Security Auditing and Reporting for the Integrity NonStop Server

Karen Copeland, HP
Lisa Partridge, XYPRO
Agenda

• Security – the need for auditing
• XYGATE Merged Audit
  • New deal
  • What is XYGATE Merged Audit
  • Features/Functions
• CLW Integration
• Merged Audit future options
• Conclusion
As cybercrime increases regulations get tougher

The Internet Crime Complaint Center reported that computer crimes rose 22.3% in 2009.

There have been 414 breaches reported so far in 2010, affecting 13M customer records.

There’s 20,000+ security regulations in the world today and more emerge every year.

The Payment Card Industry will publish version 2.0 of their Data Security Standard this fall.

The U.S. has recently passed HITECH, which adds more consequences for healthcare organizations when HIPAA standards aren’t met.

Companies continue to struggle to remain profitable during these difficult times.
Why security auditing matters . . .

“That a breach occurred is bad enough but when attackers are allowed to capture and exfiltrate data for months without the victim’s knowledge, bad gets much worse . . .” *

Figure 36: Percent of breaches that remain undiscovered for months or more

The Payment Card Industry Data Security Standard requires that companies audit, monitor, log or review activity status of the IT system and environment in 20 or more standards and calls it out specifically as actions that must be taken in 10.2 and 10.3.

https://www.pcisecuritystandards.org/index.shtml

Since 2008, 164 million records have been compromised in a breach due to hacking or malware, payment card fraud or insider breaches.

Privacy Rights Clearinghouse - Chronology of Data Breaches
http://www.privacyrights.org/data-breach/new

HP NonStop Server
Auditing sources today

The NonStop server already provides the means to capture audit by logging data from a variety of sources. Safeguard auditing must be turned on to collect much of this data. Data sources can include:

- Safeguard
- ODBC/MX
- Measure
- SSH Audit Logs
- iTP Secure WebServer
- Application Logs (ACI Base24 and HP HLR)
- Logs produced by partner products
- System EMS Logs
- JDBC/MX
- NetBatch
- SSL Logs

The challenge for customers is being able to distinguish what data is important to the business and to analyze and report against the vast amount of data that can be gathered and stored in these logs.
Security Areas

1. On Platform
   Only authorized users can access the system. Access to data and other resources are controlled.

2. Data In Motion
   Network and sensitive data moving between systems or workstations cannot be deciphered if intercepted.

3. Data At Rest
   Stored data and sensitive customer information is protected on disk or tape.

4. Compliance
   Security policies can be verified to be working and compliance regulations can be proven to be in place.
NonStop Security Reporting and Alerting
XYGATE Merged Audit

As of September 1st for J Series and H Series systems:

- XYGATE Merged Audit is included with the NonStop OS on all new systems orders.
- The XYGATE Merged Audit product provides much more sophisticated reporting than SafeArt, includes alerting capabilities, and should be of interest to all customers who need to monitor security events on their servers.
- It is provided on SUTs and installed using DSM/SCM.
- No coldload or application downtime is required for installation.
- No license file is required.
- Customers can purchase OS upgrades for their existing NonStop systems on H Series or J Series starting November 1st, 2010.
- The product is also available for separate purchase on G Series systems November 1st.
- See your NonStop sales rep for details.
NonStop Partnership
XYPRO Technology Corporation

- 27 years serving the HP NonStop community
- Specialists in security & encryption
  - Large portfolio of security and encryption products that are part of the XYGATE offering.
- Financially sound & continuously growing
- Strong corporate structure
- Fully established Follow-the-Sun support structure
  - Offices in: Los Angeles, Omaha, Toronto, London, Cape Town, Melbourne, Mexico City
- Incredible customer retention
  - Still have very first XYGATE customer
XYGATE Merged Audit

now available from HP
XYGATE Merged Audit

Features

- Well-established product available for the NonStop market for 10 years.
- A single repository on the NonStop for audit data from multiple sources.
- Report on NonStop server security activities using predefined or customized reports.
- Prepare for PCI audits or for periodic security reviews.
- Collects data for a single NonStop server or multi-server view.

