Randy Franklin Smith's ULTIMATE WINDOWS SECURITY .COM™

Auditing SharePoint® Activity for Compliance and Security

- Made possible by: LOGbinder SP, solarwinds LOG & EVENT MANAGER

Randy Franklin Smith's ULTIMATE WINDOWS SECURITY .COM™

Brought to you by:

LOGbinder SP

www.logbinder.com

Randy Franklin Smith
Creator of LOGbinder

solarwinds LOG & EVENT MANAGER

www.solarwinds.com

Rob Johnson
Sr. Sales Engineer

LOGbinder SP™
solarwinds

Preview of Key Points

- **Risks of not auditing SharePoint**
- **Native SharePoint audit foundation**
- **Building on the foundation**
  - SolarWinds® Log & Event Manager
  - LOGbinder SP

LOGbinder SP™
solarwinds

Risks of not auditing SharePoint

- **Customer information disclosure**
  - Liability, notification costs, loss of good will
- **Trade secrets and intellectual property**
- **Human resources data**
- **Regulatory penalties and liability**
  - SOX
  - PCI
  - HIPAA
  - GLBA

LOGbinder SP™ solarwinds

Native SharePoint audit foundation

- **Available in**
  - Window Server System® (WSS) 3.0
    - Not exposed in the interface
  - SharePoint 2007
  - SharePoint Foundation
    - Not exposed in the interface
  - SharePoint 2010

LOGbinder SP™ solarwinds

Native SharePoint audit foundation

- **Audit policy defined**
  - Site collection level
  - List/Library level
  - No way to set global audit policy or automatically audit new site collections
- **What can you audit?**
  - Changes to audit policy
  - Permission changes
  - Group membership changes
  - View
  - Check in/out
  - Delete/Update
  - Schema changes
  - Workflow
  - Search

LOGbinder SP™
solarwinds

Native SharePoint audit foundation

- **Where is the SharePoint audit log?**
  - Stored in the content database
  - Accessible via Audit Reports under Site Collection Administration
- **Can you rely on the native audit log?**
  - Provides an accurate audit trail
  - But limitations exist

LOGbinder SP™
solarwinds

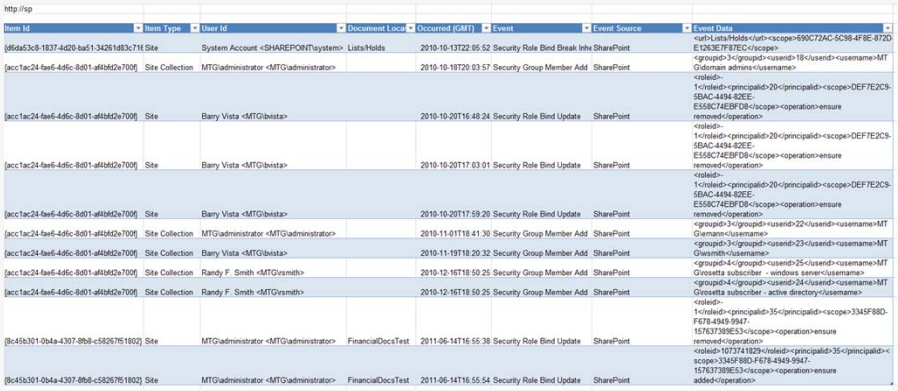
Native SharePoint audit foundation

- **Audit records written to internal table within content database**
  - Inaccessible to log management solutions
  - Consumes SQL/SharePoint® storage
  - Stores audit logs on same system where they are generated

LOGbinder SP™ solarwinds

Native SharePoint audit foundation

- **Rudimentary Excel® reports available**
  - Audit codes, object ID numbers, user and group ID numbers not translated



