Active Directory as a powerful LDAP server: the unknown tips

Alban Meunier
SmartWave SA

45 min

Introduction

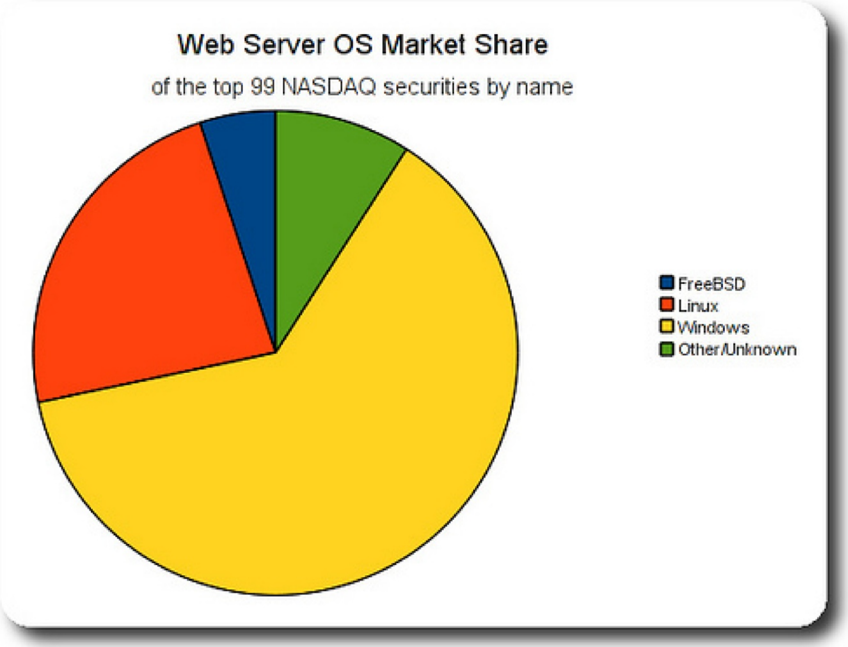
Active Directory context

- **NT inheritance**
  - SAM (Security Account Manager, Samba → V3)
  - Active Directory (2000 → 2003)
  - Active Directory Domain Service (2008 →)
- **Budget under pressure**
- **Implemented everywhere**

