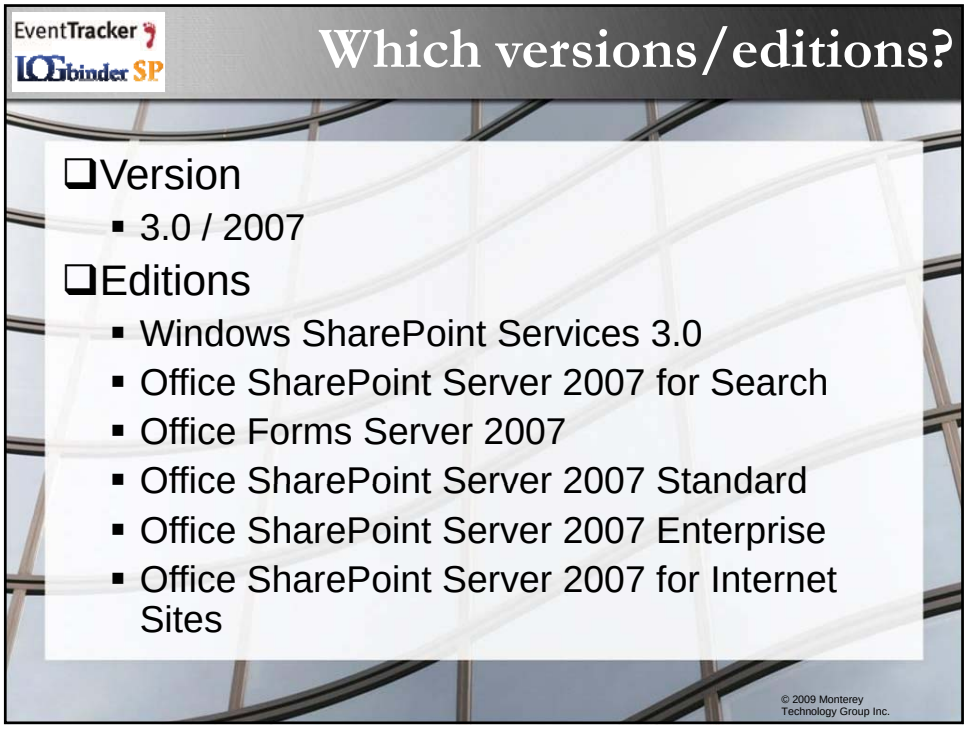
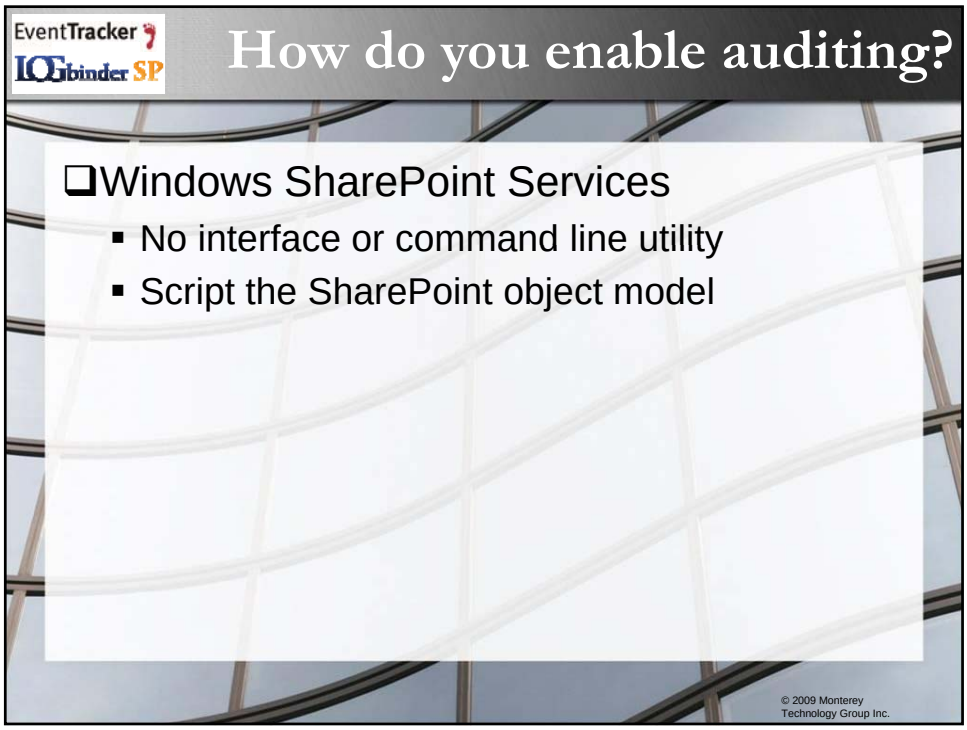
Preview of Key Points

- 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?

Does SharePoint have an audit log?

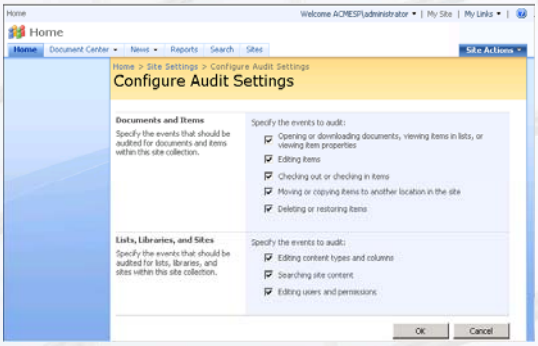
- Yes





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?

