SILENT BUT DEADLY

THE STINKY TRUTH ABOUT ACTIVE DIRECTORY PERMISSIONS

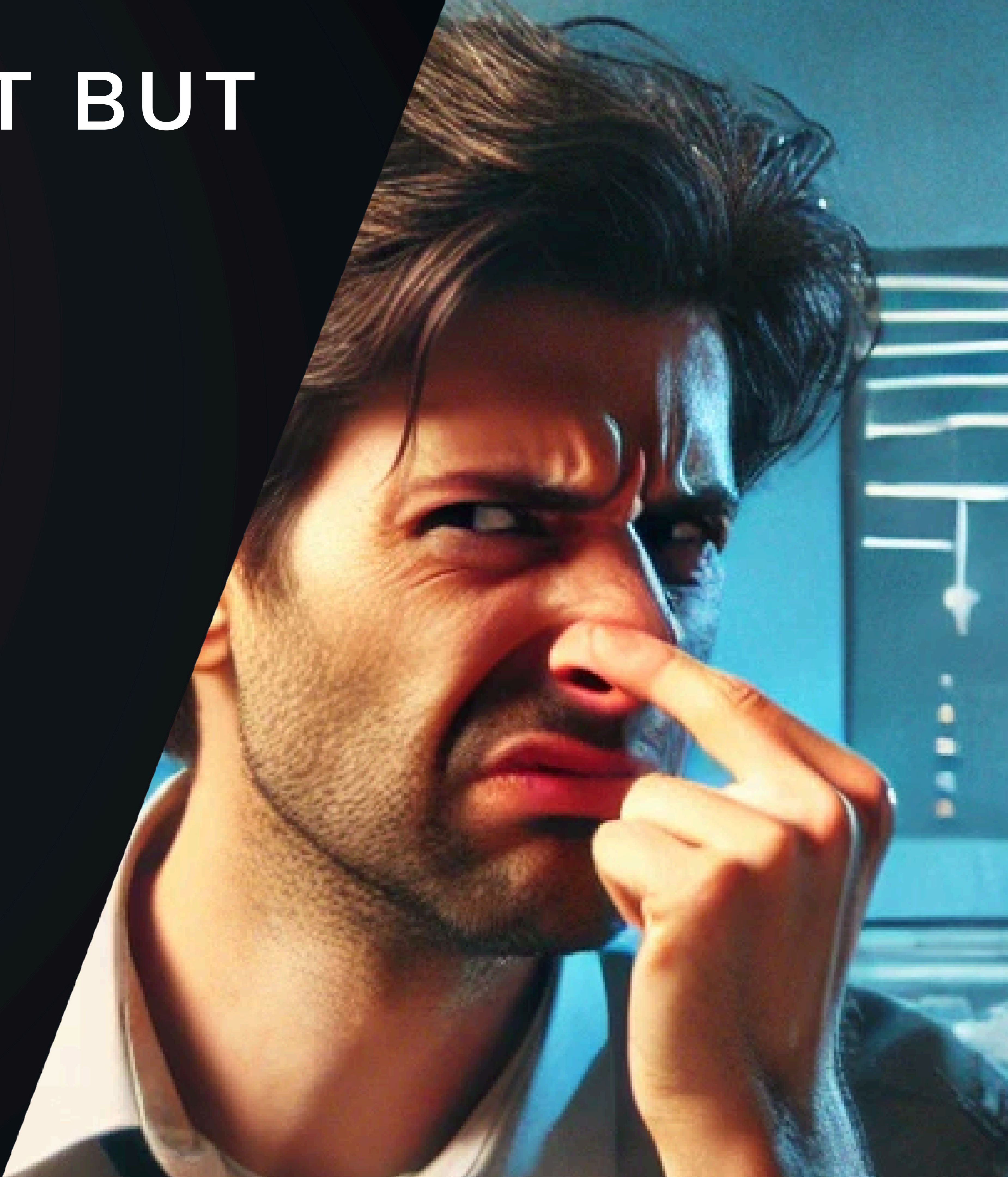
SPENCER ALESSI

SecurIT360
The physics of securing IT

Type 1 in chat if you know what a DACL is...

PERMISSIONS: SILENT BUT DEADLY, UNLESS...

- IT Support Issue
- Pentest
- Security Incident



Spencer Alessi

Sr. Pentester @SecurIT360

- **Background**: Help Desk > Sysadmin > Security
- **Day Job**: Internal Pentesting, Assume Breach, Active Directory Security
- **Ethos**: Spirit of a hacker, heart of a defender
- **Receipts**: CRTO, PNPT, CISSP, GPEN, CVEs
- **Side Hustles**: Content, Tools, SWAG!

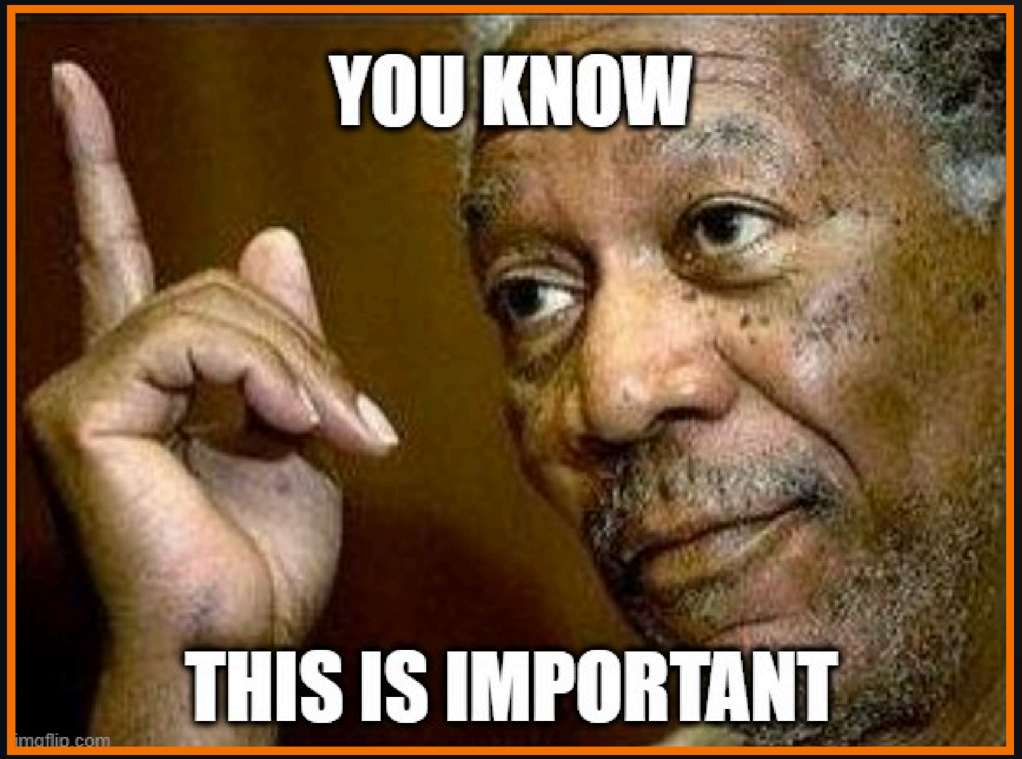
TWITTER.COM/TECHSPENCE
LINKEDIN.COM/IN/SPENCERALESSI
YOUTUBE.COM/@TECHSPENCE
ETHICALTHREAT.ETSY.COM
SECURIT360.COM

SecurIT360
The physics of securing IT

SecurIT360
OFFENSIVE SECURITY

ACTIVE DIRECTORY PERMISSIONS

Why are permissions so important? What's the big deal?

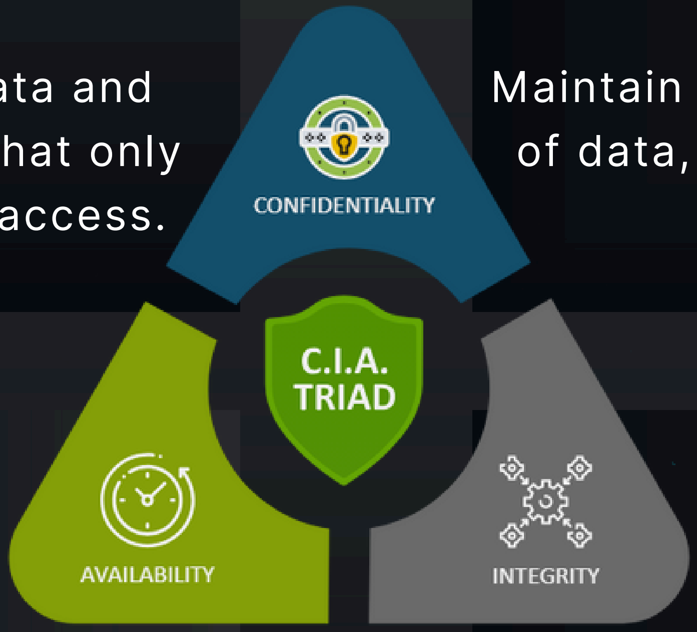


Security

Safeguard sensitive data and resources by ensuring that only authorized users have access.

Integrity

Maintain accuracy and consistency of data, preventing unauthorized changes.



Compliance

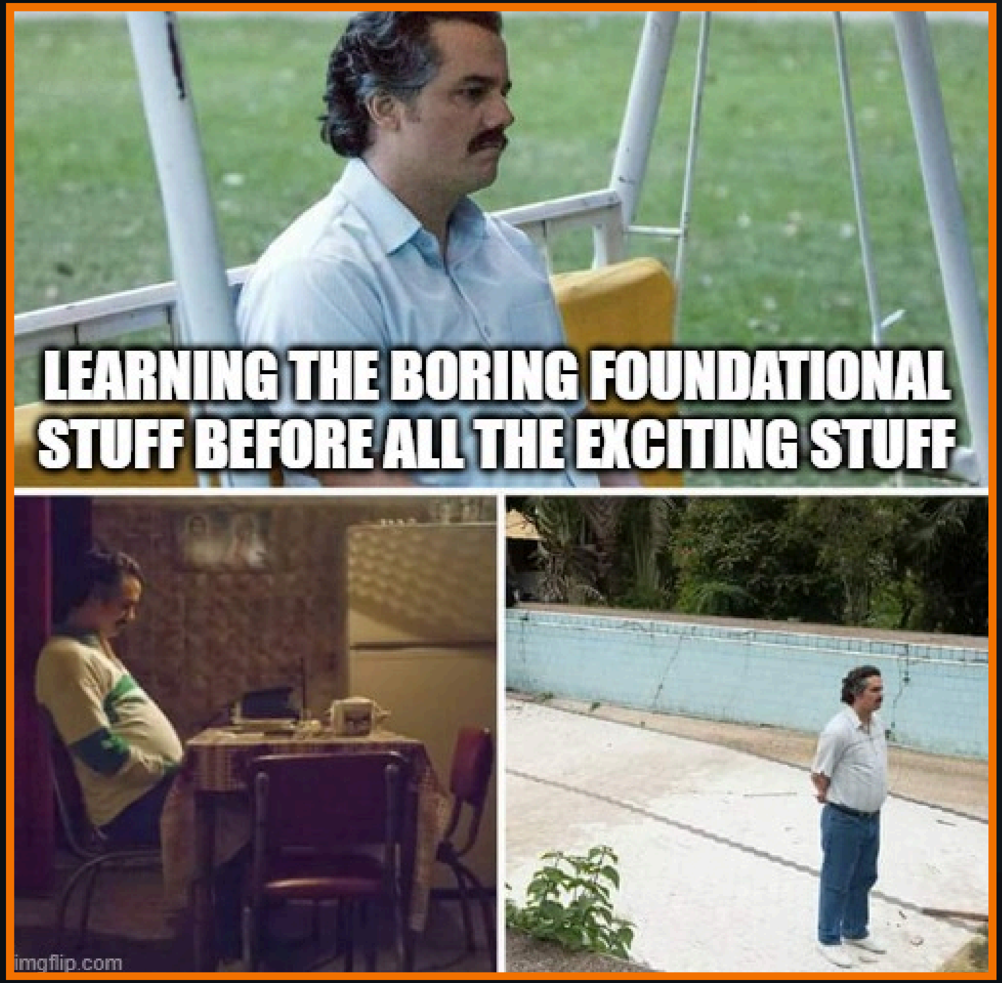
Strict permissions supports regulatory and legal compliance by ensuring that access controls meet required standards and are auditable.

