CompTIA Security+

SY0-601

08- Implementing Identity and Account Management Controls

Ahmed Sultan
Senior Technical Instructor
ahmedsultan.me/about

Outlines

8.1- Implement Identity and Account Types

8.2- Implement Account Policies

Labs

Lab 10: Managing Access Controls in Windows Server

Lab 11: Configuring a System for Auditing Policies

Lab 12: Managing Access Controls in Linux

8.1- Implement Identity and Account Types

8.2- Implement Account Policies

IDENTITY MANAGEMENT CONTROLS

- **Identity and access management (IAM)** involves both IT/security procedures and technologies and Human Resources (HR) policies.
- A background check determines that a person is who they say they are and are not concealing criminal activity, bankruptcy, or connections that would make them unsuitable or risky.
- For some jobs, especially federal jobs requiring a security clearance, background checks are mandatory.
- Some background checks are performed internally, whereas others are done by an external third party.

IDENTITY MANAGEMENT CONTROLS (cont.)

- **Onboarding** at the HR level is the process of welcoming a new employee to the organization.
- As part of onboarding, the IT and HR function will combine to create an account for the user to access the computer system, assign the appropriate privileges, and ensure the account credentials are known only to the valid user.
- These functions must be integrated, to avoid creating accidental configuration vulnerabilities, such as IT creating an account for an employee who is never actually hired.

IDENTITY MANAGEMENT CONTROLS (cont.)

- The terms of an **NonDisclosure Agreement (NDA)** might be incorporated within the employee contract or could be a separate document.
- When an employee or contractor signs an NDA, they are asserting that they will not share confidential information with a third party.

PERSONNEL POLICIES FOR PRIVILEGE MANAGEMENTs

- HR and IT must collaborate to ensure effective privilege management.
- These policies aim to ensure that the risk of insider threat is minimized.

- **Separation of Duties**
  - ✓ Separation of duties is a means of establishing checks and balances against the possibility that critical systems or procedures can be compromised by insider threats.
  - ✓ Duties and responsibilities should be divided among individuals to prevent ethical conflicts or abuse of powers.

PERSONNEL POLICIES FOR PRIVILEGE MANAGEMENT (cont.)

- **Least Privilege**
  - ✓ Least privilege means that a user is granted sufficient rights to perform his or her job and no more.
  - ✓ This mitigates risk if the account should be compromised and fall under the control of a threat actor.
  - ✓ Least privilege should be ensured by closely analyzing business workflows to assess what privileges are required and by performing regular account audits.

PERSONNEL POLICIES FOR PRIVILEGE MANAGEMENT (cont.)

- **Job Rotation**
  - ✓ Job rotation (or rotation of duties) means that no one person is permitted to remain in the same job for an extended period.
  - ✓ For example, managers may be moved to different departments periodically, or employees may perform more than one job role, switching between them throughout the year.
  - ✓ Rotating individuals into and out of roles, such as the firewall administrator or access control specialist, helps an organization ensure that it is not tied too firmly to any one individual because vital institutional knowledge is spread among trusted employees.
  - ✓ Job rotation also helps prevent abuse of power, reduces boredom, and enhances individuals' professional skills.

PERSONNEL POLICIES FOR PRIVILEGE MANAGEMENT (cont.)

- **Mandatory Vacation**
  - ✓ Mandatory vacation means that employees are forced to take their vacation time, during which someone else fulfills their duties.
  - ✓ The typical mandatory vacation policy requires that employees take at least one vacation a year in a full-week increment so that they are away from work for at least five days in a row.
  - ✓ During that time, the corporate audit and security employees have time to investigate and discover any discrepancies in employee activity.

OFFBOARDING POLICIES

- **Offboarding** is the process of ensuring that an employee leaves a company gracefully, It is also used when a project using contractors or third parties ends.
- In terms of security, there are several processes that must be completed:
  - ✓ Account management—disable the user account and privileges, Ensure that any information assets created or managed by the employee but owned by the company are accessible (in terms of encryption keys or password-protected files).
  - ✓ Company assets—retrieve mobile devices, keys, smart cards, USB media, and so on, The employee will need to confirm (and in some cases prove) that they have not retained copies of any information assets.
  - ✓ Personal assets—wipe employee-owned devices of corporate data and applications, The employee may also be allowed to retain some information assets (such as personal emails or contact information), depending on the policies in force.

