



# Active Directory Security Essentials



Planning In-Depth Security  
Establishing Secure Active Directory Boundaries

John Policelli  
[jpolicelli@msystemsgroup.com](mailto:jpolicelli@msystemsgroup.com)



## | Agenda

- Introduction
- Part I - Planning In-Depth Security
  - Security Strategy
  - Deployment Scenarios for Domain Controllers
  - Planning Through Threat Analysis
- Part II - Establishing Secure Active Directory Boundaries
  - Specifying Security and Administrative Boundaries
  - Selecting an AD Structure Based on Delegation Requirements
  - Establishing Secure Collaborations with Other Forests
- Questions and Answers



## | Introduction: TWSUG Active Directory Special Interest Group

- The mandate of this group is to meet on a regular basis to discuss Active Directory Services related-topics, engage in presentations and participate in various community activities
- Design, implementation and support of Active Directory and associated services, security, disaster recovery, interoperability with other directories, identity management and DNS



## | Introduction: Importance of AD in a Windows IT Infrastructure

- Plays a key role in:
  - Distributed network security
  - Identity management
  - Windows manageability
- Stores confidential data
- Required by several Microsoft technologies



## Introduction: Importance of Securing AD

- A default installation of Active Directory is inherently unsecured
- A considerable amount of post installation configuration is required to mitigate the risk of threats, vulnerabilities, and attacks against Active Directory
- The number of threats, vulnerabilities, and attacks against Active Directory are increasing on a regular basis and are becoming more refined
- A security breach against Active Directory could impact business continuity



## Introduction: Security Principles

- Principle of Least Privilege
  - Give an entity the least amount of access it requires to do its job and nothing more
- Principle of Adequate Protection
  - An asset must be protected to a degree consistent with its value
- Principle of Easiest Penetration
  - It must be assumed that an intruder will attempt to use any available means of penetration
  - This does not necessarily entail the most obvious means, nor is it necessarily the one against which the most solid defense has been installed
- Principle of Weakest Link
  - A security system is only as strong as its weakest link



# Active Directory Security Essentials

## Part I: Planning In-Depth Security



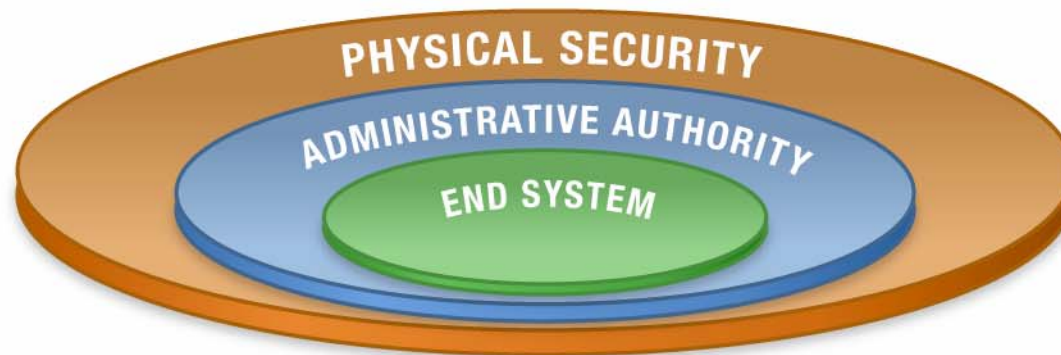
### TOPICS

- Security Strategy
- Deployment Scenarios for Domain Controllers
- Planning Through Threat Analysis



## Security Strategy

- When planning for AD security, divide all security elements into discrete security layers
- Active Directory security policies and practices can be divided into the following layers:
  - Physical Security
  - Administrative Authority
  - End System





