES ciphers provided by TLS are supported.	HTTPS This port provides an HTTPS interface for the User Documentation Server (InfoCenter) and Web Applications. Also provides a WebDav Server for snapshots and workorders. This is a secure version of port 80/8400. This port re-directs to port 443.
9443	TCP	Dynamic Encryption Encryption provided by SSL/TLS. Strong ciphers are supported. Selection of CBC and AES ciphers provided by TLS are supported.	HTTPS This port provides an HTTPS (secure HTTP) interface for SAM-O clients to the WDSL 3GPP WebServices Integration Reference Points. This is a secure version of port 8980. Used only if 5620 SAM-O Clients are connecting via SSL.
9735	TCP	None.	Corba Interface This port is used by 5620 SAM-O 3GPP-compliant clients to access the 5620 SAM-O 3GPP Corba interface and for access to 3GPP CORBA Integration Reference Points
9736	TCP	None.	TAO Orb port This is a local port to the host.

Table 7-1 5620 SAM firewall requirements (continued)

Default port	Type	Encryption	Description
9990	TCP	Dynamic Encryption Encryption provided by SSL/TLS. Strong ciphers are supported. Selection of CBC and AES ciphers provided by TLS are supported	JBoss Management Console Used to access the JBoss management console for the main server process.
9999	TCP	Dynamic Encryption Encryption provided by SSL/TLS. Strong ciphers are supported. Selection of CBC and AES ciphers provided by TLS are supported	JMX Used to access the JMX console for the main server process.
10090	TCP	Dynamic Encryption Encryption provided by SSL/TLS. Strong ciphers are supported. Selection of CBC and AES ciphers provided by TLS are supported	JBoss Management Console Used to access the JBoss management console for the JMS server process.
10099	TCP	Dynamic Encryption Encryption provided by SSL/TLS. Strong ciphers are supported. Selection of CBC and AES ciphers provided by TLS are supported	JMX Used to access the JMX console for the JMS server process.
10190	TCP	Dynamic Encryption Encryption provided by SSL/TLS. Strong ciphers are supported. Selection of CBC and AES ciphers provided by TLS are supported	JBoss Management Console Used to access the JBoss management console for the auxiliary server process.
10199	TCP	Dynamic Encryption Encryption provided by SSL/TLS. Strong ciphers are supported. Selection of CBC and AES ciphers provided by TLS are supported	JMX Used to access the JMX console for the auxiliary server process.
11800 Ports from 32768 - 65536	TCP	Static Encryption Encryption provided by AES Cipher Algorithm with 128 bit Cipher Strength.	Internal system communications protocol (JBoss Clustering) This port is required to ensure that redundant 5620 SAM Servers can monitor each other.
12010	TCP	Dynamic Encryption Encryption provided by SSL/TLS. Strong ciphers are supported. Selection of CBC and AES ciphers provided by TLS are supported.	This port is used for Warm standby Cache Sync communication between redundant SAM Servers This port is not used on the 5620 SAM Auxiliary.

Table 7-1 5620 SAM firewall requirements (continued)

Default port	Type	Encryption	Description
12300 - 12307	TCP	None.	These ports are used for detecting communication failures between SAM server clusters (Primary / Secondary / Auxiliaries)
12800	TCP	Static Encryption Encryption provided by AES Cipher Algorithm with 128 bit Cipher Strength.	Internal system communications protocol (JBoss clustering) During run-time operations, the 5620 SAM Auxiliary use this port to send and receive information to and from the 5620 SAM Server. The number of required ports depends on the number of 5620 SAM Auxiliary workstations that are installed. Note that 5620 SAM can be configured to use a different port for this purpose. The procedure is available from Nokia personnel.
29780	UDP	None.	Used to stream UDP PCMD data from SGW and PGW Network Elements Auxiliary PCMD Collector only
5620 SAM Cflowd Auxiliary			
21 Ports from 1023 - 65536	TCP	None. See SCP and SFTP as secure alternatives	FTP (Passive) This port is used to enable ftp communication between the 5620 SAM DCP Server and the 5620 SAM Server or dedicated ftp server for retrieving IPDR files.
22	TCP	Dynamic Encryption Cipher Suite and strength as per RFC 4253	SSH/SCP/SFTP This port is used to enable SSH (SFTP/SCP) communication between the 5620 SAM DCP Server and the 5620 SAM Server or dedicated ftp server for retrieving IPDR files.
1090	TCP	None.	JBoss RMI/JRMP socket for connecting to the JMX MBeanServer. Used for 5620 SAM Server to Cflowd Aux communication.
1098	TCP	None.	JBoss Socket Naming service used to receive RMI request from client proxies. Used for 5620 SAM Server to Cflowd Aux communication.
1099	TCP	None.	JBoss The listening socket for the Naming service. Used for Jboss communication between 5620 SAM and Cflowd Aux.
4444	TCP	None.	JBoss Socket for the legacy RMI/JRMP invoker. Used for Jboss communication between 5620 SAM to Cflowd Aux.
4445	TCP	None.	JBoss Socket for the legacy Pooled invoker. Used for Jboss communication between 5620 SAM to Cflowd Aux.
4446	TCP	None.	JBoss Socket for the JBoss Remoting Connected used by Unified Invoker. Used for Jboss communication between 5620 SAM to Cflowd Aux.
4447	TCP	None.	JBoss Socket for JBoss Remoting Connections.
4457	TCP	Dynamic Encryption Encryption provided by SSL/TLS. Strong ciphers are supported. Selection of CBC and AES ciphers provided by TLS are supported.	JBoss Socket for JBoss Messaging 1.x

Table 7-1 5620 SAM firewall requirements (continued)

Default port	Type	Encryption	Description
7879	TCP	None.	CPROTO
8080	TCP	None. See port 8443 for secure communications.	HTTP This port provides an HTTP Web User interface for the 5620 Cflowd Aux
8083	TCP	None.	JBoss Socket for dynamic class and resource loading.
8443	TCP	Dynamic Encryption Encryption provided by SSL/TLS. Strong ciphers are supported. Selection of CBC and AES ciphers provided by TLS are supported.	HTTPS This port provides an HTTP Web User interface for the 5620 Cflowd Aux This is a secure version of port 8080.
9443	TCP	Dynamic Encryption Encryption provided by SSL/TLS. Strong ciphers are supported. Selection of CBC and AES ciphers provided by TLS are supported.	HTTPS This port provides an HTTPS (secure HTTP) 5620 SAM Cflowd Auxiliary Server management interface. This is a secure version of port 9990. Used only if the 5620 SAM Cflowd Auxiliary Server is SSL secured.
9990	TCP	None. See port 9443 for secure communications.	HTTP This port provides an HTTP 5620 SAM Cflowd Auxiliary Server management interface.
9999	TCP	Dynamic Encryption Encryption provided by SSL/TLS. Strong ciphers are supported. Selection of CBC and AES ciphers provided by TLS are supported.	JMX Used to access the JMX console.
5620 SAM Analytics Server			
8080	TCP	None. See port 8443 for secure communications.	HTTP This port provides an HTTP Web User interface for the 5620 SAM Analytics Server. It's used by the 5620 SAM Server and web based clients for HTTP requests.
8443	TCP	Dynamic Encryption Encryption provided by SSL/TLS. Strong ciphers are supported. Selection of CBC and AES ciphers provided by TLS are supported.	HTTPS This port provides a secure HTTP Web User interface for the 5620 SAM Analytics Server. It's used by the 5620 SAM Server and web based clients for HTTPS requests This is a secure version of port 8080.
5620 SAM Auxiliary Database			
22	TCP	Dynamic Encryption Cipher Suite and strength as per RFC 4253	SSH / SFTP Vertica Administration Tools. Inter-node cluster communication only.

Table 7-1 5620 SAM firewall requirements (continued)

Default port	Type	Encryption	Description
4803	TCP	None.	Spread Client connections Inter-node cluster communication only.
4803	UDP	None.	Spread Daemon to Daemon connections Inter-node cluster communication only.
4804	UDP	None.	Spread Daemon to Daemon connections Inter-node cluster communication only.
5433	TCP	None.	JDBC Client communication port (SAM Server, Statistics Auxiliary, Cflowd Auxiliary, Analytics Server)
5433	UDP	None.	Vertica Vertica spread monitoring Inter-node cluster communication only.
5434	TCP	None.	Vertica Intra and inter cluster communication Inter-node cluster communication only.
6543	TCP	None.	Spread Monitor to Daemon connections Inter-node cluster communication only.
7299–7309	TCP	None.	RMI Auxiliary Database proxy port.
Managed Devices			
21 Ports from 1023 - 65536	TCP	None.	FTP (Passive) This port is used to enable ftp communication between the 5620 SAM Server and the managed routers. Ftp occurs to transfer information from the routers to the 5620 SAM Server such as accounting statistics. See 7.8 “FTP between the 5620 SAM Server and 5620 SAM Auxiliary Statistics Collector and the managed network” (p. 107) for a more detailed description of ftp requirements.
22	TCP	Dynamic Encryption Cipher Suite and strength as per RFC 4253	SSH / SFTP This port used by clients to request a SSH session to a managed router. Used by eNodeBs to transfer software loads from the 5620 SAM Server.
23	TCP	None.	Telnet This port used by clients to request a telnet session to a managed router.

