Module Overview

• Configuring Password Policy and User Account Lockout Settings
• Configuring Managed Service Accounts

Lesson 1: Configuring Password Policy and User Account Lockout Settings

• User Account Policies
• Kerberos Policies
• Configuring User Account Policies
• What Are Password Settings Objects?
• Configuring PSOs
• Demonstration: Configuring PSOs
• Discussion: Planning Password Policies
User Account Policies

Use the following settings to set password requirements:
• Enforce password history
• Maximum password age
• Minimum password age
• Minimum password length
• Password complexity requirements
• Account lockout duration
• Account lockout threshold

Kerberos Policies

• Kerberos policy settings determine timing for Kerberos tickets and other events

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enforce user logon restrictions</td>
<td>Enabled</td>
</tr>
<tr>
<td>Maximum lifetime for service ticket</td>
<td>600 minutes</td>
</tr>
<tr>
<td>Maximum lifetime for user ticket</td>
<td>10 hours</td>
</tr>
<tr>
<td>Maximum lifetime for user ticket renewal</td>
<td>7 days</td>
</tr>
<tr>
<td>Maximum tolerance for computer clock</td>
<td>5 minutes</td>
</tr>
<tr>
<td>synchronization</td>
<td></td>
</tr>
</tbody>
</table>

• Kerberos claims and compound authentication for DAC requires Windows Server 2012 domain controllers
Configuring User Account Policies

- Local Security Policy account settings:
  - Configured with secpol.msc
  - Apply to local user accounts

- Group Policy account settings
  - Configured with the Group Policy Management console
  - Apply to all accounts in AD DS and local accounts on computers joined to the domain
  - Can only be applied once, in Default Domain Policy
  - Take precedence over Local Security Policy settings

What Are Password Settings Objects?

- You can use fine-grained password policies to specify multiple password policies within a single domain

- Fine-grained password policies:
  - Apply only to user objects (or inetOrgPerson objects) and global security groups
  - Cannot be applied to an OU directly
  - Do not interfere with custom password filters that you might use in the same domain
Configuring PSOs

- Windows Server 2012 provides two tools for configuring PSOs
  - Windows PowerShell cmdlets
    - New-ADFineGrainedPasswordPolicy
    - Add-FineGrainedPasswordPolicySubject
  - Active Directory Administrative Center
    - Graphical user interface
    - Uses Windows PowerShell cmdlets to create and manage PSOs

Demonstration: Configuring PSOs

In this demonstration, you will see how to create a Password Settings Object for the ITAdmins group
Discussion: Planning Password Policies

What password policies would you recommend for...

- Woodgrove Bank
- New account lockout policy
- Tailspin Toys
- Best practices
Lesson 2: Configuring Managed Service Accounts

- Service Account Overview
- Challenges of Using Standard User Accounts for Services
- Managed Service Account and Virtual Accounts
- What Are Group Managed Service Accounts?
- Demonstration: Configuring Group Managed Service Accounts
- Kerberos Delegation and Service Principal Names

Service Account Overview

- Applications need resource access
  - Can create domain or local accounts to manage such access, but can potentially compromise security

- Use Service Accounts Instead
  - Local System
    - Most privileged, still vulnerable if compromised
  - Local Service
    - Least privileged, may not have enough permissions to access all required resources
  - Network Service
    - Can access network resources with proper credentials
Challenges of Using Standard User Accounts for Services

- Challenges to using standard user accounts for services include:
  - Extra administration effort to manage the service account password
  - Difficulty in determining where a domain-based account is used as a service account
  - Extra administration effort to manage the SPN

Managed Service Account and Virtual Accounts

- Use managed service accounts to automate password and SPN management for service accounts used by services and applications
- Requires a Windows Server 2008 R2 or Windows Server 2012 server installed with:
  - .NET Framework 3.5.x
  - Active Directory module for Windows PowerShell
- Recommended to run with AD DS configured at the Windows Server 2008 R2 functional level or higher
- Can be used in a Windows Server 2003 or 2008 AD DS environment:
  - With Windows Server 2008 R2 schema updates
  - With Active Directory Management Gateway Service
What Are Group Managed Service Accounts?

- Group managed service accounts extend the capability of standard managed service accounts by
  - Enabling managed service accounts to be used on more than one computer in the domain
  - Storing managed service accounts authentication information on domain controllers

- Group managed service accounts requirements:
  - Must have at least one Windows Server 2012 domain controller
  - Must have a KDS root key created for the domain

Demonstration: Configuring Group Managed Service Accounts

In this demonstration, you will see how to:

- Create the KDS root key for the domain
- Create and associate a managed service account
### Kerberos Delegation and Service Principal Names

- **Kerberos delegation of authentication**
  - Services can delegate service tickets issued to them by the KDC to another service
- **Constrained delegation**
  - Allows administrators to define which services can use service tickets issued to other services
- **SPNs help identify services uniquely**
- **Windows 2012 allows**
  - Constrained delegation across domains
  - Ability of service administrators to configure constrained delegation
Lab: Managing User and Service Accounts

- Exercise 1: Configuring Password Policy and Account Lockout Settings
- Exercise 2: Creating and Associating a Managed Service Account

Logon Information

**Virtual machines:** 20411D-LON-DC1
**User Name:** Adatum\Administrator
**Password:** Pa$$w0rd

Estimated Time: 45 minutes
Lab Scenario

A. Datum is a global engineering and manufacturing company with their head office based in London, United Kingdom. An IT office and data center are located in London to support the London location and other locations. A. Datum has recently deployed a Windows Server 2012 server and client infrastructure.

A. Datum has completed a security review for passwords and account lockout policies. You need to implement the recommendations contained in the report to control password complexity and length. You also need to configure appropriate account lockout settings. Part of your password policy configuration will include a specific password policy you need to assign to the Executive security group. This group requires a different password policy than the policy applied at the domain level.

You need to configure a new group managed service account to support a new Web-based program. Using a group managed service account will help maintain the password security requirements for the account.
## Module Review and Takeaways

- Review Question(s)
- Real-world Issues and Scenarios
- Tools
- Common Issues and Troubleshooting Tips