White Paper

Securing Storage Infrastructure

A Summary of the Security Features Offered by SGI® Storage Area Management Solutions

Table of Contents

1.0 Executive Summary

To maximize productivity and remain competitive in today's 24/7 on-demand enterprise, employees, customers, partners and suppliers, both inside and outside the company, need continuous access to data. Providing this access means that the underlying storage infrastructure must be highly available. Unfortunately, when it comes to making the service vs. security trade-off, service often wins out. As a result, storage security has traditionally been given short shrift within most enterprises.

But with regulatory compliance and auditing requirements moving to the forefront, and the threat of internal and external breaches becoming greater by the day, locking down storage infrastructure is becoming an increasingly important consideration for IT and business professionals. The challenge often faced, however, is how to maintain high levels of service and security when dozens of point tools are required to monitor, configure, and provision the heterogeneous servers, HBAs, fabric switches, and storage systems that make up today's multi-vendor storage infrastructures. To maintain service levels, a large number of IT administrators are given access to these point tools, none of which are integrated, and many of which lack security. Equally important in today's challenging economic climate is how to accomplish this without a corresponding increase in staff or budget. Given these conflicting business requirements, an important consideration when selecting and implementing a storage area management solution family should be security.

SGI InfiniteStorage® Resource Manager Suite, SGI's integrated family of Storage Resource Management (SRM) and SAN management solutions, offers comprehensive security capabilities that secure storage infrastructure while at the same time reducing operating costs and simplifying management. With SGI solutions, IT organizations can centrally manage storage security, limit access to specific SAN management features and storage elements, audit storage infrastructure changes, reduce the risk of security breach, and deliver even higher levels of service and data and application availability. This white paper summarizes the security features offered SGI InfiniteStorage Resource Manager (ISRM).

SGI InfiniteStorage Resource Manager

- SGI ISRM workgroup includes integration of CXFS + DMF
- SGI ISRM Enterprise Edition- complete enterprise solution with enterprise features

2.0 Web Browser Security

All SGI features, including active provisioning and configuration are delivered through any Java-enabled Web browser. The result is a zero-footprint administrative client that eliminates the costly and time-consuming need to update IT administrator's desktops with proprietary "thick" clients, and makes it easier for more IT staff and business unit constituents to use SGI software for true "anytime, anywhere" management.

The Web services-based architecture of SGI's storage area management platform offers built-in security advantages. Storage administrators can open a Web browser connection to the management server. Authentication is done with a username and password administered either within SGI InfiniteStorage Resource Manager (ISRM) or with a directory service such as LDAP or Active Directory (AD). If an SSL connection is used, the authentication data is encrypted. All of the Java applets that are downloaded as part of the user interface are digitally signed. In compliance with web standards, the software asks the user about accepting keys from non-recognized authorities.

By default, the management server uses the industry-standard port numbers: 443 for HTTP/s and port 80 for HTTP (non-SSL) connections. Port numbers can be modified at any time, and users can be forced to use SSL if desired.

If you are running SGI ISRM integrated with HP-SIM, only HTTP/s access is supported by default.HP-SIM uses port 50000 and will transparently redirect SGI ISRM requests to port 443.

Figure 1. All the features of SGI InfiniteStorage Resource Manager are delivered through a Web browser and a secure HTTPS connection controlled by username and password authentication pairs. In compliance with the Storage Management Initiative Specification (SMI-S), SGI software asks users authenticating via HTTPS about accepting keys from non-recognized authorities.

3.0 Embedded Database Security

The SGI® platform features an embedded Oracle database that collects asset, capacity, performance, and configuration information on every element of the storage infrastructure. The Oracle database schema is modeled according to the Common Information Model (CIM) standard so that all heterogeneous storage infrastructure elements can be visualized, navigated, monitored, provisioned, and reported on in a consistent manner. The database is only accessed by SGI ISRM software, and requires authentication for both read and write access.

3.1 Database Passwords

The database accounts that have access to the Oracle database are protected by passwords which can be changed at any time. Changing these passwords is considered a best practice, and should be done upon installation. These passwords are stored in a file on the SGI ISRM server. This file is encrypted using the Blowfish algorithm. The encryption/decryption key is hard coded into the SGI ISRM management software and is obscured through binary compilation.