Table 7-1 5620 SAM firewall requirements (continued)

Default port	Type	Encryption	Description
80	TCP	None.	HTTP This port is required for the 5620 SAM Client to communicate with the network element Web GUIs. See 5.16 “GNE, Nokia OmniSwitch, 9471 WMM, eNodeB, and DSC considerations” (p. 68) for the network elements that require this port.
161	UDP	Static Encryption When SNMPv3 is configured. Cipher and strength is NE dependant.	SNMP By default, 5620 SAM server sends SNMP messages, such as configuration requests and service deployments, to this port on the network elements.
443	TCP	Dynamic Encryption Encryption provided by SSL/TLS. Strong ciphers are supported. Selection of CBC and AES ciphers provided by TLS are supported.	HTTPS This port is required for the 5620 SAM Client to be able to communicate with the DSC.
830	TCP	Dynamic Encryption Cipher Suite and strength as per RFC 4253	SSH for eNodeB / SSHv2 for MME This port is used by the eNodeB and MME network elements for NetConf management.
1099	TCP	None.	RMI This port is required for the 5620 SAM Client to be able to communicate with the 9471 MME MI.
1234	TCP	None.	Search-agent This port is required for the 5620 SAM Client to be able to communicate with the 9471 MME MI.
1235	TCP	None.	Mosaicsysscv1 This port is required for the 5620 SAM Client to be able to communicate with the 9471 MME MI.
1491	TCP	Static Encryption When SNMPv3 is configured. Cipher and strength is NE dependant.	SNMP Streaming Used for TCP Streaming during NE discovery and resync. Only applicable to 7950 XRS, 7750 SR, 7450 ESS, and 7710 SPR, 11.0R5+.
4567	TCP	None.	Tram This port is required for the 5620 SAM Client to be able to communicate with the 9471 MME MI.
5001	TCP	None.	Proprietary Java socket connection This port is used by CPAM to communicate with the 7701 CPAA to obtain control plane information.
5010	UDP	None.	Trap Trap port used by 9500 MPR devices to send traps to SAM Clients running the NetO manager.

Table 7-1 5620 SAM firewall requirements (continued)

Default port	Type	Encryption	Description
8001	UDP	Static Encryption When SNMPv3 is configured. Cipher and strength is NE dependant.	SNMP This port is used for SNMP communication with the 9471 MME MI
8443	TCP	Dynamic Encryption Encryption provided by SSL/TLS. Strong ciphers are supported. Selection of CBC and AES ciphers provided by TLS are supported.	HTTPS This port is required for the 5620 SAM Client to be able to communicate with the 9471 WMM MI.
9683	TCP	Dynamic Encryption Encryption provided by SSL/TLS. Strong ciphers are supported. Selection of CBC and AES ciphers provided by TLS are supported.	HTTPS This port is required for the 5620 SAM Client to be able to communicate with the 9471 WMM Provisioning GUI. NOTE: Only required when using 9471 MME 4.0 or older.
11500	TCP	None.	Equipment View Used while managing 9500 MPR (MSS-1C, MPR-e) NEs using the Equipment View function as part of NetO
N/A	ICMP	N/A	ICMP Only used if the Ping Policy is enabled as part of network element mediation.
5620 SAM Database			
22	TCP	Dynamic Encryption Cipher Suite and strength as per RFC 4253	SSH This port is used by 5620 SAM for an optional rsync feature between 5620 SAM Databases
1523	TCP	Static Encryption Encryption provided by RC4 Cipher Algorithm with 128 bit Cipher Strength.	Oracle SQL*Net Listener This port is used by the 5620 SAM Server to connect to and communicate with the 5620 SAM Database. When there are redundant databases, this port is also used by Oracle DataGuard to keep the databases in sync. The data on this port is encrypted.
9002	TCP	Dynamic Encryption Encryption provided by SSL/TLS. Strong ciphers are supported. Selection of CBC and AES ciphers provided by TLS are supported.	5620 SAM Database Proxy This port is used by the 5620 SAM Server to monitor disk usage on a remote 5620 SAM Database. When there are redundant databases, it is also allows the 5620 SAM Server to initiate database switchovers and failovers.
9003	TCP	None.	Database file transfer Port This port is used by the 5620 SAM Database workstations in a redundant workstation configuration. This port allows Database transfers between the primary and standby databases. For example: when the standby database is re-instantiated, or when the standby database is installed for the first time.
5620 SAM Client and Client Delegate			

Table 7-1 5620 SAM firewall requirements (continued)

Default port	Type	Encryption	Description
20	TCP	None.	FTP Active FTP port for 9500 MPR software download from NEtO.
21 Ports from 1023 - 65535	TCP	None.	FTP 9500 MPR software download from NEtO.
22	TCP	Dynamic Encryption Cipher Suite and strength as per RFC 4253	sFTP 9500 MPR software download from NEtO
162	UDP	None.	Trap Trap port used by 9500 MPR (MPR-e) devices to send traps to 5620 SAM Clients running the NetO manager.
5010	UDP	None.	Trap Trap port used by 9500 MPR devices to send traps to 5620 SAM Clients running the NetO manager.

7.8 FTP between the 5620 SAM Server and 5620 SAM Auxiliary Statistics Collector and the managed network

7.8.1 FTP between the 5620 SAM Server and 5620 SAM Auxiliary Statistics Collector and the managed network

5620 SAM Server and 5620 SAM Auxiliary Statistics Collector will use FTP for several purposes.

The 5620 SAM Server will use FTP to receive backup images of managed devices, to send new software images to the managed devices and to receive accounting statistics from the managed devices.

If a 5620 SAM Auxiliary Statistics Collector workstation is installed, FTP will only be used to retrieve accounting statistics from managed devices.

If STM Accounting tests are being executed, the 5620 SAM Server will retrieve the test results from the managed devices by FTP.

The FTP communication is configured as an extended *passive* FTP connection, with the managed devices serving as the FTP servers and the 5620 SAM Server and 5620 SAM Auxiliary acting as the FTP client.

Extended passive FTP connections use dynamically-allocated ports on both sides of the communication channel, and are ephemeral in nature. As such, the data sent from the managed devices will be sent from a port in the range of 1024-65536. This data will be sent to the 5620 SAM Server on a port in the range of 1024-65536. Support for EPSV/EPRT ftp commands (commands that can replace PASV/PORT commands) must be enabled for connections to the 7x50 family of routers.

7.9 Firewall and NAT rules

7.9.1 Firewall and NAT rules

Firewall rules are applied to the incoming network interface traffic of the 5620 SAM workstations. As a rule, firewall rules are not applied to the outgoing network interface traffic.

For 5620 SAM installations using RHEL as the Operating System, the RHEL supplied firewall can be used to filter network traffic using filter rules lists. Only experienced system administrators with extensive knowledge of the RHEL firewall should attempt to implement the filter rules lists provided with each 5620 SAM component. All others should disable the RHEL firewall.

The installation of each 5620 SAM component will include the filter rules lists to be applied for successful communication between different 5620 SAM components, OSS Clients, and Network Elements. The table below defines the location

Table 7-2 Sample firewalld filter rules lists file locations

SAM Component	Protocol	File Location
SAM Server	IPv4 / IPv6	/opt/5620sam/server/nms/sample/firewall/
SAM Database	IPv4 / IPv6	/opt/5620sam/samdb/install/sample/firewall/
Statistics/Femto Auxiliary	IPv4 / IPv6	/opt/5620sam/auxserver/nms/sample/firewall/
SAM Client	IPv4 / IPv6	<base client install dir>/nms/sample/firewall/
SAM Client Delegate	IPv4 / IPv6	<base client install dir>/nms/sample/firewall/

It is imperative that all rules are considered completely for the 5620 SAM systems to inter-operate correctly. The following tables will define the rules to be applied to each 5620 SAM workstation. Within the section there will be a number of conditions that indicate whether or not that particular table needs to be applied.

See 8.8 “Using Network Address Translation” (p. 134) for supported NAT configurations.

7.9.2 5620 SAM server firewall and NAT rules

When there is a firewall at the 5620 SAM Server(s) interface that reaches the managed network (NIC 2 on Figure 8-2, “Distributed 5620 SAM Server/Database deployment with multiple network interfaces” (p. 129)), the following firewall rules need to be applied.

Table 7-3 SNMP Firewall rules for traffic between the 5620 SAM Server(s) and the managed network

Protocol	From port	On	To port	On	Notes
UDP	Any	Managed Network	162	Server(s)	SNMP trap initiated from the NE
UDP	>32768	Server(s)	161	Managed Network	SNMP request
UDP	Any	Server(s)	8001	Managed Network	SNMP for 9471 WMM
UDP	161	Managed Network	> 32768	Server(s)	SNMP response

Table 7-3 SNMP Firewall rules for traffic between the 5620 SAM Server(s) and the managed network (continued)

Protocol	From port	On	To port	On	Notes
TCP	>32768	Server(s)	1491	Managed Network	SNMP TCP Streaming
TCP	1491	Managed Network	> 32768	Server(s)	SNMP TCP Streaming
TCP	>32768	Managed Network	6633	Server(s)	OpenFlow
TCP	6633	Server(s)	> 32768	Managed Network	OpenFlow

Note: Due to the size of SNMP packets, IP fragmentation may occur in the network. Ensure the firewall will allow fragmented packets to reach the server(s).