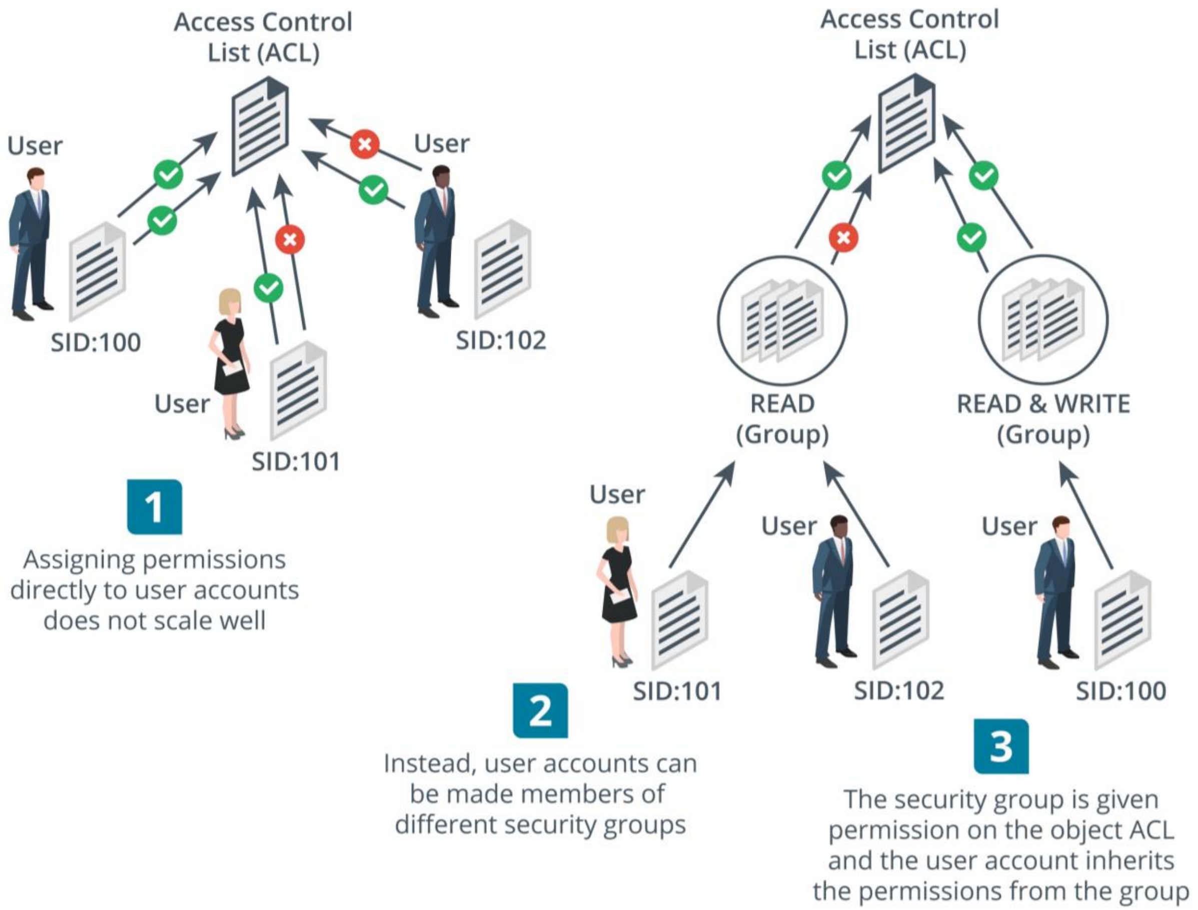
SECURITY ACCOUNT TYPES AND CREDENTIAL MANAGEMENT

- Operating systems, network appliances, and network directory products use some standard account types as the basis of a privilege management system.
- These include **standard user**, **administrative user**, **security group accounts**, and **service accounts**.
- Guest Accounts
  - ✓ A guest account is a special type of shared account with no password.
  - ✓ It allows anonymous and unauthenticated access to a resource.
  - ✓ The Windows OS creates guest user and group accounts when installed, but the guest user account is **disabled** by default.
  - ✓ Guest accounts are also created when installing web services, as most web servers allow unauthenticated access.

