

Active Directory Overview

Interpreted by CRF

Introduction

“ Understanding hacker techniques and processes is the best way to defend against cyber-attacks, and focusing on business risks is the best way to get security budget.”

In this presentation, we're going to focus on common cyber-attacks that target **Active Directory (AD)**. **Active Directory** is deployed across many organizations around the world to ***deliver networking services so that users and computers can easily authenticate and be authorized to access network resources or log on to windows systems***. AD also enables **system administrators** and **infrastructure teams** to manage corporate computer networks.

Common AD hacking techniques

- ❑ RDP brute force
- ❑ LLMNR (Link-Local Multicast Name Resolution) using responder
- ❑ Mimikatz
- ❑ Kerberoasting

The goal is to educate organizations on hacker techniques that put them at risk, and recommend actions to help reduce those risks.

Introduction (Cont.)

Many organizations are under cyber-attack every day; they're subjected to all kinds of security incidents. Some of the most damaging, such as ransomware, can bring a business to a complete halt. Below are several types of security incidents that keep security leaders awake at night. **Which ones concern you most?**



What Keeps
Security Leaders
Up at Night?

- Malware
- Financial Fraud
- Ransomware
- Compliance Failure
- Data Breach
- Data Poisoning
- Insider Threats
- Service/Application Downtime
- Revenue/Brand Loss

Active Directory Overview

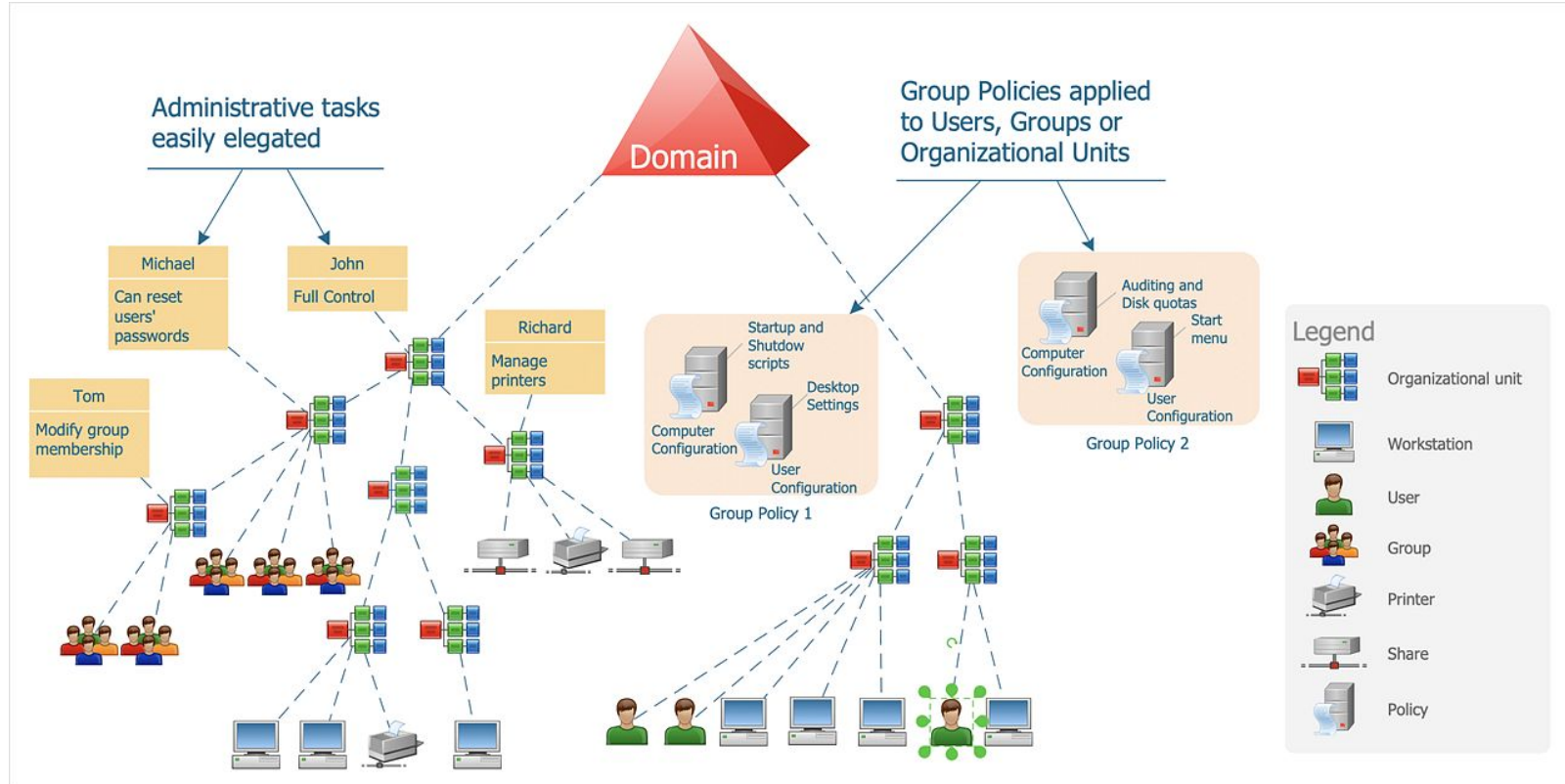
Active Directory (AD) is a directory service that helps manage:

- ❑ network
- ❑ authenticate
- ❑ group
- ❑ organize
- ❑ secure corporate domain networks

Enables users and computers to access different network resources such as log on to a windows system

- ❑ print to a network printer
- ❑ access a network file share
- ❑ access cloud resources via single sign-on,
- ❑ send a simple email.

AD Overview



AD Overview

AD has numerous groups that allow various roles and authorizations

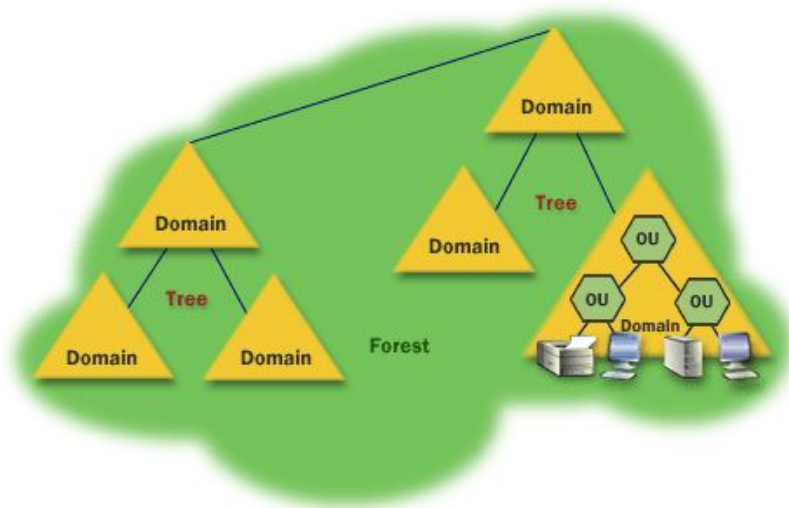
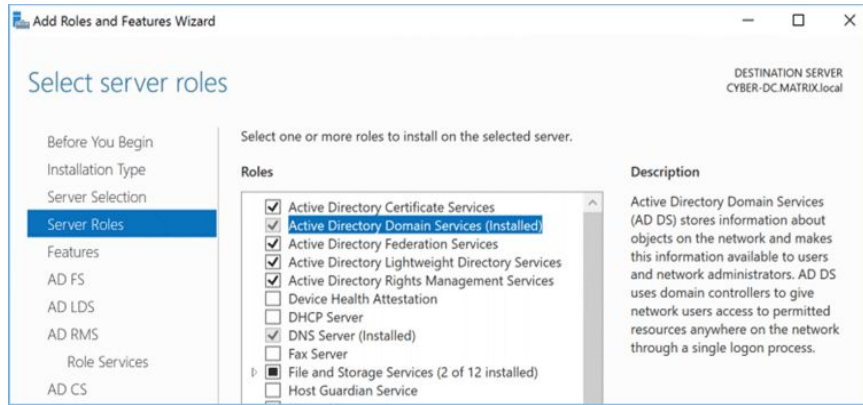
Name	Type	Description
 Allowed RODC Password Replication Group	Security Group - Domain Local	Members in this group can have their passwords re...
 Cert Publishers	Security Group - Domain Local	Members of this group are permitted to publish cert...
 Cloneable Domain Controllers	Security Group - Global	Members of this group that are domain controllers ...
 Denied RODC Password Replication Group	Security Group - Domain Local	Members in this group cannot have their passwords...
 DnsAdmins	Security Group - Domain Local	DNS Administrators Group
 DnsUpdateProxy	Security Group - Global	DNS clients who are permitted to perform dynamic ...
 Domain Admins	Security Group - Global	Designated administrators of the domain
 Domain Computers	Security Group - Global	All workstations and servers joined to the domain
 Domain Controllers	Security Group - Global	All domain controllers in the domain
 Domain Guests	Security Group - Global	All domain guests
 Domain Users	Security Group - Global	All domain users
 Enterprise Admins	Security Group - Universal	Designated administrators of the enterprise
 Enterprise Key Admins	Security Group - Universal	Members of this group can perform administrative ...
 Enterprise Read-only Domain Controllers	Security Group - Universal	Members of this group are Read-Only Domain Cont...
 Group Policy Creator Owners	Security Group - Global	Members in this group can modify group policy for ...
 HelpLibraryUpdaters	Security Group - Domain Local	
 Key Admins	Security Group - Global	Members of this group can perform administrative ...
 Protected Users	Security Group - Global	Members of this group are afforded additional prot...
 RAS and IAS Servers	Security Group - Domain Local	Servers in this group can access remote access prop...
 Read-only Domain Controllers	Security Group - Global	Members of this group are Read-Only Domain Cont...
 Schema Admins	Security Group - Universal	Designated administrators of the schema
 SQLServer2005SQLBrowserUser\$WIN-01S0KHJ45UC	Security Group - Domain Local	Members in the group have the required access and...