Table 7-4 Telnet / FTP Firewall rules for traffic between the 5620 SAM Server(s) and the managed network

Protocol	From port	On	To port	On	Notes
TCP	>32768	Server(s)	23	Managed Network	Telnet request
TCP	23	Managed Network	> 32768	Server(s)	Telnet response
TCP	Any	Server(s)	21	Managed Network	FTP requests (example: STM, Accounting Statistics, NE backups)
TCP	21	Managed Network	Any	Server(s)	FTP responses
TCP	> 1023	Managed Network	> 1023	Server(s)	Passive FTP ports for data transfer

Table 7-5 SSH / SFTP / SCP Firewall rules for traffic between the 5620 SAM Server(s) and the managed network

Protocol	From port	On	To port	On	Notes
TCP	Any	Server(s)	22	Managed Network	SAM SSH request
TCP	22	Managed Network	Any	Server(s)	SAM SSH response
TCP	Any	Managed Network	22	Server(s)	eNodeB and 1830 PSS SFTP request
TCP	22	Server(s)	Any	Managed Network	eNodeB and 1830 PSS SFTP response
TCP	> 32768	Server(s)	830	Managed Network	SSH request for eNodeB
TCP	830	Managed Network	> 32768	Server(s)	SSH response for eNodeB
TCP	> 32768	Server(s)	830	Managed Network	SSHv2 request for MME
TCP	830	Managed Network	> 32768	Server(s)	SSHv2 response for MME

Table 7-6 1830 Firewall rules for traffic between the 5620 SAM Server(s) and the managed network

Protocol	From port	On	To port	On	Notes
UDP	Any	1830	69	Server(s)	TFTP initiated by NE
UDP	Any	1830	Any	Server(s)	TFTP transfer

Table 7-7 Other Firewall rules for traffic between the 5620 SAM Server(s) and the managed network

Protocol	From port	On	To port	On	Notes
ICMP	N/A	Managed Network	N/A	Server(s)	Only used if Ping Policy is enabled.
TCP	5001	7701 CPAA Elements	> 32768	Server(s)	–

Table 7-8 Firewall rules for remote user authentication

Protocol	From port	On	To port	On	Notes
TCP/UDP	Any	SAM Server	389	LDAP Server	For LDAP authentication
TCP/UDP	Any	SAM Server	636	LDAP Server	For LDAP authentication (SSL)
UDP	Any	SAM Server	1812	RADIUS Server	For RADIUS authentication

When there is a firewall at the interface that reaches the 5620 SAM Client(s) (NIC 3 on Figure 8-2, “Distributed 5620 SAM Server/Database deployment with multiple network interfaces” (p. 129)) the following rules need to be applied.

Table 7-9 Firewall rules for traffic coming into the 5620 SAM Server(s) from the 5620 SAM Client(s) (GUI/OSS)

Protocol	From port	On	To port	On	Notes
TCP	Any	SAM-O Client	21	Server(s)	If FTP is required
TCP	Any	SAM-O Client	22	Server(s)	If SFTP/SCP is required
TCP	> 1023	SAM-O Client	> 1023	Server(s)	If (passive) FTP is required
TCP	Any	SAM-O/SAM GUI Client	1097	Server(s)	JMS
TCP	Any	SAM-O/SAM GUI Client	1099	Server(s)	JNDI
TCP	Any	SAM-O/SAM GUI Client	4447	Server(s)	JMS
UDP	Any	SAM GUI Client	6100-6119	Server(s)	NEM Proxy
TCP	Any	SAM-O Client	8080	Server(s)	HTTP
TCP	Any	SAM GUI Client	8085	Server(s)	HTTP
TCP	Any	SAM GUI Client	8087	Server(s)	HTTP(S)

Table 7-9 Firewall rules for traffic coming into the 5620 SAM Server(s) from the 5620 SAM Client(s) (GUI/OSS) (continued)

Protocol	From port	On	To port	On	Notes
TCP	Any	SAM GUI Client	8088	Server(s)	HTTP(S)
TCP	Any	SAM GUI Client	8089	Server(s)	HTTP(S)
TCP	Any	SAM GUI Client	80	Server(s)	HTTP
TCP	Any	SAM-O Client	8443	Server(s)	HTTPS
TCP	Any	SAM GUI Client	8444	Server(s)	HTTPS
TCP	Any	SAM-O Client	8980	Server(s)	HTTP
TCP	Any	SAM GUI Client	443	Server(s)	HTTPS
TCP	Any	SAM-O Client	9443	Server(s)	HTTPS
TCP	Any	SAM-O 3GPP-compliant Client	9735	Server(s)	Corba

When there is a firewall configured, and there are redundant 5620 SAM Auxiliary workstation(s), the following rules need to be applied to the appropriate interface.

Table 7-10 Firewall rules for traffic coming into the 5620 SAM Server(s) from the 5620 SAM Auxiliary Statistics / Call Trace / PCMD / Femto Server(s)

Protocol	From port	On	To port	On
TCP	Any	Auxiliary Server(s)	1097	Server(s)
TCP	Any	Auxiliary Server(s)	1099	Server(s)
TCP	Any	Auxiliary Server(s)	4447	Server(s)
TCP	Any	Femto Auxiliary Server(s)	9010	Server(s)

Table 7-11 Firewall rules for traffic coming into the 5620 SAM Server(s) from the 5620 SAM Auxiliary Cflowd Server(s)

Protocol	From port	On	To port	On
TCP	Any	Auxiliary Server(s)	21	Server(s)
TCP	Any	Auxiliary Server(s)	22	Server(s)
TCP	>1023	Auxiliary Server(s)	>1023	Server(s)
TCP	Any	Auxiliary Server(s)	1099	Server(s)
TCP	Any	Auxiliary Server(s)	7879	Server(s)
TCP	Any	Auxiliary Server(s)	8080/8443	Server(s)

When a firewall and NAT are configured to the 5620 SAM Server at the SAM client interface (NIC 3 on Figure 8-2, “Distributed 5620 SAM Server/Database deployment with multiple network

interfaces" (p. 129)) the following rules need to be applied to allow the OSS clients to retrieve the logToFile accounting statistics information. Services require the use of public addresses.

Table 7-12 Additional firewall rules required to allow services on the 5620 SAM client(s) to communicate with the 5620 SAM Server if NAT is used.

Protocol	From port	On	To port	On
TCP	Any	Server Public Address	21	Server Private Address
TCP	21	Server Public Address	Any	Server Private Address
TCP	> 1023	Server Public Address	> 1023	Server Private Address

When there is a firewall at the interface that reaches the SAM management network (NIC 1 on Figure 8-2, "Distributed 5620 SAM Server/Database deployment with multiple network interfaces" (p. 129)), the following rules apply.

Table 7-13 Firewall rules for traffic coming into the 5620 SAM Server(s) from the 5620 SAM Database Server(s)

Protocol	From port	On	To port	On
TCP	1523	Database Server(s)	Any	Server(s)
TCP	9002	Database Server(s)	Any	Server(s)

When there is a firewall at the SAM management interface (NIC 1 on Figure 8-2, "Distributed 5620 SAM Server/Database deployment with multiple network interfaces" (p. 129)) and 5620 SAM Server redundancy is configured, then the following rules need to be applied. Configuration needs to be in both directions to handle an activity switch.

Table 7-14 Firewall rules for setups with redundant 5620 SAM Servers.

Protocol	From port	On	To port	On
TCP	Any	Servers	22	Servers
TCP	22	Servers	Any	Servers
TCP	Any	Server	1099	Server
TCP	1099	Server	Any	Server
TCP	Any	Servers	8087	Servers
TCP	Any	Servers	9010	Servers
TCP	Any	Servers	11800	Servers
TCP	11800	Servers	Any	Servers
TCP	Any	Servers	12010	Servers
TCP	12010	Servers	Any	Servers
TCP	Any	Servers	12300-12307	Servers
TCP	12300-12307	Servers	Any	Servers

Table 7-14 Firewall rules for setups with redundant 5620 SAM Servers. (continued)

Protocol	From port	On	To port	On
TCP	> 32768	Servers	> 32768	Servers

When there is a firewall at the SAM management interface (NIC 1 on Figure 8-2, “Distributed 5620 SAM Server/Database deployment with multiple network interfaces” (p. 129)) and 5620 SAM Auxiliary Statistics / Call Trace Servers are configured, then the following rules need to be applied:

Table 7-15 Firewall rules for traffic coming into the 5620 SAM Server(s) from the 5620 SAM Auxiliary Statistics / Call Trace Server(s).

Protocol	From port	On	To port	On
TCP	Any	Auxiliary Server(s)	12300-12307	Server(s)
TCP	12300-12307	Auxiliary Server(s)	Any	Server(s)
TCP	Any	Auxiliary Server(s)	12800	Server(s)
TCP	12800	Auxiliary Server(s)	Any	Server(s)

When there is a firewall at the SAM management interface (NIC 1 on Figure 8-2, “Distributed 5620 SAM Server/Database deployment with multiple network interfaces” (p. 129)) and NAT is configured, then the following rules need to be applied. Services require the use of public addresses.

7.9.3 5620 SAM Database firewall and NAT rules

When there is a firewall at the interface that reaches the SAM management network (NIC 1 on Figure 8-2, “Distributed 5620 SAM Server/Database deployment with multiple network interfaces” (p. 129)), the following rules apply.

Table 7-16 Firewall rules for traffic coming into the 5620 SAM Database Server(s) from the 5620 SAM Server(s), 5620 SAM Auxiliary Statistics / Call Trace Server(s), and 5620 SAM Analytics Server

Protocol	From port	On	To port	On
TCP	Any	Server(s), Auxiliary Server(s), & Analytics Server	1523	Database Server(s)
TCP	Any	Server(s) & Auxiliary Server(s)	9002	Database Server(s)
TCP	> 32768	Server(s) & Auxiliary Server(s)	9003	Database Server(s)

When there is a firewall at the interface that reaches the SAM management network (NIC 1 on Figure 8-2, “Distributed 5620 SAM Server/Database deployment with multiple network interfaces” (p. 129)) and redundancy is configured, the following rules apply. Configuration needs to be in both directions to handle an activity switch.

Table 7-17 Firewall rules for traffic between the 5620 SAM Database Servers (redundant only)

Protocol	From port	On	To port	On
TCP	Any	Database Servers	22	Database Servers
TCP	22	Database Servers	Any	Database Servers
TCP	Any	Database Servers	1523	Database Servers
TCP	1523	Database Servers	> 9000	Database Servers
TCP	9002	Database Servers	9002	Database Servers
TCP	9003	Database Servers	9003	Database Servers

7.9.4 5620 SAM Auxiliary Server firewall and NAT rules

When there is a firewall at the interface that reaches the managed network (NIC 2 on Figure 8-2, “Distributed 5620 SAM Server/Database deployment with multiple network interfaces” (p. 129)), the following rules apply.