Attack Paths

Inadequate permissions can create vulnerabilities and potential attack paths that threat actors can exploit to escalate privileges or gain unauthorized access.

PERMISSIONS 101: PART 1

10 things to know about permissions...


LEARNING THE BORING FOUNDATIONAL STUFF BEFORE ALL THE EXCITING STUFF
imgflip.com

SECURABLE OBJECTS 1 Users, computers, groups, OUs, etc

SECURITY PRINCIPAL 2 Any entity that can be authenticated by the operating system, such as a user account. They each have a unique security identifier (SID)

PERMISSIONS 3 Rules that define the level of access an object has over another object

DELEGATED PERMISSIONS 4 Assigning specific permissions to objects without requiring that object be a member of a group

ACL, DACL, SACL and the ACE by Daniel Ulrichs

PERMISSIONS 101: *PART 2*

10 things to know about permissions...

ACCESS CONTROL ENTRY (ACE)

5

What describes access rights a security principal has to the secured object. Usually lots of these

ACCESS CONTROL LIST (ACL)

6

Ordered list of ACEs that define the protections that apply to an object and its properties. Each ACE identifies a security principal and specifies a set of access rights that are allowed, denied, or audited for that security principal

DISCRETIONARY ACCESS CONTROL LIST (DACL)

7

Identifies the users and groups that are assigned or denied access permissions on an object. It contains a list of paired ACEs (Account + Access Right) to the securable object

SYSTEM ACCESS CONTROL LIST (SACL)

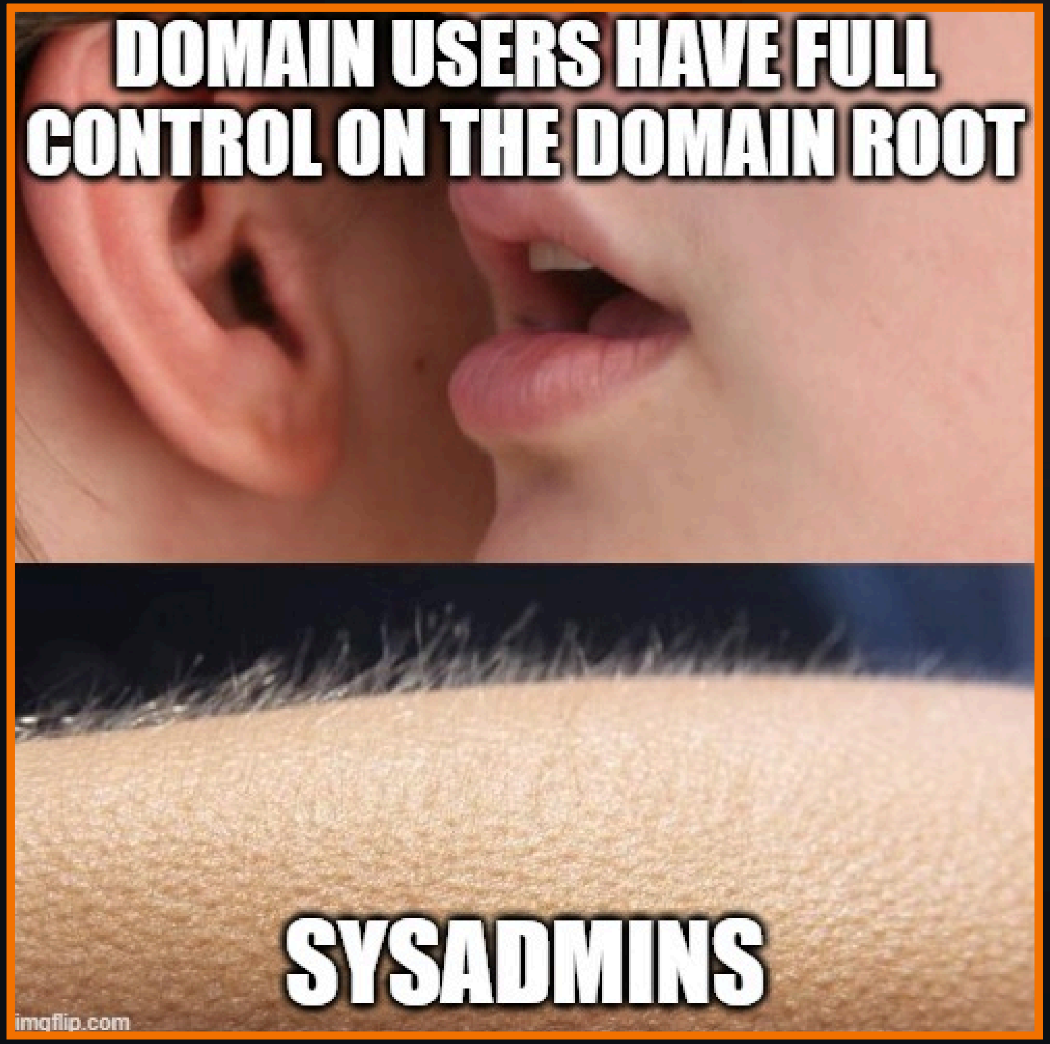
8

Allow for monitoring access to secured objects. ACEs in a SACL determine what types of access is logged in the Security Event Log

ACL, DACL, SACL and the ACE by Daniel Ulrichs

PERMISSIONS 101: PART 3

10 things to know about permissions...



ACCESS RIGHTS

9

Permissions that control what actions users can perform on objects, E.g.:

- **GenericAll** - aka full control
- **GenericWrite** - r/w all properties
- **WriteDacl** - Modify the objects DACL
- **User-Force-Change-Password** - change password without knowing previous

ACE TYPES

10

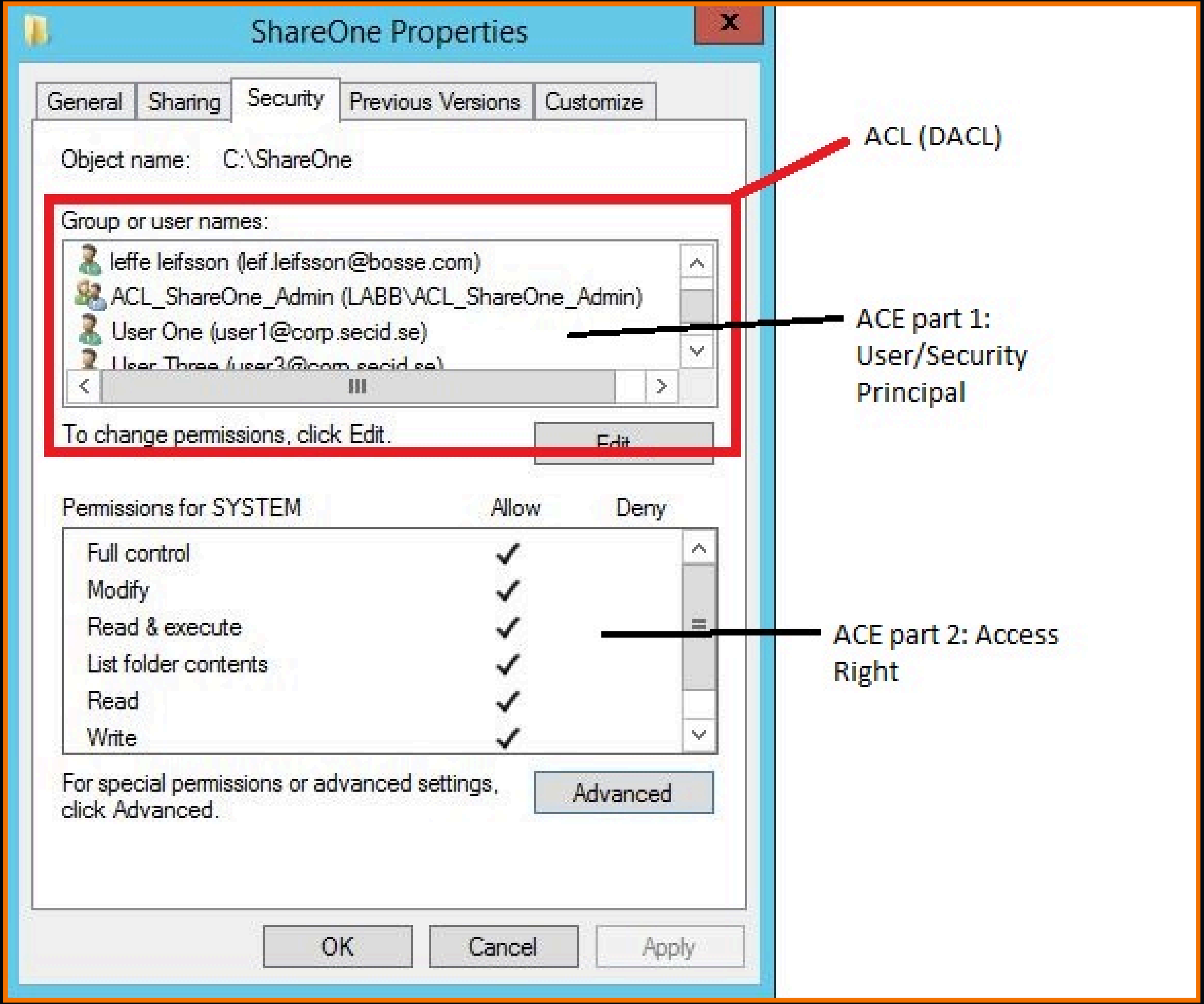
Generic - affect either all types of objects or distinguish only between containers (like folders) and non-containers (like files)

Object Specific - ACEs that apply to specific properties of an object or child object

ACL, DACL, SACL and the ACE by Daniel Ulrichs

PERMISSIONS 101: *EXAMPLE*

10 things to know about permissions...