Standard vs proprietary

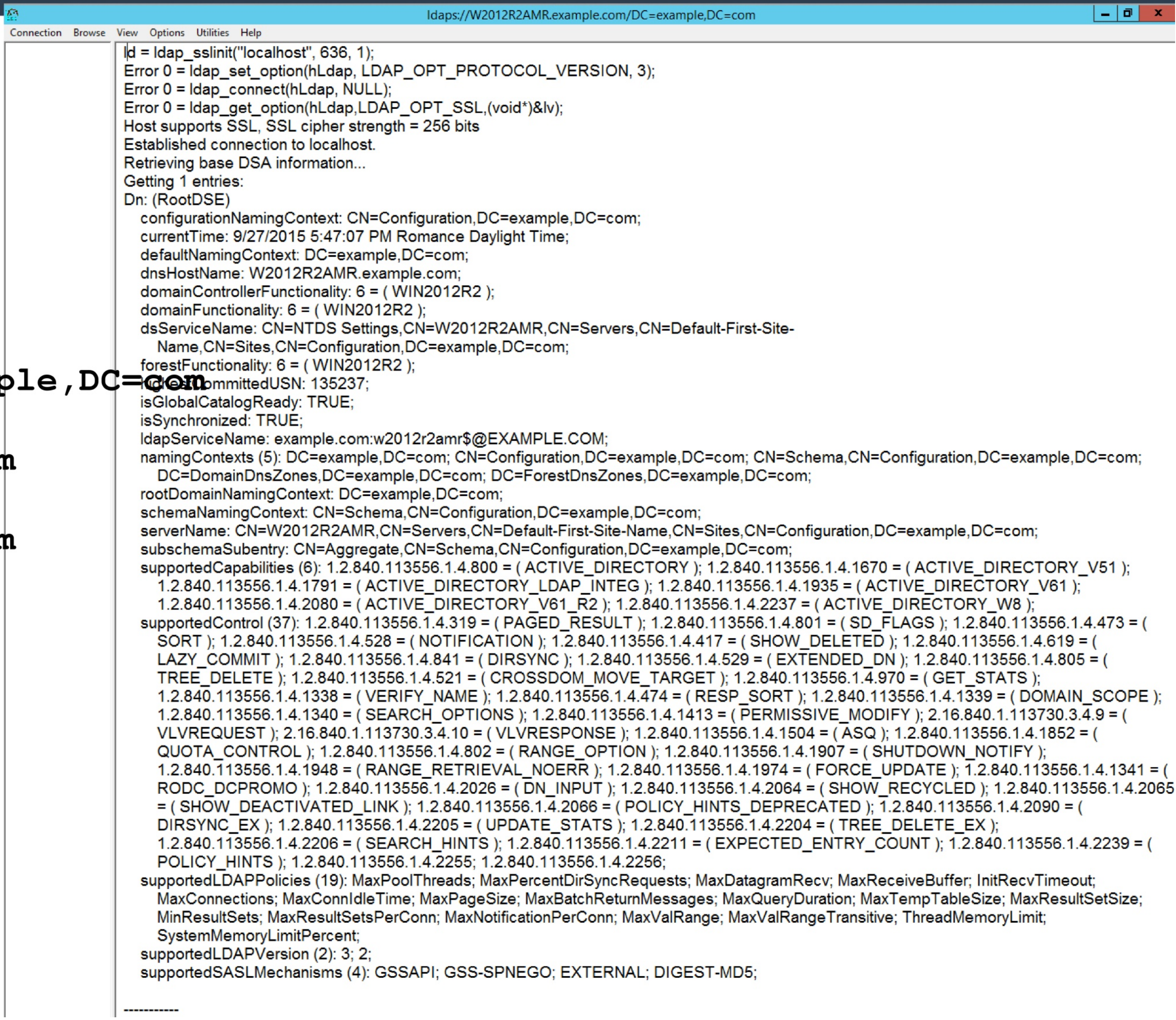
- **Winner and losers**

  https://www.netmarketshare.com/operating-system-market-share.aspx



AD: yes, looks like a LDAP server

```
DC=example,DC=com

CN=Configuration,DC=example,DC=com

CN=Schema,CN=Configuration,DC=example,DC=com

DC=DomainDnsZones,DC=example,DC=com

DC=ForestDnsZones,DC=example,DC=com
```



```
ld = ldap_sslinit("localhost", 636, 1);
Error 0 = ldap_set_option(hLdap, LDAP_OPT_PROTOCOL_VERSION, 3);
Error 0 = ldap_connect(hLdap, NULL);
Error 0 = ldap_get_option(hLdap,LDAP_OPT_SSL,(void*)&lv);
Host supports SSL, SSL cipher strength = 256 bits
Established connection to localhost.
Retrieving base DSA information...
Getting 1 entries:
Dn: (RootDSE)
   configurationNamingContext: CN=Configuration,DC=example,DC=com;
   currentTime: 9/27/2015 5:47:07 PM Romance Daylight Time;
   defaultNamingContext: DC=example,DC=com;
   dnsHostName: W2012R2AMR.example.com;
   domainControllerFunctionality: 6 = ( WIN2012R2 );
   domainFunctionality: 6 = ( WIN2012R2 );
   dsServiceName: CN=NTDS Settings,CN=W2012R2AMR,CN=Servers,CN=Default-First-Site-
      Name,CN=Sites,CN=Configuration,DC=example,DC=com;
   forestFunctionality: 6 = ( WIN2012R2 );
   highestCommittedUSN: 135237;
   isGlobalCatalogReady: TRUE;
   isSynchronized: TRUE;
   ldapServiceName: example.com:w2012r2amr$@EXAMPLE.COM;
   namingContexts (5): DC=example,DC=com; CN=Configuration,DC=example,DC=com; CN=Schema,CN=Configuration,DC=example,DC=com;
      DC=DomainDnsZones,DC=example,DC=com; DC=ForestDnsZones,DC=example,DC=com;
   rootDomainNamingContext: DC=example,DC=com;
   schemaNamingContext: CN=Schema,CN=Configuration,DC=example,DC=com;
   serverName: CN=W2012R2AMR,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=example,DC=com;
   subschemaSubentry: CN=Aggregate,CN=Schema,CN=Configuration,DC=example,DC=com;
   supportedCapabilities (6): 1.2.840.113556.1.4.800 = ( ACTIVE_DIRECTORY ); 1.2.840.113556.1.4.1670 = ( ACTIVE_DIRECTORY_V51 );
      1.2.840.113556.1.4.1791 = ( ACTIVE_DIRECTORY_LDAP_INTEG ); 1.2.840.113556.1.4.1935 = ( ACTIVE_DIRECTORY_V61 );
      1.2.840.113556.1.4.2080 = ( ACTIVE_DIRECTORY_V61_R2 ); 1.2.840.113556.1.4.2237 = ( ACTIVE_DIRECTORY_W8 );
   supportedControl (37): 1.2.840.113556.1.4.319 = ( PAGED_RESULT ); 1.2.840.113556.1.4.801 = ( SD_FLAGS ); 1.2.840.113556.1.4.473 = (
      SORT ); 1.2.840.113556.1.4.528 = ( NOTIFICATION ); 1.2.840.113556.1.4.417 = ( SHOW_DELETED ); 1.2.840.113556.1.4.619 = (
      LAZY_COMMIT ); 1.2.840.113556.1.4.841 = ( DIRSYNC ); 1.2.840.113556.1.4.529 = ( EXTENDED_DN ); 1.2.840.113556.1.4.805 = (
      TREE_DELETE ); 1.2.840.113556.1.4.521 = ( CROSSDOM_MOVE_TARGET ); 1.2.840.113556.1.4.970 = ( GET_STATS );
      1.2.840.113556.1.4.1338 = ( VERIFY_NAME ); 1.2.840.113556.1.4.474 = ( RESP_SORT ); 1.2.840.113556.1.4.1339 = ( DOMAIN_SCOPE );
      1.2.840.113556.1.4.1340 = ( SEARCH_OPTIONS ); 1.2.840.113556.1.4.1413 = ( PERMISSIVE_MODIFY ); 2.16.840.1.113730.3.4.9 = (
      VLVREQUEST ); 2.16.840.1.113730.3.4.10 = ( VLVRESPONSE ); 1.2.840.113556.1.4.1504 = ( ASQ ); 1.2.840.113556.1.4.1852 = (
      QUOTA_CONTROL ); 1.2.840.113556.1.4.802 = ( RANGE_OPTION ); 1.2.840.113556.1.4.1907 = ( SHUTDOWN_NOTIFY );
      1.2.840.113556.1.4.1948 = ( RANGE_RETRIEVAL_NOERR ); 1.2.840.113556.1.4.1974 = ( FORCE_UPDATE ); 1.2.840.113556.1.4.1341 = (
      RODC_DCPROMO ); 1.2.840.113556.1.4.2026 = ( DN_INPUT ); 1.2.840.113556.1.4.2064 = ( SHOW_RECYCLED ); 1.2.840.113556.1.4.2065
      = ( SHOW_DEACTIVATED_LINK ); 1.2.840.113556.1.4.2066 = ( POLICY_HINTS_DEPRECATED ); 1.2.840.113556.1.4.2090 = (
      DIRSYNC_EX ); 1.2.840.113556.1.4.2205 = ( UPDATE_STATS ); 1.2.840.113556.1.4.2204 = ( TREE_DELETE_EX );
      1.2.840.113556.1.4.2206 = ( SEARCH_HINTS ); 1.2.840.113556.1.4.2211 = ( EXPECTED_ENTRY_COUNT ); 1.2.840.113556.1.4.2239 = (
      POLICY_HINTS ); 1.2.840.113556.1.4.2255; 1.2.840.113556.1.4.2256;
   supportedLDAPPolicies (19): MaxPoolThreads; MaxPercentDirSyncRequests; MaxDatagramRecv; MaxReceiveBuffer; InitRecvTimeout;
      MaxConnections; MaxConnIdleTime; MaxPageSize; MaxBatchReturnMessages; MaxQueryDuration; MaxTempTableSize; MaxResultSetSize;
      MinResultSets; MaxResultSetsPerConn; MaxNotificationPerConn; MaxValRange; MaxValRangeTransitive; ThreadMemoryLimit;
      SystemMemoryLimitPercent;
   supportedLDAPVersion (2): 3; 2;
   supportedSASLMechanisms (4): GSSAPI; GSS-SPNEGO; EXTERNAL; DIGEST-MD5;

-----------
```

