Lab 8 Enterprise Information Discovery

The objective of the lab is to use the tools found in Microsoft Windows 2016 Server to explore the network you have built in the previous labs, gain a general idea as to its structure, and identify weaknesses and strengths, threats and opportunities. You will use this information in subsequent labs, for your Buildout Team projects.

This is a team assignment, but you must submit it as individuals, with all submitted work being your own.

Actions

Action 1: From your fellow classmates, form teams of no more than four members. Each team will be assigned a Windows Server 2016 instance. Your team will be on the basis of the table at which you are sitting: look for the placard on the lab tables.

For Deliverable #1, write your name, the number of your team, the name of your partners, and the date.

Connect to the CCI Virtual Environment

Action 2: You will find instructions for connecting to the CCI virtual environment in Actions 1 – 3 of
Lab 0: *Access Virtual Lab Environment*.

As advised in *Lab 0: Access Virtual Lab Environment*, you may want to uncheck various local sharing checkboxes, for security reasons.

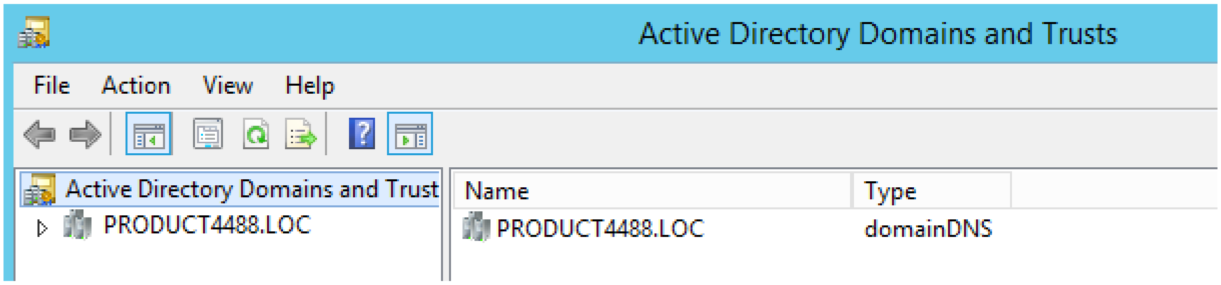
This week, you will be connecting to both your Microsoft Windows Server 2016 instance (as a team).

Action 3: Have one team member sign in to your team's Microsoft Windows 2016 Server instance using the *AdminLite* account. The password will be on the room projector.

Determine General Structural Information for this Enterprise Network

You know that the network that you've been using in your labs uses Microsoft Active Directory. You will use tools built into the Windows 2016 Server operating system to discover some details about its nature and structure.

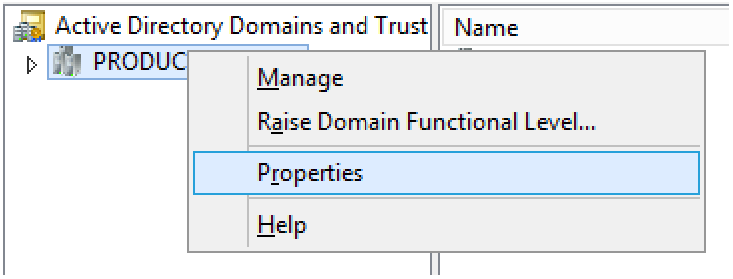
Action 4: From *Start Button* → *Administrative Tools*, select *Active Directory Domains and Trusts.*


Active Directory Domains and Trusts
File
Action
View
Help
Active Directory Domains and Trust
PRODUCT4488.LOC

Name	Type
PRODUCT4488.LOC	domainDNS

For Deliverable #2, what is the name of the enterprise's root Domain?

Right-click that Domain, and select Properties.

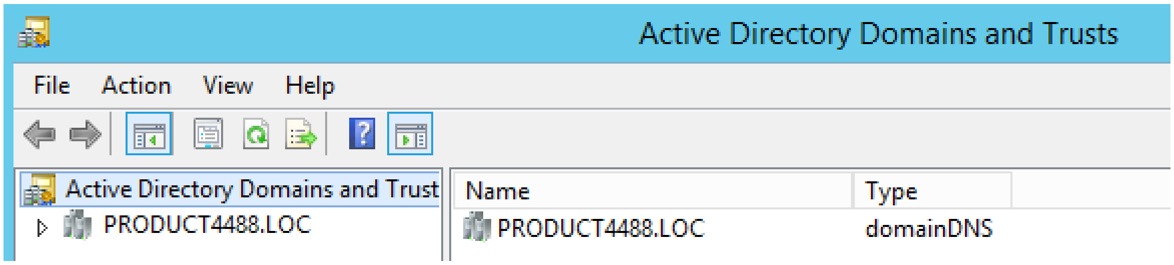

Active Directory Domains and Trust
PRODUC
Name
Manage
Raise Domain Functional Level...
Properties
Help

For Deliverable #3, what is the Domain functional level? What is the Forest functional level? Does the Forest contain the Domain, or does the Domain contain the Forest?

