ACTIVE DIRECTORY

SECURITY TECHNICAL IMPLEMENTATION GUIDE

Version 1, Release 1

10 March 2006

Developed by DISA for the DOD

Trademark Information

TABLE OF CONTENTS

Page

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

This Active Directory (AD) Security Technical Implementation Guide (STIG) provides security configuration guidance for the implementation of Active Directory on Microsoft Windows servers deployed within the Department of Defense (DOD). This STIG also provides general guidance for AD maintenance and synchronization products that might be used in conjunction with AD.

In simplest terms, AD is Microsoft's directory service for Windows. Among its important functions, it provides a distributed repository for identification and authentication data that is used within the collections of Windows computers known as domains and forests. Although AD does not have to be implemented in every group of Windows computers, it would be effectively impossible to support any more than a few Windows users in a workgroup without implementing AD. And though multiple interfaces are supported, it is important to note that AD supports access through the Lightweight Directory Access Protocol (LDAP) standard that most directory services support.

This document must be used in conjunction with the other STIGs developed by the Defense Information Systems Agency (DISA). The *Windows 2003/XP/2000 Addendum* provides crucial guidance for securing the Windows operating system (OS) on which AD and AD maintenance and synchronization products execute. The STIGs that cover database and web server products provide guidance to ensure that those services used by some AD maintenance and synchronization products also support a secure environment.

Other documents that should be used in conjunction with this STIG are the *Active Directory User Object Attributes Specification*, the *DOD Active Directory Concept of Operations*, *DOD Instruction 8551.1, Ports, Protocols, and Services Management (PPSM),* and the technical bulletins that are published by the Joint Task Force - Global Network Operations (JTF-GNO).

The *Active Directory User Object Attributes Specification* was developed to provide common naming and attribute guidance to DOD Components that deploy AD. The document specifies the naming convention and acceptable values for some of the attributes of AD User objects. Compliance with the specification is mandated by DOD Chief Information Officer (CIO) policy and is important in supporting interoperability between the Component AD deployments.

A *DOD Active Directory Concept of Operations* (CONOPS) is in final coordination. That document states, "The purpose of this CONOPS is to describe the current state of AD throughout DOD, the technical elements that comprise AD, the current DOD policy and guidance that governs and assists DOD Components executing AD, and the challenges and specifics of how DOD leadership plans to manage current and future AD implementations across the GIG [Global Information Grid] in the NetOps environment." Components are directed to that document for DOD-specific implementation direction.

DOD Instruction 8551.1, Ports, Protocols, and Services Management (PPSM) impacts network implementation. As a directory service, AD hosts and utilizes several network services. Because vulnerabilities have been documented for some of these services, DODI 8551.1 defines restrictions on the use of the associated ports, protocols, and services in order to protect network-accessible DOD resources. Requirements that reference DODI 8551.1 are defined in this document.

A final important reference is to the technical bulletins published by the JTF-GNO. Bulletins have been written to describe AD and the related DOD initiatives, the operational impact of an AD compromise, and issues involved in implementing Virtual Private Network (VPN) solutions.

1.1 Background

Microsoft introduced AD in Windows Server 2000. Although some of the function and terminology was present in the Windows NT Server OS, the implementation of AD in Windows Server 2000 marked the real incarnation of a native directory service from Microsoft. As such AD is able to act as a data store for multiple kinds of enterprise information.

It was noted above that it is possible to support Windows users without implementing AD. However such an implementation is largely impractical for groups of more than a few users. Once a workgroup encompasses many users, requires file and print services, and possibly incorporates some web or database servers, AD becomes an obligatory component of the infrastructure.

From the perspective of security, AD is almost an indistinguishable component of Windows. Administrators of Windows domains are required to use the AD tools to define user accounts. File access permissions are based on the accounts and groups defined in AD. The ongoing progression of Group Policy functions to configure more and more system settings is implemented through the storage and distribution infrastructure behind AD. Although it is discussed further in section 2.2.2, Forest and Domain Architecture, it bears emphasis that AD acts as an integrated, distributed database that spans Windows domain controllers. However, it is important to keep in mind that AD is distinct from the Windows operating system and that it is possible to have Windows servers and clients configured without an AD environment.

In Windows Server 2003 Microsoft continues to expand AD as a technology. Active Directory Application Mode (ADAM) is an LDAP-accessible directory service that runs as a user rather than system service on Windows. Multiple ADAM instances can be run on a single server to provide application-dedicated directory services. ADAM can also be used as a border directory where organizations want to deploy a higher degree of control over directory updates in synchronization operations.

One measure of the proliferation and importance of AD is the market for additional tools. Besides the directory synchronization tools available from Microsoft and other companies, there are AD maintenance tools designed to simplify and organize the administration of account provisioning and Group Policy definition. Measured in these terms AD is a technology that is widely used and highly important.

Once the functions of AD are understood, it is obvious that the importance of a secure configuration of AD cannot be overstated. Although the scope and continual development of AD makes it an impossible task to complete, this document provides some integrated guidance on how to configure AD more securely. It should be noted that Field Security Operations (FSO) support for the STIGs, Checklists, and tools is only available to DOD Customers.

1.2 Authority

DOD Directive 8500.1 requires that "all IA and IA-enabled IT products incorporated into DOD information systems shall be configured in accordance with DOD-approved security configuration guidelines" and tasks DISA to "develop and provide security configuration guidance for IA and IA-enabled IT products in coordination with Director, NSA." This document is provided under the authority of DOD Directive 8500.1.

The use of the principles and guidelines in this STIG will provide an environment that meets or exceeds the security requirements of DOD systems operating at the Mission Assurance Category (MAC) II Sensitive level, containing sensitive information.

1.3 Scope

This document describes security requirements to be applied to implementations of AD in DOD environments. The information is designed to assist Security Managers, Information Assurance Managers (IAMs), Information Assurance Officers (IAOs), and System Administrators (SAs) with the implementation of more secure AD configurations. As noted in the previous section, application of the requirements is intended to provide a certain level of assurance. Individual sites must determine the level of assurance that is appropriate to their environment and mission.

This document provides specific security guidance for AD as implemented on computers running the Windows 2000 Server or Windows Server 2003 operating systems. General guidance is provided for products or locally developed solutions that perform AD maintenance and synchronization functions.

1.4 Writing Conventions

Throughout this document, statements are written using the words "**will**" and "**should**." The following paragraphs are intended to clarify how these STIG statements are to be interpreted.

A reference that uses "**will**" indicates mandatory compliance. All requirements of this kind will be documented in the italicized policy statements in bullet format, which follow the topic paragraph. This makes all "**will**" statements easier to locate and interpret from the context of the topic. The IAO will adhere to the instruction as written. Only an extension issued by the Designated Approving Authority (DAA) will table this requirement. The extension will normally have an expiration date, and does not relieve the IAO from continuing their efforts to satisfy the requirement.

A reference to "**should**" indicates a recommendation that further enhances the security posture of the site. These recommended actions will be documented in the text paragraphs but not in the

italicized policy bullets. Nevertheless, all reasonable attempts to meet this criterion will be made.

For each italicized policy bullet, the text will be preceded by parentheses containing the italicized Short Description Identifier (SDID), which corresponds to an item on the checklist and the severity code of the bulleted item. An example of this is "(*G111: CAT II*)." If the item presently has no Potential Discrepancy Item (PDI), or the PDI is being developed, it will contain a preliminary severity code and "N/A" for the SDID (i.e., "*[N/A: CAT III]*").

1.5 Vulnerability Severity Code Definitions

During a Security Readiness Review, reports are produced that detail the vulnerabilities that are the result of deviations from the STIG requirements. These vulnerabilities are classified by severity into the following categories:

Category I	Vulnerabilities that allow an attacker immediate access into a machine, allow superuser access, or bypass a firewall.
Category II	Vulnerabilities that provide information that have a high potential of giving access to an intruder.
Category III	Vulnerabilities that provide information that potentially could lead to compromise.
Category IV	Vulnerabilities, when resolved, will prevent the possibility of degraded security.

Table 1-1. Vulnerability Severity Code Definitions

While these broad definitions reflect the standard that is applied across multiple technologies, it is helpful to list some AD-specific instances that would fit these categories.

- Category I vulnerabilities include those that allow an attacker immediate access to domain resources. An unauthorized Windows trust relationship between AD domains is an example.
- Category II vulnerabilities include those that result in the disclosure of information that has a high potential to allow an attacker to gain access into a domain or severely degrade AD functionality. Allowing everyone read access to files containing AD account data is an example.
- Category III vulnerabilities include those that result in the disclosure of information that could lead to the compromise of a domain or moderately degrade AD functionality. The failure to specify the use of strong data signing algorithms could allow an attacker to intercept and modify AD data as it traverses a network.
- Category IV vulnerabilities include those that might result in degraded domain security or AD functionality. The lack of an AD object ownership quota for users delegated the right to add printer objects could allow an AD database to be filled with invalid objects that exhaust the free space in the database.

1.6 DISA Information Assurance Vulnerability Management (IAVM)

The DOD has mandated that all IAVMs are received and acted on by all commands, agencies, and organizations within the DOD. The IAVM process provides notification of these vulnerability alerts and requires that each of these organizations take appropriate actions in accordance with the issued alert. IAVM notifications can be accessed at the Joint Task Force - Global Network Operations (JTF-GNO) web site, http://www.cert.mil.

1.7 STIG Distribution

Parties within the DOD and Federal Government's computing environments can obtain the applicable STIG from the Information Assurance Support Environment (IASE) web site. This site contains the latest copies of any STIG, as well as Checklists, Scripts, and other related security information. The NIPRNet URL for the IASE site is http://iase.disa.mil/.

1.8 Document Revisions

Comments or proposed revisions to this document should be sent via e-mail to fso_spt@disa.mil. DISA FSO will coordinate all change requests with the relevant DOD organizations before inclusion in this document.

This page is intentionally left blank.

2. ACTIVE DIRECTORY SECURITY

2.1 Introduction

Microsoft's brief definition of AD is a technology "…that enables applications to find, use, and manage directory resources (such as user names, network printers, and permissions) in a distributed computing environment". Although there are capabilities designed for interoperation with other platforms, AD is foremost the directory service for Windows environments.

Evaluating the importance of AD to an organization is linked inherently to evaluating the importance of Windows servers. This is obvious once it is understood that AD is virtually inseparable from any current Windows implementation of more than a few users. It was stated earlier, and bears repetition, that AD provides a distributed repository for identification and authentication data. As such AD is critical to enabling and securing shared resources such as files, printers, web sites, and database servers that involve information above the public confidentiality level.

Just as for other organizations, the importance of AD to DOD is inescapable. It is noted in the *DOD Active Directory Concept of Operations* that AD "…provides localized network directory services, access control, and other services to an expansive array of Component systems (databases, file servers, Community of Interest (COI) websites, etc.) and networks that are connected to the DOD Global Information Grid (GIG)." In recognition of this role and the link between AD and identification and authentication services, this STIG discusses the elements of AD that have security considerations and states requirements to provide a more secure AD environment.

Within the information technology (IT) industry in general, the standard protocol for access to directory services is LDAP. It is important to understand that LDAP has been an evolving standard with current activity focusing on LDAP version 3 (LDAPV3). It is recognized in the industry that the LDAP version 2 standard did not incorporate sufficient authentication controls and should not be used. Work within the Internet Engineering Task Force (IETF) has resulted in *Request For Comment (RFC) 2829, Authentication Methods for LDAP* and *RFC 2830, Lightweight Directory Access Protocol (v3): Extension for Transport Layer Security*. RFCs 2829 and 2830 address required security mechanisms for authentication. In *Active Directory LDAP Compliance*, Microsoft addresses these standards. Windows 2000 Server and Windows Server 2003 both support RFC 2829 and 2830, but are not fully compliant with every provision.

It is also important to note that the directory data that resides in AD is directly and indirectly accessed through other protocols. Windows clients use the Kerberos protocol to access domain controller authentication and authorization services that make determinations based on AD data. The Remote Procedure Call (RPC) protocol is used by domain controllers for AD data replication, by clients for access to Group Policy, and by administrative tools for some interfaces in the Active Directory Service Interfaces (ADSI) technology.

2.2 Security-Related Elements

Because of the close relationship, it is difficult to draw lines to clearly separate the elements of Windows from the elements of AD. And while the great majority of AD functions run on Windows servers that are "promoted" to be domain controllers, all the Windows member servers and desktop clients that connect to a Windows domain must run some elements that support AD functions. In concise terms, AD runs as a service on domain controllers and all the non-domain controller computers in a domain are clients of that service.

The *Windows 2003/XP/2000 Addendum*, and by reference Microsoft's *Windows Server 2003 Security Guide*, provide a great deal of security configuration guidance for Windows servers and clients. These references both contain specifications that address domain controllers as well. The intent of this AD STIG is to extend that information and focus security requirements specifically on AD elements for Windows 2000 Server and Windows Server 2003. This section of this document identifies the AD elements that are subject to the requirements in the next section.

It must be emphasized that this document is not intended as a comprehensive source of information on AD. In fact, an attempt has been made to include only information that is thought to be minimally necessary to identify AD elements. Microsoft and many other authors have produced a lot of documentation and many books that are available for reference. It is also noted that this document is not intended as a tutorial. It is assumed that persons attempting to comply with the stated requirements have a sound understanding of Windows and AD.

Throughout this document references are made to the *Windows 2003/XP/2000 Addendum*. That document and the following documents provided primary input and background to this document:

- Microsoft's *Windows Server 2003 Security Guide*
- Microsoft's *Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP*
- Microsoft's *Best Practice Guide for Securing Active Directory Installations* (Windows Server 2003)
- Microsoft's *Best Practice Guide for Securing Active Directory Installations and Day-to-Day Operations: Part I* and *Part II* (Windows 2000 Server)
- NSA's *Guide to Securing Microsoft Windows 2000 Active Directory*.

These and other associated documents are listed in Appendix A, Related Publications.

Based on these statements, the following subsections provide brief descriptions of AD elements for which security considerations exist. Questions about the AD technology should be researched in the referenced Microsoft documentation and web sites.

2.2.1 Active Directory Functional Level Considerations

To support a variety of environments that have multiple versions of Windows server software, the concept of domain controller functional levels was implemented in AD. A functional level should be thought of as a set of AD capabilities that all the domain controllers at that level can provide. Please note two differences for Windows Server 2000: the term mode was used rather than domain functional level and the concept of different forest functional levels did not exist.

The following characteristics of functional levels are important:

- The levels are progressive such that the "higher" levels require later OS versions on domain controllers and activate more functions.
- Once raised to a higher level, a domain or forest cannot revert to a lower level.
- There are domain functional levels and forest functional levels. All of the domain controllers in a domain must be at the same domain functional level. All the domain controllers in a forest must be at the same forest functional level.
- The Active Directory Domains and Trusts snap-in to the Microsoft Management Console (MMC) is the primary tool to raise functional levels.
- Windows 2000 mixed is the default domain functional level.
- Windows 2000 is the default forest functional level.

The following table summarizes the available levels and the Windows OS that may be running on the domain controllers in the domains and forests at that level.

Type	Functional Level	Supported DC OS		
		NT	2000	2003
Forest	Windows 2000	Y	Y	Y
	Windows Server 2003 Interim	Y		Y
	Windows Server 2003			Y
Domain	Windows 2000 mixed	Y	Y	Y
	Windows 2000 native		Y	Y
	Windows Server 2003 Interim	Y		Y
	Windows Server 2003			Y

Table 2-1. Forest and Domain Functional Levels

The AD elements that are impacted by the functional level and have a security consideration include:

- Universal groups are available at the Windows 2000 native domain level and above.
- Group nesting is available at the Windows 2000 native domain level and above.
- The SIDHistory feature is available at the Windows 2000 native domain level and above.
- Forest trusts and the Selective Authentication option for forest trusts are available at the Windows Server 2003 forest level.

Universal groups and group nesting are discussed in Section 2.2.3, Group Membership. Forest trusts are discussed in Section 2.2.4.2, Manually Defined Trusts.

2.2.2 Forest and Domain Architecture

This section discusses AD forest and domain architecture elements in three general areas:

- Domains, trees, and forests
- Replication, sites, Global Catalog servers, and Flexible Single-Master Operations (FSMO) servers
- Service dependencies and AD data files.

Domains, trees, and forests are terms used to describe hierarchical elements in AD architecture. At their simplest they each represent groups of computers that have different levels of security affiliation. It is important to identify these elements in terms of their security considerations so that related requirements can be understood.

Windows domain terminology was introduced with Windows NT server. Domains are groups of Windows computers that share a common security database for authentication. However, with the introduction of Windows 2000, the meaning of a domain was changed and the implications to security are extremely important. The following distinctions are most significant:

- Windows NT domains represent security boundaries. By default, there are no administrative accounts in one Windows NT domain that have administrative authority in another Windows NT domain.
- Domains in Windows 2000 and beyond represent administrative boundaries and allow the use of Organizational Units (OUs) to support delegated administration. Some administrative accounts defined in the forest root domain have administrative authority in **all** domains in the same forest. Also, because of the replication function of AD, some changes made by members of the Domain Administrators group are automatically replicated to all the domains in the forest.

Microsoft uses the terms isolation and autonomy to describe domain and forest boundaries. This is a complex subject, but the following greatly simplified distinction is important to security. Isolation refers to a forest boundary; administrative privileges do not cross the forest boundary. Autonomy refers to domain boundaries that allow administrative independence, but some administrative privileges do cross a domain boundary.

The concepts of domains, forests, and trees are best explained in context. The following diagram illustrates a relatively simple forest implementation.

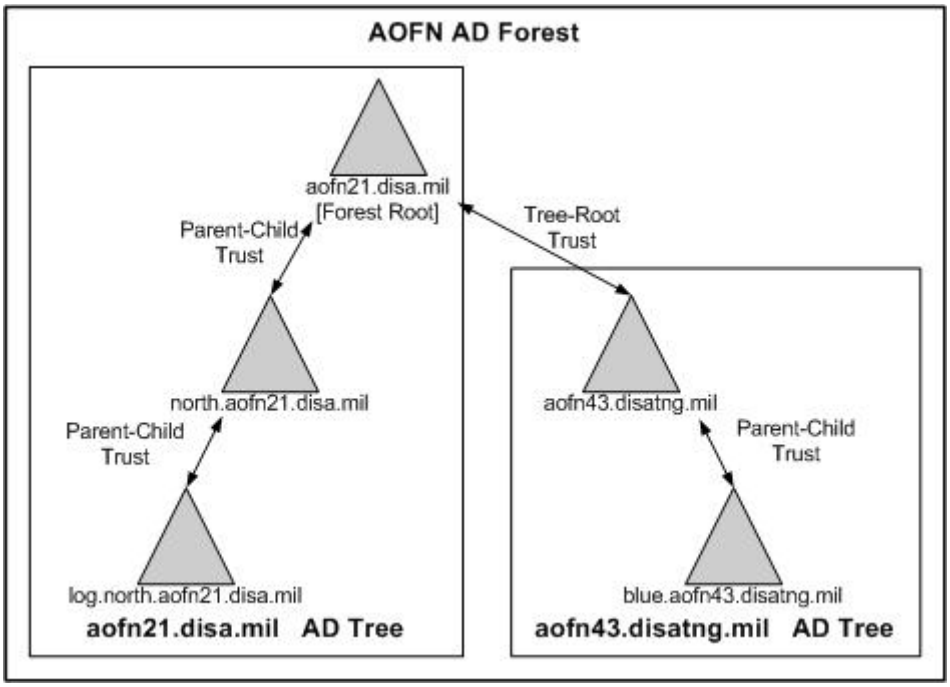

Figure 2-1. Sample AD Forest

The following characteristics of this forest architecture are important:

- The first domain in the forest, “aofn21.disa.mil”, is known as the forest root domain.
- The “north.aofn21.disa.mil” domain is a child of the aofn21.disa.mil domain. An automatic trust exists between them.
- The “log.north.aofn21.disa.mil” domain is a child of the north.aofn21.disa.mil domain. An automatic trust exists between them.
- The aofn21.disa.mil, north.aofn21.disa.mil, and the log.north.aofn21.disa.mil domains are members of the same AD tree and members of the AOFN forest. They share a common naming context that maps to their names used in the Domain Name System (DNS) server.
- The “aofn43.disatng.mil” domain is the first domain of a tree that is subordinate to the aofn21.disa.mil forest root domain. An automatic trust exists between them.
- The “blue.aofn43.disatng.mil” domain is a child of the aofn43.disatng.mil domain. An automatic trust exists between them.
- The aofn43.disatng.mil and blue.aofn43.disatng.mil domains are members of the same AD tree and members of the AOFN forest. They share a common naming context that maps to their names used in the DNS server.