3.2 SGI InfiniteStorage® Resource Manager User and Device Credentials

Users of SGI ISRM Suite are managed by storing their individual user IDs, 3DES-encrypted passwords, and user attributes in tables in the Oracle database. However, if SGI ISRM is integrated with HP-SIM, HP-SIM will perform all user authentications.

Similarly, credentials used to discover devices and applications are also 3DES-encrypted in the Oracle database.

Every installation of SGI ISRM has a unique decryption key that is stored partially in the Oracle database and is partially hard-coded in the SGI ISRM software.

4.0 Managed Business Application Security

SGI management solutions include optional Application Modules that correlate business application performance and availability with the health of underlying host servers, HBAs, fabric switches, and storage systems to facilitate root cause analysis, prevent unplanned downtime, and ensure business continuity. This section details the interactions between the SGI ISRM server and each supported managed business application.

Business Application	Communications	Network	Authentication
Oracle Database	SGI ISRM management server communicates with Oracle instances using Oracle database links.	Communication is via TNS. The default TNS port is 1521.	A user named appiq_user is created by a script provided with SGI ISRM. This user has read access to the data dictionary tables. The appiq_user account is authenticated by a password. Any password can be used, but all managed databases must have the same password.
Sybase Adaptive Server Enterprise	SGI ISRM management server communicates with Oracle instances using Oracle database links.	Communication is via ODBC. The default port is 5000.	A user named appiq_user is created by a script provided with SGI ISRM. This user account is created in the master database with read permission to view all master tables (which is the holder of the data dictionary objects) The appiq_user account is authenticated by a password. Any password can be used, but all managed databases must have the same password.
Microsoft SQL Server	SGI ISRM management server communicates with Oracle instances using Oracle database links.	Communication is via ODBC. The default port is 1433.	A user named appiq_user is created by a script provided SGI ISRM. This user account is created in all databases with read permission to view all tables. The appiq_user account is authenticated by a password. Any password can be used, but all managed databases must have the same password.

Business Application	Communications	Network	Authentication
Microsoft Exchange	SGI ISRM communicates with the Active Directory Service on the configured root domain controller for Exchange discovery	SGI ISRM communicates over LDAP with the Active Directory service listening on port 389	SGI ISRM binds to the Active Directory service through LDAP for user authentication. For configuring Exchange information during discovery setup: 1. Primary domain controller should be a DC from the root domain. 2. A user should be created within the root domain and its RD should be used to specify the “User Name” entry. * It’s the RDN of the domain user, not its Windows logon name. RDN is Relative Distinguished Name. For example, a DN for a Windows user might look like: CN=svcacct_sgise, CN=Users, DC=sgi, DC=com The RDN is “svcacct_sgise” * The user should have enough privilege to browse the Exchange container within the Active Directory’s Configuration naming context (eg. Exchange View Only Administrator role). A root domain administrator will have more than enough privilege to qualify.

5.0 Managed Host Server Security

SGI management solutions discover, monitor, and report on host servers and their operating systems, and correlate server performance and availability with the health of underlying HBAs, fabric switches, and storage systems. This section details the interactions between the SGI ISRM management server and each supported host operating environment.

Operating System	Communications	Network	Authentication
All	SGI ISRM includes CIM Extensions (agent software) for all supported host environments. The management server communicates with these CIM Extensions via TCP socket connections. An IP connection is required from the SGI ISRM management server to each host under management during communications. All communications with the CIM Extensions is encrypted using SSL technology.	The SGI ISRM management server communicates with the CIM Extensions on TCP port 4673. This port number can be modified using the –port flag. If the –mgmtServerIP command-line option is used, only connection from a designated IP address will succeed.	The administrator has the choice of using any valid account and password on the host, or of setting up pseudo-credentials. Pseudo-credentials represent a name and password that are stored on the host in a text file. These credentials are only used to authenticate the user of the CIM Extensions. They have no connection to real users of the host.

