Secure Access Management for a Secure Operational Network (SAMSON) Technology Demonstrator (TD)

SD-006 CTDC Trial Report; Test Plan and Results

Prepared By:
Bell Development Team
Bell Canada, 160 Elgin St. 17th Floor
Ottawa, ON K1S 5N4

PWGSC Contract Number: W7714-08FE01
CSA: Daniel Charlebois, DRDC-CSS

Contract Report
DRDC-RDDC-2013-C9
November 2013

IMPORTANT INFORMATIVE STATEMENTS

The information contained herein is proprietary to Her Majesty and is provided to the recipient on the understanding that it will be used for information and evaluation purposes only. Any commercial use including use for manufacture is prohibited.

www.bell.ca

Secure Access Management for a Secure Operational Network (SAMSON) Technology Demonstrator (TD)

SD-006 CTDC Trial Report

Test Plan and Results

Bell Canada
160 Elgin Street
17th Floor
Ottawa, Ontario
K1S 5N4

November 25, 2013
Version: Final 1.1

Bell

This document does not include sensitive information. Instead, this document may contain external references to separate documents containing sensitive information. This allows this document to be unclassified, as any classified, protected or proprietary information is referenced, not disclosed.

The SAMSON TD system is being designed to not be a classified system. The SAMSON system will provide access to sensitive information, but the system itself is designed to be unclassified. The SAMSON configuration data (such as specific user access control parameters and related security controls used in the Policy Decision Point algorithms) for a specific instance is sensitive information, and appropriate safeguards are provided to protect this data.

Contents

DOCUMENT HISTORY

Version	Date	Comments
Draft 1.0	2013-07-31	Initial draft
1.1	2013-09-09	Addition of Email Performancec Test Results
1.2	2013-09-13	Instant Messaging and File Service Performance test results added.
Final 1.0	2013-09-17	To address comments received on the draft version
1.1	2013-11-25	Removed DRAFT watermark and Bell copyright.

1 OVERVIEW

This document is the Classified Test and Development Center (CTDC) Trial Report - Test Plan and Results for the Secure Access Management of a Secure Operational Network (Samson). *NOTE: The CTDC is divided into two parts: The unclass portion and the classified portion. This report documents the tests on the unclass side of the CTDC.* This Trial Report describes the configuration which will be/was tested, the testing period, resources required, special testing tools/materials, location of the tests, an overview of the tests performed, the testing methodology, and the evaluation criteria.

1.1 OBJECTIVES

The CTDC Test team will carry out the installation, configuration, acceptance testing, performance, scalability, and stress testing on Samson to:

- Define the Samson configuration for CTDC;
- Define the Samson roles specific to the CTDC environment;
- Determine the time and effort required to install and configure Samson from "bare" machines;
- Provide a complete listing (Software Version Control) of all Samson and 3rd Party software used for the CTDC installation;
- Determine the resources and level of effort required to operate and support day to day operations of the Samson environment; and
- Determine the User community size and active concurrent Users that the Samson protected applications (Email, Instant Mesaging, and File Transfer) will support in the CTDC environment.

1.2 SCOPE

The scope of this CTDC Trial Report -Test Plan and Results is to describe the testing activities required to meet the testing associated with:

- Determining the resources (manpower and time) required to complete an installation and configuration of Samson to the point where successful Acceptance Testing can be carried out, this will include defining the:
    - Equipment and Virtual Machine Template Preparation
    - Installation and Configuration from the Virtual Machine Templates; the
    - Routine operational procedures to:
        - Create/Remove users;
        - Create/Remove and archiving of policies;
        - Monitoring of the audit records and logs; the
- Acceptance Testing; and
- Non Functional Testing
    - Performance
    - Storage Sizing

- Alarm/Alert mechanisms
- Endurance and Stress - Testing, which will be carried out to determine if the system will remain operational over an extended period of time under a steady state load and peak load with up to 25 users, and then extrapolated for a base of 1000 users.

Outside of the scope of the testing activities is the:

Installation of Active Directory - a specific Organizational Unit (OU) will be provided to permit integration of the Samson system and the existing Active Directory structure used by CTDC.

CTDC will be required to provide a Microsoft Exchange email server, Windows File Server, and an IM server to permit integration with the Samson Policy Enforcement Points (PEPs) for Email, FileServices, and IM.

1.3 LIST OF ABBREVIATIONS

Master User	MU
Poicy Administration Interface	PAI
Policy Decision Point	PDP
Policy Enforcement Point	PEP
Samson Administrator	SA
Samson User	SU
Security Admin	SecAdmin
Security Officer	SO
Trusted Audit Service	TAS

1.4 REFERENCE DOCUMENTS

- Samson CONOPS 2013 v1.03
- SD-007 Samson Deployment and Configuration Guide v 3.0.1b

1.5 RESOURCES

A Test Specialist will be assigned to this project.

1.6 SCHEDULE

The CTDC testing will begin on the 15th June, 2013 and is scheduled to end 30th September, 2013.

2 PROCEDURE CONTROL

This section provides guidelines for those individuals involved in the CTDC testing. Consideration is given to guidelines and activities that must be adhered to during test initiation, execution, and failure, formal change control, and document control. All test activities will be conducted by a test specialist.

2.1 TEST INITIATION

Prior to commencement of the CTDC Tests the test specialist must ensure that:

There has been the successful completion of a comprehensive Test Readiness Review (TRR). The objective of this review is to ensure that everything is in order for testing and, in so far as possible, that the test will succeed. The meeting will include a test technical overview presentation, review of the test documentation status, and identification of test limitations, if any.

In addition, any open problem report(s) and their impact(s) should have been resolved.

All revisions have been incorporated in to the Samson Deployment and Configuration document.

All VM templates, Samson Code tar files, and Samson App tar files are subject to formal change control.

Test processes are complete and ready for execution.

Hardware/software test resources have been scheduled.

All hardware and software support required to run the tests, in accordance with the test schedule, are available.

Sufficient memory and disk space is provided to permit execution of test cases.

2.2 TEST FAILURE

In the event that an installation process or test does not produce the expected results or the results are not consistent with previous results, a Problem Report (PR) will be raised by the test specialist.

