

RANDY FRANKLIN SMITH'S
ULTIMATE WINDOWS SECURITY

**Taming SharePoint Audit Logs with
LOGbinder SP and EventTracker**

Sponsored by:



© 2009 Monterey Technology Group Inc.



Brought to you by



www.logbinder.com

Randy Franklin Smith
Creator of LOGbinder SP



www.prismmicrosys.com

Isaac Thompson
Director of Engineering and Training

© 2009 Monterey
Technology Group Inc.

- Does SharePoint have an audit log?
- Which versions/editions?
- How do you enable auditing?
- What events/activity does it allow you to audit?
- Where is the log stored?
- How do you view the log?
- What's wrong with the SharePoint audit log?

- Yes

Which versions / editions?

Version

- 3.0 / 2007

Editions

- Windows SharePoint Services 3.0
- Office SharePoint Server 2007 for Search
- Office Forms Server 2007
- Office SharePoint Server 2007 Standard
- Office SharePoint Server 2007 Enterprise
- Office SharePoint Server 2007 for Internet Sites

How do you enable auditing?

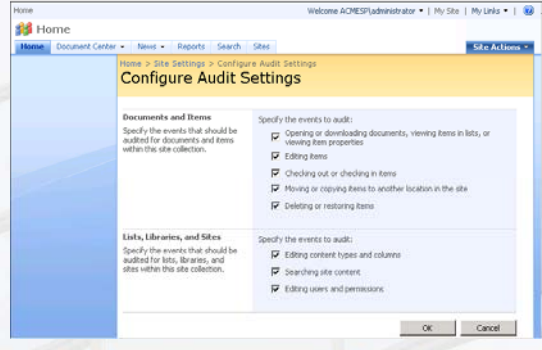
Windows SharePoint Services

- No interface or command line utility
- Script the SharePoint object model

How do you enable auditing?

Office SharePoint Services

- Site Collection Administration \ Site collection audit settings



Where is the log stored?

SharePoint content database in SQL Server

- “audit event entries ... are stored with all other content such as list items, documents...” - TechNet
- Tables in SharePoint content SQL database

Not designed for direct access

How do you view the log?

Windows SharePoint Services

- No interface or command line utility
- Script the SharePoint object model

How do you view the log?

Office SharePoint Server

- Handful of rudimentary Excel reports
- Cryptic
- Essentially broken



What do reports look like?