Table 7-18 SNMP Firewall rules for traffic coming into the 5620 SAM Auxiliary Statistics Collector Server(s) from the Managed Network

Protocol	From port	On	To port	On	Notes
UDP	>32768	Auxiliary Server(s)	161	Managed Network	SNMP request
UDP	161	Managed Network	> 32768	Auxiliary Server(s)	SNMP response

Note: Due to the size of SNMP packets, IP fragmentation may occur in the network. Ensure the firewall will allow fragmented packets to reach the server(s).

Table 7-19 SSH / Telnet Firewall rules for traffic coming into the 5620 SAM Auxiliary Statistics Collector Server(s) from the Managed Network

Protocol	From port	On	To port	On	Notes
TCP	>32768	Auxiliary Server(s)	22-23	Managed Network	SSH/SCP/Telnet request
TCP	22-23	Managed Network	> 32768	Auxiliary Server(s)	SSH/SCP/Telnet response

Table 7-20 FTP Firewall rules for traffic coming into the 5620 SAM Auxiliary Statistics Collector Server(s) from the Managed Network

Protocol	From port	On	To port	On	Notes
TCP	Any	Auxiliary Server(s)	21	Managed Network	FTP requests (example: STM, Accounting statistics, NE backups))
TCP	21	Managed Network	Any	Auxiliary Server(s)	FTP responses

Table 7-20 FTP Firewall rules for traffic coming into the 5620 SAM Auxiliary Statistics Collector Server(s) from the Managed Network (continued)

Protocol	From port	On	To port	On	Notes
TCP	> 1023	Managed Network	> 1023	Auxiliary Server(s)	Passive FTP ports for data transfer (See 7.8 "FTP between the 5620 SAM Server and 5620 SAM Auxiliary Statistics Collector and the managed network" (p. 107))

Note: FTP access is only required for the 5620 SAM Auxiliary Statistics Collector.

Table 7-21 SNMP Firewall rules for traffic coming into the 5620 SAM Auxiliary Call Trace Server(s) from the Managed Network

Protocol	From port	On	To port	On	Notes
UDP	>32768	Auxiliary Server(s)	161	Managed Network	SNMP request
UDP	161	Managed Network	> 32768	Auxiliary Server(s)	SNMP response

Note: Due to the size of SNMP packets, IP fragmentation may occur in the network. Ensure the firewall will allow fragmented packets to reach the server(s).

Table 7-22 Firewall rules for traffic coming into the 5620 SAM Auxiliary PCMD Collector(s) from the Managed Network

Protocol	From port	On	To port	On	Notes
UDP	Any	Managed Network	29780	Auxiliary Server(s)	PCMD records from SGW / PGW to 5620 SAM PCMD Auxiliary Collector.

Table 7-23 Firewall rules for traffic coming into the 5620 SAM Auxiliary Cflowd Server(s) from the Managed Network

Protocol	From port	On	To port	On	Notes
UDP	Any	Managed Network	4739	Auxiliary Server(s)	Cflowd flow records from 7750 routers to 5620 SAM Cflowd Auxiliary Server.

When there is a firewall at the interface that reaches the 5620 SAM Client(s) (NIC 3 on Figure 8-2, "Distributed 5620 SAM Server/Database deployment with multiple network interfaces" (p. 129)), the following rules apply for FTP access to the 5620 SAM Auxiliary by the OSS Client.

Table 7-24 Firewall rules for OSS Client communication to the 5620 SAM Auxiliary Server(s)

Protocol	From port	On	To port	On	Notes
TCP	Any	SAM-O Client	21/22	Auxiliary Server(s)	(S)FTP requests (logToFile statistics, and call trace information)
TCP	21/22	SAM-O Client	Any	Auxiliary Server(s)	(S)FTP responses
TCP	> 1023	SAM-O Client	Any	Auxiliary Server(s)	Passive (S)FTP ports for data transfer (See 7.8 "FTP between the 5620 SAM Server and 5620 SAM Auxiliary Statistics Collector and the managed network" (p. 107))
Only for 5620 SAM Auxiliary Call Trace Collectors					
TCP	Any	SAM-O Client	8086	Auxiliary Server(s)	HTTP interface for WebDAV for WTA
TCP	Any	SAM-O Client	8445	Auxiliary Server(s)	HTTPS interface for WebDAV for WTA
TCP	Any	SAM-O 3GPP-compliant Client	9735	Auxiliary Server(s)	Corba interface to access Call Trace information

Table 7-25 FTP/SFTP Firewall rules for the 5620 SAM Cflowd Auxiliary Server(s)

Protocol	From port	On	To port	On	Notes
TCP	Any	Auxiliary Server(s)	21/22	IPDR File Server	(S)FTP requests (logToFile statistics, and call trace information)
TCP	21/22	Target File Server	Any	Auxiliary Server(s)	(S)FTP responses
TCP	> 1023	Target File Server	Any	Auxiliary Server(s)	Passive (S)FTP ports for data transfer (See 7.8 "FTP between the 5620 SAM Server and 5620 SAM Auxiliary Statistics Collector and the managed network" (p. 107))

When there is a firewall at the interface that communicates with the 5620 SAM Servers, the following rules apply for inter process communication.

Table 7-26 Firewall rules for inter process communication on the 5620 SAM Auxiliary Statistics / Call Trace / PCMD / Femto Server(s)

Protocol	From port	On	To port	On
TCP	Any	Auxiliary Server(s)	1095	Auxiliary Server(s)

Table 7-26 Firewall rules for inter process communication on the 5620 SAM Auxiliary Statistics / Call Trace / PCMD / Femto Server(s) (continued)

Protocol	From port	On	To port	On
TCP	Any	Auxiliary Server(s)	12300-12307	Auxiliary Server(s)
TCP	12300-12307	Auxiliary Server(s)	Any	Auxiliary Server(s)
TCP	Any	Auxiliary Server(s)	12800	Auxiliary Server(s)
TCP	12800	Auxiliary Server(s)	Any	Auxiliary Server(s)

Table 7-27 Firewall rules for inter process communication on the 5620 SAM Cflowd Auxiliary Server(s)

Protocol	From port	On	To port	On
TCP	Any	Auxiliary Server(s)	1090	Auxiliary Server(s)
TCP	Any	Auxiliary Server(s)	1098	Auxiliary Server(s)
TCP	Any	Auxiliary Server(s)	1099	Auxiliary Server(s)
TCP	Any	Auxiliary Server(s)	4444	Auxiliary Server(s)
TCP	Any	Auxiliary Server(s)	4445	Auxiliary Server(s)
TCP	Any	Auxiliary Server(s)	4446	Auxiliary Server(s)
TCP	Any	Auxiliary Server(s)	4447	Auxiliary Server(s)
TCP	Any	Auxiliary Server(s)	4457	Auxiliary Server(s)
TCP	Any	Auxiliary Server(s)	8083	Auxiliary Server(s)
TCP	Any	Auxiliary Server(s)	9443	Auxiliary Server(s)
TCP	Any	Auxiliary Server(s)	9990	Auxiliary Server(s)
TCP	Any	Auxiliary Server(s)	9999	Auxiliary Server(s)

When there is a firewall at the interface that communicates with the 5620 SAM Servers, the following rules apply.

Table 7-28 Firewall rules for traffic coming into the 5620 SAM Auxiliary Statistics / Call Trace / PCMD / Femto Server(s) from the 5620 SAM Server(s)

Protocol	From port	On	To port	On
TCP	1097	Server(s)	Any	Auxiliary Server(s)
TCP	1099	Server(s)	Any	Auxiliary Server(s)
TCP	4447	Server(s)	Any	Auxiliary Server(s)
TCP	9010	Server(s)	Any	Femto Auxiliary Server(s)
TCP	> 32768	Server(s)	> 32768	Auxiliary Server(s)

Table 7-29 Firewall rules for traffic coming into the 5620 SAM Auxiliary Cflowd Server(s) from the 5620 SAM Server(s)

Protocol	From port	On	To port	On
TCP	Any	Server(s)	7879	Auxiliary Server(s)

When there is a firewall at the interface that reaches the 5620 SAM Client(s) (NIC 3 on Figure 8-2, “Distributed 5620 SAM Server/Database deployment with multiple network interfaces” (p. 129)) and NAT is used on the 5620 SAM Auxiliary Server(s), the following rules apply to allow the OSS clients to collect the logToFile accounting statistics files. Services require the use of public addresses.

Table 7-30 Additional Firewall rules required to allow services on the 5620 SAM client(s) to communicate with the 5620 SAM Auxiliary(s) if NAT is used on the Auxiliary Server(s).

Protocol	From port	On	To port	On
TCP	Any	Auxiliary Server Public Address	21	Auxiliary Server Private Address
TCP	21	Auxiliary Server Public Address	Any	Auxiliary Server Private Address
TCP	> 1023	Auxiliary Server Public Address	> 1023	Auxiliary Server Private Address

When there is a firewall at the interface that reaches the SAM management network (NIC 1 on Figure 8-2, “Distributed 5620 SAM Server/Database deployment with multiple network interfaces” (p. 129)), the following rules apply.

Table 7-31 Firewall rules for traffic coming into the 5620 SAM Auxiliary Server(s) from the 5620 SAM Database Server(s)

Protocol	From port	On	To port	On
TCP	1523	Database Server(s)	Any	Auxiliary Server(s)
TCP	9002	Database Server(s)	Any	Auxiliary Server(s)

When there is a firewall at the interface that reaches the SAM management network (NIC 1 on Figure 8-2, “Distributed 5620 SAM Server/Database deployment with multiple network interfaces” (p. 129)), the following rules apply.

Table 7-32 Firewall rules for traffic coming into the 5620 SAM Auxiliary Server(s) from the 5620 SAM Server(s)

Protocol	From port	On	To port	On
TCP	Any	Server(s)	12300-12307	Auxiliary Server(s)
TCP	12300-12307	Server(s)	Any	Auxiliary Server(s)
TCP	Any	Server(s)	12800	Auxiliary Server(s)
TCP	12800	Server(s)	Any	Auxiliary Server(s)

Table 7-33 Firewall rules for traffic between redundant 5620 SAM Auxiliary Statistics Collector Servers.