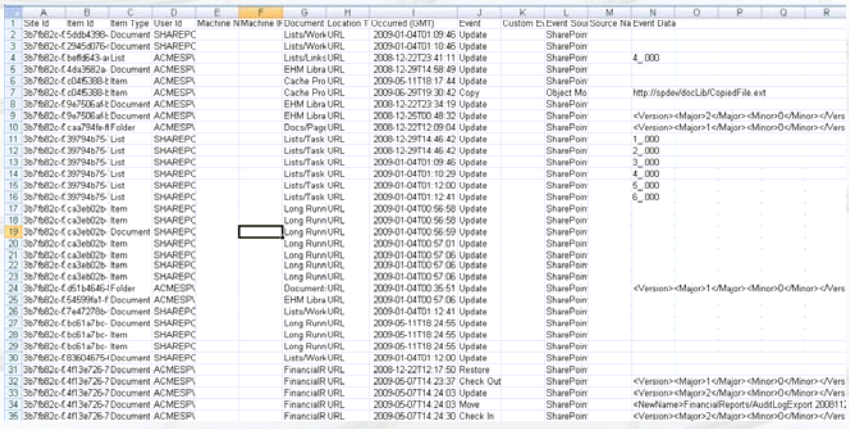
- Windows SharePoint Services
  - No interface or command line utility
  - Script the SharePoint object model

How do you view the log?

- Office SharePoint Server
  - Handful of rudimentary Excel reports
  - Cryptic
  - Essentially broken

What do reports look like?

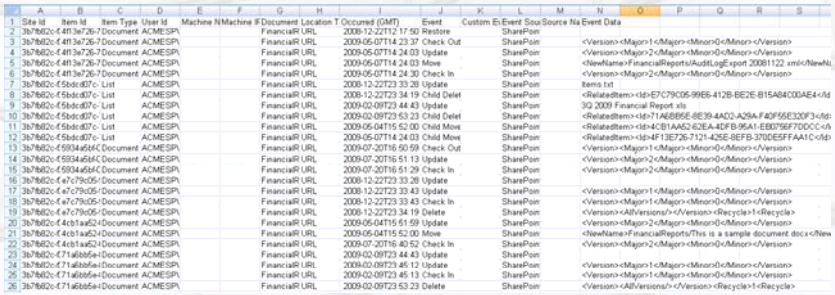
❑Content Modification



	Site Id	Item Id	Item Type	User Id	Machine N	Machine IP	Document	Location T	Occurred (GMT)	Event	Custom Ev	Event Sou	Source Na	Event Data
2	3b7b82c-f	5ddb4398-	Document	SHAREPC			Lists/Work	URL	2009-01-04T01:09:46	Update		SharePoin		
3	3b7b82c-f	2945d076-	Document	SHAREPC			Lists/Work	URL	2009-01-04T01:10:46	Update		SharePoin		
4	3b7b82c-f	beffd643-a	List	ACMESP\			Lists/Links	URL	2008-12-22T23:41:11	Update		SharePoin		4_000
5	3b7b82c-f	4da3682a-	Document	ACMESP\			EHM Libra	URL	2008-12-29T14:58:49	Update		SharePoin		
6	3b7b82c-f	d04f5388-b	Item	ACMESP\			Cache Pro	URL	2009-05-11T18:17:44	Update		SharePoin		
7	3b7b82c-f	d04f5388-b	Item	ACMESP\			Cache Pro	URL	2009-06-29T19:30:42	Copy		Object Mo		http://spdev/docLib/CopiedFile.ext
8	3b7b82c-f	9a7506a6-b	Document	ACMESP\			EHM Libra	URL	2008-12-22T23:34:19	Update		SharePoin		
9	3b7b82c-f	9a7506a6-b	Document	ACMESP\			EHM Libra	URL	2008-12-25T00:48:32	Update		SharePoin		<Version><Major>2</Major><Minor>0</Minor></Vers
10	3b7b82c-f	caa7946e-8	Folder	ACMESP\			Docs/Page	URL	2008-12-22T12:09:04	Update		SharePoin		<Version><Major>1</Major><Minor>0</Minor></Vers
11	3b7b82c-f	39794b75-	List	SHAREPC			Lists/Task	URL	2008-12-29T14:46:42	Update		SharePoin		1_000
12	3b7b82c-f	39794b75-	List	SHAREPC			Lists/Task	URL	2008-12-29T14:46:42	Update		SharePoin		2_000
13	3b7b82c-f	39794b75-	List	SHAREPC			Lists/Task	URL	2009-01-04T01:09:46	Update		SharePoin		3_000
14	3b7b82c-f	39794b75-	List	SHAREPC			Lists/Task	URL	2009-01-04T01:10:29	Update		SharePoin		4_000
15	3b7b82c-f	39794b75-	List	SHAREPC			Lists/Task	URL	2009-01-04T01:12:00	Update		SharePoin		5_000
16	3b7b82c-f	39794b75-	List	SHAREPC			Lists/Task	URL	2009-01-04T01:12:41	Update		SharePoin		6_000
