

# Improved Compliance via SharePoint Logical Access using Active Directory Groups

---

ISACA Training Week (“Geek Week”)

August 31, 2010

# Agenda

---

- Introductions
- Overview of SharePoint
- Logical Access in SharePoint
- Benefits and Risks of Leveraging Active Directory Groups
- How to Address AD Group Risk
- Additional Preventive and Detective Controls
- Closing Thoughts
- Questions

# Introductions

---

- Stoddard Manikin, CISM, CISSP  
Director, Southeast Region  
Logic Trends, Inc.  
Atlanta, GA
- Grady Boggs  
Security & Identity TSP  
Microsoft  
Atlanta, GA
- Logic Trends is a consulting and systems integration firm focused solely on Identity and Access Management (IAM)
- Founded in 2002, the Company has operations in Atlanta (HQ), Dallas, Tampa & Cleveland
- 200+ Identity & Access Management Engagements Completed
- Logic Trends is a Microsoft Gold Certified Partner



## Quick Overview of SharePoint

---

- Microsoft SharePoint 2010 is a portal product that makes it easier for people to work together
- Using SharePoint 2010, users can set up Web sites to share information with others, manage documents from start to finish, and publish reports to improve decision-making
- Originally called SharePoint Team Services and launched with Office XP (2001)
- Fourth major release is SharePoint 2010, featuring unprecedented integration with MS Office and core infrastructure components

# SharePoint 2010 Functionality

## Sites

SharePoint 2010 Sites provides a single infrastructure for all your business Web sites. Share documents with colleagues, manage projects with partners, and publish information to customers.

## Composites

SharePoint 2010 Composites offers tools and components for creating do-it-yourself business solutions. Build no-code solutions to rapidly respond to business needs.

## Insights

SharePoint 2010 Insights gives everyone access to the information in databases, reports, and business applications. Help people locate the information they need to make good decisions.



## Communities

SharePoint 2010 Communities delivers great collaboration tools—and a single platform to manage them. Make it easy for people to share ideas and work together the way they want.

## Content

SharePoint 2010 Content makes content management easy. Set up compliance measures "behind the scenes"—with features like document types, retention policies, and automatic content sorting—and then let people work naturally in Microsoft Office.

## Search

SharePoint 2010 Search cuts through the clutter. A unique combination of relevance, refinement, and social cues helps people find the information and contacts they need to get their jobs done.

# Current State of Organizational SharePoint Usage

---

- Emerging trends show that use of SharePoint is exploding within organizations as a way to share information
- Corporate access is served up internally and externally via SharePoint, creating security concerns
- Processes for administering access to SharePoint may be non-existent, immature, inconsistent or unable to keep pace with access requests
- As a consequence, logical access administration of SharePoint may be decentralized, poorly governed, and can lead to unnecessary risks

# Common Logical Access Administration Approaches

---

- Logical access to SharePoint can be controlled via native access controls, Active Directory (AD) group memberships or other third party Web access control product
- Silo Approach → Manage internally within SharePoint using “native” security
- Integrated Approach → Integrate with Active Directory to determine authorization rights based on AD security group memberships
- Enterprise Approach → Part of an enterprise-wide Identity and Access Management program with proper governance and controls; may leverage AD groups or third party security product

# SharePoint Access Administration via AD Groups

---



- We typically see a combination of approaches in real-world deployments
- From an auditor's perspective, it is best to focus the preventive controls in one place
- Ideally, access is managed primarily via AD group memberships with appropriate governance of those AD groups