Object name: C:\ShareOne

Group or user names:

- leffe leifsson (leif.leifsson@bosse.com)
- ACL_ShareOne_Admin (LABB\ACL_ShareOne_Admin)
- User One (user1@corp.secid.se)
- User Three (user3@corp.secid.se)

To change permissions, click Edit.

Permissions for SYSTEM	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	

For special permissions or advanced settings, click Advanced.

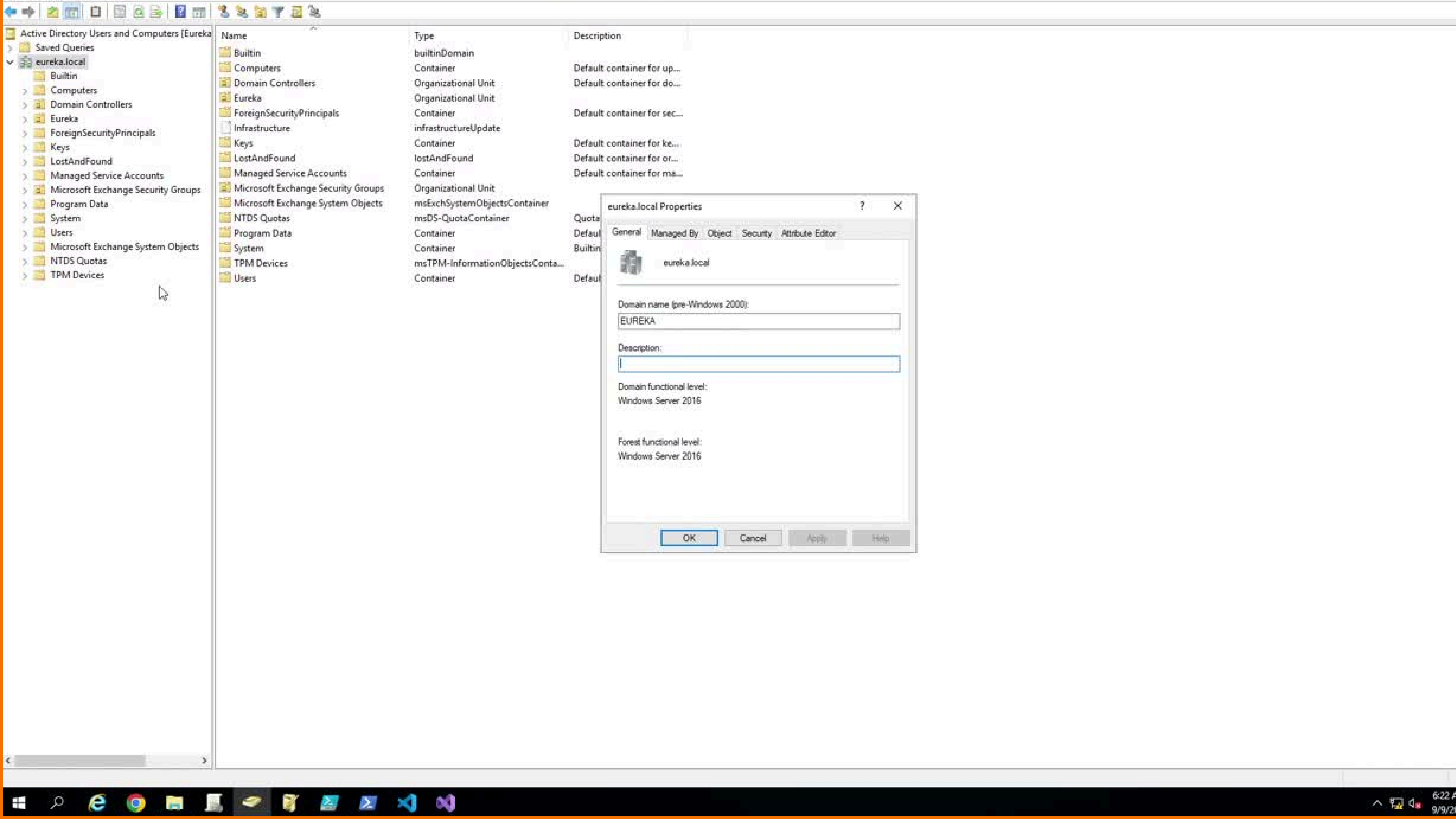
ACL (DACL)

ACE part 1: User/Security Principal

ACE part 2: Access Right

ACL, DACL, SACL and the ACE by Daniel Ulrichs

PERMISSIONS 101: DEMO



Active Directory Users and Computers [Eureka
Saved Queries
eureka.local
Builtin
Computers
Domain Controllers
Eureka
ForeignSecurityPrincipals
Keys
LostAndFound
Managed Service Accounts
Microsoft Exchange Security Groups
Program Data
System
Users
Microsoft Exchange System Objects
NTDS Quotas
TPM Devices

Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default container for up...
Domain Controllers	Organizational Unit	Default container for do...
Eureka	Organizational Unit	
ForeignSecurityPrincipals	Container	Default container for sec...
Infrastructure	infrastructureUpdate	
Keys	Container	Default container for ke...
LostAndFound	lostAndFound	Default container for or...
Managed Service Accounts	Container	Default container for ma...
Microsoft Exchange Security Groups	Organizational Unit	
Microsoft Exchange System Objects	msExchSystemObjectsContainer	
NTDS Quotas	msDS-QuotaContainer	Quota
Program Data	Container	Defaul
System	Container	Builtin
TPM Devices	msTPM-InformationObjectsConta...	
Users	Container	Defaul

eureka.local Properties

General | Managed By | Object | Security | Attribute Editor

eureka.local

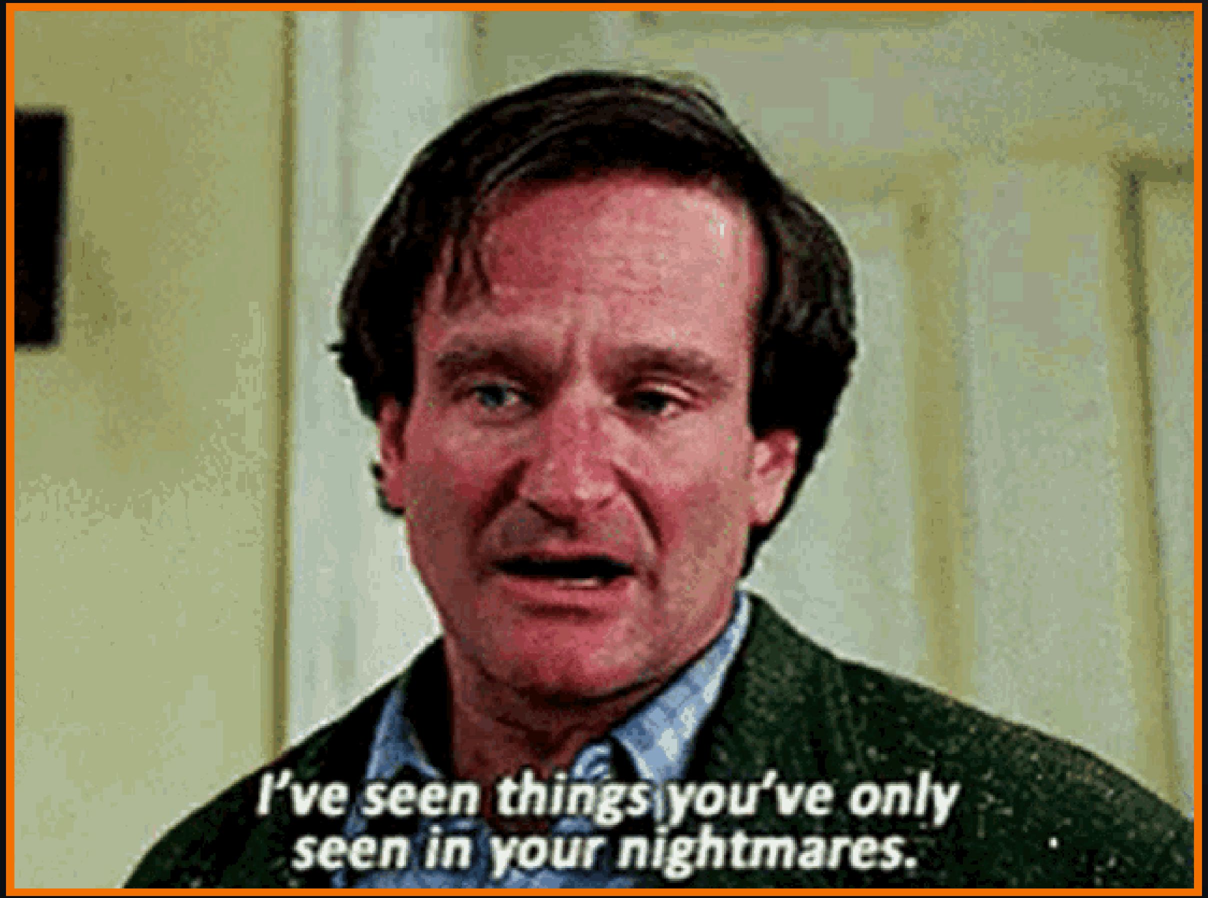
Domain name (pre-Windows 2000):
EUREKA

Description:

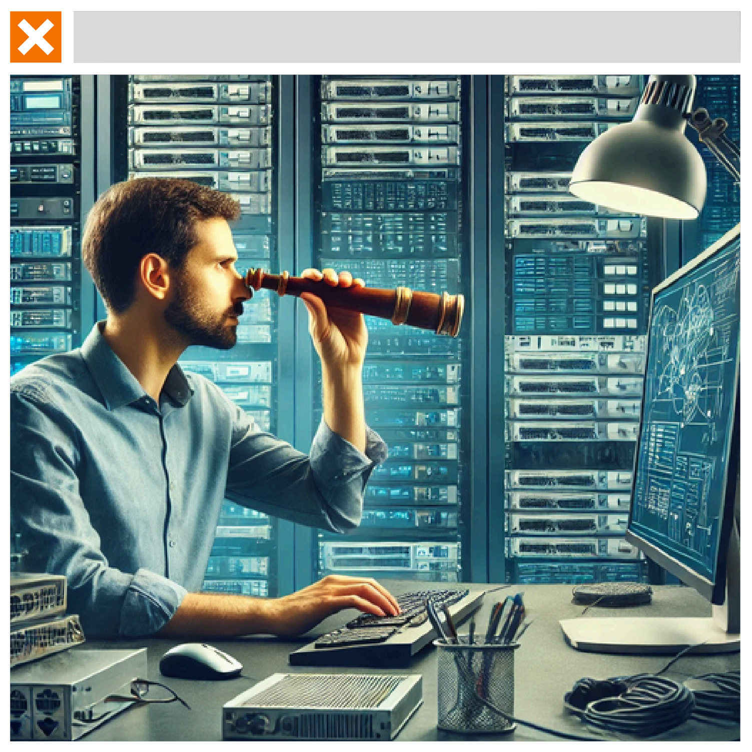
Domain functional level:
Windows Server 2016

