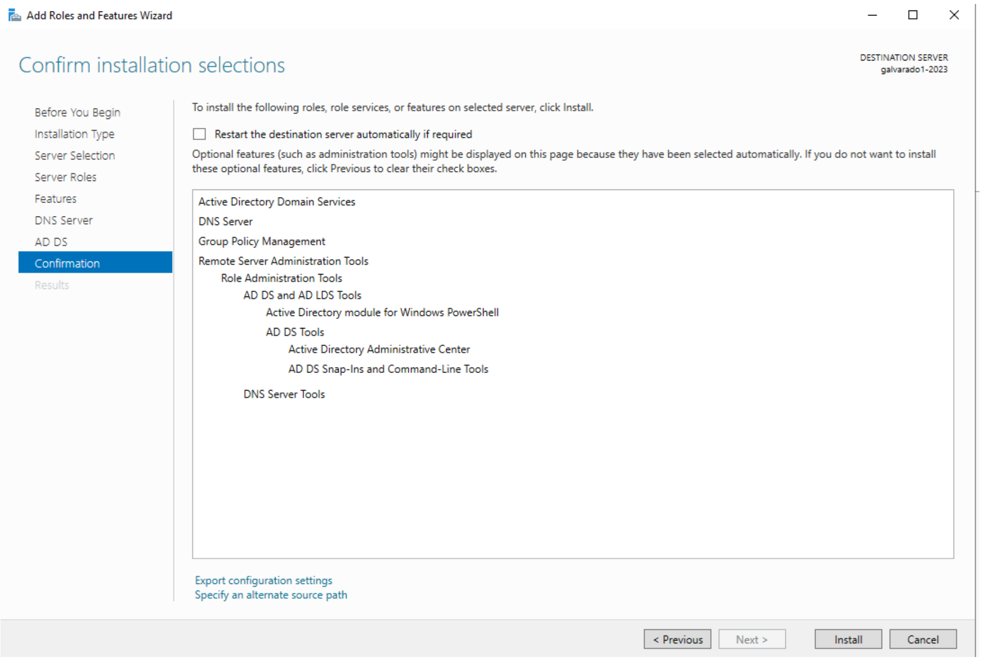
Guadalupe Alvarado

CIS 2650

Assignment 3

Installing DNS and Active Directory

Screenshot 1 – Showing the “Confirm installation selections” screen



To install the following roles, role services, or features on selected server, click Install.

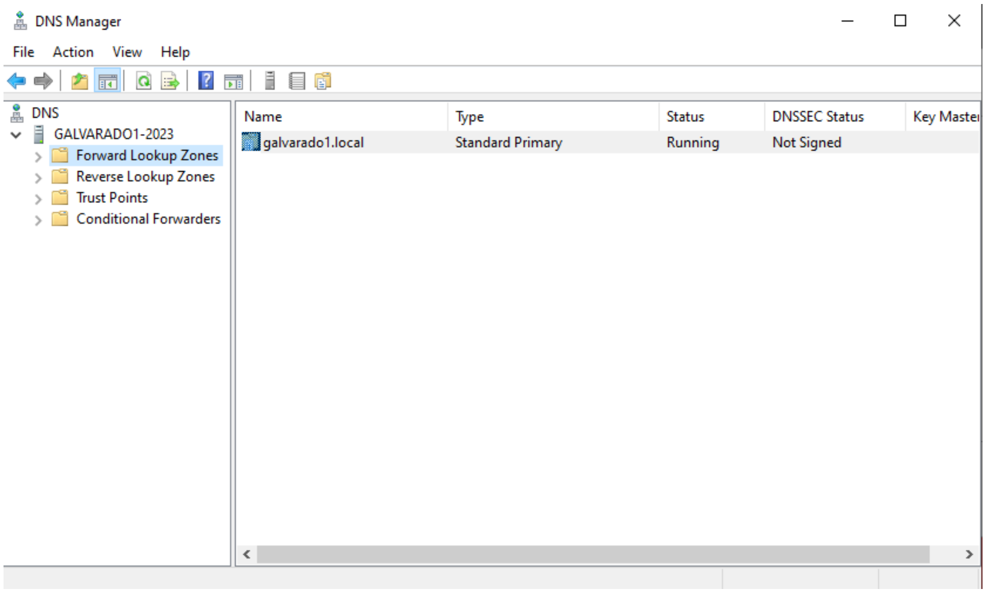
□ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

```
Active Directory Domain Services
DNS Server
Group Policy Management
Remote Server Administration Tools
    Role Administration Tools
        AD DS and AD LDS Tools
            Active Directory module for Windows PowerShell
            AD DS Tools
                Active Directory Administrative Center
                AD DS Snap-Ins and Command-Line Tools
        DNS Server Tools
```

