Compliance Security Suite for Operations Manager 2007

Jeremiah Beckett
CEO, Chief Architect
www.SecureVantage.com
Agenda

• ACS Overview
• Compliance Security Suite
  • Security Management Packs
  • Audit Collection Solutions
• Moving Forward
Audit Collection Requirements

- Compliance
  - centrally collect, monitor, archive & report security events
- Auditing
  - Maintain audit trail of internal security related activities
- Scalable & Secure
  - Infrastructure must guarantee collection and integrity of huge volumes of security events
OM 2007: Audit Collection Service

Key Design Principles:
- Near real time exporting of all security events vs batch copy
- Immutable collection policy – tamper resilient
- Network friendly, lightweight, compressed event forwarding
- Scalable (collection points and event volume)
- Schematized events for improve analysis and reporting
- Efficient on-line storage

Customer Value-Add
- Integrated with Operations Manager 2007 infrastructure
- Functionality included in the Operations Manager 2007 OMLs
- Out-of-the-box, customizable reports from Microsoft
- ACS extensions provided by Secure Vantage, including
  - Advanced security alerting and reporting library (free download)
  - Data consolidation and archiving
  - Forensic reporting for compliance and auditing
The Principles of Audit Collection

Monitored Clients

Monitored Servers

Events subject to tampering

Audit Collector

Audit DB

Events under control of auditors

Data Archival

© Copyright 2007 Secure Vantage Technologies. ALL RIGHTS RESERVED
ACS Collectors: Design Requirements

- High Performance
  - Each collector must support up to 2,500 events*/sec (continuous load)
  - Peak load support per collector: up to 100,000 events*/sec (short burst only – non sustainable)

- High Scalability
  - With default audit policy, a single collector to support:
    - 3,000 non-DC servers, or
    - 150 Domain Controllers, or
    - 20,000 workstations

*Average bytes per event over the wire =< 100 bytes
Example System for ACS Microsoft IT (Pre-production Sampling)

- **Storage**
  - EMC CX700 SAN for 2 Audit Collectors
    (via Cisco MDS9509 fiber channel switches)
  - All LUNs are RAID 5
  - Cache: 4GB per controller
    - 300MB Read Cache allocated on each controller
    - Remaining 2.3GB Write Cache allocated (mirrored across both)
    - Approx. 800MB is dedicated to each controller
  - **Total storage capacity ~1TB**

- **Network**

<table>
<thead>
<tr>
<th>Name</th>
<th>Average Event Rate (events/sec)</th>
<th>Current Event Rate (events/sec)</th>
<th>Average Uncompressed Event Size (bytes)</th>
<th>Average Event Size on Wire (bytes)</th>
<th>Compression Ratio</th>
</tr>
</thead>
<tbody>
<tr>
<td>DC 4</td>
<td>42.7</td>
<td>65</td>
<td>518.7</td>
<td>59.8</td>
<td>8.64</td>
</tr>
<tr>
<td>DC 1</td>
<td>41.3</td>
<td>41</td>
<td>516.4</td>
<td>72.5</td>
<td>7.12</td>
</tr>
<tr>
<td>DC 6</td>
<td>27.5</td>
<td>30</td>
<td>483.0</td>
<td>69.4</td>
<td>8.13</td>
</tr>
<tr>
<td>DC 5</td>
<td>202.7</td>
<td>199</td>
<td>471.9</td>
<td>62.1</td>
<td>7.60</td>
</tr>
</tbody>
</table>

© Copyright 2007 Secure Vantage Technologies. ALL RIGHTS RESERVED
What’s Missing?

- Audit Collection only gathers data from Windows Security Logs
- Data collected needs to be archived and reported on past online storage abilities
- Reporting across multiple Collectors
- Security Alerting and Operations
- Regulatory Compliance Support
Extending OM With Secure Vantage

Management Packs
- System Auditors
- Application Auditors
- Anti-virus Auditors
- Compliance Experts

Secure Vantage Solution Architecture
System Center Operations Manager 2007 and the Audit Collection Service

Operations Manager 2007 ACS Collector
Reporting Database

ACS Reporting
- Base Reporting
- Auditing Modules
- Compliance Modules
- Optimizing Modules

Secure Vantage MP Library

Secure Vantage Reporting Library

Extending OM With Secure Vantage
Secure Vantage Value-Add Solutions

- Security Solutions
  - Security Auditor Management Packs
  - Audit Collection Reporting Solutions

- Solution Features
  - Integrated Best Practices
  - Regulatory Compliance Support
  - Embedded Security Knowledge & Best Practices
  - Auditing and Operations
  - Built on System Center technology
Security Management Packs

- Security Core Auditors
  - Windows Security Auditor
  - Group Policy Auditor for Windows Server
  - Security Top Alerts MP*

- Application Auditors
  - SQL Security Auditor
  - ISA Security Auditor
  - Anti-Virus Auditors

*free download www.securevanlage.com
Windows Security Auditor MP

- ACS and Non-ACS Versions
- Server & Workstation Auditing
- Multi-Event Correlated Alerting
- Intrusion Detection
- Security Dashboards
- Public Security Health Model
- Rich Knowledge Content
- Compliance Modules