Protocol	From port	On	To port	On
TCP	Any	Auxiliary Statistics Collector	22	Auxiliary Statistics Collector
TCP	Any	Auxiliary Statistics Collector	9010	Auxiliary Statistics Collector

Table 7-34 Firewall rules for traffic between redundant 5620 SAM Auxiliary Call Trace Collector Servers.

Protocol	From port	On	To port	On
TCP	Any	Auxiliary Call Trace Collector	22	Auxiliary Call Trace Collector
TCP	Any	Auxiliary Call Trace Collector	9010	Auxiliary Call Trace Collector

7.9.5 5620 SAM Auxiliary Database Firewall Rules

Apply the following changes to the connection between the 5620 SAM Auxiliary Database and various 5620 SAM components. Note that all connections are bi-directional. Since the inter-node communication should traverse a private LAN network, it is not recommended to implement a firewall on this interface.

Table 7-35 Firewall rules for traffic between the 5620 SAM Server and the 5620 SAM Auxiliary Database

Protocol	From port	On	To port	On	Notes
TCP	>32768	Server(s)	5433	Auxiliary Databases	JDBC
TCP	>32768	Server(s)	7299–7309	Auxiliary Databases	RMI

Table 7-36 Firewall rules for traffic between the 5620 SAM Statistics Auxiliary and the 5620 SAM Auxiliary Database

Protocol	From port	On	To port	On	Notes
TCP	>32768	Statistics Auxiliary(s)	5433	Auxiliary Databases	JDBC

Table 7-37 Firewall rules for traffic between the 5620 SAM Cflowd Auxiliary and the 5620 SAM Auxiliary Database

Protocol	From port	On	To port	On	Notes
TCP	>32768	Cflowd Auxiliary(s)	5433	Auxiliary Databases	JDBC

Table 7-38 Firewall rules for traffic between the 5620 SAM Analytics Server and the 5620 SAM Auxiliary Database

Protocol	From port	On	To port	On	Notes
TCP	>32768	Analytics Server	5433	Auxiliary Databases	JDBC

7.9.6 5620 SAM Analytics Server Firewall Rules

Apply the following changes to the connection between the 5620 SAM Analytics Server and SAM Server / SAM Client. Note that all connections are bi-directional.

Table 7-39 Firewall rules for traffic between the 5620 SAM Server(s) and 5620 SAM Analytics Server

Protocol	From port	On	To port	On	Notes
TCP	>32768	Server(s)	8080	Analytics	HTTP
TCP	>32768	Server(s)	8443	Analytics	HTTPS

Table 7-40 Firewall rules for traffic between the 5620 SAM Client and 5620 SAM Analytics Server

Protocol	From port	On	To port	On	Notes
TCP	>32768	Client	8080	Analytics	HTTP
TCP	>32768	Client	8443	Analytics	HTTPS

7.9.7 5620 SAM Server to delegate workstation

Ensure that ICMP protocol traffic from the 5620 SAM Server workstation(s) can reach the 5620 SAM delegate workstation.

7.9.8 5620 SAM Client to managed network communications

Apply the following changes to the connection between the 5620 SAM Client and the managed network. Note that all connections are bi-directional.

Table 7-41 Firewall rules for traffic between the 5620 SAM Client and the DSC

Protocol	From port	On	To port	On	Notes
TCP	Any	5620 SAM Client(s)	443	Managed Network	HTTPS

Table 7-42 Firewall rules for traffic between the 5620 SAM Client and the 9471 WMM

Protocol	From port	On	To port	On	Notes
TCP	Any	5620 SAM Client (s)	1099	Managed Network	RMI

Table 7-42 Firewall rules for traffic between the 5620 SAM Client and the 9471 WMM (continued)

Protocol	From port	On	To port	On	Notes
TCP	Any	5620 SAM Client (s)	1234	Managed Network	Search-agent
TCP	Any	5620 SAM Client (s)	1235	Managed Network	Search-agent
TCP	Any	5620 SAM Client (s)	4567	Managed Network	tram
TCP	Any	5620 SAM Client (s)	8443	Managed Network	HTTPS
TCP	Any	5620 SAM Client (s)	9683	Managed Network	MME version 4.0 and older

Table 7-43 Firewall rules for traffic between the 5620 SAM Client and the eNodeB NEM

Protocol	From port	On	To port	On	Notes
UDP	Any	5620 SAM Client(s)	161	Managed Network	SNMP
TCP	Any	5620 SAM Client(s)	830	Managed Network	NetConf over SSH

Table 7-44 Firewall rules for traffic between the 5620 SAM Client and GNEs

Protocol	From port	On	To port	On	Notes
TCP	Any	5620 SAM Client(s)	80	Managed Network	HTTP (See GNE vendor for specifics)
TCP	Any	5620 SAM Client(s)	443	Managed Network	HTTPS (See GNE vendor for specifics)

Table 7-45 Firewall rules for traffic between the 5620 SAM Client (NEtO) and 9500MPR (MSS-8/4/1)

Protocol	From port	On	To port	On	Notes
TCP	20	5620 SAM Client(s)	Any	Managed Network	Active FTP
TCP	Any	5620 SAM Client(s)	21	Managed Network	FTP
TCP	21	5620 SAM Client	Any	Managed Network	FTP
TCP	22	5620 SAM Client	Any	Managed Network	sFTP
TCP	Any	5620 SAM Client	22	Managed Network	sFTP
TCP	Any	5620 SAM Client(s)	23	Managed Network	Telnet
TCP	Any	5620 SAM Client(s)	80	Managed Network	HTTP
UDP	Any	5620 SAM Client(s)	161	Managed Network	SNMP
TCP	>1023	5620 SAM Client(s)	>1023	Managed Network	Passive FTP
UDP	5010	5620 SAM Client(s)	5010	Managed Network	SNMP

Table 7-46 Firewall rules for traffic between the 5620 SAM Client (NEtO) and 9500MPR (MSS-1C / MPR-e)

Protocol	From port	On	To port	On	Notes
TCP	20	5620 SAM Client(s)	Any	Managed Network	Active FTP
TCP	21	5620 SAM Client	Any	Managed Network	FTP
TCP	Any	5620 SAM Client(s)	23	Managed Network	Telnet
UDP	Any	5620 SAM Client(s)	161	Managed Network	SNMP
TCP	>1023	5620 SAM Client(s)	>1023	Managed Network	Passive FTP
UDP	5010	5620 SAM Client	Any	Managed Network	SNMP
UDP	Any	5620 SAM Client	11500	Managed Network	Equipment View (GUI)

Table 7-47 Firewall rules for traffic between the 5620 SAM Client (NEtO) and 9400AWY

Protocol	From port	On	To port	On	Notes
TCP	Any	5620 SAM Client(s)	21	Managed Network	FTP
TCP	21	5620 SAM Client	Any	Managed Network	FTP
TCP	Any	5620 SAM Client(s)	23	Managed Network	Telnet
TCP	Any	5620 SAM Client(s)	80	Managed Network	HTTP
UDP	Any	5620 SAM Client(s)	161	Managed Network	SNMP
TCP	>1023	5620 SAM Client(s)	>1023	Managed Network	Passive FTP
UDP	5010	5620 SAM Client	Any	Managed Network	SNMP

Table 7-48 Firewall rules for traffic between the 5620 SAM Client and Omni Switches

Protocol	From port	On	To port	On	Notes
TCP	Any	5620 SAM Client(s)	80	Managed Network	HTTP
TCP	Any	5620 SAM Client(s)	443	Managed Network	HTTPS

7.10 Data privacy

7.10.1 Securing private data in the system

The tables in this section indicate how personal data is handled within 5620 SAM. The servers in a 5620 SAM deployment reside within the secure domain of the customer network.

Table 7-49 5620 SAM data privacy

Category	Description
Local user data (local authentication)	

Table 7-49 5620 SAM data privacy (continued)

Category	Description
Type of data	• Username and password • Email • IP address
Purpose	• Authentication of local 5620 SAM users • User email addresses (optional) to send notifications for certain events, for example: alarms or account status • IP address provides accountability of individual product access
Storage	• Local database • Logs
Retention	Data is retained in the database until an authorized user deletes it. Log retention time can vary based on log file size and the number of log backups.
Processing	Local user data is processed for the stated purpose.
Access	Authorized users
Safeguards	• Additional local users must be created by an authorized user • Database access is restricted to authorized users • Secure transit option is available • Passwords for local users are hashed before they are stored • Log file access is restricted to authorized users
Comments	Local authentication is performed using a local database of users and a local security scheme.
Customer profile data	
Type of data	• Name • Email • Address • Phone
Purpose	Data may be used by an authorized user for associating customers to configured services.
Storage	Local database
Retention	Data is retained in the database until an authorized user deletes it.
Processing	Customer profile data is processed for the stated purpose.
Access	Authorized users
Safeguards	• Customer profile must be created by an authorized user • Database access is restricted to authorized users
Network element data	

Table 7-49 5620 SAM data privacy (continued)

Category	Description
Type of data	• Username and password • IP address
Purpose	• NE authentication • NE IP address for NE discovery/access
Storage	• Local database • Logs Note that NE backups that are stored on the 5620 SAM server may contain data that is not stored in the 5620 SAM database. Data contained in the NE backup files will be dependent upon the NE type and version and therefore the privacy statements for the individual NEs should be consulted.
Retention	Data is retained in the database until an authorized user deletes it. Log retention can vary based on the log file size and number of log backups.
Processing	NE data is processed for the stated purpose.
Access	Authorized users
Safeguards	• NEs are configured by authorized users • Database access is restricted to authorized users • Secure transit option is available • Passwords for NE users are encrypted before being stored • Log file access is restricted to authorized users
Subscriber data	
Type of data	• MAC address • IP address • International Mobile Subscriber Identity (IMSI) • International Mobile Station Equipment Identity (IMEI) • Mobile Station International Subscriber Directory Number (MSISDN) • Access Point Name (APN)
Purpose	• Statistics • SLA compliance • Troubleshooting • Analytics • UE or network node performance information
Storage	• Local database • Logs • Auxiliary collector servers (optional): statistics, PCMD and call trace • Flow collector server (optional) • Analytics server (optional)

Table 7-49 5620 SAM data privacy (continued)

Category	Description
Retention	Data is retained in the database until an authorized user deletes it. Log retention can vary based on the log file size and number of log backups. Retention period for auxiliary servers can be configured. Retention period for statistics on flow collectors is 4 hours.
Processing	Subscriber data is processed for the stated purpose.
Access	Authorized users
Safeguards	• NEs are configured by authorized users • Database access is restricted to authorized users • Secure transit option is available • File access is restricted to authorized users • Log file access is restricted to authorized users

8 Deploying the 5620 SAM with multiple network interfaces/IP addresses

8.1 Overview

8.1.1 Purpose

This chapter provides general information about 5620 SAM deployments with multiple network interfaces and IP addresses.