SGI ISRM includes an optional deployment tool to simplify deployment and management of CIM Extensions to hosts. This works over ssh, which uses port 22 by default.

6.0 Managed Switch / Director Security

SGI management solutions discover, monitor, provision, and report on fibre channel fabric switches and directors, and manage their complex paths and interdependencies with business applications, host servers, HBAs, other fabric switches, and storage systems. This section details the interactions between the SGI ISRM management server and each supported switch.

Switch/Director	Communications	Network	Authentication	Credentials
Brocade -API	The SGI ISRM management server communicates with Brocade's family of Fibre Channel switches and directors via the Brocade Fabric Access API. An IP connection is required from the SGI ISRM management server to a single switch on each distinct fabric during communications.	The SGI ISRM management server communicates with Brocade switches primarily via remote procedure calls. Port 111 is a port mapper that determines the RPC ports to use: For Fabric OS v3.1+/4.1+: port 897, 898 For all other Fabric OS versions: ports 600–1023 Some data is received via HTTP on port 80.	User ID and password credentials are authenticated via the Brocade Fabric Access API. If there is a PKI certificate installed on the switch, the credentials are encrypted; otherwise, they are encoded.	Switch user credentials with full fabric administrative privileges are required to deliver the full range of switch and fabric management capabilities.
Brocade – SMI-S	The SGI ISRM management server communicates with Brocade's family of Fibre Channel switches and directors via the Brocade SMI-S provider. An IP connection is required from the SGI ISRM management server to the server that's running the SMI-S provider.	The SGI ISRM management server communicates with the Brocade SMI-S provider on ports 5988 and 5989.	User ID and password credentials are encrypted during submission to the SGI SMI-S EVA Provider server. No unencrypted login or password information is exchanged over the wire.	Switch user credentials with full fabric administrative privileges are required to deliver the full range of switch and fabric management capabilities.
Cisco	The SGI ISRM management server communicates with Cisco's family of fabric switches and directors via SNMP. An IP connection is required from the SGI ISRM management server to the Cisco switch during communications.	SNMP communication with Cisco switches uses ports 161 and 162.	No login is necessary through SNMP	The "Community" name string is the only credential required.
CNT	The SGI ISRM management server communicates with CNT family of fabric switches and directors via SNMP. An IP connection is required from the SGI ISRM management server to the CNT director/switch during communications.	SNMP communication with CNT switches/directors uses ports 161 and 137.	No login is necessary through SNMP.	The "Community" name string is the only credential required.

Switch/Director	Communications	Network	Authentication	Credentials
CNT	The SGI ISRM management server communicates with CNT family of fabric switches and directors via SNMP. An IP connection is required from the SGI ISRM management server to the CNT director/switch during communications.	SNMP communication with CNT switches/directors uses ports 161 and 137.	No login is necessary through SNMP.	The “Community” name string is the only credential required.
McDATA - SWAPI	The SGI ISRM server communicates with McDATA’s family of Fibre Channel switches and directors via the McDATA SWAPI interface. An IP connection is required from the SGI ISRM management server to the SWAPI API server during communications.	The SGI ISRM management server communicates with the SWAPI API server on TCP port 59521.	User ID and password credentials are passed from the SGI ISRM management server to the SWAPI API server via the SWAPI API, and leverage its built-in encryption.	Switch user credentials with full SWAPI API server user credentials are required to deliver the full range of SGI switch and fabric management capabilities.
McDATA - SNMP	The SGI ISRM server communicates with McDATA’s family of fabric switches and directors via SNMP. An IP connection is required from the SGI ISRM management server to the McDATA switch/director or to the McDATA EFC Manager during communications.	SNMP communication with McDATA switches/directors and EFC Manager uses ports 161 and 162.	No login is necessary through SNMP.	The “Community” name string is the only credential required.
QLogic	The SGI ISRM server communicates with QLogic family of fabric switches via SNMP. An IP connection is required from the SGI ISRM management server to the QLogic switch during communications.	SNMP communication with QLogic switches uses ports 161 and 162.	No login is necessary through SNMP.	The “Community” name string is the only credential required.

