Lucent Technologies
Bell Labs Innovations

What’s New in Lucent Security Management Server (LSMS)

Release 9.1

260-100-025R9.1
Issue 1
August 2006

Contents

Release 9.1

Release 9.1

What's New in Release 9.1?

Overview

The following features are new in Release 9.1 of the Lucent Security Management Server (LSMS):

- Rules Based Routing
- PDG Accounting
- SNMP Enhancements
- Enabling/Disabling Interfaces
- Compute Server on *Solaris*® Server Platforms
- Strong Password Enhancements for Sarbanes-Oxley (SOX) Compliance
- LSMS GUI Redesign of Report Editor Windows

Rules based routing

Starting with Release 9.1, the LSMS provides the option to configure a rule for HTTP, FTP, or SMTP protocol traffic to route all packets that match the rule to a proxy server, router, or other device, utilizing third party software, to perform content filtering functions such as command blocking, URL filtering, and virus scanning. The rule can be set up to route all packets of a certain traffic type (HTTP, FTP, SMTP) that are coming into the zone, going out of the zone, or both, to a content filter.

Rules-based routing permits an administrator to specify how packets will be routed on a rule-by-rule basis.

This routing applies from the time the rule is applied until one of the following occurs:

- The packet leaves the Brick device
- The packet is VPN tunneled or de-tunneled
- The packet crosses into another partition

The LSMS permits the assignment of zone rule sets from multiple groups to be assigned to a Brick device in the system group. The combination of these two features will permit an administrator in one group to control the routing of packets crossing into the policy associated with another group, thereby permitting a limited form of source routing. This is most easily prevented by ensuring that the zones in this situation are in separate partitions.

Rules-based routing can be applied in networks where:

- The proxy server (content filter) device is on one leg between two firewalls
- The firewall is situated between the client and the proxy server (content filter)
- The proxy server (content filter) is in a loopback configuration, to handle traffic coming into and out of the Brick device

PDG accounting

The Packet Data Gateway (PDG) accounting feature can be enabled for a client tunnel endpoint. When this feature is enabled, the LSMS and Brick device that supports the client tunnel endpoint provide interim accounting data updates, at configurable intervals, for all traffic that passes through the client tunnel endpoint in an active client tunnel. The collection interval for this accounting data can be based on time (minutes), traffic volume (number of bytes), or both. This PDG accounting function is a key requirement of the IP Multimedia Core Network subsystem (IMS) solution, to gather traffic data whenever a user with a Dual Mode Handset (DMH) establishes a secure connection with a Brick device, using IKEv2 EAP to access Packet Switched services over the converged network such as Multimedia Messaging Service (MMS), Wireless Access Protocol (WAP), Internet access, Voice Over Internet Protocol (VoIP), and Peer-to-Peer applications.

DMH users are authenticated and given permission to access the converged network and its suite of services via a RADIUS server and its authentication and access control protocols.

SNMP enhancements

The Brick MIB (svs-brick-mib.mib) has been enhanced to include failover pair labels, failover pair status, and fan/power supply alarm status. A new table has been added that contains information about Brick Tunnel Endpoints (TEPs). It includes status of Local IP Address Map Pools, Client license limits, and counts of IKE authentications, user authentications, Client sessions, and LAN-LAN tunnels. The LSMS SNMP Agent has been modified to correctly populate the dual-index used in several Brick MIB tables and to use a fixed index for each Brick device. This fixed index is assigned when the Brick device is added to the database and does not change when the Brick device rehomes to another LSMS or when Brick devices are added or deleted from the database. The svs-vgc-mib.mib and svs-proxyagent-mib.mib MIBs are obsolete and are no longer supported.

Enabling/disabling interfaces

Starting with LSMS Release 9.1, a configurable option is provided to enable or disable a port (interface) on a Brick device. Disabling a Brick device port (interface) through the LSMS GUI is equivalent to disconnecting the wire/fiber attached to the Brick device port. This can be done to ensure that the behavior of the Brick device does not change if someone inadvertently connects that port to a LAN. When a Brick port is disabled, no traffic is allowed to pass in or out of the Brick device through that port.

A Brick port can be disabled by selecting the Physical Ports tab on the Brick Editor, and then selecting the **Disabled** option from the **Mode** field pull-down menu on the Brick Ports Editor.

Compute server on *Solaris*® server platform

Starting with LSMS Release 9.1, Lucent Secure Compute Servers (LSCSs) are supported by *Solaris*® server platforms that are running the *Solaris*® R8.0, R9.0, or R10.0 operating system.

Compute Servers, which were already supported on *Windows*™server platforms in previous LSMS releases, provide audit (log), alarm, and user authentication services for Brick devices that are homed to them. A Compute Server differs from a Secondary LSMS in that it is not stand-alone. It is dependent on an active communication link to its associated LSMS for database access. One or more Compute Servers can be connected to a Primary or Secondary LSMS in a cluster, which can support up to five Compute Servers. Compute Servers provide operational advantages and enhanced scalability of LSMS by allowing servers to be geographically distributed in multiple locations. This feature can be used to place audit (log) servers closer to Brick device sites to reduce the amount of log data sent over expensive WAN links. Since log data for a Brick device may now be distributed across multiple LSMS and Compute Servers, the Alarm and Report functionality can collate data across all servers to provide merged alarms logs and reports.

Strong password enhancements for Sarbanes-Oxley (SOX) compliance

A new option can be enabled via the Configuration Assistant to enforce stricter rules for creating passwords that comply with the Sarbanes-Oxley (SOX) requirements.

When a new password is set for a user or administrator that is authenticated using Local Password authentication, or an existing local password is changed, if the strong password (SOX compliance) option is enabled (the default) via the Configuration Assistant, stricter password requirements would apply for password authentication. In this case, the password:

- Must be a minimum of eight characters, or the **Minimum Password Length** set for the **Local Password** Authentication Service, whichever is greater
- Must contain at least one alpha character and one non-alpha character (0-9, special characters, no restrictions)
- Cannot contain three or more repeated alphanumeric characters in a row
- Cannot contain three or more consecutive, ascending or descending, alphanumeric characters in a row

- Not contain the User Account name or its mirror (reverse character format)
- Not be one of the previous three passwords most recently used

The strong password (SOX) requirements, when enabled, apply to new or changed passwords for:

- A clean installation password of the master user
- Local passwords for User Accounts
- Local passwords for Administrator Accounts
- User login passwords for the Brick device console
- Admin key (additional key) which is needed when SecurID or RADIUS authentication methods are used

LSMS GUI redesign of Report Editor windows

The Report Editor windows in the LSMS R9.1 GUI, which are used to configure and generate the various LSMS reports (Closed Session Details, Sessions Logged, Administrative Events, VPN Events, Alarms Logged, User Authentication) have been redesigned from a Wizard format to a multi-tabbed format to promote consistency and ease-of-use in the interface.

Features available from previous LSMSR9.0 patch releases

In addition to the new features provided by LSMS Release 9.1, the following features are supported from the previous Release 9.0 patch releases:

- Cost-Based Routing
- IP Tracking
- Brick Preemption Feature

For information about these features, please refer to the LSMS documentation.

□