SECURITY GROUP-BASED PRIVILEGES

- The concept of a Security Group Account simplifies and centralizes the administrative process of assigning rights.
- Rather than assigning rights directly, the system owner assigns them to security group accounts.
- User accounts gain rights by being made a member of a security group.
- A user can be a member of multiple groups and can therefore receive rights and permissions from several sources.

SECURITY GROUP-BASED PRIVILEGES (cont.)


Access Control List (ACL)
User
SID:100
User
SID:101
User
SID:102
1
Assigning permissions directly to user accounts does not scale well
Access Control List (ACL)
READ (Group)
READ & WRITE (Group)
User
SID:101
User
SID:102
User
SID:100
2
Instead, user accounts can be made members of different security groups
3
The security group is given permission on the object ACL and the user account inherits the permissions from the group

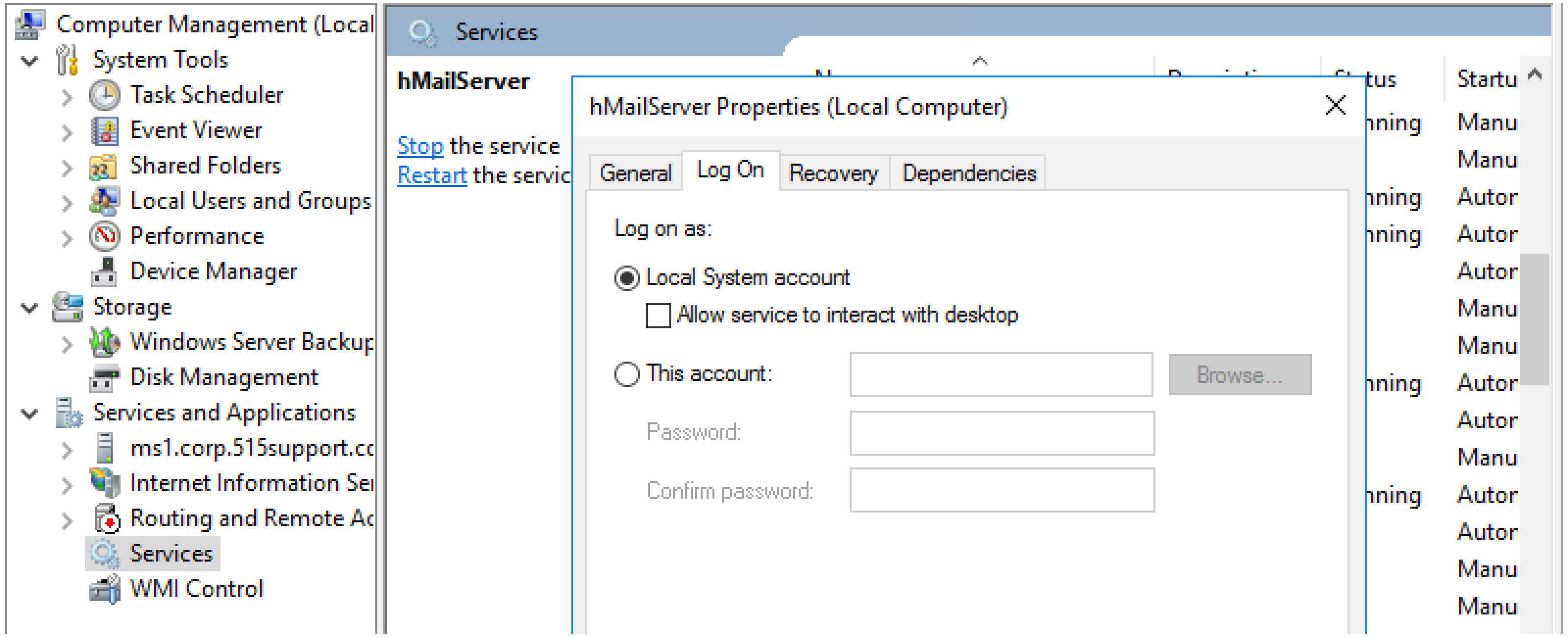
ADMINISTRATOR/ROOT ACCOUNTS

- Administrative or privileged accounts are able to install and remove apps and device drivers, change system-level settings, and access any object in the file system.
- In practice, it is very hard to eliminate the presence of default administrator accounts.
- A default account is one that is created by the operating system or application when it is installed.
- The default account has every permission available.
- In Windows, this account is called Administrator; in Linux, it is called root.
- This type of account is also referred to as a **superuser**.