17	3b7b82c-f	ca3eb02b-	Item	SHAREPC			Long Runn	URL	2009-01-04T00:56:58	Update		SharePoin		
18	3b7b82c-f	ca3eb02b-	Item	SHAREPC			Long Runn	URL	2009-01-04T00:56:58	Update		SharePoin		
19	3b7b82c-f	ca3eb02b-	Document	SHAREPC			Long Runn	URL	2009-01-04T00:56:59	Update		SharePoin		
20	3b7b82c-f	ca3eb02b-	Item	SHAREPC			Long Runn	URL	2009-01-04T00:57:01	Update		SharePoin		
21	3b7b82c-f	ca3eb02b-	Item	SHAREPC			Long Runn	URL	2009-01-04T00:57:06	Update		SharePoin		
22	3b7b82c-f	ca3eb02b-	Item	SHAREPC			Long Runn	URL	2009-01-04T00:57:06	Update		SharePoin		
23	3b7b82c-f	ca3eb02b-	Item	SHAREPC			Long Runn	URL	2009-01-04T00:57:06	Update		SharePoin		
24	3b7b82c-f	d51b4646-f	Folder	ACMESP\			Document	URL	2009-01-04T00:35:51	Update		SharePoin		<Version><Major>1</Major><Minor>0</Minor></Vers
25	3b7b82c-f	54599fa1-f	Document	ACMESP\			EHM Libra	URL	2009-01-04T00:57:06	Update		SharePoin		
26	3b7b82c-f	7e47278b-	Document	SHAREPC			Lists/Work	URL	2009-01-04T01:12:41	Update		SharePoin		
27	3b7b82c-f	bc61a7bc-	Document	SHAREPC			Long Runn	URL	2009-05-11T18:24:55	Update		SharePoin		
28	3b7b82c-f	bc61a7bc-	Item	SHAREPC			Long Runn	URL	2009-05-11T18:24:55	Update		SharePoin		
29	3b7b82c-f	bc61a7bc-	Item	SHAREPC			Long Runn	URL	2009-05-11T18:24:55	Update		SharePoin		
30	3b7b82c-f	83604675-f	Document	SHAREPC			Lists/Work	URL	2009-01-04T01:12:00	Update		SharePoin		
31	3b7b82c-f	4f13e726-7	Document	ACMESP\			FinancialR	URL	2008-12-22T12:17:50	Restore		SharePoin		
32	3b7b82c-f	4f13e726-7	Document	ACMESP\			FinancialR	URL	2009-05-07T14:23:37	Check Out		SharePoin		<Version><Major>1</Major><Minor>0</Minor></Vers
33	3b7b82c-f	4f13e726-7	Document	ACMESP\			FinancialR	URL	2009-05-07T14:24:03	Update		SharePoin		<Version><Major>2</Major><Minor>0</Minor></Vers
34	3b7b82c-f	4f13e726-7	Document	ACMESP\			FinancialR	URL	2009-05-07T14:24:03	Move		SharePoin		<NewName>FinancialReports/AuditLogExport 200811
35	3b7b82c-f	4f13e726-7	Document	ACMESP\			FinancialR	URL	2009-05-07T14:24:30	Check In		SharePoin		<Version><Major>2</Major><Minor>0</Minor></Vers