AD Overview

Active Directory Domain Services includes the following:

- A schema of objects and attributes
- A global catalog on all objects within the directory
- Ability to search and query the objects
- Replication service to deliver the catalog to other Domain Controllers










Active Directory is a hierarchy typically called a tree (Single Domain) or a **forest** (Multiple Domains) that stores information called objects. At the top of the domain is a **domain controller** (DC) which is used to host a copy of the **Active Directory Domain Services** (AD DS)—this is a schema on all the objects AD stores or delivers authentication and authorization services for



AD Overview

The AD DS data store is a vital component of Active Directory which is a database that stores and processes all the information for users, services, and applications. The AD DS store is typically named ntds.dit and located in the %systemroot%\NTDS folder located on the domain controller.

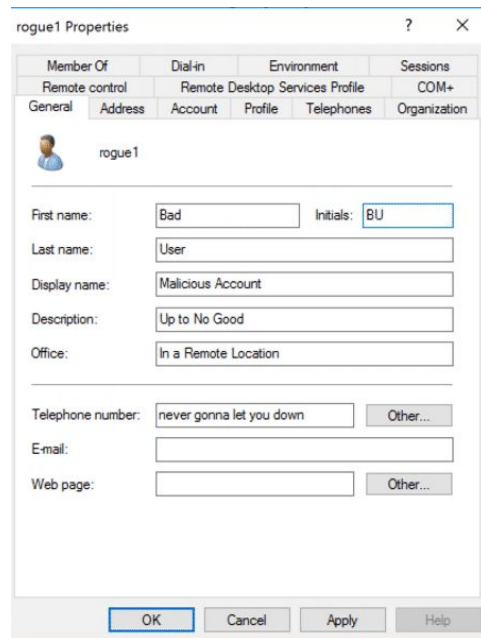
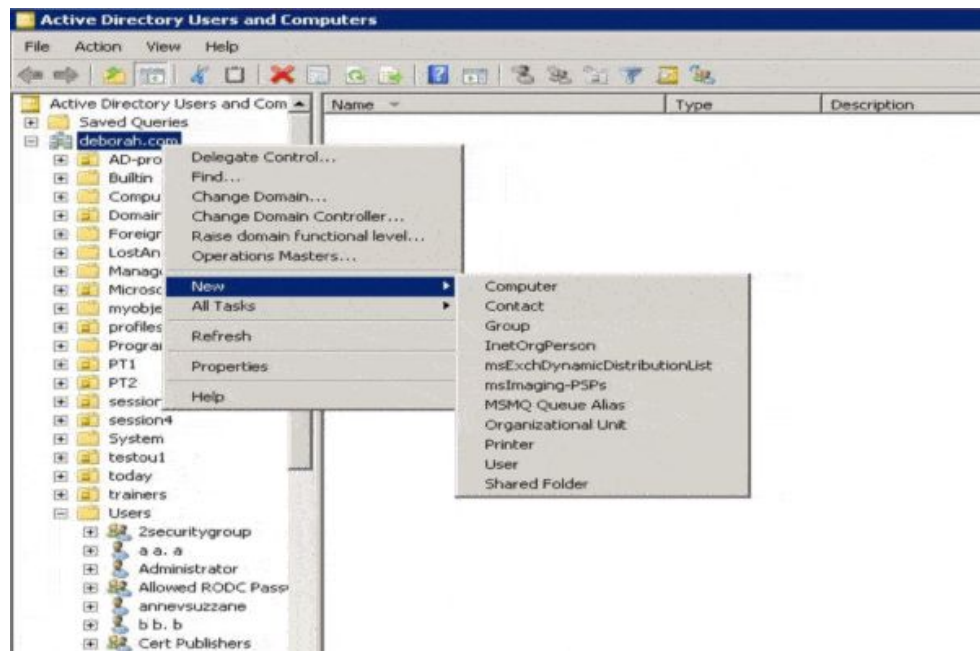
PC > Local Disk (C:) > Windows > NTDS