SERVICE ACCOUNTS

- Service Accounts are used by scheduled processes and application server software, such as databases.
- Windows has several default service account types.
- These do not accept user interactive logons but can be used to run processes and background services:
  - ✓ System—has the most privileges of any Windows account, The local system account creates the host processes that start Windows before the user logs on, Any process created using the system account will have full privileges over the local computer.
  - ✓ Local Service—has the same privileges as the standard user account, It can only access network resources as an anonymous user.
  - ✓ Network Service—has the same privileges as the standard user account but can present the computer's account credentials when accessing network resources.

SERVICE ACCOUNTS (cont.)



hMailServer Properties (Local Computer)

General | Log On | Recovery | Dependencies

Log on as:

● Local System account

□ Allow service to interact with desktop

○ This account: Browse...

Password:

Confirm password:

Lab

Lab 10: Managing Access Controls in Windows Server

8.1- Implement Identity and Account Types

8.2- Implement Account Policies

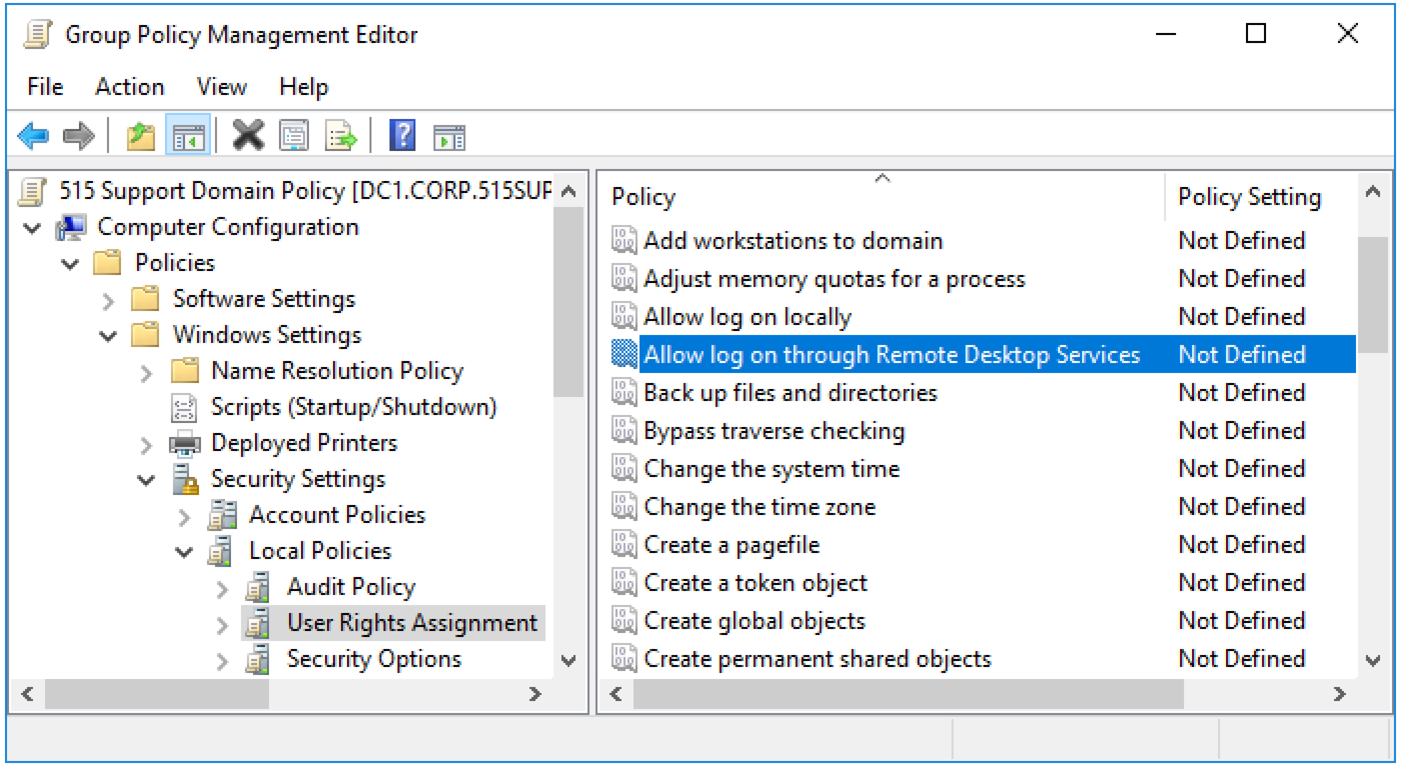
ACCOUNT ATTRIBUTES AND ACCESS POLICIES

- A user account is defined by a unique **Security Identifier (SID)**, a name, and a credential.
- Each account is associated with a profile.
- The profile can be defined with custom identity attributes describing the user, such as a full name, email address, contact number, department, and so on.
- The profile may support media, such as an account picture.
- As well as attributes, the profile will usually provide a location for storing user-generated data files (a home folder).

ACCOUNT ATTRIBUTES AND ACCESS POLICIES (cont.)

- Each account can be assigned permissions over files and other network resources and access policies or privileges over the use and configuration of network hosts.
- These permissions might be assigned directly to the account or inherited through membership of a security group or role.
- **Access policies** determine things like the right to log on to a computer locally or via remote desktop, install software, change the network configuration, and so on.