2.3 RISKS AND CONTINGENCIES

Should it be required that the performance test result modelling requires validation, it would require that a larger user community be set up. Increasing the size of the Samson test user community to a large number of users, such as 1000, requires time to load the users into Active Directory and migrate user caveat data from the LDAP Directory. This can be a time consuming activity and using the performance test tools with a large number of active users requires additional manual setup time.

Failure of the performance tests in a large user community set up could produce a time delay to the project.

2.4 CHANGE CONTROL

Changes to this plan will be subjected to the approval of the Samson Project Manager.

2.5 TEST EXECUTION

Prior to the execution of test cases, 25 users will have been loaded into the Active Directory, and Directory structure.

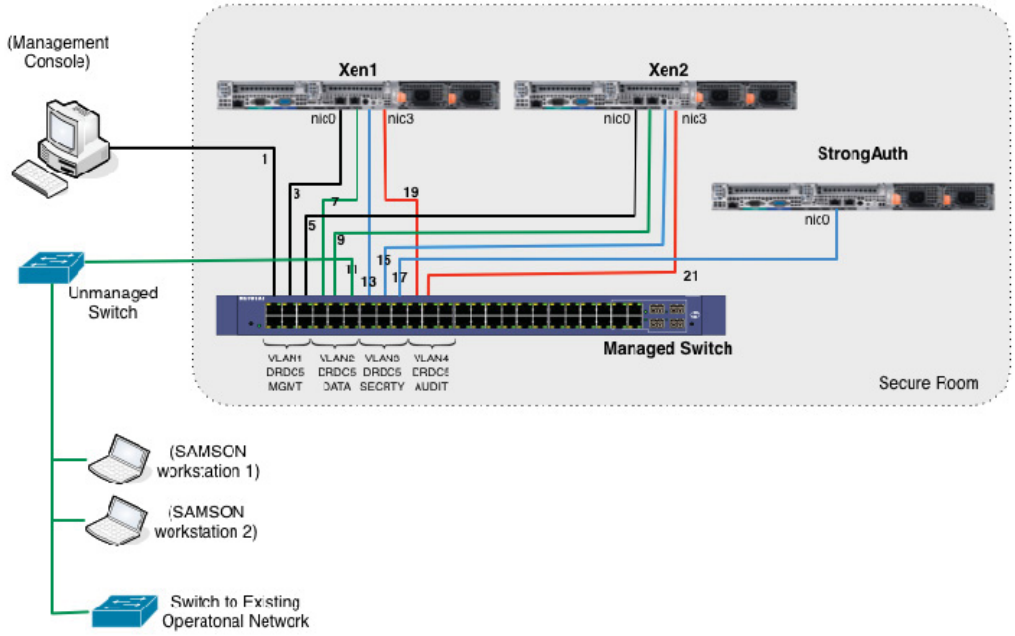
Where applicable, during execution the test specialist will record screen data and log test data related to resource utilization and performance results obtained during the testing process. This will permit analysis of the data at a later date and reconstruction of the tests.

2.6 DOCUMENTATION CONTROL

Test documentation will be updated along with other documentation as changes to the system or by the project demand.

3 PHYSICAL TEST MACHINE ENVIRONMENT

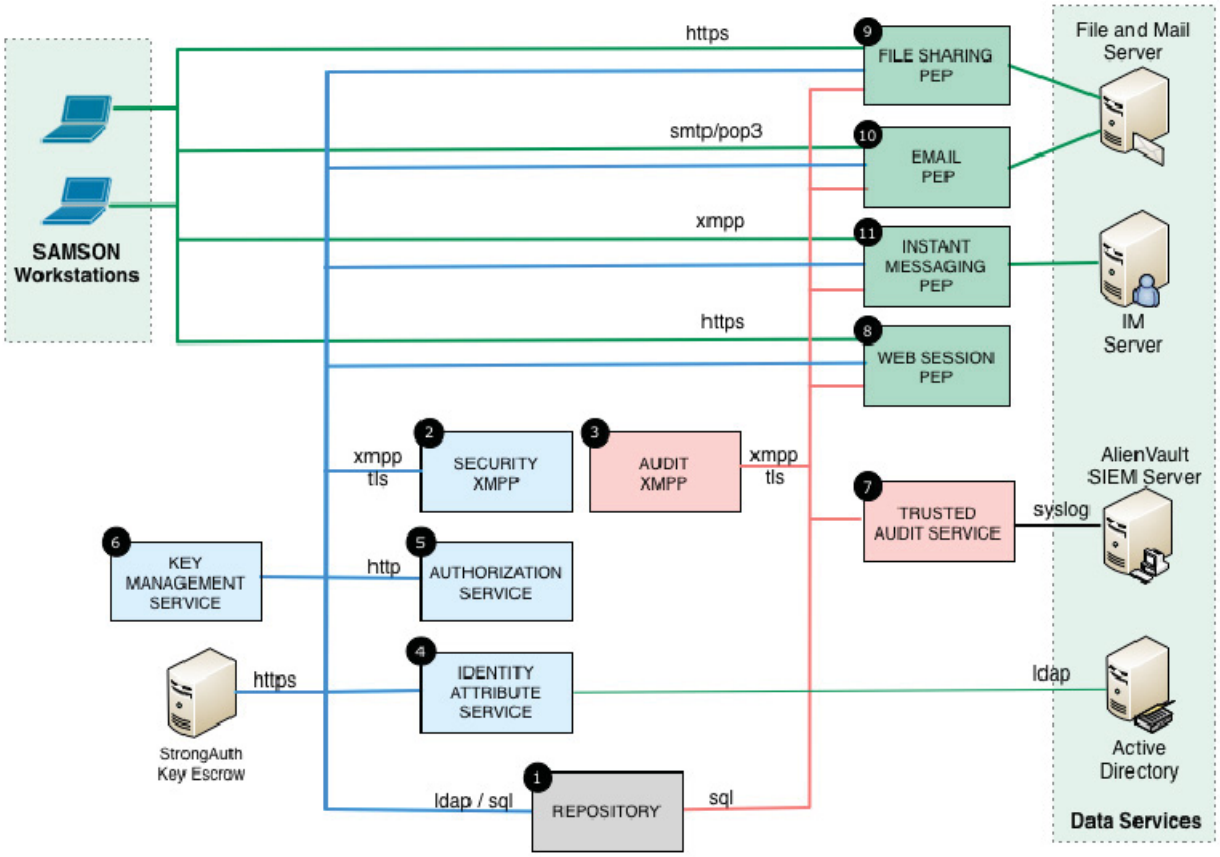
This diagram provides the details of the connectivity between the physical machines and network components.