7.0 Managed Storage System Security

SGI management solutions discover, monitor, provision, and report on external storage systems, and manage their complex paths and interdependencies with business applications, host servers, HBAs, and fabric switches. This section details the interactions between the SGI ISRM management server and supported storage systems.

Storage System	Communications	Network	Authentication	Credentials
EMC Symmetrix and DMX	The SGI ISRM management server communicates with the EMC Symmetrix and Symmetrix DMX family of storage systems via the EMC Symmetrix API. An IP connection is required from the SGI ISRM management server to the EMC Solutions Enabler server during communications.	The SGI ISRM management server communicates with the EMC Solutions Enabler on TCP port 2707.	User ID and password credentials are passed from the SGI ISRM management server to the EMC Solutions Enabler server through the EMC Symmetrix API, and leverage its built-in encryption.	EMC Solutions Enabler user credentials with full administrative privileges are required to deliver the full range of management capabilities.
EMC CLARiiON	The SGI ISRM management server communicates with EMC Clariion storage systems via the EMC Navisphere management software CLI. An IP connection is required from the SGI ISRM management server to each storage system under management during communications. In addition, the IP address of the SGI ISRM management server may need to be added as a trusted host through Navisphere.	The SGI ISRM management server communicates with Clariion storage systems on TCP port 6389.	User ID and password credentials are authenticated in a secure manner via the Navisphere CLI. No unencrypted login or password information is exchanged over the wire.	Navisphere CLI user credentials with full administrative privileges are required to deliver the full range of management capabilities
Hitachi TagmaStore, Lightning, and Thunder; Sun StorEdge 9900	The SGI ISRM management server communicates with Hitachi storage systems via Hitachi's HiCommand Device Manager Server XML API. An IP connection is required from the SGI ISRM management server to the HiCommand server during communications.	The SGI ISRM management server communicates with the HiCommand server on TCP port 2001.	User ID and password credentials are encrypted during submission to the HiCommand server. No unencrypted login or password information is exchanged over the wire.	HiCommand user credentials with full administrative privileges are required to deliver the full range of management capabilities.
HP XP Series	The SGI ISRM management server communicates with HPI XP series arrays via HP StorageWorks Command View Advanced Edition (AE) and HP StorageWorks Command View device management software or directly through the RMI interface. An IP connection is required from the SGI ISRM management server to the StorageWorks Command View server during communications.	The SGI ISRM management server communicates either directly through the RMI interface or with the HP StorageWorks Command View AE server on TCP port 2001 or with the older CommandView server on port 5988.	User ID and password credentials are encrypted during submission to the the StorageWorks Command View server. No unencrypted login or password information is exchanged over the wire.	StorageWorks Command View user credentials with full administrative privileges are required to deliver the full range of management capabilities.
HP EVA Series	The SGI ISRM management server communicates with HP EVA series arrays via the HP SMI-S EVA Provider. An IP connection is required from the SGI ISRM management server to the HP SMI-S EVA Provider server during communications.	The SGI ISRM management server communicates with the HP SMI-S EVA Provider server on TCP port 5988.	User ID and password credentials are encrypted during submission to the HP SMI-S EVA Provider server. No unencrypted login or password information is exchanged over the wire.	HP SMI-S EVA Provider credentials with full administrative privileges are required to deliver the full range of management capabilities.