Forest functional level:
Windows Server 2016

THE ACTIVE DIRECTORY PERMISSION CHALLENGE

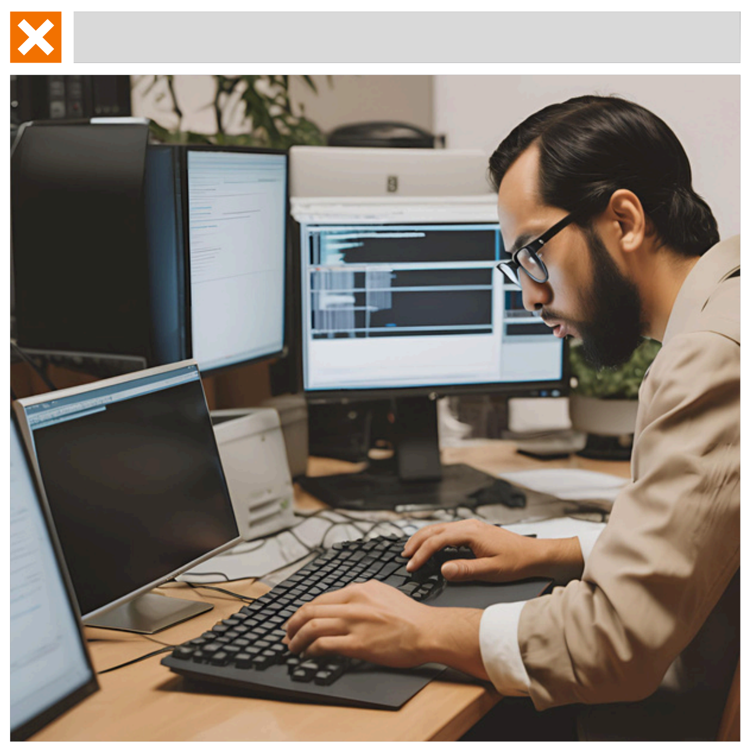


1



Know where to look

2



Know what to look for

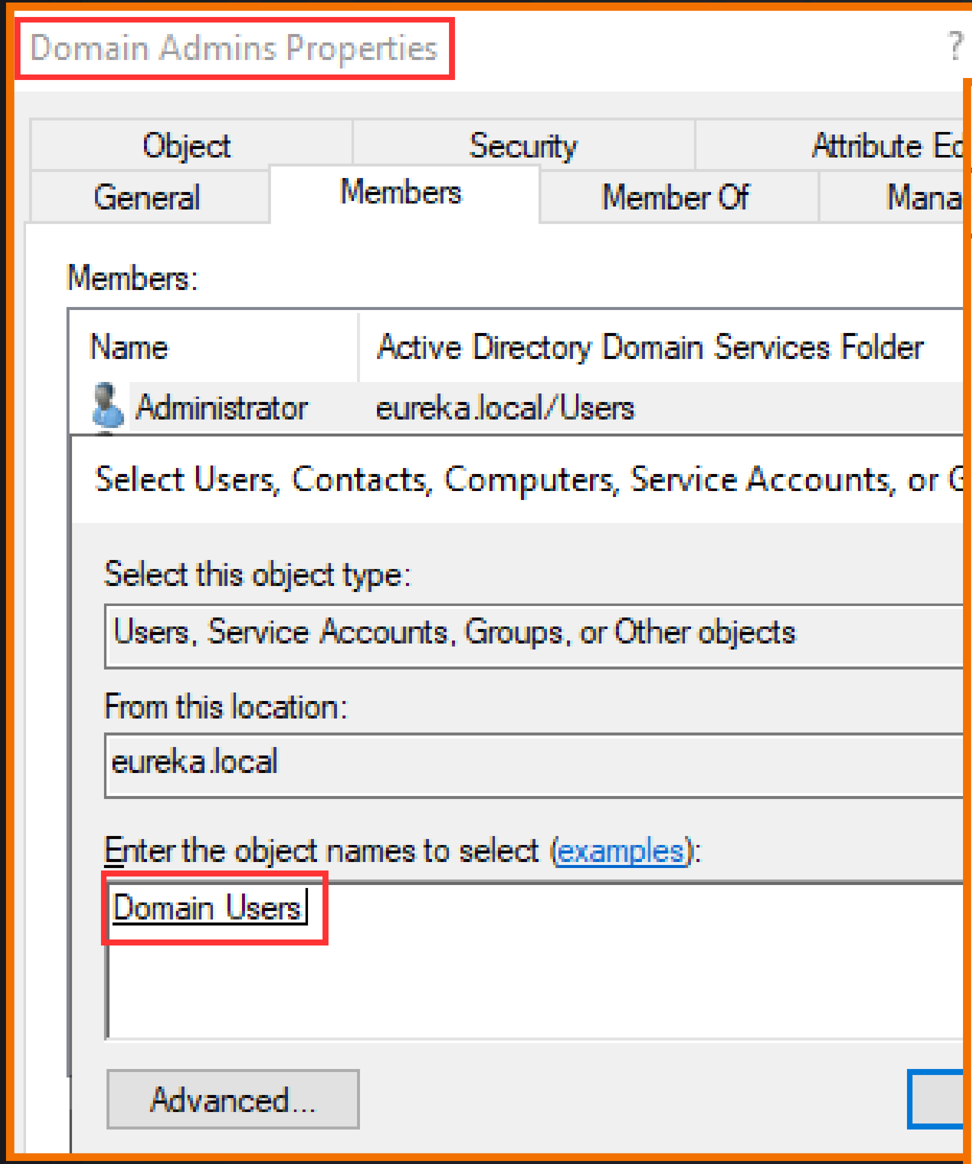
ACTIVE DIRECTORY IS DESIGNED FOR ADMINISTRATION NOT SECURITY

- *Almost* no warnings about insecure/misconfigured permissions

- It's *very* easy to make mistakes & overlook things

- It *assumes* you know what you are doing...

And that's ok. I don't know what I'm doing half the time, on a good day..



Domain Admins Properties

Members:

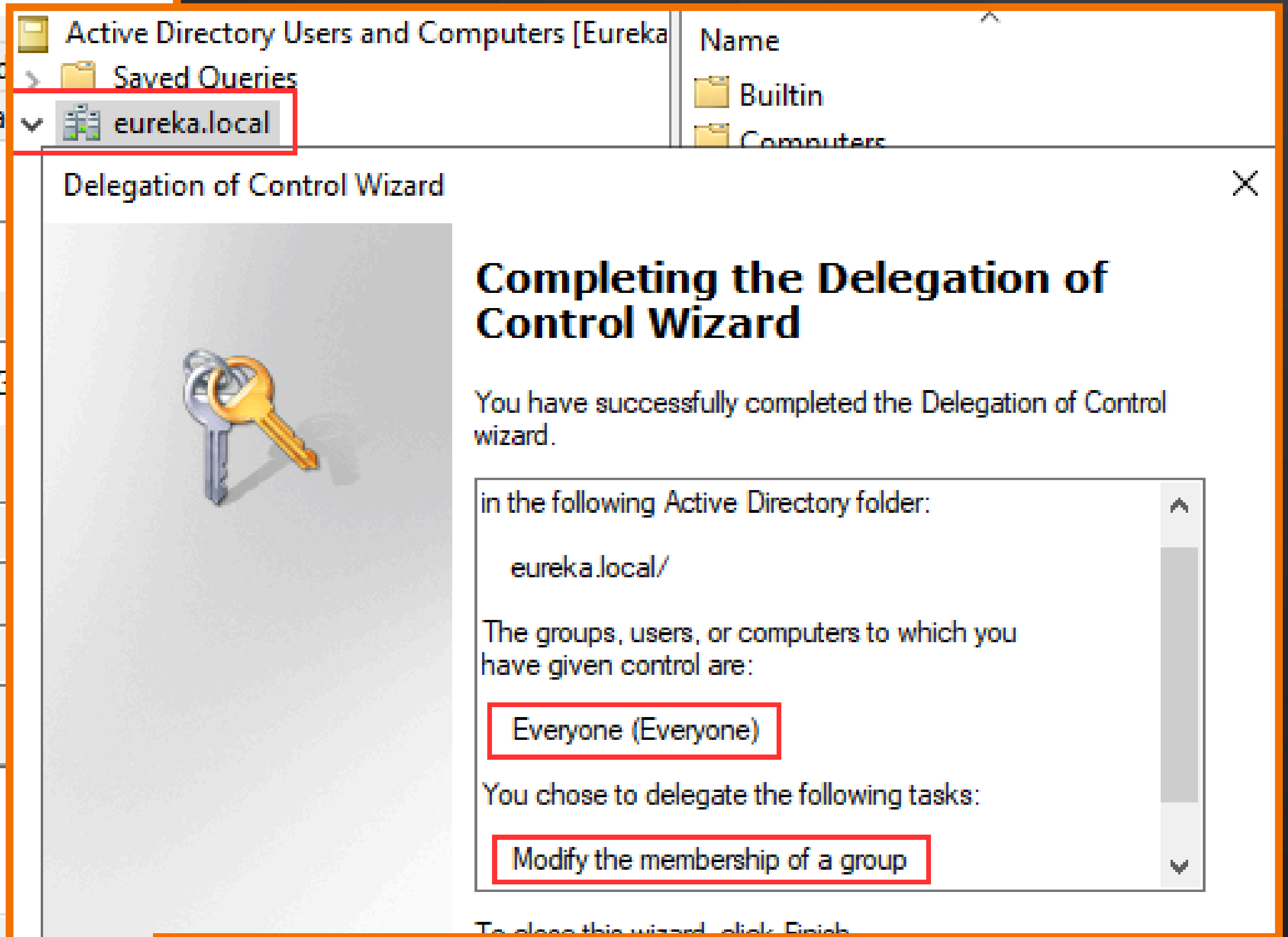
Name	Active Directory Domain Services Folder
Administrator	eureka.local/Users

Select Users, Contacts, Computers, Service Accounts, or G

Select this object type:
Users, Service Accounts, Groups, or Other objects

From this location:
eureka.local

Enter the object names to select (examples):
Domain Users



Delegation of Control Wizard

Completing the Delegation of Control Wizard

You have successfully completed the Delegation of Control wizard.

