Nsure Audit: Instrumenting Custom Applications:

Integrating and Instrumenting Applications with Nsure Audit

Jim Gerken
Nsure Lead - Novacoast, Inc.

Rick Meredith
Novell, Inc.

Chris Steipp
Developer - Novacoast, Inc.

Novell.

The Presenters

Jim Gerken

- Nsure Identity Manager Lead – Novacoast, Inc.
- Mostly does Identity Manager – DirXML these days.

Rick Meredith

- Developer: Nsure Audit Team – Novell, Inc.
- iManager plugins, Platform Agent, java channels

Chris Steipp

- Developer – Novacoast, Inc.
- Various and Sundry programming projects around Nsure

Nsure Audit Components

Instrumentation

- Push code
- Most Familiar With Application

Platform Agent

- Secure Transmission
- Caching

Secure Logging Host

- Signing and Chaining - Non-Repudiation

Data Store

- Reporting Data – Application Specific

Reasons to Instrument an Application

Systems Administration Tool

- Notification Engine
- Administration Logging/Trending

Security Tool

- Audit Trail
- Compliance Documentation

Data Integrity Tool

- System Level Data Tracking
- Process Flow Tracking

Design Choices

What functions can be instrumented?

Re-utilize existing instrumentation?

What platform to use?

Java or Native?

Is Data Properly Sized?

Can Data be Normalized?

Novell.

Design Process for NNASyslog....

Client Requirements

- Audit events from Windows Servers, Active Directory, Network Infrastructure, Unix Operating Systems, in Addition to eDirectory, Netware, and Identity Manager
- Audit events for Security Department
- Medical Organization – HIPAA Compliance

Common Thread? - None

Instrumenting Eight Systems – None of Which Are Open

Novell.

Design Process for NNASyslog....

Syslog!

- Native to Unix
- Native to Network Infrastructure
- Syslog Instrumentation For Windows Exists
- Flexible and Easy To Instrument

Issues

- Data not Normalized
- Heavy Use of Text Strings
- Clear Text Transmission

Design Process for NNASyslog....

Platform Choices

- Windows – ugh!
- Unix – not flexible, or in client environment
- Linux – Yay!

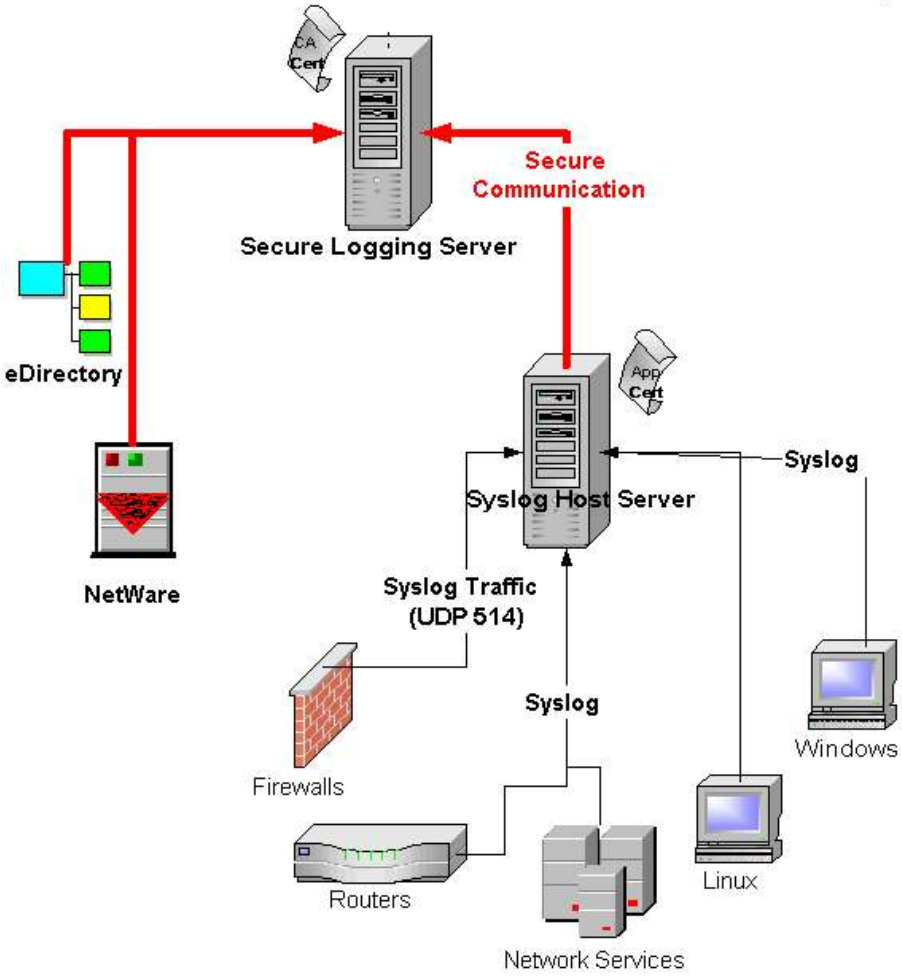
How Should Data Flow?

