## LESSON: Active Directory and Group Policy

**Before you Begin**

In this module, learners will continue to learn about the concept of centralization of core networking services. There is quite a bit of content to cover as well as four labs. You should pay attention to your pace to ensure you can deliver all of the content and demonstrate the labs during class time. For this lesson and upcoming lessons, instructors are required to ensure the following activities are completed:

* Review the “Lesson Opener” and “Real World Scenario” with the learners prior to starting the module.
* Throughout the module, you will find “Consider the Real World Scenario” slides. Review the questions found on these slides, tie the concepts back to the scenario discussed at the start of the lesson as well as content you are presenting, and encourage the learners to share their thoughts.
* Ensure learners are given opportunities for breaks throughout the lesson. The pacing guide below provides recommended breaks. However, there are additional breaks added in the slide deck, please use them if needed.
* For each lesson, you will find a “Pulse Check” slide which is the opportunity for instructors to open a poll to gather feedback from the learners. Leave the poll open for about 1 minute and after you close the poll, share the results with the learners. Encourage the learners to share their thoughts. This information will help the instructors as well as the learners better understand where they are with regards to the lesson.
* Labs are to be demonstrated live for each module. The demonstration of labs is the top priority for the lead instructor. While demonstrating each lab, encourage students to participate and explore.
* At the end of each lesson, it is important to take a few minutes to review the key concepts for the lesson, provide guidance on what the learners can do to prepare for the next lesson, and wrap up with Q&A.

### Summary

In this lesson, learners will dive into the world of Active Directory (AD) and its pivotal role in organizing and securing domains. They will explore the creation of user objects within AD Domain Services (AD DS) to establish authentication and authorization for accessing domain resources, while grasping the concept of group objects for collective permissions assignment. The lesson will guide learners through Group Policy, a critical security tool, where they'll navigate Group Policy Management Console (GPMC) and the Group Policy Management Editor to configure and manage user and computer configurations. Understanding the processing order, link order, inheritance, and the differences between Local and Domain Group Policy, learners will adeptly tailor policy settings. By exploring X.509 certificates for enhanced security and discovering third-party applications for Group Policy Management Editor, learners will gain expertise in securing domains against internal and external threats, fostering efficient domain management and security practices within a Microsoft Windows environment.

### Objectives

* Explain the different roles of Active Directory (AD).
* Describe common AD issues related to domain roles.
* Identify the key settings for configuring AD services.
* Create and manage Active Directory (AD) objects.
* Evaluate the use of built-in groups in AD.
* Explain the concept of Group Policies.
* Identify the key components of a Group Policy Object (GPO).
* Differentiate between computer and user Group Policy settings and understand how they are applied to specific objects in an AD domain.
* Explain the functionality of GPO and its importance in domain management.
* Compare and contrast GPO management in a domain environment versus local Group Policy usage.
* Identify the operational priority of GPO in a domain environment.
* Explain the purpose and function of the Group Policy Management Editor.
* Identify and describe the various settings available within the Group Policy Management Editor.
* Describe the features and capabilities of other policy management tools.