http://sp

Item Id	Item Type	User Id	Document Loca	Occurred (GMT)	Event	Event Source	Event Data
{d6da53c8-1837-4d20-ba51-34261d83c71f}	Site	System Account <SHAREPOINT\system>	Lists/Holds	2010-10-13T22:05:52	Security Role Bind Break Inhe	SharePoint	<url>Lists/Holds</url><scope>690C72AC-5C98-4F8E-872D-E1263E7F87EC</scope>
{acc1ac24-fae6-4d6c-8d01-af4bfd2e700f}	Site Collection	MTG\administrator <MTG\administrator>		2010-10-18T20:03:57	Security Group Member Add	SharePoint	<groupid>3</groupid><userid>18</userid><username>MTG\domain admins</username>
{acc1ac24-fae6-4d6c-8d01-af4bfd2e700f}	Site	Barry Vista <MTG\bvista>		2010-10-20T16:48:24	Security Role Bind Update	SharePoint	<roleid>-1</roleid><principalid>20</principalid><scope>DEF7E2C9-5BAC-4494-82EE-E558C74EBFD8</scope><operation>ensure removed</operation>
{acc1ac24-fae6-4d6c-8d01-af4bfd2e700f}	Site	Barry Vista <MTG\bvista>		2010-10-20T17:03:01	Security Role Bind Update	SharePoint	<roleid>-1</roleid><principalid>20</principalid><scope>DEF7E2C9-5BAC-4494-82EE-E558C74EBFD8</scope><operation>ensure removed</operation>
{acc1ac24-fae6-4d6c-8d01-af4bfd2e700f}	Site	Barry Vista <MTG\bvista>		2010-10-20T17:59:20	Security Role Bind Update	SharePoint	<roleid>-1</roleid><principalid>20</principalid><scope>DEF7E2C9-5BAC-4494-82EE-E558C74EBFD8</scope><operation>ensure removed</operation>
{acc1ac24-fae6-4d6c-8d01-af4bfd2e700f}	Site Collection	MTG\administrator <MTG\administrator>		2010-11-01T18:41:30	Security Group Member Add	SharePoint	<groupid>3</groupid><userid>22</userid><username>MTG\emann</username>
{acc1ac24-fae6-4d6c-8d01-af4bfd2e700f}	Site Collection	Barry Vista <MTG\bvista>		2010-11-19T18:20:32	Security Group Member Add	SharePoint	<groupid>3</groupid><userid>23</userid><username>MTG\bvsmith</username>
{acc1ac24-fae6-4d6c-8d01-af4bfd2e700f}	Site Collection	Randy F. Smith <MTG\rvsmith>		2010-12-16T18:50:25	Security Group Member Add	SharePoint	<groupid>4</groupid><userid>25</userid><username>MTG\rosetta subscriber - windows server</username>
{acc1ac24-fae6-4d6c-8d01-af4bfd2e700f}	Site Collection	Randy F. Smith <MTG\rvsmith>		2010-12-16T18:50:25	Security Group Member Add	SharePoint	<groupid>4</groupid><userid>24</userid><username>MTG\rosetta subscriber - active directory</username>
{8c45b301-0b4a-4307-8fb8-c58267f51802}	Site	MTG\administrator <MTG\administrator>	FinancialDocsTest	2011-06-14T16:55:38	Security Role Bind Update	SharePoint	<roleid>-1</roleid><principalid>35</principalid><scope>3345F88D-F678-4949-9947-157637389E53</scope><operation>ensure removed</operation>
{8c45b301-0b4a-4307-8fb8-c58267f51802}	Site	MTG\administrator <MTG\administrator>	FinancialDocsTest	2011-06-14T16:55:54	Security Role Bind Update	SharePoint	<roleid>1073741829</roleid><principalid>35</principalid><scope>3345F88D-F678-4949-9947-157637389E53</scope><operation>ensure added</operation>

LOGbinder SP™ solarwinds

Native SharePoint audit foundation

- **No alerting**
- **Audit log purging introduced with SP2010**

LOGbinder SP™
solarwinds

Native SharePoint audit foundation

- **Limitations in WSS and Foundation**
  - Audit engine present
  - Auditing only possible through application that interfaces with SharePoint API

LOGbinder SP™
solarwinds

Building on the foundation

LOGbinder SP™
solarwinds

Turn data into information

- **LOGbinder SP Agent**
  - Translates SharePoint audit records into human readable audit trail
  - Sends SharePoint audit events to the Windows event log
  - Purges events after export


Permissions updated
Occurred: 6/14/2011 12:55:54 PM
Site: http://sp
User: MTG\administrator
Object
Type: List
Subtype: Document Library
URL: /FinancialDocsTest/Forms/AllItems.aspx
Title: FinancialDocsTest
Description: n/a
Target
Name: MTG\domain users
Type: User
Permissions
Role name: Full Control
Role description: Has full control.
One instance of this event is logged for each role assigned this user. Look at adjacent events to determine all roles assigned to the user or group.

For more information, see http://logbinder.com/support

LOGbinder SP™
solarwinds

Take action on the information

- **SolarWinds LEM**
  - Built-in support for LOGbinder SP
  - Secure, long term log archival
  - Alerting
    - Recommended default alerts already implemented
  - Reporting
    - Recommended reports already implemented
    - Schedule reports daily, weekly, monthly

LOGbinder SP™
solarwinds

Bottom Line

- SharePoint increasingly used to store and process sensitive information
- Becoming an IT audit and compliance target
- Auditing, alerting, reporting is a must for any technology like SharePoint
- SharePoint native auditing is a foundation technology
- SolarWinds LEM with LOGbinder SP builds on that foundation to provide fully managed audit and security monitoring for SharePoint

Next steps

- Download evaluation copy
- Schedule a demo

www.logbinder.com/sp
www.solarwinds.com