- Filtering mechanism provides ability to extract selected data
- Customizable security alerts
- Collects ACI Base24 information (optional add-on)
- Collects HLR information (optional add-on available in 2011)
- Feeds data to enterprise audit tools & systems
- Feeds data in Syslog format to Security Information and Event Management (SIEM) solutions such as the HP Compliance Log Warehouse (CLW)

PCI/DSS 10.5.3 calls out collection of “audit data in a centralized log server or media that is difficult to alter.”
XYGATE Merged Audit
High Level Architecture

Various collection feeds come with the product

NonStop

HP NonStop Audit Sources

- Safeguard
- EMS Logs
- Measure
- ODBC/MX
- JDBC/MX
- XYGATE Logs
- ACI Base24
- HLR

Filter Processing

- XMA SQL Database
- XMA Alerts and Events
  Email, SNMP, EMS, Syslog, Custom

Report Generator
Event Monitor

Enterprise Audit Logging

CLW (Compliance Log Warehouse)

Customers are using MergedAudit to migrate NonStop data streams into these other devices as well

You can configure filtering and alerting preferences to send events to the XMA database and off the NonStop via alerts, events or both.

ACI Base24 data and HLR data can be added with future plug-in products
XYGATE Merged Audit Screenshot

Report Manager

Provides easy to use interface for reporting tasks
XYGATE Merged Audit Screenshot
Report Manager: Predefined Reports Screen

Available PCI reports are listed by PCI DSS 1.2 section ID.
XYGATE Merged Audit Screenshot

Report Manager: Criteria Setting

The user can supply criteria to further filter the results shown.
The user can choose from predefined report layouts.
### PCI 2.2.3 SFG - All Config Changes

<table>
<thead>
<tr>
<th>Outcome</th>
<th>DateTime</th>
<th>SubjUser</th>
<th>Result</th>
<th>Oper</th>
<th>ObjName</th>
</tr>
</thead>
<tbody>
<tr>
<td>SUCCESS</td>
<td>2010-09-16:09</td>
<td>SUPER.SUPER</td>
<td>Granted Create to Acl-diskfile</td>
<td>CREATE</td>
<td>$VTLH.TERRI.MYFUP</td>
</tr>
<tr>
<td>SUCCESS</td>
<td>2010-09-16:09</td>
<td>SUPER.SUPER</td>
<td>Granted Change to Acl-diskfile</td>
<td>CHANGE</td>
<td>$VTLH.TERRI.MYFUP</td>
</tr>
<tr>
<td>SUCCESS</td>
<td>2010-09-16:09</td>
<td>SUPER.SUPER</td>
<td>ACL Added 00222,* E</td>
<td>CHANGE</td>
<td>$VTLH.TERRI.MYFUP</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Product System: \X Object Type: ACL-SUBVOLUME Count: 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>SUCCESS 2010-09-16:09</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Product System: \X Object Type: ALIAS Count: 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>SUCCESS 2010-09-16:10</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Product System: \X Object Type: SAFEGUARD-CONFIG Count: 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>SUCCESS 2010-09-16:09</td>
</tr>
<tr>
<td>SUCCESS 2010-09-16:09</td>
</tr>
<tr>
<td>SUCCESS 2010-09-16:09</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Product System: \X Object Type: USER Count: 72</th>
</tr>
</thead>
<tbody>
<tr>
<td>SUCCESS 2010-09-16:09</td>
</tr>
<tr>
<td>SUCCESS 2010-09-16:09</td>
</tr>
<tr>
<td>SUCCESS 2010-09-16:09</td>
</tr>
</tbody>
</table>
## XYGATE Merged Audit Report Sample