Storage System	Communications	Network	Authentication	Credentials
HP MSA Series	The SGI ISRM management server communicates with HP MSA series arrays via the HP MSA SMI-S Provider. An IP connection is required from the SGI ISRM management server to the HP MSA SMI-S Provider server during communications.	The SGI ISRM management server communicates with the HP MSA SMI-S Provider server on TCP port 5988.	User ID and password credentials are encrypted during submission to the HP MSA SMI-S Provider server. No unencrypted login or password information is exchanged over the wire.	SGI MSA SMI-S Provider credentials with full administrative privileges are required to deliver the full range of management capabilities.
IBM FAStT / DS4000; SGI TP Series; StorageTek D-Series / FlexLine; Sun StorEdge 6130	OEM'ed from LSI Corporation. See LSI.	See LSI	See LSI	See LSI
LSI	The SGI ISRM management server communicates with LSI storage systems via the SYMbol API. An IP connection is required from the SGI ISRM management server to each storage system under management during communications.	The SGI ISRM management server communicates with LSI storage systems on TCP port 2463.	User ID and password credentials are passed in a secure manner via the SYMbol API. No unencrypted information is exchanged over the wire.	LSI user credentials with full administrative privileges are required to deliver the full range of management capabilities.
Sun StorEdge 3510 and 6920	The SGI ISRM management server communicates with Sun StorEdge 3510 and 6920 arrays via the Sun StorEdge SMI-S Provider. An IP connection is required from the SGI ISRM management server to the SMI-S Provider server during communications.	The SGI ISRM management server communicates with the SMI-S Provider server on TCP port 5988.	User ID and password credentials are encrypted during submission to the SMI-S Provider server. No unencrypted login or password information is exchanged over the wire	StorEdge SMI-S Provider user credentials with full administrative privileges are required to deliver the full range of management capabilities.
IBM ESS, DS6000, DS8000	The SGI ISRM management server communicates with IBM ESS, DS6000 and DS8000 series arrays via the DS Open API (IBM CIM Agent). An IP connection is required from the SGI ISRM management server to DS Open API server during communications.	The SGI ISRM management server communicates with the DS Open API on TCP port 5988 (http) or 5989 (https).	User ID and password credentials are encrypted during submission to the DS Open API server. No unencrypted login or password information is exchanged over the wire.	DS Open API user credentials are required to deliver the full range of management capabilities.
Network Appliance FAS900, FAS200, and NearStore	Communicates with the filer via 2 different protocols. For data collection, we use the NetApp ONTAPI library which is a Java library using XML over HTTP (TCP port 80). We're in the process of qualifying SSL connections (TCP port 443) to NetApp devices.	Receive traps from NetApp via SNMP (TCP port 162).	User administration is done using the same accounts that users use to access the web GUI or telnet.	The credentials are encrypted via the ONTAPI library. We call out a few broad requirements around user permissions in our user doc.

8.0 Role-Based Access Control

SGI InfiniteStorage Resouce Manager (ISRM) incorporates a customizable, easy to use, and robust role-based security capability that offers centralized, fine-grained control over individual storage devices and management features. The security model consists of organizations, roles, and users.

8.1 Organizations

An organization contains individual storage infrastructure elements such as business applications, servers, fabric switches, and storage systems. An unlimited number of organizations can be created to organize storage resources by physical location, administrative responsibility, business unit, and other criteria. When storage administrator Users are assigned to an organization, they will only be able to see and manage the resources that have been included in that organization.

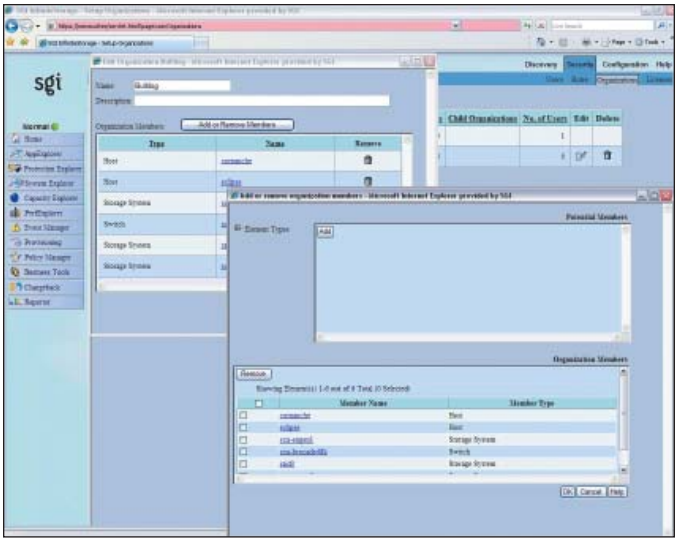

Figure 2. The organization dialog box enables you to create logical groupings that can be used to limit what storage resources appear in each IT administrator's personal view.