4 VIRTUAL MACHINE ENVIRONMENT

This diagram provides an overview of the Vitual Machines (VMs).

(The machine numbers 1 -11 in the diagram are defined in the SD-007 Samson Deployment and Configuration Guide)



5 INSTALLATION AND CONFIGURATION TEST ACTIVITIES

5.1 SOFTWARE VERSION CONTROL

Blade System	
XenServer	6.0.210
Samson VM Template	5.0
Management Console	
Windows	7
XenCenter	6
Workstations/Laptops	
Windows	7
Microsoft Office	2007
Titus Doc Classification	3.5
Titus Msg Classification	3.5
Transverse Client	1.5.2

ThirdParty	
Package	Version
Microsoft Active Directory	2008
Titus MS Office Plugin	3.5
AlienVault (SIEM)	4.1
Windows File Server	2008
StrongAuth SKLES	Build 50;Centos 5.5
MS Exchange	2007

Repository	
Package	Version
CENTOS	6.3
DNS Services (Dnsmasq)	2.63
OpenLDAP	2.4.34
Mysql	5.6.10

Security Messaging Server	
Package	Version
CENTOS	6.3
OpenFire	3.7.1

Audit Messaging Server	
Package	Version
CENTOS	6.3
OpenFire	3.7.1

Identity Attribute Service	
Package	Version
CENTOS	6.3
samsoncode.tar	439

Authorization Service (PDP Server)	
Package	Version
CENTOS	6.3
samsoncode.tar	439

KMS	
Package	Version
CENTOS	6.3
samsoncode.tar	439

Trusted Audit Service	
Package	Version
CENTOS	6.3
samsoncode.tar	439

PEP: File Share	
Package	Version
CENTOS	6.3
filepep.tar	430

PEP: Email	
Package	Version
CENTOS	6.3
emailpep.tar	430

PEP: IM Server	
Package	Version
CENTOS	5
im_pep.tar	430

PEP: Web Session Service	
Package	Version
CENTOS	6.3
websession.tar	430

5.2 ROLES AND RESPONSIBILITIES

Role	Sub-Role	Account Ownership	Responsibilities
Security Officer(SO)		N/A	Observes the installation activities undertaken by the System Administrator
System Administrator (SysAdmin)	all	XenServer Access	All System Administrators have access to the credentials for the XenServer virtualization platform
	installer	VM system root account	Configuration of the networking and application intercepts. Configuration of the startup process for the automated launch of services
		Repository Directory Server root account	Management of the directory server schema and individual organizational unit

Role	Sub-Role	Account Ownership	Responsibilities
			delegated accounts
		Repository Database root account	Management of database creation and individual database accounts
	manager	System account	Deployment and configuration of SAMSON services. Operational account under which all SAMSON processes run.
		XMPP admin accounts	The accounts (2) used to access the OpenFire administrative consoles
SAMSON Administrator (SamAdmin)	idmadmin	A SAMSON user account authenticated via Windows Domain authentication. The idmadmin sub-role is assigned by associating the IAAI_ADMIN caveat to that account.	When holding this caveat, the idmadmin has the policy right to administer SAMSON user caveats through the Identity Attribute Administrative Interface.
	policyadmin	A SAMSON user account authenticated via Windows Domain authentication. The policyadmin sub-role is assigned by associating the PAI_ADMIN caveat to that account.	When holding this caveat, the policyadmin has the policy right to administer SAMSON policies through the Policy Administrative Interface.
	auditadmin	A SAMSON user account authenticated via Windows Domain authentication. The auditadmin sub-role is assigned by associating the ARI_ADMIN caveat to that account.	When holding this caveat, the auditadmin has the policy right to a view SAMSON audit records through the Audit Review Interface.

5.3 INSTALLATION AND CONFIGURATION TESTS

A time to complete the installation and configuration acitivities is provided in the table below. This estimate (9 hours) is based on an installer having a thorough knowledge of the Samson system, strong Centos linux skills, and a solid understanding of the tcp/ip network configurations of Centos VMs in an XenServer environment. If the installer does not have these skill sets, then the time to install could increase substantially. [Note: previous installation experience on complex crypto systems, consisting of four server machines, which make use of one database, one LDAP Directory, and a high number of configuration files requiring modifications can take up to 3 days with a full set of production grade documentation. The Samson system has two databases, one ldap directory, eleven server machines, and many configuration files which need modification. It could take from 22.5 hours up to 37.5 hours for an installer with less experience to install successfully a Samson system from bare metal machines.]

It is assumed that the Test Activities 1.0, 2.0 and 3.0 will be carried out by the hosting organization (CTDC) and no time estimates are provided.

Test Activity No.	Test	Estimated Time to Complete	Pass/Fail (Yes/No)
1.0	**Preparation**		
1.1	Ensure that 2 Blade Servers for the XenServer hypervisors are available.		Pass
1.2	XenServer is installed on the Blade Servers		Pass
1.3	A XenCenter is installed on a machine and is available and configured to permit control of the XenServer machines.		Pass
1.4	A Samson VM Template is available with all the software required to complete the install and configuration process.		Pass
1.5	The Samson Deployment and Configuration document latest version is available.		Pass
2.0	**Target Environment Preparation**		
2.1	There is an Active Directory system present in the target environment		Pass

Test Activity No.	Test	Estimated Time to Complete	Pass/Fail (Yes/No)
	with a specific OU for Samson.		
2.2	The user workstations/laptops used in the SAMSON environment are joined to the Windows domain		Pass
2.3	A set of user accounts have been set up in the domain?		Pass
2.4	Within the domain, SAMSON has use of one of the AD extensionAttribute schema values associated with domain users		Pass
2.5	Individual user workstations/laptops have the Titus 3.5 labelling software (Document and Message labelling plus-ins for Microsoft Office) installed and the Titus software has been configured to use the extensionAttribute value for AD queries?		Pass
2.6	File Sharing: A Microsoft File and Print Sharing file share is present? A separate domain account has been created with read/write privilege on this file share for Samson Users.		Pass
2.7	Email: An SMTP/POP3 based mail server is present in the environment. The SMTP and POP3 services have been enabled.		Pass
2.8	Instant Messaging: An IM server with chatrooms is present in the environment		Pass

