

ACTIVE DIRECTORY DELEGATION SECURITY.

Delegation is how Active Directory hands power to someone else: rights over objects through access control lists, and the ability to act as a user through Kerberos. **Both live in attributes rather than group memberships, and attackers hunt them because few teams review them.**

- ROLES, NOT PEOPLE
- OU-SCOPED RIGHTS
- NO UNCONSTRAINED DELEGATION
- AUDIT THE ACLS

01 THE MECHANISM

Two Kinds of Delegation

Administrative delegation grants a group rights over the objects in an OU, down to a single attribute. Kerberos delegation lets a service obtain tickets on behalf of a user who authenticated to it. **Both hand one principal another's power, and both are stored where anyone can read them.** [05] [01]

Rights Hide in ACLs, Not Groups

Every directory object carries a security descriptor whose DACL lists ACEs granting or denying rights to a trustee, inherited down the tree. Granting the right to create an object implicitly grants control of everything created. **Group membership gets reviewed; ACEs seldom do.** [10] [05]

Impersonation Is a Setting

A host trusted for unconstrained delegation receives users' TGTs and can act as them anywhere; constrained delegation limits the target services; resource-based delegation moves the decision to the resource owner. **Unsecure delegation lets a server be you to whatever it chooses.** [01] [06]

02 THE FLOW

Delegate Administration

DESIGN

1

Model roles: create a group per administrative role, place the objects it manages in an OU, and delegate to the group, never to a person. Leave the default containers with the service administrators and delegate only new OUs to data administrators. [05] [02]

2

Grant narrowly: the forest owner sets the level, from full control of an OU down to a single attribute of one object type, such as resetting passwords. Make rights inheritable deliberately, and remember that a container right cascades to everything placed inside. [05]

3

Fence the control plane: domain controllers, identity systems and whatever controls them form Tier 0. Enterprise, Domain and built-in Administrators are equally powerful; keep them minimal or temporarily populated, used only on domain controllers or secure administrative hosts. [08] [02] [11]

Delegate Identity

OPERATE

1

Constrain every service: replace unconstrained delegation with "specified services only" or resource-based constrained delegation, where the resource owner lists the front ends allowed to impersonate to it (PrincipalsAllowedToDelegateToAccount), even across domains. [01] [06]

2

Flag the sensitive: set "Account is sensitive and cannot be delegated" on Domain and Enterprise Admins and privileged service accounts, and put administrative users in Protected Users: no NTLM, no RC4 or DES, no delegation, four-hour TGTs. Never add service or computer accounts. [02] [06] [04]

3

Audit what delegation touches: who holds Replicating Directory Changes All, who has WriteDACL on sensitive groups, which non-default ACEs sit on AdminSDHolder, and which non-domain-controller entities are trusted for delegation. Posture tools list the exposed entities. [06] [07] [03]

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
Scope	Rights delegated to role groups at the OU where the objects live, inheritable by design, with the default containers left to service administrators.
Guardrails	AdminSDHolder is the permission template for protected accounts and groups; SDProp re-stamps it onto them every 60 minutes with inheritance disabled.
Kerberos Boundaries	No unconstrained delegation; constrained or resource-based lists only; sensitive flag and Protected Users for accounts that must never be impersonated.
Visibility	Replication rights, WriteDACL on sensitive groups, AdminSDHolder ACEs and delegation attributes reviewed on a schedule, with exposed entities tracked to closure.

04 DELEGATION PATHS COMPARED

DELEGATION PATH	BOUNDED?	WHAT IT EXPOSES
Unconstrained Delegation	No	The host caches every authenticating user's TGT; a compromised front end impersonates them to any service, including an admin to a domain controller.
Constrained Delegation (Front End Lists Targets)	Yes	Bounded to the listed services, but a sensitive target on the list is exposed; needs domain admin to configure and stays within one domain.
Resource-Based Constrained Delegation	Yes	The resource owner lists who may impersonate to it, across domains; protocol transition is always allowed, so ACLs should check the S-1-18-2 SID.
Delegated Rights on an OU	Yes	Bounded to the OU and the rights granted, but create rights imply full control of what is created and inheritance carries it down the tree.
Sensitive Flag and Protected Users	Yes	The account cannot be delegated at all; in Protected Users it also loses NTLM, RC4 and long tickets. Not for service or computer accounts.

AD DELEGATION SECURITY.