## | Security Strategy / Physical Security

- Physical access to domain controllers
- Backup data
- Network components





## | Security Strategy / Administrative Authority

- Security management
- Secure administrative practices





## | Security Strategy / End System

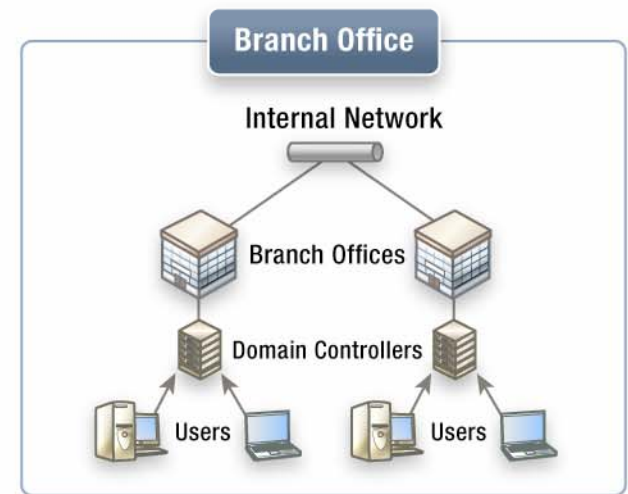
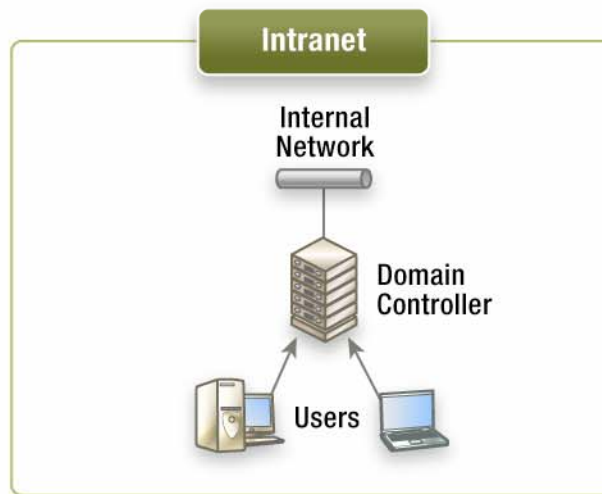
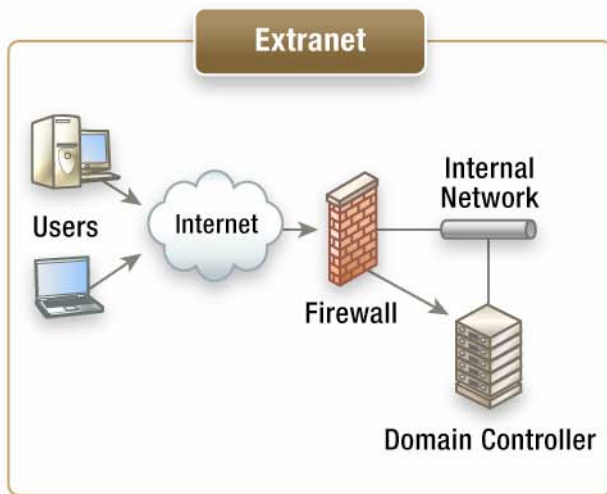
- Domain controller settings
- Policy settings
- Deployment practices





