

Beyond the MCSE: Active Directory for the Security Professional

Sean Metcalf

Trimarc

TrimarcSecurity.com

Black Hat USA 2016

Table of Contents

Overview	4
Differing Views of Active Directory	5
Active Directory Components	6
Administration	6
Forest	9
Domains	10
Schema	10
Trusts	11
Sites, Subnets, & Replication	13
Organizational Units	14
DNS	14
Domain Controllers	15
DCLocator	15
Global Catalog	16
FSMOs	16
Read-Only Domain Controllers	18
DNS Zone Hosting	19
Kerberos Handling	19
Authentication & Password Caching	20
Directory Services Restore Mode (DSRM) account	25
Active Directory Database	27
Group Policy	28
Authentication	32
The Evolution of Windows Authentication	32
NTLM	32
Kerberos	34
Active Directory Administration Groups	38
Default Groups & Permissions: DC Rights	38
AD Security Enhancements by OS	40
Forest and Domain Functional Level Security Enhancements	40
Windows 2008 R2 Forest/Domain Mode Features	41
New AD Features: Windows Server 2012	41

Key AD Security Features: 2012 R2	41
Windows 10 - New & Updated Auditing.....	42
Active Directory Security Best Practices	43
General Recommendations	43
Protect Admin Credentials.....	43
Protect Service Account Credentials.....	43
Protect Resources	44
Protect Domain Controllers	44
Protect Workstations (& Servers)	44
Logging	44
Interesting AD Facts	45
A Security Pro's AD Checklist	45
Recommended Domain Controller Event Logging.....	46
References	48

Overview

This whitepaper is meant to augment the Black Hat USA 2016 presentation “Beyond the MCSE: Active Directory for the Security Professional” which highlights the Active Directory components that have important security roles.

There are plenty of resources for learning Active Directory, including Microsoft’s websites referenced at the end of this document. This whitepaper highlights the key Active Directory components which are critical for security professionals to know in order to defend Active Directory. Many security professionals aren’t very familiar with AD to know the areas that require hardening. There are many aspects of Active Directory that are not well known often leveraged by attackers. By highlighting this information, blue teams can better understand their AD environment in order to protect it more effectively. The presentation builds on the standard Microsoft material by adding the security angle often missing in typical training books. Properly securing the enterprise means identifying and leveraging appropriate defensive technologies.

Differing Views of Active Directory

Systems administrator/engineer, security professional, and attacker each see Active Directory and how these differences matter when defending the enterprise

The Active Directory administrator/engineer focuses on uptime and ensuring that Active Directory responds to queries in a reasonable amount of time.

The security professional may monitor Domain Admin group membership, ensure that the Domain Controller security logs are forwarded to a central logging server, and that systems are patched.

The attacker focuses on the entire enterprise security posture including that of every component.

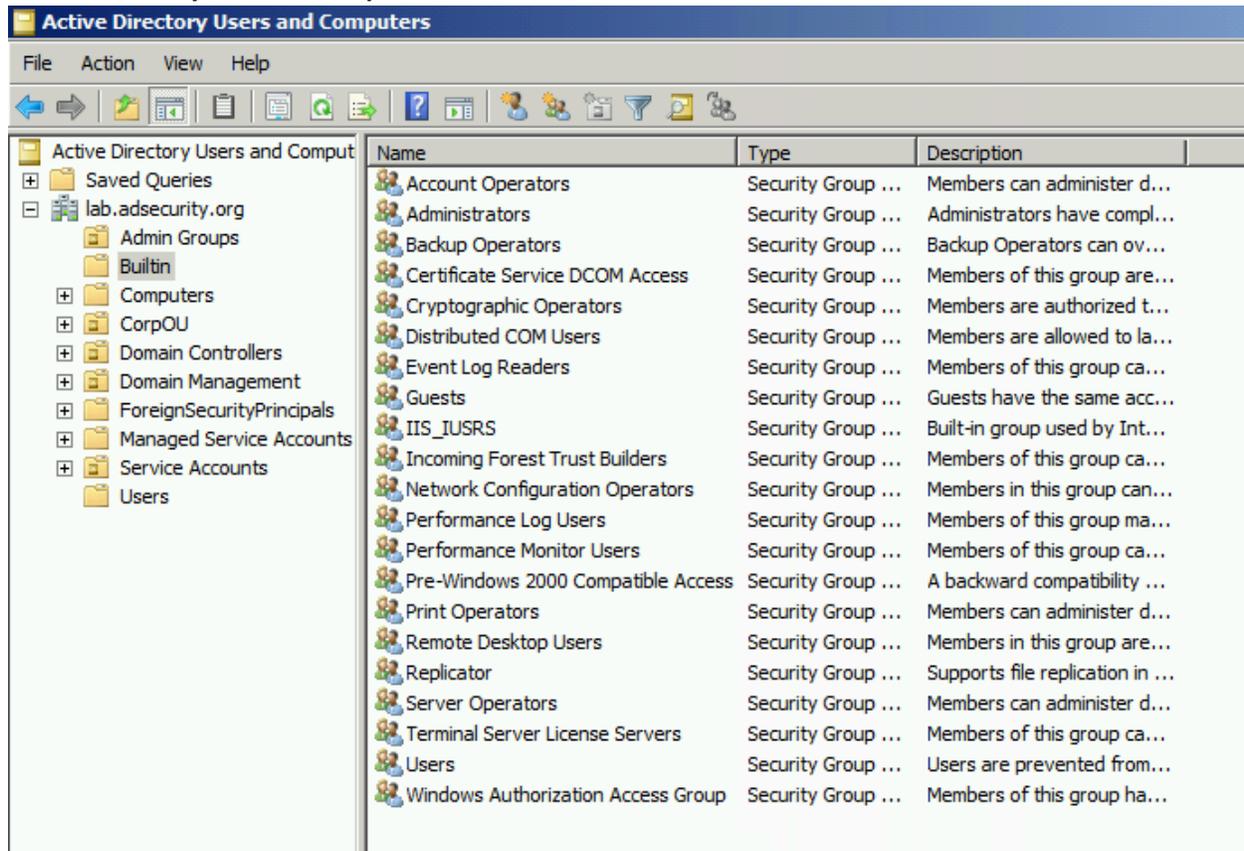
Active Directory Components

Active Directory is like a network registry where all information about users, groups, computers, servers, printers, network shares, and more are stored. Each of these are considered objects and have attributes associated with them in the directory. A user object has attributes such as first name, last name, work phone number, and group membership associated with it.

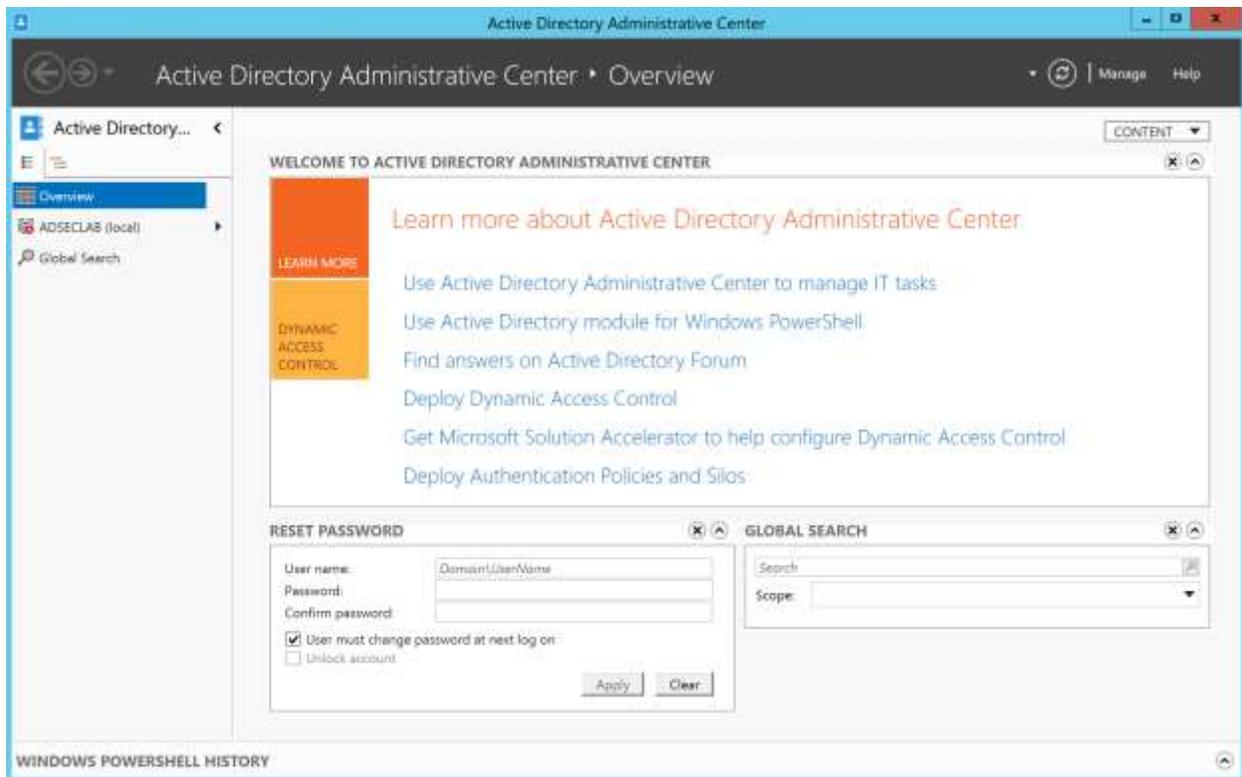
Administration

There are several methods for interactive with Active Directory.

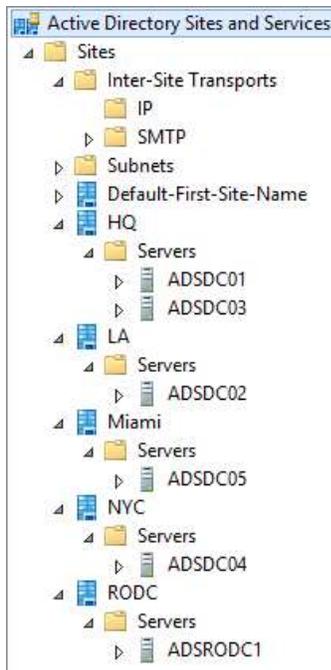
Active Directory Users & Computers



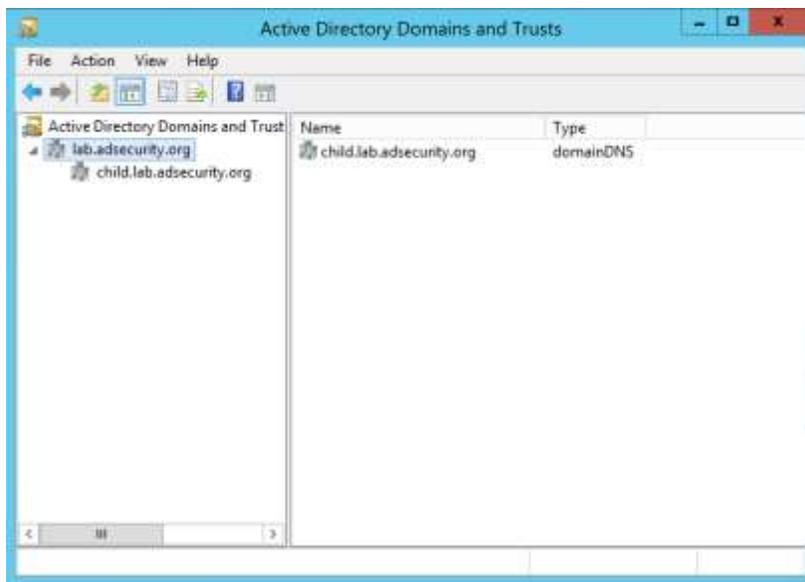
Active Directory Administrative Center – an updated admin console with a new style and PowerShell support.



AD Sites & Services



AD Domains & Trusts



PowerShell – PowerShell provides a number of methods to interact with Active Directory, from ADSI and .Net to the Active Directory PowerShell module.