There are other AD architectural characteristics that are not depicted. These include:

- An account is defined in only one domain in a forest, but can be used anywhere in the same forest (that resource access permissions permit) because of the automatic trust relationships between domains.

- Security settings that can be managed through the AD Group Policy feature are implemented at the domain level. If the same policy is desired for multiple domains, it must be copied between them.
- A forest root domain is said to be an "empty" domain if it contains only the accounts used to administer that domain and the forest.
- The concept of resource and account domains can be used to partition user definitions from the resources they access. In this model, user accounts are defined in one domain known as the account domain. Resources such as e-mail servers, web servers, database servers, and other application servers are defined in one or more domains known as resource domains.
- When a user in one domain attempts to access resources in another domain in the same forest and Kerberos authentication is being used, a domain controller that is trusted by both the user's computer and resource's server is used in the authentication process. This is likely to mean that a domain controller in the forest root domain is used in the authorization process.

The AD elements that are impacted by the forest, tree, and domain architecture and have a security consideration include:

- After a user is authenticated in his native domain, he does not have to be authenticated again to access resources in another domain in the forest. This is the effect of the automatic trusts between domains. This provides a kind of single sign-on capability.
- Some security settings, implemented through Group Policy, apply to an entire domain. This limits the ability to tailor those settings for individual users or groups.
- In cases where cross-domain resource access is common, placement and security of a forest root domain controller can have a significant impact on the authorization process.
- Implementation of an empty root domain allows stronger security policies to be defined for the sensitive accounts in that domain. It also allows fewer accounts to be defined there, including privileged accounts that might otherwise be needed to support applications. Finally a domain with fewer applications presents a smaller target that might be attacked.
- Where network perimeter protections include a demilitarized zone (DMZ) architecture, security is enhanced by the use of a separate forest for the hosts in that DMZ. This allows fewer network ports to be open because replication traffic is eliminated. It also eliminates the exposure of some information that would otherwise be replicated from the hosts on the protected side of the network.

Replication, sites, Global Catalog servers, and FSMO servers are loosely related subjects, but all have considerations related to architectural choices. From a security perspective, the configuration and placement of these elements can have an important impact to availability.

AD is implemented as a distributed database in each AD forest. Some AD data is present on every domain controller in the forest and some AD data is present on all domain controllers within a single domain. In addition to the Windows directory data held in AD, the settings and information captured for and used by the Group Policy feature are also considered AD data.

Other applications, most notably the Microsoft Exchange and Systems Management Server products, utilize AD for storage of their directory-related application data.

Replication is the mechanism by which AD data is synchronized among the domain controllers. Although most of the mechanics associated with AD replication require little configuration, there are three considerations related to configuration and security.

- Replication of AD data is handled through the Windows File Replication Service (FRS). This Windows service is mentioned later in this section as a dependency of AD.
- Replication requires network services that transmit data over Internet Protocol (IP) ports. The subject of port usage is briefly discussed in Section 2.2.6, Ports and Protocols.
- The definition of AD sites impacts replication traffic.

When Windows hosts in an AD forest are distributed across a geographical area that is connected by network links that do not operate at (or close to) Local Area Network (LAN) speeds, it is common to define AD sites. AD site definitions typically mirror physical network boundaries.

Although site definitions are most directly related to network architecture, there are security considerations that must be addressed:

- When sites are defined, it is also necessary to define site links. Site links have properties related to AD replication. The schedule property specifies what hours of the day that a site link can be used. The replication interval property specifies how often, within the schedule period, that domain controllers poll their replication partners to attempt replication. Correctly configured properties ensure that replication occurs on a timely basis so that distributed AD security data is kept current.
- An AD site is one level at which Group Policy can be applied. Group Policy is discussed in Section 2.2.5, Group Policy.
- When an AD client is logging on to a domain, it attempts to locate a domain controller within the same AD site. A proper site configuration enhances availability and reduces network traffic.

As a directory service AD has to be able to support efficient queries concerning objects throughout the span of a forest. To be more efficient, the AD Global Catalog server was implemented. A Global Catalog server is a Windows domain controller that has a subset of the directory information for every object in a forest. The server also has a copy of information that applies forest-wide, including Universal group membership and some trust information.

Global Catalog server location and access have security considerations.

- The Global Catalog server functions on domain controllers are accessed through IP ports 3268 and 3269. The subject of port usage is briefly discussed in Section 2.2.6, Ports and Protocols.
- A domain controller accesses the Universal group membership in the Global Catalog at the time each user logs on to the domain. In Windows 2000 Server, the inability for a domain controller to contact a Global Catalog server could result in denying the user

access to the domain. In Windows Server 2003, the Universal group caching function was implemented to reduce the need for synchronous contact.
- The Microsoft Exchange (2000 & later) product and the Outlook e-mail client are dependent on access to a Global Catalog server. The unavailability or corruption of the Global Catalog server could cause problems in Exchange or Outlook.
- The forest-wide scope of information present on a Global Catalog server represents an exploitable source of aggregated data about the forest.

Because AD data is distributed among the domain controllers in a forest, the design of AD had to include mechanisms to manage updates from multiple domain controllers. While the design does accommodate updates from multiple sources through the process of multi-master replication, there were some instances in which data integrity required a single-threaded approach. The resolution to this requirement is the implementation of FSMO roles. Please note that FSMO roles are also referred to as operations master roles.

FSMO roles represent specific AD management responsibilities held by assigned domain controllers. Two of the roles apply at the forest level and three at the domain level. AD elements such as AD database schema definitions and certain namespace controls must be managed at the forest level. AD elements such as security identifier (SID) assignment are managed at the domain level. Please note that the subject of FSMO roles is complex and should be thoroughly reviewed in the Microsoft documentation.

The following table summarizes the FSMO roles and lists some of the functions that each performs.

Scope	Role Name	Functions
Forest	Domain Naming Master	Controls the addition or removal of domains Controls the addition or removal of application directory partitions (2003)
	Schema Master	Controls updates to the AD database schema
Domain	PDC Emulator	Provides a source for time synchronization throughout the domain. At the forest root domain PDC Emulator, provides an authoritative time source for the entire forest Provides compatibility by acting as Windows NT Primary Domain Controller (PDC) for down-level clients and for Backup Domain Controllers (BDC) Propagates password changes from down-level clients to other domain controllers Periodically checks and resets ACLs on accounts in certain privileged groups

Scope	Role Name	Functions
Domain	RID Master	Maintains the Relative Identifier (RID) pool assignments used when a domain controller creates a SID for a new account
	Infrastructure Master	Checks references to objects in other domains in the forest (using a Global Catalog server) and maintains the references as changes occur

Table 2-2. Flexible Single-Master Operations Roles

The AD security considerations for FSMO roles include:

- The availability of the FSMO role holders is related to the availability of resources within domains. In some cases, an outage of a FSMO role holder can cause an immediate loss of client access to resources. In other cases, the loss will eventually result in the inability to make changes to AD objects.
- The integrity of the AD database is closely related to the integrity of the Schema Master role holder. While some products such as Microsoft Exchange and Systems Management Server require updates at installation time, there is no ongoing need to perform schema updates.
- The Infrastructure Master role is only relevant in forests of more than one domain. Also, placing this role on a domain controller functioning as a Global Catalog server impedes its function.

The final areas of consideration for forest and domain architectural elements are service dependencies and AD data files. Although these are simple, they are significant in terms of a secure AD environment.

In order for AD to function properly there are certain services that must be available and properly configured. Without these services, AD may function improperly or not at all. These services are DNS, a synchronized time source, and Windows FRS.

Access to a secure, properly configured DNS server is a practical prerequisite to AD. Each domain controller dynamically registers DNS service (SRV) records and host (A) records that establish the location of domain controller services including logon and authentication. A Windows server cannot be promoted to be a domain controller without access to a DNS server and a domain controller cannot function without persistent access. Windows clients use DNS to locate domain controllers so the inability of a client to access a DNS server prevents the client from using domain resources. The subject of securing DNS is complex. Please refer to the *DNS STIG* for specific details.

For multiple reasons, it is essential for Windows domain controllers in the same forest to have synchronized time.

- In the AD database objects are stored with a timestamp that includes date and time. In the event of a conflict detected during replication, the object timestamp may be used to determine which update to retain, so the integrity of the AD data is dependent on an accurate timestamp.
- The Kerberos protocol used by domain controllers for authentication and authorization functions requires time on clients and servers to be synchronized. Logon requests from clients with time outside an acceptable tolerance are denied.
- An accurate, synchronized time is critical to auditing functions. Without synchronized time, it may be impossible to correlate the events recorded in the logs of multiple computers. This could make it impossible to correctly evaluate the impact of an intrusion.

Although multiple tools are available to perform time synchronization, the Windows Time service is built into current Windows operating systems. It synchronizes server and client computer clocks across a network. The implementation of this service in Windows Server 2003 and Windows XP uses the Network Time Protocol (NTP). In Windows 2000 the Simple Network Time Protocol (SNTP) is used. These two Windows implementations use identical network packet formats over User Datagram Protocol (UDP) port 123 and are interoperable for the purposes of time synchronization in AD forests.

For computers within an AD forest, the default configuration of the Windows Time service uses a time source based on the AD domain hierarchy. The Microsoft documentation should be referenced for details, but the following information provides a simplified overview of the default configuration.

- Clients and member servers synchronize their time to the domain controller with which they authenticate.
- Domain controllers within a domain synchronize their time to the PDC Emulator FSMO role holder in their domain.
- For domains outside the forest root domain, the server holding the PDC Emulator role synchronizes its time to the PDC Emulator or any domain controller from its parent domain.
- The server holding the PDC Emulator role in the forest root domain is the authoritative source for time in the forest. It relies on its internal machine clock or has to be configured to synchronize its time to an external time source.

It is apparent from this discussion that the server holding the PDC Emulator role in the forest root domain provides a crucial function for time synchronization. There are two issues that arise as a result. The configuration of a secure time source for that server is critical to ensure an accurate time source for the forest. The designation of a standby operations master, as recommended in Section 2.3.6, Continuity, is a very important consideration for continual availability of a time source for the entire forest.

As indicated above, tools other than the Windows Time service are available to perform time synchronization. Although the Windows Time service is highly recommended because it allows a single, consistent method and does not require deployment of a separate program, specific environments may dictate the need for other tools. The most important goal should be an environment in which the ultimate time source is identical for as many servers and clients as possible.

It was noted earlier that AD relies on the Windows FRS to replicate data among the domain controllers. AD object data including identity, authentication, and authorization data is moved by way of AD replication. AD Group Policy Template data is also moved through AD replication. AD depends on a functioning replication system to ensure that logon and authorization services use current data to make access determinations. It should be noted that it is possible to configure AD to perform replication using Simple Mail Transfer Protocol (SMTP). However, due to possible propagation delays with network traffic of this type, this is not recommended.

Although the number of AD data files on domain controllers is small, their significance is substantial. The data can be grouped in four general categories of AD data and one category of data related to the FRS service on which AD depends. This data is composed of:

- The primary data store (referred to in this document as the AD database) is named “ntds.dit”.
- The files used by AD for internal transaction logging are named “edb*.log”, “res1.log”, and “res2.log”.
- Work files used by AD are named “temp.edb” and “edb.chk”.
- Group Policy Template data is stored under the SYSVOL directory.
- FRS data is stored under the Ntfrs directory.

The security considerations for these files are similar to other files. Integrity and availability are maintained through access control and data backup.

Access control for AD data files is accomplished through the file access permissions available for files on NT File System (NTFS)-formatted volumes. The common SYSTEM and Administrator full control access permissions are assigned.

Because of the way in which Windows accesses AD data, it is not possible to use common file backup methods. AD data must be backed up as part of an operation that backs up the Windows System State data. Among other items, a System State data backup includes the AD database and the Group Policy Template (GPT) data that may be necessary to restore AD.

Conversely, AD data on the domain controller cannot be restored under normal operating conditions. When it is necessary to restore AD data, the domain controller must be booted into a standalone mode called Directory Services Restore Mode (DSRM). This mode can only be entered by supplying the password that is assigned at the time a Windows server is promoted to be a domain controller. This password resides in the Security Accounts Manager (SAM) file on the domain controller.

2.2.3 Group Membership

The implementation of groups in Windows is the chief mechanism by which Role-Based Access Control (RBAC) may be implemented. By assigning user accounts to groups and referencing the groups in access permissions, users are effectively assigned roles that can be controlled more efficiently and accurately.

A brief note about terminology is important. Windows supports two distinct kinds of groups. The first is the security group. This is a group to which users are assigned for the purpose of access control. The second kind of group is a distribution group. This is a group that can be used by e-mail servers for sending mail to a persistent list of users. In this document, the term group refers to a Windows security group.

Group implementation in Windows is a complex subject that requires substantial documentation to explain well. Readers are directed to the Microsoft documentation and particularly to the *Microsoft Windows Security Resource Kit* for information. The objective of this section is to identify the most significant group issues as they impact AD. The following elements are identified:

- SID assignment and use
- Special privileged groups
- Universal groups
- Group permission strategies
- OU design
- AD object quotas.

In Windows each security principal, including users, groups, and computers, is assigned a SID at the time of creation. The SID is a unique value that identifies the security principal within the domain and forest. When a SID is assigned to a new account on a domain controller, the SID includes a RID that makes the account unique. The RID comes from a pool of values that are assigned to the domain controller by the RID master FSMO server. Thus an account SID can be identified as coming from a specific domain.

A SID is never reused. If an account is moved from one domain to another, a new SID is assigned to the account. Starting at the Windows 2000 native domain functional level, the SIDHistory feature allows old SIDs to be retained along with the new SID that is assigned when the account is moved.

SIDs play a primary role in resource authorization. When a user logs on to his domain, the SID for his account, the SIDs for all groups of which he is a member, and any SIDHistory values are extracted from the AD database. When the user attempts to access a resource, this list of SIDs is compared to the Access Control List (ACL) for the resource to determine what access is permitted.

This discussion of SID assignment and resource authorization is basic to understanding a potential vulnerability that involves resource authorization through an AD trust. The discussion of this issue is in Section 2.2.4.2, Manually Defined Trusts.

There are several pre-defined Windows groups that can be categorized as specially privileged. This is primarily true because the ACLs of many Windows resources are defined by default with access permitted to those groups. It is also true because some programs examine group membership to determine if the user is allowed to execute sensitive functions in the program.

The following briefly identifies the groups and security privilege implications for AD:

- Domain Admins and Enterprise Admins - Members of these groups have permissions to all AD objects at the domain and forest level respectively.
- Schema Admins - Members of this group have permission to modify the AD schema for a forest. This allows the addition, deletion, and modification of AD object definitions and their attributes. Among the object attributes are the default security descriptors that represent the default access permissions that are assigned to objects created from the schema definition.
- Group Policy Creator Owners - Members of this group have permission to add, delete, or modify Group Policy Objects (GPOs).
- Pre-Windows 2000 Compatible Access - Membership in this group allows users read access to many AD objects. The primary security issue associated with this group is anonymous access to AD data. This occurs when the group membership includes anonymous users or other groups that include anonymous users.
- Incoming Forest Trust Builders - In the forest root domain of Windows Server 2003 domain controllers, members of this group are allowed to create incoming, one-way forest trusts.

There are mechanisms available within AD to strengthen the security associated with privileged group membership. These include the AdminSDHolder object and the Restricted Groups Group Policy setting.

AdminSDHolder is an AD object that acts as a template for the security descriptor attributes of certain privileged accounts. Every hour the domain controller holding the PDC Emulator FSMO role compares the ACL on the AdminSDHolder object to the ACLs of accounts in certain privileged groups. This includes the Domain Admins, Enterprise Admins, and Schema Admins groups among others. If the ACL on an account differs, the ACL of that account object is overwritten using the ACL of the AdminSDHolder object. This ensures that the permissions on the account objects have not been compromised.

The Restricted Groups security setting in a Group Policy can be used to control the membership of a group. The Restricted Groups setting can be configured with two properties for each group. The “Members” property specifies the accounts that are to be members of the group. An empty Members property specifies that the group will have no members. The “Members of” property specifies which group(s) the subject group should be a member in. When the Restricted Groups setting is defined in a GPO, the group memberships are checked each time Group Policy is refreshed. As an example, if a GPO with a Restricted Groups setting is configured for the Schema Admins group and the Members property is empty, accounts that are inadvertently or maliciously added to the Schema Admins group are removed the next time Group Policy is refreshed.

A “universal” group is not a specific group, but rather one of the types of Windows groups. It can have members (accounts) from any domain in a forest and so can be useful when resource access permissions need to be applied to users in many domains. (Conversely there is no logical need for universal groups in a single-domain forest.) There are several considerations for universal groups for AD security:

- Universal groups are available starting at the Windows 2000 native domain functional level.
- Because they are forest-wide objects, universal groups are kept in the Global Catalog and changes are replicated forest-wide. This can have network traffic and propagation delay implications if membership changes are made frequently.
- Each time a user logs on to the domain, the domain controller checks the Global Catalog server to retrieve the SIDs of the universal groups that have the account as a member. Unless the Windows Server 2003 universal group caching function is available, unavailability of the Global Catalog server prevents logon.
- The use of SID filtering can cause the SID of a universal group to be discarded during resource authorization across a trust. This occurs when the universal group is created in a domain different from the user’s domain. SID filtering is discussed in Section 2.2.4.2, Manually Defined Trusts.

The concept of group membership for accounts has been discussed, but some brief words about group nesting and permissions strategy is important. Group nesting affects, and is affected by, AD configuration.

Group nesting refers to the ability to embed one group within another. It is available starting at the Windows 2000 native domain functional level. This capability makes it substantially easier and more efficient to construct access permissions. This enhanced ease and efficiency can result in more accurate and therefore more secure permissions being assigned.