Content Modification

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
Site Id	Item Id	Item Type	User Id	Machine N	Machine #	Document	Location	T Occurred (GMT)	Event	Custom E	Event S	Source N	Event Data																					
307602c-f56b4398	Document	SHAREPC				Lists/WorkURL		2009-01-04T01:09:45	Update		SharePon																							
307602c-f2945d076	Document	SHAREPC				Lists/WorkURL		2009-01-04T01:10:46	Update		SharePon																							
307602c-f6b6643-a	List	ACMESPA				Lists/LinkURL		2008-12-22T23:41:11	Update		SharePon		4,000																					
307602c-f4443952a	Document	ACMESPA				EHM Libra URL		2008-12-29T14:58:49	Update		SharePon																							
307602c-fd0463303	Item	ACMESPA				Cache Pro URL		2009-05-11T19:17:44	Update		SharePon																							
307602c-fd0463303	Item	ACMESPA				Cache Pro URL		2009-05-29T19:30:42	Copy		Object Mo		http://spdevdocLib/Copies/FILE.ext																					
307602c-f947506a48	Document	ACMESPA				EHM Libra URL		2008-12-22T23:34:19	Update		SharePon																							
307602c-f947506a48	Document	ACMESPA				EHM Libra URL		2008-12-22T23:48:32	Update		SharePon																							
307602c-fca794648	Folder	ACMESPA				Docs/PagesURL		2008-12-22T12:09:04	Update		SharePon		<Version><Major>2<Minor><Minor><Version>																					
307602c-f3994675	List	SHAREPC				Lists/Task URL		2008-12-29T14:46:42	Update		SharePon		1,000																					
307602c-f3994675	List	SHAREPC				Lists/Task URL		2008-12-29T14:46:42	Update		SharePon		2,000																					
307602c-f3994675	List	SHAREPC				Lists/Task URL		2009-01-04T01:09:45	Update		SharePon		3,000																					
307602c-f3994675	List	SHAREPC				Lists/Task URL		2009-01-04T01:10:29	Update		SharePon		4,000																					
307602c-f3994675	List	SHAREPC				Lists/Task URL		2009-01-04T01:12:00	Update		SharePon		5,000																					
307602c-f3994675	List	SHAREPC				Lists/Task URL		2009-01-04T01:12:41	Update		SharePon		6,000																					
307602c-fca3602b	Item	SHAREPC				Long RunnURL		2009-01-04T00:56:59	Update		SharePon																							
307602c-fca3602b	Item	SHAREPC				Long RunnURL		2009-01-04T00:56:58	Update		SharePon																							
307602c-fca3602b	Item	SHAREPC				Long RunnURL		2009-01-04T00:57:05	Update		SharePon																							
307602c-fca3602b	Item	SHAREPC				Long RunnURL		2009-01-04T00:57:06	Update		SharePon																							
307602c-fca3602b	Item	SHAREPC				Long RunnURL		2009-01-04T00:57:08	Update		SharePon																							
307602c-f41148464	Folder	ACMESPA				DocumentURL		2009-01-04T00:35:51	Update		SharePon		<Version><Major>1<Minor><Minor><Version>																					
307602c-f54599a4f	Document	ACMESPA				EHM Libra URL		2009-01-04T00:57:06	Update		SharePon																							
307602c-f7447278b	Document	SHAREPC				Lists/WorkURL		2009-01-04T01:12:41	Update		SharePon																							
307602c-fb061a7bc	Item	SHAREPC				Long RunnURL		2009-05-11T19:24:55	Update		SharePon																							
307602c-fb061a7bc	Item	SHAREPC				Long RunnURL		2009-05-11T19:24:55	Update		SharePon																							
307602c-fb061a7bc	Item	SHAREPC				Long RunnURL		2009-05-11T19:24:55	Update		SharePon																							
307602c-f83604675a	Document	SHAREPC				Lists/WorkURL		2009-01-04T01:12:00	Update		SharePon																							
307602c-f411367267	Document	ACMESPA				FinancialURL		2008-12-22T12:17:50	Restore		SharePon																							
307602c-f411367267	Document	ACMESPA				FinancialURL		2009-05-07T14:23:37	Check Out		SharePon		<Version><Major>1<Minor><Minor><Version>																					
307602c-f411367267	Document	ACMESPA				FinancialURL		2009-05-07T14:24:03	Update		SharePon		<Version><Major>2<Minor><Minor><Version>																					
307602c-f411367267	Document	ACMESPA				FinancialURL		2009-05-07T14:24:03	Move		SharePon		<NewName>FinancialReport/AuditLog/Eport 2009111																					
307602c-f411367267	Document	ACMESPA				FinancialURL		2009-05-07T14:24:30	Check In		SharePon		<Version><Major>2<Minor><Minor><Version>																					

What do reports look like?

