Randy Franklin Smith's ULTIMATE WINDOWS SECURITY .COM™

Managing Access Control in SharePoint

- Made possible by:

LOGbinder SP™
SharePoint Auditing Made Easy

ULTIMATE WINDOWS SECURITY .COM

- **Brought to you by**

LOGbinder SP™
SharePoint Auditing Made Easy

www.logbinder.com

Preview of Key Points

- **SharePoint permissions**
  - Permission levels
  - Inheritance
  - Item level permissions
- **Groups**
  - SharePoint
  - AD
- **Useful tools**
- **Auditing access control changes**

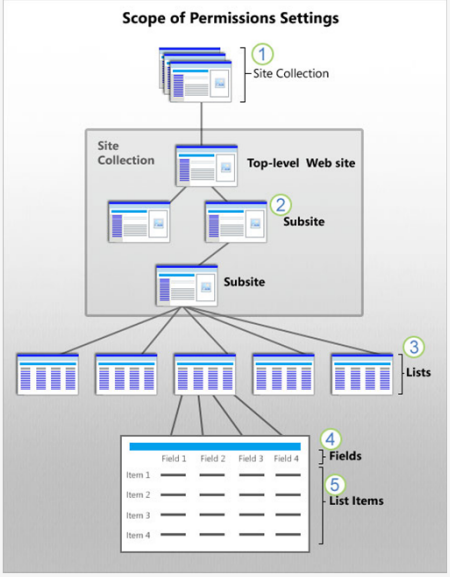
Permissions

- Not the actual assignment of access, but the **type** of access
  - View, create, edit, delete
- **3 kinds of permissions**
  - List
  - Site
  - Personal

Permission Levels

- **Permissions are not assigned**
  - Instead: permission levels
- **Permission levels**
  - Convenient combinations of permissions
- **To see the permission levels for your site**
  - Click Site Actions
  - Click Site Permissions to see the permissions page.
  - Click Permission Levels.

Permission Inheritance



- Normally permissions flow from parent objects down to child objects.
- "Stop Inheriting"
- breaks inheritance at any level to create
- unique permissions for that object down
- "Inherit permissions" to erase unique permissions and go back to normal inheritance

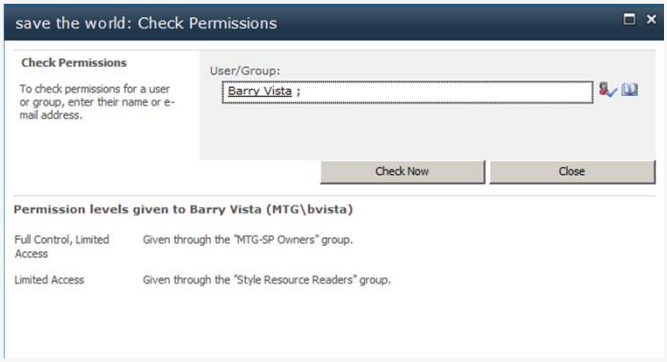
from Microsoft.com

Item Permissions

- Grant a group no permissions to the list or library
- At the item level grant permissions to appropriate objects
- Group will now show up in list permissions with “Limited Access”
- Give members link to any view of the list and they will see only list items where they have Read access

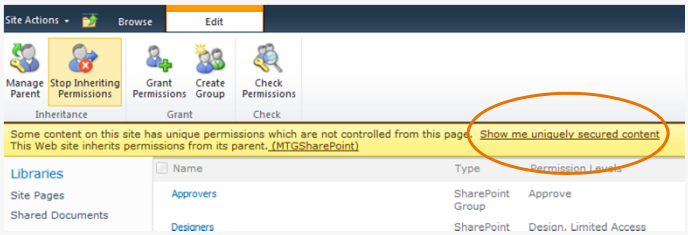
Useful tools

- What access does a given user have to an object?
  - Run “Check Permissions”



Useful tools

- **Which objects have unique permissions?**
  - "Show me uniquely secured content"



Useful tools

- **Do you allow end-user owners to manage access control?**
- **Custom People Picker to only display users from a certain OU, non AD users, etc**

http://technet.microsoft.com/en-us/library/gg602075.aspx

Groups

- **Don't assign permissions directly to users even though you can**
- **Use groups**
- **2 types of groups**
  - SharePoint
  - Active Directory

