Microsoft

Administering Windows Server Hybrid Core Infrastructure

Exam Ref AZ-800

Orin Thomas

Microsoft

Exam Ref AZ-800 Administering Windows Server Hybrid Core Infrastructure

Orin Thomas

NEED MORE REVIEW? **HYBRID PASSWORD SYNCHRONIZATION FOR AZURE AD DS**

You can learn more about domain-joining a Windows Server IaaS VM at *https://docs.microsoft.com/en-us/azure/active-directory-domain-services/tutorial-configure-password-hash-sync*.

Manage Azure AD Connect Health

Azure AD Connect Health is a tool available in the Azure Active Directory admin center, shown in Figure 1-33, that allows you to monitor the health of synchronization between your organization's on-premises directory and Azure Active Directory.

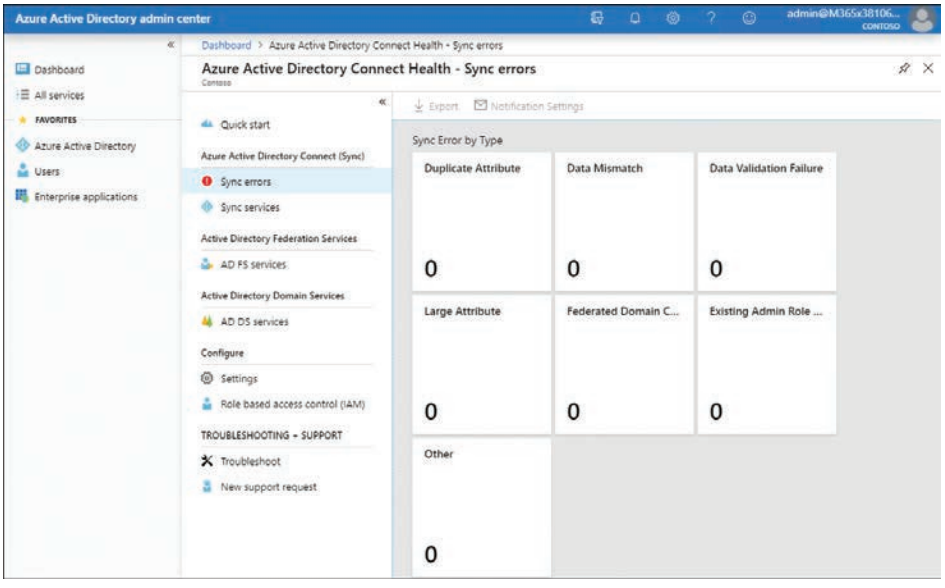

FIGURE 1-33 Azure AD Connect Health.

You can use Azure AD Connect health to view information about the following:

- **Sync errors** This option displays errors such as Duplicate Attribute, Data Mismatch, Data Validation Failure, Large Attribute, Federated Domain Change, and Existing Admin Role Conflicts.
- **Sync services** This option handles information about which services are synchronizing with Azure Active Directory.
- **AD FS services** This option displays information about AD FS when Azure AD Connect is configured for federation. Includes information about errors and issues.
- **AD DS services** This option displays information about domains and forests connected to Azure Active Directory.

NEED MORE REVIEW? **AZURE AD CONNECT HEALTH**

You can learn more about Azure AD Connect Health at *https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-azure-ad-connect*.

Manage authentication in on-premises and hybrid environments

Azure AD Connect supports a variety of user sign-in options, which are related to the method you use to synchronize directory information from Active Directory Domain Services to Azure AD. You configure which sign-in option you will use when setting up Azure AD Connect, as shown in Figure 1-34. The default method, password sync, is appropriate for the majority of organizations that will use Azure AD Connect to synchronize identities to the cloud.