AD: yes, looks like a LDAP server

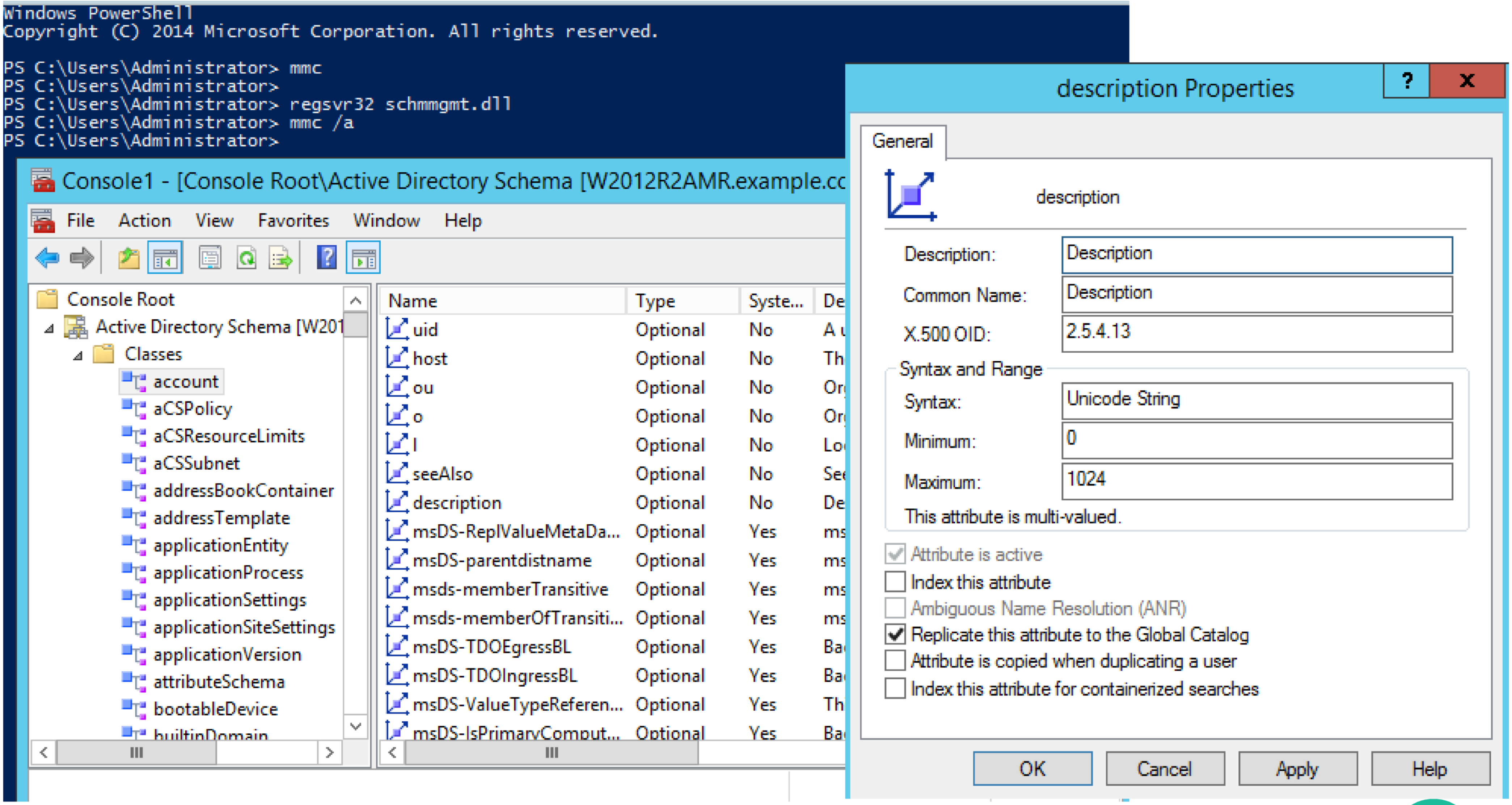
- **Root DSE**
- **15 Supported Controls**
  - Server sort, Pages result
  - AD related like *crossdom_move_target*, …
  - Note: C++ source code available
    https://msdn.microsoft.com/en-us/library/aa366977(v=vs.85).aspx
- **LDAP listener (389/636, 3268/3269)**
- **CN=Schema,CN=Configuration,DC=example,dc=com**
- ….

Schema

https://msdn.microsoft.com/en-us/library/ms675085(v=vs.85).aspx

- **Standard schema**
  - OrganizationalUnit, OrganizationalPerson
  - InetOrgPerson (2003 ->)
  - NIS: nisMap, nisNetgroup, nisObject
- **Microsoft schema**
  - Because AD is a Microsoft product: Ms..., NT…
  - Because AD is part of Windows server: PKI, RRAS, site, DNS, IPSEC, ...
  - Because Microsoft is Microsoft
    - groupOUniqueNames, Group-of-Names (Ldap-Display-Name = ….), Group
    - Top: 118 attributes
      - When-Created, NT-Security-Descriptor, Object-Guid, USN-Changed, ...
      - Description, WWW-Home-Page, Is-Member-Of-DL, …

Schema



```
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> mmc
PS C:\Users\Administrator>
PS C:\Users\Administrator> regsvr32 schmmgmt.dll
PS C:\Users\Administrator> mmc /a
PS C:\Users\Administrator>
```

Console1 - [Console Root\Active Directory Schema [W2012R2AMR.example.cc
File
Action
View
Favorites
Window
Help

Console Root
- Active Directory Schema [W201
  - Classes
    - account
    - aCSPolicy
    - aCSResourceLimits
    - aCSSubnet
    - addressBookContainer
    - addressTemplate
    - applicationEntity
    - applicationProcess
    - applicationSettings
    - applicationSiteSettings
    - applicationVersion
    - attributeSchema
    - bootableDevice
    - builtinDomain

Name	Type	Syste...	De
uid	Optional	No	A u
host	Optional	No	Th
ou	Optional	No	Or
o	Optional	No	Or
l	Optional	No	Lo
seeAlso	Optional	No	See
description	Optional	No	De
msDS-ReplValueMetaDa...	Optional	Yes	ms
msDS-parentdistname	Optional	Yes	ms
msds-memberTransitive	Optional	Yes	ms
msds-memberOfTransiti...	Optional	Yes	ms
msDS-TDOEgressBL	Optional	Yes	Ba
msDS-TDOIngressBL	Optional	Yes	Ba
msDS-ValueTypeReferen...	Optional	Yes	Th
msDS-IsPrimaryComput...	Optional	Yes	Ba

description Properties

General

description

Description: Description

Common Name: Description

X.500 OID: 2.5.4.13

Syntax and Range

Syntax: Unicode String

Minimum: 0

Maximum: 1024

This attribute is multi-valued.