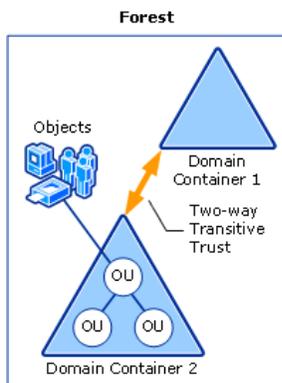
```

Administrator: Windows PowerShell
PS C:\>
PS C:\> get-command -module activedirectory

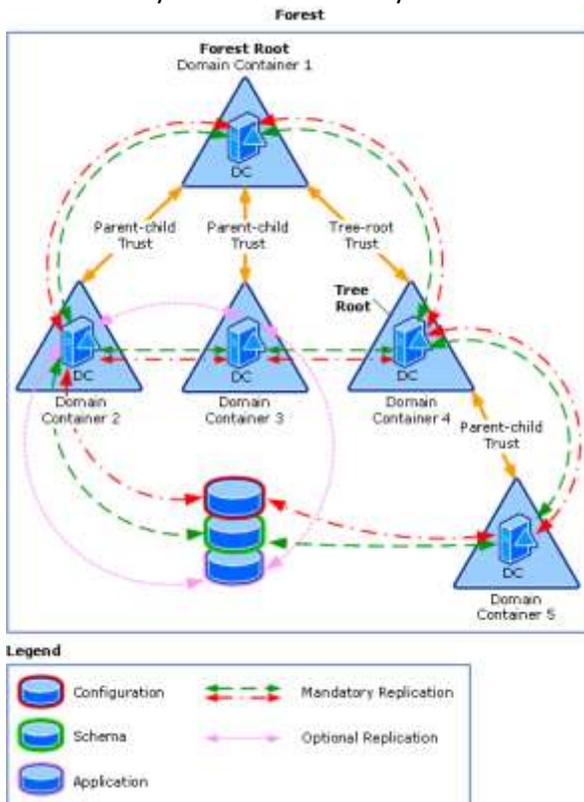
commandType      Name                                     Version      Source
-----
Cmdlet           Add-ADCentralAccessPolicyMember        1.0.0.0     activedirectory
Cmdlet           Add-ADComputerServiceAccount           1.0.0.0     activedirectory
Cmdlet           Add-ADDomainControllerPasswordReplicat 1.0.0.0     activedirectory
Cmdlet           Add-ADFineGrainedPasswordPolicySubjec 1.0.0.0     activedirectory
Cmdlet           Add-ADGroupMember                       1.0.0.0     activedirectory
Cmdlet           Add-ADPrincipalGroupMembership         1.0.0.0     activedirectory
Cmdlet           Add-ADResourcePropertyListMember       1.0.0.0     activedirectory
Cmdlet           Clear-ADAccountExpiration               1.0.0.0     activedirectory
Cmdlet           Clear-ADClairTransformLink             1.0.0.0     activedirectory
Cmdlet           Disable-ADAccount                       1.0.0.0     activedirectory
Cmdlet           Disable-ADOptionalFeature              1.0.0.0     activedirectory
Cmdlet           Enable-ADAccount                        1.0.0.0     activedirectory
Cmdlet           Enable-ADOptionalFeature                1.0.0.0     activedirectory
Cmdlet           Get-ADAccountAuthorizationGroup         1.0.0.0     activedirectory
Cmdlet           Get-ADAccountResultantPasswordReplicat 1.0.0.0     activedirectory
Cmdlet           Get-ADAuthenticationPolicy             1.0.0.0     activedirectory
Cmdlet           Get-ADAuthenticationPolicySilo         1.0.0.0     activedirectory
Cmdlet           Get-ADCentralAccessPolicy               1.0.0.0     activedirectory
Cmdlet           Get-ADCentralAccessRule                 1.0.0.0     activedirectory
Cmdlet           Get-ADClairTransformPolicy              1.0.0.0     activedirectory
Cmdlet           Get-ADClairType                         1.0.0.0     activedirectory
Cmdlet           Get-ADComputer                          1.0.0.0     activedirectory
Cmdlet           Get-ADComputerServiceAccount            1.0.0.0     activedirectory
Cmdlet           Get-ADCCloningExcludedApplicationList  1.0.0.0     activedirectory
Cmdlet           Get-ADDefaultDomainPasswordPolicy       1.0.0.0     activedirectory
Cmdlet           Get-ADDomain                             1.0.0.0     activedirectory
Cmdlet           Get-ADDomainController                  1.0.0.0     activedirectory
Cmdlet           Get-ADDomainControllerPasswordReplicat 1.0.0.0     activedirectory
Cmdlet           Get-ADDomainControllerPasswordReplicat... 1.0.0.0     activedirectory
Cmdlet           Get-ADFineGrainedPasswordPolicy         1.0.0.0     activedirectory
Cmdlet           Get-ADFineGrainedPasswordPolicySubjec 1.0.0.0     activedirectory
Cmdlet           Get-ADForest                             1.0.0.0     activedirectory
Cmdlet           Get-ADGroup                              1.0.0.0     activedirectory
Cmdlet           Get-ADGroupMember                       1.0.0.0     activedirectory
Cmdlet           Get-ADObject                             1.0.0.0     activedirectory
Cmdlet           Get-ADOptionalFeature                   1.0.0.0     activedirectory
Cmdlet           Get-ADOrganizationalUnit                1.0.0.0     activedirectory
Cmdlet           Get-ADPrincipalGroupMembership          1.0.0.0     activedirectory
Cmdlet           Get-ADReplicationAttributeMetadata      1.0.0.0     activedirectory
Cmdlet           Get-ADReplicationConnection              1.0.0.0     activedirectory
Cmdlet           Get-ADReplicationFailure                 1.0.0.0     activedirectory
Cmdlet           Get-ADReplicationPartnerMetadata        1.0.0.0     activedirectory
Cmdlet           Get-ADReplicationQueueOperation         1.0.0.0     activedirectory
Cmdlet           Get-ADReplicationSite                    1.0.0.0     activedirectory
Cmdlet           Get-ADReplicationSiteLink               1.0.0.0     activedirectory
Cmdlet           Get-ADReplicationSiteLinkBridge         1.0.0.0     activedirectory
Cmdlet           Get-ADReplicationSubnet                  1.0.0.0     activedirectory
Cmdlet           Get-ADReplicationUpToDateenessVectorTa 1.0.0.0     activedirectory
Cmdlet           Get-ADResourceProperty                  1.0.0.0     activedirectory
Cmdlet           Get-ADResourcePropertyList               1.0.0.0     activedirectory
Cmdlet           Get-ADResourcePropertyValueType         1.0.0.0     activedirectory
Cmdlet           Get-ADRootDSE                            1.0.0.0     activedirectory
Cmdlet           Get-ADServiceAccount                    1.0.0.0     activedirectory
Cmdlet           Get-ADTrust                              1.0.0.0     activedirectory
Cmdlet           Get-ADUser                               1.0.0.0     activedirectory
Cmdlet           Get-ADUserResultantPasswordPolicy       1.0.0.0     activedirectory
Cmdlet           Grant-ADAuthenticationPolicySiloAccess  1.0.0.0     activedirectory
  
```

Forest

Forests are the Active Directory structure and security boundary and domains are the administrative and replication boundary. Unfortunately, many organizations have designed their AD environment with the false belief that the AD domain is the security boundary. This is not the case and enables full forest compromise with the compromise of a single domain. Furthermore, the authentication and authorization boundary can be extended beyond the forest to other forests and/or domains, often without full understanding of the security implications.



A forest is a complete instance of Active Directory in a single namespace, with each forest being the single entity containing all Domains, Domain Controllers, Organizational Units, etc. within the forest. The forest has a single schema which defines object types and associated properties. By default, forest data is contained within the forest and not shared outside of the forest. All intra-forest trust relationships are automatically created as two-way transitive trusts.



The first Domain Controller promoted in a new forest also instantiates the first forest domain, called the forest root domain as well as the forest name.

Security Note:

The Active Directory forest is the security boundary. Administrators in one domain can gain administrative access to other domains in the forest. Creating trusts from one forest to another extends the authentication boundary as well as potentially unintentionally exposing information. Compromise of any domain in the forest and/or any trusted domain could lead to complete forest compromise.

Microsoft Forest reference:

<https://technet.microsoft.com/en-us/library/cc759073%28v=ws.10%29.aspx>

Domains

An Active Directory Domain partitions the Active Directory forest to allow smaller AD databases which replicate domain data separately from other domains. From a Domain perspective, all properties of all objects within the Domain are replicated to all Domain Controllers within that Domain only. The Domain provides a replication boundary as well as one of authentication and security policy. Domains do not provide protection from a malicious Domain Admin in another Domain in the Forest.

Security Note:

An Active Directory domain contains all the data for the domain which is stored in the domain database (NTDS.dit) on all Domain Controllers in the domain. Compromise of one Domain Controller and/or the AD database file compromises the domain. The Active Directory forest is the security boundary, not the domain. Creating trusts from one domain to another extends the authentication boundary as well as potentially unintentionally exposing information.

Schema

The schema is the forest-wide template that defines the objects and their properties hosted in Active Directory. The schema must not only be protected from failure, but also protected from inadvertent or random changes since the schema affects every user, system and application that is part of the forest. Changes to Active Directory schema should be infrequent, but well tested. Object and attribute additions are not reversible; objects can be disabled but not deleted once created. There is a special group in Active Directory that has rights to modify the schema called Schema Admins. This group remains empty, secured, and monitored so no changes can be made without prior approval.

Security Note

The schema defines all objects and their properties. Unauthorized modification of the schema could unintentionally expose data or corrupt the Active Directory forest.

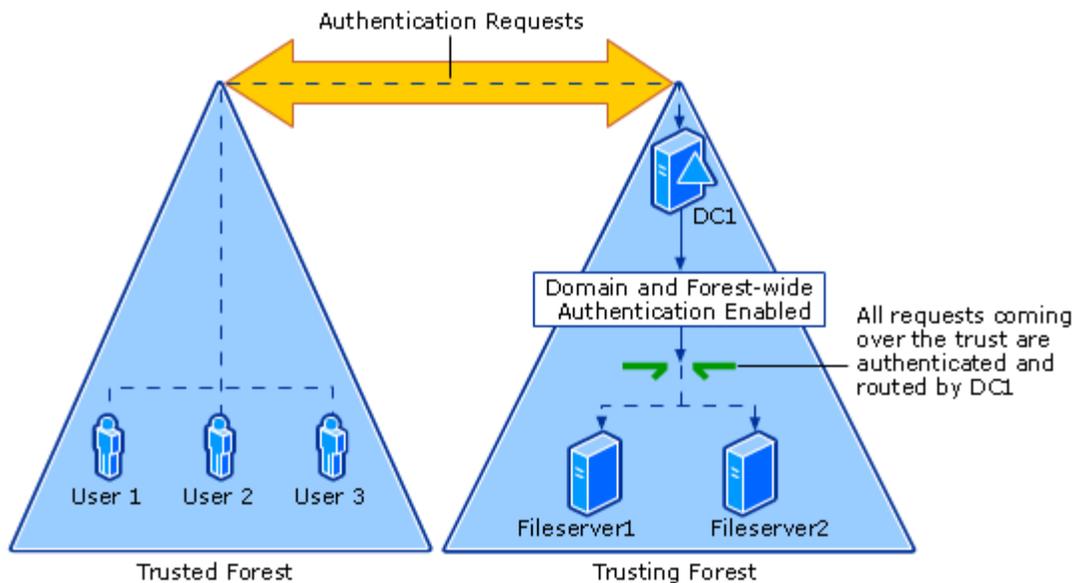
Microsoft Schema Reference

<https://technet.microsoft.com/en-us/library/cc961756.aspx>

Trusts

A trust is a connection between domains or forests leveraged to extend authentication and are authentication pipelines that must be present in order for users in one domain to access resources in another domain.

Some trusts are one-way only enabling users from one domain/forest to access resources in another domain/forest. A two-way, or bidirectional, trust enables users in either domain/forest to access resources in the other.



<https://technet.microsoft.com/en-us/library/cc786873%28v=ws.10%29.aspx>

There are two primary types of trusts: Domain and Forest. Within an Active Directory forest with multiple domains, there are implicit two-way transitive trusts between the parent domain and the child domains in the forest. These trusts are transitive meaning that authentication can flow from one domain to another while transiting a third. Transitivity determines whether a trust can be extended outside of the two domains with which it was formed. A transitive trust can be used to extend trust relationships with other domains; a nontransitive trust can be used to deny trust relationships with other domains. Additionally, within a forest there is another trust that can be manually created called a Shortcut Trust. This type of trust is used to improve authentication between domains in a forest when a user in ChildDomainA needs to authenticate to ChildDomainB since the authentication needs to transit ParentDomain. A Shortcut Trust created between ChildDomainA and ChildDomainB improves authentication.

Trust type	Transitivity	Direction	Description
External	Nontransitive	One-way or two-way	Use external trusts to provide access to resources that are located on a Windows NT 4.0 domain or a domain that is located in a

			separate forest that is not joined by a forest trust. For more information, see Understanding When to Create an External Trust .
Realm	Transitive or nontransitive	One-way or two-way	Use realm trusts to form a trust relationship between a non-Windows Kerberos realm and an Active Directory domain. For more information, see Understanding When to Create a Realm Trust .
Forest	Transitive	One-way or two-way	Use forest trusts to share resources between forests. If a forest trust is a two-way trust, authentication requests that are made in either forest can reach the other forest. For more information, see Understanding When to Create a Forest Trust .
Shortcut	Transitive	One-way or two-way	Use shortcut trusts to improve user logon times between two domains within An Active Directory forest. This is useful when two domains are separated by two domain trees. For more information, see Understanding When to Create a Shortcut Trust .