What do reports look like?

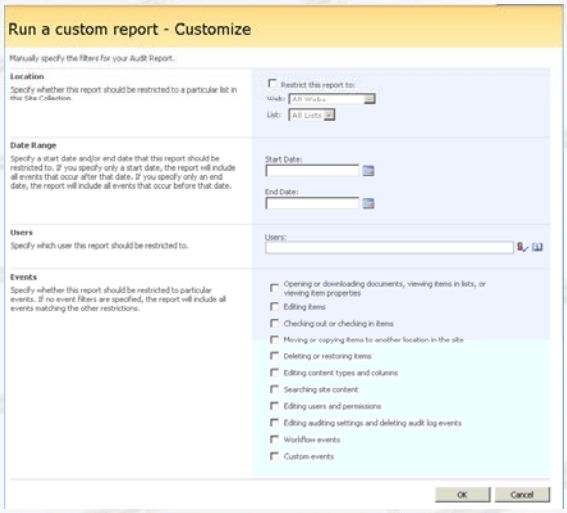
❑Security Settings



	Site Id	Item Id	Item Type	User Id	Machine N	Machine IP	Document	Location T	Occurred (GMT)	Event	Custom Ev	Event Sou	Source Na	Event Data
2	3b7b82c-f	4f13e726-7	Document	ACMESP\			FinancialR	URL	2008-12-22T12:17:50	Restore		SharePoin		
3	3b7b82c-f	4f13e726-7	Document	ACMESP\			FinancialR	URL	2009-05-07T14:23:37	Check Out		SharePoin		<Version><Major>1</Major><Minor>0</Minor></Version>
4	3b7b82c-f	4f13e726-7	Document	ACMESP\			FinancialR	URL	2009-05-07T14:24:03	Update		SharePoin		<Version><Major>2</Major><Minor>0</Minor></Version>
5	3b7b82c-f	4f13e726-7	Document	ACMESP\			FinancialR	URL	2009-05-07T14:24:03	Move		SharePoin		<NewName>FinancialReports/AuditLogExport 20081122.xml</NewNa
6	3b7b82c-f	4f13e726-7	Document	ACMESP\			FinancialR	URL	2009-05-07T14:24:30	Check In		SharePoin		<Version><Major>2</Major><Minor>0</Minor></Version>
7	3b7b82c-f	5bdcd07c-	List	ACMESP\			FinancialR	URL	2008-12-22T23:33:28	Update		SharePoin		Items.txt
8	3b7b82c-f	5bdcd07c-	List	ACMESP\			FinancialR	URL	2008-12-22T23:34:19	Child Delet		SharePoin		<RelatedItem><Id>E7C79C05-99E6-412B-BE2E-B15AB4C00AE4</Id
9	3b7b82c-f	5bdcd07c-	List	ACMESP\			FinancialR	URL	2009-02-09T23:44:43	Update		SharePoin		3Q 2009 Financial Report.xls
10	3b7b82c-f	5bdcd07c-	List	ACMESP\			FinancialR	URL	2009-02-09T23:53:23	Child Delet		SharePoin		<RelatedItem><Id>71A6BB5E-8E39-4AD2-A29A-F40F55E320F3</Id:
11	3b7b82c-f	5bdcd07c-	List	ACMESP\			FinancialR	URL	2009-05-04T15:52:00	Child Move		SharePoin		<RelatedItem><Id>4CB1AA52-62EA-4DFB-95A1-EB0756F7DDCC</Id
12	3b7b82c-f	5bdcd07c-	List	ACMESP\			FinancialR	URL	2009-05-07T14:24:03	Child Move		SharePoin		<RelatedItem><Id>4F13E726-7121-425E-8EFB-370E65FFAA1C</Id
13	3b7b82c-f	5934a5bf-C	Document	ACMESP\			FinancialR	URL	2009-07-20T16:50:59	Check Out		SharePoin		<Version><Major>1</Major><Minor>0</Minor></Version>
14	3b7b82c-f	5934a5bf-C	Document	ACMESP\			FinancialR	URL	2009-07-20T16:51:13	Update		SharePoin		<Version><Major>2</Major><Minor>0</Minor></Version>
15	3b7b82c-f	5934a5bf-C	Document	ACMESP\			FinancialR	URL	2009-07-20T16:51:29	Check In		SharePoin		<Version><Major>2</Major><Minor>0</Minor></Version>
16	3b7b82c-f	e7c79c05-7	Document	ACMESP\			FinancialR	URL	2008-12-22T23:33:28	Update		SharePoin		
17	3b7b82c-f	e7c79c05-7	Document	ACMESP\			FinancialR	URL	2008-12-22T23:33:43	Update		SharePoin		<Version><Major>1</Major><Minor>0</Minor></Version>
18	3b7b82c-f	e7c79c05-7	Document	ACMESP\			FinancialR	URL	2008-12-22T23:33:43	Check In		SharePoin		<Version><Major>1</Major><Minor>0</Minor></Version>
19	3b7b82c-f	e7c79c05-7	Document	ACMESP\			FinancialR	URL	2008-12-22T23:34:19	Delete		SharePoin		<Version><AllVersions/></Version><Recycle>1<Recycle>
20	3b7b82c-f	4cb1aa52-f	Document	ACMESP\			FinancialR	URL	2009-05-04T15:51:59	Update		SharePoin		<Version><Major>2</Major><Minor>0</Minor></Version>
21	3b7b82c-f	4cb1aa52-f	Document	ACMESP\			FinancialR	URL	2009-05-04T15:52:00	Move		SharePoin		<NewName>FinancialReports/This is a sample document.docx</New
22	3b7b82c-f	4cb1aa52-f	Document	ACMESP\			FinancialR	URL	2009-07-20T16:40:52	Check In		SharePoin		<Version><Major>2</Major><Minor>0</Minor></Version>
23	3b7b82c-f	71a6bb5e-f	Document	ACMESP\			FinancialR	URL	2009-02-09T23:44:43	Update		SharePoin		
24	3b7b82c-f	71a6bb5e-f	Document	ACMESP\			FinancialR	URL	2009-02-09T23:45:12	Update		SharePoin		<Version><Major>1</Major><Minor>0</Minor></Version>
25	3b7b82c-f	71a6bb5e-f	Document	ACMESP\			FinancialR	URL	2009-02-09T23:45:13	Check In		SharePoin		<Version><Major>1</Major><Minor>0</Minor></Version>
26	3b7b82c-f	71a6bb5e-f	Document	ACMESP\			FinancialR	URL	2009-02-09T23:53:23	Delete		SharePoin		<Version><AllVersions/></Version><Recycle>1<Recycle>