in the following Active Directory folder:

eureka.local/

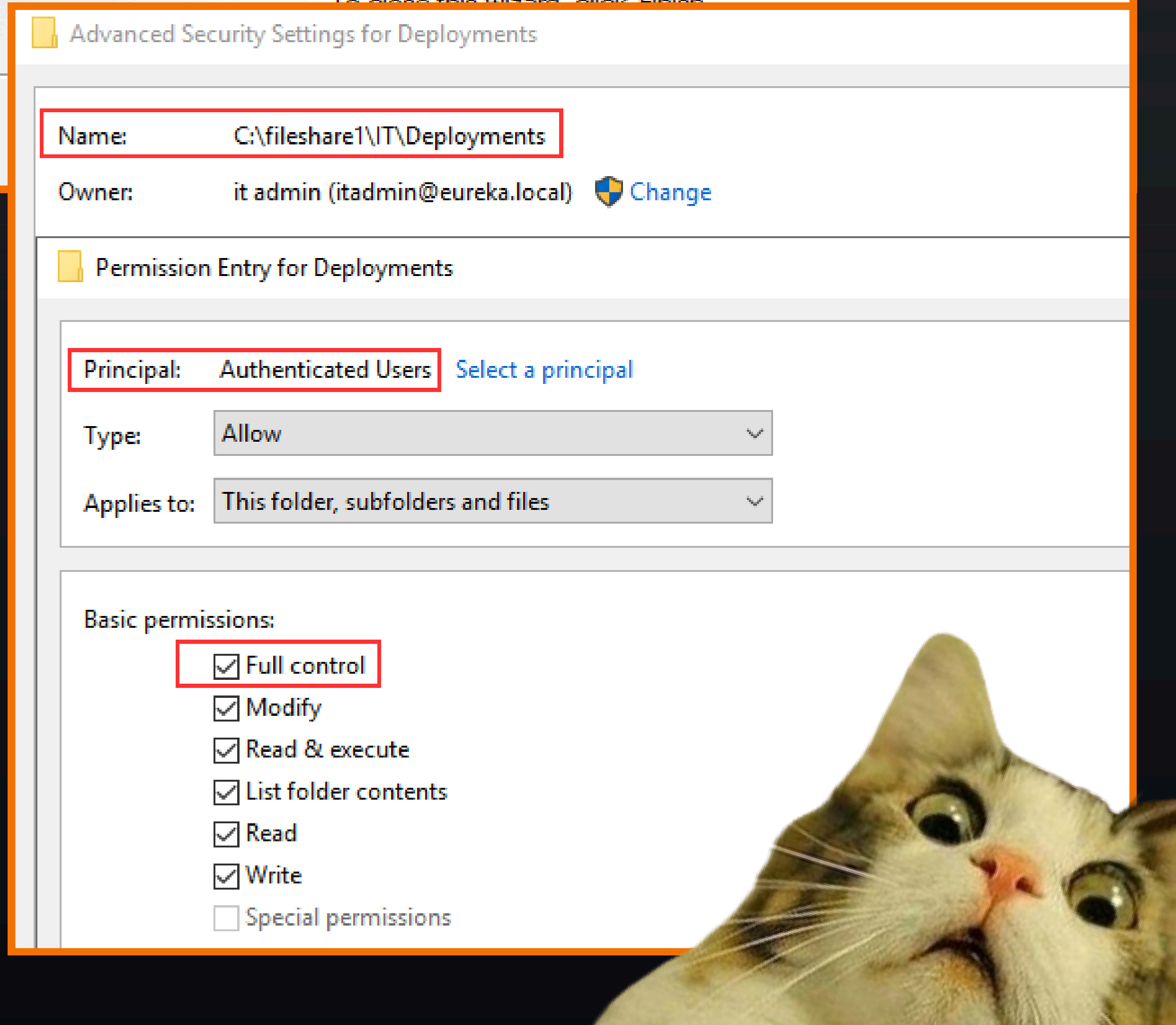
The groups, users, or computers to which you have given control are:

Everyone (Everyone)

You chose to delegate the following tasks:

Modify the membership of a group

To close this wizard, click Finish



Advanced Security Settings for Deployments

Name: C:\fileshare1\IT\Deployments

Owner: it admin (itadmin@eureka.local) Change

Permission Entry for Deployments

Principal: Authenticated Users Select a principal

Type: Allow

Applies to: This folder, subfolders and files

Basic permissions:
☑ Full control
☑ Modify
☑ Read & execute
☑ List folder contents
☑ Read
☑ Write
□ Special permissions

WHERE TO LOOK

- Security Groups
- Organizational Units
- Group Policies
- File Shares
- Logon Scripts
- Certificate Services/Templates
- Administrative & Service Accounts
- User & Computer objects
- Everywhere...

More on this in a second...

WHAT TO LOOK FOR:
USE CASE #1

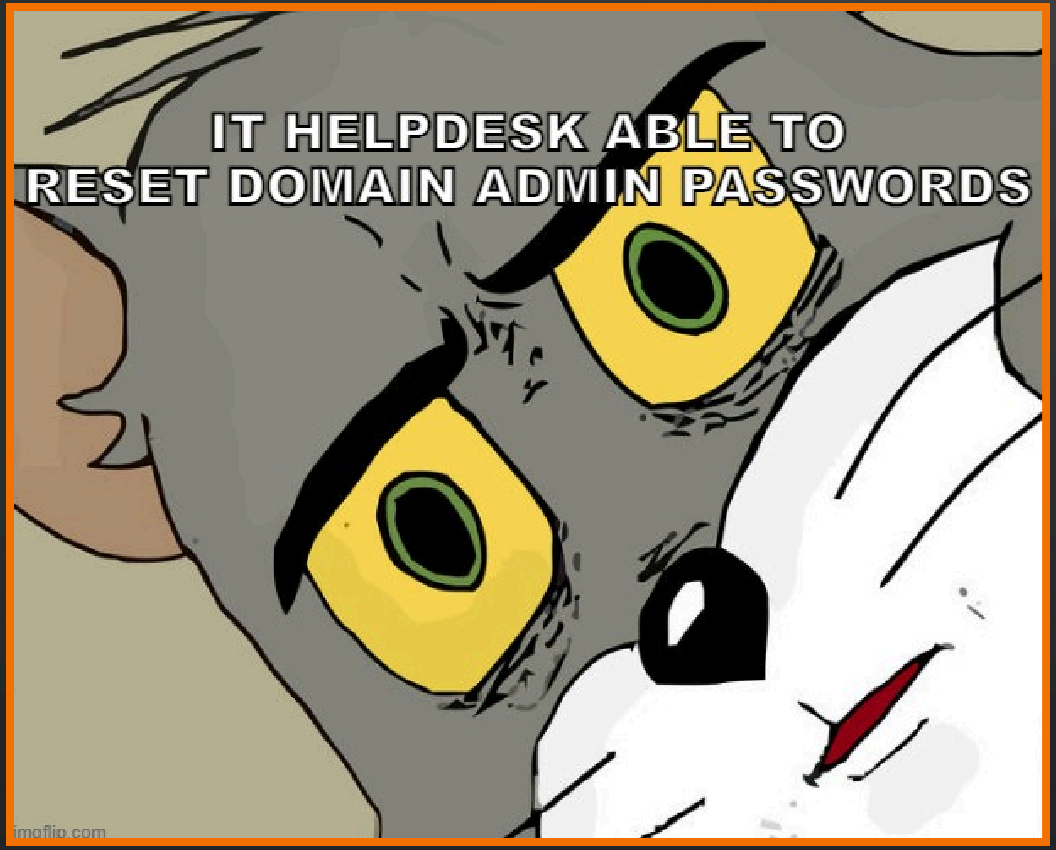
Low privilege security principals (*unsafe users*) that have unsafe permissions on *high-privilege* securable objects/resources

Example: **Domain Users** with FullControl on the **Account Operators** Security Group

WHAT TO LOOK FOR: USE CASE #2

Administrative security principals with unsafe permissions on high-privilege securable objects/resources

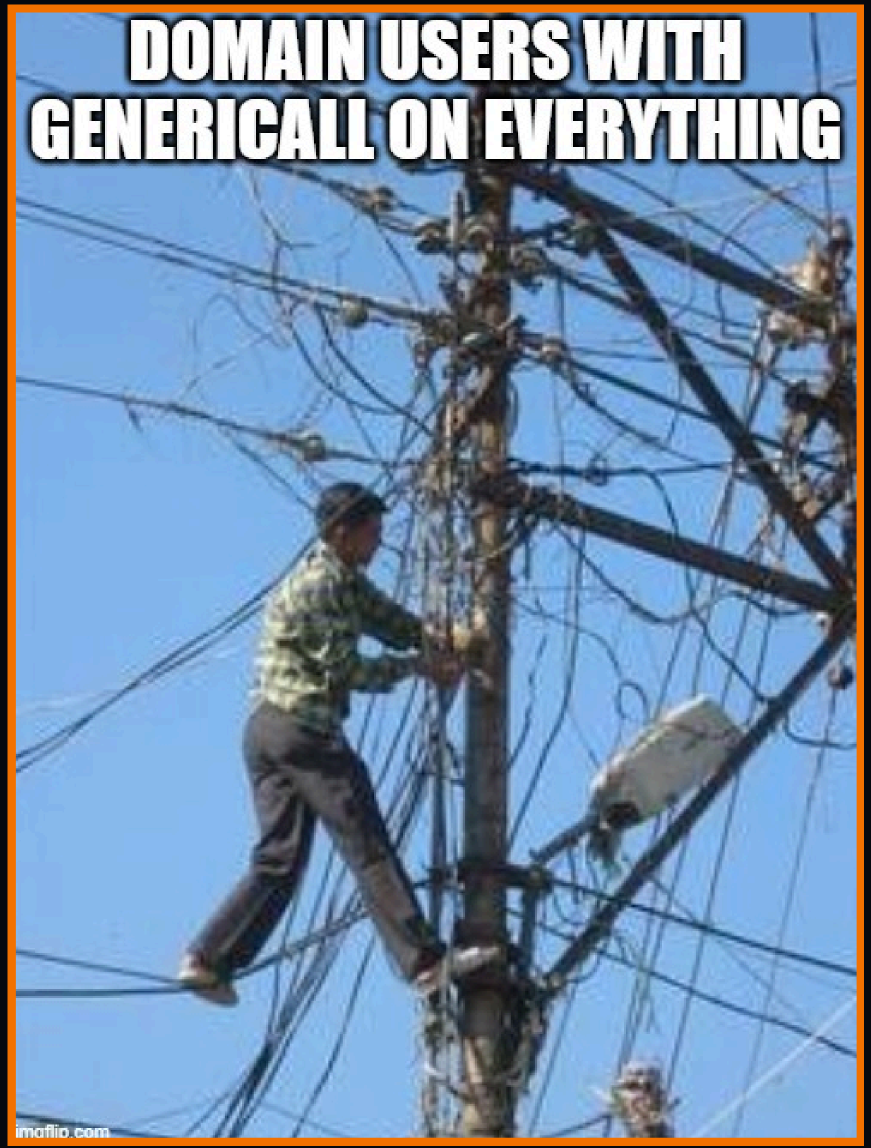
Example: **IT Help Desk** with User-Force-Change-Password on the **Domain Admins** Security Group