[https://technet.microsoft.com/en-us/library/cc730798\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc730798(v=ws.11).aspx)

Active Directory stores information about trusts in Trusted Domain Objects (TDOs) which represent each trust relationship within a domain. A unique TDO is created with each trust and stored in the domain system container.

Domain Trust TDO Attributes store trust transitivity, type, and the reciprocal domain names.

Forest Trust TDOs store additional attributes to identify all of the trusted namespaces from its partner forest. Including attributes: domain tree names, user principal name (UPN) suffixes, service principal name (SPN) suffixes, and security ID (SID) namespaces.

Domain Controllers (2003+) authenticates users and applications using Kerberos V5 or NTLM, with the Kerberos V5 protocol configured as the default protocol for all supported versions of Windows. If any computer involved in a transaction does not support Kerberos V5, the NTLM protocol will be used.

Kerberos AES needs to be explicitly enabled on manually created trusts to ensure Kerberos across the trust leverages AES.

Additionally, there are different options for trusts:

- SID History Filtering (Quarantine): Does not allow SID History data to be included in the authentication and the data is filtered out.
- Selective Authentication: Changes the default access rules that external users have to the forest. The most notable is that there is no access to resources across this trust type, not even read access. With Selective Authentication, an external user must have explicit delegated access to the resource in order to receive a Kerberos ticket to access it.

Authentication Setting	Interforest Trust Type	Description
Domain-wide Authentication	External	Permits unrestricted access by any users in the trusted domain to all available shared resources located in the trusting domain. This is the default authentication setting for external trusts.

Forest-wide Authentication	Forest	Permits unrestricted access by any users in the trusted forest to all available shared resources located in any of the domains in the trusting forest. This is the default authentication setting for forest trusts.
Selective Authentication	External and Forest	Restricts access over an external or forest trust to only those users in a trusted domain or forest who have been explicitly given authentication permissions to computer objects (resource computers) residing in the trusting domain or forest. This authentication setting must be manually enabled.

[https://technet.microsoft.com/en-us/library/cc755321\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc755321(v=ws.10).aspx)

Trust information can be enumerated via WMI on the Domain Controllers or by querying the Trusted Domain Object in the domain.

WMI Class Name	Namespace	Version Compatibility
Microsoft_TrustProvider	root\microsoftactivedirectory	Windows 2000 Server and Windows Server 2003
Microsoft_DomainTrustStatus	root\microsoftactivedirectory	Windows 2000 Server and Windows Server 2003
Microsoft_LocalDomainInfo	root\microsoftactivedirectory	Windows 2000 Server and Windows Server 2003

[https://technet.microsoft.com/en-us/library/cc756944\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc756944(v=ws.10).aspx)

Security Note

The Active Directory forest is the security boundary. Administrators in one domain can gain administrative access to other domains in the forest. Creating trusts from one forest/domain to another extends the authentication boundary as well as potentially unintentionally exposing information. Compromise of any domain in the forest and/or any trusted domain could lead to complete forest compromise. SID History filtering should be enabled to protect against leveraging SID History to compromise a trusting domain. Selective Authentication should be enabled when possible to limit data exposed across the trust to only explicitly authorized accounts and groups.

Sites, Subnets, & Replication

Active Directory replication topology is divided into multiple sites to optimize replication.

Active Directory uses the concept of sites to map Active Directory resources to a geographical or network area. AD clients use sites to discover Domain Controllers and other resources such as DFS shares. Sites effectively map Active Directory to physical locations.

Subnets are configured in AD to map network subnets to Active Directory sites. This linkage enables resource discovery.

Active Directory sites are also used by certain enterprise services to ensure that data is transferred via the quickest possible route. Exchange uses AD sites for routing mail, data redundancy, and fail-over. Distributed File System (DFS) leverages AD sites for referring clients to the closest DFS source. It is necessary to ensure the site link costs are configured appropriately, otherwise mail routing may be delayed and DFS clients may get referrals from distant sites.

Replication topology is divided into multiple sites to optimize replication.

Within sites - Replication minimizes latency by using fast, frequent updates which is triggered by changes & designed to occur as frequently as needed and without compression.

Between sites - Compressed to conserve network bandwidth and occurs according to a schedule so that the frequency of replication over WAN links can be controlled.

Security Note

If clients are in a subnet not defined in Active Directory, they won't have an associated site and are unable to discover a local Domain Controller. This can make user activity tracking more difficult when monitoring DC security event logs. Additionally, the users on these clients will be directed to resources associated with other sites which also may complicate user activity tracking.

Organizational Units

Organizational Units (OUs) are logical containers in an Active Directory domain and can contain most types of objects including users, groups, computers, printers, etc. While OUs are useful to organize resources in a domain, OUs are not meant to replicate an org chart.

Organizational Units are best used when created to enable delegation or Group Policy deployment. Many times the OU structure grows organically which can cause potential security issues.

Should have a defined purpose & add value to the design - Unless the reason for creating an OU is to make administration easier, it may be easier not to create it.

Security Note

OUs should only be created for a clear purpose. Extraneous OUs complicate administration and make it difficult to know where certain objects should be created and be hosted. Since OUs are used to define and apply delegated administration and security policy via Group Policy, placing objects in the wrong OU could lead to domain compromise.

DNS

DNS (Domain Name Service) is essentially a database of name and IP address mappings. This database is commonly called a zone file. A DNS server is considered authoritative for a name if it contains and loads the zone with that name and is listed in as a Name Server for that zone. Active Directory leverages the forward and reverse zone types. The forward lookup zone is the most commonly used and enables a network name to be resolved into an associated IP address. The reverse zone simply does the opposite; it enables an IP address to resolve as a network name. The first record in any zone file is a Start of Authority (SOA) resource record (RR). The SOA RR identifies a primary DNS name server for the zone as the best source of information for the data within that zone and as an entity processing the updates for the zone. This DNS Server is authoritative for the zone if it is listed in the SOA RR.

In forward zone files, for every name there is an IP address and a record type designator. The record type designates the record as a host (A), an alias (CNAME), a mail exchanger (MX), a service (SRV), or other type of DNS record. Active Directory uses SRV resource records in DNS to designate and locate

server roles. When an Active Directory Domain Controller is installed, it registers itself with DNS with Domain Controller specific SRV records. SRV records also exist for other services such as global catalog servers.

Since DNS is a required Active Directory dependency, it is automatically installed & configured by default when a new Active Directory Forest is instantiated.

The Active Directory Integrated zone type stores DNS information in AD which is a typical configuration in most organizations since this provides multi-master replication (DNS can be updated on any DC). Computers can securely self-register DNS records simplifying DNS management.

Security Note

DNS is typically hosted on Active Directory Domain Controllers and configured to be AD-integrated zones for optimal performance, administration, and replication. Since this data is in AD, LDAP queries may be used to pull data about the environment. Additionally, any Microsoft DNS vulnerabilities could be used to compromise Active Directory.

If administration of DNS isn't managed appropriately, unauthorized DNS administration could redirect clients to compromise accounts and ultimately the domain.

Domain Controllers

Prior to Active Directory, a single Windows NT domain was the extent of the environment and trusts were required to extend it. Domain Controllers (DCs) for the domain were all read-only and were called "Backup Domain Controllers" with a single writable DC called the "Primary Domain Controller" (PDC) where all domain changes are performed. History repeats itself starting with Windows Server 2008 where an organization can add Read-Only Domain Controllers (RODCs) to the existing writable DCs. However, adding an RODC to Active Directory is not exactly straightforward and won't work in all situations. This talk covers the benefits and issues with RODCs in the environment along with methods to avoid common pitfalls.

Promotion of a member server to a Domain Controller is done by running DCPromo which uses a template NTDS.dit file as the base AD database. DCPromo finds a local DC to replicate current AD domain data.

The Domain Controller provides authentication & directory services and hosts the domain DFS root (\\domain.com\) as well as NETLOGON and SYSVOL.

Security Note

Domain Controllers are the most critical servers in an enterprise since compromise of one DC or the NTDS.dit database file for the domain (or a backup), can result in domain compromise.

DCLocator

DCLocator is how clients discover Domain Controllers

- Clients use the DCLocator API to invoke DsGetDcName (NetLogon).
- (DNS) DsGetDcName calls DnsQuery API to read the Service Resource (SRV) records and A records from DNS (that specifies the SRV record for the domain).

- _service._protocol.DnsDomainName
- _ldap._tcp.DnsDomainName
- (DNS) The client sends an LDAP “ping” via UDP to the DC names returned by the previous DNS lookup.
- The first DC to respond is selected.
- The NetLogon service caches this DC name for use.

Global Catalog

By default, the first Domain Controller in a domain is automatically made a Global Catalog (GC), though all DCs in the domain should host the Global Catalog. Global Catalog servers contain a partial replica (all objects, selected properties) of all Domains in the Forest. The global catalog is used for directory operations such as logons and forest-wide searches, but replicated attributes can be limited. It’s a service and a physical database for objects in the directory for its own domain and all other domains in the forest. Only the attributes marked to be replicated to GCs are replicated across domains to the GCs in domains. GC attribute replication is configurable via the PartialAttributeSet attribute. Only objects likely to be queried by users should be published to the GC. Authentication of a user requires global knowledge of the user’s group memberships. Universal Group membership requires GC for logon. Furthermore, applications such as Exchange use the Global Catalog extensively.

Security Note

The Global Catalog stores information for the entire forest, so targeting a search against a GC provides forest-wide information. Data stored in attributes that replicate to GCs is available in the forest and may be accessible via trusts, so this data should be protected appropriately.

FSMOs

Multi-master replication among peer domain controllers is impractical for some type of changes, so only one domain controller, called the operations master, accepts requests for such changes. Because multi-master replication plays an important role in an Active Directory-based network, it is important to know what these exceptions are. In any Active Directory forest, five different operations master roles are assigned to the initial domain controller during installation.

The location of the various forest and domain Flexible Master Single Operator (FSMO) role holders is important since each of these roles one exist once in a forest or domain.

There are two forest FSMO role holders.

The **Schema Master** is the only Domain Controller in the forest that hosts the writable schema partition (it is read-only on all other forest DCs). When a schema update needs to occur, the update operation is performed on this DC by a member of the Schema Admins group. Once the schema update is complete, it is replicated from the Schema Master FSMO role owner to all other DCs in the directory.

The **Domain Naming Master** is the only Domain Controller in the forest the can add/delete domains and application partitions to the Active Directory forest. It can also add or remove cross references to

domains in external directories. Only the Domain Naming Master FSMO role owner can write to the Partitions container or its children.

There are three domain FSMO role holders.

The **Primary Domain Controller Emulator** (PDC or PDCE) needs to be placed in a central location since there are a large number of critical actions the PDC performs:

- Account lockout is processed on the PDC emulator.
- Password changes performed by other DCs in the domain are replicated preferentially to the PDC emulator.
- Forest PDC is preferred time server for the AD Forest.
- Receives preferential (rapid) replication for password changes. DCs receiving authentication requests with bad passwords check with PDC.
- Performs account lockouts.
- Forest PDC manages forest trusts.
- Performs domain trust maintenance - Scavenger runs every 24hrs).
- Default target for DFS & GPO management operations.
- Owns the DFS object for the domain and writes changes.
- Manages SYSVOL migration from FRS to DFS.
- Runs SDProp process which protects privileged groups & account ACLs.
- Handles DC cloning operation (Windows 2012 R2 and newer).

The **RID Master** contains all of the available RIDs for the domain. When a new security principal is created, the DC uses a RID from its RID pool and adds it to the domain SID to create a new SID associated with the new security principal (user, computer, security group, etc). When a new DC is promoted, it requests a pool of RIDs from the RID Master (500 by default) and creates new security principals from this pool, renewing the RID pool as needed to ensure it has enough RIDs to satisfy requests for new security principals.

Domain SID + RID = Object SID

The RID Master is also responsible for moving an object from one domain to another during an inter-domain object move.

The **Infrastructure Master** tracks objects in different domains. The most common scenario is when a user in one domain is added to a group in another. Since that user doesn't exist in the same domain as the group. The group's domain needs to create a reference in its database to track that user. This task is handled by the Infrastructure Master. At least it is until the Recycle Bin is enabled in the forest at which point, all Domain Controllers in the forest track cross-domain reference objects.

If all the domain controllers in a domain also host the GC, then all the domain controllers have the current data, and it is not important which domain controller owns the Infrastructure Master role.

When the Recycle Bin is enabled, every DC performs cross-domain object reference updates when the object is renamed/moved/deleted, which means the Infrastructure Master no longer performs these tasks.

Security Note

While Domain Controllers all contain domain data, there are 5 FSMOs that are critical for types of Active Directory operation. Disruption of the PDC FSMO role holder can cause issues with proper AD performance. Additionally, the FSMOs are typically busier than other DCs. The best practice is to co-host all domain FSMOs on the same DC, preferably one well-connected.