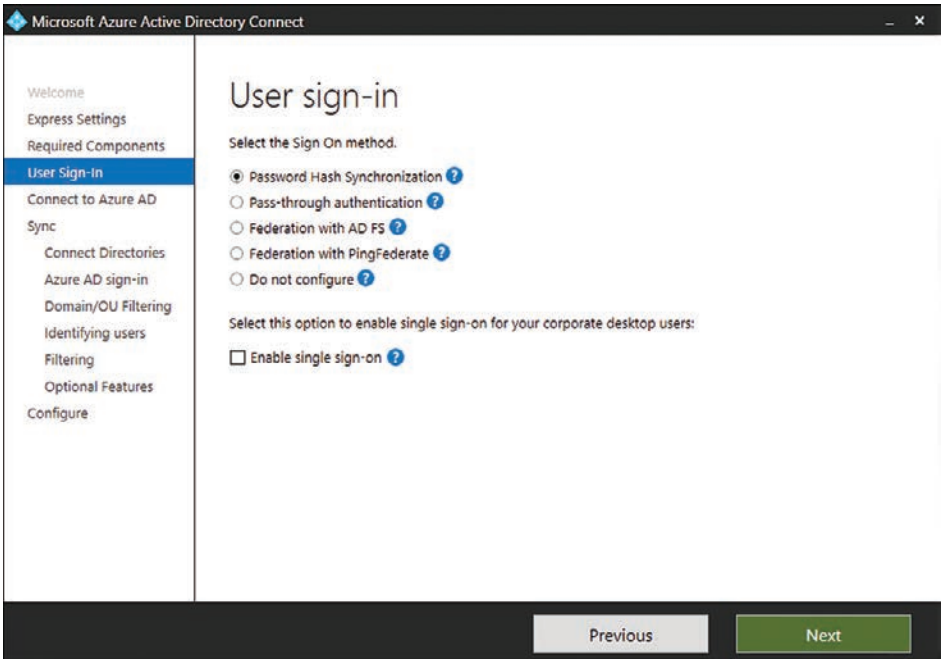

FIGURE 1-34 User sign-in.

Password synchronization

Hashes of on-premises Active Directory user passwords synchronize to Azure AD, and changed passwords immediately synchronize to Azure AD. Actual passwords are never sent to Azure AD and are not stored in Azure AD. This allows for single sign-on for users of computers that are joined to an Active Directory domain that synchronizes to Azure AD. Password synchronization

also allows you to enable password writeback for self-service password reset functionality through Azure AD.

Pass-through authentication

When authenticating to Azure AD, the user's password is validated against an on-premises Active Directory domain controller. Passwords and password hashes are not present in Azure AD. Pass-through authentication allows you to apply on-premises password policies. It requires that Azure AD Connect have an agent on a computer joined to the domain that hosts the Active Directory instance that contains the relevant user accounts. Pass-through authentication also allows single sign-on for users of domain-joined machines.

With pass-through authentication, the user's password is validated against the on-premises Active Directory controller. The password doesn't need to be present in Azure AD in any form. This allows for on-premises policies, such as sign-in hour restrictions, to be evaluated during authentication to cloud services.

Pass-through authentication uses a simple agent on a Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, or Windows Server 2022 domain-joined machine in the on-premises environment. This agent listens for password-validation requests. It doesn't require any inbound ports to be open to the internet.

You can also enable single sign-on for users on domain-joined machines that are on the corporate network. With single sign-on, enabled users only need to enter a username to help them securely access cloud resources.

Active Directory Federation

Active Directory Federation allows users to authenticate to Azure AD resources using on-premises credentials. It also requires the deployment of an Active Directory Federation Services infrastructure. This is the most complex identity synchronization configuration for Azure Active Directory and is only likely to be implemented in environments with complicated identity configurations.

Configure and manage AD DS passwords

Most of the accounts used in your organization will be domain-based rather than local accounts. Except for the occasional local account, users, services, and computers authenticate against Active Directory Domain Services (AD DS). By using password policies, administrators can specify the rules for allowable passwords. They determine how long and how complicated passwords must be, as well as how often they must be changed, how often they can be changed, and whether previously used passwords can be used again.

Unless you take special steps, the properties of passwords used with domain accounts are determined through domain-based password policies. You configure password policies by editing Group Policy Objects (GPOs) linked at the domain level. This fact is important, and although you can set password policies at GPOs linked at the organizational unit (OU) and site level, these policies have no effect on the properties of user passwords.

Remember that you can have only one set of domain password policies configured through Group Policy. The GPO order at the domain level determines the domain password policy. The exceptions to the rule about one password policy per domain are fine-grained password policies.

Password policies are located in the Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies node of a GPO. Although most administrators think of password policy and account lockout policy as parts of the same whole, they are actually separate. Windows Server ships with a default password policy, but account lockout policy is not enabled.