You will be asked questions about Domain and Forest functional levels in a future quiz.

For Deliverable #4, are there any trust relationships between the Domain under examination, and any other Domains?

Attempt to expand the Forest tree by clicking the down arrow to the left of the root Domain.


Active Directory Domains and Trusts
File
Action
View
Help
Active Directory Domains and Trust
PRODUCT4488.LOC

Name	Type
PRODUCT4488.LOC	domainDNS

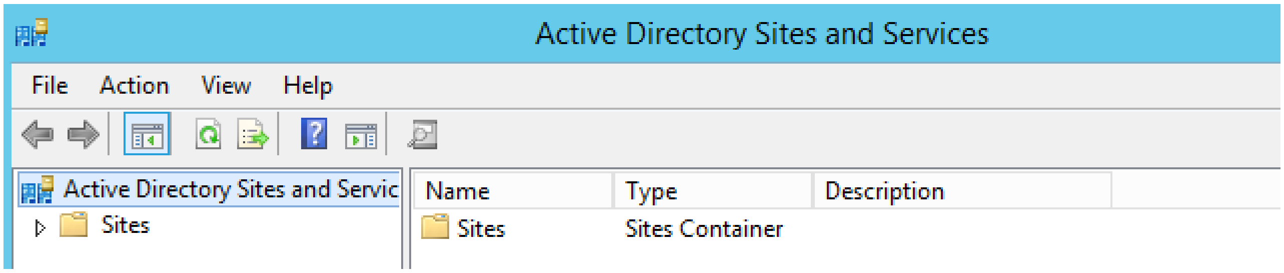
For Deliverable #5, does the tree expand to reveal more Domains? From what you have discovered in this tool, would you describe the general of your lab enterprise network as "flat", with only one Domain that also happens to be the root Domain, or does there appear to be a hierarchy of parent and child Domains?

Close the *Active Directory Domains and Trusts* tool.

Action 5: Domains are a fundamental structural unit of a Microsoft Active Directory network – some may argue that they're *the* fundamental structural unit. Domains can contain child Domains and other structural container units, such as Sites and Organizational Units (OU).

Now you will use another tool to examine the Active Directory structure:

From *Start Button* → *Administrative Tools*, select *Active Directory Sites and Services*.



- Active Directory Sites and Servic
  - Sites

Name	Type	Description
Sites	Sites Container	

Expand the Sites folder.

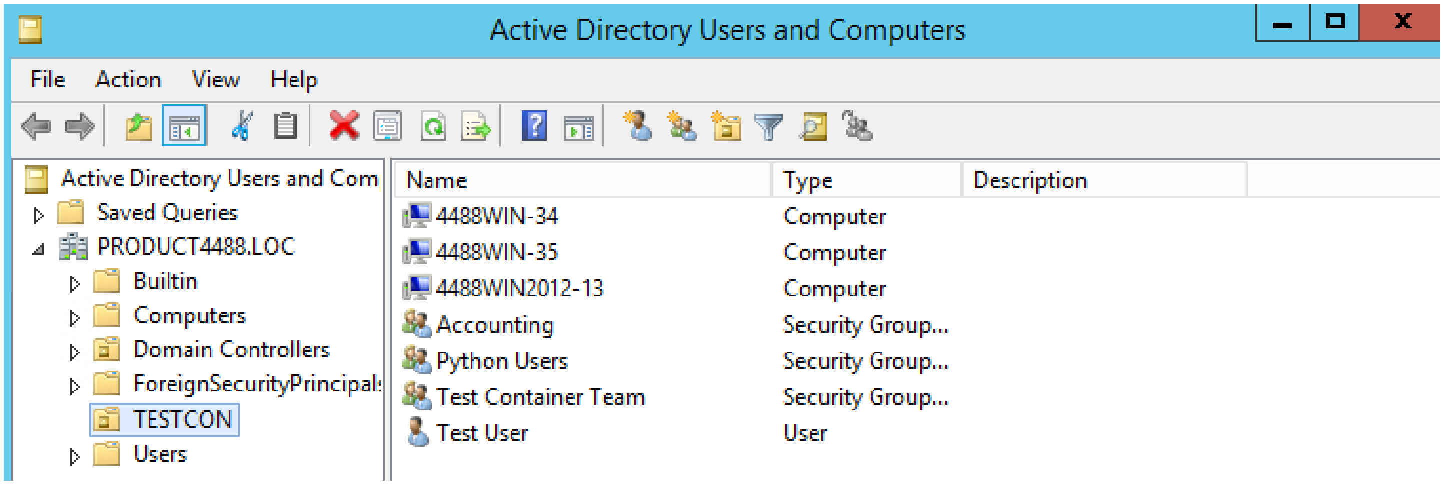
For Deliverable #6, do you see any Sites existing within this Active Directory structure? If so, what are they? What function does an Active Directory Site perform?

