



SNMP Security Pack



Providing SNMPv3 support

Ubizen AETHIS
Member of the Ubizen group

The **SNMP Security Pack** is a plug-in to HP OpenView Network Node Manager (NNM), allowing NNM (4.1 and later) to use SNMPv3 with security. SNMPv3 provides safe configuration and control operations. Recent extensions of the Security Pack make it also usable by most SNMP managers. Its administration offers logical contexts, view-based access control, and remote configuration. The user-based authentication mechanism is based on MD5, SHA, and a loosely synchronized monotonically increasing time indicator. The user-based privacy mechanism is based on Data Encryption Standard (DES) Cipher Block Chaining (CBC) mode, 16-byte key algorithms, and multiple levels of compliance. SNMPv3 is available for networks, systems, applications, manager-to-manager communications, and proxy management of legacy systems.



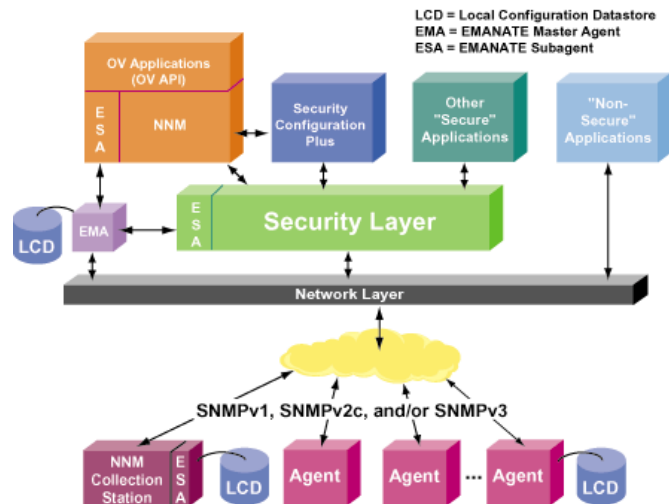
By providing SNMPv3 support, the SNMP Security Pack offers NNM customers the benefits of a comprehensive approach to management security, including authentication, authorization, access control, data integrity, key management, and encryption options. Security Pack allows NNM customers to use set commands to alter device or network configuration in a secure fashion and to add security to other sensitive SNMP transactions, such as the exchange of network topology between multiple NNM.

Overview

The SNMP Security Pack supports two local configuration datastores (LCDs), one of which is used by the BRASS server and the other by the EMANATE[®] Master Agent. The LCDs provide access control table parameters, as well as parameters for configuring trap destinations. The SNMP Security Pack contains the following products:

Bilingual Request and Security Subsystem (BRASSTM) allows the NNM to support secured communications via SNMPv3.

BRASS provides a C programming API that allows one or many management applications to access a single, shared SNMP stack and security database.



EMANATE[®] Master Agent offers an SNMPv3 agent, so that SNMPv3 management can be performed. EMANATE also assists in configuring the manager's datastore. EMANATE is a run-time extensible, SNMP agent based upon a Master Agent/Subagent architecture, which allows for subagents to be loaded and unloaded dynamically at run-time.

Tcl-based scripting facility complements OpenView NNM. The Tcl facility provides a Graphical User Interface (GUI) that makes configuring SNMPv3 easier. It also provides the functionality that allows the configuration to take place.

Security Mechanisms

By employing SNMPv3, Security Pack offers five main types of threat protection (shown below).


Threat	Protection
Masquerade	Verifies the identity of the message's origin by checking the integrity of the data.
Modification of Information	Thwarts accidental or intentional alterations of in-transit messages by checking the integrity of the data, including a time stamp.
Message Stream Modification	Thwarts replay attacks by checking message stream integrity, including a time stamp.
Unauthorized Access	Verifies operator authorization and protects critical data from intentional and/or accidental corruption by using an Access Control Table. (Supports policy-based management)
Disclosure	Prevents eavesdropping by protocol analysers, etc. by using encryption.

To deploy sophisticated security mechanisms such as those provided by SNMPv3, each management application must have access to the LCD that includes "secrets" shared with an agent. As a result, each copy of NNM must coordinate its use of the LCD and secrets with other NNMs and/or SNMPv3 entities. Security Pack provides this coordination transparently by maintaining the SNMPv3 datastore and by performing SNMP operations at NNM's request. This prevents multiple NNMs or other SNMPv3 applications from conflicting in their use of the security datastore.

Summary

Using SNMP Security Pack, SNMPv3 is easy to configure and use, and memory requirements are minimized. Most importantly, SNMP Security Pack enables smooth coexistence and transition from SNMPv1, preserving the vast customer investment in SNMP-based management. In summary, the SNMP Security Pack provides several important benefits to NNM customers:

- ✓ Multifaceted security management, including authentication, privacy, and authorization/access control,
- ✓ Support for SNMPv1, SNMPv2c, and SNMPv3 simultaneously and transparently,
- ✓ Simplification of SNMPv3 security agent configuration files for all NNMs and SNMPv3 managed nodes,
- ✓ Hiding of SNMPv3 clock synchronization details,
- ✓ Sensitivity to the memory constraints and ease-of-use requirements relevant to agents, management stations, and administrators,
- ✓ The SNMP Security Pack is available for HP OpenView NNM 4.1 and later on HP-UX, Solaris, and Windows NT.

	SNMP Research Contact information (European Competence Center)
	Ubizen AETHIS Rue du Bosquet, 7 - B-1348 Louvain-la-Neuve - Belgium Tel.: + 32 10 456 130 - Fax: + 32 10 456 155 Email: SNMP@aethis.ubizen.com - Website: http://www.aethis.com