SCOPE · CONSTRAIN · AUDIT

05 PROGRAM OPERATIONS

Delegate to roles, never to people.

Implement role-based access as AD groups with rights delegated per OU; existing groups fit some roles (DNS zone management is Microsoft’s example), others need new groups. Document every delegation so a permission review can tell intent from drift. [02] [05]

Keep the top tier tiny and separate.

Enterprise, Domain and built-in Administrators must be treated as equally powerful because a member of one can join the other two. Reduce them to the fewest accounts, consider temporary membership, and never let them log on to lower-plane systems. [02] [11] [08]

Hunt dangerous ACEs on a schedule.

Replicating Directory Changes All on the domain head for anything but domain controllers means DCSync; WriteDACL on a sensitive group means self-granted control; a stray ACE on AdminSDHolder is re-applied to every protected object hourly. [07] [09] [06] [03]

Retire unconstrained delegation.

Find non-domain-controller entities trusted for delegation, switch them to specified services or resource-based lists, flag privileged accounts sensitive, and give administrators AES keys before adding them to Protected Users. [06] [01] [04]

06 CONTROL MAPPING

ATT&CK

T1003.006 OS Credential Dumping: DCSync abuses the Directory Replication Service to pull password data; mitigation M1015 manages the ACL for Replicating Directory Changes and related replication permissions; detection watches replication requests from non-domain-controller endpoints. [07] [09]

MICROSOFT GUIDANCE

Least-privilege administrative models: role groups with delegated rights, the sensitive flag on Administrator accounts, and restrictions on the EA, DA and BA groups; Avenues to Compromise names excessive membership in those groups as the most common misconfiguration. [02] [11]

JOINT GOVERNMENT GUIDANCE

Detecting and Mitigating Active Directory Compromises (ASD, CISA, NSA, CCCS, NCSC-UK, NCSC-NZ) covers the 17 most common compromise techniques, unconstrained delegation and DCSync among them, with detection and mitigation per technique. [12]

POSTURE ASSESSMENTS

Defender for Identity flags insecure Kerberos delegation, non-admin accounts with DCSync permissions, non-default AdminSDHolder rights, WriteDACL on sensitive groups, privileged accounts without the sensitive flag, and accounts in built-in operator groups. [06]

07 WHAT THIS DOES NOT SOLVE

Rights You Never Granted

Nested groups, primaryGroupId and SID History give access no ACL review shows. **Audit effective access, not ACEs alone.** [06]

The Application Itself

Delegation trusts the front end to behave; even resource-based delegation fails if that entity is sensitive. **Harden the host.** [06] [01]

The Cloud Half

One account privileged in both Entra ID and AD bridges the planes. **Split the roles.** [06] [08]

A Poisoned Template

SDProp enforces whatever AdminSDHolder says, so a planted ACE persists hourly. **Baseline and diff it.** [03] [06]

08 MYTHS VS. REALITY

MYTH	REALITY
“Administrators is less privileged than Domain Admins.”	The three top groups are equally powerful; a member of one can join the other two. [02]
MYTH	REALITY
“Constrained delegation makes a service safe.”	Constrained entities are abusable when any listed target is sensitive ; a compromised front end still cascades. [06] [01]
MYTH	REALITY
“Only Domain Admins can DCSync.”	Any principal holding Replicating Directory Changes All can replicate secrets; audit the domain head. [07] [09]
MYTH	REALITY
“Put every admin and service account in Protected Users.”	Never service or computer accounts, and test highly privileged users first ; members need AES keys. [04]
MYTH	REALITY
“Full control of an OU is harmless.”	Create rights mean control of everything created, containers included , and inheritance spreads it. [05]

09 SPEAK THE PROGRAM — KEY TERMS

ACE

One entry in an object's DACL granting or denying rights to a trustee; **inherited down the tree** unless blocked.

ADMINSDHOLDER / SDPROP

The permission template for protected groups and the **hourly process** that re-applies it.

UNCONSTRAINED DELEGATION

A host that receives users’ TGTs and can **impersonate them to any service.**

RBCD

Resource-based constrained delegation: the **resource owner** lists which front ends may impersonate to it.

SENSITIVE FLAG

“Account is sensitive and cannot be delegated” (NOT_DELEGATED); **credentials never forwarded.**

CONTROL PLANE

Tier 0: domain controllers, identity systems and **anything that controls them.**