

Feature Brief



Log Management with Clavister InSight™

Clavister SSP™ Security Services Platform

firewall • VPN termination • intrusion prevention • anti-virus
anti-spam • content filtering • traffic shaping • authentication

CLAVISTER®

Protecting Values

Introduction

Clavister Security Services Platform (SSP™) is our proven, feature-rich, service-oriented framework for providing best-in-class security solutions. Clavister SSP™ consists of **Clavister Network Security Elements**, **Clavister Lifecycle Systems**, and **Clavister Lifecycle Services**. Clavister SSP™ combines precise control, fine-granular administration, and seamless scalability making it easy to provision the perfect solution for any customer; be it a small organization, a large Internet Service Provider, a Managed Security Service Provider, or a multimedia-ready telecommunication operator.

Clavister Network Security Elements

These are the physical building blocks that you install in your network. Clavister SSP™ currently offers two network security elements; Clavister Security Gateway Series and Clavister Secure Access Gateway. The Clavister Security Gateway is available both as a pre-packaged turnkey appliance solution for fast and easy deployment or as a distributed software-only solution for your preferred hardware platform. The Clavister Secure Access Gateway Series is available as a pre-package turnkey appliance solution only and offers SSL VPN, Single Sign-On (SSO) and multi-factor authentication (MFA).

Clavister Lifecycle Systems

The Clavister Lifecycle Systems is a set of software components enabling true network security management throughout the entire lifecycle, including deployment, monitoring and reporting, configuration and integration, as well as analysis, optimization and troubleshooting. Clavister FineTune™ and the Web-based administration user interface enable you to manage a large set of Clavister Network Security Elements. Clavister InSight™ is our premium Security Event and Information Management (SEIM) system, which does not only support Clavister security network elements, but also a majority of other network devices. By correlating data from all network elements, you get a complete log of all activities in your network. Clavister PinPoint™ completes the Clavister Lifecycle Systems suite with accurate and precise real-time information packaged in a convenient dashboard-style application.

Clavister Lifecycle Services

The Clavister Lifecycle Services empowers you and your products with tools, services, and resources that help maximize benefits and eliminate problems, including planning, deployment, optimization, operations and maintenance. The Clavister Lifecycle Services include the Clavister Service Provisioning Network (CSPN) for automated signature updates, the Clavister xPansion Lines™ license upgrade framework and Clavister's award-winning Technical Support.

The Clavister SSP™ service-oriented framework provides you with a secure environment for your business; either as a service provided to you by a Managed Security Service Provider (MSSP) or as systems and services integrated in your own network.

For more information about Clavister products and services, please visit us at: www.clavister.com.

Overview

Clavister InSight™ Syslog Server allows you to collect, normalize and manage syslog data from your Clavister Security Gateways. But it also works with other leading security products, including firewalls. Once you use Clavister InSight™ Syslog Server, a third-party syslog server is not required and should not be used with Clavister InSight™.

The Clavister InSight™ Syslog Server helps you do away with manual configuration of devices. While some devices can export log files in a readable format, others typically do not write log information to a readable file. In such cases, Clavister InSight™ relies on a syslog server to capture log information. The Clavister InSight™ Syslog Server helps eliminate the need for manual configuration of devices, automatically detects and configures devices. The Clavister InSight™ Syslog Server can be installed on any machine in the network.

This document highlights the advantages and benefits in using Clavister InSight™ Syslog Server.

Log Data Collection and Management

The Clavister InSight™ Syslog Server is typically installed into the same hardware platform as the Clavister InSight™ system – however it can be optionally installed into a separate machine platform. The primary reason for a separate installation of the Clavister InSight™ Syslog Server is when the overall load processing volume is very high.

The Clavister InSight™ Syslog Server saves significant amount of disk space by automatically writing to a compressed file. This will result in significant savings on a monthly and yearly basis for a large or busy customer generating gigabytes of log data every day. For example, a customer generating 4 GB of logs data per day would normally require about 120 GB per month of disk space to store this amount of log data. This would mean up to 1.4 TB of storage per year. This would cost this customer approximately \$70,000 just for procuring storage. On the other hand if this customer uses Clavister InSight™ Syslog server, then they only need about 12 GB per month or 140 GB per year to store raw logs, which could easily be purchased for less than \$5,000.