**Report Manager: Logon Report**

### PCI 8.5 SFG - Logon Report

<table>
<thead>
<tr>
<th>Outcome</th>
<th>DateTime</th>
<th>From User</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>FAILURE</td>
<td>2010-09-16:06</td>
<td>NULL.NULL</td>
<td>Wrong-password Verifyuser to User XYPRO.JORGE 222.214</td>
</tr>
<tr>
<td>FAILURE</td>
<td>2010-09-16:07</td>
<td>XYPRO.JORGE</td>
<td>Wrong-password Verifyuser to Alias sup-jorge 255.255</td>
</tr>
<tr>
<td>SUCCESS</td>
<td>2010-09-16:08</td>
<td>NULL.NULL</td>
<td>Success Verifyuser to User XYPRO.BARRY 222.011</td>
</tr>
<tr>
<td>SUCCESS</td>
<td>2010-09-16:08</td>
<td>NULL.NULL</td>
<td>Success Verifyuser to User XYPRO.BARRY 222.011</td>
</tr>
<tr>
<td>FAILURE</td>
<td>2010-09-16:09</td>
<td>NULL.NULL</td>
<td>Wrong-password Verifyuser to Alias sup-jorge 255.255</td>
</tr>
<tr>
<td>FAILURE</td>
<td>2010-09-16:09</td>
<td>NULL.NULL</td>
<td>Wrong-password Verifyuser to Alias mayxanh 232.044</td>
</tr>
<tr>
<td>SUCCESS</td>
<td>2010-09-16:09</td>
<td>XYPRO.BARRY</td>
<td>Success Authenticate to User XYPRO.BARRY 222.011</td>
</tr>
<tr>
<td>SUCCESS</td>
<td>2010-09-16:09</td>
<td>NULL.NULL</td>
<td>Success Verifyuser to User XYPRO.BARRY 222.011</td>
</tr>
<tr>
<td>SUCCESS</td>
<td>2010-09-16:09</td>
<td>XYPRO.BARRY</td>
<td>Success Authenticate to User XYPRO.BARRY 222.011</td>
</tr>
<tr>
<td>SUCCESS</td>
<td>2010-09-16:10</td>
<td>XYPRO.BARRY</td>
<td>Success Authenticate to User XYPRO.BARRY 222.011</td>
</tr>
<tr>
<td>SUCCESS</td>
<td>2010-09-16:10</td>
<td>NULL.NULL</td>
<td>Success Verifyuser to User DEMO.MANAGER 100.255</td>
</tr>
<tr>
<td>FAILURE</td>
<td>2010-09-16:11</td>
<td>NULL.NULL</td>
<td>Unknown-user Verifyuser to Alias xypro.com 000.000</td>
</tr>
<tr>
<td>FAILURE</td>
<td>2010-09-16:11</td>
<td>NULL.NULL</td>
<td>Wrong-password Verifyuser to User XYPRO.ROB 222.229</td>
</tr>
</tbody>
</table>

**Product System:** \X Count: 13

**Product System:** \Y Count: 26

### Logon Failures

<table>
<thead>
<tr>
<th>Outcome</th>
<th>DateTime</th>
<th>From User</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>SUCCESS</td>
<td>2010-09-16:06</td>
<td>NULL.NULL</td>
<td>Success Verifyuser to User QA.KATHRYN 232.101</td>
</tr>
<tr>
<td>SUCCESS</td>
<td>2010-09-16:09</td>
<td>NULL.NULL</td>
<td>Success Verifyuser to User QA.DENNIS 232.043</td>
</tr>
<tr>
<td>SUCCESS</td>
<td>2010-09-16:09</td>
<td>NULL.NULL</td>
<td>Success Verifyuser to User QA.DENNIS 232.043</td>
</tr>
<tr>
<td>SUCCESS</td>
<td>2010-09-16:10</td>
<td>NULL.NULL</td>
<td>Success Verifyuser to User QA.DENNIS 232.043</td>
</tr>
<tr>
<td>SUCCESS</td>
<td>2010-09-16:10</td>
<td>NULL.NULL</td>
<td>Success Verifyuser to User XYPRO.NOEL 222.010</td>
</tr>
<tr>
<td>SUCCESS</td>
<td>2010-09-16:10</td>
<td>XYPRO.NOEL</td>
<td>Success Verifyuser to User XYPRO.NOEL 222.010</td>
</tr>
</tbody>
</table>
XYGATE Merged Audit Report Sample
Report Manager: Safeguard Audit Log Initialization