☑ Attribute is active
☐ Index this attribute
☐ Ambiguous Name Resolution (ANR)
☑ Replicate this attribute to the Global Catalog
☐ Attribute is copied when duplicating a user
☐ Index this attribute for containerized searches

Schema

- **MS Exchange extension**
- **Your own extension**
  - `ldifde.exe -v -i -f mySuperSchemaExt.ldif`
  - Syntax for attributes and objectClass
  - Validate each record by

```
dn:
changetype: modify
add: schemaUpdateNow
schemaUpdateNow: 1
-
```

Example

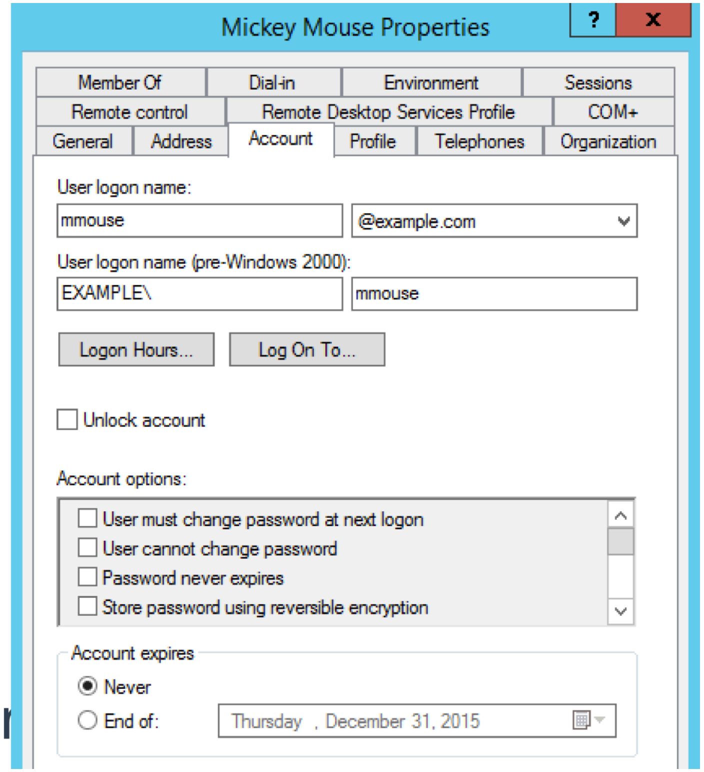
```
dn: CN=myUniqueKey,CN=Schema,CN=Configuration,DC=example,DC=com
changetype: add
adminDescription: myUniqueKey
adminDisplayName: myUniqueKey
attributeID: 1.3.6.1.4.1.38427.389.200.2
attributeSyntax: 2.5.5.12
cn: myUniqueKey
IsDefunct: FALSE
isMemberOfPartialAttributeSet: TRUE
isSingleValued: FALSE
lDAPDisplayName: myUniqueKey
objectClass: attributeSchema
objectClass: top
oMSyntax: 64
rangeLower: 1
rangeUpper: 64
searchFlags: 5
showInAdvancedViewOnly: FALSE
systemOnly: FALSE

dn:
changetype: modify
add: schemaUpdateNow
schemaUpdateNow: 1
-
```

```
dn: CN=myUser,CN=Schema,CN=Configuration,..
changetype: ntdsschemaadd
adminDescription: Auxiliary class for USER
adminDisplayName: myUser
cn: myUser
defaultHidingValue: FALSE
defaultSecurityDescriptor: D:S:
governsID: 1.3.6.1.4.1.38427.389.100.1
IsDefunct: FALSE
ldapDisplayName: myUser
mayContain: myUniqueKey
objectClass: classSchema
objectClass: top
objectClassCategory: 3
possSuperiors: user
rDNAttID: cn
showInAdvancedViewOnly: FALSE
subClassOf: user
systemOnly: FALSE
```

Common objects

- **Users**
  - SamAccountName
  - UserPrincipalName
  - UserAccountControl
  - Some common values
    - 512 / 514 (Enabled/Disabled)
    - 66048 / 66050 same but Password never
    - 262688/ 262690 same but Smartcard required
  - Advanced

```
(!(userAccountControl=2)) vs
(!(userAccountControl:1.2.840.113556.1.4.803:=2))
```



User logon name:
mmouse @example.com

User logon name (pre-Windows 2000):
EXAMPLE\ mmouse

□ Unlock account

Account options:
- □ User must change password at next logon
- □ User cannot change password
- □ Password never expires
- □ Store password using reversible encryption

Account expires
- ● Never
- ○ End of: Thursday , December 31, 2015

Common objects

- **Group of users, contacts, computers, groups**
- **Group type**
  - Security *`(groupType=2147483648)`*
  - Distribution *`(!(groupType=*))`*
- **Group scope**
  - Domain local *`(groupType=4)`*
  - Global *`(groupType=2)`*
  - Universal *`(groupType=8)`*

Group membership

- **the cross domain challenge**

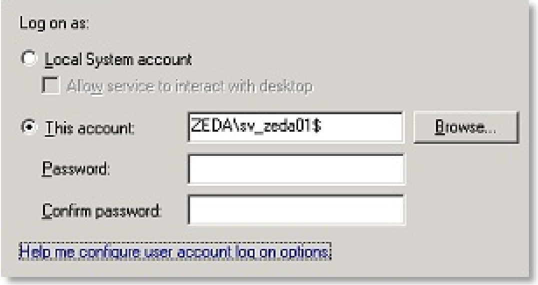
```
(&(objectclass=user)
(memberof=CN=grp1,OU=Groups,DC=example,DC=com))
```

- **nested groups**

```
(&(objectclass=group)
(member:1.2.840.113556.1.4.1941:=CN=user.99,OU=Users,DC=example,DC=com))
```

Common objects

- **Contacts** (no SSID = no authN)
- **Computers** *`(objectclass=computer)`*
- **Others**
  - Managed Service Account (2008R2 ->, Win7 ->)
    - New-ADServiceAccount [accountname]
    - Install-ADServiceAccount [accountname]



Log on as:

○ Local System account

□ Allow service to interact with desktop

● This account: ZEDA\sv_zeda01$

Password:

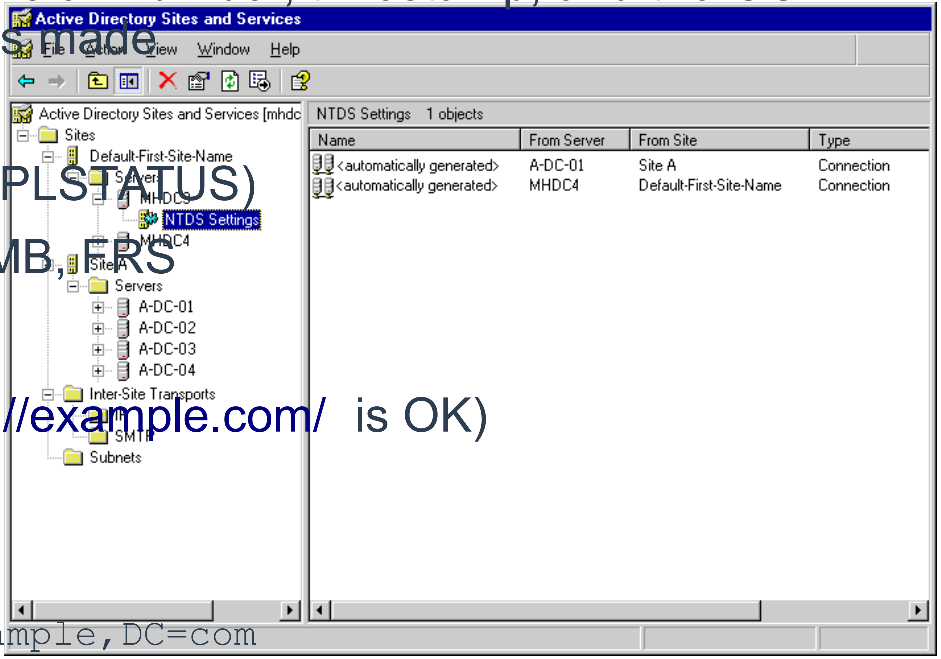
Confirm password:

Windows domain

- **GUID**
  - Global Unique Identifier = 128 bits uniqueKey = objectGUID
  - Unique across the world for each object
- **SSID**
  - Security Identifier from NT users and groups, stored in objectSID
  - For ACL and access rights
  - Can change when moving the hosting domain (Merge, split, migrate)
  - `S-1-5-32-544` :
    - A revision level, 1
    - An identifier authority value, 5 (NT Authority)
    - A domain identifier, 32 (Builtin)
    - A relative identifier, 544 (Administrators)
    - A relative identifier, 513 (domain users)

Windows domain

- **Replication**
  - One or more sites
  - Update Sequence Number (USN)
  - Stamps - Each object has a stamp with the version number, timestamp, and the GUID of the domain controller where the change was made
  - Knowledge Consistency Checker (KCC)
  - REPADMIN /SHOWREPL * /CSV (now ADREPLSTATUS)
  - LDAP (389,636,3268) and Kerberos, DNS, SMB, FRS
- **Global catalog**
  - Domain wise and not server specific (=> ldap://example.com/ is OK)
  - Subset of entries and data
  - Find servers hosting GC
    - BaseDN: `cn=sites,CN=Configuration,DC=example,DC=com`
    - Scope: subtree
    - Filter: `(&(objectCategory=nTDSDSA)(options:1.2.840.113556.1.4.803:=1))`



NTDS Settings 1 objects

Name	From Server	From Site	Type
<automatically generated>	A-DC-01	Site A	Connection
<automatically generated>	MHDC4	Default-First-Site-Name	Connection

Authentication

- user identification
- id/password
  - DN, GUID (LDAP://servername/<GUID=XXXXX>), SID
- Kerberos
- Strong authentication (Certificate)
- FIDO in future AD release
- Machine authentication

Access rights

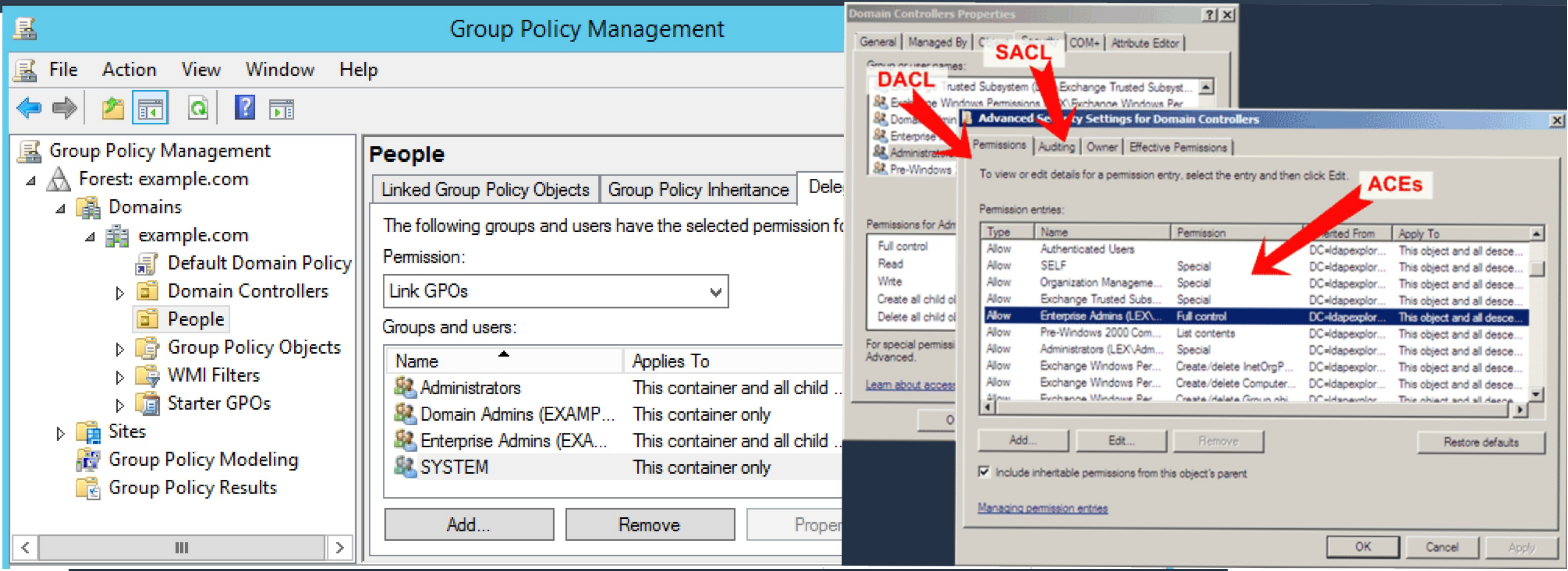
- **default behavior**
- **Security descriptor vs Access Control List**
  - NTSecurityDescriptor
  - msExchMailboxSecurityDescriptor
- **Manage access rights**
  - Group Policy Management Console (GPMC)
  - dsacls.exe

    ```
    dsacls “cn=mickey mouse,ou=people,dc=example,dc=com”
    ```

  - Powershell

    ```
    (Get-Acl 'cn=mickey
    mouse,ou=people,dc=example,dc=com').access | ft
    identityreference, accesscontroltype -AutoSize
    ```

Access rights



People

Linked Group Policy Objects | Group Policy Inheritance | Dele

The following groups and users have the selected permission f

Permission: Link GPOs

Groups and users:

Name	Applies To
Administrators	This container and all child ..
Domain Admins (EXAMP...	This container only
Enterprise Admins (EXA...	This container and all child ..
SYSTEM	This container only

Group or user names:
Trusted Subsystem (... \Exchange Trusted Subsyst...
Exchange Windows Permissions ...\Exchange Windows Per
Doma...
Enterprise ...
Administrato...
Pre-Windows ...