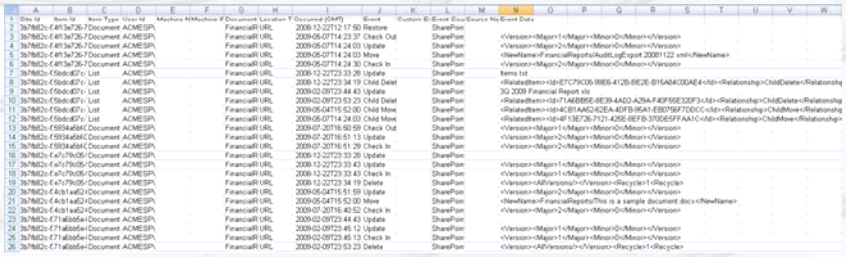
What do reports look like?

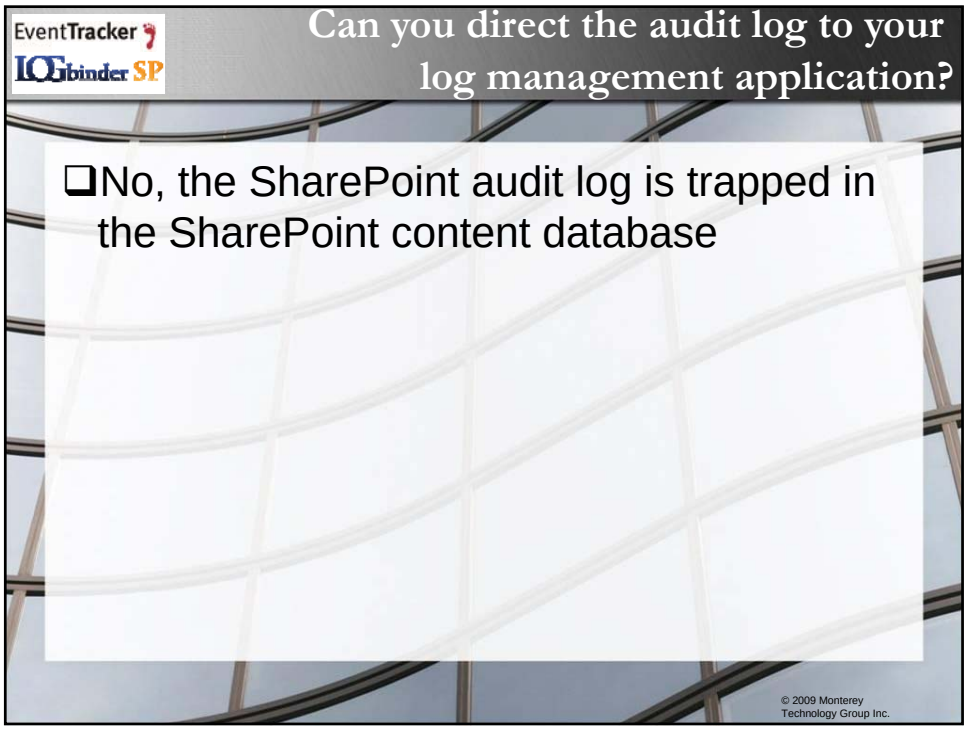
- Custom Report

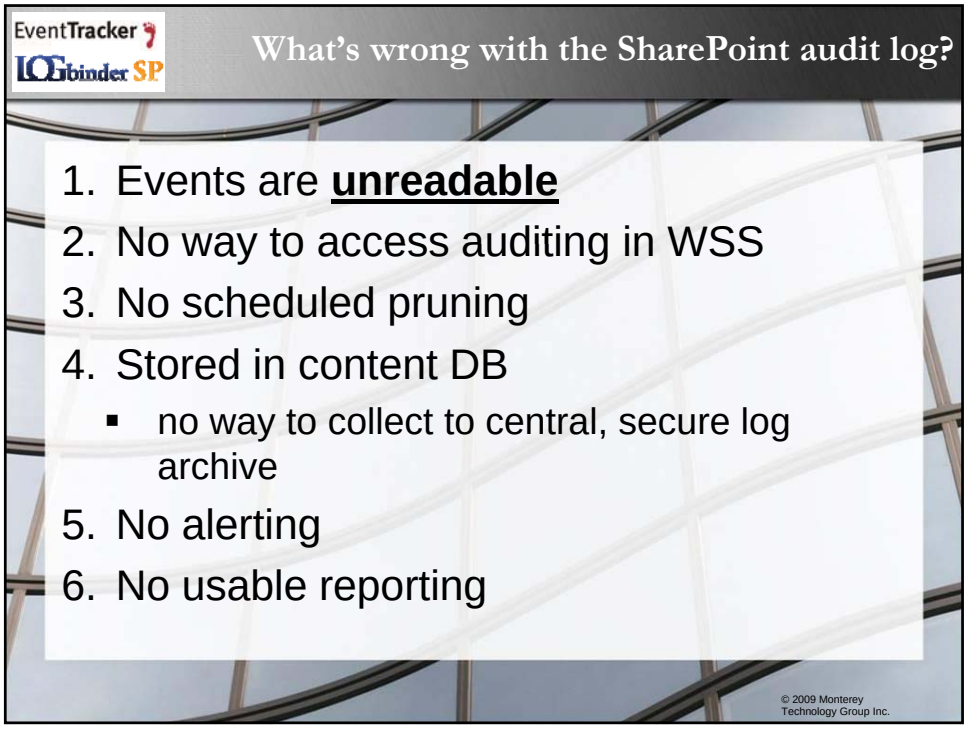


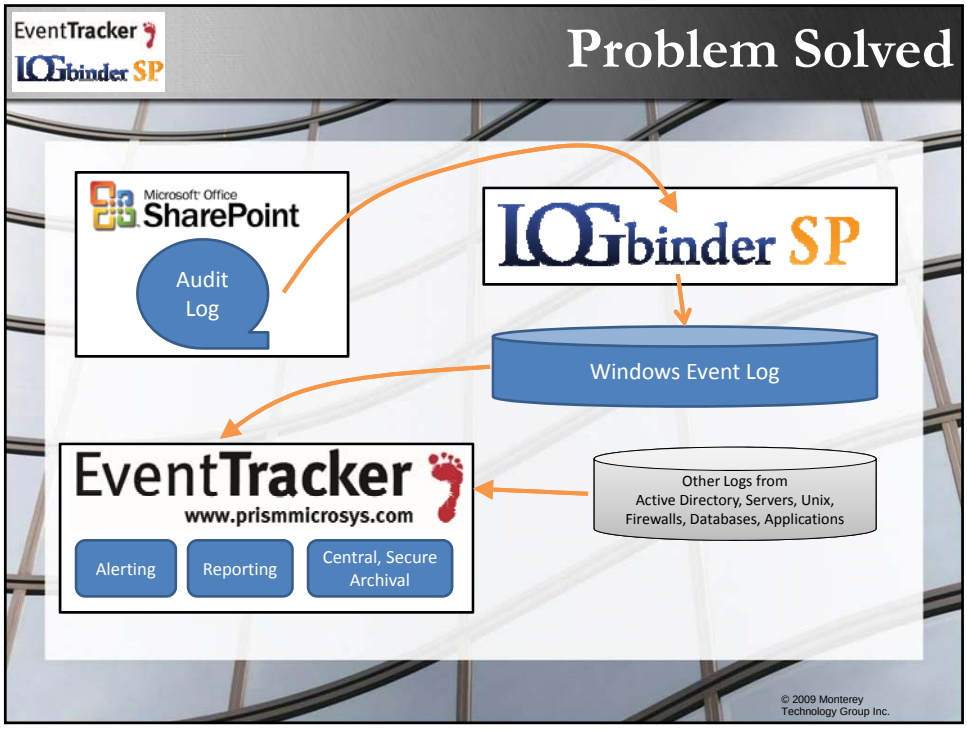
What do reports look like?