Test Activity No.	Test	Estimated Time to Complete	Pass/Fail (Yes/No)
2.9	The IM server is using the Windows domain for its user account base and a separate domain account called "spectrum" has been established for the domain.		Pass
3.0	**Samson Hardware Preparation**		
3.1	The 2 Blade servers are available with: dual quad core processors (8 cores), 16GBRAM 4 physical NICs 160GB storage		Pass
3.2	A 24-port Managed Switch is available and configured with four 6 port VLANs (MGMT network, DATA network, SECURITY network, and AUDIT network.)		Pass
3.3	3 desktop/laptop systems are available? (1 for the management console (on the MGMT network)); (2 for domain workstations (on the DATA network))		Pass
3.4	Is a StrongAuth appliance available		Fail
3.5	Alternate Crypto Database is available for installation (if StrongAuth is not available)?		Pass
3.6	All required Hardware is available as per Section 3.2.1 of the Deployment and Configuration Guide?		Pass

Test Activity No.	Test	Estimated Time to Complete	Pass/Fail (Yes/No)
3.7	Checklist of Configuration Elements has been completed	60 min	Pass
3.8	Define IP Addresses for each Machine and complete the Machine Network Configuration Table	30 min	Pass
4.0	**Creating Samson Machines**		
4.1	Has a VM on the XenServer been created by the "installer" from the VM Template (as per Section 4.2.1 of the Deployment and Configuration Guide)?	15 min	Pass
4.2	Has the Networking for the VM been configured by the "installer" as per Section 4.2.2 of the Deployment and Configuration Guide?	10 min	Pass
5.0	Repository Machine		
5.1	Has the Repository Virtual Machine been created by the "installer" as per Section 5.1 of the Deployment and Configuration Guide?	30 min	Pass
5.2	Have the MySQL, OpenLDAP, and the DNS Services been started by the "installer"?	5 min	Pass
6.0	Security Machine		
6.1	Has the Security Machine been created by the "installer" and configured as per Section 5.2 of the Deployment and Configuration Guide?	15 min	Pass
6.2	Is the Security Machine listening on ports 5222, 5223, and 9091		Pass
7.0	Audit Machine		

Test Activity No.	Test	Estimated Time to Complete	Pass/Fail (Yes/No)
7.1	Has the Audit Machine been created by the “installer” and configured as per Section 5.3 of the Deployment and Configuration Guide?	10 min	Pass
7.2	Is the Audit Machine listening on ports 5222, 5223, and 9091		Pass
8.0	Security Gateways		
8.1	Has an Identity Attribute Machine been created by the “installer” as per Section 6.1 of the Deployment and Configuration Guide?	30 min	Pass
8.2	Has an Authorization Machine been created by the “installer” as per Section 6.2 of the Deployment and Configuration Guide?	10 min	Pass
8.3	Has the Key Management Machine been created by the “installer” as per Section 6.3 of the Deployment and Configuration Guide?	10 min	Pass
8.4	Option 1:Using local key storage (6.3.1) Option 2:Using StrongAuth (6.3.2)	10 min (Option 1)	Pass
8.5	Has the Trusted Audit Machine been created by the “installer” as per Section 6.4 of the Deployment and Configuration Guide?	5 min	Pass
8.6	Has a PEP been created by the “installer” with a dispatcher installed as per Section 7.1 of the Deployment and Configuration Guide?	10 min	Pass
8.7	Verify the Dispatcher Testing has been carried out successfully by the “installer” as per Section 7.1.2 of the Deployment and Configuration	15 min	Pass

Test Activity No.	Test	Estimated Time to Complete	Pass/Fail (Yes/No)
	Guide?		
8.8	Has a File Service PEP been created successfully by the “installer” as per Section 7.2 of the Deployment and Configuration Guide?	15 min	Pass
8.9	Has an Email PEP been created successfully by the “installer” as per Section 7.3 of the Deployment and Configuration Guide?	15 min	Pass
8.11	Has an IM PEP been created successfully by the “installer” as per Section 7.4 of the Deployment and Configuration Guide?	15 min	Pass
8.12	Has a Web Session PEP been created successfully by the “installer” as per Section 7.5 of the Deployment and Configuration Guide?	60 min	Pass
8.13	Were the Samson Web Services certificates generated and installed successfully by the “installer” as per Section 7.5.1 of the Deployment and Configuration Guide?	15 min	Pass
	Total Time = Complete system setup + Creating each machine * 10 (Section 4.2.1 and Section 4.2.2)	295 min (4 hours 55 mins) + 250 min (4 hrs 10 min) Total Setup Time = 9hrs 5 min	

6 FUNCTIONAL TESTS

The activities associated with the conducting of the Functional Tests are provided in this section.

6.1 FUNCTIONAL TESTS PREPARATION

Test Activity No.	Test Preparation	Roles	Time	Pass/Fail (Yes/No)
	As the "manager" establish a number of Samson test users in AD	manager	10 min	Pass
	Establish a number of Samson test users in the Samson Directory Server	idmadmin	5 min	Pass
	Assign caveats to the Samson test users in the Directory Server	idmadmin	5 min	Pass
	Develop Samson Policies to be used in the functional tests	policydmin	10 min	Pass
	As a Samson user create a number of Word documents on the protected File Server with various caveat designations.	Samson User	15 min	Pass
	Carry out the functional tests for File Services	All	20 min	Pass

6.2 FILE SERVICES FUNCTIONAL TESTS & RESULTS

6.2.1 TESTS & RESULTS - FILE SERVICES

Control end user access and functionality to file resources (Microsoft Word documents) on a common file server using the users and resource assigned caveats in conjunction with established SAMSON Policy rules.