UNSAFE USERS

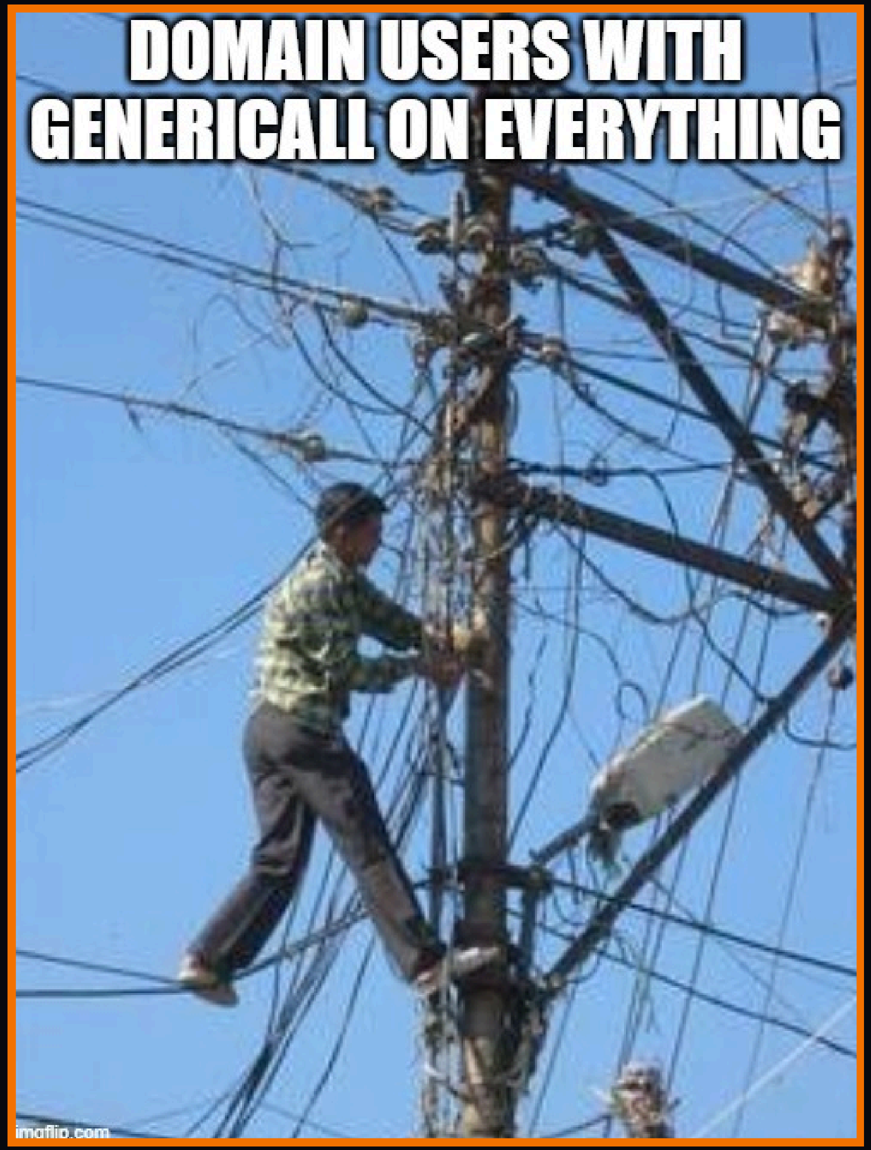
Broad groups of users that don't typically have administrative access.

- Domain Users
- Authenticated Users
- Everyone
- Non-administrative Security Groups



UNSAFE PERMISSIONS

Overly broad/misconfigured access that could allow unauthorized users or groups to modify or access critical objects.



- Full Control - GenericAll
- Write/Modify - GenericWrite, WriteAllProperties, WriteDacl
- User-Force-Change-Password
- Owns, change owner
- Create child objects, delete child objects
- Add/delete delegations
- Delete
- Replicate directory changes, replicate directory changes all (DCSync)

WHERE TO START: USE CASE #1

- **Lowest privileged** securable objects/resources

- **Non-administrative** groups, users, computers, and OUs
- Such as...Domain Users, Everyone, Authenticated Users, end-user computers, etc.

Low privilege trustees --> high privilege resources

Tier 0 Blog Posts An excellent journey of learning about Tier 0 by Jonas Bülow Knudsen

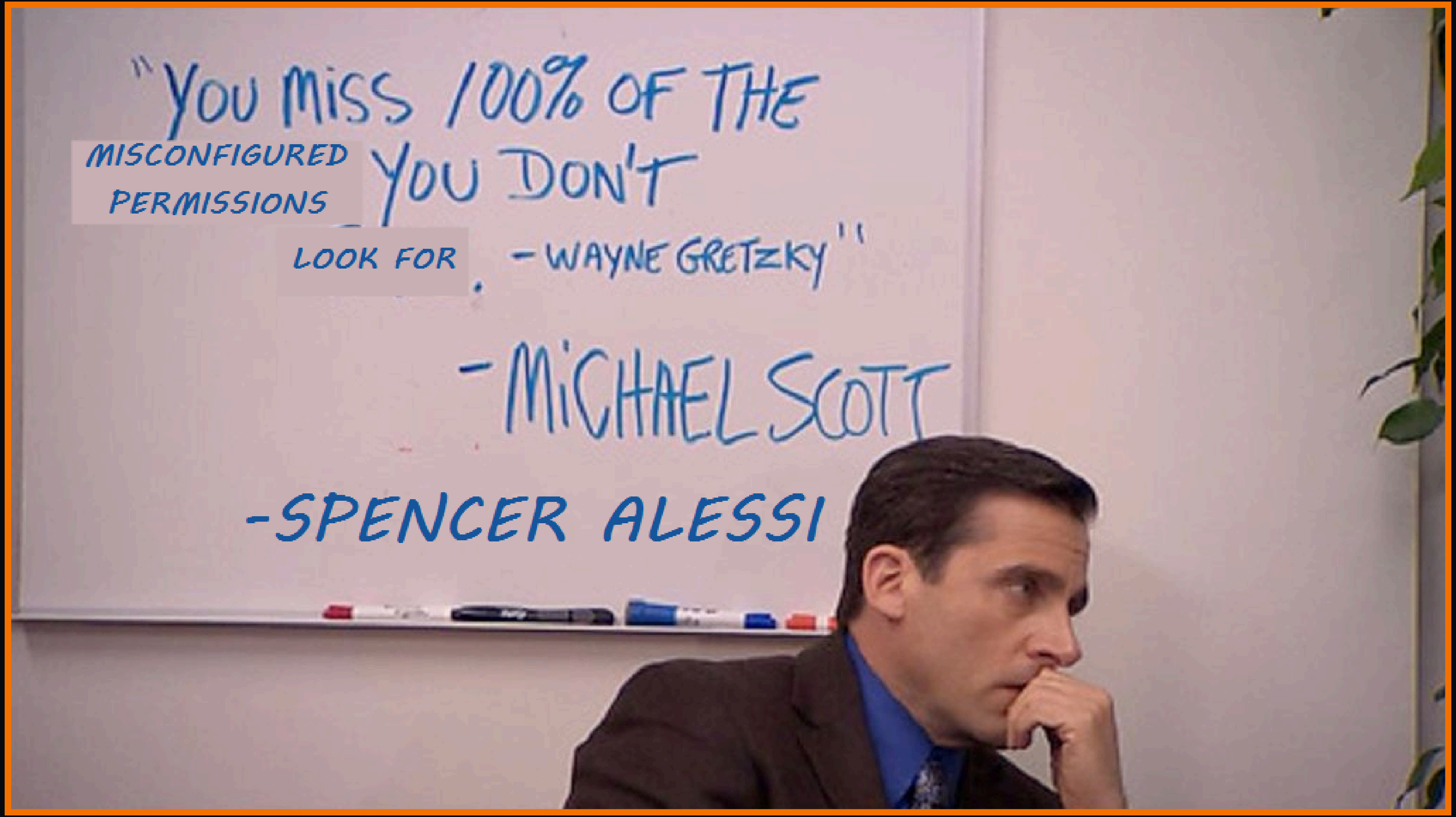
WHAT NEXT

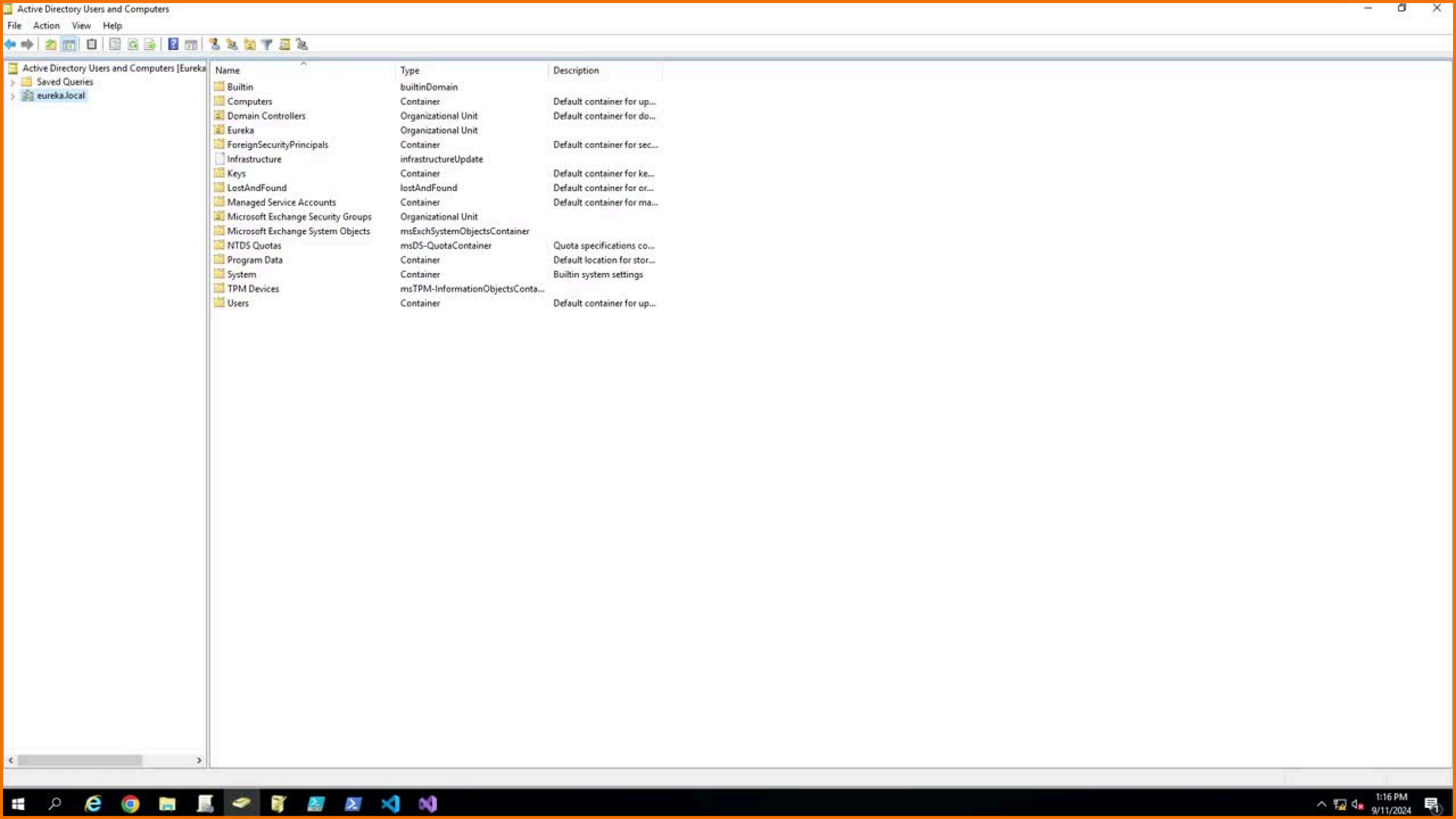
- **Highest privileged** securable objects/resources
- **Tier 0** groups, users, computers, servers and OUs
- Such as...Domain Admins, Enterprise Admins, Domain Controllers, jump boxes/PAWs, IT admin workstations, critical servers, service accounts, administrative OUs, etc.