### Lesson Activities and Teaching Strategies

|  |  |  |
| --- | --- | --- |
| Estimated Time | Lesson Portion | Directions |
| 5 min | **Lesson Opener:**  Active Directory and Group Policy | * Introduce learners to the importance of Active Directory and Group Policy in Microsoft Security. |
| 5 min | **Real World Scenario:**  Active Directory and Group Policy | * Review the real world scenario challenge and inform learners that you will be constantly coming back to this scenario throughout the lesson to discover how to solve and apply concepts to this real situation. |
| 20 min | **Cyber Uncovered:**  Active Directory (AD) Fundamentals | * Emphasize the importance of understanding the historical development of Active Directory (AD) and its role in securing domains, setting the stage for a comprehensive exploration of AD's features and concepts. * Detail the core function of AD in managing permissions for users, computers, groups, and objects within domains, highlighting its critical role in access control and security. * Trace the progression from manual data sharing to the introduction of Active Directory, highlighting the limitations of the flat domain model and showcasing how AD's hierarchical structure revolutionized domain organization for large organizations. * Introduce the fundamental concepts of identification, authentication, and authorization in Windows authentication, emphasizing their role in shaping access control and establishing the principle of least privilege. * Demonstrate how Active Directory empowers network administrators to efficiently create, manage, and organize objects, users, and domains, enabling streamlined access control and permissions assignment. * Illustrate the hierarchical structure of Active Directory, explaining how objects like users, groups, and computers are organized into trees and domains, and how trust relationships facilitate resource sharing. * Describe the vital role of domain controllers in hosting AD DS, elaborating on how AD DS controls access to domain resources and introducing the Active Directory Users and Computers (ADUC) role for centralized management. * Guide learners through the concept of object containers, particularly Organizational Units (OUs), and how they are utilized to organize users, groups, and computers while enforcing uniform policies. * Explain the significance of Sites & Services in managing physical network structures. * Clarify the concepts of transitive and non-transitive trusts, one-way and two-way trusts, and their impact on domain relationships, while providing real world examples to reinforce understanding. * Introduce the role of X.509 certificates in enhancing security within and beyond a domain, exploring how they support encrypted, verifiable communications and authentication, and their utilization for safeguarding domain resources. * Be prepared to discuss the implication of the real world scenario presented at the beginning of class on network types and devices. There are specific prompts that you should ask learners to reflect on to apply this concept to the real world scenario. |
| 20 min | **Cyber Uncovered:**  AD Objects | * Begin by highlighting the significance of Active Directory (AD) user management in domain administration and security, setting the stage for a comprehensive exploration of user creation, administration, and profiles. * Walk learners through the process of creating user objects, emphasizing the distinction between mandatory and optional fields, and guide them in setting additional options after the creation wizard. Detail the diverse formats for user login and elaborate on user object administration, including password management, name changes, and group affiliations. * Introduce the concept of user profiles and their role in maintaining personalized desktop and home folder configurations. Explain the difference between local and roaming profiles, highlighting their impact on user experience and device flexibility within a domain. * Provide an in-depth exploration of Active Directory groups, emphasizing their role in simplifying access assignment and resource management. Distinguish between different group types (Domain Local, Global, Universal) and their respective permissions settings, while showcasing their versatility and hierarchical relationships. * Clarify the conversion possibilities and permission scopes associated with different group types. Guide learners through the process of upgrading or downgrading groups, emphasizing the implications for access control across domains and within a forest. * Examine the initial setup of built-in groups that are automatically installed with AD DS, outlining their roles and potential applications. Encourage learners to consider their usability and explore the option of creating custom groups based on organizational needs. * Detail the significance of computer objects in AD, explaining their representation of Windows client and server systems. Emphasize automatic addition of computer objects upon domain joining and the manual addition process, enabling learners to effectively manage devices within the domain. * Be prepared to discuss the implication of the real world scenario presented at the beginning of class on network types and devices. There are specific prompts that you should ask learners to reflect on to apply this concept to the real world scenario. |
| 20 min | **Lab:**  Creating & Managing AD Objects | * Remind learners to use this lab to practice and apply the concepts they learned throughout the day. * Learners will receive direct feedback on their lab to properly assess their knowledge and determine areas in which they might need additional assistance. |
| 5 min | **Break** | * Share a timer on the screen so there is clarity as to when class will resume. Ensure cameras and microphones are disabled during the break. |
| 20 min | **Cyber Uncovered:**  Group Policy Introduction | * Begin by explaining the significance of Group Policy as an efficient and effective security tool used in Active Directory for implementing security configurations. * Emphasize that Group Policies are hierarchical infrastructure elements that allow for the management of user and computer settings in a domain. * Discuss the differences between policies and preferences. * Discuss how GPOs are synced to the domain, pushing out the Group Policies to all users and end devices. * Introduce the main components of Group Policy Objects * Discuss how computer configuration GPOs are initiated during startup or shutdown and applied to the local computer and provide an example, such as a script clearing browser history during computer shutdown. Provide an example, such as mapping a network drive upon user login. * Be prepared to discuss the implication of the real world scenario presented at the beginning of class on network types and devices. There are specific prompts that you should ask learners to reflect on to apply this concept to the real world scenario. |