- On a **Windows Active Directory** network, access policies can be configured via group policy objects (GPOs).
- GPOs can be used to configure access rights for user/group/role accounts.

ACCOUNT ATTRIBUTES AND ACCESS POLICIES (cont.)



Policy	Policy Setting
Add workstations to domain	Not Defined
Adjust memory quotas for a process	Not Defined
Allow log on locally	Not Defined
Allow log on through Remote Desktop Services	Not Defined
Back up files and directories	Not Defined
Bypass traverse checking	Not Defined
Change the system time	Not Defined
Change the time zone	Not Defined
Create a pagefile	Not Defined
Create a token object	Not Defined
Create global objects	Not Defined
Create permanent shared objects	Not Defined

ACCOUNT PASSWORD POLICY SETTINGS

- System-enforced account policies can help to enforce credential management principles by stipulating requirements for user-selected passwords:
  - ✓ Password length—enforces a minimum length for passwords, There may also be a maximum length.
  - ✓ Password complexity—enforces password complexity rules (that is, no use of username within password and combination of at least eight upper/lower case alpha-numeric and non-alpha-numeric characters).
  - ✓ Password aging—forces the user to select a new password after a set number of days.
  - ✓ Password reuse and history—prevents the selection of a password that has been used already, The history attribute sets how many previous passwords are blocked.

ACCOUNT RESTRICTIONS

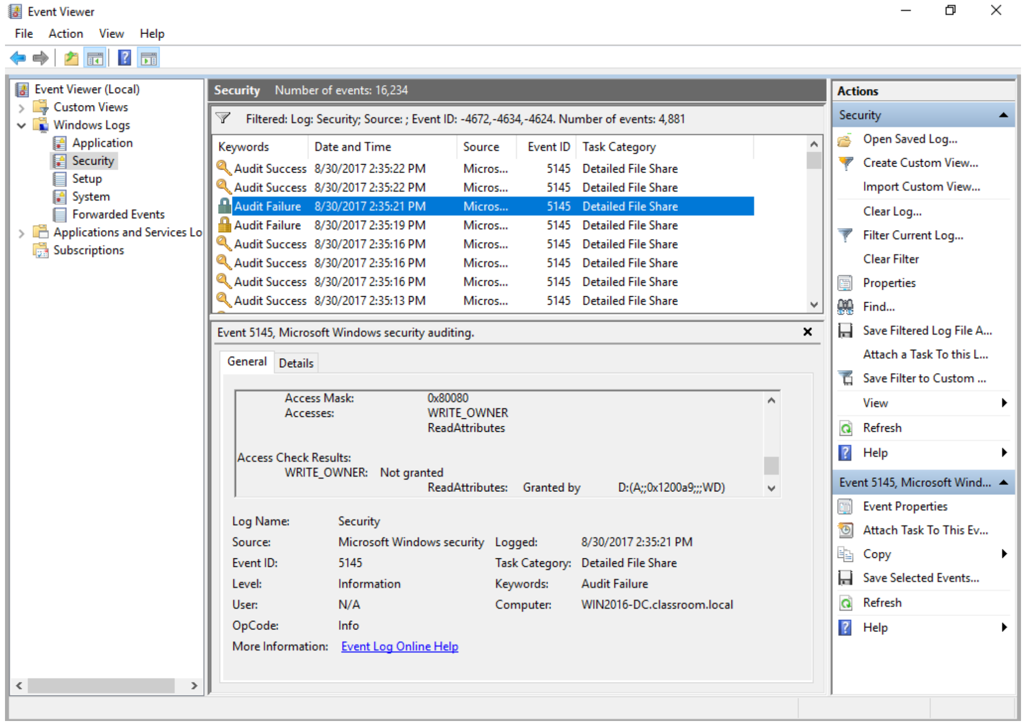
- To make the task of compromising the user security system harder, account restrictions can be used.
- Location-Based Policies
  - ✓ A user or device can have a logical network location, identified by an IP address, subnet, virtual LAN (VLAN), or organizational unit (OU).
  - ✓ This can be used as an account restriction mechanism.
  - ✓ For example, a user account may be prevented from logging on locally to servers within a restricted OU.
- Geofencing
  - ✓ Refers to accepting or rejecting access requests based on location.
  - ✓ Geofencing can also be used for push notification to send alerts or advice to a device when a user enters a specific area.
  - ✓ This is often used for asset management to ensure devices are kept with the proper location.