## Deployment Scenarios for Domain Controllers

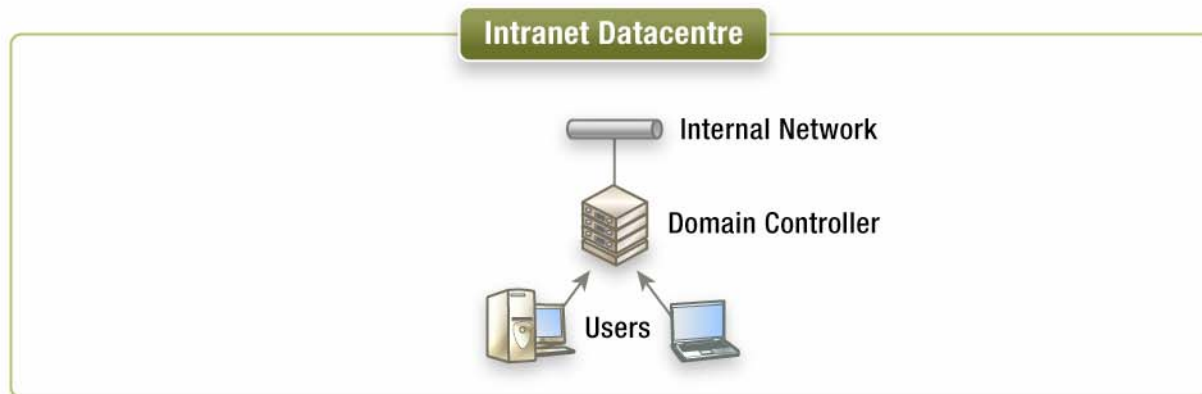
- The three most common operating environments are:
  - Intranet Datacentre
  - Branch Office
  - Extranet Datacentre
- The environment domain controllers are deployed plays a factor in the practicability of implementing AD security





## Deployment Scenarios for DCs / Intranet Datacentre

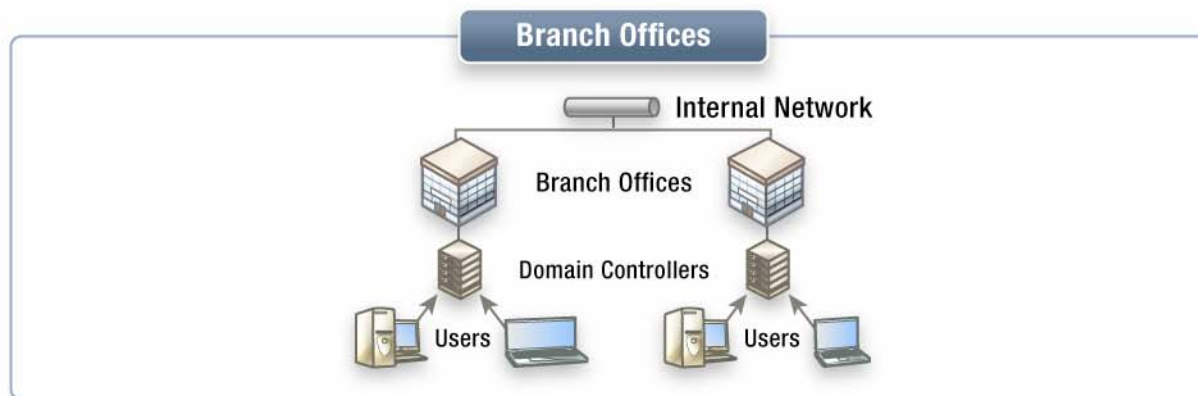
- The most common deployment scenario for DCs and easiest scenario to deploy and administer DCs
- Readily supports the requirements of a managed environment
- Centrally designed and managed DC and administrative policies
- Written administrative practices for building, deploying, and managing domains and DCs





## Deployment Scenarios for DCs / Branch Offices

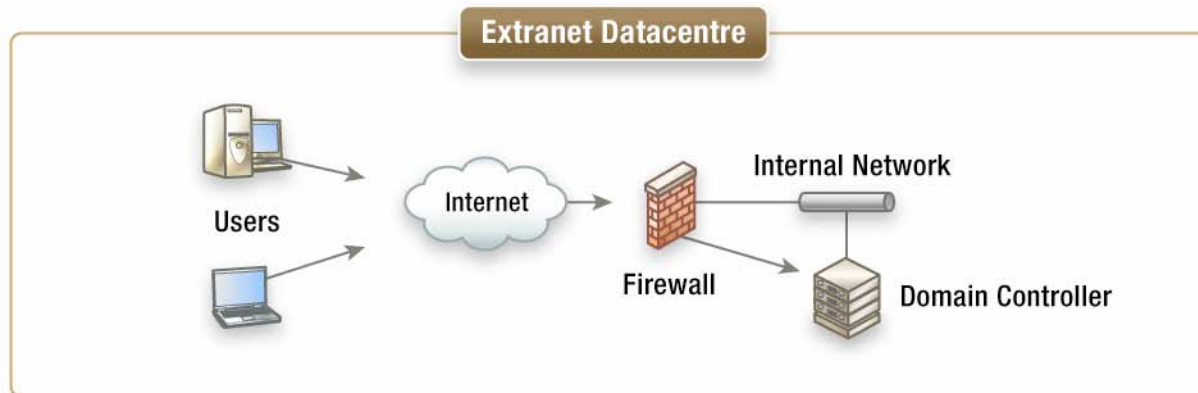
- Presents the greatest challenges in supporting the requirements of a secure, managed environment
- Decentralized DC management or remote management of DCs by administrators in the datacenter
- Lack of uniformity in the application of DC management and administrative practices