Close the *Active Directory Sites and Services* tool.

Action 6: You've now examined the Domains and Sites within your Active Directory. Now you're going to take a look at another fundamental structural unit – one on which administrative boundaries are based – and this is the Organizational Unit (OU).

In previous labs, your team created an OU for its own use, you joined your team server and team member workstations to a Domain, you moved those computers into your OU, you created groups and users accounts within that OU, and then you created one or more Group Policy Objects (GPO) linked to and enforced over that OU.

From *Start Button* → *Administrative Tools*, select the *Active Directory Users and Computers* tool.



- Active Directory Users and Com
  - Saved Queries
  - PRODUCT4488.LOC
    - Builtin
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipal:
    - TESTCON
    - Users

Name	Type	Description
4488WIN-34	Computer	
4488WIN-35	Computer	
4488WIN2012-13	Computer	
Accounting	Security Group...	
Python Users	Security Group...	
Test Container Team	Security Group...	
Test User	User	

For Deliverable #7, how many Organizational Unit (OU) containers exist within your Active Directory? Are any OU containers nested within any other OU containers? Would you consider the enterprise OU structure to be "flat"? What is the name of your own team's Organizational Unit (OU)?

Determine the Number of Assets and User Accounts in the Enterprise

Action 7: For a variety of reasons, administrators will want to keep track of assets within their Active Directories, and to count them. This serves a number of purposes: assigning workloads, design scaling and performance management, licensing, security, and so on.

For Deliverable #8, how many computers reside within your OU? How many are servers? How many are workstations? Are any Domain Controllers? What operating systems do they use?

Hint: right-click each computer object in your Organizational Unit (OU), and then select *Properties*, to view information on each computer object.

For Deliverable #9, how many group objects exist within your OU? Of which Group Type?

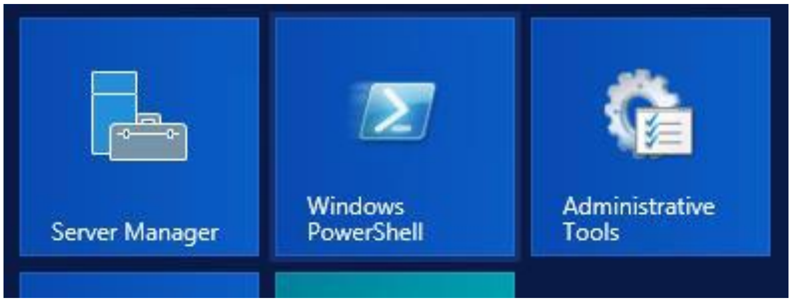
For Deliverable #10, how many user objects exist within your OU?

Action 8: You could manually click through all of *Active Directory Users and Computers* to examine individual Active Directory objects. However, if you were asked the following question, how long do you think it might take for you to calculate an answer?

How many user objects exist in your entire enterprise, in all Domains, Sites, and Organizational Units? How many of these user accounts are enabled, and how many user accounts are disabled?

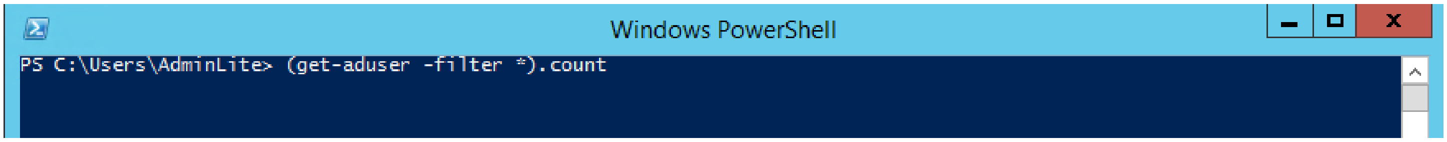
While you could use the Graphical User Interface (GUI) to answer that question, a Command Line Utility (CLI) utility might be much faster.