high privilege resources <-- Low privilege trustees

MANUAL PERMISSION REVIEW: *DEMO*

- Already misconfigured AD environment
- eureka.local (domain root)
- Domain Controllers OU
- Eureka>Admins OU
- SCCM Admin



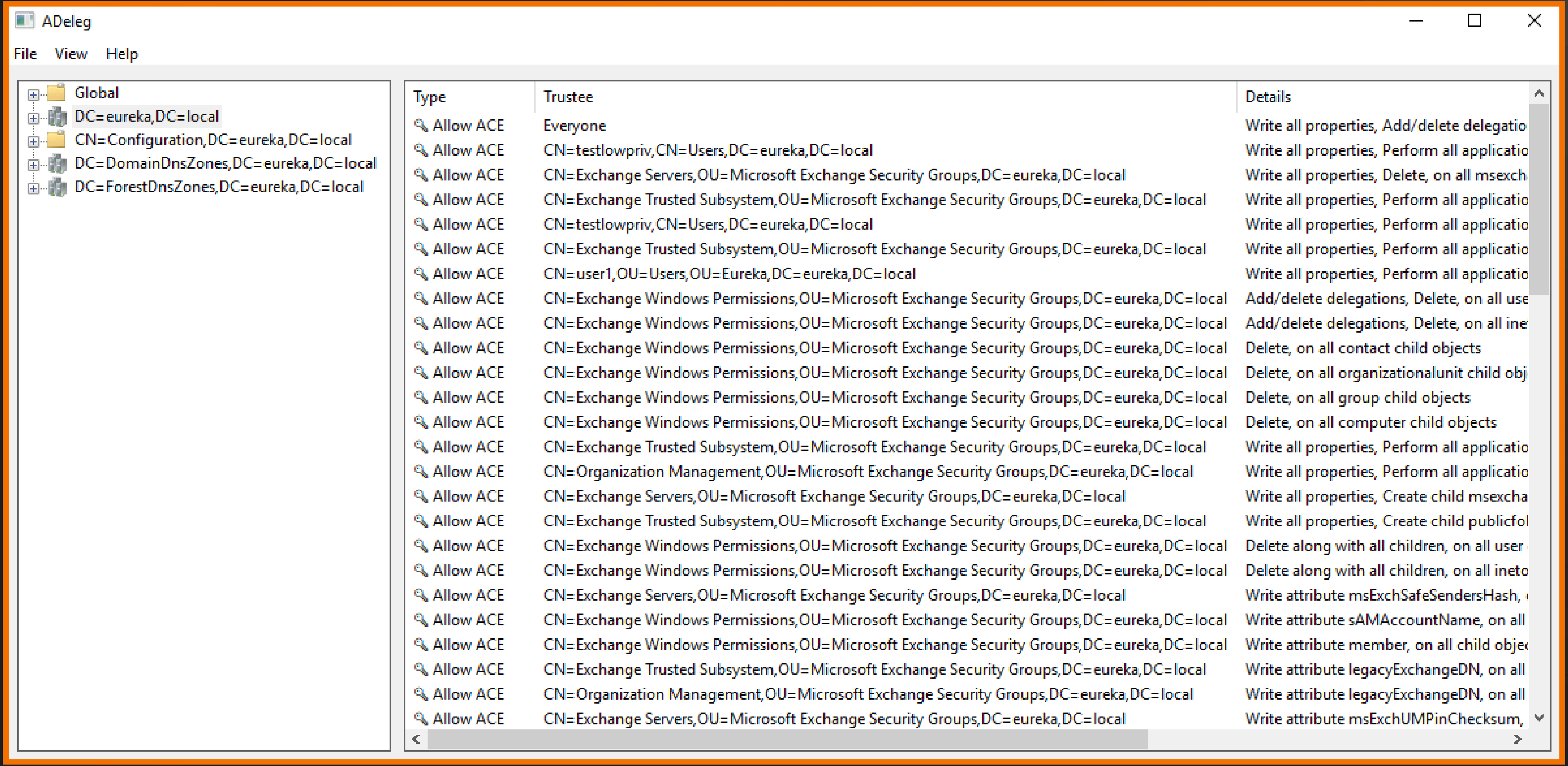

Active Directory Users and Computers
File
Action
View
Help
Active Directory Users and Computers [Eureka
Saved Queries
eureka.local
1:16 PM
9/11/2024

Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default container for up...
Domain Controllers	Organizational Unit	Default container for do...
Eureka	Organizational Unit	
ForeignSecurityPrincipals	Container	Default container for sec...
Infrastructure	infrastructureUpdate	
Keys	Container	Default container for ke...
LostAndFound	lostAndFound	Default container for or...
Managed Service Accounts	Container	Default container for ma...
Microsoft Exchange Security Groups	Organizational Unit	
Microsoft Exchange System Objects	msExchSystemObjectsContainer	
NTDS Quotas	msDS-QuotaContainer	Quota specifications co...
Program Data	Container	Default location for stor...
System	Container	Builtin system settings
TPM Devices	msTPM-InformationObjectsConta...	
Users	Container	Default container for up...

Created by Matthieu Buffet
https://github.com/mtth-bfft/adeleg

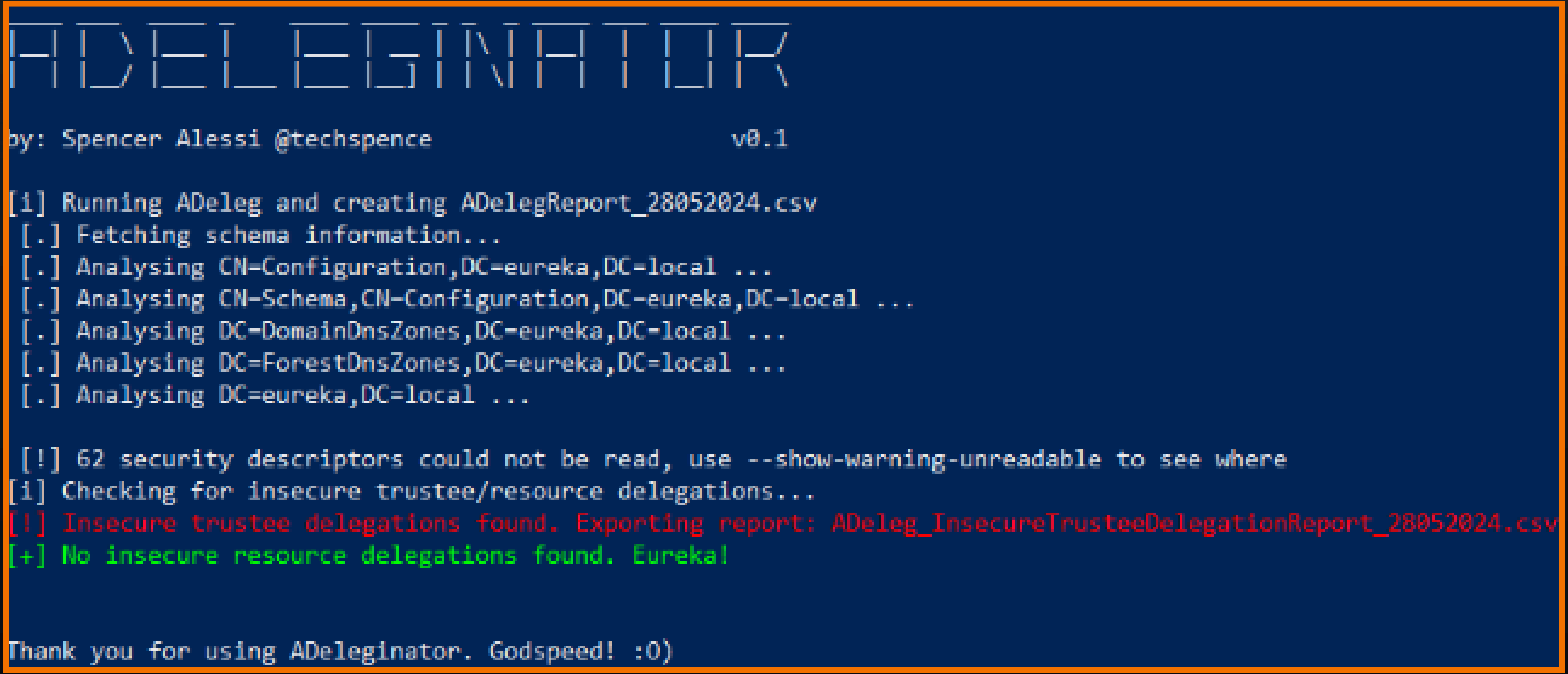
TOOLS TO HELP

- **ADeleg & ADeleginator**
- PingCastle
- PurpleKnight
- ScriptSentry
- Locksmith



- Global
- DC=eureka,DC=local
- CN=Configuration,DC=eureka,DC=local
- DC=DomainDnsZones,DC=eureka,DC=local
- DC=ForestDnsZones,DC=eureka,DC=local