## Deployment Scenarios for DCs / Extranet Datacentre

- Variation of the Intranet Datacentre deployment scenario
- DCs can serve two purposes:
  - To manage servers and resources within the extranet
  - Can be placed in an outward-facing position to facilitate authentication and authorization for customers and partners
- Administrators may manage accounts within the extranet itself or they might have accounts within the enterprise intranet that are used to manage the extranet





## Planning Through Threat Analysis

- Proactive and reactive mitigation is essential in making AD deployments and administration secure
- Proactive planning protects assets by alleviating any threat to the system that might be caused by user mistakes and by attacks that are based on known threats
- Reactive planning provides contingency plans to implement under the following conditions:
  - Threat analysis fails to anticipate a threat
  - It is not possible to completely mitigate a threat
  - Security recommendations cannot be implemented



## Planning Through Threat Analysis / Threat Types

- Spoofing Identity
  - Illegally obtaining access and use of another person's authentication information
- Tampering with Data
  - The malicious modification of data
- Repudiation
  - Associated with users who deny performing an action, yet there is no way to prove otherwise
- Information Disclosure
  - The exposure of information to individuals who are not supposed to have access to it



## Planning Through Threat Analysis / Threat Types - Continued

- Denial of Service
  - An explicit attempt to prevent legitimate users from using a service or system
- Elevation of Privilege
  - Where an unprivileged user gains privileged access
- Social Engineering
  - Any type of behavior that can inadvertently or deliberately aid an attacker in gaining access to a user's password



## Planning Through Threat Analysis / Threat Sources

- Anonymous users
- Authenticated users
- Data administrators
- Service administrators
- Users with physical access to DCs



Anonymous  
User



Authenticated  
User



Data  
Administrator



Service  
Administrator



User with  
physical access  
to DCs



## | Planning Through Threat Analysis / Threat Sources – Anonymous Users

- Represents unauthenticated access to the network
- Results in a reduced level of security for Active Directory
- Can result in:
  - Information disclosure
  - Spoofing identity
  - Denial of service
  - Elevation of privilege



**Anonymous User**



## | Planning Through Threat Analysis / Threat Sources – Authenticated Users

- Represents any user who has successfully completed the authentication process
- Authenticated users have access to information in the directory and on DCs
- Can result in:
  - Information disclosure
  - Spoofing identity
  - Denial of service
  - Elevation of privilege



Authenticated User



## | Planning Through Threat Analysis / Threat Sources – Data Administrator

- Represents users who manage data in the directory that do not control the directory service or its configuration
- Can result in:
  - Information disclosure
  - Spoofing identity
  - Denial of service
  - Elevation of privilege
  - Tampering with data



Data Administrator



## | Planning Through Threat Analysis / Threat Sources – Service Administrator

- Represents users who manage directory service configuration and policies
- Sufficiently privileged to perform every administrative task, access and obtain full-control over all information (assets) stored in and protected by Active Directory
- Can result in:
  - Information disclosure
  - Spoofing identity
  - Denial of service
  - Elevation of privilege
  - Tampering with data
  - Repudiation



Service Administrator



## | Planning Through Threat Analysis / Threat Sources - Users with Physical Access to DCs

- Represents any situation in which an individual has access to an area where DCs and administrative workstations reside
- Can result in:
  - Information disclosure
  - Spoofing identity
  - Denial of service
  - Elevation of privilege
  - Tampering with data



User with physical access to DCs



## | Planning In-Depth Security – DEMO

# Active Directory...Gone in 60 Seconds

# NetPro Directory Experts Conference 2006

March 26-29, 2006 – Las Vegas!