ACCOUNT AUDITS

- **Accounting and auditing processes** are used to detect whether an account has been compromised or is being misused.
- A security or audit log can be used to facilitate detection of account misuse:
  - ✓ Accounting for all actions that have been performed by users.
  - ✓ Change and version control systems depend on knowing when a file has been modified and by whom.
  - ✓ Accounting also provides for non-repudiation (that is, a user cannot deny that they accessed or made a change to a file).
  - ✓ The main problems are that auditing successful access attempts can quickly consume a lot of disk space, and analyzing the logs can be very time-consuming.
  - ✓ Detecting intrusions or attempted intrusions.

ACCOUNT AUDITS (cont.)

- Here records of failure-type events are likely to be more useful, though success-type events can also be revealing if they show unusual access patterns.



Security Number of events: 16,234

Filtered: Log: Security; Source: ; Event ID: -4672,-4634,-4624. Number of events: 4,881

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	8/30/2017 2:35:22 PM	Micros...	5145	Detailed File Share
Audit Success	8/30/2017 2:35:22 PM	Micros...	5145	Detailed File Share
Audit Failure	8/30/2017 2:35:21 PM	Micros...	5145	Detailed File Share
Audit Failure	8/30/2017 2:35:19 PM	Micros...	5145	Detailed File Share
Audit Success	8/30/2017 2:35:16 PM	Micros...	5145	Detailed File Share
Audit Success	8/30/2017 2:35:16 PM	Micros...	5145	Detailed File Share
Audit Success	8/30/2017 2:35:16 PM	Micros...	5145	Detailed File Share
Audit Success	8/30/2017 2:35:13 PM	Micros...	5145	Detailed File Share

Event 5145, Microsoft Windows security auditing.