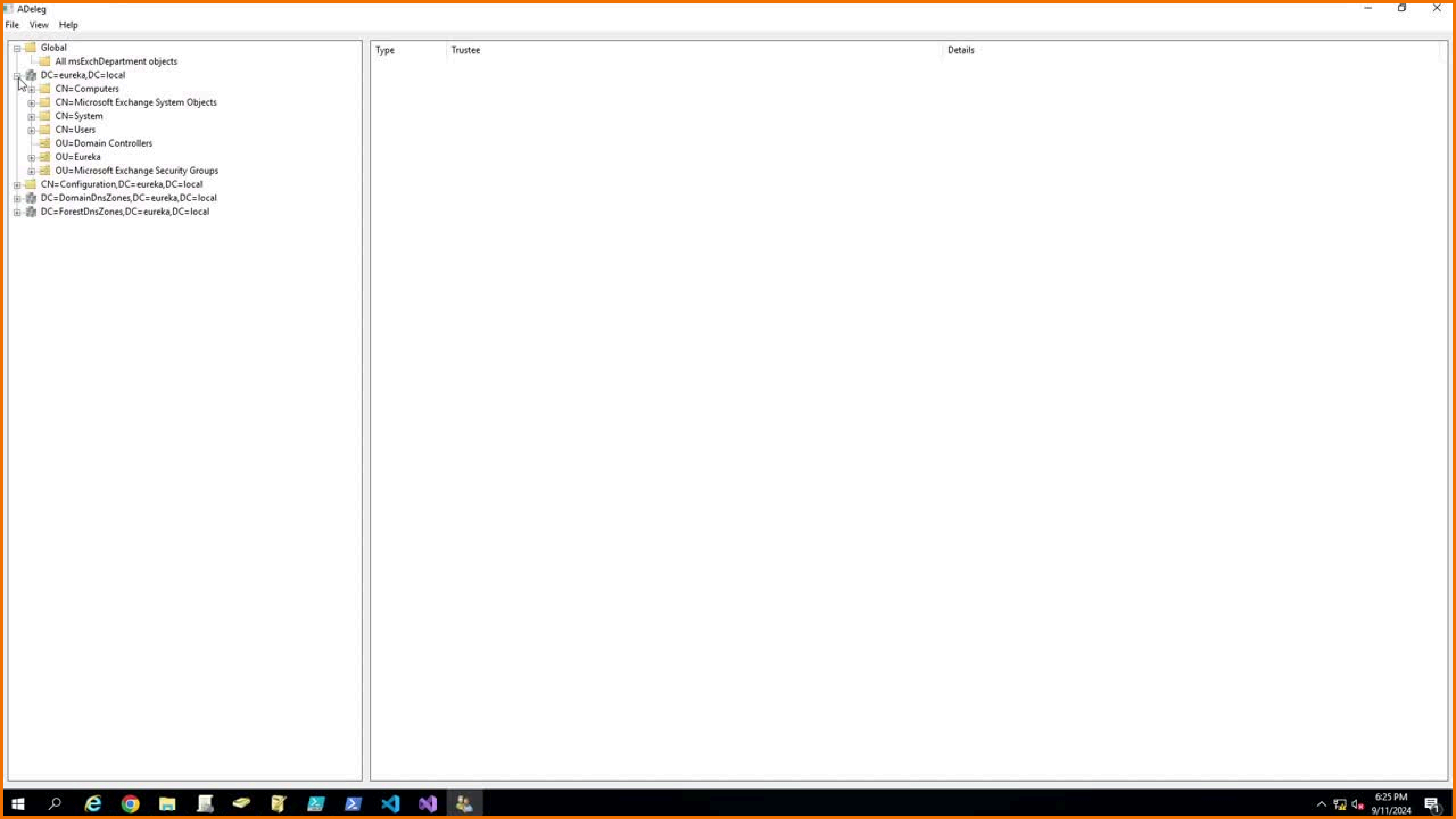
Type	Trustee	Details
Allow ACE	Everyone	Write all properties, Add/delete delegatio
Allow ACE	CN=testlowpriv,CN=Users,DC=eureka,DC=local	Write all properties, Perform all applicatio
Allow ACE	CN=Exchange Servers,OU=Microsoft Exchange Security Groups,DC=eureka,DC=local	Write all properties, Delete, on all msexch
Allow ACE	CN=Exchange Trusted Subsystem,OU=Microsoft Exchange Security Groups,DC=eureka,DC=local	Write all properties, Perform all applicatio
Allow ACE	CN=testlowpriv,CN=Users,DC=eureka,DC=local	Write all properties, Perform all applicatio
Allow ACE	CN=Exchange Trusted Subsystem,OU=Microsoft Exchange Security Groups,DC=eureka,DC=local	Write all properties, Perform all applicatio
Allow ACE	CN=user1,OU=Users,OU=Eureka,DC=eureka,DC=local	Write all properties, Perform all applicatio
Allow ACE	CN=Exchange Windows Permissions,OU=Microsoft Exchange Security Groups,DC=eureka,DC=local	Add/delete delegations, Delete, on all use
Allow ACE	CN=Exchange Windows Permissions,OU=Microsoft Exchange Security Groups,DC=eureka,DC=local	Add/delete delegations, Delete, on all ine
Allow ACE	CN=Exchange Windows Permissions,OU=Microsoft Exchange Security Groups,DC=eureka,DC=local	Delete, on all contact child objects
Allow ACE	CN=Exchange Windows Permissions,OU=Microsoft Exchange Security Groups,DC=eureka,DC=local	Delete, on all organizationalunit child obj
Allow ACE	CN=Exchange Windows Permissions,OU=Microsoft Exchange Security Groups,DC=eureka,DC=local	Delete, on all group child objects
Allow ACE	CN=Exchange Windows Permissions,OU=Microsoft Exchange Security Groups,DC=eureka,DC=local	Delete, on all computer child objects
Allow ACE	CN=Exchange Trusted Subsystem,OU=Microsoft Exchange Security Groups,DC=eureka,DC=local	Write all properties, Perform all applicatio
Allow ACE	CN=Organization Management,OU=Microsoft Exchange Security Groups,DC=eureka,DC=local	Write all properties, Perform all applicatio
Allow ACE	CN=Exchange Servers,OU=Microsoft Exchange Security Groups,DC=eureka,DC=local	Write all properties, Create child msexcha
Allow ACE	CN=Exchange Trusted Subsystem,OU=Microsoft Exchange Security Groups,DC=eureka,DC=local	Write all properties, Create child publicfol
Allow ACE	CN=Exchange Windows Permissions,OU=Microsoft Exchange Security Groups,DC=eureka,DC=local	Delete along with all children, on all user
Allow ACE	CN=Exchange Windows Permissions,OU=Microsoft Exchange Security Groups,DC=eureka,DC=local	Delete along with all children, on all ineto
Allow ACE	CN=Exchange Servers,OU=Microsoft Exchange Security Groups,DC=eureka,DC=local	Write attribute msExchSafeSendersHash,
Allow ACE	CN=Exchange Windows Permissions,OU=Microsoft Exchange Security Groups,DC=eureka,DC=local	Write attribute sAMAccountName, on all
Allow ACE	CN=Exchange Windows Permissions,OU=Microsoft Exchange Security Groups,DC=eureka,DC=local	Write attribute member, on all child objec
Allow ACE	CN=Exchange Trusted Subsystem,OU=Microsoft Exchange Security Groups,DC=eureka,DC=local	Write attribute legacyExchangeDN, on all
Allow ACE	CN=Organization Management,OU=Microsoft Exchange Security Groups,DC=eureka,DC=local	Write attribute legacyExchangeDN, on all
Allow ACE	CN=Exchange Servers,OU=Microsoft Exchange Security Groups,DC=eureka,DC=local	Write attribute msExchUMPinChecksum,



```
by: Spencer Alessi @techspence                    v0.1

[i] Running ADeleg and creating ADelegReport_28052024.csv
 [.] Fetching schema information...
 [.] Analysing CN=Configuration,DC=eureka,DC=local ...
 [.] Analysing CN=Schema,CN=Configuration,DC=eureka,DC=local ...
 [.] Analysing DC=DomainDnsZones,DC=eureka,DC=local ...
 [.] Analysing DC=ForestDnsZones,DC=eureka,DC=local ...
 [.] Analysing DC=eureka,DC=local ...

 [!] 62 security descriptors could not be read, use --show-warning-unreadable to see where
[i] Checking for insecure trustee/resource delegations...
[!] Insecure trustee delegations found. Exporting report: ADeleg_InsecureTrusteeDelegationReport_28052024.csv
[+] No insecure resource delegations found. Eureka!


Thank you for using ADeleginator. Godspeed! :O)
```

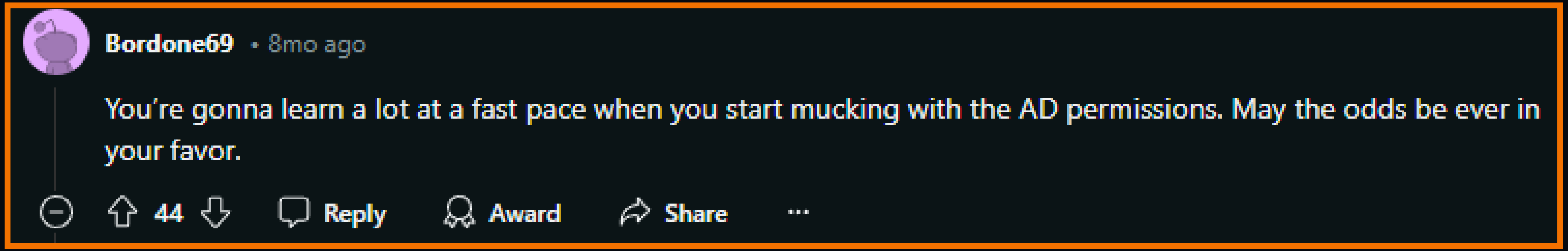
https://github.com/techspence/ADeleginator

ADELEG & ADELEGINATOR: *DEMO*



- Global
  - All msExchDepartment objects
- DC=eureka,DC=local
  - CN=Computers
  - CN=Microsoft Exchange System Objects
  - CN=System
  - CN=Users
  - OU=Domain Controllers
  - OU=Eureka
  - OU=Microsoft Exchange Security Groups
- CN=Configuration,DC=eureka,DC=local
- DC=DomainDnsZones,DC=eureka,DC=local
- DC=ForestDnsZones,DC=eureka,DC=local

REMEDIATION ADVICE



Bordone69 • 8mo ago

You're gonna learn a lot at a fast pace when you start mucking with the AD permissions. May the odds be ever in your favor.

- Document, document, document...
- Over communicate
- Challenge assumptions
- Test & learn
- Have a rollback plan

RESOURCES

- ACL, DACL, SACL and the ACE by Daniel Ulrichs
- Microsoft Delegated Admin Documentation
- Trimarc Whitepaper: Owned or Pwned by Jim Sykora
- ADeleg & ADeleginator
- ADeleg: The Active Directory Security Tool You’ve Never Heard Of
- Webinar - How To Harden Active Directory To Prevent Cyber Attacks

Cloud Security

- Cloud Security Validation
  - SaaS, public, private, hybrid, Azure, Amazon, M365, Google,etc.
  - CASB, ZTNA, SASE, SSE
- 24/7 Threat Monitoring
- Zero Trust Assessment and Guidance
- Cloud Security Data Protection & Privacy Strategy/Roadmap

The Cyber360 OS

- Ongoing Risk Monitoring and Measurement
- Tailored to your needs
- Assigned CISO w/ Risk Dashboard
- Achieve Compliance standards and obtain Cyber Insurance

24/7 Threat Detection & Response

- MDR, EDR, XDR
- Threat Hunting
- Attack Surface Monitoring
- Threat Intelligence

🙏THANK YOU

Offensive Security

- Penetration Testing
  - Internal/External
  - Assumed Breach/Social Engineering
  - Network, Web App, Mobile
  - IoT
  - Physical
- Red/Purple Team Exercises

Privacy & Compliance

- Audit, Assessment, & Advisory
- DPIA
- CMMC, HIPAA, NIST, CCPA, GDPR, GLBA, NYDFS, PCI, ISO 27000, others
- Information Governance
- Web Tracking Privacy Assessment

CISO Services

- GRC & Program Development
  - Risk Management
  - Vendor management
  - Vulnerability Management
  - Other programs
- Security Awareness Training

QUESTIONS?

DevSecOps

- Application Testing
- Dev Process Eval & Design
- Ongoing Code Review

Incident Response & Forensics

- Full Service Response & Forensics
- Planning & Preparations
- Evidence and Data Collection
- Table Top Exercises