Permissions for Adm

Full control
Read
Write
Create all child ol
Delete all child ol

For special permissi Advanced.

Learn about acces

Advanced Security Settings for Domain Controllers

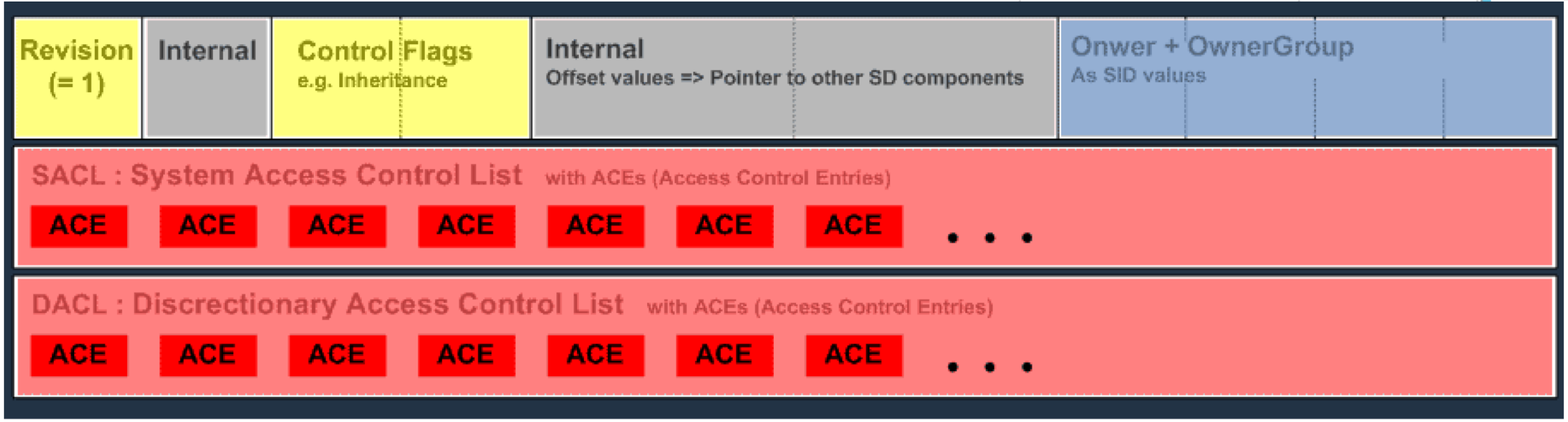
To view or edit details for a permission entry, select the entry and then click Edit.

Permission entries:

Type	Name	Permission	Inherited From	Apply To
Allow	Authenticated Users		DC=ldapexplor...	This object and all desce...
Allow	SELF	Special	DC=ldapexplor...	This object and all desce...
Allow	Organization Manageme...	Special	DC=ldapexplor...	This object and all desce...
Allow	Exchange Trusted Subs...	Special	DC=ldapexplor...	This object and all desce...
Allow	Enterprise Admins (LEX\...	Full control	DC=ldapexplor...	This object and all desce...
Allow	Pre-Windows 2000 Com...	List contents	DC=ldapexplor...	This object and all desce...
Allow	Administrators (LEX\Adm...	Special	DC=ldapexplor...	This object and all desce...
Allow	Exchange Windows Per...	Create/delete InetOrgP...	DC=ldapexplor...	This object and all desce...
Allow	Exchange Windows Per...	Create/delete Computer...	DC=ldapexplor...	This object and all desce...
Allow	Exchange Windows Per...	Create/delete Group obj...	DC=ldapexplor...	This object and all desce...

☑ Include inheritable permissions from this object's parent

Managing permission entries



Revision (= 1)	Internal	Control Flags e.g. Inheritance	Internal Offset values => Pointer to other SD components	Onwer + OwnerGroup As SID values

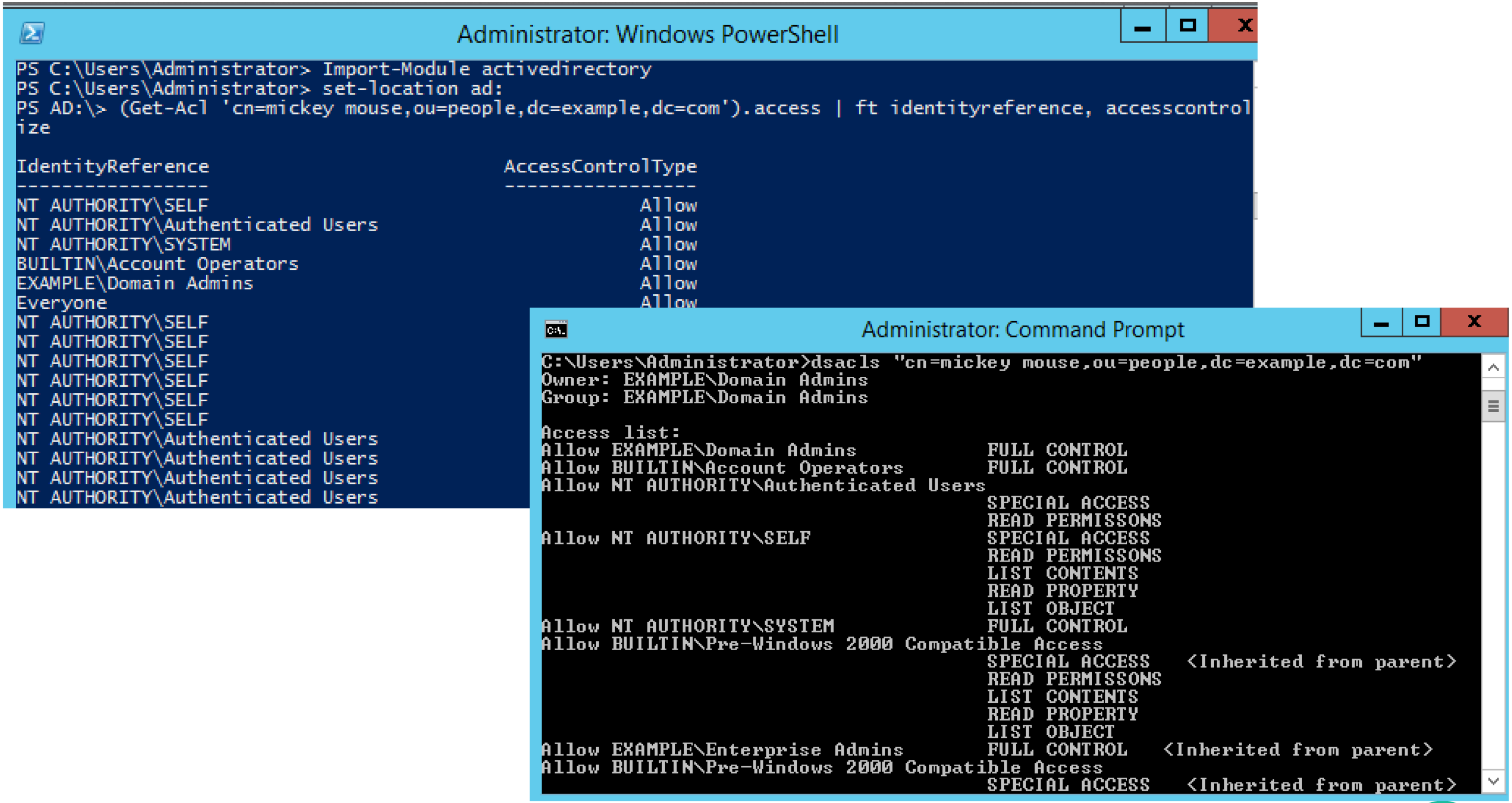
SACL : System Access Control List with ACEs (Access Control Entries)