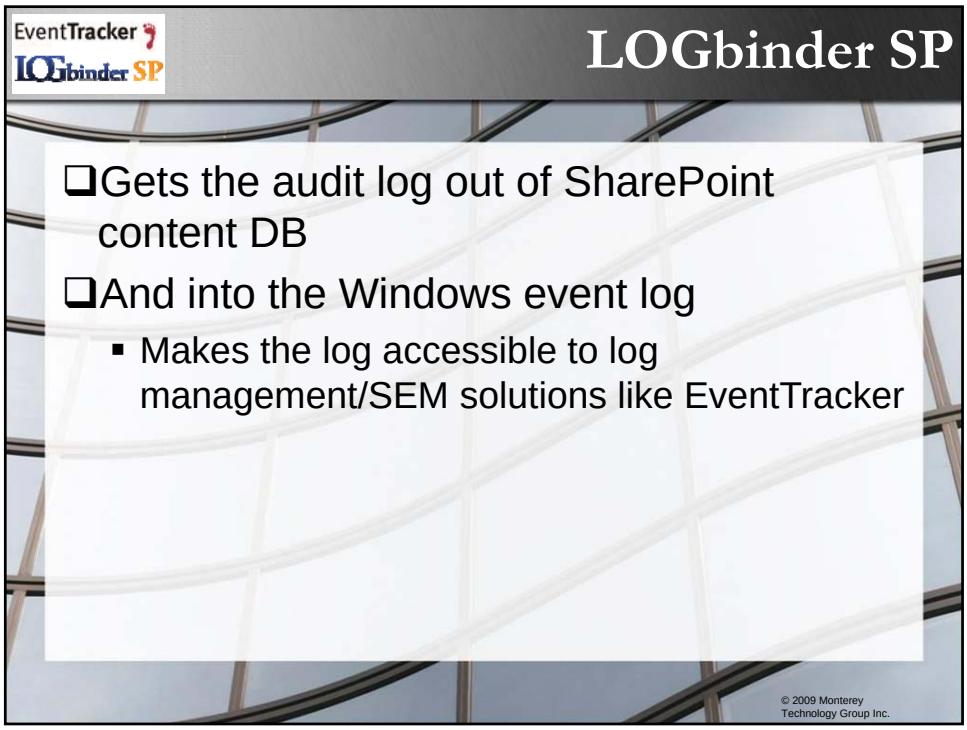
- Custom Report











LOGbinder SP

- Translates events into something you can read and use

Turn this...

Into this ...

Permissions removed
Occurred: 2/23/2009 11:59:43 PM
Site: http://shpt
User: ACMESP\administrator
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

LOGbinder SP

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

LOGbinder SP solves SharePoint Audit Problems

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

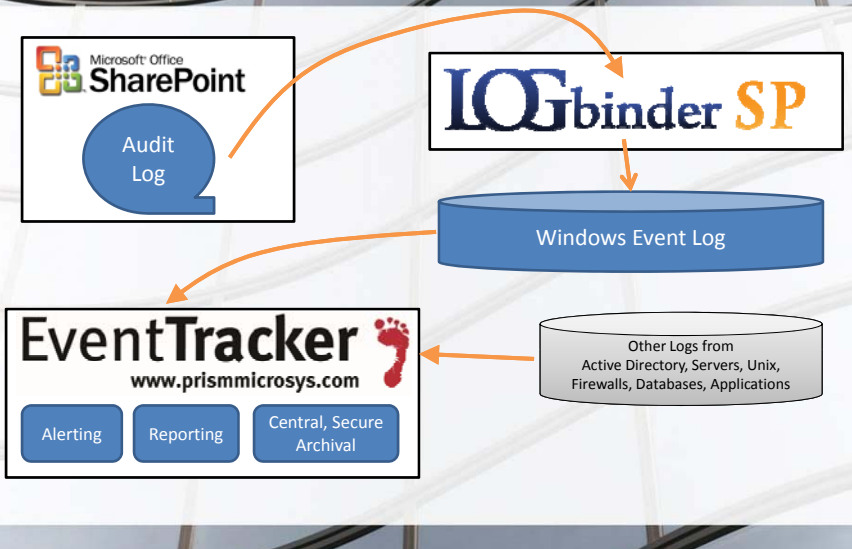
LOGbinder SP

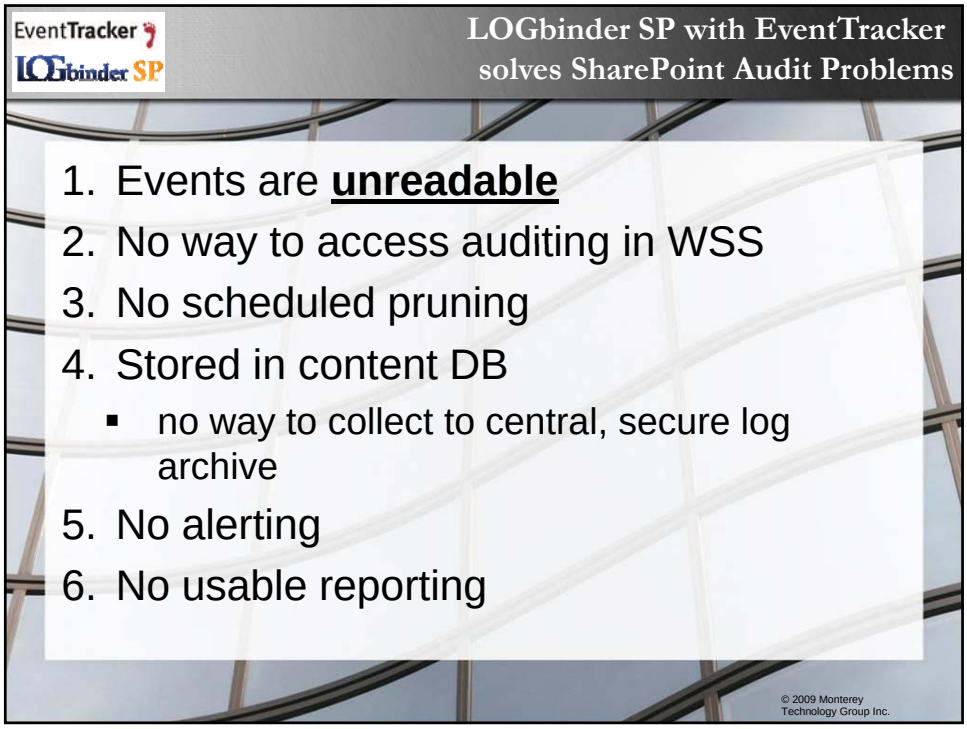
- Unintrusive
  - Does not require local admin
  - Does not modify SharePoint in anyway
    - Separate, discreet service
  - Very small < 1MB