Groups

- **SharePoint groups**
  - Like local groups on a file server
  - Advantage: end user site owners can create and manage their own groups
  - Disadvantage: buried in SharePoint, not visible in AD
- **AD groups**
  - Less convenient for end user site owners
  - Much better for long term security

Auditing Access Control Changes

- **SharePoint group**
  - Created, deleted
- **SharePoint group member**
  - Added, removed
- **Unique permissions**
  - Created, removed
- **Permissions**
  - Updated, removed
- **Unique permission levels created**
- **Permission level**
  - Created, deleted, modified
- **SharePoint site collection administrator**
  - Added, removed

Auditing Access Control Changes

- **Enable auditing at the site collection level**
- **SharePoint records events in internal audit log**

SharePoint Audit Log

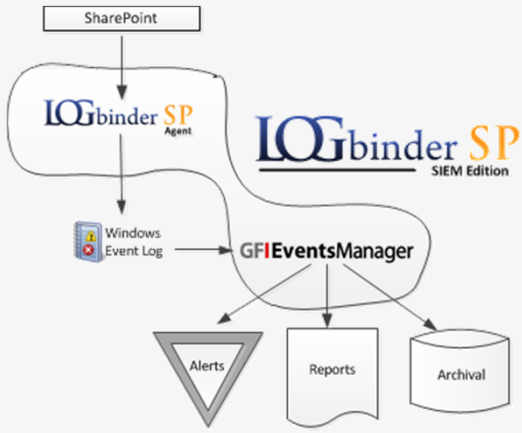
- Stored in content database
- Accessible only through SharePoint API
- No alerting, only rudimentary Excel reports
- Inaccessible to log management/SIEM products
- Extremely cryptic event codes and object keys
- Requires extensive knowledge and programming of SharePoint object model

LOGbinder SP

- Thin agent service that
  - Reads the SharePoint audit log
  - Resolves object IDs and translates cryptic event codes
  - Writes out easy to understand events to the Windows event log
  - Your log management solution takes over

LOGbinder SP SIEM Edition

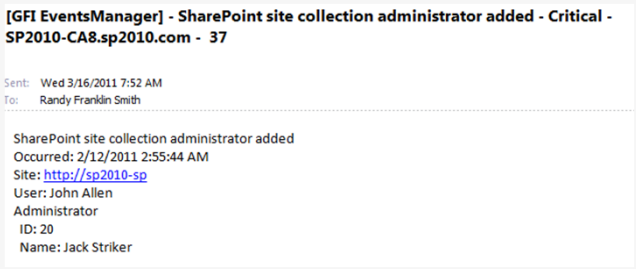
- **LOGbinder SIEM Edition adds**
  - Alerting
  - Reporting
  - Archival



Access Control Changes Report

Occurred	Site	User	Event ID	Operation	Description
3/15/2011 12:00:00PM	http://sp2010-sp	Administrator	29	Unique permissions created	Parent Object Type: Web Subtype: n/a URL: http://sp2010-sp Title: SP2010 Description: SharePoint.LOGbinder Test Site Object URL: Shared Documents This object no longer inherits permissions from the parent.
3/15/2011 12:00:00PM	http://sp2010-sp	John Allen	32	Permissions removed	Object Type: List Subtype: Document Library URL: /Shared Documents/Forms/AllItems.aspx Title: Shared Documents Description: Share a document with the team by adding it to this document library. Target Name: Jack Striker Type: User
3/15/2011 12:00:00PM	http://sp2010-sp	John Allen	37	SharePoint site collection administrator added	Administrator ID: 17 Name: Jack Striker

Administrator Change Alert



[GFI EventsManager] - SharePoint site collection administrator added - Critical - SP2010-CA8.sp2010.com - 37

Sent: Wed 3/16/2011 7:52 AM
To: Randy Franklin Smith

SharePoint site collection administrator added
Occurred: 2/12/2011 2:55:44 AM
Site: http://sp2010-sp
User: John Allen
Administrator
ID: 20
Name: Jack Striker

Bottom Line

- **Structure sites and subsites with access control in mind**
  - Leverage inheritance
- **Don't assign permissions to users**
- **Use AD groups instead of SharePoint groups**
- **Audit access control changes**
  - LOGbinder SP Agent Edition
    - if you have log management already
  - LOGbinder SP SIEM Edition
    - If you need alerting, reporting and archival

- **Brought to you by**

LOGbinder SP™
SharePoint Auditing Made Easy

www.logbinder.com