XYGATE Merged Audit

Bundled with HPE Integrity NonStop X servers

Meet new security challenges

As cybercrimes grow more sophisticated every year, new laws are being passed and existing security standards are being enhanced that require companies to prove that they have implemented appropriate steps to secure sensitive data. Securing data and resources properly requires protecting confidentiality, integrity, and availability. However, to pass formal compliance audits and prove that your business secures its data appropriately, you should report on the security-related activities occurring on your system.

HPE understands that for our customers, a breach in security not only means financial penalties and losses, but also loss of business reputation and bad publicity. HPE NonStop customers need to verify that security rules are being followed and receive alerts promptly when problems arise.

XMA is a sophisticated audit collection solution that produces activity reports for security audits.

How XMA works

XMA is an easy-to-use product that collects and filters data from various system logs and audit logs into a single, normalized SQL database to generate reports. It can also send alerts to help you monitor security activities on your system.

XMA enables the NonStop system to integrate seamlessly with security information and event management (SIEM) devices. Its features include:

- A single repository for audit, event and application log data

- Automatic alerting of security events through email, EMS, SNMP Traps, IP, and custom delivery destinations

- Integrate NonStop data with Elastic stack

- A single-server or multi-server view

- A customizable reporting tool

- A filtering mechanism to extract selected data

- A Windows® event monitor to display any event or item in near real time based on customized filters built by the user

- User-definable alerts

- Log adapter for streaming audit data to the ArcSight SIEM

- ACI BASE24 and BASE24-eps information (optional plug-in)

- HPE Integrated Home Subscriber Server (I-HSS) events (optional plug-in)

- AJB Retail Transaction Switch (RTS) events (optional plug-in)

- GreenHouse SECOM events (optional plug-in)

ArcSight Log Adapter

XMA comes with a custom log adapter definition for use with the ArcSight SIEM. Any log data collected from the HPE NonStop server is properly formatted and coded, which is later reviewed and understood without any special configuration changes to the ArcSight SIEM.

ACI BASE24 plug-in

A plug-in for XMA that enables event capture for BASE24 applications is also available for separate purchase from HPE. This plug-in allows you to include BASE24 events in your audit tracking report. The BASE24 plug-in is available for servers running L-Series, J-Series, and H-Series RVUs.

ACI BASE24-eps plug-in

A plug-in for XMA that enables event capture for BASE24-eps applications is also available for separate purchase from HPE. This plug-in allows you to include BASE24-eps events in your audit tracking report. The BASE24-eps plug-in is available for NonStop servers running L-Series and J-Series RVUs.

HPE I-HSS plug-in

A plug-in for XMA that enables event capture from HPE I-HSS applications is available for separate purchase from HPE. This plug-in is especially useful for telecommunications customers who want to include HLR and I-HSS events in their audit tracking reports. The I-HSS plug-in is available for NonStop servers running L-Series, J-Series and H-Series RVUs.

Verifone Retail Transaction Switch plug-in

Formerly AJB RTS, the Retail Transaction Switch is a suite of corporate level electronic payments solutions for configuration management, fraud management, E2EE and tokenization, reconciliation reporting, settlement, and transaction switching. When operating on an HPE NonStop server, related security audit activity can be captured by XMA and inserted into its SQL database for reporting and alerting and delivery to an SIEM. The AJB RTS plug-in is available for NonStop servers running L-Series and J-Series RVUs.

GreenHouse Secure Command Manager (SECOM) plug-in

SECOM, from GreenHouse, audits user activity, as well as terminal I/O, and this audit and trace data is supported by XMA. SECOM users can easily incorporate their SECOM audit data with the rest of their NonStop security and audit data, and optionally feed it into an enterprise device. The SECOM plug-in is available for NonStop servers running L-Series and J-Series RVUs.