Read-Only Domain Controllers

The Read-Only Domain Controller (RODC) was designed to be the ideal replacement of a writable Domain Controller at a branch office or location where the security of the server cannot be guaranteed. Typically, a DC provides two-way replication (inbound & outbound) with other domain DCs to ensure that changes performed on any are replicated to all. With a RODC, no changes to Active Directory are possible and replication is unidirectional (inbound only). The configuration of a RODC requires a Windows Server 2008+ writable DC upstream of the RODC's site to ensure the RODC receives replicated changes.

The RODC stores all the Active Directory objects and attributes that a writable Domain Controller contains (except for account passwords and filtered attributes); however, changes cannot be made on the RODC. Any updates to AD must be made on a writable Domain Controller and then replicated back to the RODC. The RODC refers the client to a writable Domain Controller where the changes are performed and then replicated back to the RODC. Applications that communicate with the RODC only have the ability to perform LDAP read requests to the RODC; any write requests receive an LDAP referral response to a writable Domain Controller, typically upstream in a hub site.

Since the RODC only enables inbound replication, this behavior is different from the bidirectional replication that Windows 2000 and 2003 DCs utilize. Since the 2000/2003 DCs do not recognize the RODC behavior as a DC, they will not replicate domain partition data to it (though 2000, 2003, & 2008 writable DCs replicate with each other without issue). A Windows Server 2008+ writable DC understands RODC behavior and will replicate content to the RODC.

RODCs provide the following benefits:

- **Read-only Active Directory Database** – Read-only copy of Active Directory provides a more secure option for distant locations such as a branch office. Changes attempted against the RODC are referred to the next upstream DC.
- **Read-only DNS Server** – DNS on the RODC can be configured as a DNS Secondary of the Active Directory Integrated DNS zone file or of a Primary standard DNS zone.
- **Credential Caching** – By default no passwords are stored on a RODC (including computer passwords), though specific groups can be configured for password caching. Physical attacks on Active Directory stored domain credentials on RODCs are not possible when password caching is disabled.

- **Administrator Role Separation** – Administration of a RODC can be delegated to a domain user account without providing “keys to the kingdom” access or significantly decreasing the security posture of Active Directory.
- **Reduced Exposure** – Filtering specific object attributes to ensure they don’t exist on RODCs. For example, there may be attributes that were added after the instantiation of Active Directory such as specific attributes that are confidential (SSNs, employee status, etc).
- **Unidirectional Replication** – The only replication that occurs on a RODC is inbound replication from a fully writable 2008 DC. This reduces the amount of replication traffic that occurs in the environment as well as the number of connections and connection objects at the primary site. This also protects the rest of the directory from memory corruption of the database due to hardware failure or improper shutdown at a remote site.
- **SYSVOL Modification Isolation** – If SYSVOL is modified on a RODC in the field, the change stays on the RODC and is not replicated out. This includes added, deleted, and modified SYSVOL files.

DNS Zone Hosting

The RODC can host a read-only copy (secondary zone) of the primary (Infoblox) or Active Directory-integrated DNS zone. The workstations and servers in the RODC’s site should point to the RODC as their primary DNS server for name resolution if DNS name resolution should stay in the site whenever possible. When these clients attempt to perform dynamic DNS registration updates, they are initially sent to the client’s primary DNS server which in this case is the RODC. The RODC will refer the client to a DNS server with a writable copy of the DNS zone (configured as authoritative master) which is either the Windows DNS server hosting the AD-integrated DNS zone or an Infoblox DNS server hosting the master (primary) DNS zone. The dynamic DNS clients may also find the DNS server that can perform the DNS zone updates by performing a SOA lookup for the MNAME record. If the RODC is configured as the second DNS server for clients in the site, the clients will communicate with the DNS server configured as the first DNS server in their network settings and fail over to the RODC as needed.

Kerberos Handling

Both writable DCs and RODCs are configured as KDCs for their site. Each RODC has its own unique Kerberos account (i.e., krbtgt_12345) used to grant Kerberos ticket-granting tickets (TGT) which are different from the writable Domain Controllers’ Kerberos krbtgt account (writable DCs also contain RODC Kerberos accounts). This separation of Kerberos accounts between DCs and RODCs provides “cryptographic isolation”. When a security principal (user, computer, service account, etc) in the RODC site authenticates against the RODC and the RODC has the password cached locally, the user receives a Kerberos ticket-granting ticket. This TGT is only valid within the RODC site for resources that authenticate against the RODC and if the user presents this TGT to a server providing the desired service (that authenticated against a writable DC), the authentication data (Privileged Authentication Certificate or PAC) in the user’s TGT is discarded and re-authenticated by a writable Domain Controller before updating the TGT with service ticket information. This TGT is used to acquire the Service Ticket which

authenticates the user to the service on the server. This is done to protect the enterprise from a compromised RODC forging Kerberos tickets (TGT) since RODC TGTs are only valid in the RODC's site; the RODC PAC is discarded by a writable DC when the TGT is used outside of the RODC site.

When an account attempts to authenticate to a RODC and the password is not cached locally, the authentication request is forwarded to the next upstream DC (typically the RODCs replication partner). This process is outlined in more detail in the next section.

While security principal credentials may be cached on RODCs, the existence of the security credentials on the RODC may be compromised if the RODC is stolen or RODC data is inappropriately exfiltrated. However, the potentially exposed credentials are limited to those allowed to be saved on the RODC and only the secrets (passwords) stored on the RODC could be discovered if the RODC is compromised. The *msDS-RevealedList* attribute on the RODC lists the accounts that have stored credentials.

NOTE: *By default, no credential secrets are stored on the RODC except for the RODC's unique Kerberos account (krbtgt) and the RODC's computer account.*

Authentication & Password Caching

By default, the RODC does not cache (or ever have access to) any passwords. The Allowed RODC Password Replication Group specific to one or many RODCs can be created and configured to allow specific user and computer passwords on the RODC (this group is empty by default). When the user (or computer) authenticates with the RODC, the RODC checks its local AD database for the user's password. If the password is cached on the RODC, authentication occurs similarly to a writable DC. If the password does not exist locally on the RODC, the RODC forwards the authentication request to an upstream writable DC and the upstream DC replies to the RODC with the authentication response. The RODC requests the user's password and if the user account is in the Allowed RODC Password Replication Group, the 2008 DC replicates the password to the RODC which the RODC then stores in its local AD database. The 2008 DC determines whether or not the RODC is authorized to receive the requested password based on the Allow group. This process works in the same manner for computer authentication and computer passwords.

NOTE: *RODCs don't necessarily cache passwords in memory. The passwords are replicated down to the RODC as either a single replicated object or as part of a standard replication event and are stored in the RODC's local*

There are 2 groups created when RODCs are installed in the Active Directory Domain that control what accounts may have passwords replicated to the RODC and which may never be replicated.

These groups and their default members are listed here:

1. The Denied RODC Password Replication Group
 - Enterprise Admins
 - Domain Admins
 - Schema Admins
 - Domain-wide krbtgt account

- Cert Publishers
 - Enterprise Domain Controllers
 - Enterprise Read-Only Domain Controllers
 - Group Policy Creator Owners
2. The Allowed RODC Password Replication Group
- Administrators
 - Server Operators
 - Account Operators
 - Backup Operators

The RODC Password Replication Policy (PRP) maintains four items:

1. **Allowed List** – Passwords that can be replicated to the RODC (explicit allow). This list is stored in the *msDS-Reveal-OnDemandGroup* attribute on the RODC. When an RODC is installed, the Allowed RODC Password Replication Group is added to this attribute.
2. **Denied List** - Passwords that cannot be replicated to the RODC (explicit deny). This list is stored in the *msDS-NeverRevealGroup* attribute on the RODC. When an RODC is installed, the Denied RODC Password Replication Group is added to this attribute.
3. **Revealed List** – Accounts that were authenticated and have passwords cached on RODCs. If a RODC is compromised, this list is used to reset those passwords. This list is stored in the *msDS-RevealedList* attribute on the RODC.
4. **Authenticated List** - Accounts authenticated by a RODC (account passwords may or may not be cached on the RODC). This list is stored in the *msDS-AuthenticatedToAccountList* attribute on the RODC.

Identifying what security principals were authenticated on a specific RODC is as simple as reviewing the list in the RODC computer properties or by querying the *msDS-AuthenticatedToAccountList* attributes on the RODC. This list may be used to determine what accounts may need to be added to the Allowed List (the RODC Group Updater PowerShell script can build the RODC Site Group membership based on the accounts listed in the *msDS-AuthenticatedToAccountList* attribute).

An interesting side-effect of the RODC is that once a password is cached on the RODC (either pre-populated or for user logon), it stays on the RODC until it is changed. There is no way to force delete a password from the RODC cache. The only way this can be done is to remove the user from the Allowed RODC Password Replication Group specific to the RODC, have the user change their password and authenticate against the RODC. The RODC would then deactivate the user's password on the next replication.

There is a scenario where a user may not have authenticated since the RODC was stood up and the WAN link goes down. This means the user's password is not cached on the RODC and the user's authentication request cannot be processed until the WAN link is up again. If the user had authenticated within the site prior to the WAN link going offline, then the user would be authenticated

by the RODC. The passwords of users in the Allowed RODC Password Replication Group can be prepopulated on the RODC either by clicking on Prepopulate Passwords on the RODC object in Active Directory Users & Computers or by running the repadmin command:
Repadmin /rodcpwdrepl [DSA_LIST] <Hub DC> <User1 Distinguished Name> [<Computer1 Distinguished name> <User2 Distinguished Name>...]

NOTE: *In order for a user to be authenticated by a RODC when the WAN link is down, the RODC must have both the user and the computer's password the user is using.*

NOTE: *Smart-card authentication is processed in a similar fashion except instead of the user's password; the smart-card certificate is cached on the RODC for authentication when the WAN link is down.*

NOTE: *RODCs never store trust passwords.*

RODC Attributes

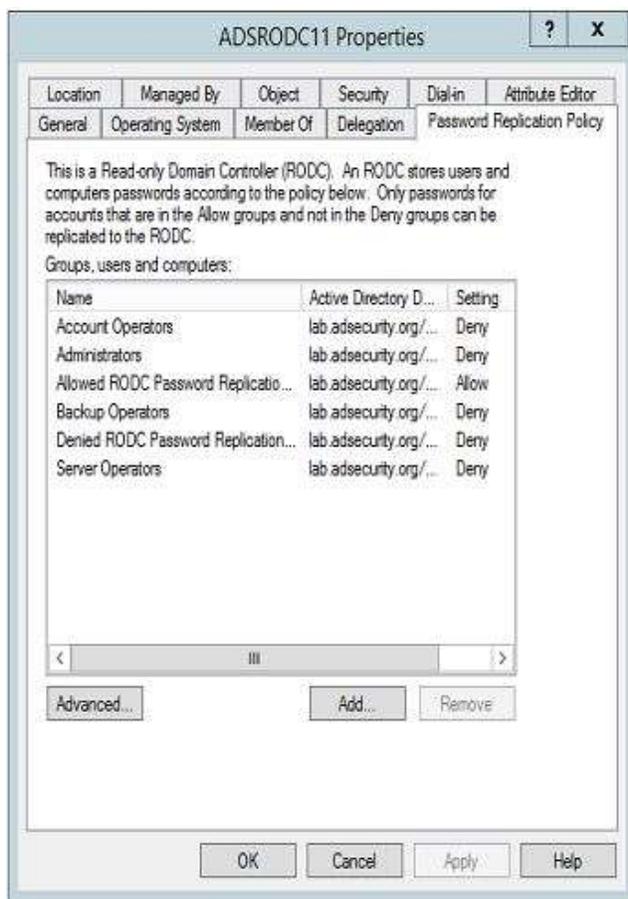
- **msDS-Reveal-OnDemandGroup:** Contains the distinguished name (DN) of the Allowed List. Members of the Allowed List are permitted to replicate to the RODC.
- **msDS-NeverRevealGroup:** Points to the distinguished names of security principals that are denied replication to the RODC.
- **msDS-RevealedList:** List of security principals whose passwords have ever been replicated to the RODC.
- **msDS-AuthenticatedToAccountList:** This attribute contains a list of security principals in the local domain that have authenticated to the RODC.

Since RODCs do not cache passwords by default, in order for an RODC to authenticate a user, the user and the user's workstation's password needs to be cached on the RODC. This is typically performed by adding a group to the domain "RODC Allowed Password Replication group".

Password Replication Policy controls what password data is replicated to RODCs.

- Allowed RODC Password Replication Group: Added to the msDS-Reveal-OnDemandGroup.
- Denied RODC Password Replication Group: Added to the msDS-NeverRevealGroup.

Domain password data not placed on RODCs by default.