Click *Start Button* and select *Windows PowerShell* to open the Windows PowerShell Command Line Interface:



At the command prompt, enter

```
(get-aduser -filter *).count
```



```
PS C:\Users\AdminLite> (get-aduser -filter *).count
```

This will query Active Directory and produce a count of Active Directory users. There are entire books on PowerShell scripting, and one could conduct tens of thousands of different network management operations from these commands and scripts.

For user accounts that are enabled:

```
(get-aduser -filter *|where {$_.enabled -eq "True"}).count
```

For user accounts that are disabled:

```
(get-aduser -filter *|where {$_.enabled -ne "False"}).count
```

For Deliverable #11, answer the following question: How many user objects exist in your entire enterprise, in all Domains, Sites, and Organizational Units? How many of these user accounts are enabled, and how many user accounts are disabled?

Close the *Windows PowerShell*.

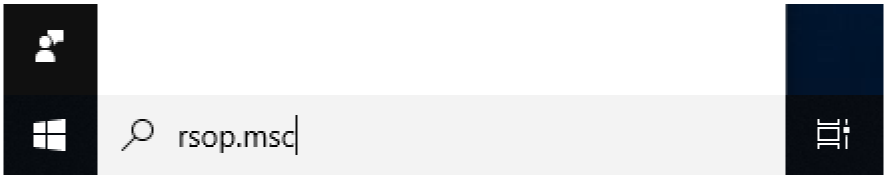
Examine Your Team's Computers for Effects of Existing Group Policies

Action 9: At this time, one team member should connect to the CCI Virtualization environment, and connect to a Microsoft Windows 10 virtual instance.

Log in using an individual Domain user account created for in a previous lab.

Check to see which Group Policies are being applied against your Windows 10 computer by running the *Resultant Set of Policy* tool.

From the Start button, enter into the Search programs and files box the command rsop.msc <ENTER>.

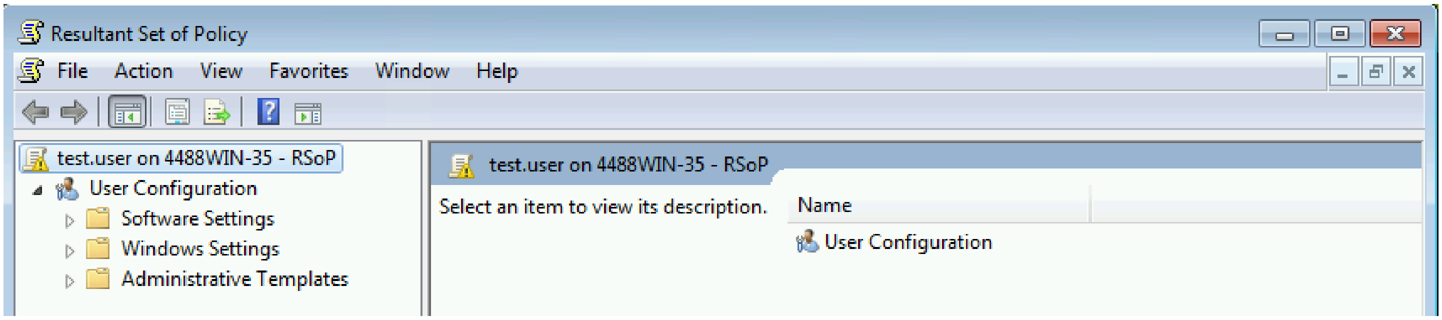


```
rsop.msc
```

Depending on the level of permissions granted to the user account with which you are presently logged in, you may get an error:

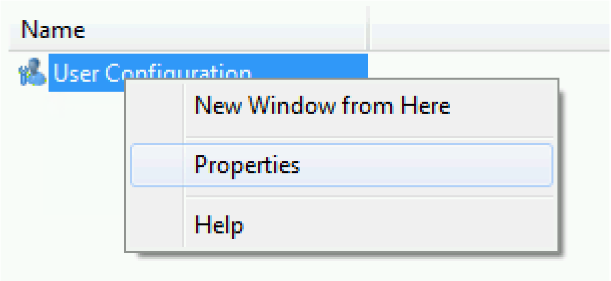
Click *Close* to continue, to close the error pop-up box, if you receive such an error.