Security Settings

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Site Id	Item Id	Item Type	User Id	Machine N	Machine #	Document	Location	T Occurred (GMT)	Event	Custom E	Event S	Source N	Event Data												
307602c-f411367267	Document	ACMESPA				FinancialURL		2008-12-22T12:17:50	Restore		SharePon														
307602c-f411367267	Document	ACMESPA				FinancialURL		2009-05-07T14:23:37	Check Out		SharePon		<Version><Major>1<Minor><Minor><Version>												
307602c-f411367267	Document	ACMESPA				FinancialURL		2009-05-07T14:24:03	Update		SharePon		<Version><Major>2<Minor><Minor><Version>												
307602c-f411367267	Document	ACMESPA				FinancialURL		2009-05-07T14:24:03	Move		SharePon		<NewName>FinancialReport/AuditLog/Eport 2009111												
307602c-f411367267	Document	ACMESPA				FinancialURL		2009-05-07T14:24:30	Check In		SharePon		<Version><Major>2<Minor><Minor><Version>												
307602c-f56bd07c	List	ACMESPA				FinancialURL		2008-12-22T23:33:28	Update		SharePon		Items.txt												
307602c-f56bd07c	List	ACMESPA				FinancialURL		2008-12-22T23:34:19	Child Delet		SharePon		<RelateItem><Id>E7C7905-99E5-412B-8E2E-8154B400A4E4</Id>												
307602c-f56bd07c	List	ACMESPA				FinancialURL		2009-02-09T23:44:43	Update		SharePon		3Q 2009 Financial Report.xls												
307602c-f56bd07c	List	ACMESPA				FinancialURL		2009-02-09T23:53:23	Child Delet		SharePon		<RelateItem><Id>4C81A4D3-82E4-40FB-95A1-E8D795F7DCC0</Id>												
307602c-f56bd07c	List	ACMESPA				FinancialURL		2009-05-04T15:52:30	Child Move		SharePon		<RelateItem><Id>4F13E276-7121-425E-8E5B-370CE5F7A41C</Id>												
307602c-f56bd07c	List	ACMESPA				FinancialURL		2009-05-07T14:24:03	Child Move		SharePon		<RelateItem><Id>4F13E276-7121-425E-8E5B-370CE5F7A41C</Id>												
307602c-f5934464f	Document	ACMESPA				FinancialURL		2009-07-20T16:50:59	Check Out		SharePon														
307602c-f5934464f	Document	ACMESPA				FinancialURL		2009-07-20T16:51:13	Update		SharePon		<Version><Major>2<Minor><Minor><Version>												
307602c-f5934464f	Document	ACMESPA				FinancialURL		2009-07-20T16:51:29	Check In		SharePon		<Version><Major>2<Minor><Minor><Version>												
307602c-f47c7905	Document	ACMESPA				FinancialURL		2008-12-22T23:33:28	Update		SharePon		<Version><Major>1<Minor><Minor><Version>												
307602c-f47c7905	Document	ACMESPA				FinancialURL		2008-12-22T23:34:19	Child Delet		SharePon		<Version><Major>1<Minor><Minor><Version>												
307602c-f47c7905	Document	ACMESPA				FinancialURL		2008-12-22T23:33:43	Check In		SharePon		<Version><Major>1<Minor><Minor><Version>												
307602c-f47c7905	Document	ACMESPA				FinancialURL		2008-12-22T23:34:19	Delete		SharePon		<Version><AllVersions><Version><Recycle1><Recycle>												
307602c-f431a462	Document	ACMESPA				FinancialURL		2009-05-04T15:52:30	Update		SharePon		<Version><Major>2<Minor><Minor><Version>												
307602c-f431a462	Document	ACMESPA				FinancialURL		2009-05-04T15:52:00	Move		SharePon		<NewName>FinancialReports/This is a sample document.docx</New												
307602c-f431a462	Document	ACMESPA				FinancialURL		2009-07-20T16:40:52	Check In		SharePon		<Version><Major>2<Minor><Minor><Version>												
307602c-f71a6856a	Document	ACMESPA				FinancialURL		2009-02-09T23:44:43	Update		SharePon		<Version><Major>1<Minor><Minor><Version>												
307602c-f71a6856a	Document	ACMESPA				FinancialURL		2009-02-09T23:45:12	Update		SharePon		<Version><Major>1<Minor><Minor><Version>												
307602c-f71a6856a	Document	ACMESPA				FinancialURL		2009-02-09T23:45:13	Check In		SharePon		<Version><Major>1<Minor><Minor><Version>												
307602c-f71a6856a	Document	ACMESPA				FinancialURL		2009-02-09T23:53:23	Delete		SharePon		<Version><AllVersions><Version><Recycle1><Recycle>												

What do reports look like?

Custom Report

Run a custom report - Customize

Manually specify the filters for your Audit Report.

Location
Specify whether this report should be restricted to a particular list in the site collection.

Restrict the report to:
 List: All Lists

Date Range
Specify a start date and/or end date that this report should be restricted to. If you specify only a start date, the report will include all events that occur after that date. If you specify only an end date, the report will include all events that occur before that date.

Start Date:
 End Date:

Users
Specify which user the report should be restricted to.

Users:

Events
Specify whether this report should be restricted to particular events. If no event filters are specified, the report will include all events matching the other restrictions.

- Opening or downloading documents, viewing items in lists, or viewing item properties
- Editing items
- Checking out or checking in items
- Moving or copying items to another location in the site
- Deleting or restoring items
- Editing content types and columns
- Searching site content
- Editing users and permissions
- Editing auditing settings and deleting audit log events
- Workflow events
- Custom events

OK Cancel

What do reports look like?