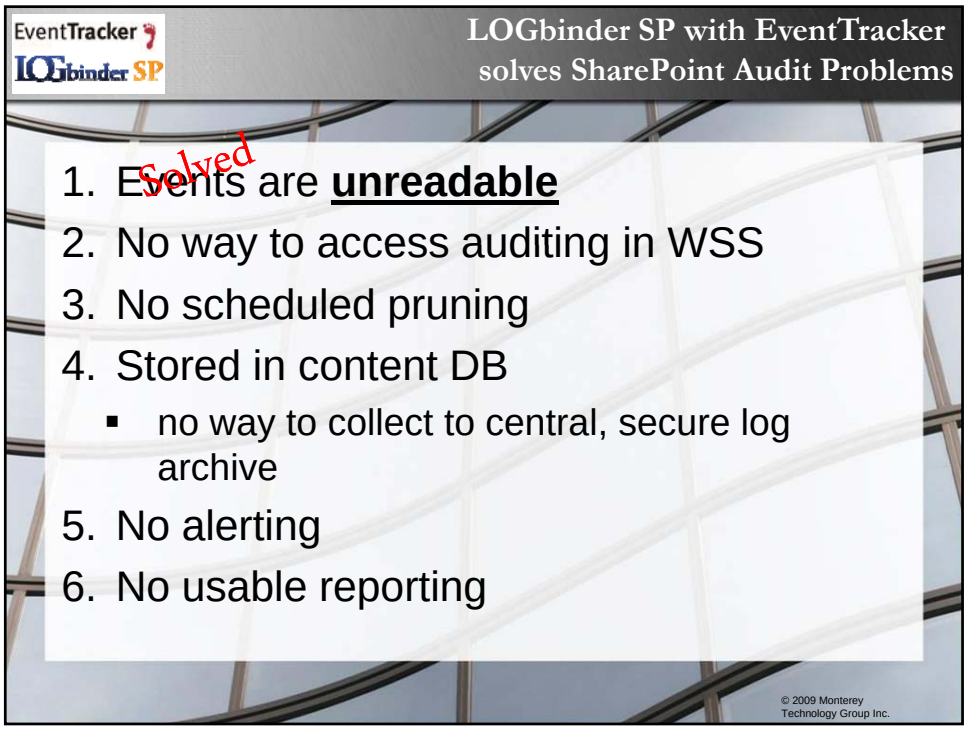
EventTracker

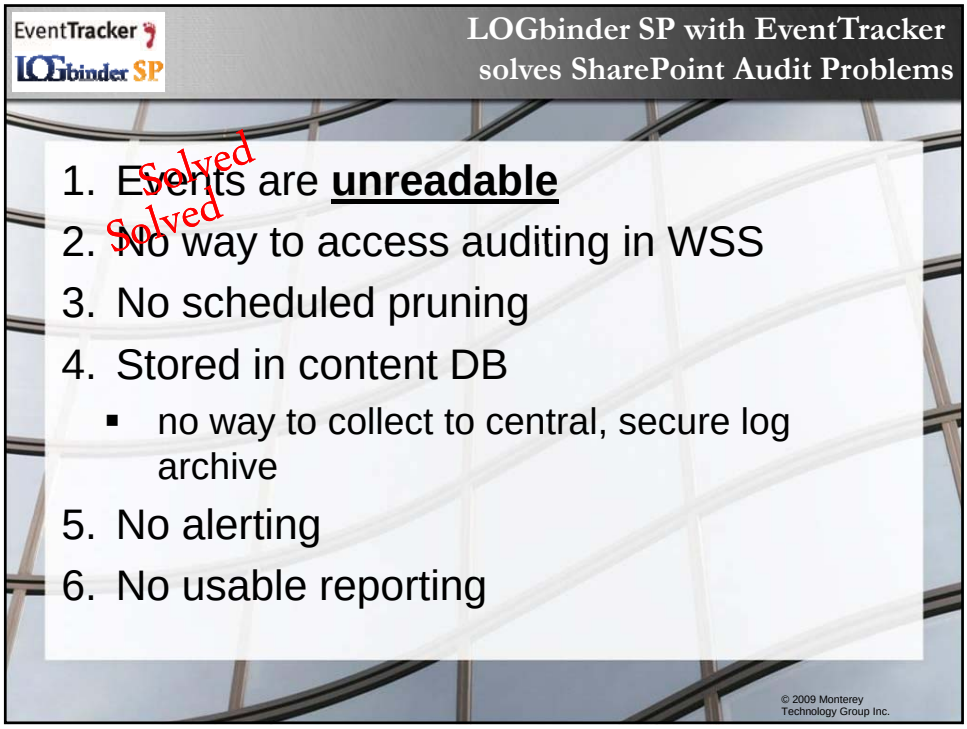
- Provides centralized log collection and management
  - Alerting
    - Pre-built alerts for SharePoint events from LOGbinder SP
  - Reporting
    - Pre-built reports for SharePoint events from LOGbinder SP
  - Search
  - Secure, long term, efficient archival