6.2.2 SPECIAL REQUIREMENTS

Four users were set up within the IDM system, by the "idmadmin", with the caveats as indicated:

TestUser1 (ottawa) caveat=ceo

TestUser2 (toronto) caveat=ceo, canus

TestUser3 (chicago) caveat=ceo,canus

TestUser4, (newyork) caveat=canus.

Policies were controlled by a "policyadmin" and audit records were viewed by the "auditadmin".

The Titus plugin and interface to Microsoft Word 2007 was used to select user assigned caveats to the resources.

6.2.3 ASSUMPTIONS

Users are authenticated by the Microsoft Active Directory. Windows Explorer was used to access the resources on the File Server. The testing was carried out on file level resources not at the folder level.

6.2.4 USER INTERFACE

In normal use, SAMSON users will access the file server through Windows 7, Windows Explorer file manager application, and the Microsoft Word 2007 application

SAMSON Policies will prevent users from seeing the existence of files to which they are not in the Community of Interest (ceo and/or canus) entitled.

6.2.5 INSTALLATION AND SETUP

Through the windows File Server mapped network drive there is one folder called "data" that the test user will obtain access to by logging into using their Windows AD account.

The data folder was populated with a number of user Word documents and based on the users assigned caveats – caveats were attached to the Word document;

6.2.6 ASSURANCE

Assurance that the SAMSON services are performing in accordance with the user and file objects assigned caveats and the authorization policy rules, was confirmed by the "auditadmin" reviewing the Audit records for the transcations.

6.2.7 TEST COVERAGE MATRIX

Userid	Policy Actions	Nationality	UserCaveat	Clearance	Resource Caveat	Result (Pass/Fail)
other1	user is denied all access	other	none	secret	ceo,canus	Pass
ottawa	user has read only access to resources labelled ceo	can	ceo	secret	ceo	Pass
ottawa	user has full access to ceo; no access to canus	can	ceo	secret	ceo	Pass
newyork	user has no access to ceo; read only access to canus	can	canus	secret	canus	

Userid	Policy Actions	Nationality	UserCaveat	Clearance	Resource Caveat	Result (Pass/Fail)
toronto	user has read only access to ceo and canus	can	canus,ceo	secret	canus,ceo	
chicago	user has full access to ceo; read only access to canus	can	ceo,canus	secret	canus,ceo	
newyork	user has no access to ceo; full access to canus	us	canus	secret	canus	
chicago	user has full access to canus; read access to ceo	us	canus,ceo	secret	canus,ceo	
toronto	user has full access to ceo and canus	can	canus,ceo	secret	canus,ceo	

6.3 INSTANT MESSAGING TESTS & RESULTS

6.3.1 OBJECTIVE

Instant Messaging (IM) testing was carried out only on the IM Client to Server;

The IM Client to Server component was tested by setting up a conference room and ensuring that:

- specific users can enter a conference room, which has been assigned a specific caveat;
- other users can join the conference room;
- be denied access to the conference room; or
- unable to see the plain text messages between Samson protected users.

6.3.2 TEST COVERAGE MATRIX:

The test cases explored combinations of valid and invalid boundary values for conditions being tested.

All user interfaces were through the TransVerse IM client application.

The following users, policies and caveats were used for the IM Services:

Users: ottawa, georgew, johna

Policies: CEO,(read, write); CANUS,(read,write)

Conference Room Caveats: CEO or CANUS

Marked-Up Conference Room Caveats: CEO or CANUS

Results: Rx=user received; tx= user transmits; tx(ceo) [indicates a Marked Up CEO caveat multi-user conference]; no msg indicates that the users chat room window displayed no message.

The Instant Messaging application services test matrix is as follows:

Chat Room Caveat (ceotestroom1)	user1	policy	user1 idm caveats	user2	user2 policy	user2 idm caveats	user3	user3 policy	usr3 idm caveats	Result
Ceo	georgew	ceo,canus	canus	ottawa	ceo, canus	ceo	johna	ceo, canus	ceo, canus	
	Action	Result		Action	Result		Action	Result		
	tx	rx			rx			rx		
		rx		tx	rx			rx		
		rx			rx		tx	rx		
	tx(canus)	rx			rx			rx		
		rx		tx(canus)	rx			rx		
		rx			rx		tx(canus)	rx		
	tx(ceo)	rx			rx			rx		
		rx		tx(ceo)	rx			rx		
		rx			rx		tx(ceo)	rx		

6.4 EMAIL TESTS & RESULTS

6.4.1 OBJECTIVES

The E-Mail Messaging Tests were carried out to validate the capability of the SAMSON TD system to:

Control access to Outlook client message sender and recipients to E-Mail service resources on a Microsoft Exchange Server 2007 SP1 using the sender/recipient users and message resources with attachments, with assigned caveats in conjunction with established SAMSON Policy rules.

6.4.2 SPECIAL REQUIREMENTS

Four users were set up within the IDM system with the caveats as indicated:

TestUser1 (ottawa) caveat=ceo,canus

TestUser2 (chicago) caveat=ceco,canus

TestUser3 (toronto) caveat=ceo,canus

TestUser4 (newyork) caveat=ceo,canus

Policies were controlled by the "policyadmin" and audit records were viewed by the "auditadmin".

The Titus plugin and interface to Microsoft Outlook Client 2007 was used to select user assigned caveats to the message resources.

6.4.3 ASSUMPTIONS

Users were authenticated by the Microsoft Active Directory. Files used for attachments were stored in the SAMSON Windows File server data folder under "at rest" encryption protection. The testing was carried out on messages with no attachments.

6.4.4 USER INTERFACE

In normal use, SAMSON users access the E-Mail Services through Windows 7, Microsoft Outlook Client, and the Titus Trusted Labelling Service provides the message caveats available to the sender through the Outlook Client application.

SAMSON Policies prevent senders attaching files within the Windows File Server data folder, to which they are not in the Community of Interest (ceo and/or canus).