Microsoft has suggested some strategies that utilize group nesting when applying permissions. The use of these strategies provides an organized way to implement RBAC. There are three basic strategies; they are referenced by letter sequences:

- A-G-DL-P - In this strategy, accounts are added to global groups, global groups are added to domain local groups, and resource permissions are granted to domain local groups.
- A-G-G-DL-P - This strategy adds nesting of global groups where that helps to reduce the overall number of groups. Accounts are added to global groups, global groups are nested in global groups, global groups are added to domain local groups, and resource permissions are granted to domain local groups.
- A-G-(G-)U-DL-P - This strategy adds universal groups or replaces one level of global groups with universal groups. Accounts are added to global groups, global groups are nested in global groups, global groups are nested in universal groups, universal groups are added to domain local groups, and resource permissions are granted to domain local groups.

Two common characteristics are consistent throughout all of these strategies. Accounts are always added to global groups and permissions are only granted to domain local groups.

OUs are mentioned here primarily to ensure that the distinction between an OU and a group is noted. An OU is a grouping of users or computers that is defined in AD for ease of management. An OU does not have a SID attribute. Groups are assigned SIDs that can be referenced in ACLs that are used to control resource access. OUs are used with GPOs to apply security settings and other configuration settings.

It should also be noted that administration of OUs can be delegated to non-Administrator accounts. This helps to implement the security principles of separation of duties and least privilege.

The final AD element to be discussed in the context of group membership is AD object quotas. This subject is only loosely connected to groups in that two built-in groups are automatically exempt from it.

The AD object quota was introduced in Windows Server 2003. It is a means by which a limit can be imposed on the number of objects that a single account can own in a given AD database partition. This control provides a defense against inadvertent or deliberate attempts to exhaust the capacity of an AD database. This could occur when a member of the Group Policy Creator Owners group creates a scripted loop that adds GPOs.

The security considerations for AD object quotas include:

- Separate quotas are applied to each AD database partition except that quotas do not apply to the schema partition.
- Deleted objects, known also as tombstones, are factored into the count of owned objects. It is possible to alter the factor so that tombstones count for less than one object.
- Quotas can be defined as the default applied to all accounts or for individual accounts.
- When not defined, the default quota is no limit.
- Members of the Enterprise Admins and Domain Admins groups are exempt from quotas.

2.2.4 Trust Relationships

AD trust relationships are an inherent part of domain and forest architecture. Trusts are the mechanism for allowing a user to authenticate to one domain and access resources in another domain without authenticating again. Trusts always exist between domains in the same forest, but can be configured between domains in different forests, between two forests (with Windows Server 2003), and between a domain in a forest and a Windows NT domain or UNIX Kerberos realm outside the forest.

Every time a domain is defined, the trust configuration within the forest is automatically altered. Identifying trust types and their configuration options is essential for understanding the impact on resource access control. This section first describes certain trust properties and associated options. The following subsections describe the trusts that are created by default or by manual administrator action.

This section describes some common properties of trusts, terminology used with trust descriptions, and a figure illustrating how trusts might be defined. The following subsections describe the trusts that are automatically and manually defined in AD environments.

There are two properties that significantly impact the effect of every trust. These are transitivity and direction. For some trust types the direction property is fixed; other types allow configuration.

The property of transitivity refers to a logical relationship. It is explained generically by considering the relationship between three elements. If there is a relationship between A and B, and the same relationship between B and C, then transitivity exists if the same relationship exists between A and C. When this is applied to trusts, it would mean that: domain A trusts domain B, domain B trusts domain C, and for a transitive trust domain A trusts domain C.

The property of direction refers to one-way or two-way trust flow. It is possible to think of flow as the direction in which user credentials (SIDs) travel for resource authorization. If a user in domain A attempts to access a resource in domain B, and a one-way trust (at least) exists between A and B, the user's credentials travel from A to B. When users from each domain can access resources in the other, a two-way trust exists.

There are two additional sets of terminology that are used in trust descriptions:

- Trusted and trusting - A trusted domain is the domain where the user is authenticated and his SIDs are extracted from AD. A trusting domain is the domain that accepts the user's SIDs as passed from the trusted domain.
- Incoming and outgoing - An incoming trust specifies that the local domain is trusted by another domain. An outgoing trust specifies that another domain is trusted by the local domain.

A final concept that is important for the trust discussion is the trust path. A trust path refers to the number of domain controllers that have to be contacted in order to validate that a trust relationship exists that allows a specific access to occur. This concept becomes significant in a complex forest with an extensive tree structure. In that case, the trust path between a domain "far down" in one tree to a domain far down in another tree can require traversal of several domains in each tree. In Windows Server 2003 domains, a client cannot traverse more than 10 trusts to access a resource.

Trust concepts are best explained in context. The following diagram illustrates where different trust types might be implemented and is useful for the following discussions.

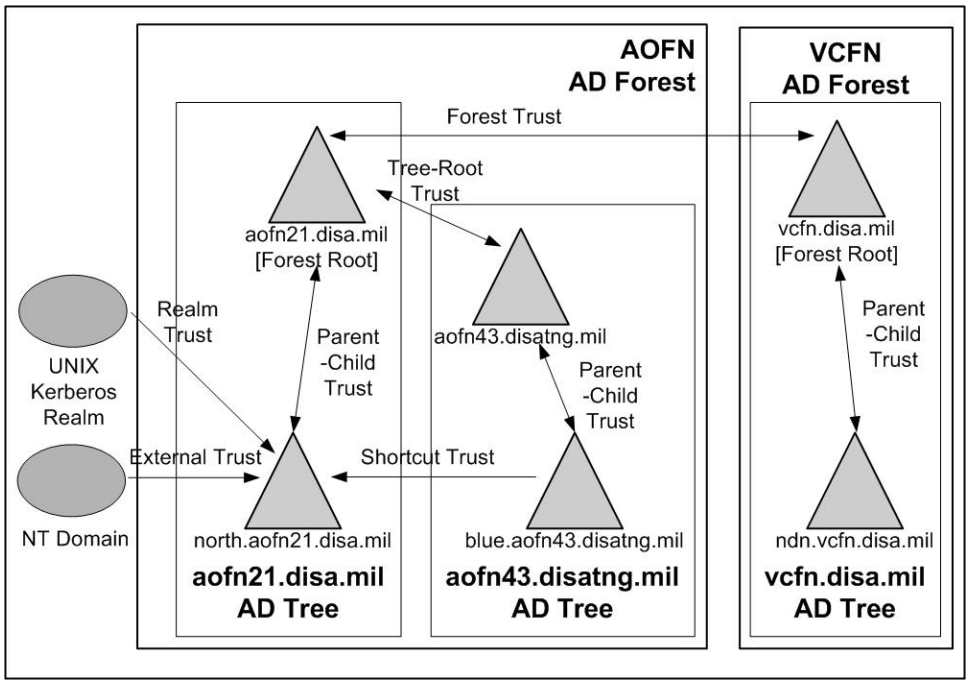

Figure 2-2. Sample Trusts

2.2.4.1 Automatically Defined Trusts

It was noted earlier that adding a domain to a forest automatically alters the trust configuration in the forest. Specifically, as a domain is added to an existing forest, a trust is automatically added between it and the domain to which it is logically connected. This logical connection is in one of the following forms:

- A parent-child trust relationship exists between two domains within the same tree.
- A tree-root trust relationship exists between the forest root domain and the first domain in a different tree in the forest.

Trusts between domains within a forest are identified by relationship type. They are created with the following properties:

Trust Type	Transitivity	Direction
Parent-child	Transitive	Two-way
Tree-root	Transitive	Two-way

Table 2-3. Automatic Trust Types

These properties reflect the fact that forest design is intended to enable resource access across domains. That is, the two-way, transitive nature of these trusts allows a user in any of the

domains to access resources in the other domains to which that user has the appropriate access permissions. This is a primary reason why the way in which forest and domain architecture is implemented has such significant security considerations.

2.2.4.2 Manually Defined Trusts

There are situations in which trusts are needed beyond those created automatically within a forest. In most cases this reflects a desire to extend trust beyond the forest boundary, but there is one implementation that is used within a forest.

The following trust types are manually created as needed:

- External - An external trust can be created between two domains in different forests or between an AD domain and a Windows NT domain.
- Forest - A forest trust can be created between the forest root domains of two forests. However, forest trusts can only be created between forests that are operating at the Windows Server 2003 forest functional level. This requires that all the domain controllers in both forests are running Windows Server 2003.
- Shortcut - A shortcut trust can be defined between two domains in the same forest. A shortcut trust is used where the trust path is long or network connections between domain controllers in the trust path cannot efficiently support the authorization traffic.
- Realm - A realm trust can be created between a domain and a non-Windows system such as a system hosting a UNIX or Linux OS with Kerberos version 5.

These trusts are created with the following properties:

Trust Type	Transitivity	Direction	Authentication	SID Filtering
External	Non-transitive	One-way	Domain-wide or Selective	Enabled or Disabled
Forest	Transitive (within forests)	One-way or two-way	Forest-wide or Selective	Enabled or Disabled
Shortcut	Partial	One-way or two-way	N/A	N/A
Realm	Either (With supporting partner)	One-way	N/A	N/A

Table 2-4. Manual Trust Types

The Authentication property became available in Windows Server 2003. It supports more granular control over trusts. It is implemented through an additional property for external and forest trusts and a new permission for AD computer objects:

- The trust Authentication property defaults to a value that allows all users in the trusted forest or domain to be authenticated via the trust. The other option is Selective authentication.

- The “Allowed to authenticate” permission for AD computer objects is not set by default. It can be set to Allow or Deny for specific users or groups.

When an external or forest trust has the Selective authentication option set and a user from a trusted forest or domain attempts to access an object, the Allowed to authenticate permission on the computer object in the trusting domain is checked. If the permission is set to “Allow”, access is permitted.

The SID Filtering property was added in a security patch to Windows 2000 Server and was built into Windows Server 2003. It was designed to prevent an elevation of privilege attack that could result from the way authorization data from trusted forests is used. Information on this vulnerability is documented in Microsoft security bulletin MS02-001.

In Section 2.2.3, Group Membership, the concept of account SIDs was discussed. As noted there, when a user logs on, the SID for his account, the groups he is a member of, and any SIDHistory attribute values are extracted from the AD database. When a user attempts to access a resource through an external or forest trust, this collection of SID authentication data is passed to the domain where the resource exists.

A vulnerability existed because trusting domains did not verify that the SIDs in the authentication data all came from the trusted domain. If the authentication data is compromised by the addition of SIDs known to have access permissions to the resource, then an unauthorized user may gain access that he would not otherwise have.

When the SID Filtering property is enabled, the trusting domain removes any SID in the authentication data that was not generated in the trusted domain. This ensures that only accounts created in the trusted domain are eligible for access to resources in the trusting domain.

Some notes on the use of SID Filtering are important:

- The removal of SIDHistory values from authentication data could cause an unintended denial of access. SIDHistory SIDs are removed because they do not appear to be from the trusted domain.
- SID Filtering can cause the SIDs for universal groups to be removed from authentication data. When the universal group was not created in the same domain as the user, its SID does not appear to be from the trusted domain.
- SID Filtering must only be enabled for trusts that span forest boundaries. An attempt to enable SID Filtering on domains within a forest will cause trust and replication failures.
- The term “quarantine” is sometimes used to describe SID Filtering and is an operand of the Domain Manager (netdom.exe) command line program used to configure SID Filtering.

The following AD security considerations apply to manual trust definitions:

- Establishing a trust relationship outside a forest makes one or both participants dependant on the security practices of the other. In simple terms for a forest trust, the trusting forest is relying on the identification and authentication practices in the trusted forest.

Therefore it is important that all the users in both forests who are members of the highly privileged groups (Domain Admins, Enterprise Admins, and Schema Admins) are considered to be highly trusted individuals by both organizations involved in the trust.

- Trusts may be configured through multiple tools. Two common tools are the AD Domains and Trusts MMC snap-in and the Domain Manager (netdom.exe) command line program.
- Whenever possible, one-way trusts should be chosen over two-way. In cases such as perimeter configurations with a separate forest, a one-way trust alone can be used to allow accounts from the protected-side forest to be trusted in the perimeter forest while preventing accounts in the perimeter forest from being trusted in the protected-side forest.

Because of the possible impact on Windows OS security, a brief note on trust configurations and some specific Group Policy settings is necessary. Some Windows NT components allowed and used anonymous access to retrieve Windows data for configuration and communication tasks. The operations involved in the establishment of a trust relationship are one example. The following table describes the registry entries and associated Group Policy settings that are related to this anonymous access.

OS	Registry Entry	Group Policy
Windows 2000 Server	RestrictAnonymous	Additional restrictions for anonymous connections
Windows Server 2003	RestrictAnonymous	Network access: Do not allow anonymous enumeration of SAM accounts
	RestrictAnonymousSam	Network access: Do not allow anonymous enumeration of SAM accounts and shares

Table 2-5. Anonymous Access Settings

Secure values for these entries are required by the *Windows 2003/XP/2000 Addendum*. However, it is acknowledged that using the most secure values causes trusts with Windows NT 4.0 domains to fail. For this reason, it is permissible to use the less secure values in those environments. However, once all the domains involved in trusts are at Windows 2000 and above, there is no longer a requirement for these values as far as trust support is concerned.

Please note that the reduced security OS settings for anonymous access may be required for other applications in an environment. It is important that those cases are properly documented so that this need for reduced security settings can eventually be resolved.

2.2.5 Group Policy

Group Policy is a Windows feature implemented through AD that has several functions. Very generally speaking, it provides a method to define Windows configurations and enforce those configurations for the computers and users within a Windows domain. Although explicit security settings are one prominent aspect of Group Policy, there are many others.

Group Policy implementation and use are very complex subjects. Microsoft has stated that the Group Policy implementation in Windows Server 2003 has almost 1,000 configurable settings. This statement reflects the fact that a few brief notes cannot adequately explain such a complex technology. The information here is intended only to identify the most significant elements of this technology as it relates to AD security. Readers are strongly encouraged to review the Microsoft documentation including the *Microsoft Windows Security Resource Kit* for information.

It is noted that the discussion here is addressed primarily at how Group Policy is applied through Windows domain controllers. The interaction with locally defined Group Policy is mentioned, but it is not the focus of this information.

The following subjects are discussed in this section:

- Physical components
- Default GPOs
- GPO application
- Group Policy Management Console (GPMC) and Group Policy Results Tool
- Auditing and backup.

Group Policy is stored logically in GPO objects in AD. From a physical viewpoint most policies have two data components. The Group Policy Container (GPC) is stored in the AD database. The Group Policy Template (GPT) is stored in the SYSVOL folder on Windows domain controllers. The Windows FRS replicates the GPTs in the SYSVOL folder among all domain controllers in a domain. Synchronization between the AD database and SYSVOL contents is a consideration for backup and restore operations.

When a Windows server is promoted to be a domain controller, two GPOs are automatically built. The Default Domain Policy GPO is the default policy linked to the domain; it is applied to users and computers throughout the domain. The Default Domain Controllers Policy GPO is the default policy linked to the Domain Controllers OU; it is applied to all domain controllers in the domain.

Implementing GPOs can be complex. In the simplest terms, there are two basic parts to the process: definition and linking. Definition is simply the creation of a GPO and setting its properties. Linking refers to the process of specifying the AD object to which a specific GPO is to be applied. A GPO has no effect until it is linked to an AD object.

GPOs can be linked at three levels of objects:

- GPOs linked to an AD site are applied to all users and computers at that site.
- GPOs linked to the domain are applied to all users and computers in that domain.
- GPOs linked to an OU are applied to all users and computers in that OU.

Two of these levels always apply to an individual user or computer. The user or computer always belongs to an AD site (even if it is just the default site). The user or computer always belongs to an AD domain. Users and computers should belong to an OU, and most GPOs are linked to OUs.

A single user or computer may be subject to multiple GPOs. In addition to this, it is important to understand that GPOs are applied in a specific sequence. This sequence is sometimes referred to as "LSDOU":

- Local - GPOs defined on the local computer
- Site - GPOs linked to the applicable AD site
- Domain - GPOs linked to the applicable domain
- OU - GPOs linked to all applicable OUs.

Within each of these categories, there may be multiple GPOs. The settings in the GPOs are aggregated to arrive at the final settings for the user or computer. The sequence in which they are applied within each category is determined by the link order that is configured. Also the concept of inheritance applies. Inheritance refers to the fact that polices applied to parent containers are also applied to the child containers. In practice this means that a policy applied to an OU also applies to all the OUs defined within that OU.

There are three GPO options that can be used to change normal GPO application behavior.

- Enforcement (No override) - This option specifies that a GPO takes precedence over any GPOs linked to child containers.
- Block inheritance - This option specifies that objects in child containers do not inherit GPOs from parent containers.
- Loopback processing - This option specifies that the computer GPOs should be applied when any user logs on to the computer. Loopback processing operates in merge mode or replace mode. In merge mode the user parts of the computer's GPO are applied along with the user's OU GPO. In replace mode the computer's GPO is applied instead of the user's GPO.

Filtering can also impact GPO application. Security filtering occurs when a GPO is linked to a computer or user, but the computer or user account does not have Read and Apply permissions for the GPO. An account must have these permissions in order for a GPO to be applied. In Windows Server 2003, Windows Management Interface (WMI) filtering was added. WMI filtering allows the characteristics of a computer to be checked to determine if a GPO should be applied. Criteria are specified through WMI Query Language (WQL) statements.

A final consideration for GPO application is the designation of a slow link. Because GPO application occurs each time a computer connects to a domain, when the user logs on to the domain, and periodically thereafter, the speed of the connection from the client to the domain controller could substantially impact performance. To account for this, the speed of the link from the domain controller to the client is evaluated. If that speed is below a configured threshold (default 500 kilobits per second (kbps)), the link is designated as a slow link and some GPOs are not applied. Those that are not applied include scripts, folder redirection, disk quotas, and application deployment. This behavior can be overridden through a Group Policy setting.

The following AD security considerations apply to the GPOs:

- Linking a GPO to an AD site is restricted to members of the Enterprise Admins group.
- Linking a GPO to a domain is restricted to members of the Domain Admins group.
- Linking a GPO to an OU can be delegated through permissions on the GPO.
- GPOs cannot be linked to the Users and Computers containers in AD. For this reason users and computers need to be moved into OUs.

Considering the impact of GPO inheritance and the support for delegation of GPO administration, it becomes apparent that intelligent OU design can be quite important. If OU design is carefully considered before domain implementation, it can save considerable time later.

There are multiple ways for an administrator to maintain and evaluate GPO application, but two tools deserve particular mention: the GPMC and the Group Policy Results tool.

The GPMC consists of an MMC snap-in and some scriptable interfaces for managing Group Policy. The GPMC can be used from Windows Server 2003 or Windows XP computers and it can be used to manage Group Policy on Windows 2000 Server computers as well as Windows Server 2003 computers. The GPMC package can perform editing, backup/restore, and import/export tasks. It provides the Group Policy Modeling interface, formerly known as Resultant Set of Policy (RSoP) planning mode, and the Group Policy Results interface, known formerly as RSoP logging mode. The GPMC is the recommended tool for integrated management of Group Policy.

The Group Policy Results Tool (gpresult.exe) is a command line tool that can be used to display the effective group policy for the current user and computer that results from the application of all GPOs at the local, site, domain, and OU levels. This can be an effective tool for diagnosing GPO application issues.

The final Group Policy subjects are auditing and backup. Auditing changes to GPOs can be done in much the same way as auditing changes to data files. Each GPO has audit settings that can be enabled. For high security environments such as the DOD, proper values for audit settings are required by policy, important for incident investigation, and necessary to ensure the capture of data required for prosecution of malicious behavior.