Name	Date modified	Type	Size
 edb.chk	2/5/2021 6:46 PM	Recovered File Frag...	8 KB
 edb	2/5/2021 6:46 PM	Text Document	10,240 KB
 edb00003	1/19/2021 5:48 PM	Text Document	10,240 KB
 edbres00001.jrs	1/19/2021 3:20 PM	JRS File	10,240 KB
 edbres00002.jrs	1/19/2021 3:20 PM	JRS File	10,240 KB
 edbtmp	1/19/2021 4:41 PM	Text Document	10,240 KB
 ntds.dit	2/7/2021 11:35 AM	DIT File	20,480 KB
 ntds.jfm	2/5/2021 6:46 PM	JFM File	16 KB
 temp.edb	2/7/2021 11:35 AM	EDB File	424 KB

AD Overview

The Active Directory Domain Services schema is the definition of all the objects stored in the directory and enforces rules on the new objects created and object updates.

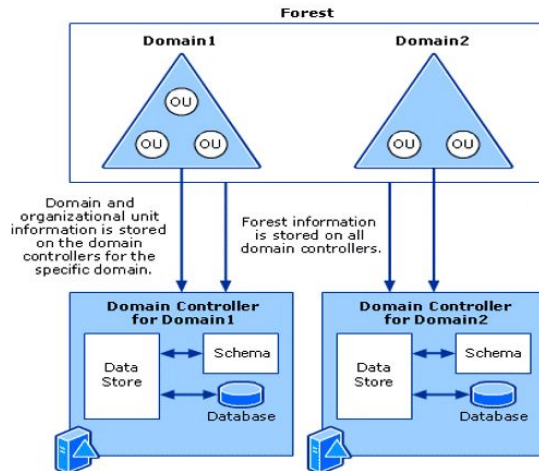
These are separated into object types such as classes for examples, users and computers, or attributes, which is the information contained within the object such as first and last name.



AD Overview

Domains are typically used to group and **manage the objects within the organization**, such as **applying rules and policies** on how the objects should be used and adding the ability for role and scope policies on who has access to what, or who can make changes or updates to the Active Directory.

Active Directory also provides the ability to **group objects into containers**, or, as I tend to call them given my background in systems management—collections. These containers are called **Organizational Units (OUs)** and are used to structure the business and provide easier management. This allows for a role and scope approach.



Active Directory provides two types of trust to establish the level of trust between domains. One is **directional trust**, *which is one-way trust between domains*; the other is **transitive trust**, *a two-way domain trust that includes subdomains*.

AD Overview (Azure AD)

Cloud-based identity service that can synchronize your **Active Directory Data Store** and **extend the capabilities to enable additional cloud services**, such as Single Sign-On and Multi-Factor Authentication

Used to connect and authenticate across many SaaS-based applications including Microsoft 365.



A fully compromised Domain Admin Account is a true security incident; response likely means rebuilding your Active Directory Domain ~Joseph Carson

AD Overview

Below are some of the most common causes of security incidents. As you can tell from this, a good security strategy is one that covers all the basics—and much more.



Common Breach Causes

- Poor access management
- Insecure applications and APIs
- Misconfigured cloud storage
- Distributed Denial of Service (DDOS) attacks
- Overprivileged users
- Shared credentials
- Password only security controls
- Securing third-party access and remote employees
- Shadow IT

Reference

<https://thycotic.com/company/blog/2021/02/23/active-directory-security-guide-to-reducing-ad-risks/>