8.2 Roles

SGI ISRM roles define a combination of read/write/control privileges and access to the different functional components the product. Privileges define access levels for different classes of storage elements (e.g. Applications, Hosts, Switches, Storage Systems), and for the different functional components of SGI ISRM (e.g. Provisioning, System Explorer, Application Explorer, Policy Manager, Reporter, Chargeback, etc.). A number of pre-defined roles are included out-of-the-box. These roles can be customized or entirely new roles can be created from scratch. When storage administrator Users are created and assigned to a Role, they will be constrained to the functional components and storage element access defined by that Role.

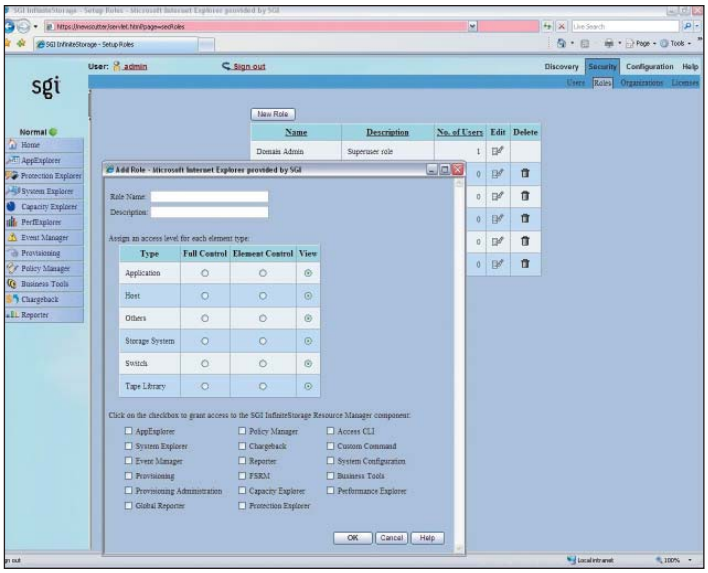

Figure 3. Fine-grained roles enable IT organizations to centrally control what storage element types can be managed, how much management control is delegated, and what features of SGI ISRM are available to each IT administrator.

8.3 Users

Authorizations for SGI ISRM functionality is based upon the logged-in user. An unlimited number of users can be created, each having the following properties:

- User ID and Password– authentication credentials
- Name – administrator's full name
- Role – what features of SGI ISRM can be accessed, what storage resource types can be managed, and how much management control is delegated
- Contact Information – Phone and e-mail information
- Organizations – which storage resources can the user access. Users can be associated with any number of organizations

If SGI ISRM is run standalone, authentication can be done using either the embedded Oracle database (as mentioned earlier, passwords are 3DES-encoded) or externally via a Lightweight Directory Access Protocol (LDAP) directory service such as Active Directory (AD). Use of external authentication centralizes all security related requirements to the enterprise AD/LDAP infrastructure, such as password expiration, resets, and password complexity requirements.

Having distinct users also provides comprehensive audit trails. Every time a user provisions a storage resource, changes an asset record, etc., an audit trail captures what changed and who changed it.

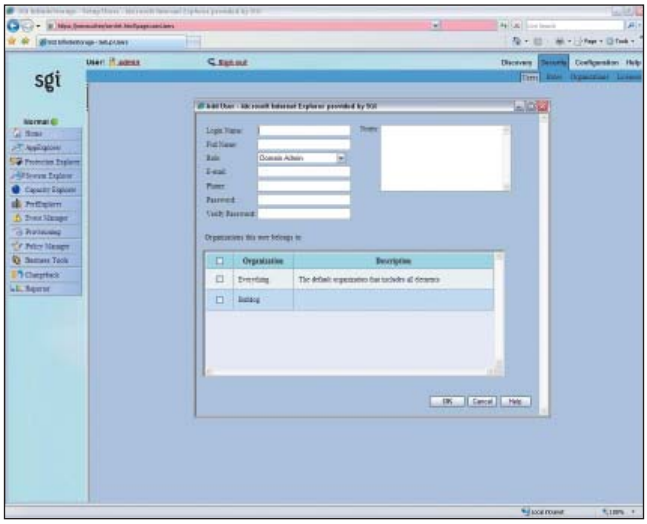

Figure 4. The Add User dialog box enables you to create new SGI ISRM users and add them to specific Roles and Organizations that limit management authority.