Backup of GPOs can be accomplished in multiple ways. The GPMC can be used to save GPOs for recovery and for distribution to other domains. GPO data is also backed up when the Windows System State data is backed up. This was briefly discussed in Section 2.2.2, Forest and Domain Architecture. In environments with active use of GPOs, the GPMC tool offers a more efficient approach to the task and could reduce recovery time.

2.2.6 Ports and Protocols

It is noted in the introduction to this document and in other locations that AD's operation as a directory service provides and consumes services that involve network traffic. Because of the close integration with Windows, it is difficult to identify those ports and services that are unique to the function of AD. The objective of this section is to identify the network services, standard ports, and the associated AD and Windows services that are needed for an AD environment.

AD is a network service provider in two respects:

- On each domain controller, AD responds to directory query and update traffic formatted in LDAP on IP port 389. When a properly configured PKI certificate is installed, AD supports encrypted sessions to respond to directory query and update traffic formatted in LDAPS on IP port 636.
- On domain controllers that are also Global Catalog servers, AD responds to directory query traffic formatted in LDAP on IP port 3268. When a properly configured PKI certificate is installed, AD supports encrypted sessions to respond to directory query traffic formatted in LDAPS on IP port 3269.

AD and the Windows services that AD depends on are network service consumers in several respects:

- Operations such as configuring access permissions can use an LDAP query to a domain controller on port 389 to enumerate user and group accounts.
- When a computer or user logs on to a domain controller, that domain controller contacts a Global Catalog server on IP port 3268 or 3269 to determine universal group membership.
- AD accesses DNS servers on IP port 53 for multiple purposes. Domain controllers update DNS service location records that are read by AD clients. Domain controllers query DNS servers to obtain the addresses of other Windows servers.
- AD uses ICMP ping packets between domain controllers and AD clients to evaluate link speed for GPO processing.
- The Windows FRS uses the Microsoft-DS service on IP port 445 for AD data replication and the RPC Endpoint Mapper service on IP port 135.
- The domain controller that holds the PDC Emulator FSMO role can provide a time synchronization service using NTP on IP port 123.
- The Windows Local Security Authority (LSA) works in conjunction with AD for authentication and authorization. It uses several IP ports. When Kerberos authentication and authorization are utilized, IP port 88 is used.

The following table lists the network services, ports, and related Windows services that are required for AD functions. Although all of these ports are not used with every domain controller and client, they would be used somewhere in a complete AD configuration.

Port	TCP\UDP	Service	Windows System Service
N/A	N/A	ICMP (ping)	Group Policy
53	TCP\UDP	DNS	DNS

Port	TCP\UDP	Service	Windows System Service
88	TCP\UDP	Kerberos	Key Distribution Center
123	UDP	NTP \ SNTP	Windows Time
135	TCP	RPC Endpoint Mapper	LSA, FRS, Group Policy
389	TCP\UDP	LDAP	LSA, Group Policy
445	TCP	Microsoft-DS / SMB	Group Policy
636	TCP\UDP	LDAPS	LSA
3268	TCP	MS Global Catalog	LSA
3269	TCP	MS Global Catalog SSL	LSA
1024-65536	TCP	RPC (dynamic)	LSA, FRS, Group Policy

Table 2-6. AD Port\Protocol Use

Please note that this information is subject to change as Microsoft's implementation changes. Although the data is presently consistent with the information in Microsoft Knowledge Base article 832017, users should check the Microsoft documentation before changing configurations based on this information.

It must also be noted that although almost all of these Windows services work only on the documented port numbers, some of these services can be configured to use different port numbers. By default the LSA and FRS Windows services support RPC network service calls on a dynamic port number above 1023. But it is possible to create Windows registry entries that override that behavior and specify explicit, fixed values.

- In key HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters, the "TCP/IP Port" value can be used to specify a port for AD replication traffic.
- In key HKLM\SYSTEM\CurrentControlSet\Services\NTFRS\Parameters, the "RPC TCP/IP Port Assignment" value can be used to specify a port for FRS traffic.

Refer to the Microsoft documentation for details. Please note that changes to these parameters must be done with extreme care and only in coordination with local network management personnel. Errors in registry settings or a firewall block of a specific port could result in the failure of services that support AD.

Directory synchronization tools that can be used with AD also rely on access to network services. These tools are very briefly described in Section 2.2.7, Synchronization Tools and Technology. The following table lists the network services, ports, and related tool or technology.

Port	TCP\UDP	Service	Tool\Technology
53	TCP\UDP	DNS	MIIS
80	TCP	HTTP	MIIS using DSfW
88	TCP\UDP	Kerberos	MIIS
135	TCP	RPC Endpoint Mapper	ADAM
389	TCP\UDP	LDAP	ADAM, SimpleSync, MIIS
443	TCP	HTTPS	MIIS using DSfW
464	UDP	Kerberos kpasswd	MIIS

Port	TCP\UDP	Service	Tool\Technology
636	TCP\UDP	LDAPS	ADAM, SimpleSync, MIIS

Table 2-7. Synchronization Port\Protocol Use

As with the information in the AD Port\Protocol Use table, users should check the Microsoft documentation before using this data.

Some of the network services in these lists have been associated with significant security vulnerabilities. In particular, some services associated with ports 135 and 445 are identified as high risk. For this reason, their use across certain network boundaries is restricted. DOD policy on this is described in *DOD Instruction 8551.1, Ports, Protocols, and Services Management (PPSM)* and the associated *Ports, Protocols, and Services (PPS) Assurance Category Assignments List*. The *PPS Assurance Category Assignments List* provides detailed guidance for specific services and port numbers. It is available to DOD and Government users through the IASE web site.

In order to support an AD environment that spans DOD enclave boundaries and is compliant with the DOD policy, the use of VPN technology is the only known acceptable solution. Please refer to the *Network Infrastructure STIG* and the *Enclave STIG* for information on VPN implementation.

2.2.7 Synchronization Tools and Technology

As in other large organizations, the implementation of AD within DOD has not been uniform. This is the predictable result of varying procurement cycles, budget challenges, and mission needs. Even when deployment follows similar timelines, isolated AD environments have been built to provide necessary security boundaries. This means generally that more AD forests exist than are required in a strictly technical sense. In research compiled by the DOD Active Directory Interoperability Working Group (DADIWG), there are indications that more than 1,500 AD forests exist today within DOD.

To be able to support DOD's net-centric strategy, it has become necessary to implement solutions that allow information in multiple AD forests to be shared and synchronized. Although some software is bundled with Windows to support this, the need for more robust solutions has resulted in the development of commercial-off-the-shelf (COTS) products by Microsoft and other companies. This section provides a very brief description of a few of the Windows components and COTS products that support synchronization of AD data.

Windows provides two tools that support the bulk import and export of AD data:

- The Comma Separated Value (CSV) Data Exchange (CSVDE) program provides import and export of AD data in comma-separated value format. CSVDE contacts the domain controller on IP port 389.
- The LDAP Data Interchange Format (LDIF) Data Exchange (LDIFDE) program provides import, export, and modification of AD data using LDIF files. LDIF is a file format

standard for directory service data. LDIFDE can contact the domain controller on IP port 389 or a Global Catalog server on IP port 3268.

The primary security issues with CSVDE and LDIFDE are protection of the data files. Whether in transit or in a file system, the data could contain sensitive information or the aggregate of the information could be sensitive.

CPS Systems sells the SimpleSync COTS product. SimpleSync performs directory synchronization operations between several different types of directory services including AD and other LDAP-based products. SimpleSync can communicate with domain controllers over LDAP on IP port 389 or LDAPS on IP port 636.

Microsoft sells the Microsoft Identity Integration Server (MIIS) as a COTS directory tool. Microsoft offers the Identity Integration Feature Pack (IIFP) as a downloadable feature for Windows Server 2003. IIFP supports a subset of the directory services supported by MIIS, but otherwise both components provide the same type of service. This service is able to gather and synchronize directory data from a number of sources including AD. MIIS stores its data in a Microsoft SQL Server database and allows complex manipulation of the directory information. MIIS is the successor to the Microsoft Metadirectory Services (MMS) product that was available for Windows 2000 Server.

Directory Services Markup Language (DSML) Services for Windows (DSfW) is a downloadable feature from Microsoft. DSfW enables access to AD by using Simple Object Access Protocol (SOAP) over Hypertext Transport Protocol (HTTP) or Hypertext Transfer Protocol over SSL (HTTPS). DSfW requires the use of a gateway program running under the Microsoft Internet Information Server (IIS) web server. The Directory Services Data Exchange (DSDE) program is available with DSfW to use as a client to access DSfW.

The final component to be described does not by itself provide directory synchronization services. Microsoft offers ADAM as a downloadable feature that can run on Windows Server 2003 or Windows XP. ADAM provides a generic, LDAP-accessible directory service that runs in a user context rather than a system context. Multiple instances of ADAM can run on a single host.

ADAM can be used as part of an AD synchronization solution. It can be deployed as a border directory between two organizations in the following manner. Using the MIIS product, one organization can extract directory data from their AD and populate an ADAM instance. The second organization can use MIIS to review or filter that ADAM data and import it into their AD. More complex scenarios are being examined and documented by the DADIWG.

The following characteristics of ADAM are relevant to security:

- The physical components of ADAM are similar to those of AD. There is a database and transaction log files.

- Although some common tools can be used, there are some unique administration tools for ADAM. This includes the ADAM ADSI Edit MMC snap-in (ADAM-adsiedit.msc) and the Dsdbutil, Dsdiag, and Dsmgmt programs.
- Running on Windows XP, ADAM does not support auditing.
- Users can be defined within ADAM; they are one type of ADAM security principal. Windows security principals can also be defined as ADAM security principals. Groups defined within ADAM can contain ADAM security principals and Windows security principals.

Without respect to the specific product or technology used, the following general security issues must be considered for directory synchronization tools and technology:

- Data files holding substantial aggregations of directory data can become sensitive. Examination of a sufficient aggregate might disclose force strength or content.
- The exchange of "contact object" data such as that used in Global Address List (GAL) synchronization does not normally represent sensitive traffic because that data is not used in identification, authentication, or authorization operations.
- Permitting anonymous access to directory data can only be considered acceptable if the confidentiality category of the associated system is public.
- Mutual authentication, that is authentication of the client by the server and the server by the client, is necessary to help deter a spoofing attack. Invalid directory data could result in the disclosure of sensitive data if that directory data is used in access control decisions.
- The use of query and update restrictions such as quotas can help to deter denial of service attacks.
- The vulnerability of certain network services must be taken into account when considering access to directory services in a network that spans enclave boundaries.
- Limiting write access to the directory through access permissions, quotas, or other update controls can help to prevent inadvertent or erroneous overwrite of directory data or flooding of the target directory.

2.3 Security Requirements

The AD software and associated data components comprise the core of authentication and authorization management that is performed in Windows 2000 and later domain configurations. It is therefore obvious that maintaining the confidentiality, integrity, and availability of Windows domains is directly dependant on the secure configuration and operation of AD components.

The threats to AD components have much in common with the threats to other software and data components. But because the data is replicated to an extent throughout an AD forest, the vulnerabilities can be more serious. Users may disrupt availability through malicious or simply unintended actions. When a user with administrative-level privileges initiates a harmful action, the consequences can range from a small-scale denial of service to the effective disruption of all the Windows servers and clients within a forest.

This section provides the specific security requirements that apply to the AD components in Windows 2000 Server and Windows Server 2003 and to products that may be used to manipulate AD data. This section is broken into subsections that align with the IA Controls subject areas

defined in DOD Instruction 8500.2, Information Assurance (IA) Implementation. These subject areas are as follows:

- Security Design and Configuration
- Identification and Authentication
- Enclave and Computing Environment
- Enclave Boundary Defense
- Physical and Environmental
- Continuity
- Vulnerability and Incident Management.

Some of these areas are further divided to provide a more cohesive presentation. The Personnel subject area is not included as there are no controls in that subject area that are addressed in an AD security review.

It is important to understand some of the terminology used in this section:

- AD database - AD data is stored primarily in a file named ntds.dit. This is not a database in the sense of a general-purpose data store, but it does provide the data repository for AD and so is referred to by the term AD database in this document.

- AD maintenance and synchronization products or solutions - There are products by Microsoft, other vendors, and in the public domain that read and update AD data. It is also possible that Components may write their own applications as part of local solutions to do this. These products and solutions can perform various functions from simple reporting to access control configuration and complex identity provisioning. While specific guidance for these products may be provided in future versions of this document, at present the requirements for these products refer to them as maintenance and synchronization products or solutions.

It is essential to note that the requirements stated in this document are intended for use in a specific context. That context is the high security (sometimes referred to as limited functionality) configuration required for DOD Automated Information System (AIS) components. Such a configuration is achieved by compliance with the other DOD information assurance guidance. This refers specifically to the *Windows 2003/XP/2000 Addendum*, the *Domain Name System STIG*, the *Enclave STIG*, and the *Network Infrastructure STIG*. Some AD maintenance or synchronization solutions utilize web servers and database management systems. In those cases, compliance with the *Database STIG* and the *Web Server STIG* is also assumed.

Finally, it should be noted that the requirements here are based on the versions of Microsoft Windows 2000 Server and Windows Server 2003 with the current service packs and security fixes at the time this document was written. Specifically, changes introduced with Windows Server 2003 Release 2 are not reflected. As with the implementation of all security configuration guidance, DOD Components should test configuration settings to ensure that their specific environment is not impacted in unintended ways.

2.3.1 Security Design and Configuration

This section describes AD security requirements based on applicable DODI 8500.2 IA Controls in the Security Design and Configuration subject area. These requirements address five general areas: product design characteristics, configuration and implementation integrity, network services, software integrity, and security service partitioning.

2.3.1.1 Product Design

Software must be properly designed and implemented to maintain the security of the data it manipulates. When the data is used in identification, authentication, or authorization services, the software is identified as an IA product. Once identified as such, the software must be formally evaluated to establish objectively that it meets certain design and implementation requirements that address potential vulnerabilities. The currently accepted evaluation criteria are specified in the Protection Profiles of the Common Criteria.

Windows 2000 Server has been evaluated and Windows Server 2003 is in evaluation for conformance at the Common Criteria Evaluation Assurance Level (EAL) 4 Augmented. These efforts meet the formal evaluation requirements for AD components of Windows as an IA product.

When maintenance and synchronization products update AD data that is used in identification, authentication, or authorization services, they function as IA products and must also be formally evaluated.

- *(DS05.0100: CAT III) The IAM will ensure the acquisition of AD synchronization and maintenance products that create or update security principal accounts meets the applicable Common Criteria, NIAP, or FIPS evaluation and validation requirements specified in NSTISSP No. 11 and DODI 8500.2.*

- *(DS05.0110: CAT III) The IAM will ensure AD synchronization and maintenance products that create or update security principal accounts from sensitive systems meet the medium robustness requirements defined in DODI 8500.2 when any of the following is true:*

  - *AD synchronization or maintenance data traverses public networks.*
  - *AD synchronization or maintenance data resides on systems that are accessible by individuals not authorized to access the information.*

It should be noted that when synchronization products are used to perform e-mail contact or GAL synchronization functions they are not normally identified as IA products. However, if the items synchronized are used by an AIS to perform identification, authentication, or authorization, the synchronization products are identified as IA products.

2.3.1.2 Configuration and Implementation Integrity

As noted in section 2.2.2, Forest and Domain Architecture, the AD schema includes the definitions of AD objects and their attributes. Modifications to the schema could render domain

controllers or applications inoperable. To help ensure that schema modifications are appropriately designed and implemented, they must be subject to a configuration management process.

- *(DS00.0100: CAT III) If the AD schema is altered by the addition, change, or deletion of objects, the IAM will ensure a documented configuration management (CM) process is used for the implementation of those added, changed, or deleted schema elements.*

It is important to note that certain product installation procedures might attempt to perform schema modifications without explicit notification. While the intent is not malicious, the impact could be negative in the short or long term if an object definition is altered and a conflict is created. SAs responsible for product installations are advised to carefully review product documentation for this issue.

An AD trust is a defined interconnection between two or more parties in different forests. While it does facilitate resource sharing, it must be thought of as potentially weakening the isolation provided by the forest architecture. It was noted in section 2.2.4, Trust Relationships, that external, forest, and realm AD trusts enable a user from a trusted domain or forest to access resources in the trusting domain or forest without requiring the re-authentication of that user. If a trust were defined improperly or between the wrong parties, it could allow access to resources that had weak access control permissions.

Simply looking at a trust definition is not sufficient to determine if the trust is intended and authorized. To do that it is necessary to maintain a baseline of information about authorized trusts. By comparing this baseline information to the AD trust definitions, improper trusts would be exposed.

- *(DS10.0100: CAT III) The IAO will ensure the following documentation is maintained for each external, forest, and realm AD trust defined on each forest or domain:*

  - *Trust type (external, forest, or realm)*
  - *Fully qualified domain names of each party*
  - *MAC and confidentiality (classification) levels of each party*
  - *Direction (one-way or two-way)*
  - *Transitivity*
  - *Status of selective authentication option and SID filtering (quarantine) option.*

Cryptographic algorithms support data encryption and signing functions. Windows and other products implement these algorithms internally and through standard protocols such as LDAPS to protect the confidentiality and integrity of AD data. Unfortunately some of the implementations include algorithm or key length selections that are too weak to be acceptable for use in DOD. If a weak algorithm were used, it might be possible for an attacker to access or intercept signed and encrypted AD data, decipher it, and replace it with modified data.

To protect against the use of weak algorithms, implementations that have been validated by the National Institute of Standards and Technology (NIST) are required. Existing requirements in the

Windows 2003/XP/2000 Addendum address the Windows AD components; synchronization and maintenance software must also be addressed.

- *(DS05.0120: CAT II) SAs will ensure AD synchronization and maintenance software is configured to use FIPS 140-2 approved encryption, key exchange, digital signature, and hash algorithms for all required data signing or encryption functions.*

2.3.1.3 Network Services

The nature of AD as a directory service means that AD data is transmitted across networks. In some cases AD forest implementations span DOD enclave boundaries and AD data is transmitted over wide area networks. There are two security considerations when DOD enclave boundaries are traversed: AD services and other colocated services.

It was noted in section 2.2.6, Ports and Protocols, that there are a number of ports and services used by AD and by synchronization and maintenance solutions for AD. These ports and services enable queries, updates, and data transfer that supports identification, authentication, and authorization as well as AD data replication between domain controllers. Enabling these ports in network infrastructure components such as firewalls and routers can make the AD services accessible to attack from hosts that have gained unauthorized access to the network.

Even when all AD services have been made as secure as possible, consideration must be given to the fact that networks are shared resources. Colocated hosts might include UNIX systems running directory server applications such as OpenLDAP or file servers using the Common Internet File System (CIFS) protocol on port 445. Because these other systems may have vulnerabilities that make them susceptible to attack, enabling ports on firewalls or routers to support AD could elevate the risk of compromise of other systems on the same network.

Both Windows domain controllers and other hosts using the same network protocols are protected through compliance with the guidance in *DODI 8551.1, Ports, Protocols, and Services Management (PPSM)*. Since network traffic for some of the services used by AD is not permitted across any of the network boundaries defined through DODI 8551.1, it is necessary to employ DOD-approved VPN technology to support AD. Although not required for every network environment, data encryption is likely to be a requirement that the selected VPN solution must provide. The *Network Infrastructure STIG* and the *Enclave STIG* provide reference information on PPS and VPN use.