## FIFTH ANNUAL EVENT HIGHLIGHTS MICROSOFT IDENTITY & ACCESS MANAGEMENT TECHNOLOGIES!

NetPro presents the **Directory Experts Conference (DEC)**, the only event dedicated to advancing the skills of the most experienced Active Directory and MIIS users.

DEC features technical education, networking and face-to-face interaction with key Microsoft product managers, plus a pre-conference Disaster Recovery workshop!

March 26-29, 2006  
Green Valley Ranch Resort & Casino  
Las Vegas, NV

### Speakers Include:

- **Stuart Kwan**, Director of Program Management for Identity & Access, Microsoft
- **Andreas Luther**, MIIS Group Program Manager, Microsoft
- **Paul Rich**, Senior Architectural Engineer, Microsoft
- **Guido Grillenmeier**, Senior Consultant, Microsoft Services, HP
- **Wook Lee**, Senior Engineer, HP
- **Jesse Sutela**, Senior IT Consultant, HP
- **Don Jones**, Director, ScriptingAnswers.com
- **John Enck**, Research VP, Gartner



[www.dec2006.com](http://www.dec2006.com)



# Active Directory Security Essentials

## Part II: Establishing Secure Active Directory Boundaries



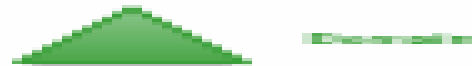
### TOPICS

- Specifying Security and Administrative Boundaries
- Selecting an AD Structure Based on Delegation Requirements
- Establishing Secure Collaborations with Other Forests



## Specifying Security and Administrative Boundaries

- The forest is the ultimate security boundary, not the domain
- The AD forest represents the outermost boundary within which users, computers, groups, and other objects exist
- Service administrators have abilities that cross domain boundaries





## | Specifying Security and Administrative Boundaries / Delegating Administration

- Reasons to delegate administration:
  - Organizational
  - Operational
  - Legal
- May need to delegate control over service management, data management, or both
- The goal of delegation is to achieve either autonomy or isolation



## | Specifying Security and Administrative Boundaries / Delegating Administration – Autonomy and Isolation

- Autonomy
  - The ability of admins to manage independently part or all of the AD service or the data in the directory
- Isolation
  - The ability of admins to prevent other admins from interfering in or accessing part or all of the AD service or the data in the directory



## | Specifying Security and Administrative Boundaries / Delegating Administration – Autonomy and Isolation - Continued

Administrative Role	Autonomy Means to ...	Isolation Means to ...
Service administrator	Manage independently all or part of service administration (service autonomy)	Prevent other service administrators from controlling or interfering with service administration (service isolation)
Data administrator	Manage independently all or part of the data that is stored in Active Directory or on member computers (data autonomy)	Prevent other data administrators from controlling or viewing data in Active Directory or on member computers (data isolation)



## | Specifying Security and Administrative Boundaries / Trusting Service Administrators

- All administrators who manage domains in a forest must be highly trusted
- All Domain Admins of all domains in the forest must be considered equally privileged and equally trusted
- The compromise of a single service administrator account in the forest can compromise the entire forest
- The compromise of a single domain controller in the forest can compromise the entire forest



## | Selecting an AD Structure Based on Delegation Requirements

- Begin by placing all organizations in a single-domain forest
- For each business unit with unique administrative requirements, determine the appropriate level of autonomy and isolation
- Separate forests for service isolation
- Separate forests for forest-level service autonomy
- Separate forests for data isolation from service owners