ACE ACE ACE ACE ACE ACE ACE . . .

DACL : Discrectionary Access Control List with ACEs (Access Control Entries)

ACE ACE ACE ACE ACE ACE ACE . . .

Access rights

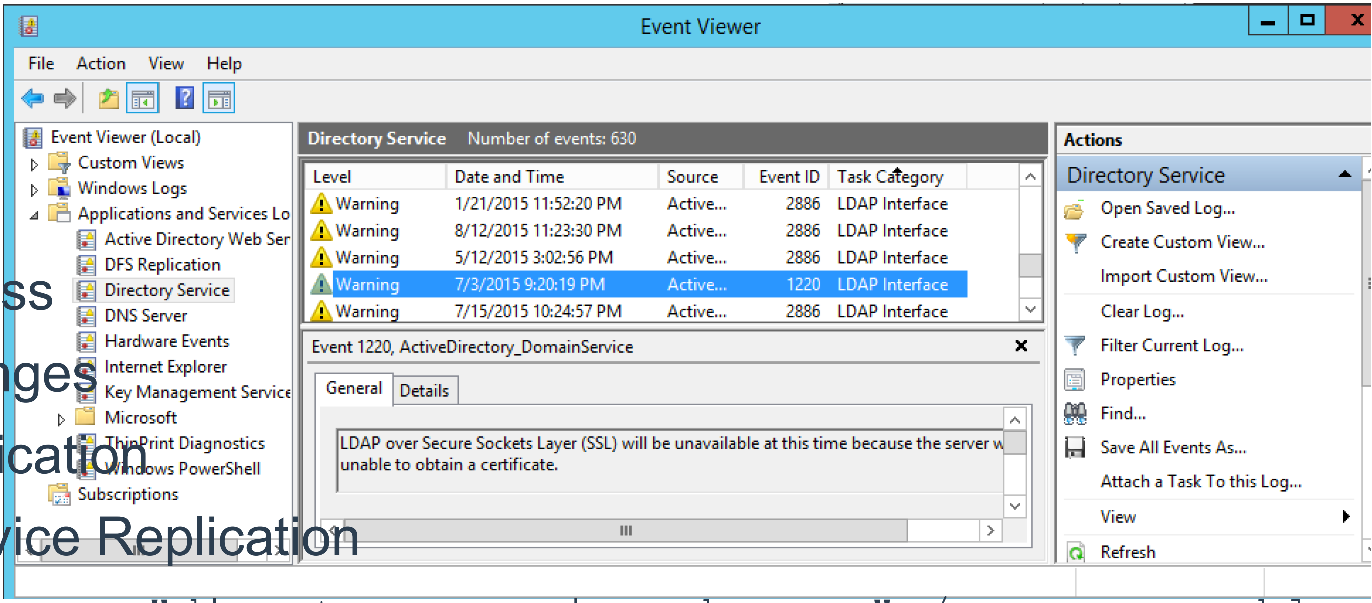


```
PS C:\Users\Administrator> Import-Module activedirectory
PS C:\Users\Administrator> set-location ad:
PS AD:\> (Get-Acl 'cn=mickey mouse,ou=people,dc=example,dc=com').access | ft identityreference, accesscontrol
ize

IdentityReference                          AccessControlType
-----------------                          -----------------
NT AUTHORITY\SELF                                      Allow
NT AUTHORITY\Authenticated Users                       Allow
NT AUTHORITY\SYSTEM                                    Allow
BUILTIN\Account Operators                              Allow
EXAMPLE\Domain Admins                                  Allow
Everyone                                               Allow
NT AUTHORITY\SELF
NT AUTHORITY\SELF
NT AUTHORITY\SELF
NT AUTHORITY\SELF
NT AUTHORITY\SELF
NT AUTHORITY\SELF
NT AUTHORITY\Authenticated Users
NT AUTHORITY\Authenticated Users
NT AUTHORITY\Authenticated Users
NT AUTHORITY\Authenticated Users
```

```
C:\Users\Administrator>dsacls "cn=mickey mouse,ou=people,dc=example,dc=com"
Owner: EXAMPLE\Domain Admins
Group: EXAMPLE\Domain Admins

Access list:
Allow EXAMPLE\Domain Admins                FULL CONTROL
Allow BUILTIN\Account Operators            FULL CONTROL
Allow NT AUTHORITY\Authenticated Users
                                           SPECIAL ACCESS
                                           READ PERMISSONS
Allow NT AUTHORITY\SELF                    SPECIAL ACCESS
                                           READ PERMISSONS
                                           LIST CONTENTS
                                           READ PROPERTY
                                           LIST OBJECT
Allow NT AUTHORITY\SYSTEM                  FULL CONTROL
Allow BUILTIN\Pre-Windows 2000 Compatible Access
                                           SPECIAL ACCESS    <Inherited from parent>
                                           READ PERMISSONS
                                           LIST CONTENTS
                                           READ PROPERTY
                                           LIST OBJECT
Allow EXAMPLE\Enterprise Admins            FULL CONTROL    <Inherited from parent>
Allow BUILTIN\Pre-Windows 2000 Compatible Access
                                           SPECIAL ACCESS    <Inherited from parent>
```