- *(DS10.0110: CAT II) If the AD forest implementation spans DOD enclave boundaries, the IAM will ensure AD data is routed through a VPN or other network configuration that is compliant with the Network Infrastructure STIG and DOD Instruction 8551.1.*

- *(DS05.0130: CAT II) If an AD synchronization or maintenance solution involves the use of LDAP or HTTP across DOD enclave boundaries, the IAO will ensure AD synchronization and maintenance data is routed through a VPN or other network configuration that is compliant with the Network Infrastructure STIG and DOD Instruction 8551.1.*

- *(DS05.0140: CAT II) If an AD synchronization or maintenance solution involves the use of LDAPS or HTTPS across DOD enclave boundaries, the IAO will ensure AD synchronization and maintenance data is routed through a solution that is compliant with the restrictions specified under DOD Instruction 8551.1, such as a DMZ configuration and traffic filtering or a VPN solution compliant with the Network Infrastructure STIG.*

NOTE: When AD implementations employ potentially vulnerable protocols across DOD enclave boundaries, it is especially important to comply with the registration requirements specified under DODI 8551.1. This helps to ensure that DOD network configuration changes do not inadvertently result in a loss of connectivity.

2.3.1.4 Software Integrity

Preserving the integrity of AD data is linked to preserving the integrity of the software that manipulates that data and the AD environment. Although there are many programs involved with AD, special focus is needed on the interfaces that allow user manipulation. While these programs may include a check to verify that the calling user has administrator-level privileges, some programs may not and others could have flaws that allow such a check to be bypassed. Because of this it is necessary to focus on the access controls for this software.

Windows server software comes with several command-line and GUI programs that can display, add, modify, and delete AD data as well as configure the AD environment. Some of these programs are:

- Multi-purpose - The AD Installation Wizard (dcpromo.exe), NTDS Utility (ntsdutil.exe), and Group Policy Restore Utility (dcgpofix.exe) programs perform various functions.
- Import and export - The CSVDE (csvde.exe) and LDIFDE (ldifde.exe) programs can import to and export from the AD database.
- MMC snap-ins - Various administrative functions are scattered across the AD Users and Computers (dsa.msc), AD Domains and Trusts (domain.msc), AD Sites and Services (dssite.msc), AD Schema (schmmgmt.msc), Group Policy (gpedit.msc), Domain Controller Security Policy (dcpol.msc), and Domain Security Policy (dompol.msc) interfaces.
- Windows Server 2003 additions - The directory service add (dsadd.exe), display (dsget.exe), modify (dsmod.exe), move (dsmove.exe), query (dsquery.exe), and remove (dsrm.exe) programs were added in Windows Server 2003 to provide additional command-line AD data manipulation tools.

These programs are considered sensitive because they support administrative updates to AD or they support the extraction of various scopes of information from the AD database. If an unauthorized user is allowed to access these programs that is one step in allowing that user to compromise the confidentiality, integrity, or availability of the AD environment or data.

Existing requirements in the *Windows 2003/XP/2000 Addendum* address access control for the programs installed by default with the server software.

Microsoft also makes programs available on the Windows server CD and through download from their web site that can manipulate AD data and the environment. Some of these programs are:

- The Domain Controller Diagnostic tool (dcdiag.exe) analyzes the Windows environment for issues that affect AD.
- The Directory Service Access Control List tool (dsacls.exe) allows display and modification of AD object permissions.
- The LDAP utility (ldp.exe) is a general tool to display and modify AD data.
- The Domain Manager tool (netdom.exe) performs a variety of functions including creation of trusts and management of domain computer accounts.
- The Domain Secure Channel utility (nltest.exe) can be used to display and test AD trust relationships.
- The Replication Administration (repadmin.exe) and Replication Monitor (replmon.exe) tools display and modify AD replication functions.
- The ADSI Edit MMC snap-in (adsiedit.msc) allows detailed display and modification of AD database objects.

These additional tools are installed as Support Tools in Windows. As with the Microsoft programs identified earlier, these tools allow administrative updates to AD or they allow various scopes of information to be extracted from the AD database. If an unauthorized user is allowed to access these programs that is one step in allowing that user to compromise the confidentiality, integrity, or availability of the AD environment or data.

The default installation of these programs does not provide adequate access control, so explicit specifications are included here.

Object	Name	Type	Access
…\%ProgramFiles%\ Support Tools\	Administrators SYSTEM [Other IAO-authorized groups]	Allow Allow Allow	Full Control Full Control Read, Execute With propagation

Table 2-8. Support Tools Access Permissions

- *(DS10.0120: CAT II) The SA will ensure access permissions are configured to restrict access to authorized accounts for the Windows server Support Tools.*

Beyond the software that is bundled with the Windows server versions, there are additional Microsoft and third-party synchronization or maintenance products that manipulate the AD environment and data. Unauthorized access to these programs might allow that user to compromise the confidentiality, integrity, or availability of the AD environment or data.

- *(DS05.0150: CAT II) The SA will ensure access to AD synchronization or maintenance software libraries (including executable and configuration files) is limited so that:*

  - *Only authorized application processes or SAs that require it have update access*
  - *Only authorized application processes, SAs, or other users that require it and are within applicable license agreements have read and execute access.*

Virtually all commercial software requires maintenance to correct vulnerabilities. When a malicious user takes advantage of a vulnerability that is not patched or is never discovered by the vendor, the operating environment and data may be seriously compromised. Because software that is not supported by the vendor could have un-patched or unknown vulnerabilities, it is DOD policy that unsupported software cannot be used.

- *(DS05.0160: CAT I) The IAO will ensure AD synchronization or maintenance software is removed or upgraded prior to the vendor dropping support.*

- *(DS05.0170: CAT II) The IAO will ensure the site has a formal migration plan for removing or upgrading AD synchronization or maintenance software prior to the date the vendor drops security patch support.*

AD Synchronization or maintenance software that is used as part of routine operations is assumed to be providing a function necessary to accomplishing a Component's mission. Unauthorized or improper changes to this software could result in a loss of function. The lack of a documented baseline of the software could be an impediment to recovery in the event of an incident. These risks are addressed by including the AD Synchronization or maintenance software in a configuration management process.

- *(DS05.0180: CAT III) The IAO will ensure AD synchronization or maintenance software that is used to support routine, scheduled DOD operations is included in the baseline inventory maintained by the Configuration Control Board and as part of the Certification & Accreditation documentation, and that a copy of the inventory is stored in a fire-rated container or otherwise not collocated with the original.*

Public domain software that manipulates AD data is currently available through the Internet. The installation or use of this software represents a risk to information systems because the Government does not have access to the original source code to review, extend, or repair it when needed. The software could contain incorrect or intentionally malicious code that would impact the confidentiality, integrity, and availability of the AD environment or data.

- *(DS05.0190: CAT II) The IAM will ensure binary or machine executable public domain software and other software with limited or no warranty (such as those known as freeware or shareware) is not used to fulfill an AD synchronization or maintenance function unless the following conditions are met:*

  - *The software is necessary for mission accomplishment and there are no alternative IT solutions available.*

- *The software is assessed for information assurance impacts and approved for use by the DAA.*

While open source software is not subject to this specific restriction, other requirements are mandated. It is permissible to use open source software as long as it conforms to the same DOD policies that govern COTS and GOTS software. This includes those requirements relating to IA and IA-enabled components. Specific guidance is found in the DOD Memorandum, *Open Source Software (OSS) in the DOD.*

2.3.1.5 Security Service Partitioning

Windows domain controllers perform system access and resource authorization checks. In this context these servers function as integral parts of the security support structure. When these servers are also used as file servers or to run applications, their attack surface is significantly enlarged by the presence of additional programs, data, and accounts. Therefore, the security of domain controllers is weakened when they are assigned other functions.

It is recognized that the combination of a domain controller with a file server represents less risk than other combinations. In fact, access to AD Group Policy Templates and scripts requires user and computer access to shared files on the domain controller. However, steps to partition AD data from user and application code allow more precise access controls to be defined for both.

- *(DS10.0130: CAT II) If the domain controller functions as a file server, the SA will ensure the AD database, log files, and SYSVOL (GPT) directory do not reside on the same logical partition as directories and files owned by users.*

- *(DS05.0200: CAT III) The SA will ensure source code for an AD synchronization or maintenance application does not reside in the same directory as the data input or output to that application.*

The combination of a domain controller with applications host represents a risk that has been determined to be unacceptable for most environments. The following issues contribute to this determination:

- Application servers such as web or database servers typically require a significant increase in the number of installed programs, the number of active processes, and the number of privileged users defined. Any of these elements may include vulnerabilities exploited in an attack on the domain controller.
- Some applications require the use of accounts that are members of the Administrators group. When this is permitted on a domain controller, those accounts are effectively domain administrators with the potential for significant access to resources throughout the domain.
- Some applications require the use of network services on ports that conflict with those used by AD components. The most common examples of this are MS Exchange and ADAM. In these cases, non-standard port numbers are typically used to circumvent this

issue. When this is done, traffic to the non-standard ports may not be correctly identified and processed by the host and network intrusion detection systems.
- The compromise of administrative accounts, particularly on a root domain controller, could lead to a loss of access control over an entire AD forest.
- The use of an e-mail client application to read mail may provide a simple means by which a privileged user unintentionally introduces malicious code.

To address these issues, the use of applications on domain controllers is restricted.

- *(DS10.0140: CAT III) The IAO will ensure Windows domain controllers are not utilized as hosts for applications including database servers, e-mail servers or clients, network address assignment (DHCP) servers, or web servers.*

It should be noted that this restriction does not apply to DNS servers. As noted in the *DNS STIG*, the secure implementation of the Microsoft Windows DNS server requires integration with AD.

2.3.2 Identification and Authentication

This section describes AD security requirements based on applicable DODI 8500.2 IA Controls in the Identification and Authentication subject area. These requirements address items that are used to identify and authenticate a user.

SAs may choose to automate AD maintenance or synchronization operations by using scripts that execute under a Windows account with appropriate access privileges. If the target of the operation is AD data used in identification, authentication, or authorization services, a compromise of the account could lead to the disclosure, modification, or destruction of sensitive AD data. Even if the data is not used in one of these sensitive services, the compromise of the account could lead to the unauthorized disclosure of AD data.

To protect accounts used in scripts from compromise, passwords cannot be embedded in those scripts. If it is necessary to store the password for use by an automated process, the file containing the password must be encrypted.

- *(DS05.0210: CAT I) The IAO will ensure passwords are not embedded in scripts used with AD synchronization or maintenance solutions and that stored passwords are encrypted.*

As an alternative to scripts that require account passwords, SAs should investigate whether the script could be converted to run as a Windows service. This would allow the password to be stored securely by Windows rather than in an external file.

The DSRM system state used for AD restore operations was mentioned in Section 2.2.2, Forest and Domain Architecture. When a Windows server is promoted to be a domain controller, a password must be selected for use when that domain controller is booted into DSRM. In DSRM, the user at the server console has the ability to manipulate the AD database file without the software-enforced protections of the normal domain security environment. If a malicious user gained physical access to a domain controller and obtained this password, he would be able to

capture, modify, or delete the AD database. Depending on the AD object, malicious modifications might later be propagated throughout the forest by normal AD replication.

To strengthen control of access to DSRM, password complexity requirements must be followed.

- *(DS10.0150: CAT II) The IAO will ensure the password defined for use in DSRM is at least eight (8) characters and is composed of at least one of each of the four character types: upper case, lower-case, numeric, and special characters.*

The password that controls DSRM access resides in the SAM file on the domain controller. When the domain controller is running in the normal Active Directory mode, the SAM file is not accessible to the standard tools that check for the presence and age of passwords.

DODI 8500.2 requires password expiration. In the case of the DSRM-related password, periodic changes enhance security by ensuring that a password is defined, the correct value is authoritatively known, and a potentially compromised password is replaced. Because access to the password is very limited, the yearly expiration period specified in the *Windows 2003/XP/2000 Addendum* for application accounts is appropriate.

- *(DS10.0151: CAT II) The IAM will ensure that there is a local policy in place that requires the password defined for use in DSRM to be changed on a yearly basis.*

There are two methods available to change this password. The first requires a service outage for the domain controller. The server is booted into DSRM, a "net user" command or Local Users and Groups MMC snap-in is invoked to change the password, and the server is booted again to return to AD mode. The second method can be done without a service interruption. In Windows 2000 Server, the setpwd utility can be used. In Windows Server 2003, the "set dsrm password" subcommand of the NTDS Utility (ntsdutil.exe) can be used. Please refer to the Microsoft documentation for specific command information.

A requirement to restrict physical access to the DSRM password is stated in Section 2.3.6, Continuity.

The use of digital certificates can strengthen the identification and authentication process when compared to the use of passwords. However, the use of self-signed certificates and certificates from unauthorized certificate authorities must be avoided. If such certificates are used, it may create a false sense of security, be the source of interoperability issues, or permit circumstances in which unauthorized users gain access to AD data.

- *(DS05.0220: CAT II) The IAO will ensure PKI certificates used in sessions between AD servers and maintenance or synchronization clients are issued by the DOD PKI or DOD-approved external PKIs.*

It is noted that certain Components have been granted a waiver by their CIO that allows the use of non-DOD PKI certificates that are generated under a Component-wide certificate authority.

The use of these certificates, although not optimal from a DOD interoperability perspective, is not considered a deviation from this requirement.

2.3.3 Enclave and Computing Environment

This section describes AD security requirements based on applicable DODI 8500.2 IA Controls in the Enclave and Computing Environment subject area. These requirements address eight areas: specific content, architecture and trusts, data access control for files, data access control for objects, data change auditing, group membership and privilege control, functional configuration, and data transmission confidentiality and integrity.

2.3.3.1 Specific Content

The content of specific AD items is generally more an issue of standards than security. But the content of one category of AD attribute is currently designated for a security function within DOD. This function is known generically as the affiliation display.

As with most large enterprises, communication among the DOD Components relies heavily on the use of e-mail. All manner of issues are communicated, discussed, and resolved through messages distributed by e-mail systems. The authors of these messages include military officers, civilian employees, and contractors; and there may be foreign nationals among those groups. Affiliation refers to an individual's status as a contractor or foreign national.

Certain types of communications are more appropriate or have different authority based on the affiliation of the individual. Consequently it is sometimes significant to know if a particular sender or recipient has a certain affiliation. If an individual is not accurately identified, that person might receive or be excluded from receiving information that is essential to mission accomplishment.
The default AD schema defines attributes for the Contact, inetOrgPerson, and User objects that can be populated with an individual's e-mail addresses. Extensions to the schema may add additional attributes. When these attributes are populated, their values must address the affiliation display requirement.

- *(DS00.0110: CAT III) The IAO will ensure AD attributes used in e-mail addresses and e-mail display names include the abbreviation "ctr" for all contractors and the appropriate country code for all foreign nationals.*

DOD policy that specifies the naming convention and acceptable values for some AD User object attributes is detailed in the *Active Directory User Object Attributes Specification*. Although the focus of that document is standards and not security, it impacts the implementation of AD and must be used in conjunction with the requirements in this document.

2.3.3.2 Architecture and Trusts

The way in which AD is implemented in terms of domain and forest architecture has an enormous impact to Windows security. The type and characteristics of manually defined AD

trusts also has a very significant impact. The resulting AD environment profoundly affects account and resource definitions, user authentication, and resource access control.

This section discusses security requirements and considerations for AD architecture and trusts. Please reference the information in section 2.2.2, Forest and Domain Architecture, and section 2.2.4, Trust Relationships, for a brief technology background on these subjects.

The large number of individual needs and environmental constraints within an organization the size of DOD makes it impossible in a practical sense to define a comprehensive list of strict AD architecture security requirements. A configuration that provides an appropriate level of security in one instance could be unreasonably weak in another. As a result, most of the guidance here is written as recommendations that the Components need to interpret for their particular environment.

The following guidance should be applied when determining when to implement unique forests or domains:

- The IAO should ensure that separate AD forests are implemented when there is a need for one group of users and resources to be isolated from another. Isolation refers to two considerations: trusts and administration. Whereas domains in a single forest are automatically connected by transitive, two-way trusts, there are no default trust relationships between forests. The second issue is that administrators of one forest are not able to change the security configuration of the users and resources in another forest.

  One example in which separate forests are recommended is a perimeter configuration such as a DMZ. If external users accessing DMZ resources have no requirement to access resources on the internal side of the DMZ, a separate forest for the DMZ should be considered.

- The IAO should ensure that separate AD domains are implemented when there is a need for one group of users to work autonomously from another. Autonomy also has trust and administration considerations. Because domains in a forest are automatically connected by transitive, two-way trusts, users can be granted access to resources in other domains without the need for additional user accounts. From the administration perspective, domain administrators can perform all configuration tasks for the domain, but some administrators of the root domain still have the ability to change the security configuration of the users and resources in a child domain.

- The IAO should consider the use of an empty root domain when the number of domains in the forest is large and specific requirements dictate the need for individual domain administration.

  In this case stronger security policies (such as requirements for longer passwords) can be implemented to protect the more sensitive forest-wide roles used in the root domain. Fewer users can be defined in the root domain, thus reducing the attack surface of that domain. And forest root domain controllers can be dedicated to their AD functions.

- The IAO should ensure that a separate AD domain is implemented for a software development project when the activities of that project have a high potential to impact a production environment.

It must be acknowledged that AD implementations consisting of the fewest forests and domains generally provide ease of administration, less complexity, and lower cost. However, it must also be understood that fewer security barriers accompany those benefits. Such barriers might deter or prevent a successful attack by an insider or an intruder who compromises a domain account.

One measure that can be taken to improve the implemented AD architecture is the exclusion of Windows NT servers as domain controllers. Windows NT does not support the same level of security that can be achieved with Windows 2000 Server or Windows Server 2003. Also, because Windows NT is no longer supported, there may be un-patched vulnerabilities that increase the risk of successful attack. Finally, when a Windows NT server is a domain controller, it forces Windows 2000 Server or Windows Server 2003 servers in the same domain to be configured less securely in order to support interoperability.

It must be noted that the *Windows 2003/XP/2000 Addendum* designates the use of Windows NT Server, as a domain controller or for any other purpose, to be a severity category I finding. This reflects the fact that Microsoft no longer provides support or patches for Windows NT Server.

In the past operational requirements may have precluded a migration from Windows NT. However, in many cases Windows NT is no longer used as a domain controller. In these environments, preventing the addition of new Windows NT domain controllers does enhance security. This can be accomplished by setting the domain functional level to a value that does not allow Windows NT.

- *(DS10.0160: CAT III) In AD domains that have no Windows NT domain controllers, the IAO will ensure the domain functional level is Windows 2000 native or Windows Server 2003.*

As with AD architecture, it is impossible in a practical sense to define a comprehensive list of strict AD trust security requirements for all DOD environments. Following are a few requirements than can be followed and some recommendations to develop a more secure environment.

As noted in section 2.2.4, Trust Relationships, AD trusts are defined automatically between domains in a forest and can be defined manually between forests and between domains in different forests. If a trust is defined between two domains and the permissions for a file in the trusting domain do not sufficiently restrict access, the contents of the file could be disclosed or modified by an unauthorized user in the trusted domain. Because trusts eliminate a level of authentication, it is very important that they are defined only when needed.