Using the comprehensive role-based security features of SGI ISRM, IT organizations can:

- Grant read-only access to storage reports for CIOs or business unit managers that want chargeback information
- Delegate management of Oracle storage to database administrators, while keeping them away from Microsoft Exchange and file server storage
- Secure the SAN from both innocent mistakes and malicious intent
- Comply with internal audits
- Ensure that department IT managers can only manage the resources in their geographic location
- Give operations personnel read-only access to event management
- Allow principal SAN engineers to provision and reconfigure elements within the infrastructure
- Centrally manage storage security from a single console. Some customers are disabling access to their individual device/element managers because these tools lack security and are not integrated with each other. By forcing administrators to go through SGI ISRM, which can handle the majority of all daily storage operations, these customers are ensuring that security policies are consistently enforced and audit trails for all SAN changes are captured.

9.0 Auditing and Logging

The SGI ISRM management server logs all user activity in the user Audit. log logfile stored on the management server. This file is located in the following directory in a default Windows-based installation:

%MGR_DIST%\logs\userAudit.log

Every activity is stamped with the date and time and the name of the user who performed the activity. This file can be used to audit zoning and LUN configuration changes for compliance and internal security analysis.

10.0 Co-Existence with Anti-Virus Software

SGI InfiniteStorage Resource Manager has been tested against anti-virus software products such as Symantec Norton AntiVirus Corporate Edition and McAfee VirusScan to ensure that these solutions can co-exist in the same IT infrastructure. No interoperability issues have been found. In addition, the CIM providers (agents) that are required by SGI ISRM for managed servers do not interfere with the agents required by the anti-virus software solutions. SGI does not recommend or require any changes to the configuration of anti-virus software packages on any SGI ISRM server or managed host.

SGI does recommend excluding the Oracle Database that supports SGI ISRM from virus scanning activities while attempting to use SGI capabilities, since this may lead to a significant decrease in performance.

11.0 Summary

Enterprises today cannot afford to make security vs. service tradeoffs. To maximize productivity and remain competitive in today's 24/7 on-demand enterprise, employees, customers, partners and suppliers, both inside and outside the company, need continuous access to data. Yet with intrusions from within the enterprise accounting for more than 70% of all security breaches, and with storage environments growing in size and complexity, controlling access to the resources that store business data has never been more important.

SGI ISRM is designed to provide fast, efficient, secure management of multi-vendor storage infrastructures. By leveraging the wide range of storage security features it offers, enterprise IT organizations can manage storage operations with greater simplicity and less cost, exceed service levels, and rest easier knowing that the storage infrastructure has been locked down through a secure, centralized management platform.

12.0 For More Information

SGI is “Enabling the storage utility”™ for today’s data-intensive enterprise. SGI’s integrated storage resource management (SRM) and storage area network (SAN) management solutions allow data storage to be quickly and efficiently delivered as a strategic, on-demand computing resource to meet real-time business objectives.

SGI InifiniteStorage Resoucse Manager, SGI’s award-winning product family, enables IT organizations to discover, visualize, monitor, report on, chargeback on, and provision multi-vendor storage infrastructures from a single, Web-based enterprise platform with unprecedented simplicity and speed. Quick to deploy, easy to use, and offering complete investment protection, SGI solutions are clearly differentiated from all competitive offerings by their common, modular platform; seamless integration; broad range of heterogeneous device support; unequalled scalability; support for industry standards; and business application-to-storage system correlation capabilities.

For more information about SGI, visit http://www.SGI.com.

Corporate Office
1140 E. Arques Avenue
Sunnyvale, CA 94085
(650) 960-1980
www.sgi.com

North America +1 800.800.7441
Latin America +55 11.5185.2860
Europe +44 118.912.7500
Japan +81 3.5488.1811
Asia Pacific +1 650.933.3000

4067 [11.01.2007] **J15346**