8.1.2 Contents

8.2 Deploying the 5620 SAM with multiple network interfaces/IP addresses

8.2.1 Deploying the 5620 SAM with multiple network interfaces/IP addresses

The 5620 SAM Server and 5620 SAM Auxiliary Collector (statistics / call trace / PCMD) components of the application communicate with very different entities: a managed network, a collection of Clients (GUIs and OSS), and between each other. Since these entities usually exist in very different spaces, Nokia recognizes the importance of separating these different types of traffic. Nokia therefore supports configuring the 5620 SAM Server and 5620 SAM Auxiliary such that it uses different network interfaces (IP addresses) to manage the network and to service the requirements of the 5620 SAM Clients.

5620 SAM Server uses an internal communications system (JGroups/JMS) to handle bi-directional access to the 5620 SAM Server for the 5620 SAM Clients and the 5620 SAM Auxiliary Collectors. In 5620 SAM, this communication system can be configured to allow the 5620 SAM Clients and 5620 SAM Auxiliary Collectors to communicate using different network interfaces on the 5620 SAM Server. This adds significant flexibility when isolating the different types of traffic to the 5620 SAM Server. If using this mode, special attention must be paid to the firewall rules on the network interfaces on the 5620 SAM Server and 5620 SAM Auxiliary Collector (NICs 1 and NICs 3 on Figure 8-2, “Distributed 5620 SAM Server/Database deployment with multiple network interfaces” (p. 129)).

It is a security requirement that all IP communications from a 5620 SAM Auxiliary Collector to the 5620 SAM Main server use only one IP address. This IP Address must be the same IP address as the Auxiliary Collector IP address configured when installing the Main Server. Any other IP communications originating from a different IP address on the Auxiliary Collector will be rejected by the 5620 SAM Main Server.

When installing 5620 SAM components on workstations with multiple interfaces, each interface must reside on a separate subnet, with the exception of interfaces that are to be used in IP Bonding.

Figure 8-1, “Collocated 5620 SAM Server/Database deployment with multiple network interfaces” (p. 128) illustrates a collocated 5620 SAM Server/Database deployment where the 5620 SAM is configured to actively use more than one network interface.

It is not necessary to use the first network interface on the 5620 SAM Server workstation (i.e. ce0, bge0) to communicate with the 5620 SAM GUI Clients.

Figure 8-1 Collocated 5620 SAM Server/Database deployment with multiple network interfaces

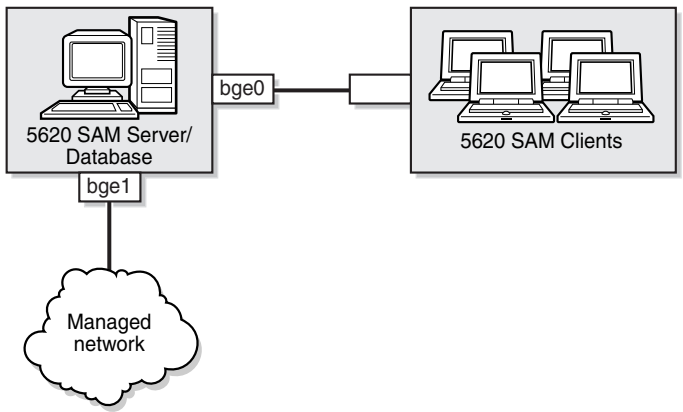


Figure 8-2 Distributed 5620 SAM Server/Database deployment with multiple network interfaces

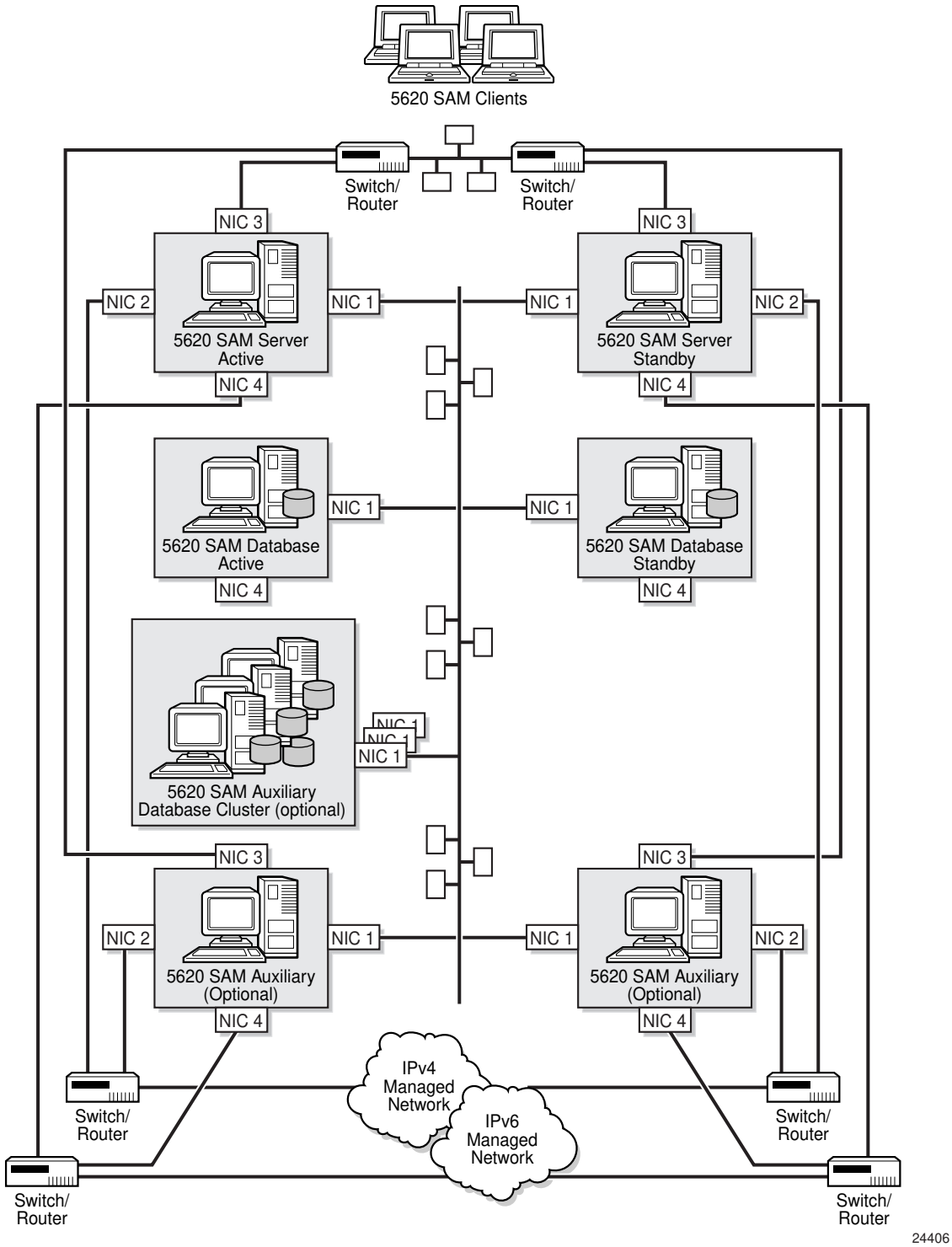


Figure 8-2, “Distributed 5620 SAM Server/Database deployment with multiple network interfaces” (p. 129) illustrates a distributed, redundant 5620 SAM deployment where the 5620 SAM components are configured to actively use more than one network interface.

Due to limitations with the inter-process and inter-workstation communication mechanisms, a specific network topology and the use of hostnames may be required (see 8.10 “Use of hostnames for the 5620 SAM Client” (p. 137)). Contact an Nokia representative to obtain further details.