Features and benefits

Ease of creating and viewing reports

With XYGATE Merged Audit, viewing and delivering information is straightforward. When creating reports, XMA enables you to:

- Set your selection criteria to control the information you wish to see in a report

- Choose the columns you want to include in a report

- Customize your report view by selecting which columns to display and how to display them

- Group and sort the information any way you like

- Add custom headers and footers

- Save your design templates for future reuse

- Repeat report generation for daily, weekly, monthly, or custom production

Whether you are generating reports to the NonStop Spooler or to a Windows PC, XMA provides all the information and tools you need to get the right information to the right people at the right time.
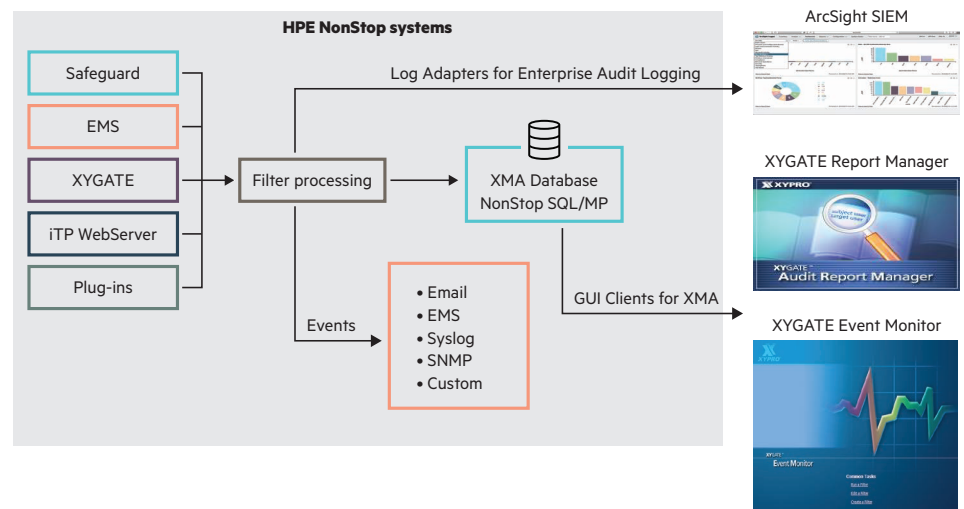

Figure 1. XMA Architecture

Simplified alerting

XMA's advanced filtering capabilities allow you to define your own rules, so you can rapidly alert the appropriate people and systems when events of interest occur. The XYGATE Event Monitor (XEM) GUI comes with XMA and allows you to monitor and be notified of security events right on the desktop in graphic, acoustic, and action-oriented formats.

Audit integrity

XMA's automatic archiving and database cleanup facilities offer reliability, so no important information is lost or missed. Unlike other audit "rollover" and "maxfile" settings, XMA manages data based on defined date and time ranges, and verifies that you always have the data you need.

Many system, user, and application events are written to other data sources such as Safeguard, Event Management System (EMS), Java Database Connectivity (JDBC)/MX, and Open Database Connectivity (ODBC)/MX. XMA handles all of these sources of NonStop auditing (including the ACI BASE24, BASE24-eps, AJB, and I-HSS options) and intelligently merges them to form a single audit database.

XMA allows you to send events to SIEM devices, where the event can be stored for reporting but remains in an unmodifiable format. XMA supports ArcSight, RSA NetWitness (formerly enVision), LogRhythm, QRadar, Splunk, and many other SIEM devices.

Ordering information

Product name	Product ID (L-Series)	Product ID (J-Series)	Product ID (H-Series)
XYGATE Merged Audit	Note 1	Note 2	Note 3
XMA BASE24 plug-in	BE378AL	QXMABASE24	HXMABASE24
XMA BASE24-eps plug-in	BE368AL	QXMAB24EPS	NA
XMA HLR plug-in	BE379AL	QXMAHLR	HXMAHLR
XMA AJB RTS plug-in	BE369AL	QXMAAJBRTS	NA

Note 1: XMA is included in the L-Series commercial NonStop OS bundle BE338AC. For systems using the L-Series Telco NonStop OS (BE071AM), XMA is included as one of the four products in the security bundle SKU BE014AC which need to be purchased separately.
Note 2: XMA is included in the J-Series security bundle QSN52 (and the older QSN51).
Note 3: XMA is included in the H-Series security bundle HSN51.

Make the right purchase decision. Click here to chat with our presales specialists.

Learn more at
hpe.com/us/en/servers/nonstop.html

f 𝕏 in ✉

Sign up for updates