General | Details

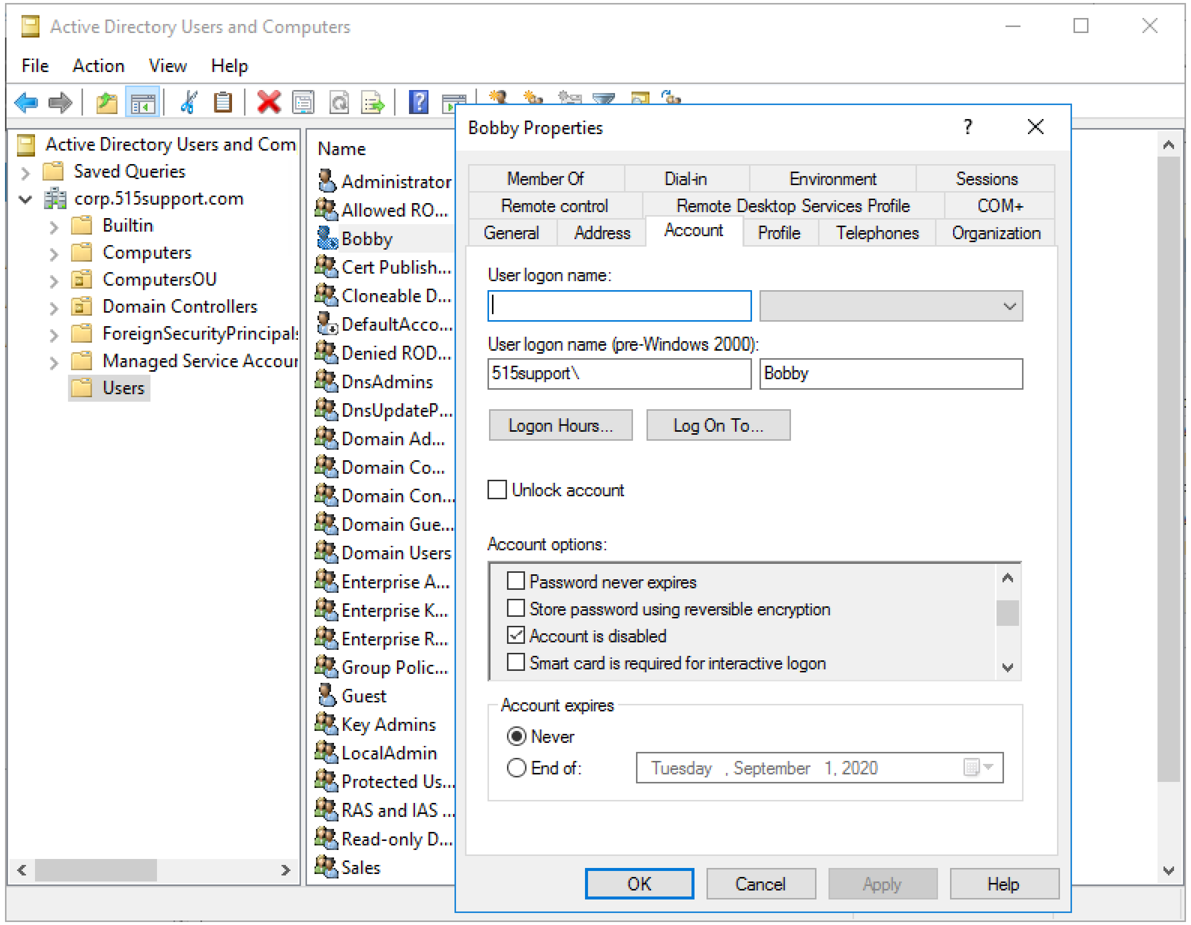
```
          Access Mask:              0x80080
          Accesses:                 WRITE_OWNER
                                    ReadAttributes

Access Check Results:
          WRITE_OWNER:   Not granted
                                    ReadAttributes:   Granted by      D:(A;;0x1200a9;;;WD)
```

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	8/30/2017 2:35:21 PM
Event ID:	5145	Task Category:	Detailed File Share
Level:	Information	Keywords:	Audit Failure
User:	N/A	Computer:	WIN2016-DC.classroom.local
OpCode:	Info		
More Information:	Event Log Online Help		

ACCOUNT LOCKOUT AND DISABLEMENT

- If account misuse is detected or suspected, the account can be manually disabled by setting an account property.
- This prevents the account from being used for login.
- Note that disabling the account does not close existing sessions.
- You can issue a remote logoff command to close a session.
- Account disablement means that login is permanently prevented until an administrator manually re-enables the account.

ACCOUNT LOCKOUT AND DISABLEMENT (cont.)



User logon name:

User logon name (pre-Windows 2000): 515support\ Bobby

☐ Unlock account

Account options:

- ☐ Password never expires
- ☐ Store password using reversible encryption
- ☑ Account is disabled
- ☐ Smart card is required for interactive logon