6.4.5 E-MAIL – FUNCTIONAL TESTS AND RESULTS

Single Sender to Single Recipient – No attachments

Test Case #	Sender	Sender	Sender	Recipient	Recipient	Msg	Attachment	PDP Decision	Results
	name	idm caveat	policy	name	policy	caveat		permit	Pass/Fail
1	toronto	ceo,canus	ceo	chicago	ceo	ceo	none	**y**	msg delivered to sender
2	toronto	ceo,canus	ceo	Chicago	ceo	canus	none	n	sender policy violation canus recipient cannot receive ceo msg
3	toronto	ceo,canus	ceo	Chicago	canus	ceo	none	n	
4	toronto	ceo,canus	ceo	chicago	canus	canus	none	n	
5	chicago	canus	canus	toronto	ceo	ceo	none	n	sender chicago with an idm caveat of canus only; cannot select msg with a ceo caveat
6	chicago	canus	canus	tormto	ceo	canus	none	n	
7	chicago	canus	canus	toronto	canus	ceo	none	n	sender chicago with an idm caveat of canus only; cannot select msg with a ceo caveat
8	chicago	canus	canus	toronto	canus	canus	none	**y**	

7 NON FUNCTIONAL TESTS

7.1 PERFORMANCE

The objectives for performance of resources will be met by the generation of system input loads emulating systems type input conditions and the measurement of processes related to the input conditions, in terms of throughput, response times and utilization of resources. This will be augmented, where appropriate, by the use of modeling techniques to assist in determining the scaling requirements of Samson infrastructure components. This combination of actual measurements and modeling techniques will produce results, which will assist CTDC Engineers/Architects to provide cost effective solutions.

The performance tests will determine the storage capacity required for audit records.

7.2 MODELLING

The use of modeling techniques to predict or estimate performance, and scalability will be used.

7.3 TYPES OF TESTS

The types of non functional tests conducted will be:

Performance Testing – This type of testing collects data in terms of throughput, response times and utilization i.e. the number of transactions per second (TPS) and the transaction response time (TRT) (average/median/90 percentile, minimum, maximum,) the system can deliver over a range of system loads, measured by average percentage CPU utilization.

The performance tests will be carried out using a number of clients, up to 5, to provide the level of concurrency. The output will be measured for transaction response time and throughput with up to the 5 users concurrently carrying out transactions. An average throughput for the operation will be recorded. This test scenario will provide an indication of performance metrics, which can be used to calculate the maximum number of users that can carry out the specific process at the same time before the configuration requires additional resources or reconfiguration. The performance metrics will be tabulated in the format shown in the table below.

Number of Clients	CPU (%age util)	Average Response Time (milliseconds)	Throughput (users /sec)
1			
3			
5			

7.4 PERFORMANCE TEST RESULTS

7.4.1 EMAIL

An email message Python test tool was developed to generate user send SMTP traffic, and a user retrieve POP call. Two sets of performance numbers were collected one with no Samson email components in the system message flow and the other with the Samson email PEP in the system message flow. This provided an indication of the Samson email PEP overhead. The tests were conducted with no attachments, with a 250Kbyte attachment and with a 850Kbyte attachment to determine the impact of attachment size on the Samson email PEP.

The results in terms of throughput (messages per second) and response time for each message (seconds per message) are provided in the following tables.

No Samson Email PEP in the Message Flow

total msgs sent or retrieved	Msgs per user	Users	Attachment Size	Time (secs)	protocol	CPU (%age)	Disk (blk/sec)	Throughput (msgs/sec)	Response time per msg (secs/msg)
25	25	1		0.43	smtp	No SAMSON mediation		58.14	0.02
75	25	3		1.48	smtp			50.68	0.02
125	25	5		1.88	smtp			66.49	0.02
25	25	1	250KB	2.11	smtp			11.85	0.08
75	25	3	250KB	3.98	smtp			18.84	0.05
125	25	5	250KB	6.98	smtp			17.91	0.06
25	25	1	850KB	6.17	smtp			4.05	0.25
75	25	3	850KB	11.64	smtp			6.44	0.16
125	25	5	850KB	20.49	smtp			6.10	0.16
25	25	1		0.14	pop			178.57	0.01
225	25	3		1.12	pop			200.89	0.00
625	25	5		2.36	pop			264.83	0.00
25	25	1	250KB	1.78	pop			14.04	0.07
225	25	3	250KB	8.01	pop			28.09	0.04

total msgs sent or retrieved	Msgs per user	Users	Attachment Size	Time (secs)	protocol	CPU (%age)	Disk (blk/sec)	Throughput (msgs/sec)	Response time per msg (secs/msg)
625	25	5	250KB	18.35	pop			34.06	0.03
25	25	1	850KB	5.83	pop			4.29	0.23
225	25	3	850KB	23.57	pop			9.55	0.10
625	25	5	850KB	52.21	pop			11.97	0.08

With the Samson Email PEP

total msgs sent or retrieved	Msg per user	Users	Attachment Size	Time (secs)	protocol	CPU (%age)	Disk (blk/sec)	Throughput msgs/sec	Response time per msg secs/msg
25	25	1		163	smtp	16.7	345	0.15	6.52
75	25	3		207	smtp	21.51	584	0.36	2.76
125	25	5		259	smtp	25.28	900	0.48	2.07
25	25	1	250KB	209	smtp	18.74	1165	0.12	8.36
75	25	3	250KB	309	smtp	24.61	3049	0.24	4.12
125	25	5	250KB	410	smtp	31.44	7123	0.30	3.28
25	25	1	850KB	217	smtp	19.65	3578	0.12	8.68
75	25	3	850KB	319	smtp	31.25	27593	0.24	4.25
	25	5	850KB		smtp				
25	25	1		103	pop	16.6	122	0.24	4.12
225	25	3		310	pop	23.39	334	0.73	1.38
625	25	5		520	pop	31.32	3173	1.20	0.83
25	25	1	250KB	121	pop	18.97	1410	0.21	4.84
225	25	3	250KB	333	pop	32.47	4059	0.68	1.48

total msgs sent or retrieved	Msg per user	Users	Attachment Size	Time (secs)	protocol	CPU (%age)	Disk (blk/sec)	Throughput msgs/sec	Response time per msg secs/msg
625	25	5	250KB	563	pop	42.23	23368	1.11	0.90
25	25	1	850KB	124	pop	24.2	20159	0.20	4.96
225	25	3	850KB		pop				
625	25	5	850KB		pop				

The results indicate that with one user sending an email with no attachments, without a Samson email PEP in the message flow, it takes 0.02 secs to send the message and 0.01 secs to retrieve the message. With the Samson Email PEP active in the message flow, with one user and no attachments it takes 6.52 secs to send the message and 4.12 secs to retrieve the message.