PCI 10.2.6 EMS - SFG Audit Log Initialization

<table>
<thead>
<tr>
<th>System</th>
<th>Event#</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>\X</td>
<td>6</td>
<td>21:03 15SEP10 007,01,417 \X.$ZSMP: Audit file \X.$DATAB_SAFE.A0000616 has been closed; audits are now directed to \X.$DATAB_SAFE.A0000617</td>
</tr>
<tr>
<td>\Y</td>
<td>6</td>
<td>01:04 16SEP10 253,01,460 \XYS7000.$ZSMP: Audit file \XYS7000.$DSMSCM_SAFE.A0000298 has been closed; audits are now directed to \XYS7000.$DSMSCM_SAFE.A0000299</td>
</tr>
</tbody>
</table>

SFG - Audit Log Initializations
### PCI 10.2.4 SFG - Daily Violations Report

<table>
<thead>
<tr>
<th>Outcome Date/Time</th>
<th>Login</th>
<th>Oper</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>FAILURE 2010-09-15</td>
<td>XYPRO.TERII1</td>
<td>PURGE</td>
<td>Denied Purge to Diskfile-pattern $VTLH.TERII.MYFUP</td>
</tr>
</tbody>
</table>
## Merged Audit
### HLR Plug-in Report Sample

**HLR - Sensitive PARAMS Report - Detail**

<table>
<thead>
<tr>
<th>Outcome</th>
<th>DPA Usr</th>
<th>Operation</th>
<th>ObjType</th>
<th>Object Name</th>
<th>DataType</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>SUCCESS</td>
<td>ICAP</td>
<td>UPDATE</td>
<td>GSUB</td>
<td>KEY=655016620096404</td>
<td>FLAG</td>
<td>CLIP-ACT 1</td>
</tr>
<tr>
<td>SUCCESS</td>
<td>ICAP</td>
<td>UPDATE</td>
<td>GSUB</td>
<td>KEY=655016620096404</td>
<td>PARAMS</td>
<td>CLIP-AUTH 1, CLIP-ACT 1, CLIPOVERRIDE 0</td>
</tr>
<tr>
<td>Session ID: 000000000000000000002010-08-30</td>
<td>Sequence Number: 000000518</td>
<td>Count: 2</td>
<td>SUCCESS</td>
<td>ICAP</td>
<td>UPDATE</td>
<td>GSUB</td>
</tr>
<tr>
<td>SUCCESS</td>
<td>ICAP</td>
<td>UPDATE</td>
<td>GSUB</td>
<td>KEY=655016620096404</td>
<td>PARAMS</td>
<td>GPRS-BARRED-WHILE-ROAMING 1, CAMEL-ACTIVE 1, GSM-O-CSI-ACTIVE 1, GPRS-CSI-ACTIVE 1, CAMEL-CSI-NAME AIJK1</td>
</tr>
<tr>
<td>Session ID: 000000000000000000002010-08-30</td>
<td>Sequence Number: 000000520</td>
<td>Count: 2</td>
<td>SUCCESS</td>
<td>ICAP</td>
<td>UPDATE</td>
<td>GSUB</td>
</tr>
<tr>
<td>SUCCESS</td>
<td>ICAP</td>
<td>UPDATE</td>
<td>GSUB</td>
<td>KEY=655016620096404</td>
<td>PARAMS</td>
<td>CAMEL-ACTIVE 1, ECMN-SMS-CSI-ACTIVE 1, CAMEL-RQST-LOC-INFO 1, CAMEL-RQST-SUB-STATE 1, CAMEL-CSI-NAME AIJK1</td>
</tr>
</tbody>
</table>
XYGATE Merged Audit
PC-Based Report Scheduling