## | Selecting an AD Structure Based on Delegation Requirements / Implications for AD in Extranet Deployment

- Outward-facing DCs in an extranet present a risk due to Internet exposure
- AD implementations in an extranet should maintain complete service isolation from the rest of the organization
- Implement a separate AD forest for the extranet
- Any service administrator with responsibilities that span the intranet forest and the extranet forest should have a separate administrative account in each forest



## Establishing Secure Collaboration with Other Forests

- Inter-forest collaboration may be necessary for specific business or technical requirements
- Trust relationships can be used to setup resource sharing between pairs of domains from separate forests or between all domains in two forests
  - External Trust
  - Forest Trusts



## | Establishing Secure Collaboration with Other Forests / Trust Risks

- External Trusts
  - SIDs from untrusted domains can be added to access tokens, and the SIDs can be accepted by DCs in a trusting domain
- Forest Trusts and External Trusts
  - Users from a different forest can be added to administrative groups in the forest root domain or in other domains in the trusting domain



## | Establishing Secure Collaboration with Other Forests / SIDHistory and External Trusts

- SIDHistory is a migration feature that facilitates smooth migrations and allows continued use of account's current powers by preserving user's old account and group SIDs
- When a user logs on to a domain, the authenticating DC determines if the user has any values present in the SIDHistory attribute, and it includes those SIDs in the authorization data



## | Establishing Secure Collaboration with Other Forests / Security Risks Posed by sIDHistory

- If a particular SID can be added to a user's sIDHistory attribute, that user can gain unauthorized access to resources in the trusting domain, including administrative privileges
- Constitutes an elevation-of-privilege threat



## | Establishing Secure Collaboration with Other Forests

# sIDHistory Demo



## | Establishing Secure Collaboration with Other Forests / Blocking SIDs from Untrusted Domains

- SID filtering prevents attacks by malicious users who might try to grant elevated user rights to another user account
- SID filtering removes any SIDs that are not related to the user's account domain



## | Establishing Secure Collaboration with Other Forests / Security Risks Associated with Forest Trusts

- A high-level administrator in the trusted forest might have malicious goals
- When a forest trust is in place, one can add users from the trusted forest to the domain local security groups in the trusting forest
- Adding users from one forest to administrative groups in the forest root domain of another forest compromises the isolation of the forests



## | Establishing Secure Active Directory Boundaries / Recommendations

- Specifying Security and Administrative Boundaries
  - Determine whether delegation is driven by organizational, operational, or legal requirements
  - Determine whether the requirements indicate the need for autonomy, isolation, or both
  - Assess the level of trust that you have in service administrators (forest and domain)



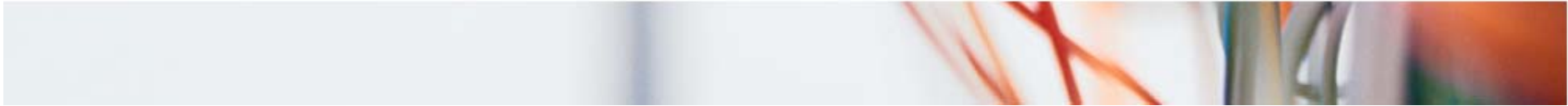
## | Establishing Secure Active Directory Boundaries / Recommendations

- Selecting an AD Structure Based on Delegation Requirements
  - Use the scenarios in “[Designing the Active Directory Logical Structure](#)” to identify the AD structure that matches your delegation requirements
  - Place outward-facing domain controllers that are deployed in an extranet in a separate forest



## | Establishing Secure Active Directory Boundaries / Recommendations

- Establishing Secure Collaboration with Other Forests
  - Create forest trust relationships only when all forest administrators and all domain administrators are trusted individuals
  - Ensure that SID filtering is enforced by default before creating an external trust between two domains in isolated forests



# Active Directory Security Essentials

## Questions and Answers