The email message throughput graph, Figure 4, indicates the throughput rate of the email system when the Samson email PEP is intercepting the traffic. A trendline is shown with a 250KB attachment, which indicates that approximately 20 concurrent users would generate a throughout rate of approximately 0.5 message per second. On the single CPU virtualized email PEP server, the maximum CPU utilization achieved was just over 30%.

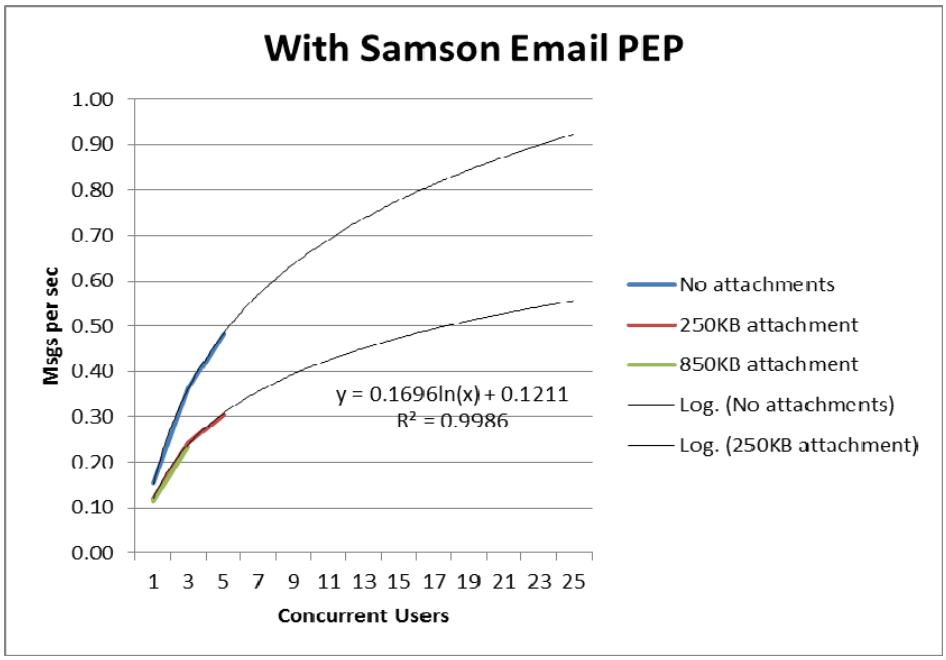
Based on the Microsoft MAPI Messaging Benchmark (MMB3) Model for the Exchange Server: Each user will send 84 messages per 8 hour work day with an average size message size of 74.9KB. Based on this, the number of users that can be supported by a Microsoft Exchange Server integrated with Samson, with a message throughput rate of 0.5 messages per second is:

Messages per day = 0.5 * 8 * 60 * 60 = 14,400 msgs per day;

Number of users = 14,400/84 = 171 users

The current configuration of the Samson Email environment will support up to 171 Outlook users, as outlined in the Email test results and calulations.

Figure 4: Email Throughput with the Samson Email PEP



Further, using an Email Message Throughput rate of 0.5 email per second (30 emails per minute), the user community size, number of active users, and session time can be calculated from the model:

Email Msg Throughput = (Total Number of Users * %age Active Users)/Session Time

> The Email performance test results show that the Samson Email Services will support a user community size of 1000 users, where 150 are active in sending and receiving an email every 5 minutes.

It should be recognized that the current DRDC test environment is scaled as an entry level system, with minimum CPU and memory allocation per virtualized server.

The metrics obtained indicate that the introduction of the Samson email PEP and services can introduce an overhead of up to 8 seconds per message. This is without any tuning of the system. The Samson Email PEP and associated backend services are very busy carrying out:

- the intercept to obtain a copy of the message;
- decoding the message to get the attachments;
- starting a dispatcher for this transaction;
- carrying out the policy check;
- generating a new key and storing it;
- retrieving that key;

- carrying out the encryption;
- re-encoding and re-wrapping the new encrypted email;
- getting the intercept to re-read the new message and send it off to the server; and
- generating an audit record.

Future development activity should address the efficiency of this workload, for example having a number of dispatchers established in a "pool" eliminating a dispatcher start up cost, more efficient cryptographic key generation and management, etc.

7.4.2 INSTANT MESSAGING

A Python Instant Messaging (IM) test tool was developed to generate multiple user chat messages to a Samson protected chatroom with multiple Samson users resident in the chatroom. Two sets of performance numbers were collected one with no Samson IM components in the chat message flow and the other with the Samson IM PEP in the chat message flow. This provided an indication of the Samson IM PEP overhead. The tests were conducted with all users generating 500 chats, with no think time or user keyboard time. The time taken from the start of the first chat message being sent to the last chat message received was recorded.

The results in terms of throughput (chats per second) and response time for each chat (seconds per message) are provided in the following tables.

No Samson IM PEP

Total No of chat msgs sent & received	Chats per user sent	Clients	Time (secs)	Chats per sec	Secs per chat
1500	500	2	20.9	72	0.01
2000	500	3	21.3	94	0.01
3000	500	5	21.7	138	0.01