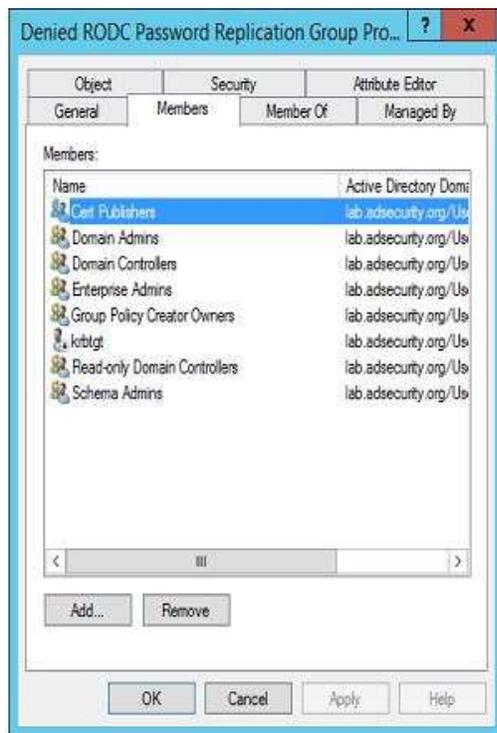
Denied RODC Password Replication Group Membership:

- *Cert Publishers*
- *Domain Admins*
- *Enterprise Administrators*
- *Schema Admins*
- *Group Policy Creator Owners*
- *Krbtgt*
- *Domain Controllers*
- *Read Only Domain Controllers*

RODC Administrator Role Separation (ARS)

- RODC administration can be delegated.

- RODC administrator is not a Domain Admin
- Full administrator on the RODC
- Can modify SYSVOL, but RODC SYSVOL changes are not replicated.
- RODC administrators should be in the “Allowed RODC Password Replication Group”



When placing a RODC at a site, there are several important considerations:

1. Think twice about placing a RODC in the same site as a DC. RODCs are meant to be used where there are security and/or other concerns (delegation, replication, etc). If a writable DC is in the site, it makes more sense to place another DC there instead of a RODC. Do not place a RODC in a site with an existing 2003 DC since users will see unusual behavior depending on which DC authenticates them.
2. If a location requires a DC that hosts additional services (roles), the DC placed at the site should be a RODC. DCs should not host services beyond core Active Directory services, especially those that require local administrators to logon to the server to manage.
3. There must be a 2008 DC upstream from the RODC to enable proper replication. It is best to have two 2008 DCs nearby to enable efficient replication.
4. If security concerns at the site are paramount, all of the users located at the site serviced by a RODC should be members of a site group which is added to the password policy for the RODC. This will ensure the user passwords are cached for logon in the event the network connection to a nearby writable DC is down.

5. All of the computers (workstations & servers) located at the site serviced by a RODC should be members of a site group which is added to the password policy for the RODC. This will ensure the computer passwords are cached ensuring proper computer operation in the event the network connection to a nearby writable DC is down.
6. RODCs never communicate with other RODCs. This means if there are multiple RODCs in the same site, they may have different accounts cached and possibly different password policies. This scenario is why it typically does not make sense to place two RODCs in a site.
7. DCLocator behavior was updated with Windows Vista and Windows Server 2008 (and newer) to enumerate DCs in the NextClosestSite when there is no local site DC. By default, sites identified as “next closest” containing an RODC (no writable DC) are filtered out as configured in the NextClosestSiteFilter setting on the computer.

Deploying RODCs in the environment is an excellent reason to re-evaluate account lockout policies. If the lockout policy is set to ensure the lockout persists for hours, it makes RODC deployment more complex. If a user at a RODC site locks their account and the WAN is offline, he/she will have to wait until the lockout time period ends before being able to log in.

RODC Challenges

- Best practice: Don't place writable DC and RODC in the same site.
- Branch office location with Exchange server requires writable DC.
- RODCs don't communicate with other RODCs.
- RODCs don't store user & computer passwords by default therefore RODCs don't authenticate users by default – authentication is chained to upstream writable DC.
- User's password as well as computer's password are required to authenticate user on RODC.
- After authentication, RODC requests password from writable DC. If allowed by Password Replication Policy, the writable DC replicates password to RODC.

Security Note

RODCs may at first seem to be a great way to provide DC services without exposing the domain data stored on it. It's important to understand the limitations of RODCs and how they operate to ensure proper deployment and use.

Directory Services Restore Mode (DSRM) account

Every Domain Controller has an internal “Break glass” local administrator account to DC called the Directory Services Restore Mode (DSRM) account. The DSRM password is set when DC is promoted and is rarely changed. The primary method to change the DSRM password on a Domain Controller involves running the ntdsutil command line tool.

Beginning with hotfix [KB961320](#) on Windows Server 2008, there is the option to synchronize the DSRM password on a DC with a specific domain account. Note that this must be performed every time the password is changed; it does not create an automatic sync partnership.

[Changing the DSRM Account Password:](#)

Run the following command on every DC (or remotely against every DC by replacing “null” with DC name).

- NTDSUTIL
- set dsrm password
- reset password on server null
- <PASSWORD>
- Q
- Q

[Synchronize the DSRM Account Password with a Domain Account \(2k8 & newer\):](#)

In an elevated CMD prompt where you have logged on as a Domain Admin, run:

```
NTDSUTIL
SET DSRM PASSWORD
SYNC FROM DOMAIN ACCOUNT <your user here>
Q
Q
```

What’s interesting about the DSRM password is that the DSRM account is actually “Administrator”. *This means that once an attacker has the DSRM password for a Domain Controller (or DCs), it’s possible to use this account to logon to the Domain Controller over the network as a local administrator.*

```
mimikatz(commandline) # token::elevate
Token Id : 0
User name :
SID name : NT AUTHORITY\SYSTEM

396 14960 NT AUTHORITY\SYSTEM S-1-5-18 (04g,20p) Primary
-> Impersonated !
* Process Token : 6752951 ADSECLAB\LukeSkywalker S-1-5-21-1581655573-3923512380-696647894-2629 (15g,25p)
Primary
* Thread Token : 6753692 NT AUTHORITY\SYSTEM S-1-5-18 (04g,20p) Impersonation (Delegation)

mimikatz(commandline) # lsadump::sam
Domain : ADSDC03
SysKey : 185e91797d952d1f4063395d1c844350
Local SID : S-1-5-21-1065499013-2304935823-602718026
SAMKey : 1f86c3e2b82a9ff24190cc5261a0a9b7

RID : 000001f4 (500)
User : Administrator
LM :
NTLM : 7c08d63a2f48f045971bc2236ed3f3ac
```

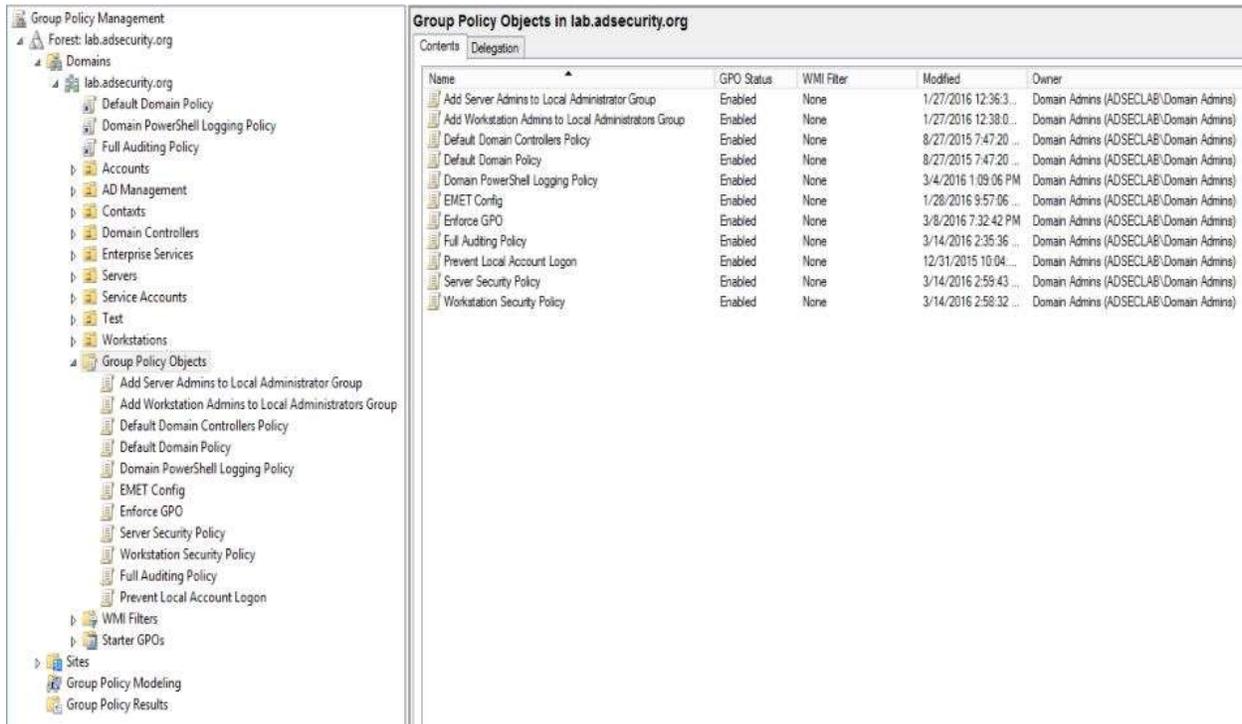
Security Note

If the DSRM password on all Domain Controllers is not changed regularly, it’s possible the domain could be compromised if the password is improperly disclosed or guessed.

See “Sneaky Active Directory Persistence #11: Directory Service Restore Mode (DSRM)” (<https://adsecurity.org/?p=1714>) for more details.

Group Policy

“Group Policy is an **infrastructure** that allows you to **implement specific configurations** for users and computers. Group Policy settings are contained in **Group Policy objects (GPOs)**, which are **linked** to the following Active Directory directory service containers: **sites, domains, or organizational units (OUs)**. The **settings within GPOs** are then **evaluated** by the affected **targets**, using the hierarchical nature of Active Directory.”



The screenshot displays the Group Policy Management console for the forest lab.adsecurity.org. The left pane shows the hierarchy of Group Policy Objects (GPOs) under the 'Group Policy Objects' container. The right pane shows a list of GPOs with columns for Name, GPO Status, WMI Filter, Modified, and Owner.

Name	GPO Status	WMI Filter	Modified	Owner
Add Server Admins to Local Administrator Group	Enabled	None	1/27/2016 12:36:3...	Domain Admins (ADSECLAB\Domain Admins)
Add Workstation Admins to Local Administrators Group	Enabled	None	1/27/2016 12:38:0...	Domain Admins (ADSECLAB\Domain Admins)
Default Domain Controllers Policy	Enabled	None	8/27/2015 7:47:20 ...	Domain Admins (ADSECLAB\Domain Admins)
Default Domain Policy	Enabled	None	8/27/2015 7:47:20 ...	Domain Admins (ADSECLAB\Domain Admins)
Domain PowerShell Logging Policy	Enabled	None	3/4/2016 1:09:06 PM	Domain Admins (ADSECLAB\Domain Admins)
EMET Config	Enabled	None	1/28/2016 9:57:06 ...	Domain Admins (ADSECLAB\Domain Admins)
Enforce GPO	Enabled	None	3/8/2016 7:32:42 PM	Domain Admins (ADSECLAB\Domain Admins)
Full Auditing Policy	Enabled	None	3/14/2016 2:35:36 ...	Domain Admins (ADSECLAB\Domain Admins)
Prevent Local Account Logon	Enabled	None	12/31/2015 10:04:...	Domain Admins (ADSECLAB\Domain Admins)
Server Security Policy	Enabled	None	3/14/2016 2:59:43 ...	Domain Admins (ADSECLAB\Domain Admins)
Workstation Security Policy	Enabled	None	3/14/2016 2:58:32 ...	Domain Admins (ADSECLAB\Domain Admins)

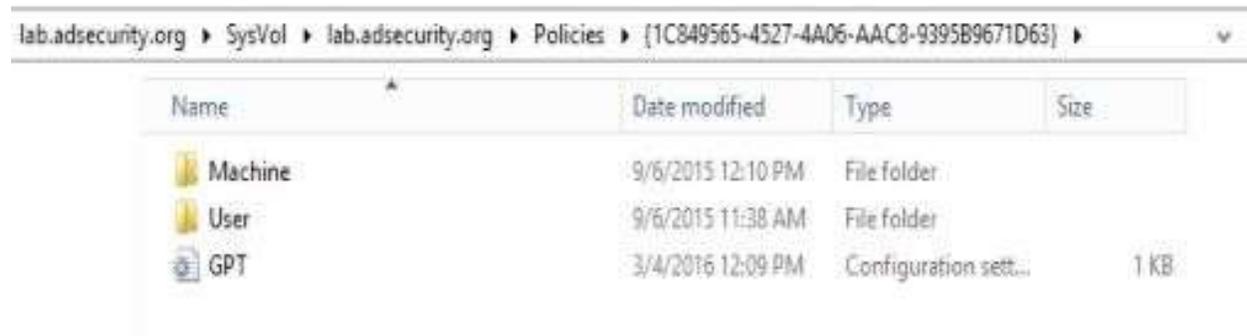
Group Policy Objects have three components: Group Policy Container (GPC) in Active Directory (<DOMAIN>, System, Policies), Group Policy Template (GPT) in SYSVOL contains the content (\\<DOMAIN>\SYSVOL\<DOMAIN>\Policies\), and Client-Side Extensions (CSEs) on client devices process GPOs.