How to Implement?

Where is Data Stored? – Attribute Mapping

Novell.

Implementation of NNASyslog - Layout



Novell.

Implementation of NNASyslog - Design

Decide on your Application ID

- Get one from Novell
- Use FFF0-FFFF

Compile List of Events

- This will eventually be your .lsc file

External vs. Embedded Keys

- Is Non-Repudiation Unnecessary?
- Is Non-Repudiation Optional?
- Is Non-Repudiation Required?

Caching vs. Non-Caching

- Dangers to Both!

Implementation of NNASyslog - Coding

```
#include <logevent.h>

unsigned char      *PKey = {
 "-----BEGIN RSA PRIVATE KEY-----\r\n"
 "MIIBOwIBAAJBALbEj/+zMrG26WCdW01YQMjaweYEWi0gTHM4X6tgvA47GjbUXDKY\r\n"
 "imO8jqGnFTP2ZB2MDM7+vz8ipKtkcv7WR08CAwEAAQJAfMt4e6MTUU9QyTyI1CYX\r\n"
 "jk34qaN9I2TzbpUmlfFmVtwSwLthbsokqtLl2hP7GcDWP1OjJbQQ0TaZHnrtjorB\r\n"
 "KQIhAN8E3CPlVORKppVaDlhWtECGGcLvj4Q533pWxNAjj34lAiEA0cvburq0ntsL\r\n"
 "2BT/Q87ZF/6dsIZcRkn3fpSPF2Xg02MCIQDSWK4duS8Bh5tpIKCJF3Y5qYHgx7zQ\r\n"
 "VRmANRi6y9+KdQIgH8F7wQgBzwnZARwsh1cIBVnFBLNRxFHt5HsYLbJ+FYECIQC5\r\n"
 "7QSTJt9T2J8Ye9cU1f1+hsYdBUOYf5IPUtqjORahNA==\r\n"
 "-----END RSA PRIVATE KEY-----\r\n"
 };
```


Novell.

Implementation of NNASyslog - Coding

```
LOGHANDLE handle;
unsigned long                LogError;
unsigned char                CertPath[_MAX_PATH+1];
unsigned char                PkeyPath[_MAX_PATH+1];
// Get Handle to the Platform Agent
  Handle=LogOpen(CertPath, PKeyPath, LE_FILE_CREDENTIALS|
  LE_SIGNED_CHAIN|LE_NO_CACHING, &LogError);
  //or
  Handle=LogOpen(CertPath, PKeyPath, LE_FILE_CREDENTIALS|
  LE_SIGNED_CHAIN, &LogError);
  //or
  Handle=LogOpen(Cert, PKey, LE_SIGNED_CHAIN, &LogError);
// Log the Event
  LogEventExt(Handle, component, EventIDLog, log_level, 1, 0,
  OrigHost,0, 0, 0, 0, (unsigned char *)Host, ShortMessage, 0, Seq,
  0, 0, MIME_TEXT_PLAIN, ndx-2, theMessage+2)
  //or
  LogEventDirect(Handle, component, EventIDLog, ....
LogClose(Handle);
```

Reporting Issues

Explore the Raw Data

Explore Data as Stored

How to set Notification Criteria

How to Report on Data

Novell.

Summary

Know your Application and Data

Pick your Platform and Language Properly

Normalize Data for Easy Reporting

Novell.

For More Info.....

- These slides are available at
  http://www.novacoast.com/seminars/brainshare2005.php

- Novell Nsure Audit NDK
  http://developer.novell.com/ndk/naudit.htm

- Novell Forge – Audit SDK thread
  http://forge.novell.com/modules/xfmod/newsportal/thread.php?group_id=1157&group=novell.devsup.naudit

```
<xsl:template match=”QUESTION”>
        <call-template name=”ANSWER”/>
</xsl:template>
```


Novell.

Novell®

Novell