With the Samson IM PEP

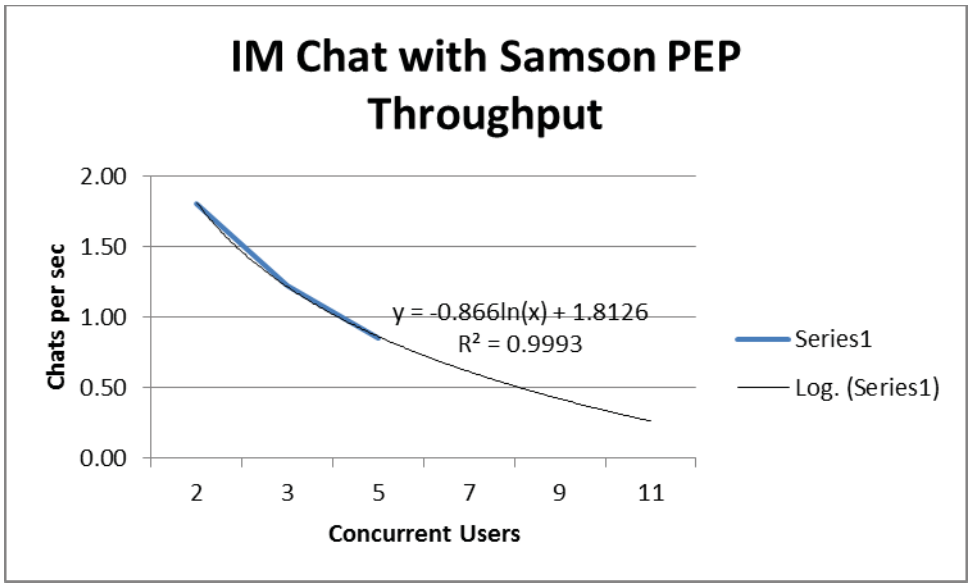
Total No of chat msgs sent & received	Chats per user sent	Clients	Time (secs)	CPU (%age)	Disk (blks/sec)	Chats per sec	Secs per chat
1500	500	2	830	16.24	973	1.81	0.55
2000	500	3	1630	12.77	1890	1.23	0.82
3000	500	5	3520	19.37	1058	0.85	1.17

The results indicate that with 5 users, a throughput rate of 0.85 chats per second or 51 chat messages per minute can be sustained. Using a Chat Throughput rate of 50 chat messages a minute the user community size, number of active users, and chat session time can be calculated from the model:

Chat Throughput = (Total Number of Users * %age Active Users)/Chat Session Time

> Based on the test results and model calculations the Samson IM PEP can support a user community of 1000, where 150 are active and carrying out a chat session every 20 seconds.

Figure 5: Samson IM Throughput



The shape of the graph in Figure 5 indicates that the IM system with the Samson IM PEP is not scaling effectively. An investigation into this revealed that the Spectrum package used as part of the IM PEP was not configured to handle the type of load that was being generated by the test tool. The Spectrum configuration was modified to provide proof of this assertion. In addition, it was found that using the StrongAuth Key Escrow appliance was causing a considerable delay. Future development work should focus on these issues within the IM environment.

7.4.3 FILE SERVICES

A File Services Python test tool was developed to carry out an upload and download of Samson protected files from the mounted drive to a local drive. Two sets of performance numbers were collected one with no Samson file services components in the file transfer flow and the other with the Samson File Services PEP in the file transfer flow. This provided an indication of the Samson File Services PEP overhead. The tests were conducted with 1MByte files.

The results in terms of throughput (files per second) and response time for each file transfer (seconds per message) are provided in the following charts.

No Samson File Services PEP

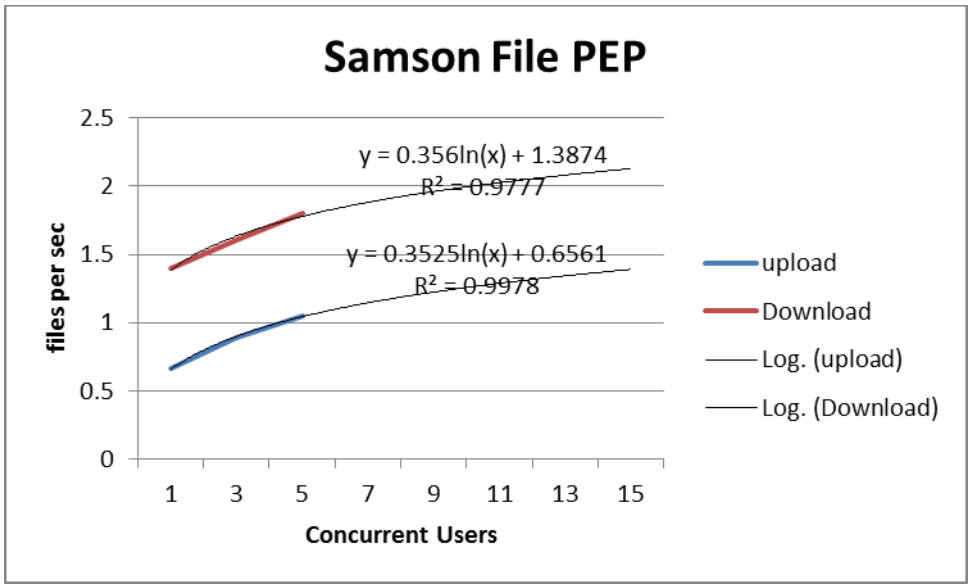
Files	Clients	Time (secs)	File Size	Upload/Download	Throughput (files/sec)	Response Time (Sec/file)
50	1	3.2	1MB	Upload	15	0.064
50	3	7.9	1MB	Upload	19	0.158
50	5	16.1	1MB	Upload	16	0.322
50	1	5.8	1MB	Download	9	0.116
50	3	18.1	1MB	Download	8	0.362
50	5	25.2	1MB	Download	9	0.504

With Samson File Services PEP

Files	Clients	Time (secs)	File Size	Upload/Download	Throughput (files/sec)	Response Time (Sec/file)
50	1	76	1MB	Upload	0.66	0.66
50	3	169	1MB	Upload	0.89	0.30
50	5	239	1MB	Upload	1.05	0.21
50	1	35.7	1MB	Download	1.4	1.40
50	3	92	1MB	Download	1.6	0.54
50	5	138	1MB	Download	1.8	0.36

As shown in Figure 6 below the results can be extrapolated to show that, an average file transfer (upload or download) throughput rate of 1.5 files per second (90 files per min), for 10 concurrent users, can be achieved by the Samson File Services.

Figure 6: Samson File Services Throughput



Using a File Transfer (Upload/Download) Throughput rate of 90 files per minute the user community size, number of active users, and session time can be calculated from the model:

File Transfer Throughput = (Total Number of Users * %age Active Users)/Session Time

The file transfer performance test results show that the Samson File Services will support a user community size of 1000 users, where 400 are active in transferring (uploading or downloading) a 1 MByte file every 5 minutes.