*Includes Audit Collection Forensic Analyzer*
Group Policy Auditor MP

- Windows Server Policy Auditing
- Rich Policy Discovery
- Change Audit & Impact Analysis
- Historical Change Reporting
- Compliance Alerting

RSoP in Operations Manager
Application Auditor MPs

- Core Application Auditors (SQL & ISA)
  - Account & Permission Changes
  - Object Changes (ie Tables, SP, Config, etc.)
  - Authentication Events
- Anti-Virus Auditors
  - FCS, McAfee, Symantec, Trend Micro
  - Availability and Integrity auditing
MP Knowledge Content

- Industry Expert Guidance
  - Microsoft Security MVP
  - Microsoft Group Policy MVP
  - Microsoft Ops Mgr MVP
- Online Training Links
- Regulation Knowledge
- Technical Article Links
Security Event Knowledge

Summary
This indicates the system's audit policy was modified. Pluses indicate auditing was enabled, minuses indicate it was disabled.

Configuration
To view a system's audit policy settings, you can open the Local Security Policy console on the computer and maneuver to Security Settings\Local Policies\Audit Policy.

Causes
Event 612 occurs when the audit policy of a system changes.

Additional Information
This is an important event that might indicate tampering with the Security Log.

Success and Failure Auditing Reference
- - Success disabled, Failure disabled
- + Success disabled, Failure enabled
+ + Success enabled, Failure enabled
+ - Success enabled, Failure disabled

External Knowledge Sources
Online Security Encyclopedia - Event 612
Compliance MP Libraries

- Extend Standard MPs
  - Operational Views
  - Health Monitors
  - Knowledge Content
- Compliance Modules
  - CoBITs, FISMA, HIPAA, ISO, PCI, SOX and others
## Compliance Knowledge

### Summary

**HIPAA**

Security Standards for the Protection of Electronic Protected Health Information

**$\S$164.312 Technical Safeguards**

The Security Rule defines technical safeguards in §164.304 as "the technology and the policy and procedures for its use that protect electronic protected health information and control access to it."

### Configuration

**Technical Safeguard Matrix**

<table>
<thead>
<tr>
<th>Standards</th>
<th>Section</th>
<th>Control</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control</td>
<td>164.312(a) (1)</td>
<td>Unique User Identification</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Emergency Access Procedure</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Automatic Logoff</td>
<td>Addressable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Encryption and Decryption</td>
<td>Addressable</td>
</tr>
<tr>
<td>Audit Controls</td>
<td>164.312(b)</td>
<td>Required</td>
<td></td>
</tr>
<tr>
<td>Integrity</td>
<td>164.312(c) (1)</td>
<td>Mechanism to Authenticate Electronic Protected Health Information</td>
<td>Addressable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Access Control Authentication</td>
<td>Addressable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Transmission Security</td>
<td>Addressable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Integrity Controls</td>
<td>Addressable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Encryption</td>
<td>Addressable</td>
</tr>
</tbody>
</table>

### External Knowledge Sources

- Centers for Medicare & Medicaid
- Office for Civil Rights (HIPAA) ~ Health & Human Services

### Summary

**Unique User Identification $\S$164.312(a)(1)(i)**

*Assign a unique name and/or number for identifying and tracking user identity.*

User identification enables organizations to validate and track user activity.

### Configuration

While the rule does not describe or provide a single format for user identification Microsoft Windows Active Directory supports this rule with assigning unique Security Identifiers (SID) to user accounts.

### Causes

Event 624 occurs when a new user account is created in Active Directory

### Additional Information

When you create a user account, you'll find an expected instance of event ID 624, User account created. But because of the way that the MMC Active Directory Users and Creators snap-in interacts with AD, you'll also see a series of event ID 642 instances interspersed with an instance of event ID 626, User account enabled, and event ID 628, User account password set.

### External Knowledge Sources

- Centers for Medicare & Medicaid
- Office for Civil Rights (HIPAA) ~ Health & Human Services

**Copyright 2007 Secure Vantage Technologies. ALL RIGHTS RESERVED**
Public Security Health Model

- Security Controls
  - Acct Mgt, AV, System, Policy
- Framework Specific
  - FISMA, ISO, PCI
- Unknown
DEMO

Security Management Packs
Security Reporting Libraries

- Base Reporting
  - Core event analysis and auditing
- Auditing Modules
  - Targeted activity auditing modules
- Compliance Modules
  - Guidance, control mapping and accountability
- Optimization Modules
  - Vertical solutions for historical and consolidated reporting services
Secure Vantage Reporting

Technology Features

- Localization Support
- User SID Filtering
- Event Correlation and Enrichment
- Dynamic Reporting Schema
- Archiving and Restoration
- Compliance Knowledge

Usability Features

- Comprehensive Forensic Analysis
- Dynamic Grouping and Sorting
- PDF Optimization
- Document Maps aka Bookmarks
- Multi-Select Filter Options
- Summary to Detail Drilldown
- Noise Filtering Templates
Security Reporting Core