# Reliance on AD Group Access Uncovers Risks

---

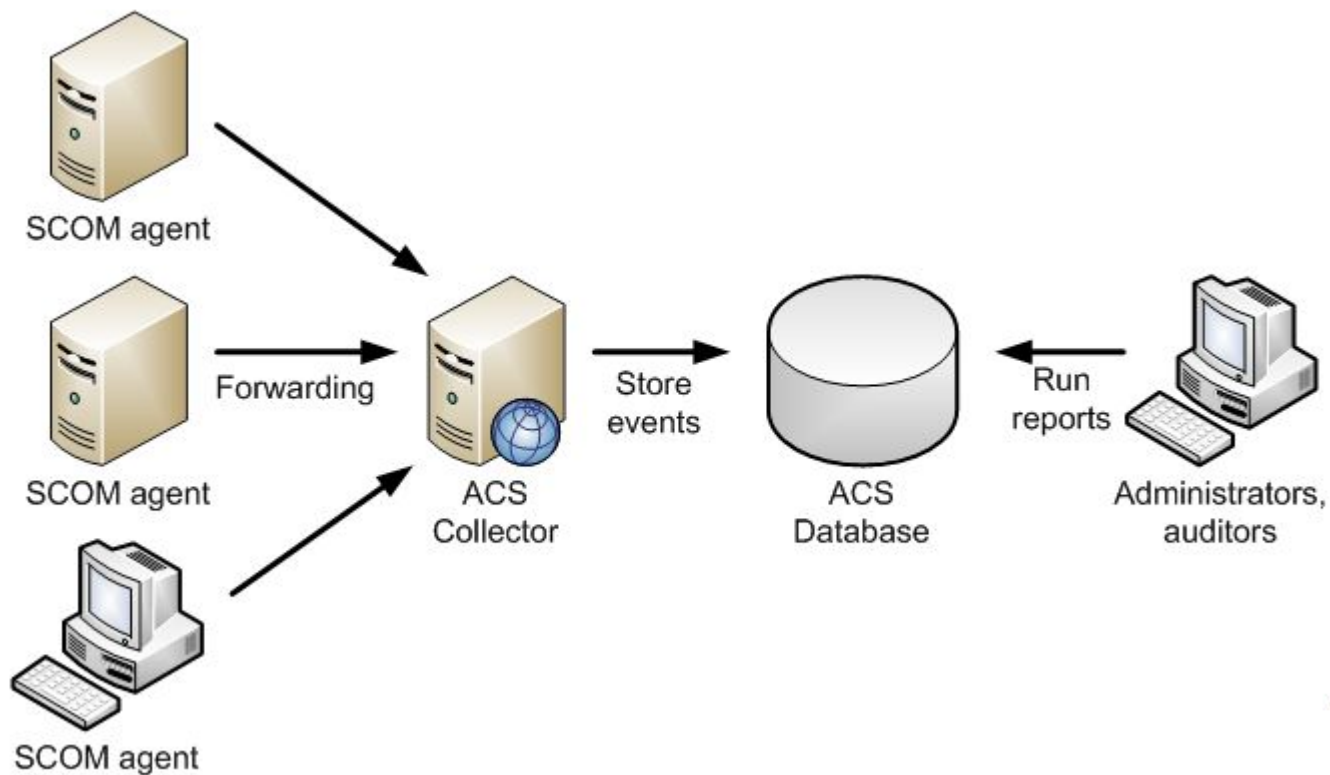
- Relying on AD groups for access permissions in an organization can reveal existing issues with AD group implementation
  - **Flawed governance model** for creating groups, assigning users to groups, removing duplicate group
    - For example, you don't want a developer creating roles on the fly; should be decided by business owner
  - **Group proliferation** issues where new groups are frequently created without checking existing groups leading to duplicates; groups are created as one-off permission solutions; group descriptions may be non-existent or lack sufficient explanation to be helpful
  - A user's accumulated access may be **infrequently reviewed/certified**, resulting in inappropriate access

## Ideal Ways to Address These Risks

---

- Introduce role governance model that also governs processes and actors for creation, modification and deletion of AD groups
- These controls and processes are best implemented in an automated (rule-based) or semi-automated fashion (request-based)
- Review groups (roles) and group memberships (users) on a periodic basis (access reviews/attestation)
- Tools are available for these purposes, typically called Access Governance or Role Lifecycle Management software
- Leading vendors include Omada, Oracle, CA, SailPoint, and Aveksa

# Additional AD Auditing (Detective Controls)



# Why the Security Event Log is Important

---

- Change and privileged use is monitored
- Security threats can be identified, e.g. hacking and viral activity
- Misuse of resources can be tracked
- Auditors and security officers can monitor for misuse for regulatory compliance
- Administrators can track activity, e.g. account lockouts

## Problems with Traditional Log Files

---

- Only keeps a certain amount of historical information locally
- Security eventlog is only as trustworthy as the administrators
- Analysis of distributed logs is difficult and time-consuming
- Delegation to auditors or security officers is not possible
- No centralized “as it happens” live monitoring is possible

## Closing Thoughts

---

- Formalize an enterprise wide Identity and Access Management program
- Leverage Active Directory as much as possible for logical access
- Ensure proper preventative controls are in place (i.e., rule-based and request-based entitlements)
- Ensure proper governance is used to manage AD group creation or management
- Ensure proper detective controls are in place (i.e.), and use these reports to fine tune your preventative controls
- Perform routine recertification or attestation processes

# Questions

## Contacts



Grady Boggs

Microsoft

404-713-1509

[gboggs@microsoft.com](mailto:gboggs@microsoft.com)



Stoddard Manikin

Logic Trends, Inc.

770-551-5045

[smanikin@logictrends.com](mailto:smanikin@logictrends.com)