- *(DS10.0170: CAT II) The IAO will ensure external, forest, and realm AD trusts are defined only as required to support authorized access.*

Configuring an AD trust between systems that are at different DOD classification levels could substantially increase risk. Such a configuration would require the use of a controlled interface and it has not been determined that such a configuration for AD trusts could be adequately secured. Depending on the direction of the trust, data at one classification might be made available to a user in a lower classification level.

- A trust could allow a user in the trusted domain at a lower classification level to read data in the trusting domain at a higher classification level.
- A trust could allow a user in a trusted domain at a higher classification level to copy data to the trusting domain at a lower classification level.

- *(DS10.0180: CAT I) The IAO will ensure external, forest, and realm AD trusts are not configured between systems at different classification levels.*

Configuring an AD trust between a DOD system and a non-DOD system could also substantially increase risk. A compromise in the non-DOD forest or domain could lead to a compromise of the DOD forest or domain. However, there may be cases in which information sharing requirements between DOD and non-DOD Government agencies, coalition partners, or contractors justify such a configuration. In order to ensure that the risks of this configuration are properly recognized and mitigating actions for the network connections are taken, there are multiple conditions for this configuration.

- *(DS10.0181: CAT I) The IAO will ensure external, forest, and realm AD trusts are not configured between DOD and non-DOD systems unless:*

  - *The network connections comply with all requirements for external connections defined in the Network Infrastructure STIG, including a Memorandum of Agreement (MOA) between the two parties*
  - *Explicit approval of the trust by the DAA is documented.*

It was noted in section 2.2.4.2, Manually Defined Trusts, that the function that enables the SID History feature in Windows could be a vulnerability leading to an elevation of privilege attack. If a user in a trusted domain were able to forge credentials passed to a trusting domain, that user might gain unauthorized, privileged access to the resources in the trusting domain. In order to help prevent the use of forged credentials over trusts, the SID filtering option must be enabled.

- *(DS10.0190: CAT II) The IAO will ensure SID filtering is enabled on all external and forest trusts.*

NOTE: Implementation of this requirement could have a significant impact. Although SID filtering is the default for trusts created under Windows 2000 Server with SP4 (and later) and Windows Server 2003, the setting can be altered. Without proper review and update of resource permissions, implementation of the requirement could result in denied access to authorized users.

It should be noted that enabling SID filtering could have an impact on the use of Universal groups. A user in a trusted domain who was a member of Universal group in a different domain, would not be able to access resources in the trusting domain that were secured by access permissions using the Universal group. In this case a new group should be created in the trusted domain and the access permissions of the resource in the trusting domain should be updated.

Although the use of SID History is convenient, it should generally be used as a short-term measure during user migrations between domains. Removing SID History values that are no longer used enhances inter-domain security.

- The SA should periodically (at least semiannually) review the AD database and clear sIDHistory attribute values that are no longer needed.

With the addition of forest trusts in Windows Server 2003, it is possible to simplify trust configurations. A single forest trust could replace a large number of individual external trusts. However, because a forest trust may be effective over a much wider scope, an additional access control is needed to maintain a high security environment. The Selective Authentication trust option and the Allowed to Authenticate permission provide and enable this control. If these items are not configured, a user in a trusted forest might be able to gain unauthorized access to a resource with weak access permissions in the trusting forest.

When the Selective Authentication option is set on a forest trust, the Allowed to Authenticate permission must be configured on the resource server. The computer in the trusting forest in which the resource is located must have the Allowed to Authenticate permission granted to the user or group in the trusted forest that wants to access the resource. In this way access through a forest trust is granted only to the users specifically authorized by the administrator of the server in the trusting forest.

- *(DS10.0200: CAT II) The IAO will ensure the Selective Authentication option is enabled on all forest trusts.*

NOTE: Implementation of this requirement could have a significant impact. Without proper review and update of the Allowed to Authenticate permission, implementation of the requirement could result in denied access to authorized users.

The following additional guidance should be applied when determining how to implement AD trusts.

- The IAO should ensure that whenever possible one-way trusts are defined instead of two-way trusts or trusts in both directions.

  A domain in a perimeter configuration defined as a separate forest could be a good candidate for a one-way trust. In this case the trust would be defined with an internal domain as the trusted domain and the perimeter domain as the trusting domain. This would allow users authenticated on the internal domain to update resources in the perimeter domain without separate credentials or re-authentication.

- When there is a need for a large majority of domains in one forest to trust the domains in another forest and the risk has been determined to be acceptable, the IAO should ensure that a forest trust is defined instead of multiple external trusts.

- The IAO should ensure that shortcut trusts are defined to improve intra-forest trust processing and avoid availability problems that could be caused by network outages along the trust path.

2.3.3.3 Data Access Control - Files

Access to AD data is controlled at two levels. The first of these is the file system object level. This refers simply to AD directories and files on NTFS-formatted volumes. The usual access permissions for files can be applied. The second level of AD data access control is the AD object level. Within the AD database, AD objects have permissions similar to the file access permissions. To preserve the confidentiality, integrity, and availability of AD data, both the file and AD object access permissions must be properly configured.

AD data files include the AD database, log files, work files, and the GPT directory (SYSVOL). FRS, a Windows component critical to supporting AD replication, stores data in a database and log files. If these elements are located in the default locations and the guidance in the *Windows 2003/XP/2000 Addendum* is followed, inherited permissions would provide adequate access control. But because this data can be moved elsewhere and it is critical in order for AD to function, explicit specifications are included here.

Please note that the permissions for the database, log, and work files differ between Windows 2000 Server and Windows Server 2003. The permissions for the account names with an asterisk in the following table are only required for Windows Server 2003.

Component	Object	Name	Type	Access
Database	…\ntds.dit	Administrators SYSTEM CREATOR OWNER* Local Service*	Allow Allow Allow	Full Control Full Control [None on file] Create Folders / Append Data
Log files and log reserve files	…\edb*.log, …\res1.log …\res2.log	Administrators SYSTEM CREATOR OWNER* Local Service*	Allow Allow Allow	Full Control Full Control [None on file] Create Folders / Append Data
Work files	…\temp.edb …\edb.chk	Administrators SYSTEM CREATOR OWNER* Local Service*	Allow Allow Allow	Full Control Full Control [None on file] Create Folders / Append Data

Component	Object	Name	Type	Access
GPT parent directory	…\SYSVOL	Administrators Authenticated Users CREATOR OWNER Server Operators SYSTEM	Allow Allow [None on dir.] Allow Allow	Full Control Read, Read & Execute, List Folder Contents [None on dir.] Read, Read & Execute, List Folder Contents Full Control
GPT policies directory	…\SYSVOL\ *domain*\Policies	Administrators Authenticated Users CREATOR OWNER Group Policy Creator Owners Server Operators SYSTEM	Allow Allow [None on dir.] Allow Allow Allow	Full Control Read, Read & Execute, List Folder Contents [None on dir.] Read, Read & Execute, List Folder Contents, Modify, Write Read, Read & Execute, List Folder Contents Full Control
FRS directory	…\Ntfrs	Administrators SYSTEM	Allow Allow	Full Control Full Control

Table 2-9. AD Data Access Permissions

It should be noted that the full path to these files has to be determined from the Windows registry entries for AD. This is due to the fact that other products utilizing Microsoft's Extensible Storage Engine create files with some of the same names.

If improper access permissions are defined for these files, unauthorized users might be able to read, modify, or delete AD data. Because this data includes identification, authentication, and authorization data, a compromise could have grave consequences to an entire domain or forest.

- *(DS00.0120: CAT I) The SA will ensure access permissions are configured to restrict access to authorized accounts for the AD database file, log files, work files, GPT (SYSVOL) directories, and FRS directory.*

Data used in AD maintenance and synchronization operations has to be considered input to and output from the AD database. In this context, a compromise to the confidentiality and integrity of AD maintenance and synchronization files could eventually impact AD domain functions or other operations that use the data.

Identification of AD maintenance and synchronization data depends on the product and technology being used. Some examples are:

- The Microsoft ADAM feature utilizes a file structure similar to AD. This includes an ADAM database (adamntds.dit) and log files (edb*.log) for each instance on a server.
- The CSVDE and LDIFDE programs can read import files and write export files.

If weak access permissions are defined for these files, unauthorized users might be able to read, modify, or delete directory data. When this data includes identification, authentication, and authorization data and that data is used to update an AD database, a compromise could have grave consequences to an entire domain or forest.

- *(DS05.0230: CAT I) The SA will ensure access permissions for AD maintenance or synchronization data files are configured so that:*

  - *Update access is restricted to SYSTEM, Administrators, and authorized application processes.*
  - *Read access is restricted to SYSTEM, Administrators, authorized application processes, and other IAO-approved users.*

A final issue for data access control for files is related to aggregates of AD data. Aggregates of data outside the AD database are typically the output from or input to maintenance and synchronization operations. While some aggregates reflect insignificant data, others could effectively disclose sensitive Component force or configuration data.

If an unauthorized user gains access to a substantial aggregate of AD data contained in maintenance or synchronization files, that data could be used in an attack or to select valuable targets to attack. While access permissions for maintenance or synchronization files are required, the added value of the aggregate deserves the additional protection provided by data encryption.

- *(DS05.0240: CAT II) The IAO will ensure when AD maintenance or synchronization files include a substantial aggregate of the directory data for an entire geographic command, the data are stored in files encrypted using FIPS 140-2-validated cryptographic algorithms.*

2.3.3.4 Data Access Control - AD Objects

In a manner very similar to file system objects, AD database objects are assigned access permissions. ACLs for AD database objects are initially created from the default security descriptor for the object type in the AD schema.

Although the access permissions for all AD objects are important, there are two types that require more vigilant review because they are likely to be altered during normal administrative activities. These types are GPOs and OUs. The following table lists the acceptable access permissions for these objects.

Object	Name	Type	Access
[*Group Policy* - e.g., Default Domain]	Administrators Creator Owner SYSTEM	Allow Allow Allow	Full Control Full Control Full Control
	Authenticated Users [or other user groups]	Allow	Read Apply Group Policy
[*Organizational Unit* - e.g., Domain Controllers]	Administrators Creator Owner SYSTEM	Allow Allow Allow	Full Control Full Control Full Control
	Authenticated Users [or other user groups]	Allow	Read

Table 2-10. AD Database Object Access Permissions

Please note that different permissions may be required and are acceptable when documented by the IAO:

- It is anticipated that the Apply Group Policy permission could be set to Deny in some cases as part of the exclusion of a specific group policy using security filtering.
- When OU administration is delegated, permissions beyond Read may be allowed to groups authorized to administer those OUs.

If improper access permissions are defined for AD objects, those objects might be modified, enabling vulnerabilities that lead to immediate unauthorized access or complete disruption of a system. This makes it imperative to properly configure AD object permissions.

- *(DS00.0130: CAT I) The SA will ensure access permissions are configured to restrict access to authorized accounts for AD database objects including Group Policy Objects and Organizational Units.*

As ongoing research is completed, it is expected that guidance for access permissions for other AD objects will be provided in future versions of this document.

As a mechanism to enable bulk access to AD objects, the “Synchronize directory service data” user right was defined for Windows domain controllers. An account granted this right is allowed to read all AD objects and properties, bypassing the access control permissions defined for them.

The high-level privilege associated with this right is too powerful for any normal environment. If an unauthorized user has access to an account with this right, the confidentiality of all data stored in the AD database is compromised. Since Windows processes that need this level of access execute under the SYSTEM account, all AD objects are defined with permissions that allow access by SYSTEM, and granular access permissions can be defined for individual objects, there is no known need to grant the Synchronize directory service data user right.

- *(DS10.0210: CAT I) The IAO will ensure no accounts are granted the Synchronize directory service data user right.*

The nature of directory data is such that read access to it is generally required for a large number of users. Functions such as assigning discretionary file access to specific users or groups and accessing printers require that a user be able to enumerate AD object data. Technically this process could execute under authenticated user credentials or a null (anonymous) connection.

AD was written initially to allow anonymous access to object data. This is to some extent consistent with the IETF LDAP standards. While this is appropriate for some environments, it is almost never appropriate to allow anonymous access in DOD environments. Unfortunately some early Windows programs, most notably some functions implemented in Windows NT, were written to access AD object data through anonymous connections. Consequently when this access is disabled in AD, certain Windows NT functions no longer work.

Since access to AD objects is controlled through ACLs, anonymous access can be enabled by defining object ACLs with groups that contain anonymous users. This was implemented through a built-in Windows group named "Pre-Windows 2000 Compatible Access". If the Everyone group is nested in the Pre-Windows 2000 Compatible Access group and anonymous users are part of the Everyone group, anonymous access to AD data is permitted.

In Windows Server 2003 an additional control over anonymous access was implemented. This control is through the dsHeuristics attribute of the Directory Service object. The default setting of this attribute specifies that only authenticated users may initiate an LDAP request. Because the Directory Service object is in the Configuration partition of the AD database, and that partition is replicated forest-wide, the setting of the dsHeuristics attribute is effective for all Windows Server 2003 domain controllers in a forest.

In environments using current Windows software, there should be no need to allow anonymous access to AD data. If an unauthorized user gains anonymous access, that data could be useful in subsequent attacks on the forest or domain. While some of the data would be insignificant, there are elements such as user and group names that are very significant for devising an attack and selecting a target. For this reason, settings must be configured to prevent anonymous access.

- *(DS10.0220: CAT II) The IAO will ensure the Pre-Windows 2000 Compatible Access group does not contain the Everyone or Anonymous Logon groups.*

- *(DS10.0230: CAT II) The SA will ensure the dsHeuristics attribute is configured to prevent anonymous access.*

NOTE: Configuration of the dsHeuristics attribute to disable anonymous access is effective only on domain controllers running Windows Server 2003.

NOTE: Implementation of these requirements could have a significant impact. In domains including Windows NT hosts, implementation of the requirement could result in denied access to authorized users and processes running on Windows NT hosts.

Beyond the specific requirement for the Everyone group, the following recommendation applies:

- The IAO should restrict the membership of the Pre-Windows 2000 Compatible Access group to few or no members.

2.3.3.5 Data Change Auditing

In the event of a system compromise, the existence of appropriate audit data can be critical to understanding the extent and significance of the damage. The ability to select the appropriate remedial actions may depend on a review of audit data. It is also important to collect and retain audit data to have the ability to track and verify the actions of authorized users. In the event of unintended configuration errors, audit data may indicate the source of the error.

To track changes to the AD database, log files, work files, and the GPT directory (SYSVOL), specific audit settings for the files are necessary. If the guidance in the *Windows 2003/XP/2000 Addendum* and the *Windows Server 2003 Security Guide* is followed, there is no need for additional audit setting requirements for data files.

To ensure that changes and attempted changes to sensitive objects in the AD database are tracked, specific audit settings are necessary for objects in the domain partition of the AD database. The following are the minimum settings required.

***Domain* Object**			
Type	**Name**	**Access**	**Scope**
Failure	Everyone	[All access types]	*Domain* object only
Success	Everyone	Write All Properties Modify Permissions Modify Owner	*Domain* object only
Success	Administrators	All Extended Rights	*Domain* object only
Success	Domain Users	All Extended Rights	*Domain* object only

Please note that "*Domain*" is the actual Windows domain name. For example, this could be "DC=aofn21,DC=disa,DC=mil".

***Domain*,CN=System,CN=AdminSDHolder Object**			
Type	**Name**	**Access**	**Scope**
Failure	Everyone	[All access types]	AdminSDHolder object only
Success	Everyone	Modify Permissions Modify Owner Write All Properties	AdminSDHolder object only

***Domain*,CN=System,CN=Policies Object and *Domain*,CN=System,CN=Policies,CN=*GPC Child* Objects**			
Type	**Name**	**Access**	**Scope**
Failure	Everyone	[All access types]	Policies object and all *GPC child* objects

***Domain*,CN=System,CN=Policies Object and *Domain*,CN=System,CN=Policies,CN=*GPC Child* Objects**			
Type	**Name**	**Access**	**Scope**
Success	Everyone	Modify Permissions Modify Owner Create groupPolicyContainer Objects Delete Delete groupPolicyContainer Objects Delete Subtree	Policies object only
Success	Everyone	Modify Permissions Write All Properties	all *GPC child* objects

***Domain*,CN=System,CN=RID Manager$ Object**			
Type	**Name**	**Access**	**Scope**
Failure	Everyone	[All access types]	RID Manager$ object only
Success	Everyone	All Extended Rights Write All Properties	RID Manager$ object only

***Domain*,CN=Infrastructure Object**			
Type	**Name**	**Access**	**Scope**
Failure	Everyone	[All access types]	Infrastructure object only
Success	Everyone	All Extended Rights Write All Properties	Infrastructure object only

***Domain*,OU=Domain Controllers Object**			
Type	**Name**	**Access**	**Scope**
Failure	Everyone	[All access types]	Domain Controllers OU and all child objects
Success	Everyone	Modify Permissions Modify Owner Create All Child Objects Delete Delete All Child Objects Delete Subtree	Domain Controllers OU only
Success	Everyone	Write All Properties	Domain Controllers OU and all child objects

Table 2-11. Domain Partition Object Audit Settings

If audit settings are not configured properly for objects in the domain partition of the AD database, it may not be possible to determine the source and extent of unintentional configuration errors and unauthorized intrusions.

- *(DS00.0140: CAT II) The SA will ensure auditing is properly configured for the objects in the domain partition of the AD database.*

As ongoing research is completed, it is expected that guidance for audit settings of other AD objects will be provided in future versions of this document.

Because the impact of these settings depends on activity in the local environment, SAs are advised to monitor the Security event logs on their domain controllers and make adjustments for any increase in the amount of log data.

As actions on specific AD data files and database objects must be audited, the same is true for AD maintenance and synchronization data. This extends the path of accountability to the data input to and output from the AD database. If AD maintenance and synchronization operations are not audited, it may not be possible to determine the source and extent of unintentional configuration errors and unauthorized intrusions.

There are four considerations to the implementation of AD maintenance and synchronization auditing:

- Programs performing maintenance or synchronization functions must be configured to collect audit data.
- Programs must be available that allow the audit data to be reviewed.
- The audit data must be protected from unauthorized access.
- The audit data must be protected from premature destruction.

- *(DS05.0250: CAT II) The IAO will ensure AD synchronization or maintenance applications are configured to capture audit-related data through the Windows event logging facility (preferred) or another method.*

A special requirement applies to the use of the Microsoft ADAM feature that may be incorporated in maintenance or synchronization solutions. At the present time Microsoft states that auditing is not supported when ADAM runs on Windows XP Professional.

- *(DS15.0100: CAT I) The IAO will ensure instances of ADAM used for synchronization or maintenance of production AD data are not hosted on Windows XP-based computers.*

The requirements for audit data review capability, access protection, and retention are already met on Windows servers when the maintenance or synchronization solutions utilize the Windows event logging facility. In this case, existing requirements in the *Windows 2003/XP/2000 Addendum* address the issues. However, some products or solutions may not use this facility so the requirements are reflected here.