A Group Policy can be applied to Domain, OU, or Site – typically an OU and its application can be filtered by security and/or WMI filter.

Group Policy Object AD attributes:

- displayName: The GPO's name (not the GUID)
- gPCFileSysPath: The Group Policy Template location in SYSVOL
- gPCMachExtensionNames: Client-Side Extensions (CSEs) needed by the client to process the machine-side settings in the GPO
- gPCUserExtensionNames: Client-Side Extensions (CSEs) needed by the client to process the user-side settings in the GPO
- gpLink: Configured on the AD object the Group Policy is linked to that references the GPO GUIDs linked to it.

Group Policy settings are stored in files in the SYSVOL share hosted on and replicated by all Domain Controllers in the domain.



Name	Date modified	Type	Size
Machine	9/6/2015 12:10 PM	File folder	
User	9/6/2015 11:38 AM	File folder	
GPT	3/4/2016 12:09 PM	Configuration sett...	1 KB

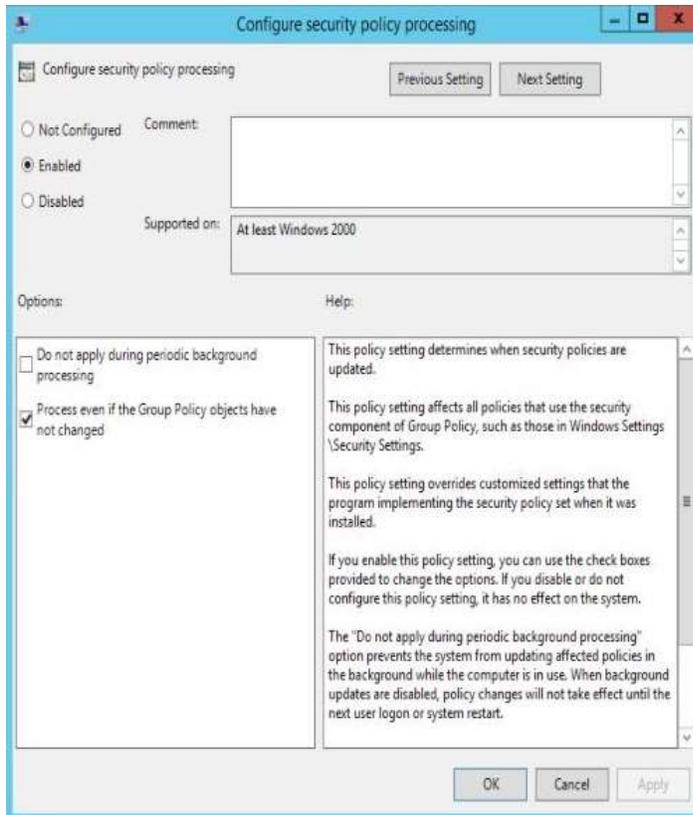
- Machine – this folder contains the machine specific settings for the GPO.
- User – this folder contains the user specific settings for the GPO.
- GPT.INI – this file contains the configuration settings for the GPO.

Group Policy Refresh Time

Group Policy “refreshes” every 90 minutes on domain member computers and on Domain Controllers every 5 minutes (by default).

Refresh does not mean reapply. By default, GPO refresh only checks the GPO for changes at which point the GPO settings are reapplied. The best practice is to modify client GPO refresh behavior to ensure GPO settings are frequently reapplied (this can be pushed out via GPO).

- *Computer Configuration, Policies, Administrative Templates, System, Group Policy, Configure security policy processing:* Enabled.
- Also check the box for “*Process even if the Group Policy objects have not changed*”



Group Policy Extensions

- **Administrative templates.** Registry-based Group Policy, used to mandate registry settings that govern the behavior & appearance of the desktop, including the operating system components & applications.
- **Security settings.** Sets security options for computers and users within the scope of a Group Policy object to define local computer, domain, and network security settings.
- **Scripts.** Automate computer startup & shutdown and user logon & logoff. Supports Microsoft Visual Basic, Scripting Edition (VBScript); JavaScript; PERL; and MS-DOS batch files (.bat and .cmd).
- **Folder redirection.** Redirect Windows special folders from their default user profile location to an alternate location on the network.

Group Policy Notes

- There are default GPOs for the domain and Domain Controllers with specific GUIDs.
- GPOs are tracked in AD by the GPO GUID, not the AD object GUID.

- The “No Override” option ensures that the settings in a Group Policy are applied even if a GPO closer to the resource has contradicting settings.

Security Note

Group Policy provides central management of security policies for users and computers. Site-linked Group Policies are not obvious in the Group Policy Management Console (GPMC) by default. These GPOs effectively cross domain boundaries and may have unintended consequences. Unused GPOs should be deleted since it's possible an admin could unintentionally link to this GPO which may have unintended consequences. Group Policy delegation should be reviewed regularly to ensure that only appropriate admin groups have modify rights. Unauthorized users with modify rights to linked GPOs could result in domain/forest compromise.

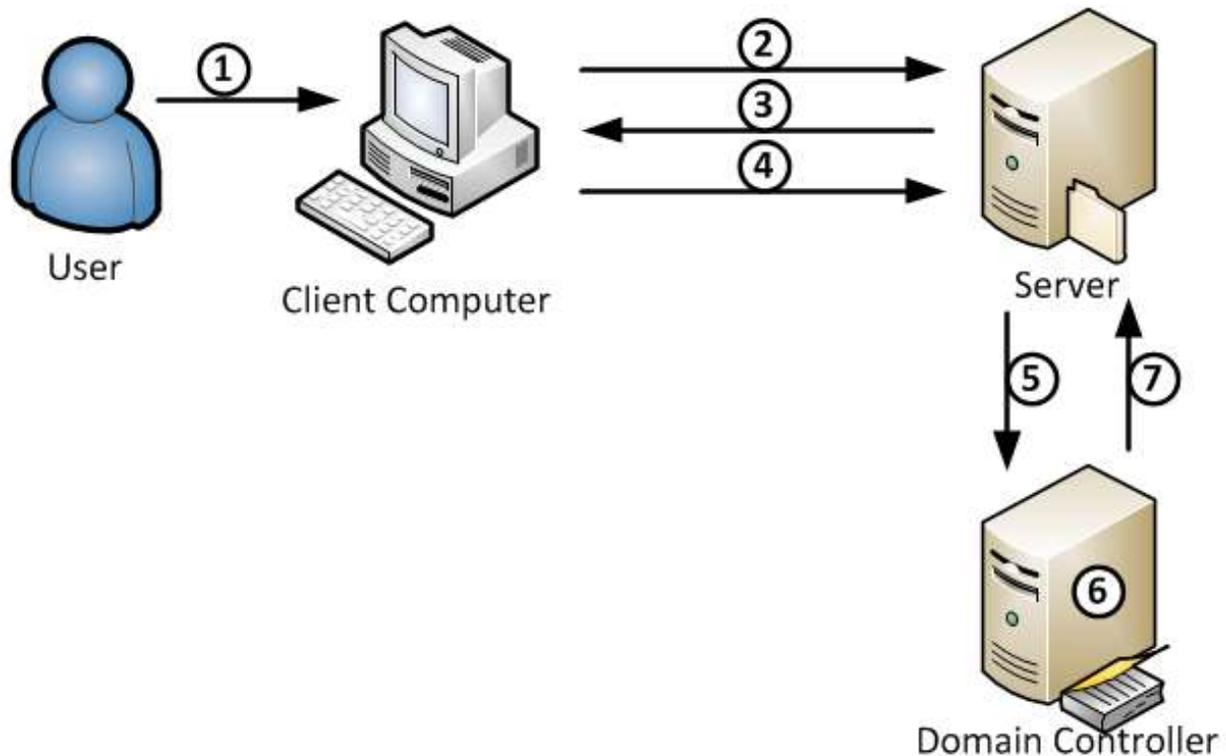
Authentication

The Evolution of Windows Authentication

Current versions of Windows still support authentication rooted in technology from the early 80s with only minor updates in later decades. However, LAN Manager authentication (LM, NTLM, NTLMv2) supported in current versions of Windows date back over 20 years! These core Windows authentication protocols have been strengthened over the years as much as possible, but they were designed during a different time when there were relatively few interconnected devices and security was a lower priority. From LM which used a very poor hashing mechanism, to NTLMv1 which greatly improved the hashing mechanism, to NTLMv2 which added improved salting to protect the password hash from being cracked. The release of Active Directory in the year 2000 officially brought MIT's Kerberos to the Windows world. Kerberos became the default authentication protocol for Active Directory with some Microsoft additions to the protocol for compatibility reasons. Issues with Microsoft's Kerberos implementation continue to be highlighted including methods of forging Kerberos tickets once specific password data is exposed (ex. Golden and Silver tickets), as well as Kerberoast offline password cracking using only Kerberos TGS service tickets.

Microsoft recognized the issues with Windows and the issues inherent with legacy Windows authentication methods thanks to tools such as Mimikatz which makes password dumping from Windows systems trivial (with the appropriate access). The next generation of Windows authentication is called Microsoft Passport. Microsoft Passport involves a user logging onto the Windows 10 computer with multi-factor (PIN, face, iris, fingerprint, etc) and either creating a new account or associating an existing account with an Identity Provider (IDP). Windows generates a public/private key pair with the private key stored securely outside of the Windows 10 OS, typically in a Trusted Platform Module (TPM). The public key is associated with the account so that a challenge can be sent that can only correctly respond to the IDP. Another key point to the Microsoft Passport credential system is that the user needs to enroll every device used to access the service (IDP). Since Passport is a key feature being released with Windows Server 2016 (currently in tech preview or "beta"), though Windows 10 supports it at release, there isn't much information available on how it actually works such as the key implementation details.

NTLM



Challenge/Response authentication

1. User logs onto workstation & password is converted to password hash.
2. User initiates connection to server with NTLM Authentication.
3. Server responds with challenge data.
4. Client encrypts the challenge data using the password hash & sends to server.
5. Sever forwards user name, challenge, & client challenge response to DC.
6. DC looks up user name and uses the user's password data to encrypt the challenge. If the result is the same, the DC tells the server authentication is good.

NTLM Scenarios:

- Outlook and Exchange use NTLM authentication extensively.
- NTLM auth forced when connecting to system via IP address.

NTLM Attacks:

- SMB Relay - simulate SMB server or relay to attacker system.
- Intranet HTTP NTLM auth – Relay to Rogue Server
- NBNS/LLMNR – respond to NetBIOS broadcasts
- HTTP -> SMB NTLM Relay

- WPAD (network proxy)
- ZackAttack
- Pass the Hash (PtH)

Security Note

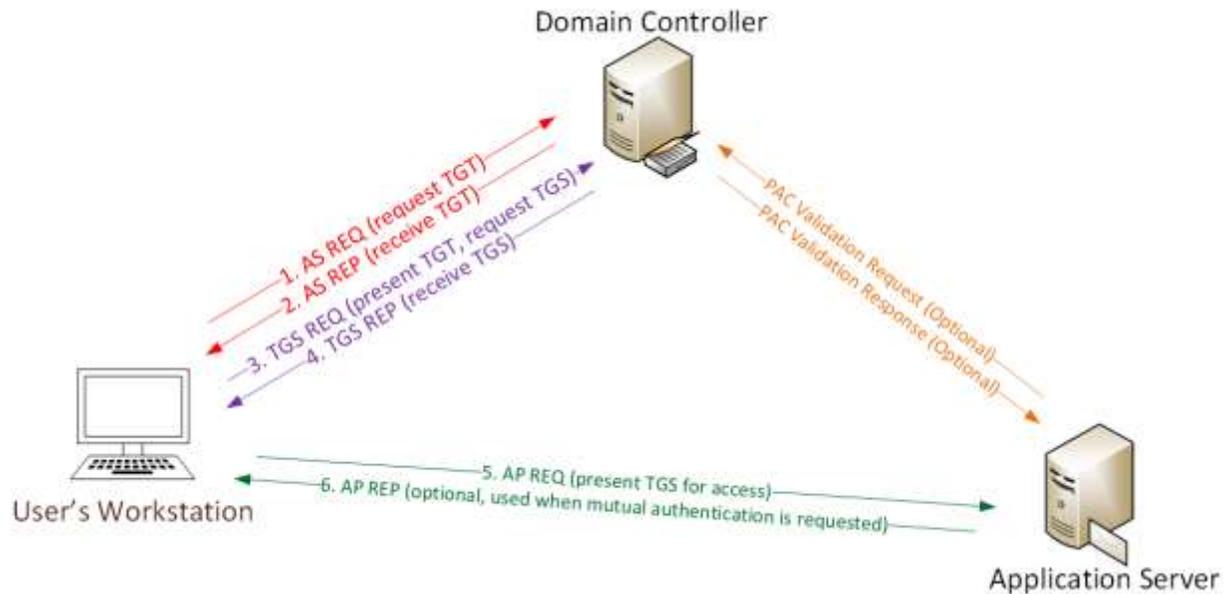
Any LM/NTLMv1 authentication should be removed from the environment. Audit NTLM authentication (<https://technet.microsoft.com/en-us/library/jj865672%28v=ws.10%29.aspx>) and work to disable it where possible.