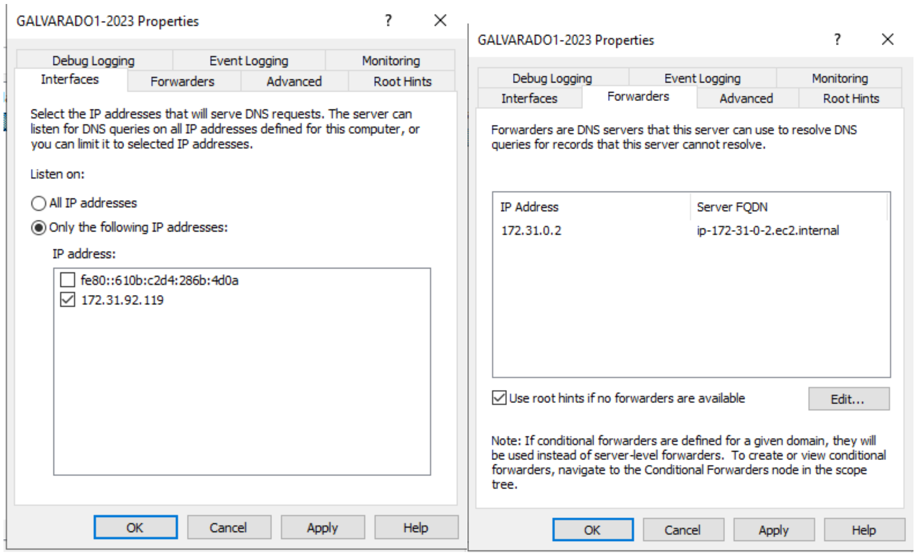
Preparing DNS for Active Directory

Screenshot 2 – Showing the DNS MMC window showing the new zone that you just created



Name	Type	Status	DNSSEC Status	Key Maste
galvarado1.local	Standard Primary	Running	Not Signed	

Screenshot 3 – **Showing the “Interfaces” tab and “Forwarders” tabs**



GALVARADO1-2023 Properties

Select the IP addresses that will serve DNS requests. The server can listen for DNS queries on all IP addresses defined for this computer, or you can limit it to selected IP addresses.

Listen on:

○ All IP addresses

● Only the following IP addresses:

IP address:

□ fe80::610b:c2d4:286b:4d0a

☑ 172.31.92.119

GALVARADO1-2023 Properties

Forwarders are DNS servers that this server can use to resolve DNS queries for records that this server cannot resolve.

IP Address	Server FQDN
172.31.0.2	ip-172-31-0-2.ec2.internal

☑ Use root hints if no forwarders are available

Note: If conditional forwarders are defined for a given domain, they will be used instead of server-level forwarders. To create or view conditional forwarders, navigate to the Conditional Forwarders node in the scope tree.