- *(DS05.0260: CAT III) The IAO will ensure tools necessary to review AD synchronization or maintenance audit data are available.*

- *(DS05.0270: CAT III) The IAO will ensure AD synchronization or maintenance audit data files are backed up at least weekly onto a different system or media than the system being audited.*

- *(DS05.0280: CAT III) The IAO will ensure backups of AD synchronization or maintenance audit data files are retained for at least one year.*

- *(DS05.0290: CAT II) The IAO will ensure the access permissions for AD synchronization or maintenance audit data files are no less restrictive than for the Windows log files.*

2.3.3.6 Group Membership and Privilege Control

Restricting Windows user rights is among the most important tasks in strengthening the security posture of a Windows forest and domain. Permission to use many of these rights is the characteristic that distinguishes privileged users. Because rights are usually granted at the group level, it is logical that restricting group membership is part of the task of restricting privileges. The focus in this document is on groups because the requirements related to specific user rights are covered in detail in the *Windows 2003/XP/2000 Addendum* and the *Windows Server 2003 Security Guide* and should be referenced there.

Another aspect of privilege control has to do with certain types of permissions on objects. Specifically, permission to own or update certain types of AD objects such as OUs can be a delegated administrative privilege.
The goal of this section is primarily to document group membership considerations and also to document some specific account and privilege controls that have particular impact on AD security.

It was noted in section 2.2.3, Group Membership, that there are several groups automatically created when Windows is installed that have default privileges over AD files and database objects. Membership in some of these groups grants permissions to the members to change configuration settings that can impact an entire AD forest. With the exception of the Domain Admins group, membership in the other groups is generally not required to support common administrative tasks.

Ensuring that the membership in privileged groups is controlled requires the maintenance of baseline documentation and periodic reviews to determine that unauthorized users are not members. If an unauthorized user is able to gain membership in the Enterprise Admins, Schema Admins, or Incoming Forest Trust Builders groups, that user would be able to display, add, or change AD objects that could impact the confidentiality, integrity, or availability of an entire forest. Gaining membership in the Domain Admins or Group Policy Creator Owners groups would allow the user to display, add, or change AD objects that could impact the confidentiality, integrity, or availability of an entire domain.

- *(DS10.0240: CAT II) The IAM will limit the number of users and document those users assigned to the following security groups: Domain Admins, Enterprise Admins, Schema Admins, Group Policy Creator Owners, and Incoming Forest Trust Builders.*

Because of the individual needs and environmental constraints within DOD Components, it is impossible in a practical sense to define a comprehensive list of strict group membership requirements. A hierarchy that provides appropriate control for a large unit could be

unreasonably complex in another. As a result, most of the guidance here is written as recommendations that the Components need to interpret for their particular environment.

The following guidance should be applied when managing group membership:

- The IAO should ensure that the number of users assigned to the Domain Admins group of an empty or small forest root domain is limited to a very small number of users.

- The IAO should consider restricting membership in the Enterprise Admins, Schema Admins, and Incoming Forest Trust Builders groups to no (zero) members and adding a local Administrator account to the groups temporarily when needed.

  Because membership in Schema Admins would only be required when updates to the AD schema are needed, such as the installation of products like Microsoft Exchange or Systems Management Server, the Schema Admins group should almost always be empty.

- The IAO should consider the use of group policy that uses the Restricted Groups setting. Implementing such a policy would provide periodic, automated refreshes of the memberships of privileged groups.

One aspect of privileged group membership that can be stated as a requirement deals with cross-forest memberships. After the establishment of a forest trust, it is possible to make a user from the trusted forest a member of a group in the trusting forest. While this may be reasonable for certain data access situations, it is not generally an acceptable practice for administrative privilege assignment.

If a user from one forest is added to an administrative group in another forest, the isolation of administrative privileges at the forest boundary is being compromised. This may be a deliberate design decision and is reasonable when a resource forest is established. A typical case would be an MS Exchange architecture designed to isolate e-mail from other organization functions. However, other cases are generally indicative of a violation of the separation of duties principle.

- *(DS10.0250: CAT II) The IAO will ensure Windows built-in administrative groups do not contain groups or users from another forest unless the two forests are subject to the same security policy and control of a single organization.*

It is acknowledged that there are cases when a single person requires administrative privileges in more than one forest. This is likely to occur when a perimeter forest is being used. In this case the user can be assigned individual accounts. By using an individual account in each forest, the risk is reduced that a compromise in one forest will spread to another.

One strategy that can be used to limit privileges is the creation and delegation of OUs. Creating an OU for user accounts that have similar privileges and other OUs for users without can provide groupings to which appropriate group policy can be linked. A similar strategy can be applied to computers. Just as domain controller accounts are assigned to the Domain Controllers OU and that OU has the Default Domain Controllers Policy linked to it, it may be desirable to create OUs

for other categories of computers and create and link policies to them. Once OUs have been created it is also possible to delegate control over those OUs. This allows for privileged users who are limited in scope.

The structure of OUs and the delegation strategy must be designed for their specific environment. The following guidance is recommended:

- The IAO should ensure that user accounts and computer accounts are assigned to OUs.
- The IAO should consider the use of group policies to limit access to sensitive member servers and administrative workstations.
- The IAO should delegate control of OUs to groups instead of individual users. This implementation of RBAC simplifies security administration.

As noted, delegating control over OUs creates limited-scope administrators. Ensuring that this privilege is controlled requires the maintenance of baseline documentation and periodic reviews. If an unauthorized user is able to gain control over an OU, that user could change the security policies applicable to the OU. This could result in weak security policies that would increase the risk of a successful attack against the affected resources.

- *(DS10.0260: CAT II) The IAM will limit the number of users and document those users who have been delegated AD object ownership or update permissions but are not members of Windows built-in administrative groups.*

Although the concern is not confined to AD or privileged users, the structure of Windows groups deserves a brief discussion because it affects, and is affected by, AD implementation. The various group types that can be used in Windows were briefly discussed in section 2.2.3, Group Membership. The assignment of privileges and access permissions to groups rather than individual users is done in almost all environments as an implementation of RBAC that simplifies security administration.

It was noted earlier that the domain functional level of a domain affects the group implementation. Most notably it occurs when domains are raised to the Windows 2000 native domain functional level. There are two items of significant impact to group structure.

- Universal groups are available. Their membership is replicated to all Global Catalog servers.
- The ability to nest domain global groups within domain global groups is available.

The structure of groups must be designed for the specific environment. The following guidance is recommended:

- The IAO should ensure that access and privilege permissions are assigned to domain local groups rather than users or other types of groups. This helps to preserve control of permissions at the domain level.

- The IAO should ensure that Universal groups are used to define groups that span domains and that single-domain forests do not use Universal groups. When Universal groups are not used, dependence on the Global Catalog server is reduced.
- The IAO should ensure that domain global groups rather than individual users are members of Universal groups. In addition to being more efficient because it reduces replication traffic among Group Catalog servers, it helps to preserve control of user memberships at the domain level.

As a reminder, these recommendations can be thought of as implementations of the A-G-DL-P, A-G-G-DL-P, and the A-G-G-U-DL-P strategies that were discussed in section 2.2.3, Group Membership.

There is a tendency to assign accounts used in maintenance or synchronization operations to the Administrators group. This usually results in granting greater privileges than actually needed and therefore violates the principle of least privilege. If a maintenance or synchronization account is assigned greater privileges than required, the operation may be able to read, change, or delete AD data files or database objects for which the account was not authorized.

- *(DS05.0300: CAT II) The IAO will ensure Windows accounts used by synchronization operations to access directory data are configured with the least privileges technically feasible. Specifically these accounts will not be members of Windows built-in administrative groups within a domain unless no alternative access control permissions can be configured.*

A maintenance or synchronization solution could involve the use of a Windows service. The privilege level of the account used for that service is also subject to the least privilege principle. Microsoft has documented that the ADAM feature does not require ADAM service accounts to be members of an Administrators group so a specific requirement can be followed.

- *(DS15.0110: CAT II) The IAO will ensure ADAM service accounts are not members of Windows built-in administrative groups within a domain or on the local computer.*

Any special privileges needed for production maintenance or synchronization operations should be limited to those activities and not assigned as individual user accounts.

- *(DS05.0310: CAT II) The IAO will ensure Windows accounts used to access directory data in production AD synchronization operations are dedicated to that purpose.*

The ability to create objects within the AD database is generally limited to members of administrative groups or to specific instances in which computer accounts dynamically create objects such as DNS entries. However, there are some cases in which non-administrative users or groups are granted the permission to create AD objects as part of a strategy for delegation of administrative tasks.

A primary example of delegation is the case of GPOs. Members of the Group Policy Creator Owners group can create GPO objects in the AD database. This privilege can also be delegated to other user accounts through the GPMC tool.

While delegating object creation can be advantageous, there are also risks associated with it. An inexperienced or malicious user might use the capability in a way that causes a denial of service for the domain controller. This can happen when so many objects are added that the server runs out of space for the AD database. In this case, it may become impossible to make additions or changes to the database.

A new feature was added to Windows Server 2003 as a mitigating control to this type of attack. This feature is the ownership quota for AD objects. It limits the number of objects that a user, group, computer, or service account is allowed to own in a specific AD database partition. The quota can be implemented two ways: as a default limit that applies to the partition for any account without a specific quota, or as the limit for the partition for a specific account.

If an unauthorized user is able to add an unlimited number of AD objects such as GPOs, a denial of service could occur for the affected domain controller. Logically, users who are not members of administrative groups are more likely to attempt this kind of attack. Also, the domain partition is most likely to be vulnerable because delegation capabilities are commonly granted on objects in that partition.

- *(DS10.0270: CAT IV) The IAO will ensure an ownership quota for AD domain partition objects is defined for those users and groups who are not members of Windows built-in administrative groups but have been delegated the ability to create AD objects.*

It is noted that Microsoft does not currently offer guidance with a specific quota number because implementation environments differ. Also, because the number of tombstones is a factor in the object ownership calculation, the volatility of the specific environment can affect the quota. Therefore Components that delegate the ability to create AD objects should evaluate their ownership patterns and select an appropriate value for their environment.

2.3.3.7 Functional Configuration

In terms of controls that can be configured for Windows server, maintenance, and synchronization programs that support AD functions, there are a few items that do not fit easily into the other subsections of the Enclave and Computing Environment controls. This section discusses those items and the associated requirements to enhance security.

The concept of an AD site was briefly discussed in section 2.2.2, Forest and Domain Architecture. Defining AD sites has an impact on AD data replication. Although most replication within an AD domain occurs automatically and as required, the existence of multiple sites introduces an additional consideration. After defining AD sites, site links must be created to define the connections between them. Site links have schedule and replication interval properties that impact the time and frequency with which replication between sites is attempted.

If replication between domain controllers at different sites does not occur on a timely basis, information updated on the domain controllers in one site is not available to the domain controllers in the other site. Although the impact varies according to the data, this is generally undesirable if it continues for more than one day.

- *(DS10.0280: CAT III) When the forest implementation includes multiple AD sites, the IAO will ensure the schedule and replication interval properties of each site link are configured to force replication at least daily.*

In order for AD functions to execute on a domain controller, there are certain Windows services that must be running. Without these services, group policy is not available when clients log on to the domain, the server cannot replicate with other servers, and Kerberos authorization processes may fail to function or function improperly.

Service-dependent AD functions can be disrupted by changing the startup type specification for the required Windows services. If the startup type is changed maliciously or unintentionally from "automatic" to "manual" or "disabled", AD functions on the affected domain controller may be unavailable.

- *(DS10.0290: CAT II) The SA will ensure the startup type for the following Windows services is set to automatic on all domain controllers: Distributed File System, DNS Client, File Replication Service, Intersite Messaging, Kerberos Key Distribution Center, and Windows Time.*

AD maintenance and synchronization solutions generally consist of one or more COTS or GOTS products with predefined and configurable functions. A requirement is stated in section 2.3.1, Security Design and Configuration, for a formal security evaluation of those products that update AD identification, authentication, or authorization data. However, in many cases it is possible to alter or supplement the functions that these products perform by adding locally written programs or changes to programs supplied with the product.

Even though such changes are intended as valuable enhancements, their addition to a previously validated collection of functions could cause unintended, negative consequences. If changes are made to functions that update data used in identification, authentication, or authorization services, the potential exists for the compromise of that IA-related data. In order to ensure that the locally written programs or changes are not implemented improperly, review under a configuration management process is needed.

- *(DS05.0320: CAT III) If an AD maintenance or synchronization solution is altered by the addition of locally written programs or changes to COTS or GOTS programs, and if those programs create or update security principal accounts, the IAO will ensure a documented configuration management (CM) process exists for the implementation of the programs.*

2.3.3.8 Data Transmission Confidentiality and Integrity

When data is transmitted over networks, it may be subject to vulnerabilities that allow the confidentiality or integrity of the data to be compromised. Compliance with requirements in the *Enclave STIG* and the *Network Infrastructure STIG* provides protection against many of these vulnerabilities, but there are actions that can be taken at the application level to further strengthen security.

AD data is transmitted across networks in several instances. This consists primarily of AD replication, configuration, and maintenance and synchronization data. This includes query and update operations that use LDAP. It is essential that the confidentiality and integrity of this data be maintained in order to ensure that the integrity and availability of Windows domain controllers, member servers, and clients are maintained.

Requirements in the *Windows 2003/XP/2000 Addendum* address encryption for common Windows network traffic. Compliance with those requirements provides the protection needed for ordinary AD operations. There are however some additional requirements to address maintenance and synchronization operations.

AD maintenance and synchronization data that is transmitted over wireless connections or over networks that are not subject to DOD controls requires encryption to ensure the confidentiality of the data. If an unauthorized user intercepts the data, sensitive information such as the names and locations of Windows accounts and data resources could be disclosed.

- *(DS05.0330: CAT II) The IAO will ensure when AD maintenance or synchronization is performed over wireless or non-DOD networks, the data is encrypted for transport using FIPS 140-2-validated cryptographic algorithms.*

Substantial aggregates of AD data, even when transported over networks with other security controls, must receive special consideration. Aggregates of data outside the AD database are typically the output from or input to maintenance and synchronization operations. While some aggregates reflect insignificant data, others could effectively disclose too much Component force or configuration data.

If an unauthorized user intercepts a substantial aggregate of AD data in transmission, that data could be used in an attack or to select valuable targets to attack. Even with network security controls protecting maintenance or synchronization data, the added value of the aggregate deserves the additional protection provided by data encryption.

- *(DS05.0340: CAT II) The IAO will ensure when a single AD maintenance or synchronization operation involves a substantial aggregate of the directory data for an entire geographic command, the data is encrypted for transport using FIPS 140-2-validated cryptographic algorithms.*

When a maintenance or synchronization solution involves a server and client architecture, mutual authentication is used to ensure the identities of both. In current implementations this often means that the server authenticates the client through a password or PKI certificate, and the client authenticates the server through a PKI certificate.

Policy on PKI usage is stated in *DODI 8520.2, Public Key Infrastructure (PKI) and Public Key (PK) Enabling*. In the context of maintenance or synchronization, there are two significant requirements: use of DOD PKI certificates and checking the validity of the certificates. The requirement to use DOD certificates was stated in section 2.3.2, Identification and Authentication. The validity-checking requirement is addressed here.

If servers or clients do not validate the status of PKI certificates, the unauthorized party may be able to collect client passwords and sensitive AD data. Therefore some method of certificate validation is necessary.

- *(DS05.0350: CAT III) The IAO will ensure AD maintenance or synchronization solutions that utilize PKI certificates incorporate Certificate Revocation List (CRL), Online Certificate Status Protocol (OCSP), or other checking to ensure the validity of certificates.*

Data signing is one method used at the application level to maintain transmission integrity. If the guidance for SMB packet signing and LDAP data signing in the *Windows 2003/XP/2000 Addendum* is followed, there is no need for additional requirements for ordinary AD operations. However, because AD maintenance or synchronization solutions might use different protocols and controls, a requirement for those products is needed.

- *(DS05.0360: CAT III) The IAO will ensure AD maintenance and synchronization solutions are configured to use integrity mechanisms such as data signing to ensure the integrity of transmitted data.*

In addition to data signing, other mechanisms to enhance the integrity of network sessions are sometimes available in AD maintenance or synchronization solutions. When protocols such as TLS are configured to require mutual authentication, network session integrity is enhanced because both parties are authenticated through a common mechanism. Because product implementations vary, this guidance is written generally to require enabling those options that assure session integrity and detect or prevent session hijacking.

- *(DS05.0370: CAT III) The IAO will ensure AD maintenance and synchronization solutions are configured to use mutual (both server and client) authentication mechanisms such as those available through Transport Layer Security (TLS).*

A final data integrity issue for AD is related to the use of synchronized time. Within Windows there are a number of actions that depend on the assumption that the time setting is synchronized among servers and clients. It was noted in section 2.2.2, Forest and Domain Architecture, that proper AD replication, Kerberos authentication and authorization functions, and useful audit data generation depend on accurate time references. If the time setting of a domain controller is set to a value significantly different than other servers or clients in a domain, AD data could be lost or corrupted, clients could be denied logon to a domain or access to resources, or audit data could have inaccurate timestamps.

- *(DS00.0150: CAT II) The IAO will ensure a mechanism for synchronizing time is implemented on all domain controllers.*

Because the Windows Time service is available on all computers running current versions of Windows, it is logical to use it as the standard tool throughout an AD forest. However, there are environments in which a large number of non-Windows systems, different tool sets, or network protocol restrictions might indicate a different solution. Because alternative tools or methods could accomplish the same objective, the following guidance is a recommendation.

- The IAO should ensure that a single tool or method is used to synchronize the time on all domain controllers within the same forest to a common ultimate time source. The Windows Time service, configured to use the AD domain hierarchy, is a recommended solution. The only exception to this guidance is for the server holding the PDC Emulator FSMO role in the forest root domain.

When the Windows Time service is deployed in the forest using the AD domain hierarchy as the time source, the forest root domain PDC Emulator has to be configured to synchronize its time with a trustworthy external source. If this is not done, the time for an entire forest could depend on an imprecise server hardware clock or an unreliable, non-DOD server or network.

- *(DS10.295: CAT II) If the Windows Time service is used, the IAO will ensure that the forest root domain PDC Emulator is configured to synchronize its time with a DOD-authorized time source external to the forest in which it resides.*

Time synchronization tools are commonly capable of automatic switching to alternate sources when a primary source is not available. However, such a switch could indicate malicious activity. Logging of time source switch events enables detection of such activity.

- *(DS00.0151: CAT III) The IAO will ensure that time synchronization tools capable of switching time sources create a log entry when a switch is made.*

Please note that this level of logging is configurable through the "EventLogFlags" Group Policy setting and is enabled by default in Windows Server 2003. But for Windows 2000 Server it requires the addition of Windows registry entries. The registry entries are documented in Microsoft Knowledge Base article 307937.

It should also be noted that the Windows Time service in Windows Server 2003 supports a very detailed level of event logging. This level of logging is primarily useful for troubleshooting problems, but it may be helpful in some environments to implement on the forest root domain PDC Emulator. Please refer to the documentation in Microsoft Knowledge Base article 816043 and the Windows Time Service Technical Reference on the Microsoft TechNet web site.

2.3.4 Enclave Boundary Defense

This section describes AD security requirements based on applicable DODI 8500.2 IA Controls in the Enclave Boundary Defense subject area. These requirements address items that are related to remote access to AD data.

All remote access to DOD information systems, including privileged and unprivileged, requires a restricted access path that includes encryption and strong authentication. This reflects the fact that data flow is being permitted into and out of a protected enclave.

The Terminal Services Windows component is one tool that might be used for remote access. Security-related settings that are required when using Terminal Services are described in Appendix B of the *Windows 2003/XP/2000 Addendum.*

A discussion of privileged user remote access is provided in the *Enclave STIG*. In the context of AD maintenance or synchronization, a privileged user is one authorized to change the configuration of the product or solution. If an unauthorized user is able to gain privileged remote access, that user may be able to change configuration controls to allow AD data to be read, updated, or deleted. To mitigate that vulnerability, stronger access controls are required and session logs must be created and reviewed for each session.