In addition, the Clavister InSight™ Syslog Server saves network bandwidth by transferring only the change in data, usually referred to as the "delta", in compressed format over the network. This speeds the reporting and facilitates 'near real-time' information reporting and it does not deplete network resources. This is important in all networks, but especially so in usage-sensitive and distributed WAN environments. User configurable delta file transfer helps meet your unique requirements based on log file size, network bandwidth, and system resources.

The Clavister InSight™ Syslog Server saves log data in normalized and standard Open Log File Format (OLF) log format from multiple firewalls from different vendors. Distributed Clavister InSight™ Syslog Server helps you localize the log collection thus reducing the syslog traffic over the WAN. Changes to all distributed syslog servers can be applied from Clavister InSight™ main console.

Clavister InSight™ Syslog Server automatically detects and collects log data from all configured devices. Users configure only the devices so they are enabled to permit the Clavister InSight™ Syslog Server to 'listen' to the syslog messages. There is no additional configuration required within Clavister InSight™ Syslog Server.

Conclusion

This Feature Brief describes Clavister InSight™ log management and how to use it with your Clavister SSP™ installation. Below are some key customer benefits:

Clavister SSP™ Key Benefits

- **Robust Security**
The purpose-built security offering from Clavister provides a complete set of security features, including Stateful Packet Inspection (SPI) firewall with DoS and DDoS protection, VPN with strong encryption, and User Authentication.
- **Rapid Deployment**
The Clavister Security Gateway provides effortless and rapid deployment. A trained technician can easily deploy and configure new network security elements within minutes, even across continents.
- **Flexible Traffic Control**
The highly sophisticated bandwidth management capabilities in the Clavister Security Gateway make it possible to not only guarantee bandwidth for business critical applications or server, but also to optimize the entire traffic flow in your network and avoid inefficient bandwidth usage.
- **Lowered Costs for Administration**
The powerful administration system that comes with Clavister Security Gateway enables organizations to lower the costs for administration through centralized management. The administration system makes it possible to deploy and configure all devices across the network, no matter if they are located next door or across the globe.
- **High Performance**
Scalable performance with unsurpassed maximum bandwidth, concurrent connections and simultaneous VPN tunnels makes the Clavister Security Gateway the ideal choice even in the most demanding environments like Internet Service Provider Networks, Data Centers, and telecom operators.

- Low Total Cost of Ownership (TCO)

Clavister's goal is to provide complete security solutions more cost efficiently than any competitor. Clavister SSP™ with its unique combination of integrated features, world-class service and support, and powerful administration system provide the lowest TCO and the best price/performance ratio possible.

Clavister InSight™ Log Management Key Benefits

- Comes with own high-performance syslog server, the Clavister InSight™ Syslog Server
- Optimized to save disk space and to conserve network bandwidth
- Supports Open Log File Format (OLF)
- Distributed and localized log collecting
- Easy deployment and maintenance for all logging devices, including the Clavister InSight™ Syslog Server

Feedback

Clavister Product Marketing is always interested in feedback from our readers. Please direct suggestions, comments or questions regarding this document to product-marketing@clavister.com. Please include the title of the document in your email.

About Clavister

Clavister - a Swedish privately owned company developing IT security products, including its award-winning Clavister Security Services Platform (SSP™). This service-oriented framework enables organizations to monitor network traffic, protecting critical business assets and blocking undesirable surfing. It will also protect you against intrusion, viruses, worms, Trojans, and overload attacks. It requires minimal servicing, with central administration, and has exceptionally flexible configuration possibilities. Its seamless scalability makes it easy to provision the perfect solution for any customer; be it small organizations, large Internet Service Providers, Managed Security Service Providers, or multimedia-ready telecom operators.

Clavister was founded 1997 in Sweden, with R&D and headquarters based in Örnköldsvik and Sales and Marketing based in Stockholm. Its solutions are marketed and sold through International sales offices, distributors, and resellers throughout EMEA and Asia. Clavister also offers its technology to OEM manufacturers.

For more information, please visit us at www.clavister.com.

Limitation of Responsibilities

The information in this document represents the current view of Clavister AB on the issues discussed as of the date of publication. Because Clavister must respond to changing conditions, it should not be considered to be a commitment for Clavister, and Clavister cannot guarantee the accuracy of any information presented after the date of publication. This document is for informational purposes only. CLAVISTER MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the written permission of Clavister. Clavister may have trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Clavister, the furnishing of this document does not give you any license to these trademarks, copyrights, or other intellectual property.

Part Number: [clavister-fbr-insight_log_management](#) (0801)