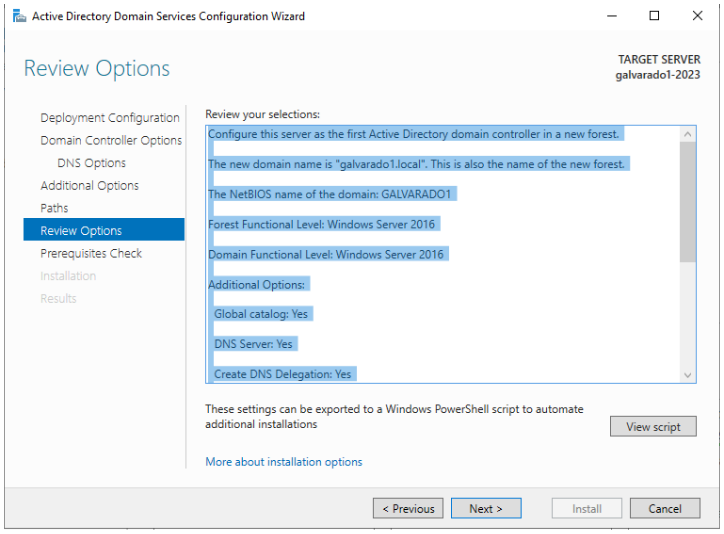
Question 1: In two to three paragraphs, describe the difference between the major DNS zone types (primary, secondary, forward, and reverse). Describe the process that DNS uses for zone transfers between primary and secondary zones.

A: **Primary DNS zones have the original domain data, and they allow changes. Secondary zones are read-only copies of the primary zones for backup and to help with high traffic. They keep updated through Zone Transfers. Forward zones change domain names to IP addresses, and reverse zones do the opposite.**

Zone transfers help keep data consistent between primary and secondary zones. The Secondary DNS server regularly checks the Primary DNS server for data changes. If there are changes, the Secondary server requests a data transfer. Transfers can be full (AXFR), where all data is sent, or incremental (IXFR), where only changed data is sent. IXFR is usually more efficient. Transfers are started by the secondary server to keep its data in sync with the primary server.

Configuring Active Directory

Screenshot 4 – Showing the "Review Options" screen



Review your selections:

Configure this server as the first Active Directory domain controller in a new forest.

The new domain name is "galvarado1.local". This is also the name of the new forest.

The NetBIOS name of the domain: GALVARADO1

Forest Functional Level: Windows Server 2016

Domain Functional Level: Windows Server 2016

Additional Options:

Global catalog: Yes

DNS Server: Yes

Create DNS Delegation: Yes

These settings can be exported to a Windows PowerShell script to automate additional installations

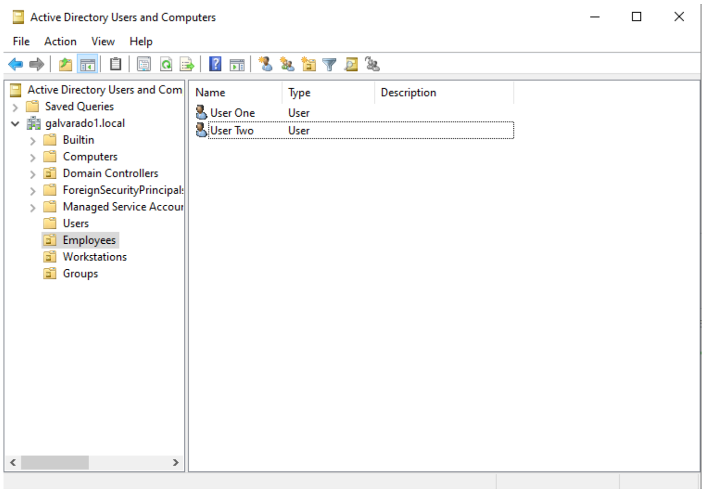
Question 2: In two to three paragraphs, describe what FSMO roles are. Detail each FSMO type and their purpose in Active Directory.

A: ***FSMO roles are unique roles assigned to domain controllers in Active Directory (AD). These roles handle special tasks and help prevent conflicts for smooth AD operations. There are two types of FSMO roles: forest-wide and domain-wide. Forest-wide roles are Schema Master and Domain Naming Master. The Schema Master oversees changes to the schema, which defines all objects and attributes in an AD forest. The Domain Naming Master manages changes to domain names, like adding, removing, or renaming them.***

Domain-wide roles are Relative ID (RID) Master, Primary Domain Controller (PDC) Emulator, and Infrastructure Master. The RID Master assigns relative IDs to each domain controller. The PDC Emulator handles password changes and creates group policy objects. The Infrastructure Master updates references from objects in its domain to objects in other domains.