- *(DS05.0380: CAT II) The IAO will ensure remote access to privileged functions of AD maintenance and synchronization solutions is secured through a managed access control point such as a Remote Access Server (RAS) and increased session security such as that provided through a VPN.*

- *(DS05.0390: CAT II) The IAO will ensure remote sessions for privileged users of AD maintenance and synchronization solutions are logged and that the logs are reviewed at least weekly.*

Remote access by non-privileged users also requires stronger access controls. If an unauthorized user is able to gain non-privileged access, that user may be able to gain read access to sensitive Component force or configuration data held in AD maintenance or synchronization files.

- *(DS05.0400: CAT III) The IAO will ensure remote access to user (non-privileged) functions of AD maintenance and synchronization solutions is secured through a managed access control point such as a RAS.*

Remote access to AD maintenance or synchronization solutions implies that the user is accessing the server through a network path that includes elements outside the control of the host enclave. If an unauthorized user is able to gain access to a vulnerable network segment, that user may be able to intercept the AD data in transit. To address this threat, encryption is required on all remote access sessions.

- *(DS05.0410: CAT II) The IAO will ensure all remote access to AD maintenance and synchronization solutions is encrypted.*

To meet the requirements for secure remote access, a VPN solution is frequently used. While VPN implementations do provide desirable session protection, they can also be used to conceal malicious traffic. A network-based intrusion detection system (IDS) addresses this threat. A discussion of network IDS functions can be found in the *Enclave STIG*. The requirement here enforces the specific need for AD traffic that uses a VPN to be examined for intrusive behavior.

- *(DS10.0300: CAT II) The IAO will ensure VPN traffic for AD data is visible to a network IDS.*

2.3.5 Physical and Environmental

This section describes the AD security requirements based on applicable DODI 8500.2 IA Controls in the Physical and Environmental subject area. These requirements address a specific need for the physical security of certain servers involved in AD and AD maintenance or synchronization functions.

Physical access restrictions are necessary for all servers. Such restrictions address common physical threats that are caused in normal office environments where power disruptions, spilled liquids, and cabling disconnections can happen accidentally. These restrictions also address attempts by malicious individuals to disrupt the operation of the server or extract data that may be otherwise protected in transit.

Protections for certain Windows servers are even more significant. Domain controllers that hold the FSMO roles in the forest root domain are particularly important to the availability and integrity of resources on Windows servers throughout the forest. Data such as that in the AD schema presents an attractive target for attacks employing poisoning or corruption strategies designed to impact an entire forest.

If an unauthorized user is able to obtain physical access to the servers holding the FSMO roles in the forest root domain, that user could disrupt the operation of the entire forest. The impact of this disruption can vary widely from a short-term outage of a particular function to destruction that could require complete restoration of the domain and delays to inter-forest resource access. Because of this potential impact, access to these specific servers must be more restricted than for most.

- *(DS10.0310: CAT II) The IAO will ensure physical access to the forest root domain controllers that hold FSMO roles is restricted to specifically authorized personnel.*

Some AD maintenance or synchronization solutions do not require Windows server software as their host. However, the functions they perform can have a direct, significant impact to Windows domain controllers, the domain, and even the entire forest. If an unauthorized user is able to obtain physical access to the machine hosting the AD maintenance or synchronization solution, that user may be able to compromise the AD environment or data just as if they had physical access to a Windows domain controller. To address this threat, all hosts of AD maintenance or synchronization solutions must be subject to the same physical access controls as other Windows domain controllers.

- *(DS05.0420: CAT II) The IAO will ensure physical access to host machines used to support normal, scheduled AD synchronization or maintenance operations is no less restricted than access to Windows domain controllers.*

2.3.6 Continuity

This section describes AD security requirements based on applicable DODI 8500.2 IA Controls in the Continuity subject area. These requirements address three general objectives:

- AD data and AD maintenance and synchronization data and programs must be backed up according to their unique requirements.
- Information that is required to restore and reconstruct the AD environment and forest and domain architecture must be captured.
- AD architecture should be implemented in such a way as to reduce recovery requirements and shorten recovery time.

Windows domains cannot function properly without valid and current AD data. Identification, authentication, and authorization functions are all directly dependant on the AD database. Corruption or loss of the data effectively disables a domain controller and can immediately or eventually disable an entire domain and forest. To be able to recover when AD data is corrupted or lost, the proper data backup must have been done.

In Section 2.2.2, Forest and Domain Architecture, it was noted that AD data must be backed up as part of an operation that backs up the Windows System State data. Among other items, a System State data backup includes the AD database and the GPT (SYSVOL) data that are necessary to restore AD.

- *(DS00.0160: CAT II) The IAO will ensure backup procedures properly capture the AD database and Group Policy Template (SYSVOL) data daily (preferred) or at least weekly on all domain controllers. This backup must incorporate a System State data backup.*

AD maintenance and synchronization solutions might be used in production operations where AD replication does not provide a function to transport needed data. If an incident causes the corruption or loss of AD maintenance and synchronization data or programs in those environments, current data may not be available when needed. Although normal system backups should capture the COTS programs, special attention must be focused on capturing the data and local programs involved.

- *(DS05.0430: CAT II) The IAO will ensure backup procedures capture the AD maintenance or synchronization data that is used in production DOD operations.*

- *(DS05.0440: CAT III) If an AD maintenance or synchronization solution is altered by the addition of locally written programs or changes to COTS or GOTS programs, the IAO will ensure backup procedures capture the AD maintenance or synchronization application code.*

In the event of an incident that requires restoration or reconstruction of domain controllers, certain information may be required that is not available from a data backup. This information ranges from passwords and software inventories to architecture information needed to rebuild an AD forest. If this information is not available when one or more domain controllers must be

restored or rebuilt, it may result in a permanent loss of AD data including identification, authentication, and authorization data.

The DSRM system state used for AD restore operations was mentioned in section 2.2.2, Forest and Domain Architecture. When a Windows server is promoted to be a domain controller, a password must be selected for use when that domain controller is booted into DSRM. If that password is not available when needed, it will not be possible to restore the AD database from the backup.

- *(DS10.0320: CAT II) The IAO will ensure the password defined for use in DSRM for each domain controller is stored in a locked, fire-rated container or is subject to other appropriate protections from loss.*

Events caused by natural or man-made circumstances can result in the physical loss of all domain controllers in a domain or forest. If this occurs, reconstruction of the AD environment is necessary. Beyond the backup media required to perform restores, the availability of some AD implementation information can make reconstruction significantly more efficient. If information about the forest, tree, and domain structure is not available, it can be very difficult to restore domain controllers quickly and effectively.

- *(DS10.0330: CAT III) The IAO will ensure disaster recovery plans include AD architecture details identifying the forest, tree, and domain structure covering all systems designated as MAC I or II.*

Please note that a separate plan for AD recovery is not required. On the contrary, the best implementation would be an integrated plan for the enclave that includes AD and other essential applications.

For those environments in which AD maintenance and synchronization solutions are used in production operations, an inventory of the software required to support those operations is needed. This information can be used to validate that all resources needed for operation are available in the recovery environment.

- *(DS05.0450: CAT III) The IAO will ensure disaster recovery plans include identification of AD synchronization or maintenance software that is used to support production DOD operations on all systems designated as MAC I or II.*

Incidents that require some limited type of AD recovery are far more common than disasters. The simple failure of a disk can disable a domain controller and require some recovery action. Failure in a network component can disable critical communications needed during Windows logon and resource authorization. It is important to understand that there are some AD implementation steps that can be taken to lessen the impact of some incidents.

The basic strategy behind simplifying recovery related to AD is the quantity, placement, and functional role of domain controllers. If these steps are not taken, recovery that might otherwise be largely transparent to users could require outages ranging from hours to days.

One of the easiest recovery strategies is simple redundancy. The presence of multiple domain controllers within each domain can allow local identification, authentication, and authorization functions to continue while a failed domain controller is restored.

- *(DS10.0340: CAT II) The IAO will ensure more than one domain controller is operational in each Windows domain that contains servers designated as MAC I or II.*

The large number of individual needs and environmental constraints within an organization the size of DOD makes it impossible in a practical sense to define a comprehensive list of strict AD recovery requirements. A configuration appropriate to a large Component presence could be unreasonable in cost and complexity terms for another. As a result, the following guidance is written as recommendations that the Components need to interpret for their particular environment.

The following guidance should be applied when determining when to deploy servers and how to assign AD FSMO and Global Catalog roles:

- The IAO should ensure that the Domain Naming and Schema Master roles are assigned to domain controllers that are not holding any other FSMO roles.

- The IAO should ensure that the Infrastructure Master role is assigned to a domain controller that is not a Global Catalog server unless there is only one domain in the forest or all domain controllers are Global Catalog servers.
- The IAO should consider assigning the PDC Emulator role to a domain controller holding no other FSMO roles.

- The IAO should ensure that at least one domain controller per AD site is a Global Catalog server.

- The IAO should ensure that at least one domain controller per domain, that holds few or no FSMO roles, is designated as a standby operations master to assume the other roles.

2.3.7 Vulnerability and Incident Management

This section describes the AD security requirements based on applicable DODI 8500.2 IA Controls in the Vulnerability and Incident Management subject area. These requirements address the need to be prepared for incidents and to ensure that vulnerabilities in AD maintenance and synchronization products are addressed.

In certain circumstances it may be necessary to alter normal operating configurations in order to address a potential or ongoing computer network attack (CNA). Although the details of a specific attack and the desired defense posture vary, potential configuration changes need to be identified in advance of any CNA incident. The approach to defensive actions is established according to the Information Operations Condition (INFOCON) guidance. Details about INFOCON guidance can be found in the *Enclave STIG*.

The configuration of manual AD trusts is one area that fits well into an implementation of INFOCON guidance. Because manual AD trusts usually represent a policy that expands resource access from one domain or forest to another, there are times when it may be appropriate to temporarily disable this access. If a CNA incident results in the compromise of a trusted domain or forest, an enabled AD trust may result in the compromise of the trusting domain or forest. To address this threat, the procedures to disable specific trusts are included in the INFOCON response plan.

- *(DS10.0350: CAT III) Based on the determination of the IAM, the IAO will ensure the local \ applicable incident response plan includes procedures to disable external, forest, or realm AD trusts defined on each domain as the INFOCON posture increases to higher levels of readiness.*

No software products are immune from the identification and exploit of vulnerabilities. Many vulnerabilities have been linked to deficient programming practices and, although those issues have received a lot of attention, serious problems are still discovered. The proliferation of vulnerability and exploit information on the Internet exacerbates these problems by making the information widely and easily accessible. Unfortunately, mitigating action is often not taken, even when a fix has been identified and made available.

AD maintenance and synchronization products are not unique in this respect. Although they represent a much lesser known target than a Windows OS, the probability that they contain vulnerable code is still present. If an AD maintenance or synchronization product is found to have a vulnerability and the mitigating patch is not applied, an attacker may be able to exploit the vulnerability to compromise the confidentiality, integrity, or availability of the related AD domains and forests.

To make certain that vulnerabilities are addressed, a formal commitment to security patch implementation is essential. It is not necessary to have a unique policy for AD maintenance and synchronization products, just a policy that covers them. Manual or automated documentation indicating that patches have been applied provides auditable evidence that mitigating action has been taken.

- *(DS05.0460: CAT II) The IAO will ensure all security related patches to AD synchronization and maintenance applications are applied and that completion is documented for each applicable asset.*

APPENDIX A. RELATED PUBLICATIONS

Government Publications:

Department of Defense Directive 8500.1, "Information Assurance (IA)," 24 October 2002

Department of Defense Instruction 8500.2, "Information Assurance (IA) Implementation," 6 February 2003

Department of Defense Instruction 8520.2 "Public Key Infrastructure (PKI) and Public Key (PK) Enabling," April 1, 2004

Department of Defense Instruction 8551.1, "Ports, Protocols, and Services Management (PPSM)," 13 August 2004

Department of Defense Memorandum, "Open Source Software (OSS) in the Department of Defense (DOD)," 28 May 2003

Department of Defense, "Department of Defense Active Directory Concept of Operations", Final Coordinating Draft, Rev 1.1, 24 June 2005

Department of Defense, "Active Directory User Object Attributes Specification", Version 1.0, April 2005

Defense Information Systems Agency (DISA), "Database Security Technical Implementation Guide"

Defense Information Systems Agency (DISA), "Domain Name System Security Technical Implementation Guide"

Defense Information Systems Agency (DISA), "Enclave Security Technical Implementation Guide"

Defense Information Systems Agency (DISA), "Web Server Security Technical Implementation Guide"

Defense Information Systems Agency (DISA), "Windows 2003/XP/2000 Addendum"

National Security Agency (NSA), "Guide to Securing Microsoft Windows 2000 Active Directory," Version 1.0, December 2000

Vendor Publications:

Microsoft Corporation, "Active Directory Application Mode Technical Reference (Draft)", April 2004

Microsoft Corporation, “Active Directory LDAP Compliance”, October 2003

Microsoft Corporation, “Best Practice Guide for Securing Active Directory Installations”, 2003

Microsoft Corporation, “Best Practice Guide for Securing Active Directory Installations and Day-to-Day Operations: Part I”, 2003

Microsoft Corporation, “Best Practice Guide for Securing Active Directory Installations and Day-to-Day Operations: Part II”, 2003

Microsoft Corporation, “Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP”, 2003

Microsoft Corporation, “Windows Server 2003 Security Guide”

Microsoft Press, “Microsoft Windows Security Resource Kit”, March 12, 2003

Other Publications:

Internet Engineering Task Force, “Request for Comments 2829, Authentication Methods for LDAP”, May 2000

Internet Engineering Task Force, “Request for Comments 2830, Lightweight Directory Access Protocol (v3): Extension for Transport Layer Security”, May 2000

Web Sites:

Government:

Information Assurance Support Environment (IASE)	http://iase.disa.mil/ http://iase.disa.smil.mil/
IASE - Ports and Protocols	http://iase.disa.mil/ports/index.html
Joint Task Force Global Network Operations (JTF-GNO)	http://www.jtfgno.mil/ http://www.jtfgno.smil.mil/

Vendor:

Microsoft Windows Server 2003 Active Directory	http://www.microsoft.com/windowsserver2003/technologies/directory/activedirectory/default.mspx
Microsoft Windows Server 2003 Active Directory Application Mode (ADAM)	http://www.microsoft.com/windowsserver2003/adam/default.mspx

Web Sites:

Microsoft Windows Server 2003 Security Guide	http://www.microsoft.com/technet/security/prodtech/windowsserver2003/w2003hg/sgch00.mspx
Microsoft Best Practice Guide for Securing Active Directory Installations (Windows 2003)	http://www.microsoft.com/windowsserver2003/techinfo/overview/adsecurity.mspx
Microsoft Best Practice Guide for Securing Active Directory Installations and Day-to-Day Operations (Windows 2000)	http://www.microsoft.com/technet/prodtechnol/windows2000serv/technologies/activedirectory/maintain/bpguide/default.mspx
Microsoft Lifecycle Dates	http://support.microsoft.com/lifecycle/search/ http://support.microsoft.com/gp/lifesupsps
Microsoft Security Bulletin Search	http://www.microsoft.com/technet/security/current.aspx

Other:

Internet Engineering Task Force (IETF)	http://www.ietf.org/

Please note that, for the site links above that span lines, it may be necessary to manually paste the complete links into your web browser.

This page is intentionally left blank.

APPENDIX B. LIST OF ACRONYMS

ACL	Access Control List
AD	Active Directory
ADAM	Active Directory Application Mode
ADSI	Active Directory Service Interfaces
AIS	Automated Information System
CA	Certification Authority
CIFS	Common Internet File System
CIO	Chief Information Officer
CNA	Computer Network Attack
COI	Community of Interest
COTS	Commercial-Off-the-Shelf
CRL	Certificate Revocation List
CSV	Comma Separated Value
CSVDE	CSV Data Exchange
DAA	Designated Approving Authority
DADIWG	DOD Active Directory Interoperability Working Group
DC	Domain Controller
DHCP	Dynamic Host Configuration Protocol
DISA	Defense Information Systems Agency
DMZ	Demilitarized Zone
DNS	Domain Name System
DOD	Department of Defense
DODI	DOD Instruction
DSDE	Directory Services Data Exchange
DSfW	DSML Services for Windows
DSML	Directory Services Markup Language
DSRM	Directory Services Restore Mode
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards
FRS	File Replication Service
FSMO	Flexible Single-Master Operations
FSO	Field Security Operations
GAL	Global Address List
GC	Global Catalog
GIG	Global Information Grid
GOTS	Government-Off-the-Shelf
GPC	Group Policy Container
GPMC	Group Policy Management Console
GPO	Group Policy Object

GPT	Group Policy Template
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over SSL
IA	Information Assurance
IAM	Information Assurance Manager
IAO	Information Assurance Officer
IASE	Information Assurance Support Environment
IAVM	Information Assurance Vulnerability Management
ID	Identifier
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IIFP	Identity Integration Feature Pack
IIS	Internet Information Services
INFOCON	Information Operations Condition
IP	Internet Protocol
IPSec	Internet Protocol Security
IT	Information Technology
JTF-GNO	Joint Task Force - Global Network Operations
Kbps	Kilobits per second
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LDAPS	Lightweight Directory Access Protocol over SSL
LDIF	LDAP Data Interchange Format
LDIFDE	LDIF Data Exchange
LSA	Local Security Authority
MAC	Mission Assurance Category
MIIS	Microsoft Identity Integration Server
MMC	Microsoft Management Console
MMS	Microsoft Metadirectory Services
MOA	Memorandum of Agreement
MS-DS	Microsoft - Directory Service
NIAP	National Information Assurance Partnership
NIPRNet	Non-secure Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NT	New Technology
NTFS	NT File System
NTP	Network Time Protocol

OCSP	Online Certificate Status Protocol
OSS	Open Source Software
OU	Organizational Unit
PDI	Potential Discrepancy Item
PKI	Public Key Infrastructure
PM	Program Manager
PPS	Ports, Protocols, and Services
PPSM	Ports, Protocols, and Services Management
RAS	Remote Access Server
RBAC	Role-Based Access Control
RFC	Request for Comment
RID	Relative Identifier
RPC	Remote Procedure Call
RSoP	Resultant Set of Policy
SA	System Administrator
SAM	Security Accounts Manager
SDID	Short Description ID
SID	Security Identifier
SMB	Server message block
SNTP	Simple Network Time Protocol
SOAP	Simple Object Access Protocol
SSL	Secure Sockets Layer
STIG	Security Technical Implementation Guide
TCP	Transmission Control Protocol
TCP/UDP	Transmission Control Protocol / User Datagram Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
UI	User Interface
URL	Uniform Resource Locator
VPN	Virtual Private Network
WMI	Windows Management Instrumentation
WQL	WMI Query Language

Please note that some items in this list have multiple, valid expansions. The following resources were used to resolve ambiguities.

DOD Joint Acronyms and Abbreviations
http://www.dtic.mil/doctrine/jel/doddict/acronym_index.html

Microsoft Glossary and Acronyms for PC and Server Technologies
http://www.microsoft.com/whdc/resources/support/glossary.mspx