8.3 5620 SAM Server multiple IP addresses deployment scenarios

8.3.1 5620 SAM Server multiple IP addresses deployment scenarios

The 5620 SAM Server supports the configuration of different IP addresses for the following purposes:

- One or multiple network interfaces can be used to manage the network. (NIC 2 on Figure 8-2, “Distributed 5620 SAM Server/Database deployment with multiple network interfaces” (p. 129)) This network interface contains the IP address that the managed devices will use to communicate with the 5620 SAM Server and 5620 SAM Auxiliary. If managing a network element with both an in-band and out-of-band connection, the same network interface on the 5620 SAM Server must be used for both communication types.
- One network interface can be used to service the requirements of the 5620 SAM clients (GUIs and OSS) (NIC 3 on Figure 8-2, “Distributed 5620 SAM Server/Database deployment with multiple network interfaces” (p. 129)). This network interface contains the IP address that all clients (GUIs and OSS) will use to communicate with the 5620 SAM Server. All clients (GUIs and OSS) must be configured to use the same IP address to communicate to the 5620 SAM Server. This IP address can be different from the one used by the managed devices to communicate with the 5620 SAM Server.
- One network interface can be used to communicate with the 5620 SAM Database, 5620 SAM Auxiliary Database, and 5620 SAM Auxiliary Collectors as well as any redundant 5620 SAM components should they be present (NIC 1 on Figure 8-2, “Distributed 5620 SAM Server/Database deployment with multiple network interfaces” (p. 129)). This network interface contains the IP address that the 5620 SAM Database, 5620 SAM Auxiliary Database, and redundant 5620 SAM components will use to communicate with the 5620 SAM Server. This IP address can be different from the addresses used by the 5620 SAM clients and the managed devices to communicate with the 5620 SAM Server.
- In a redundant 5620 SAM installation, the 5620 SAM Servers and 5620 SAM Auxiliary Collectors must have IP connectivity to the 5620 SAM Server peer.
- Additional network interfaces may be configured on the 5620 SAM Server workstation, at the customer’s discretion, to perform maintenance operations such as workstation backups.
- IPv4 and IPv6 network elements can be managed from the same interface or from separate interfaces. (NIC3 and/or NIC4 on Figure 8-2, “Distributed 5620 SAM Server/Database deployment with multiple network interfaces” (p. 129)).

8.4 5620 SAM Auxiliary Statistics Collector multiple IP addresses deployment scenarios

8.4.1 5620 SAM Auxiliary Statistics Collector multiple IP addresses deployment scenarios

The 5620 SAM Auxiliary Statistics Collector supports the configuration of different IP addresses for the following purposes:

- One or multiple network interfaces can be used to retrieve information from the managed network. (NIC 2 on Figure 8-2, “Distributed 5620 SAM Server/Database deployment with multiple network interfaces” (p. 129)) This network interface contains the IP address that the managed devices will use to retrieve the accounting statistics files, and performance statistics from the network elements.
- One network interface can be used to service the requirements of the OSS clients (NIC 3 on Figure 8-2, “Distributed 5620 SAM Server/Database deployment with multiple network interfaces” (p. 129)). This network interface contains the IP address that all OSS clients will use to communicate with the 5620 SAM Auxiliary Statistics Collector. OSS Clients will use this IP address to retrieve the logToFile statistics collection data from the 5620 SAM Auxiliary Statistics Collector.
- One network interface can be used to communicate with the 5620 SAM Server, 5620 SAM Database, 5620 SAM Auxiliary Database cluster as well as any redundant 5620 SAM components should they be present (NIC 1 on Figure 8-2, “Distributed 5620 SAM Server/Database deployment with multiple network interfaces” (p. 129)). This network interface contains the IP address that the 5620 SAM Server, 5620 SAM Database, 5620 SAM Auxiliary Database, and redundant 5620 SAM components will use to communicate with the 5620 SAM Auxiliary Statistics Collector. This IP address can be different from the addresses used by the 5620 SAM OSS clients and the managed devices to communicate with the 5620 SAM Auxiliary Statistics Collector.
- In a redundant 5620 SAM installation, the 5620 SAM Auxiliary Statistics Collector must have IP connectivity to the 5620 SAM Server peer.
- Additional network interfaces may be configured on the 5620 SAM Auxiliary Statistics Collector workstation, at the customer’s discretion, to perform maintenance operations such as workstation backups.
- IPv4 and IPv6 network elements can be managed from the same interface or from separate interfaces. (NIC3 and/or NIC4 on Figure 8-2, “Distributed 5620 SAM Server/Database deployment with multiple network interfaces” (p. 129)).

8.5 5620 SAM Auxiliary Call Trace Collector multiple IP addresses deployment scenarios

8.5.1 5620 SAM Auxiliary Call Trace Collector multiple IP addresses deployment scenarios

The 5620 SAM Auxiliary Call Trace Collector supports the configuration of different IP addresses for the following purposes:

- One network interface can be used to retrieve information from the managed network. (NIC 2 on Figure 8-2, “Distributed 5620 SAM Server/Database deployment with multiple network interfaces” (p. 129)) This network interface contains the IP address that the managed devices will use to send the call trace messages from the network elements.
- One network interface can be used to service the requirements of the 9958 WTA client (NIC 3 on Figure 8-2, “Distributed 5620 SAM Server/Database deployment with multiple network interfaces” (p. 129)). This network interface contains the IP address that all clients will use to communicate with the 5620 SAM Auxiliary Call Trace Collector. 9958 WTA will use this IP address to retrieve the Call Trace data from the 5620 SAM Auxiliary Call Trace Collector.
- One network interface can be used to communicate with the 5620 SAM management complex as well as any redundant 5620 SAM components should they be present (NIC 1 on Figure 8-2, “Distributed 5620 SAM Server/Database deployment with multiple network interfaces” (p. 129)). This network interface contains the IP address that the 5620 SAM management complex components will use to communicate with the 5620 SAM Auxiliary Call Trace Collector. If a redundant 5620 SAM Auxiliary Call Trace Collector is present, this network interface will also be used to sync Call Trace and Debug Trace data collected from the network, with the peer 5620 SAM Auxiliary Call Trace Collector. This IP address can be different from the addresses used by the 9958 WTA clients and the managed devices to communicate with the 5620 SAM Server.
- In a redundant 5620 SAM installation, the 5620 SAM Auxiliary Call Trace Collector must have IP connectivity to the 5620 SAM Server peer.
- Additional network interfaces may be configured on the 5620 SAM Auxiliary Call Trace Collector workstation, at the customer’s discretion, to perform maintenance operations such as workstation backups.
- IPv4 and IPv6 network elements can be managed from the same interface or from separate interfaces. (NIC3 and/or NIC4 on Figure 8-2, “Distributed 5620 SAM Server/Database deployment with multiple network interfaces” (p. 129)).

8.6 5620 SAM Auxiliary Cflowd Collector multiple IP addresses deployment scenarios

8.6.1 5620 SAM Auxiliary Cflowd Collector multiple IP addresses deployment scenarios

The 5620 SAM Auxiliary Cflowd Collector supports the configuration of different IP addresses for the following purposes:

- One network interface can be used to retrieve information from the managed network. (NIC 2 on Figure 8-2, “Distributed 5620 SAM Server/Database deployment with multiple network

interfaces" (p. 129)) This network interface contains the IP address that the managed devices will use to send the cflowd flow data from the network elements.

- One network interface can be used to send the formatted IPDR files to the target file server (NIC 3 on Figure 8-2, "Distributed 5620 SAM Server/Database deployment with multiple network interfaces" (p. 129)). This network interface contains the IP address that all clients will use to communicate with the 5620 SAM Auxiliary Cflowd Collector.
- One network interface can be used to communicate with the 5620 SAM management complex as well as any redundant 5620 SAM components should they be present (NIC 1 on Figure 8-2, "Distributed 5620 SAM Server/Database deployment with multiple network interfaces" (p. 129)). This network interface contains the IP address that the 5620 SAM management complex components will use to communicate with the 5620 SAM Auxiliary Cflowd Collector. This IP address can be different from the addresses used by the clients and the managed devices to communicate with the 5620 SAM Server.
- In a redundant 5620 SAM installation, the 5620 SAM Auxiliary Cflowd Collector must have IP connectivity to the 5620 SAM Server peer.
- Additional network interfaces may be configured on the 5620 SAM Auxiliary Cflowd Collector workstation, at the customer's discretion, to perform maintenance operations such as workstation backups.

8.7 5620 SAM Auxiliary PCMD Collector multiple IP addresses deployment scenarios

8.7.1 5620 SAM Auxiliary Cflowd Collector multiple IP addresses deployment scenarios

The 5620 SAM Auxiliary Cflowd Collector supports the configuration of different IP addresses for the following purposes where a minimum of two separate interfaces must be used — one for management traffic and one for PCMD data collection:

- One network interface can be used to retrieve information from the managed network. (NIC 2 on Figure 8-2, "Distributed 5620 SAM Server/Database deployment with multiple network interfaces" (p. 129)) This network interface contains the IP address that the managed devices will use to send the PCMD data from the network elements.
- One network interface can be used for retrieval of the formatted PCMD files by the target file server (NIC 3 on Figure 8-2, "Distributed 5620 SAM Server/Database deployment with multiple network interfaces" (p. 129)). This network interface contains the IP address that all clients will use to communicate with the 5620 SAM Auxiliary Cflowd Collector.
- One network interface can be used to communicate with the 5620 SAM management complex as well as any redundant 5620 SAM components should they be present (NIC 1 on Figure 8-2, "Distributed 5620 SAM Server/Database deployment with multiple network interfaces" (p. 129)). This network interface contains the IP address that the 5620 SAM management complex components will use to communicate with the 5620 SAM Auxiliary PCMD Collector. This IP address can be different from the addresses used by the clients and the managed devices to communicate with the 5620 SAM Server.
- In a redundant 5620 SAM installation, the 5620 SAM Auxiliary PCMD Collector must have IP connectivity to the 5620 SAM Server peer.

- Additional network interfaces may be configured on the 5620 SAM Auxiliary PCMD Collector workstation, at the customer's discretion, to perform maintenance operations such as workstation backups.