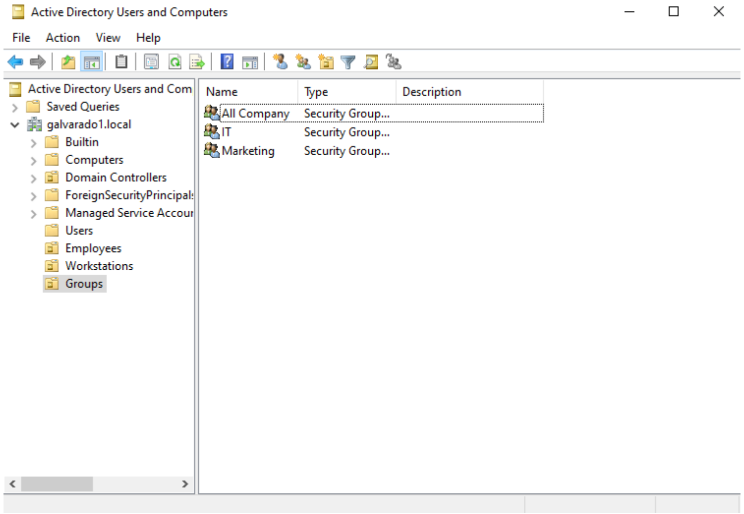
Adding Objects to Active Directory

Screenshot 5 – Showing the “Employees” OU with the two users in the OU



Name	Type	Description
User One	User	
User Two	User	

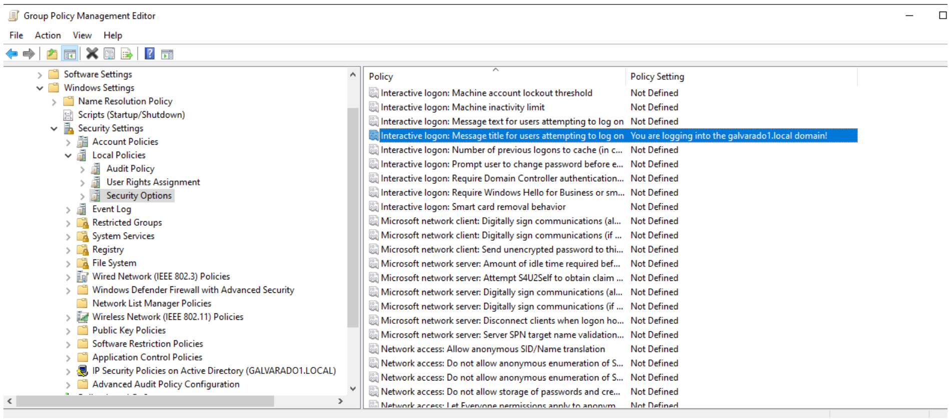
Screenshot 6 – Showing the “Groups” OU with the three groups you just created



Name	Type	Description
All Company	Security Group...	
IT	Security Group...	
Marketing	Security Group...	

Creating Group Policy Objects

Screenshot 7 – Showing the Group Policy settings in the Group Policy Management Window (expanded to show the settings you set above)



- Software Settings
- Windows Settings
  - Name Resolution Policy
  - Scripts (Startup/Shutdown)
  - Security Settings
    - Account Policies
    - Local Policies
      - Audit Policy
      - User Rights Assignment
      - Security Options
    - Event Log
    - Restricted Groups
    - System Services
    - Registry
    - File System
    - Wired Network (IEEE 802.3) Policies
    - Windows Defender Firewall with Advanced Security
    - Network List Manager Policies
    - Wireless Network (IEEE 802.11) Policies
    - Public Key Policies
    - Software Restriction Policies
    - Application Control Policies
    - IP Security Policies on Active Directory (GALVARADO1.LOCAL)
    - Advanced Audit Policy Configuration