| 5 min | **Pulse Check** | * After the poll is concluded, review the results with the learners. Encourage those in the red zone to attend office hours and/or to reach out to the instructors for assistance. |
| 5 min | **Break** | * Share a timer on the screen so there is clarity as to when class will resume. Ensure cameras and microphones are disabled during the break. |
| 20 min | **Cyber Uncovered:**  Group Policy Management | * Explain that Group Policy Objects (GPOs) are powerful tools in Active Directory (AD) that enable the configuration of user and computer settings for domain security. * Emphasize the importance of GPOs in securing the domain from internal and external threats. * Discuss how GPOs can be customized with default and advanced settings to enhance domain security. * Explain that administrators can link GPOs to specific organizational units (OUs) or the entire domain. * Describe the security benefits provided by GPOs, such as enforcing complex password policies and auditing user logins. * Explain how GPOs can automate software installations, ensuring timely updates and reducing administrative workloads. * Compare Local Group Policies, specific to individual computers, with Domain Group Policies that affect all computers and users in the AD domain. * Emphasize that local policies are not centrally managed and can only be modified on the local computer. * Highlight the significance of the processing order in GPOs, emphasizing that incorrect order can lead to policies being overwritten. * Explain the processing order based on link order, where GPOs processed last have the highest precedence. * Explain the concept of blocking inheritance in an OU to prevent higher-level policies from being applied. * Discuss the option to enforce a parent-level GPO to override a "block inheritance" setting in a child OU. * Be prepared to discuss the implications of the real world scenario presented at the beginning of class on network types and devices. There are specific prompts that you should ask learners to reflect on to apply this concept to the real world scenario. |
| 20 min | **Lab:**  Basic GPO Configuration | * Remind learners to use this lab to practice and apply the concepts they learned throughout the day. * Learners will receive direct feedback on their lab to properly assess their knowledge and determine areas in which they might need additional assistance. |
| 5 min | **Break** | * Share a timer on the screen so there is clarity as to when class will resume. Ensure cameras and microphones are disabled during the break. |
| 15 min | **Cyber Uncovered:**  Group Policy Management Editor | * Explain the significance of Group Policy Management Editor as an administrative tool for configuring GPOs effectively. * Emphasize the importance of thorough documentation before editing GPOs to ensure desired settings and configurations across the domain. * Introduce the Group Policy Management Editor and its role in managing GPOs. * Discuss the ability to configure, enable, and disable local policies within the GPO editor. * Provide examples of tasks administrators can perform using the editor, such as setting desktop wallpaper themes, limiting application installations, disabling removable devices, and restricting access to tools like regedit. * Explain the two levels of configuration within GPOs: Computer configuration and user configuration. * Describe the hierarchy tree structure of GPO settings and how administrators navigate to the desired options for modification. * Walk through an example scenario in which you disable the user’s ability to log in remotely. * Discuss various editing options available within the Group Policy Management Editor. * Mention the existence of third-party software applications that offer similar functionalities to the Microsoft Group Policy Management Editor. * Explain how these applications may provide additional features like change detection and alerting, history tracking for auditing purposes, and compatibility with Microsoft Active Directory. * Be prepared to discuss the implications of the real world scenario presented at the beginning of class on network types and devices. There are specific prompts that you should ask learners to reflect on to apply this concept to the real world scenario. |
| 20 min | **Lab:**  Set up Group Policy for Chrome Browser | * Remind learners to use this lab to practice and apply the concepts they learned throughout the day. * Learners will receive direct feedback on their lab to properly assess their knowledge and determine areas in which they might need additional assistance. |
| 20 min | **Lab:**  Logon Script GPO Configuration | * Remind learners to use this lab to practice and apply the concepts they learned throughout the day. * Learners will receive direct feedback on their lab to properly assess their knowledge and determine where they might need additional assistance. |
| 5 min | **Lesson Closure** | * For this lesson, spend just a few minutes reminding the learners what the key ”take-aways'' were from the lesson and what they should do to prepare for the next module. Topics to focus on should include centralization of networking services, specifically how Active Directory provides better security for authentication, authorization, and endpoint management and configuration through group policy. * You will be able to use the data collected in the pulse check to help with the lesson closure. Remind those learners that reported being in the “red zone” to take advantage of office-hours. * Recommend that the learners ensure they submit all of the assignments on-time to ensure the appropriate credit is provided to them. * Recommend that the students read-ahead and come prepared for the next lesson. * Q&A |
|  | **Additional Time Filler (if needed)** | * Kahoot * Discuss interview prep and questioning * Use breakout rooms for additional lab practice * Continue Real World Scenario Conversation |

### 