Kerberos

Kerberos communication within a domain is pretty straightforward – the domain Kerberos service account is used to sign and encrypt every authentication ticket (TGT). This enables the TGT to be used throughout the domain and presented to any DC in the domain. This works since the Kerberos service account ([KRBTGT](#)) is effectively the trust anchor used for the domain and is why losing control of the KRBTGT account password hash equates to losing control of the domain.

When a user authenticates to Active Directory, the authenticating Domain Controller creates a TGT (authentication ticket) for the user that contains the groups the user is a member of (including groups from other domains in the forest, such as universal groups), signs, and encrypts the ticket using the KRBTGT password hash. When presented later to the DC for a service ticket (TGS), the TGT ticket and its contents are validated. The DC effectively copies the contents of the TGT into a TGS (service ticket) that the user presents to the target service. One component of the TGS is encrypted with the target service's password hash and the other with the user's password hash. If the target service can open the TGS, it is accepted. This means that the user's TGT can be reused to get service tickets during the TGT's lifetime (10 hours by default). The TGT is also portable, so if an attacker can steal a user's TGT, it can be reused on any other computer on the network, at the same time, to access any resource to which the user has access.

When an attacker gains access to the KRBTGT password hash on the domain, it is possible for them to generate their own TGTs (called "Golden Tickets") that are accepted by all the Domain Controllers in the domain since they are signed and encrypted with the domain Kerberos service account data. Simply put, a Golden Ticket is a valid TGT.

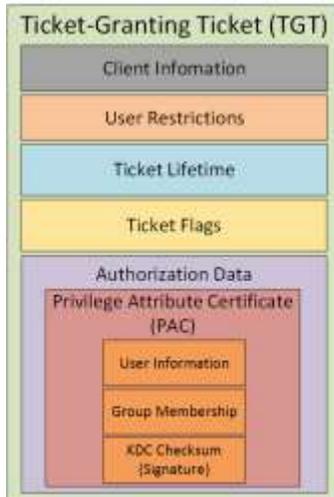


Kerberos TGT (Authentication or Logon Ticket) Process

1. User logs onto the workstation with Domain credentials.
2. The user's password is converted to several hash types: NTLM and AES (Windows 7 and newer).
3. AS-REQ: Authentication request sent to Domain Controller.
4. AS-REP: The KDC verifies Authentication Data and replies with TGT.

TGT format (TGS is similar):

- Client information – workstation FQDN & IP address
- User Restrictions – logon schedule, workstation restrictions, etc.
- Domain Kerberos Policy - Ticket Lifetime (Default: 10 hour lifetime & 7 day max)
- Ticket Flags – Encryption, ticket type (impersonation, can it be delegated, etc)
- Auth Data - PAC
 - User Info: User name, user SID, profile info, etc
 - Group Membership: Group RIDs
 - PAC Signature



Kerberos TGS (Service Ticket) Process

1. TGS-REQ: Client sends the TGT to the DC requesting a TGS for a specific service.
2. Domain Controller validates the TGT by opening & validate checksum.
3. DC looks up the Service Principal name for the Kerberos service in the TGS-REQ and identifies the associated Service Account.
4. The DC creates a TGS ticket based on data in the TGT and encrypts it with the Service Account password hash.
5. TGS-REP: DC sends the TGS to the client.

Note that a TGS has a server component & user component.

Kerberos Key Points

- NTLM password hash for Kerberos RC4 encryption.
- Logon Ticket (TGT) provides user auth to DC.
- Kerberos policy only checked when TGT is created.
- DC validates user account only when TGT > 20 mins.
- Service Ticket (TGS) PAC validation is optional & rare.
 - Server LSASS sends PAC Validation request to DC's netlogon service (NRPC).
 - If it runs as a service, PAC validation is optional (disabled)

- If a service runs as System, it performs server signature verification on the PAC (computer account long-term key).
- Microsoft uses the NTLM password hash for Kerberos RC4 encryption.
- Kerberos policy is only checked when the TGT is created & the TGT is the user authenticator to the DC.
- The DC only checks the user account after the TGT is 20 minutes old to verify the account is valid or enabled. TGS PAC Validation only occurs in specific circumstances. When it does, LSASS on the server sends the PAC Validation request to the DC's netlogon service (using NRPC)
- If it runs as a service, PAC validation is optional (disabled). If a service runs as System, it performs server signature verification on the PAC (computer account long-term key).

Kerberos Attacks

There are several attacks against Kerberos that have been discussed over the years, including:

- Replay Attack (<http://windowsitpro.com/active-directory/understanding-how-kerberos-authentication-protects-against-replay-attacks>)
- Offline Password Cracking ([https://files.sans.org/summit/hackfest2014/PDFs/Kicking%20the%20Guard%20Dog%20of%20Hades%20-%20Attacking%20Microsoft%20Kerberos%20-%20Tim%20Medin\(1\).pdf](https://files.sans.org/summit/hackfest2014/PDFs/Kicking%20the%20Guard%20Dog%20of%20Hades%20-%20Attacking%20Microsoft%20Kerberos%20-%20Tim%20Medin(1).pdf))
- Forged Tickets - Golden/Silver (<https://adsecurity.org/?p=1515>)
- Pass the Ticket (<http://www.slideshare.net/gentilkiwi/abusing-microsoft-kerberos-sorry-you-guys-dont-get-it>)
- Over-pass the hash or pass the key (<http://blog.gentilkiwi.com/securite/mimikatz/overpass-the-hash> or <https://adsecurity.org/?p=556>)

Security Note

While there can be issues with Kerberos in the standard Active Directory deployment, these issues can be mitigated through proper security deployment in Active Directory (primarily by limiting and protecting admins and ensuring service accounts have long, complex passwords). Kerberos improves on NTLM in several ways, but still has limitations, especially surrounding encryption protocols and their weaknesses.

Kerberos References

- <https://technet.microsoft.com/en-us/library/cc961966.aspx>
- <https://msdn.microsoft.com/en-us/library/cc237937.aspx>
- <http://blogs.msdn.com/b/openspecification/archive/2009/04/24/understanding-microsoft-kerberos-pac-validation.aspx>
- <https://msdn.microsoft.com/en-us/library/dd240254.aspx>
- <https://msdn.microsoft.com/en-us/library/cc233952.aspx>
- <https://msdn.microsoft.com/en-us/library/cc233891.aspx>

- <https://msdn.microsoft.com/en-us/library/cc233896.aspx>

Active Directory Administration Groups

Default Groups & Permissions: DC Rights

Often delegation is performed by adding groups and accounts to the default admin groups in the domain without fully understanding the ramifications.

Administrators

- Full administrative rights to the domain and the Domain Controller.

Domain Admins

- Member of the Administrators group in the domain.
- Member of the local Administrators group on every computer in the domain (when joined to the domain).

Enterprise Admins (Forest Root Domain only)

- Member of every domain's Administrators group in the forest.

Server Operators

- Effectively "administrator" on Domain Controllers.

Account Operators

- Create/delete/modify users, groups, and computers in the domain (except admins).
- Logon & shut down Domain Controllers

Backup Operators

- Backup & restore Domain Controllers regardless of permissions
- Logon & shut down Domain Controllers

Print Operators

- Manage, create, share, & delete printers connected to domain controllers in the domain
- Load & unload device drivers on Domain Controllers

Logon & shut down Domain Controllers

- Remote Desktop Users
- Remotely log on to Domain Controllers

Group Policy Creator Owners

- Members of this group can modify Group Policy in the domain.

DNS Admins

- Administrative access to the DNS Server service

Schema Admins (Forest Root Domain only)

- Members of this group can modify the Active Directory schema.

Groups with AD admin rights

- Domain Admins
- Enterprise Admins
- Domain “Administrators”
- Groups with DC logon rights

Groups with DC Logon Rights (default)

- Account Operators
- Backup Operators
- Print Operators
- Remote Desktop Users
- Server Operators

Active Directory Security Groups:

[https://technet.microsoft.com/en-us/library/dn579255\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/dn579255(v=ws.11).aspx)

Security Note

Leveraging default AD groups to delegate rights can be a quick way to provide necessary admin rights, but it is also an easy way to over-permission Active Directory to many more people than desired (and necessary).

AD Security Enhancements by OS

Forest and Domain Functional Level Security Enhancements

There are a number of security features and enhancements available with each release of Windows Server. These are documented here to provide a potential roadmap to move towards.

Domain Functional Level	Available Features
Windows 2000 Native	<ul style="list-style-type: none"> • Universal groups (distribution & security groups) • Group Nesting • Group conversion between security & distribution groups • Security Identifier History (SIDHistory)
Windows 2003 Server	<ul style="list-style-type: none"> • Domain Controller rename functionality • Logon time stamp updates (LastLogonTimestamp) • Ability to set "UserPassword" attribute as the effective password on inetOrgPerson & user objects. • Ability to redirect new objects to locations other than the Users & Computers containers • Ability for Authorization Manager to store authorization policies in AD. • Constrained delegation • Selective Authentication on AD Forest trusts.
Windows Server 2008	<ul style="list-style-type: none"> • Distributed File System (DFS) replication support for SYSVOL. • Domain-based DFS namespaces in Windows Server 2008 Mode. • Advanced Encryption Standard (AES 128 & AES 256) support for Kerberos. • Last interactive logon information • Fine-grained password policies • Personal Virtual Desktops
Windows Server 2008 R2	<ul style="list-style-type: none"> • Authentication mechanism assurance which identifies logon method type (smart card or user name/password). • Automatic SPN management for services running under context of a Managed Service Account.
Windows Server 2012	<ul style="list-style-type: none"> • "KDS support for claims, compound authentication, and Kerberos armoring" contains two settings that require Windows Server 2012 DFL: Always provide claims & Fail unarmored authentication requests.
Windows Server 2012 R2	<ul style="list-style-type: none"> • DC-side protections for Protected Users. Protected User authentication no longer allows: <ul style="list-style-type: none"> ○ NTLM authentication ○ Kerberos DES or RC4 cipher suites in pre-authentication ○ Delegation – either unconstrained or constrained delegation. ○ Renew user tickets (TGTs) beyond the initial 4 hour lifetime • Authentication Policies • Authentication Policy Silos
Windows Server 2016	TBD

Forest Functional Level	Available Features
Windows 2000 Native	
Windows 2003 Server	<ul style="list-style-type: none"> • Forest trust • Domain rename • Linked-value replication • Ability to deploy a Read-Only Domain Controller (RODC)

	<ul style="list-style-type: none"> • Improved Knowledge Consistency Checker (KCC) algorithms and scalability. • Ability to create instances of the dynamic auxiliary class named dynamicObject in a domain directory partition • Ability to convert an inetOrgPerson object into a User object and vice versa. • Ability to create instances of new group types to support role-based authorization. • Deactivation and redefinition of attributes and classes in the schema. The following attributes can be reused: ldapDisplayName, schemaIdGuid, OID, and mailID. • Domain-based DFS namespaces running in Windows Server 2008 Mode
Windows Server 2008	
Windows Server 2008 R2	<ul style="list-style-type: none"> • Active Directory Recycle Bin (requires enabling)
Windows Server 2012	
Windows Server 2012 R2	
Windows Server 2016	TBD

Windows 2008 R2 Forest/Domain Mode Features

- Kerberos AES support (128 & 256 bit keys)*
- Fine Grained Password Policy*
- Managed Service Accounts
- Authentication Mechanism Assurance
- Offline Domain Join
- Audit / Restrict NTLM Authentication

* - starting with Windows 2008.

New AD Features: Windows Server 2012

- Constrained Delegation across Domain/Forest
- Group Managed Service Accounts
- Compound Authentication & Kerberos FAST (Kerberos Armoring)
- Dynamic Access Control (attribute-based access)

Key AD Security Features: 2012 R2

- LSA Protection
- "Protected Users" Security Group
- Protected Users Host/Domain Protection
- Authentication Policies & Silos
- Forest boundary enforcement for Kerberos Delegation

Security Note

Moving all Domain Controllers up to the latest version of Windows provides security enhancements that are well worth the resources required to make the move. Domain Controllers are critical infrastructure and needs the latest security available in the platform to properly protect them and Active directory (since the DC operating system determines what security features AD has).