Policy	Policy Setting
Interactive logon: Machine account lockout threshold	Not Defined
Interactive logon: Machine inactivity limit	Not Defined
Interactive logon: Message text for users attempting to log on	Not Defined
Interactive logon: Message title for users attempting to log on	You are logging into the galvarado1.local domain!
Interactive logon: Number of previous logons to cache (in c...	Not Defined
Interactive logon: Prompt user to change password before e...	Not Defined
Interactive logon: Require Domain Controller authentication...	Not Defined
Interactive logon: Require Windows Hello for Business or sm...	Not Defined
Interactive logon: Smart card removal behavior	Not Defined
Microsoft network client: Digitally sign communications (al...	Not Defined
Microsoft network client: Digitally sign communications (if ...	Not Defined
Microsoft network client: Send unencrypted password to thi...	Not Defined
Microsoft network server: Amount of idle time required bef...	Not Defined
Microsoft network server: Attempt S4U2Self to obtain claim ...	Not Defined
Microsoft network server: Digitally sign communications (al...	Not Defined
Microsoft network server: Digitally sign communications (if ...	Not Defined
Microsoft network server: Disconnect clients when logon ho...	Not Defined
Microsoft network server: Server SPN target name validation...	Not Defined
Network access: Allow anonymous SID/Name translation	Not Defined
Network access: Do not allow anonymous enumeration of S...	Not Defined
Network access: Do not allow anonymous enumeration of S...	Not Defined
Network access: Do not allow storage of passwords and cre...	Not Defined
Network access: Let Everyone permissions apply to anonym...	Not Defined

Question 3: Describe the differences between “User Settings” and “Computer Settings” in group policy.

***A:* In Group Policy, "User Settings" apply to users and affect the user environment regardless of the computer they use within the Active Directory domain. These settings can dictate desktop appearance, Control Panel access, network drives mapping, and more. On the other hand, "Computer Settings" apply to computers, impacting system services, file system, network configurations, and security settings, no matter who logs on. User Settings tailors the environment per user upon log-in, while Computer Settings defines system and security parameters for the computer upon boot-up.**

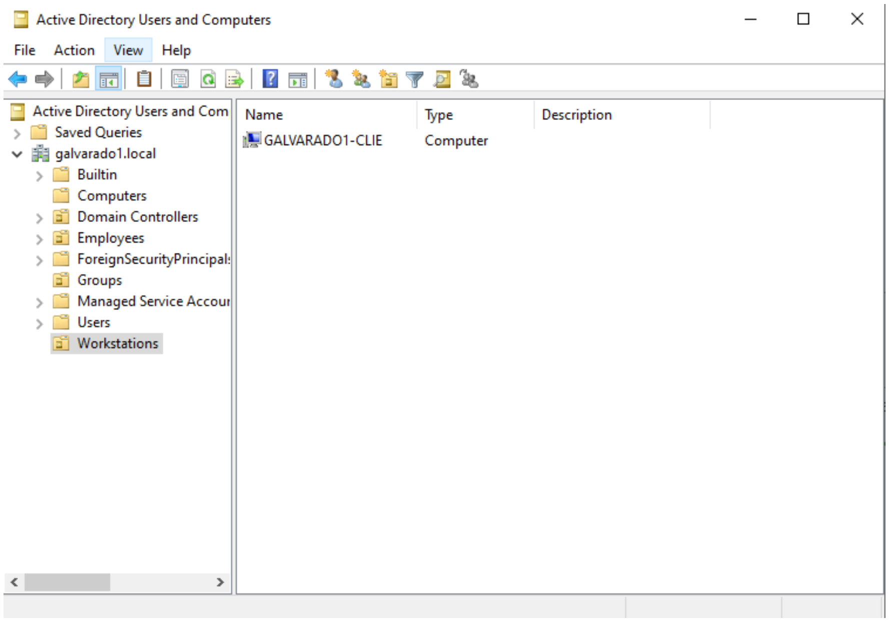
Question 4: Assume you have a single OU with three users. You want to create a GPO that applies to only one of those users. In two paragraphs, describe the options you have to filter the GPO to apply to only a subset of users in that OU.