Custom Report

Item ID	Item Title	Item Type	Item ID	Event	Location	Event Date	Event Type	Event Data
1	38782C-E83A7B-7-Document	ACME/SP	Financial URL	2009-02-22T12:57:50	Restore	SharePoint	<Version>=Major=1<Major>=Minor=0<Minor>=Version	
2	38782C-E83A7B-7-Document	ACME/SP	Financial URL	2009-02-07T14:23:37	Check Out	SharePoint	<Version>=Major=2<Major>=Minor=0<Minor>=Version	
3	38782C-E83A7B-7-Document	ACME/SP	Financial URL	2009-02-07T14:24:03	Update	SharePoint	<NewName>=FinancialURL/auditLog.aspx:20081122:with:Name:Name	
4	38782C-E83A7B-7-Document	ACME/SP	Financial URL	2009-02-07T14:24:03	Move	SharePoint	<Version>=Major=2<Major>=Minor=0<Minor>=Version	
5	38782C-E83A7B-7-Document	ACME/SP	Financial URL	2009-02-07T14:24:30	Check In	SharePoint	<Version>=Major=2<Major>=Minor=0<Minor>=Version	
6	38782C-E83A7B-7-Document	ACME/SP	Financial URL	2009-02-07T14:24:30	Check In	SharePoint	<Version>=Major=2<Major>=Minor=0<Minor>=Version	
7	38782C-E83A7B-7-Document	ACME/SP	Financial URL	2009-02-22T12:57:50	Update	SharePoint	Items list	<Relationship>=Child/Parent=Relationship
8	38782C-E83A7B-7-Document	ACME/SP	Financial URL	2009-02-22T12:57:50	Update	SharePoint	30,2009 Financial Report.xls	<Relationship>=Child/Parent=Relationship
9	38782C-E83A7B-7-Document	ACME/SP	Financial URL	2009-02-07T14:24:03	Child Move	SharePoint	<Relationship>=Child/Parent=Relationship	<Relationship>=Child/Parent=Relationship
10	38782C-E83A7B-7-Document	ACME/SP	Financial URL	2009-02-07T14:24:03	Child Move	SharePoint	<Relationship>=Child/Parent=Relationship	<Relationship>=Child/Parent=Relationship
11	38782C-E83A7B-7-Document	ACME/SP	Financial URL	2009-02-07T14:24:03	Child Move	SharePoint	<Relationship>=Child/Parent=Relationship	<Relationship>=Child/Parent=Relationship
12	38782C-E83A7B-7-Document	ACME/SP	Financial URL	2009-02-07T14:24:03	Child Move	SharePoint	<Relationship>=Child/Parent=Relationship	<Relationship>=Child/Parent=Relationship
13	38782C-E83A7B-7-Document	ACME/SP	Financial URL	2009-02-22T12:57:50	Check Out	SharePoint	<Version>=Major=1<Major>=Minor=0<Minor>=Version	
14	38782C-E83A7B-7-Document	ACME/SP	Financial URL	2009-02-22T12:57:50	Update	SharePoint	<Version>=Major=2<Major>=Minor=0<Minor>=Version	
15	38782C-E83A7B-7-Document	ACME/SP	Financial URL	2009-02-22T12:57:50	Check In	SharePoint	<Version>=Major=2<Major>=Minor=0<Minor>=Version	
16	38782C-E83A7B-7-Document	ACME/SP	Financial URL	2009-02-22T12:57:50	Update	SharePoint	<Version>=Major=1<Major>=Minor=0<Minor>=Version	
17	38782C-E83A7B-7-Document	ACME/SP	Financial URL	2009-02-22T12:57:50	Check In	SharePoint	<Version>=Major=1<Major>=Minor=0<Minor>=Version	
18	38782C-E83A7B-7-Document	ACME/SP	Financial URL	2009-02-22T12:57:50	Check In	SharePoint	<Version>=Major=1<Major>=Minor=0<Minor>=Version	
19	38782C-E83A7B-7-Document	ACME/SP	Financial URL	2009-02-22T12:57:50	Check In	SharePoint	<Version>=Major=1<Major>=Minor=0<Minor>=Version	
20	38782C-E83A7B-7-Document	ACME/SP	Financial URL	2009-02-22T12:57:50	Check In	SharePoint	<Version>=Major=1<Major>=Minor=0<Minor>=Version	
21	38782C-E83A7B-7-Document	ACME/SP	Financial URL	2009-02-22T12:57:50	Check In	SharePoint	<Version>=Major=1<Major>=Minor=0<Minor>=Version	
22	38782C-E83A7B-7-Document	ACME/SP	Financial URL	2009-02-22T12:57:50	Check In	SharePoint	<Version>=Major=1<Major>=Minor=0<Minor>=Version	
23	38782C-E83A7B-7-Document	ACME/SP	Financial URL	2009-02-22T12:57:50	Check In	SharePoint	<Version>=Major=1<Major>=Minor=0<Minor>=Version	
24	38782C-E83A7B-7-Document	ACME/SP	Financial URL	2009-02-22T12:57:50	Check In	SharePoint	<Version>=Major=1<Major>=Minor=0<Minor>=Version	
25	38782C-E83A7B-7-Document	ACME/SP	Financial URL	2009-02-22T12:57:50	Check In	SharePoint	<Version>=Major=1<Major>=Minor=0<Minor>=Version	
26	38782C-E83A7B-7-Document	ACME/SP	Financial URL	2009-02-22T12:57:50	Check In	SharePoint	<Version>=Major=1<Major>=Minor=0<Minor>=Version	
27	38782C-E83A7B-7-Document	ACME/SP	Financial URL	2009-02-22T12:57:50	Check In	SharePoint	<Version>=Major=1<Major>=Minor=0<Minor>=Version	
28	38782C-E83A7B-7-Document	ACME/SP	Financial URL	2009-02-22T12:57:50	Check In	SharePoint	<Version>=Major=1<Major>=Minor=0<Minor>=Version	
29	38782C-E83A7B-7-Document	ACME/SP	Financial URL	2009-02-22T12:57:50	Check In	SharePoint	<Version>=Major=1<Major>=Minor=0<Minor>=Version	
30	38782C-E83A7B-7-Document	ACME/SP	Financial URL	2009-02-22T12:57:50	Check In	SharePoint	<Version>=Major=1<Major>=Minor=0<Minor>=Version	