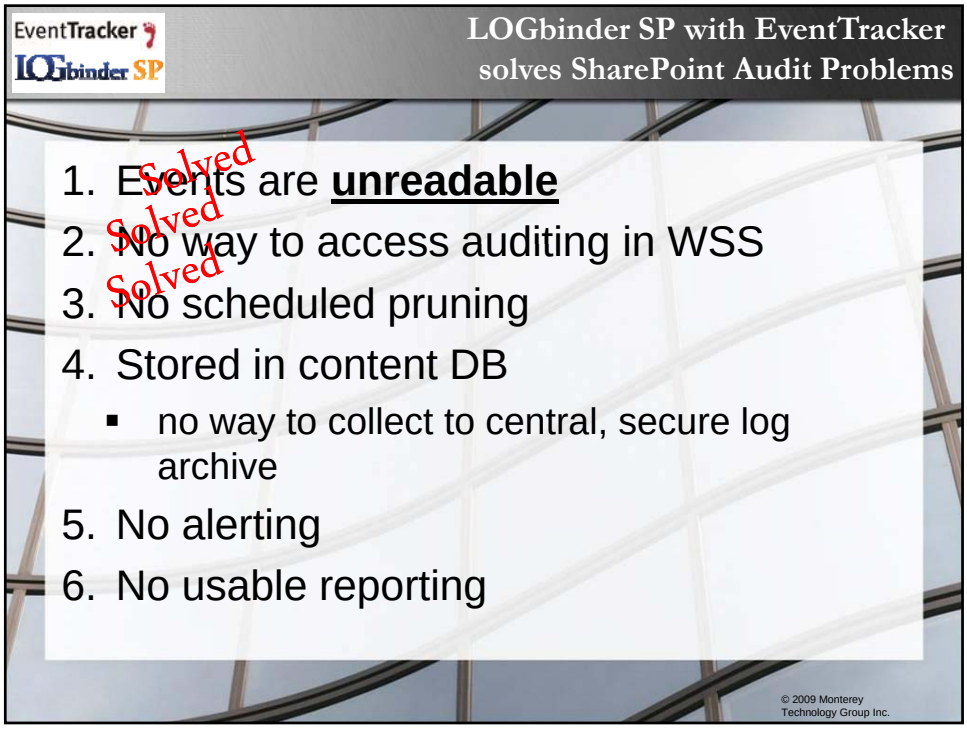
Problem Solved

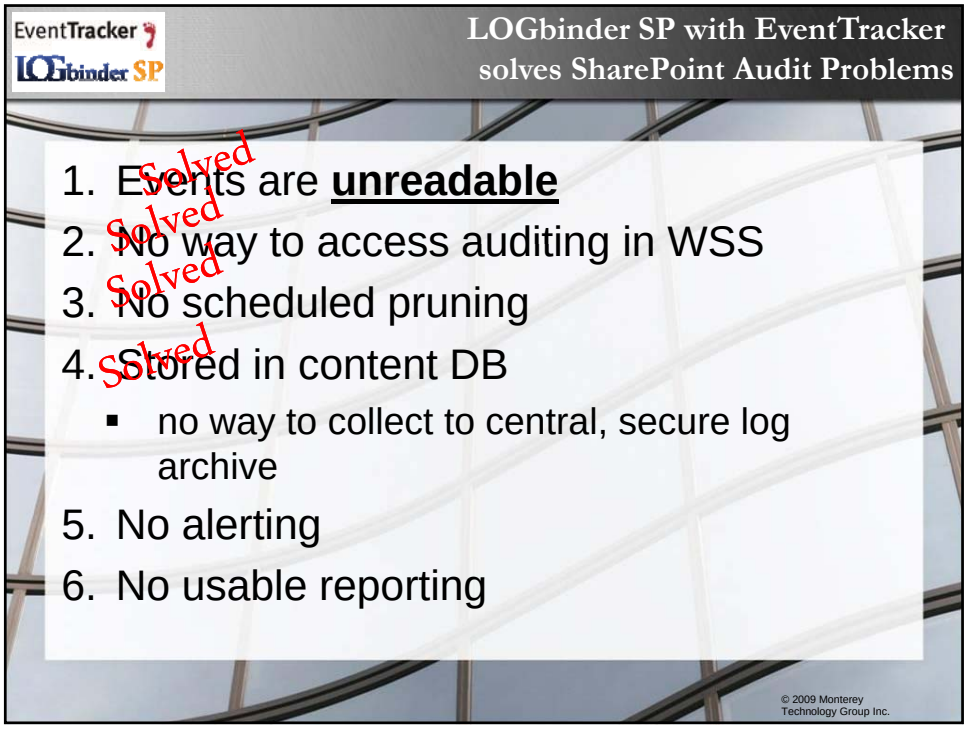


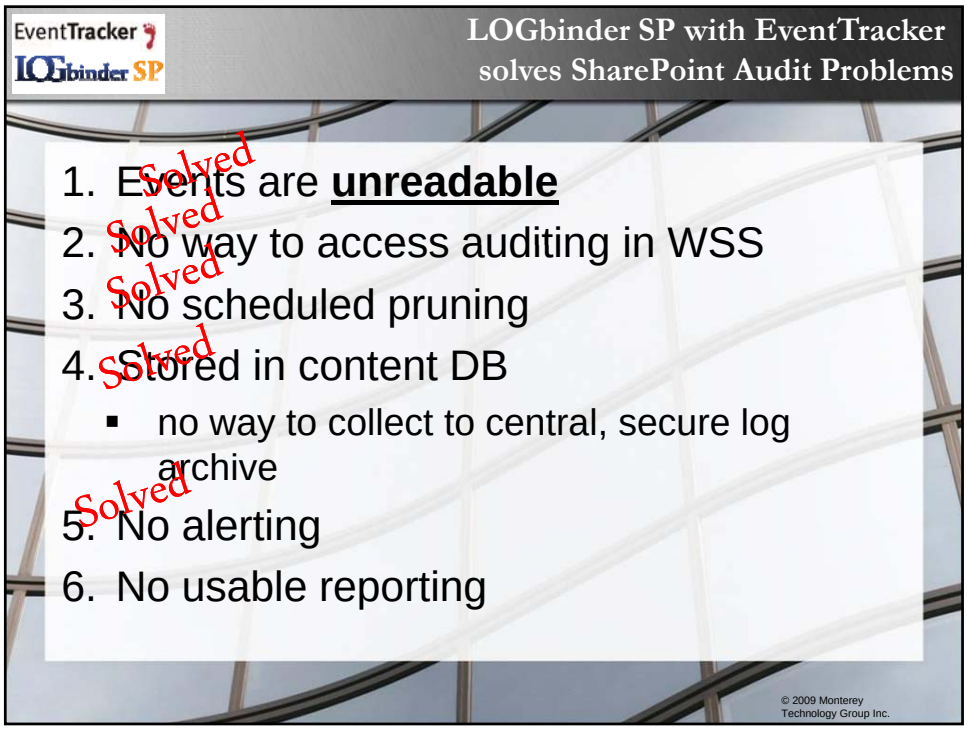












LOGbinder SP with EventTracker solves SharePoint Audit Problems

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

Want to Learn More?

- ❑Download LOGbinder SP
- ❑Visit www.LOGbinder.com
- ❑Download EventTracker
- ❑Visit www.prismmicrosys.com