***A:* One method to apply a Group Policy Object (GPO) to a single user in an Organizational Unit (OU) is through Security Filtering. This involves creating a GPO, linking it to the OU, and then specifying in the Security Filtering section which users the GPO applies to. Remove 'Authenticated Users' from the Security Filtering and add the specific user you want the policy to apply to.**

Alternatively, you can use Item-Level Targeting in Group Policy Preferences to control the application of GPO settings. This allows you to target specific users for individual preference items within the GPO. So, the GPO settings would apply only to the user you've specified. This method offers granular control, but it's only available in newer Windows Server versions and may not work with all policy settings.

Adding a computer to the Domain

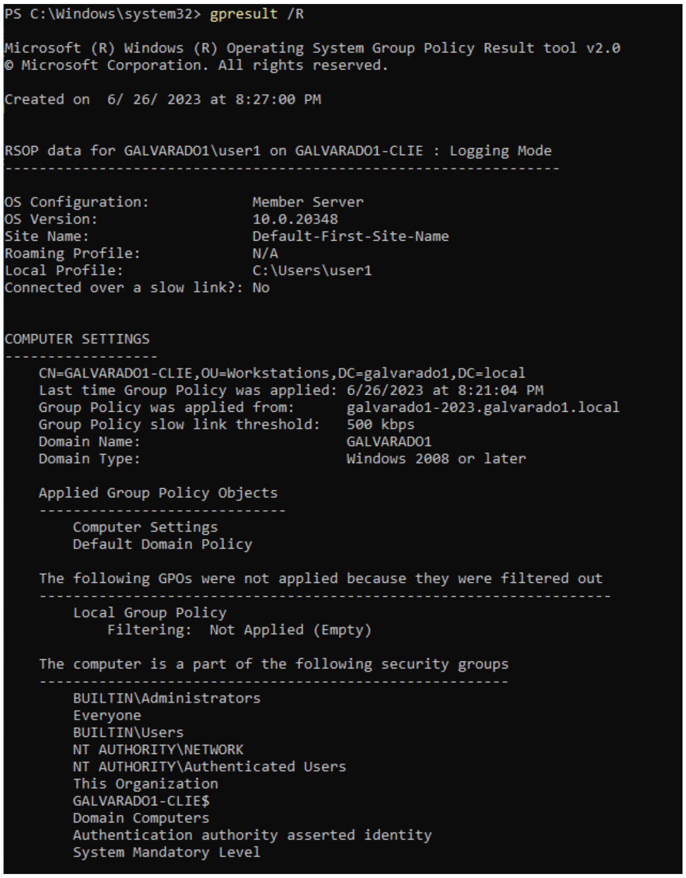
Screenshot 8 – Showing the new computer object in the “Workstations” OU