How do you configure alerts?

No support

Can you direct the audit log to your log management application?

No, the SharePoint audit log is trapped in the SharePoint content database

1. Events are **unreadable**
2. No way to access auditing in WSS
3. No scheduled pruning
4. Stored in content DB
 - no way to collect to central, secure log archive
5. No alerting
6. No usable reporting

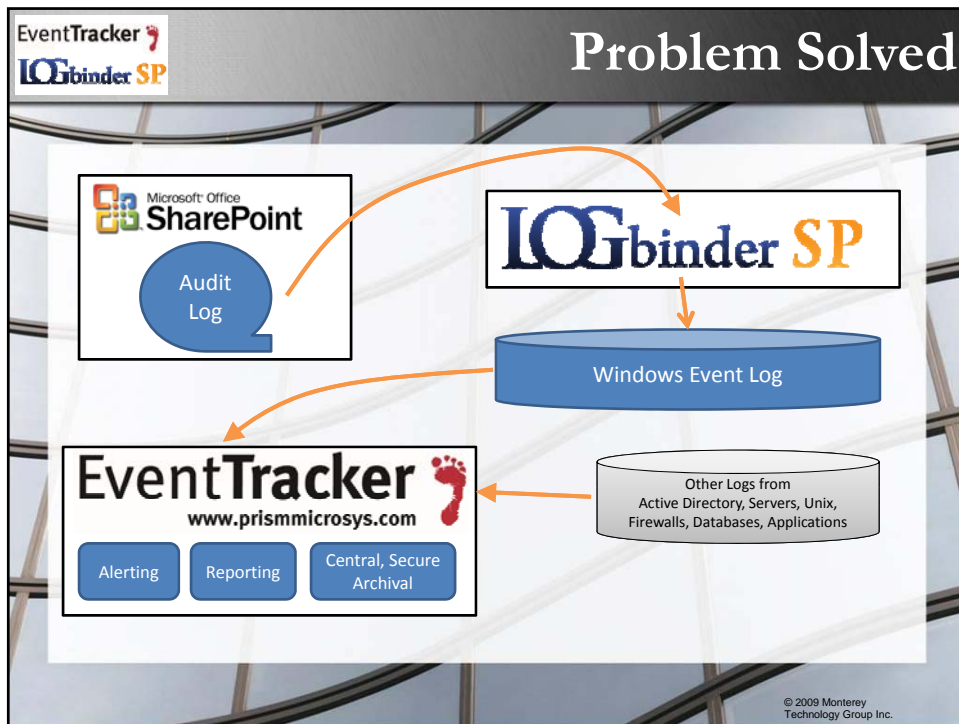
Problems solved by

LOGbinder SP

www.logbinder.com

With

EventTracker 
www.prismmicrosys.com



- ## LOGbinder SP
- Gets the audit log out of SharePoint content DB
 - And into the Windows event log
 - Makes the log accessible to log management/SEM solutions like EventTracker
- © 2009 Monterey Technology Group Inc.

☐ Translates events into something you can read and use

Turn this...