• Each Report can be scheduled automatically & be delivered via email or ftp in various file formats
XYGATE Merged Audit

Configuring Alerts

• The heart of Merged Audit is the FILTERS file
  • This file contains FILTERs, which determine which audit records are written to the database and generate actions such as:
    ▪ Sending audit data to a SIEM via Syslog
    ▪ Sending an EMS message where it can be picked up by Prognosis or ASAP
    ▪ Sending an alert via email, text message, or pager
    ▪ Sending a message via an SNMP Trap, which can be picked up by enterprise-wide applications like OpenView, Tivoli and others.
XYGATE Merged Audit
Configuring Alerts

• A filter “skeleton”

FILTERDEF
BEGIN $MY-FILTER
STATUS [ACTIVE | INACTIVE]
MOVER_BEGIN
 MOVER_SELECT_BEGIN
   define MOVERs here
 MOVER_SELECT_END
MOVER END
!Data selection:
DATA_BEGIN
 DATA_SELECT_BEGIN
   Describe audit events here
 DATA_SELECT_END
DATA END

!Actions:
ACTIONCOLL_BEGIN
   ACTION_BEGIN
     Define actions here
 ACTION_END
ACTIONCOLL_END
FILTERDEFEND
XYGATE Merged Audit

Configuring Alerts

• To configure an email alert:
  • Define NonStop server TCP/IP process & outgoing port
  • Define the receiving email server
  • Design the Subject Line for the email
  • Design the body of the email you want sent for each event you’re interested in alerting via email.

• Token Substitution
  • Allows you to insert the contents of columns for the particular event into the email subject or message. So for example, Merged Audit can send an email that says “OPER.JOE logged on as SUPER.SUPER”
XYGATE Merged Audit

A Sample EMAIL Configuration

- ACTION_BEGIN
- ACTIONTYPE MAIL
- MAIL_SRV MAIL.xypro.com
- MAIL_PORT 25
- MAIL_FROM xma@xypro.com
- MAIL_TO tlhill@xypro.com
- MAIL_IPPROCESS $ZTC0
- MAIL_SUBJECT
  | (INSTALL.SYSTEMNAME) | | (AUDIT.SUBJECTLOGIN) | altered | (AUDIT.OBJECTNAME) |
- MAIL_BODY
  "NODE: | (INSTALL.SYSTEMNAME) | "
  "Time: | (AUDIT.RECORDLCT) | "
  "Event: | (AUDIT.SUBJECTLOGIN) | altered | (AUDIT.OBJECTNAME) | "
  " | (AUDIT.RESULT) | "
  "Outcome (Success = 1; Fail = 3) = | (AUDIT.OUTCOME) | "
- MAIL_BODY_END
- MAXRECORDAGE 3600 ! 1 hour
- ACTION_END
XYGATE Merged Audit
Configuring EMAIL

• Resulting EMAIL sent by the FILTER on the previous slide:

```
From:  terri_h@xypro.com
To:    Terri Hill
Cc:    
Subject: X SUPER.SUPER altered SAFEGUARD

NODE:   \X
Time:    2010-09-16 16:34:56.388839
Event:  SUPER.SUPER altered SAFEGUARD
         Max attempts 3 to 6
Outcome (Success = 1; Fail = 3) = 1
```
HP Compliance Log Warehouse
HP Compliance Log Warehouse (CLW)

Compliance Event Management for NonStop

High performance appliance with compliance analysis and real-time alerts

Secure, centralized event capture and analysis

- Collects, compresses and stores log record data in a replicated repository designed for high speed analysis to support audits or forensic investigations.
- Supports multiple servers across the data center.

Automates expensive data capture

- Collects and parses millions of events
- Provides multiple types of reports as well as ad hoc reporting for compliance analysis.