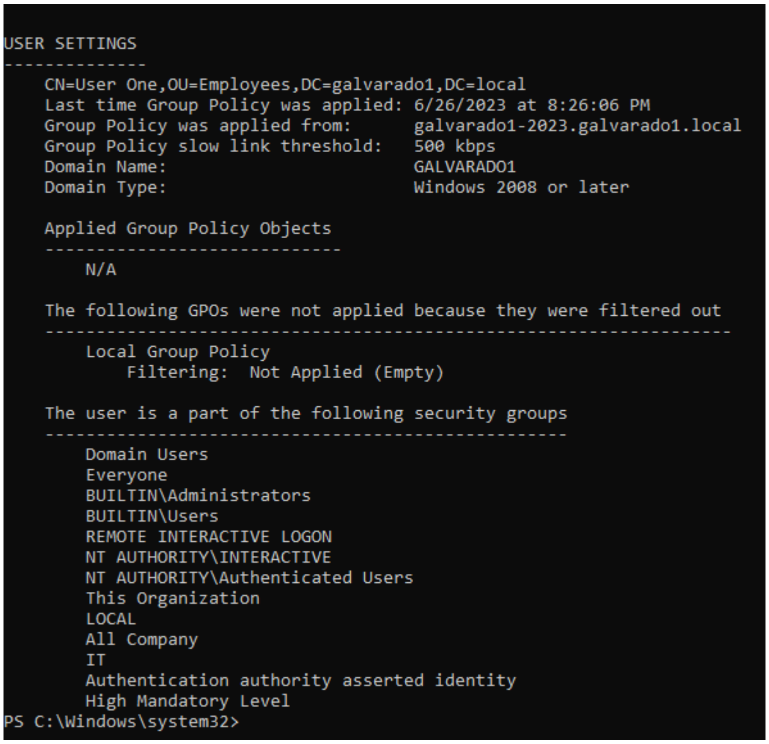
Name	Type	Description
GALVARADO1-CLIE	Computer	

Giving Domain Users Administrator Rights on Windows Client Computer

Screenshot 9 – Showing the output of the gpresult command



```
PS C:\Windows\system32> gpresult /R

Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
© Microsoft Corporation. All rights reserved.

Created on  6/ 26/ 2023 at 8:27:00 PM


RSOP data for GALVARADO1\user1 on GALVARADO1-CLIE : Logging Mode
-----------------------------------------------------------------

OS Configuration:            Member Server
OS Version:                  10.0.20348
Site Name:                   Default-First-Site-Name
Roaming Profile:             N/A
Local Profile:               C:\Users\user1
Connected over a slow link?: No


COMPUTER SETTINGS
------------------
    CN=GALVARADO1-CLIE,OU=Workstations,DC=galvarado1,DC=local
    Last time Group Policy was applied: 6/26/2023 at 8:21:04 PM
    Group Policy was applied from:      galvarado1-2023.galvarado1.local
    Group Policy slow link threshold:   500 kbps
    Domain Name:                        GALVARADO1
    Domain Type:                        Windows 2008 or later

    Applied Group Policy Objects
    -----------------------------
        Computer Settings
        Default Domain Policy

    The following GPOs were not applied because they were filtered out
    -------------------------------------------------------------------
        Local Group Policy
            Filtering:  Not Applied (Empty)

    The computer is a part of the following security groups
    -------------------------------------------------------
        BUILTIN\Administrators
        Everyone
        BUILTIN\Users
        NT AUTHORITY\NETWORK
        NT AUTHORITY\Authenticated Users
        This Organization
        GALVARADO1-CLIE$
        Domain Computers
        Authentication authority asserted identity
        System Mandatory Level
```



```
USER SETTINGS
--------------
    CN=User One,OU=Employees,DC=galvarado1,DC=local
    Last time Group Policy was applied: 6/26/2023 at 8:26:06 PM
    Group Policy was applied from:      galvarado1-2023.galvarado1.local
    Group Policy slow link threshold:   500 kbps
    Domain Name:                        GALVARADO1
    Domain Type:                        Windows 2008 or later

    Applied Group Policy Objects
    -----------------------------
        N/A

    The following GPOs were not applied because they were filtered out
    -------------------------------------------------------------------
        Local Group Policy
            Filtering:  Not Applied (Empty)

    The user is a part of the following security groups
    ---------------------------------------------------
        Domain Users
        Everyone
        BUILTIN\Administrators
        BUILTIN\Users
        REMOTE INTERACTIVE LOGON
        NT AUTHORITY\INTERACTIVE
        NT AUTHORITY\Authenticated Users
        This Organization
        LOCAL
        All Company
        IT
        Authentication authority asserted identity
        High Mandatory Level
PS C:\Windows\system32>
```

*****The deliverable for Assignment 3 will be this document completed with the required screenshots and answers to the questions. You will submit this document in Canvas.**