Windows 10 - New & Updated Auditing

- Added a default process SACL to LSASS.exe (Mimikatz logging)
 - Advanced Audit Policy Configuration\Object Access\Audit Kernel Object
- New Security Account Manager read (enumeration) events
 - Event ID 4798 & 4799
- New Audit Subcategories
 - Group Membership query
- New fields in the logon event
 - MachineLogon (Y/N)
 - ElevatedToken (Y/N)
 - RestrictedAdminMode (Y/N)
 - GroupMembership

What's new in Windows 10 auditing

<https://technet.microsoft.com/en-us/itpro/windows/whats-new/security-auditing>

Active Directory Security Best Practices

General Recommendations

- Manage local Administrator passwords (LAPS).
- Implement RDP Restricted Admin mode (as needed).
- Remove unsupported OSs from the network.
- Monitor scheduled tasks on sensitive systems (DCs, etc).
- Ensure that OOB management passwords (DSRM) are changed regularly & securely stored.
- Use SMB v2/v3+
- Default domain Administrator & KRBTGT password should be changed every year & when an AD admin leaves.
- Remove trusts that are no longer necessary & enable SID filtering as appropriate.
- All domain authentication should be set (when possible) to:
"Send NTLMv2 response only\refuse LM & NTLM."
- Audit NTLM use and restrict where possible ([https://technet.microsoft.com/en-us/library/jj865674\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/jj865674(v=ws.10).aspx)).
- Block internet access for DCs, servers, & all administration systems.
- Disable NetBIOS over TCPIP and turn off multicast name resolution (LLMNR).
(<https://www.trustwave.com/Resources/SpiderLabs-Blog/Top-Five-Ways-SpiderLabs-Got-Domain-Admin-on-Your-Internal-Network/> & <http://www.viopoint.com/so-simple-but-so-effective/>)

Protect Admin Credentials

- No "user" or computer accounts in admin groups.
- Ensure all admin accounts are "sensitive & cannot be delegated".
- Add all admin accounts to "Protected Users" group (requires Windows Server 2012 R2 Domain Controllers).
- Disable all inactive admin accounts and remove from privileged groups.
- Limit AD admin membership (DA, EA, Schema Admins, etc.) & only use custom delegation groups.
- 'Tiered' Administration mitigating credential theft impact.
- Ensure admins only logon to approved admin workstations & servers.
- Leverage time-based, temporary group membership for all admin accounts.

Protect Service Account Credentials

- Limit to systems of the same security level.
- Leverage "(Group) Managed Service Accounts" (or pw >20 characters) to mitigate credential theft (kerberoast).
- Implement FGPP (DFL =>2008) to increase PW requirements for SAs and administrators.
- Logon restrictions - prevent interactive logon & limit logon capability to specific computers.
- Disable inactive SAs & remove from privileged groups.

Protect Resources

- Segment network to protect admin & critical systems.
- Deploy IDS to monitor the internal corporate network.
- Network device & OOB management on separate network.

Protect Domain Controllers

- Only run software & services to support AD.
- Minimal groups (& users) with DC admin/logon rights.
- Ensure patches are applied before running DCPromo (especially MS14-068 and other critical patches).
- Validate scheduled tasks & scripts.

Protect Workstations (& Servers)

- Patch quickly, especially privilege escalation vulnerabilities.
- Deploy security back-port patch (KB2871997).
- Set Reg key to 0 (KB2871997 / Windows 8.1/2012R2 and newer):
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\Wdigest
- Deploy workstation whitelisting (Microsoft AppLocker) to block code exec in user folders - home directory & profile path.
- Deploy workstation application sandboxing technology (EMET) to mitigate application memory exploits (0-days).

Logging

- SIEM or equivalent to centralize as much log data as possible.
- User Behavioral Analysis system for enhanced knowledge of user activity (such as Microsoft ATA).
- Enable enhanced auditing:
- "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings"
- Enable PowerShell module logging ("*") & forward logs to central log server (WEF or other method).
- Enable CMD Process logging & enhancement (KB3004375) and forward logs to central log server.

Interesting AD Facts

All Authenticated Users have read access to:

- Most (all) objects & their attributes in AD (even across trusts!).
- Most (all) contents in the domain share “SYSVOL” which can contain interesting scripts & files.

A standard user account can:

- Have elevated rights through the magic of “SID History” without being a member of any groups.
- Have the ability to modify users/groups without elevated rights through custom OU permissions.
- Compromise an entire AD domain simply by improperly being granted modify rights to an OU or domain-linked GPO.

A Security Pro’s AD Checklist

- ✓ Identify who has AD admin rights (domain/forest).
- ✓ Identify who can logon to Domain Controllers (& admin rights to virtual environment hosting virtual DCs).
- ✓ Scan Active Directory Domains, OUs, AdminSDHolder, & GPOs for inappropriate custom permissions.
- ✓ Ensure AD admins (aka Domain Admins) protect their credentials by not logging into untrusted systems (workstations).
- ✓ Limit service account rights that are currently DA (or equivalent).

Recommended Domain Controller Event Logging

Event Item	Recommendation
Account Logon: Audit Credential Validation	Success and Failure
Account Logon: Audit Kerberos Authentication Service	Success and Failure
Account Logon: Audit Kerberos Service Ticket Operations	Success and Failure
Account Logon: Audit Other Account Logon Events	Success and Failure
Account Management: Audit Application Group Management	No Auditing
Account Management: Audit Computer Account Management	Success and Failure
Account Management: Audit Distribution Group Management	No Auditing
Account Management: Audit Other Account Management Events	Success and Failure
Account Management: Audit Security Group Management	Success and Failure
Account Management: Audit User Account Management	Success and Failure
Detailed Tracking: Audit DPAPI Activity	Success and Failure
Detailed Tracking: Audit Process Creation	Success and Failure
Detailed Tracking: Audit Process Termination	No Auditing
Detailed Tracking: Audit RPC Events	No Auditing
DS Access: Audit Detailed Directory Service Replication	No Auditing
DS Access: Audit Directory Service Access	Success and Failure
DS Access: Audit Directory Service Changes	Success and Failure
DS Access: Audit Directory Service Replication	No Auditing
Logon/Logoff: Audit Account Lockout	Success
Logon/Logoff: Audit User/Device Claims	No Auditing
Logon/Logoff: Audit IPsec Extended Mode	No Auditing
Logon/Logoff: Audit IPsec Main Mode	Success and Failure
Logon/Logoff: Audit IPsec Quick Mode	No Auditing
Logon/Logoff: Audit Logoff	Success
Logon/Logoff: Audit Logon	Success and Failure
Logon/Logoff: Audit Network Policy Server	No Auditing
Logon/Logoff: Audit Other Logon/Logoff Events	Success and Failure
Logon/Logoff: Audit Special Logon	Success and Failure
Object Access: Audit Application Generated	No Auditing
Object Access: Audit Certification Services	No Auditing
Object Access: Audit Detailed File Share	No Auditing
Object Access: Audit File Share	No Auditing
Object Access: Audit File System	Failure
Object Access: Audit Filtering Platform Connection	No Auditing
Object Access: Audit Filtering Platform Packet Drop	No Auditing
Object Access: Audit Handle Manipulation	No Auditing
Object Access: Audit Kernel Object	No Auditing
Object Access: Audit Other Object Access Events	No Auditing
Object Access: Audit Registry	Failure

Object Access: Audit Removable Storage	No Auditing
Object Access: Audit SAM	No Auditing
Object Access: Audit Central Access Policy Staging	No Auditing
Policy Change: Audit Audit Policy Change	Success and Failure
Policy Change: Audit Authentication Policy Change	Success and Failure
Policy Change: Audit Authorization Policy Change	No Auditing
Policy Change: Audit Filtering Platform Policy Change	No Auditing
Policy Change: Audit MPSSVC Rule-Level Policy Change	Success
Policy Change: Audit Other Policy Change Events	No Auditing
Privilege Use: Audit Non-Sensitive Privilege Use	No Auditing
Privilege Use: Audit Sensitive Privilege Use	Success and Failure
Privilege Use: Audit Other Privilege Use Events	No Auditing
System: Audit IPSec Driver	Success and Failure
System: Audit Other System Events	No Auditing
System: Audit Security State Change	Success and Failure
System: Audit Security System Extension	Success and Failure
System: Audit System Integrity	Success and Failure
Global Object Access Auditing: File System (Global Object Access Auditing)	
Global Object Access Auditing: Registry (Global Object Access Auditing)	

Security Auditing Recommendations

<https://technet.microsoft.com/en-us/windows-server-docs/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations>

References

- Securing Active Directory – An Overview of Best Practices
<https://technet.microsoft.com/en-us/library/dn205220.aspx>
- Understanding Trusts
[https://technet.microsoft.com/en-us/library/cc736874\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc736874(v=ws.10).aspx)
- Active Directory Domains and Trusts
<https://technet.microsoft.com/en-us/library/cc770299.aspx>
- Trust Types
[https://technet.microsoft.com/en-us/library/cc775736\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc775736(v=ws.10).aspx)
- Active Directory Replication Overview
<https://technet.microsoft.com/en-us/library/cc961788.aspx>
- How Active Directory Replication Topology Works
[https://technet.microsoft.com/en-us/library/cc755994\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc755994(v=ws.10).aspx)
- How the Active Directory Replication Model Works
[https://technet.microsoft.com/en-us/library/cc772726\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc772726(v=ws.10).aspx)
- Group Policy Basics
http://blogs.technet.com/b/musings_of_a_technical_tam/archive/2012/02/13/understanding-the-structure-of-a-group-policy-object.aspx
- Optimizing Group Policy Performance
<https://technet.microsoft.com/en-us/magazine/2008.01.gpperf.aspx>
- Organizational Units
[https://technet.microsoft.com/en-us/library/cc758565\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc758565(v=ws.10).aspx)
- Organizational Unit Design
<http://www.windowsnetworking.com/articles-tutorials/windows-server-2008/Crash-Course-Active-Directory-Organizational-Unit-Design.html>
- How DNS Support for Active Directory Works
[https://technet.microsoft.com/en-us/library/cc759550\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc759550(v=ws.10).aspx)
- Active Directory-Integrated DNS
<https://technet.microsoft.com/en-us/library/cc978010.aspx>

- Understanding DNS Zone Replication in Active Directory Domain Services
<https://technet.microsoft.com/en-us/library/cc772101.aspx>
- What is an RODC?
[https://technet.microsoft.com/en-us/library/cc771030\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc771030(v=ws.10).aspx)
- AD DS: Read-Only Domain Controllers
[https://technet.microsoft.com/en-us/library/cc732801\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc732801(v=ws.10).aspx)
- Read-Only Domain Controllers Step-by-Step Guide
[https://technet.microsoft.com/en-us/library/cc772234\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc772234(v=ws.10).aspx)
- Service Principal Names (SPNs) Overview
[https://msdn.microsoft.com/en-us/library/ms677949\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/ms677949(v=vs.85).aspx)
<https://technet.microsoft.com/en-us/library/cc961723.aspx>
<http://blogs.technet.com/b/qzaidi/archive/2010/10/12/quickly-explained-service-principal-name-registration-duplication.aspx>
- Register a Service Principal Name for Kerberos Connections
<https://msdn.microsoft.com/en-us/library/ms191153.aspx>
- What's new in Windows 10 auditing
<https://technet.microsoft.com/en-us/itpro/windows/whats-new/security-auditing>
- Security Auditing Recommendations
<https://technet.microsoft.com/en-us/windows-server-docs/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations>
- Active Directory Security Groups:
[https://technet.microsoft.com/en-us/library/dn579255\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/dn579255(v=ws.11).aspx)
- Active Directory Reading Library
https://adsecurity.org/?page_id=41
- Read-Only Domain Controller (RODC) Information
<https://adsecurity.org/?p=274>
- Active Directory Recon Without Admin Rights
<https://adsecurity.org/?p=2535>
- Mining Active Directory Service Principal Names
<http://adsecurity.org/?p=230>
- SPN Directory:
http://adsecurity.org/?page_id=183

- Will Schroeder (@harmj0y): I have the PowerView (Offensive Active Directory PowerShell) Presentation
<http://www.slideshare.net/harmj0y/i-have-the-powerview>
- MS14-068: Vulnerability in (Active Directory) Kerberos Could Allow Elevation of Privilege
<http://adsecurity.org/?tag=ms14068>
- Microsoft Enhanced security patch KB2871997
<http://adsecurity.org/?p=559>
- Tim Medin's DerbyCon 2014 presentation: "Attacking Microsoft Kerberos: Kicking the Guard Dog of Hades"
<https://www.youtube.com/watch?v=PUyhIN-E5MU>
- Microsoft: Securing Privileged Access Reference Material
<https://technet.microsoft.com/en-us/library/mt631193.aspx>
- Mimikatz
https://adsecurity.org/?page_id=1821
- Attack Methods for Gaining Domain Admin Rights in Active Directory
<https://adsecurity.org/?p=2362>
- Microsoft Local Administrator Password Solution (LAPS)
<https://adsecurity.org/?p=1790>
- The Most Common Active Directory Security Issues and What You Can Do to Fix Them
<https://adsecurity.org/?p=1684>
- How Attackers Dump Active Directory Database Credentials
<https://adsecurity.org/?p=2398>
- Sneaky Active Directory Persistence Tricks
<https://adsecurity.org/?p=1929>