- Base Reporting
  - Forensic Analyzer
  - IT Auditors Pack
- Auditing Modules
  - Anomaly Identification Reporting
  - Admin Tracker
  - Data Access Tracker
  - Intrusion Detection Reporting
Forensic Analyzer

- Report Analysis
  - Account Management
  - Auditing Integrity
  - Directory Services
  - Logon Activity
  - Object Access
  - Policy Changes
  - Privilege Use
  - Windows Firewall
  - Event Load Analysis

*Included with Windows Security Auditor*
IT Auditors Pack

- Feature Highlights
  - Audit Scenario Reporting
  - Designed by Microsoft Security MVP
  - Support Windows & Vista events
  - Free Download Version

- Better than Out-of-Box
  - Enriched Attributes
  - Document Maps
  - User SID Filtering
  - Dynamic Grouping
  - Advance Filter Options
  - Event Detail Drilldown
IT Auditors Pack+

- Usage Scenario's
- Guidance
  - Audience
  - Frequency
  - Rationale
  - Regulations
    - CoBITs
    - ISO
    - PCI
    - SOX
    - FISMA, HIPAA and others
DEMO

Audit Collection Reporting
Optimization Modules

- Vertical Solutions (Support all Reporting Modules)
- ACS Archiver
  - Compressed Log Archiving
  - Historical Reporting
- Collector Consolidator
  - Aggregated Collector Reporting
  - Correlated Noise Filtering
  - AD Enriched Reports
Audit Collection Archiver

**Exporter Module**
- Daily Partition Archival
- Additional 8-12x Compression Ratio
  - 60-80x compression of original .evt
  - 100gig .evt file ~ 12gig in ACS ~ 1.5gig Archived

**Loader Module**
- Restore Archive sets
- Dynamically recreates SDK views
- Supports loading from multiple collectors
Archiver Architecture
Integration Services Overview

- **Security Log Provider**
  - Registration of new Windows Security events
  - Supports local and proxy event services
  - Integrates events with ACS collection stream
  - Ideal for Windows Application Security events

- **Alerting and Reporting Services**
  - Enables heterogeneous security auditing and reporting with Operations Manager
  - Standardized event schema supports existing reporting modules
  - Archiving and historical reporting capabilities
ACS Integration Services

Security Event Registration

- Event Definition Submission
- SVT Event Repository
- SVT Event Schema Map (XML Metadata)
- Generate Event Log Message Map
- Event Log Messages Format
- Register Messages with Security Log & Audit Collection

Security Event Creation

- Event Collection
- SVT Provider
- Write Messages to Security Log

Uses SVT Event Schema to map events to the format expected by the Event Log and for integration with Audit Collection Services and associated solutions. *Available as Windows Service or DLL

ACS Integration Services
Integration Services Value

- Extensible Architecture
  - Integrate In-House Application Security
- New Opportunities
  - Heterogeneous Security Reporting
  - Cross Platform/Application Intrusion Detection
- Partner Involvement (nonWindows)
  - Engyro Corporation
  - eXc Software
AD Mentat ~ Codenamed Duncan

- AD Audit Reporting
- Uses SQL Reporting
- ACS Report Integration
- Express & Studio

Data Discovery
- Domains & OU Objects
- Users & Groups
- Object ACLs

Reporting
- Group Membership
- User Details
- Audit Scenarios
- Delta Comparisons
- ACS Report Hooks

'Mentats are able to sift large volumes of data and devise concise analyses in a process that goes far beyond logical deduction'
Solution Availability

- Security Auditor MPs
  - Windows Security Auditor
  - Group Policy Auditor for Windows Server
  - Security Top Alerts MP (free download)*
  - SQL Security Auditor
  - ISA Security Auditor
  - Anti-Virus Auditors

- Security Reporting Solutions
  - Base Reporting
  - Auditing Modules
  - Compliance Modules
  - Optimization Modules

Availability
- Available
- Available
- Mar 2007
- Mar 2007
- Summer 2007
Pricing

Management Packs
- Licensed per Management Group & Monitored Device
- Standard & Enterprise
  - Standard: Windows Security Events and Group Policy Auditing
  - Enterprise: Standard + Application Security Auditing
- Standard MP $1,200 ; $85 per Server

Audit Collection
- Licenses per Audit Collector Database
- Standard & Enterprise
  - Standard: Archiver & Base Reports
  - Enterprise: Standard + Auditing & Compliance Modules
- Standard License: $6,000
Secure Vantage 2007 Roadmap

- Security MPs
  - Server Auditors
  - Application Auditors
  - Anti-Virus Auditors
- Audit Collection Reporting
  - Compliance and IT audit scenario reporting
  - Archiving and Consolidation services
- Extending Reporting
  - Non-Windows and Application security reporting
  - Audit Collection Integration Services
  - Active Directory Reporting
Compliance Security Suite

QnA

www.SecureVantage.com

© Copyright 2007 Secure Vantage Technologies. ALL RIGHTS RESERVED