You will now see the *Resultant Set of Policy* tool and its results:



Select an item to view its description.

To see which Group Policy Object is enforcing this configuration, right-click *User Configuration* in the right pane, and select *Properties*:



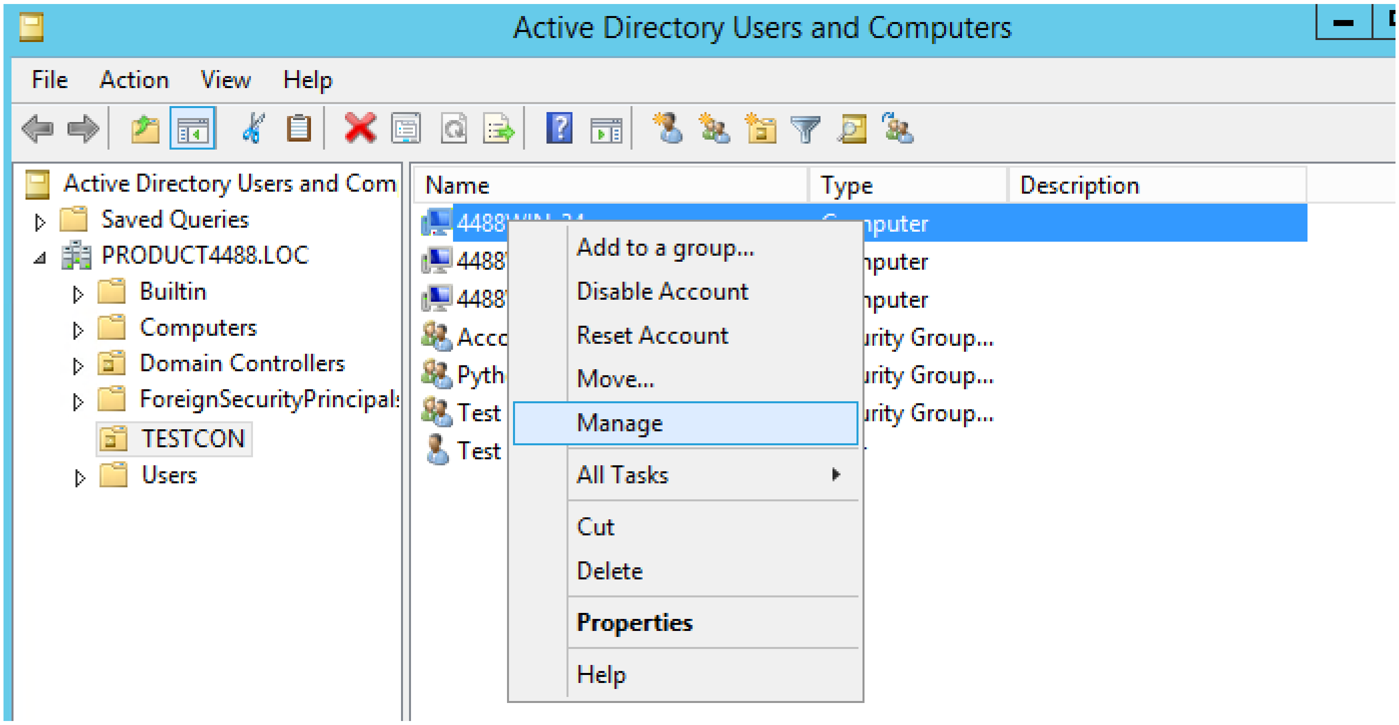
Check all of the boxes to display details about which Group Policy Object(s) is/are being applied against your workstation and/or the user account with which you are logged in to that workstation:

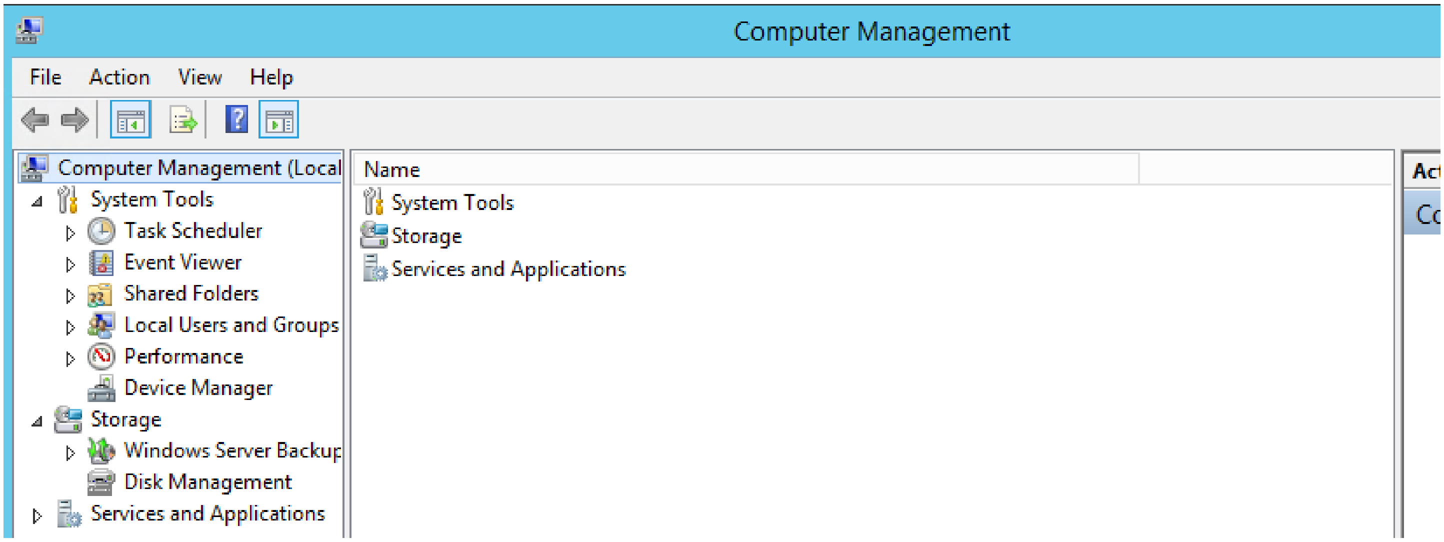
For Deliverable #12, name the Group Policy Objects (GPO) that are being enforced against the computers in your Organizational Unit, and their scopes.

Examine Your Team's Computers for Configuration

Action 10: While there are many more things that network administrators must do to manage networks, one of them involves configuration and device management.

Return to *Active Directory Users and Computers* on your team Windows 2016 Server computer, right-click one of the computers in your team Organizational Unit (OU), and select *Manage*:





For Deliverable #13, select two of the manageable items above – e.g. an event, a share, a performance metric, a device or disk status, or a service status – and report something about it.

In the next series of labs, you will consider the limitations of individual server-centric management, and begin to design and implement more scalable means of managing networks that could contain tens of thousands of users and workstations, hundreds of servers and applications – and hundreds of thousands of interconnections – and what it might take to effectively and efficiently administrate and secure them.

Deliverables

Deliverable 1: From Action 1, write your name, the number of your team, the name of your partners, and the date.

Deliverable 2: From Action 4, what is the name of the enterprise's root Domain?

Deliverable 3: From Action 4, what is the Domain functional level? What is the Forest functional level? Does the Forest contain the Domain, or does the Domain contain the Forest?

Deliverable 4: From Action 4, are there any trust relationships between the Domain under examination, and any other Domains?

Deliverable 5: From Action 4, does the tree expand to reveal more Domains? From what you have discovered in this tool, would you describe the general of your lab enterprise network as "flat", with only one Domain that also happens to be the root Domain, or does there appear to be a hierarchy of parent and child Domains?

Deliverable 6: From Action 5, do you see any Sites existing within this Active Directory structure? If so, what are they? What function does an Active Directory Site perform?

Deliverable 7: From Action 6, how many Organizational Unit (OU) containers exist within your Active Directory? Are any OU containers nested within any other OU containers? Would you consider the enterprise OU structure to be "flat"? What is the name of your own team's Organizational Unit (OU)?

Deliverable 8: From Action 7, how many computers reside within your OU? How many are servers? How many are workstations? Are any Domain Controllers? What operating systems do they use?

Deliverable 9: From Action 7, how many group objects exist within your OU? Of which Group Type?

Deliverable 10: From Action 7, how many user objects exist within your OU?

Deliverable 11: From Action 8, answer the following question: How many user objects exist in your entire enterprise, in all Domains, Sites, and Organizational Units? How many of these user accounts are enabled, and how many user accounts are disabled?

Deliverable 12: From Action 9, name the Group Policy Objects (GPO) that are being enforced against the computers in your Organizational Unit, and their scopes.

Deliverable 13: From Action 10, select two of the manageable items above – e.g. an event, a share, a performance metric, a device or disk status, or a service status – and report something about it.