Real-Time Alerts

- Real Time Alert Manager scans logs and record data from numerous sources in real-time to alert when potential security related or natural events occur.
- Alerts trained personnel for action.
The Data Streaming transfer method uses syslog (incorporated into Merged Audit) to use UDP to stream or “push” data to the CLW continually from the NonStop server.

This data transfer method offers close to “real time” data availability for reporting.

There is some risk - if network is interrupted during update a potential event data loss is possible.
NonStop OS Bundle
Security additions

What is included with the OS for audit and compliance reporting?
What is HP doing?

As of September 1st, orders for new NonStop servers now include new security products as part of the basic OS software suite provided with the system.

This change affects Integrity NonStop servers that run J Series or H Series software. One of the new products included is:

   XYGATE Merged Audit
   (With all features as currently sold by XYPRO)

• Supported on H06.06 or later and J06.03 or later
• No special firmware required.
• System needs to include Pathway
Further benefits

Deploy when you’re ready
- Product is delivered on your RVU SUT
- Configure and install both products or just the product(s) you want
- No coldload necessary to put these products into production
- No license file needed to access product functionality

Support is provided by HP through the HP Support Center – the same number you call for all your other NonStop support questions or needs
- HP will engage partner if necessary behind the scenes

Ordering through HP is easy
- Products available worldwide in OS with small price increase
- Avoids the need to qualify a new vendor in some markets
Customers with Existing Systems

J Series or H Series platforms

Customers with existing systems can upgrade their OS to include the Security enhancement.

Upgrades are available after Nov 1st, 2010, to any customer running J Series or H Series systems.

Included in J06.10 or H06.21 SUTs, but may be installed on downrev RVUs to J06.03 or H06.07.

Upon purchase, future SUTs for your system will include this software product and its latest versions.

See your HP Sales person to receive a quote
NonStop Systems
Future XYGATE Merged Audit offerings

G Series
XYGATE Merged Audit will be available for separate purchase from HP after November 1\textsuperscript{st}, 2010 for G Series NonStop systems.

Special Merged Audit Plug-ins

ACI Base24 Support
A special plug-in for XYGATE Merged Audit will provide integration of ACI Base24 log data into the Merged Audit database. This product is available for separate purchase from HP after November 1\textsuperscript{st}, 2010.

HLR Support
A special plug-in for XYGATE Merged Audit will allow customers to include log data from HLR into their Merged Audit database. This product will be available for separate purchase from HP in early 2011.

Both Plug-ins are available for systems running J Series, H Series and G Series software.
## Schedule and Availability

<table>
<thead>
<tr>
<th>September</th>
<th>October</th>
<th>November</th>
<th>December</th>
<th>2011</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>New security products now included with new orders for NonStop OS on J Series and H Series</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Security Product upgrades now available for J Series and H Series customers with existing systems</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>XYGATE Merged Audit becomes available from HP for the first time!</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>XYGATE Merged Audit available for separate purchase on G Series</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>XYGATE Merged Audit plug-in for ACI Base24 applications becomes available for J Series, H Series and G Series</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>XYGATE Merged Audit plug-in for HLR application environments becomes available for J Series, H Series and G Series</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

See your NonStop sales representative for more information.
NonStop Systems
Areas under future consideration

More logs are being investigated to be collected by Merged Audit in the future. There’s no schedule at this time. Items being examined include:

iTP Secure WebServer
SSH Logs
SSL Logs
NetBatch
Other “partner” application logs

If you have another area you’re interested in, please let us know.
The wolves are at the door . . . be sure you know what’s happening on your system.
Questions?
NonStop Security Contacts

Who to contact

Karen Copeland
NonStop Product Manager for Security
karen.copeland@hp.com

Wendy Bartlett
Distinguished Technologist, NonStop
wendy.bartlett@hp.com

Lisa Partridge
VP Marketing and Sales, XYPRO Corporation
Lisa_p@xypro.com
Outcomes that matter.