Logs

- **Event viewer**
- **GPO**
  - Directory Service Access
  - Directory Service Changes
  - Directory Service Replication
  - Detailed Directory Service Replication



Directory Service Number of events: 630

Level	Date and Time	Source	Event ID	Task Category
Warning	1/21/2015 11:52:20 PM	Active...	2886	LDAP Interface
Warning	8/12/2015 11:23:30 PM	Active...	2886	LDAP Interface
Warning	5/12/2015 3:02:56 PM	Active...	2886	LDAP Interface
Warning	7/3/2015 9:20:19 PM	Active...	1220	LDAP Interface
Warning	7/15/2015 10:24:57 PM	Active...	2886	LDAP Interface

Event 1220, ActiveDirectory_DomainService

General | Details

LDAP over Secure Sockets Layer (SSL) will be unavailable at this time because the server w
unable to obtain a certificate.

- `auditpol /set /subcategory:"directory service changes" /success:enable`
- **In SASLs**
- **LDAP logging**
  - → 2012
  - 2012 →
    `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics\"16 LDAP Interface Events"=dword:00000005`

Tools

- **Microsoft Management Console (MMC)**
- **ADUC vs ADAC**
- **adsiedit.msc**
- **ldp.exe**
- **ldifde.exe**

```
ldifde -i -u -f myData.ldif -s server:port -b username domain
password -j . -c "cn=Configuration,DC=xxxx"
```

- **DS tools (dsquery, dsadd, dsmod, dsacls)**
- **Powershell**
  - `Import-Module ActiveDirectory -PSSession $s`

Password policy

Reset password: the challenge

- **Prepare access rights**
  - Create a basic domain account with no additional privileges
  - Use Delegate control wizard from within ADUC
    - User objects
    - Reset password
    - Write lockoutTime (if unlock is enabled)
    - Write shadowlastchange
- **Prepare Password**

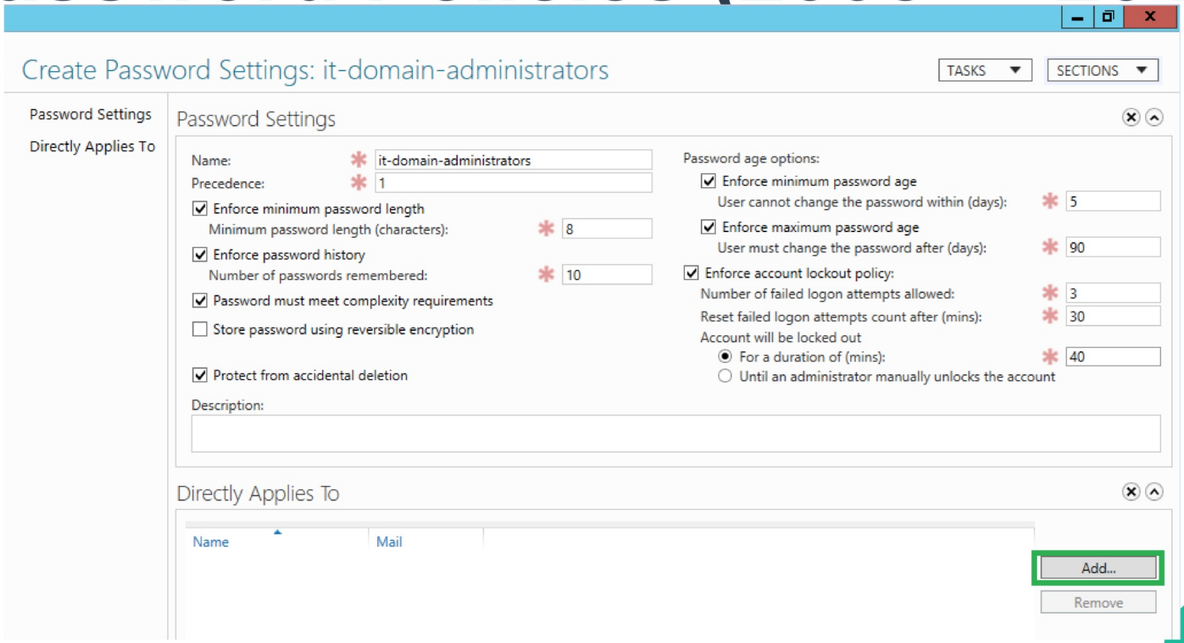
  MySecretPassword → **double quote** → “MySecretPassword” → **base64 UTF-16** →
  IAAcIE0AeQBTAGUAYwByAGUAdABQAGEAcwBzAHcAbwByAGQAHSA=
- **Apply to user**

  LDAPS → ldapmodify

  UnicodePwd::
  IAAcIE0AeQBTAGUAYwByAGUAdABQAGEAcwBzAHcAbwByAGQAHSA=

Password policy

- **Default domain password policy (gpmc.msc)**
  - Password Policy (history, strength)
  - Account Lockout Policy ()
- **F̲ine-G̲rained P̲assword Policies (2008 -> 2012 -> GUI in ADAC**



Create Password Settings: it-domain-administrators

Password Settings

Name: it-domain-administrators
Precedence: 1
☑ Enforce minimum password length
Minimum password length (characters): 8
☑ Enforce password history
Number of passwords remembered: 10
☑ Password must meet complexity requirements
□ Store password using reversible encryption

☑ Protect from accidental deletion

Description:

Password age options:
☑ Enforce minimum password age
User cannot change the password within (days): 5
☑ Enforce maximum password age
User must change the password after (days): 90
☑ Enforce account lockout policy:
Number of failed logon attempts allowed: 3
Reset failed logon attempts count after (mins): 30
Account will be locked out
● For a duration of (mins): 40
○ Until an administrator manually unlocks the account

Directly Applies To

Name	Mail

Looking around

- AD LDS
- ADFS (Identity federation)
- Microsoft Azure Active Directory

Conclusion

- Active Directory is a true LDAP server
- Multiple MS tools set
- Standard and MS oriented approach coexist
- Take time to discover and test capabilities

Questions are welcome now or later