#	A	B	C	D	E	F	G	H
1	Site ID	Item ID	Item Type	User	Doc Location	Occurred	Event	Event Data
	38798E0C-F5D4-4164-B5C0-DF8225E0CF	5F3C228C-A48E-4959-88C0-DD98B0D395	4		/Class	3/3/2009 11:59:43 AM	30	removed-- in:0x00000000-00000000-00000000-00000000-00000000-00000000-00000000-00000000
2		RM						AF4EE834DD-1100e4-



Into this ...

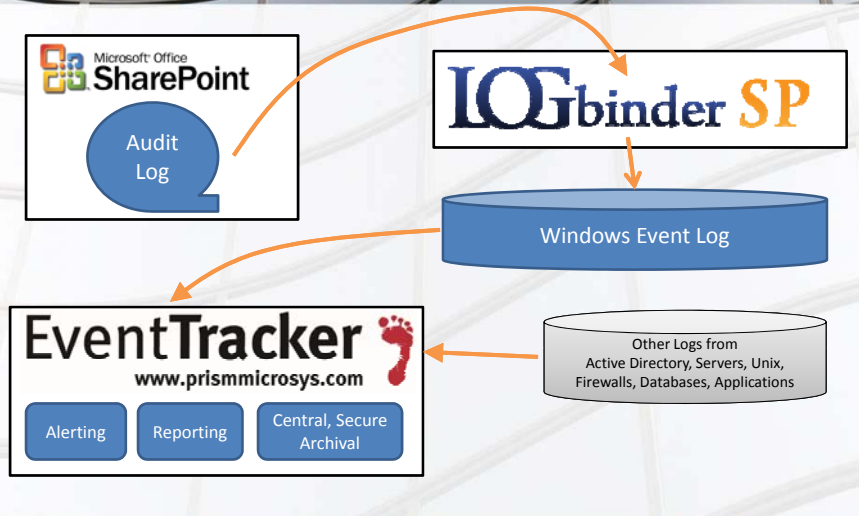
Permissions removed
 Occurred: 2/23/2009 11:59:43 PM
 Site: <http://shopt>
 User: ACMESPIadministrator
 Object
 Type: List Item
 Subtype: n/a
 URL: /Projects/InvisiRay
 Title: InvisiRay Project
 Description: Confidential project plans for InvisiRay
 User/Group
 Name: Duncan O' Neill
 Type: User

- ☐ Prunes the SharePoint audit log as events exported to Windows event log
 - Prevents wasted consumption of expensive SQL DB storage

1. Stored in content DB, no way to collect to central, secure log archive
2. Events are **unreadable**
3. No alerting
4. No way to access auditing in WSS
5. No scheduled pruning

- Unintrusive
 - Does not require local admin
 - Does not modify SharePoint in anyway
 - Separate, discreet service
 - Very small < 1MB

- ❑ Provides centralized log collection and management
 - Alerting
 - Pre-built alerts for SharePoint events from LOGbinder SP
 - Reporting
 - Pre-built reports for SharePoint events from LOGbinder SP
 - Search
 - Secure, long term, efficient archival



1. Events are unreadable
2. No way to access auditing in WSS
3. No scheduled pruning
4. Stored in content DB
 - no way to collect to central, secure log archive
5. No alerting
6. No usable reporting

1. ^{solved} Events are unreadable
2. No way to access auditing in WSS
3. No scheduled pruning
4. Stored in content DB
 - no way to collect to central, secure log archive
5. No alerting
6. No usable reporting

1. Events are unreadable
2. No way to access auditing in WSS
3. No scheduled pruning
4. Stored in content DB
 - no way to collect to central, secure log archive
5. No alerting
6. No usable reporting

1. Events are unreadable
2. No way to access auditing in WSS
3. No scheduled pruning
4. Stored in content DB
 - no way to collect to central, secure log archive
5. No alerting
6. No usable reporting

1. Events are unreadable
2. No way to access auditing in WSS
3. No scheduled pruning
4. Stored in content DB
 - no way to collect to central, secure log archive
5. No alerting
6. No usable reporting

1. Events are unreadable
2. No way to access auditing in WSS
3. No scheduled pruning
4. Stored in content DB
 - no way to collect to central, secure log archive
5. No alerting
6. No usable reporting

1. Events are unreadable
2. No way to access auditing in WSS
3. No scheduled pruning
4. Stored in content DB
 - no way to collect to central, secure log archive
5. No alerting
6. No usable reporting

- | | |
|--|--|
| <input type="checkbox"/> Download
LOGbinder SP | <input type="checkbox"/> Download
EventTracker |
| <input type="checkbox"/> Visit
www.LOGbinder.com | <input type="checkbox"/> Visit
www.prismmicrosys.com |