8.8 Using Network Address Translation

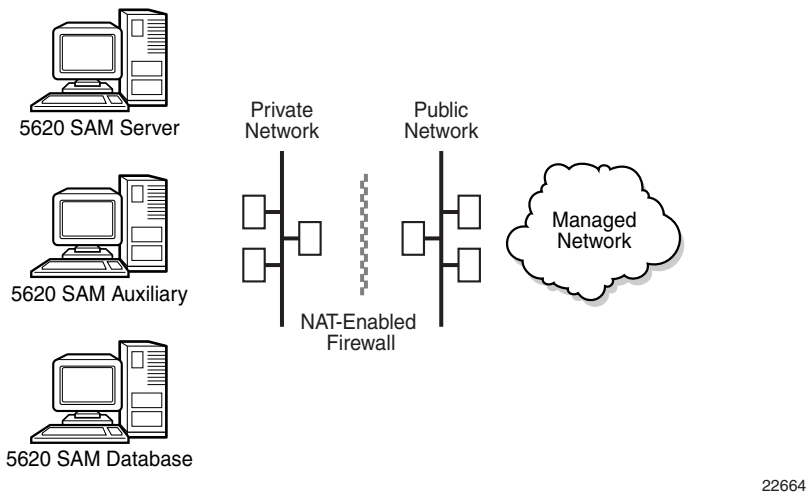
8.8.1 Using Network Address Translation

5620 SAM supports the use of Network Address Translation (NAT) between the following components:

- The 5620 SAM Server and 5620 SAM Clients (GUIs or OSS)
- The 5620 SAM Auxiliary Server and 5620 SAM OSS Clients
- The 5620 SAM Server and the managed network
- The 5620 SAM Auxiliary Statistics Collector and the managed network
- The 5620 SAM Auxiliary PCMD Collector and the managed network

The figure below illustrates a deployment of 5620 SAM where NAT is used between the 5620 SAM Server and the managed network.

Figure 8-3 5620 SAM Server deployments with NAT between the Server and the managed network



Note: Network Address Translation is not supported between the 5620 SAM Auxiliary Call Trace Collector and the Managed Network.

The following two figures illustrates a deployment of 5620 SAM where NAT is used between the 5620 SAM Server and the 5620 SAM Clients (GUIs, OSS or Client Delegates). In Figure 8-4, "5620 SAM Server deployment using NAT with IP Address communication" (p. 135) , SAM Clients on the private side and public side of the NAT-Enabled Firewall must connect to the public IP address of

the SAM Server. A routing loopback from the SAM Server private IP address to the SAM Server public IP address must be configured in this scenario as all SAM Clients must communicate to the SAM Server through the SAM Server public IP address.

The 5620 SAM Auxiliary will need to be able to connect to the public IP address of the 5620 SAM server.

Figure 8-4 5620 SAM Server deployment using NAT with IP Address communication

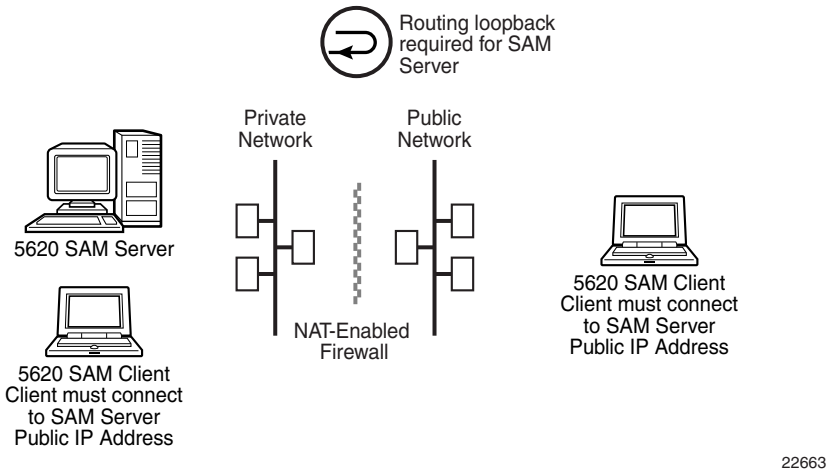
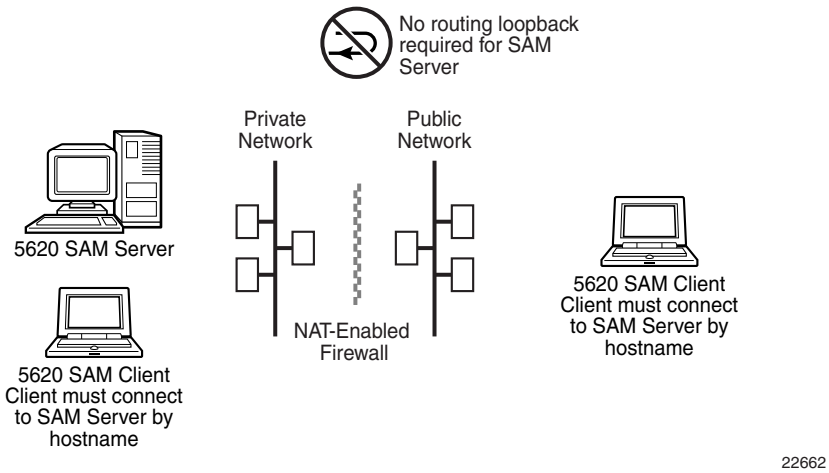


Figure 8-5 5620 SAM Server deployment using NAT with Name Resolution based communication

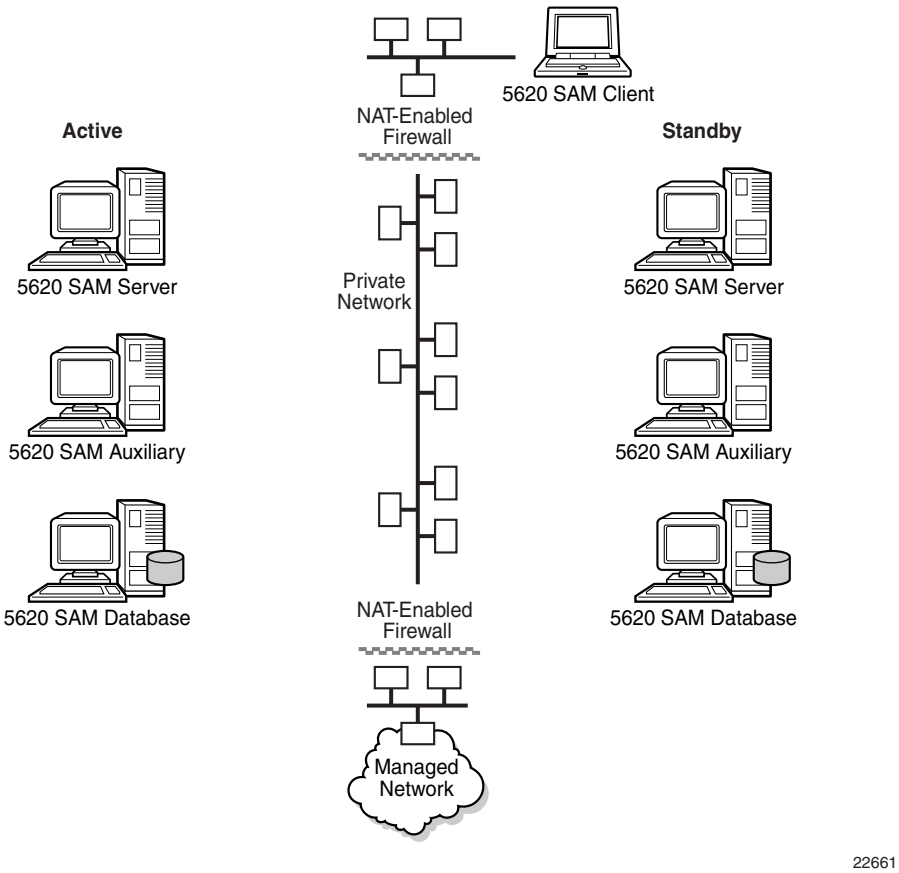


In Figure 8-5, “5620 SAM Server deployment using NAT with Name Resolution based communication” (p. 135) , a name resolution service on the public side of the NAT-Enabled Firewall is configured to resolve the SAM Server hostname to the public IP address of the SAM server.

Name resolution service on the private side of the NAT-Enabled Firewall is configured to resolve the SAM Server hostname to the private IP address of the SAM server. Clients on both sides of the NAT-Enabled Firewall are configured to communicate with the SAM Server via hostname where the SAM Server hostname must be the same on both sides of the NAT-Enabled Firewall.

The figure below illustrates a deployment of 5620 SAM where NAT is used between the 5620 SAM complex, 5620 SAM clients, and the managed network.

Figure 8-6 5620 SAM deployment with NAT



For installations using NAT between the SAM Server and SAM Client, a reverse DNS look-up mechanism must be used for the client, to allow proper startup.

NAT rules must be in place before 5620 SAM installation can occur, since the installation scripts will access other systems for configuration purposes.

Note: Network Address Translation is not supported between the 5620 SAM Auxiliary Call Trace Collector and the Managed Network.

8.9 Configuring 5620 SAM Server to utilize multiple network interfaces

8.9.1 Configuring 5620 SAM Server to utilize multiple network interfaces

The configuration of the 5620 SAM Server application to use multiple interfaces is done at installation time. At that time, the installation utility prompts the user to enter the IP addresses of the various network interfaces that are to be used within the 5620 SAM network management complex.

8.10 Use of hostnames for the 5620 SAM Client

8.10.1 Use of hostnames for the 5620 SAM Client

There are a number of situations where it is necessary for the 5620 SAM Client to be configured to use a hostname rather than a fixed IP address to reach the 5620 SAM Server.

For situations where the 5620 SAM Server's public address is exposed to multiple networks with different IP addresses, a hostname can be used instead of a fixed IP address. This is most useful when NAT is used between 5620 SAM clients and the 5620 SAM Server that can be accessed via multiple networks.

For situations where the 5620 SAM Client and the 5620 SAM Auxiliary are using different network interfaces to the 5620 SAM Server, the 5620 SAM Client must use a hostname to reach the 5620 SAM Server.

In both cases, a hostname can be used by configuring DNS, or by configuring the local host file to ensure that the hostname can be translated to an IP address.

The 5620 SAM Server must be installed using the Hostnames for Communications option for this scenario.