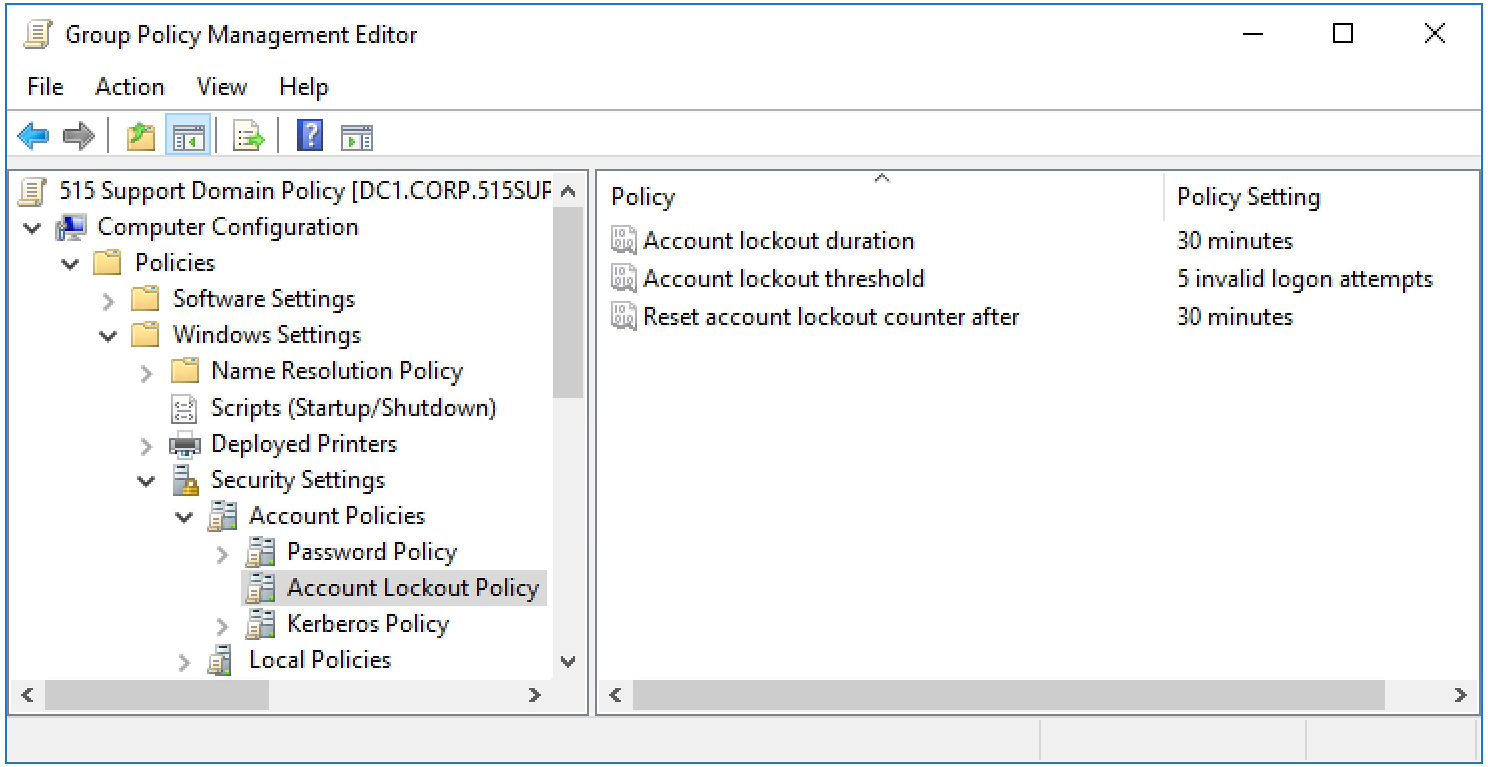
Account expires

- ● Never
- ○ End of: Tuesday , September 1, 2020

ACCOUNT LOCKOUT AND DISABLEMENT (cont.)

- An account lockout means that login is prevented for a period.
- This might be done manually if a policy violation is detected, but there are several scenarios for automatically applying a lockout:
  - ✓ An incorrect account password is entered repeatedly.
  - ✓ The account is set to expire, Setting an account expiration date means that an account cannot be used beyond a certain date, This option is useful on accounts for temporary and contract staff.
  - ✓ When using time- or location-based restrictions, the server periodically checks whether the user has the right to continue using the network, If the user does not have the right, then an automatic logout procedure commences.

ACCOUNT LOCKOUT AND DISABLEMENT (cont.)



Policy	Policy Setting
Account lockout duration	30 minutes
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	30 minutes

Lab

Lab 11: Configuring a System for Auditing Policies

Lab 12: Managing Access Controls in Linux