Password policy items

The following list shows five main password policies that you are likely to use when configuring a password policy for your organization, and one that you probably won't use. These password policies are the following:

- **Enforce password history** This policy means that the configured number of previously used passwords is stored within Active Directory. It stops users from using the same set of small passwords. The default and maximum value is 24 remembered passwords.
- **Maximum password age** This policy specifies the maximum length of time that can elapse before a password must be changed. The default value is 42 days. You can set it to 999 days. Setting the value to 0 days means that there is no maximum password age.
- **Minimum password age** You use this policy to restrict users from changing their password instantly. This policy exists because some users spend a couple of minutes repeatedly changing their password until they have exhausted the password history and return to using their original password. Users can change their password after the specified period has elapsed. The default value is 1 day.
- **Minimum password length** This policy sets the minimum number of characters in a password. Longer passwords are more secure than shorter ones. Windows Server supports passwords up to 128 characters long when changed using GUI tools, and 256 when modified using PowerShell.
- **Password must meet complexity requirements** This policy ensures that passwords use a mix of numerals, symbols, and uppercase and lowercase alphabet characters. When enabled, it also stops users from using their account name in the password.

The policy that you are unlikely to need is the **Store Passwords Using Reversible Encryption** policy. This policy has been available in most previous versions of the Windows Server operating system. It provides backward compatibility for applications that could not access passwords stored in Active Directory using the native method of encryption. Unless your organization is running some software that was written back when Windows NT 4.0 was the Windows Server operating system, you probably won't need to enable this policy.

Delegate password settings permissions

People tend to be good at remembering passwords that they have used for a long time. They tend not to be so good at remembering new passwords, especially if those passwords contain a mix of numbers, letters, and symbols. Users who frequently have to change their passwords are more likely to end up forgetting those passwords. If an account lockout policy is enforced, users are more likely to end up calling the service desk to get their password reset. The stricter an organization's password policy is, the more time the service desk has to spend untangling users from forgotten passwords.

Instead of having users call the service desk to have their password reset, you can delegate the ability to reset user passwords to someone in the user's own department, such as an administrative assistant or office manager. Taking this step can increase security because someone in the user's own department can more easily verify the user's identity than a service desk technician can. It also shifts work away from the service desk, which enables service desk technicians to concentrate on other tasks.

The default Active Directory settings give members of the Account Operators, Domain Admins, or Enterprise Admins Active Directory groups the right to change user passwords. You can delegate the ability to manage password settings on a per-OU basis through the delegation of a control wizard. When you do this, you move user accounts into specific OUs that match your administrative requirements. For example, you can move all user accounts of people who work in the research department to the Research OU, and then delegate the right to reset passwords and force password change at the next logon to the research department's departmental manager. You can also delegate the ability to manage password settings at the domain level, though most organizations do this by adding users to the Account Operators, Domain Admins, or Enterprise Admins groups.

To delegate the right to reset passwords and force password changes at the next logon, run the **Delegation of Control Wizard**. You can access this wizard by right-clicking an OU in Active Directory Users and Computers and then selecting **Delegate Control**. You should be careful to select only the **Reset user passwords and force password change at next logon** task and not grant non-IT department users the right to perform other tasks.

Larger organizations should consider providing a self–service password reset portal. Self–service password reset portals enable users to reset their Active Directory user account passwords after performing a series of tasks that verify their identity. This process provides users with a quick method of resetting forgotten passwords and reduces the number of password reset requests for service desk technicians. Connecting your on-premises interest of AD DS to Azure Active Directory provides you with the option of implementing self-service password reset.

Fine-grained password policies

Fine-grained password policies enable you to have separate password policies within a single domain. For example, with fine-grained password policies you can have a password policy that applies to general users and have a stricter set of policies that apply to users with sensitive accounts, such as members of the IT department. Unlike Group Policy–based password

policies, which apply at the domain level, you apply fine-grained password policies to global security groups or individual user accounts. This means that multiple fine-grained password policies might apply to a single account. In this situation, use precedence settings to ensure that the appropriate policy always applies. (Precedence is covered later in this lesson.) Fine-grained password policies can't be applied to domain local or universal security groups, only to global security groups. The Active Directory domain must be at the Windows Server 2008 or later functional level or higher before you can use fine-grained password policies.

MANAGING FINE-GRAINED PASSWORD POLICIES

You create and manage fine-grained password policies through the Active Directory Administrative Center. To create a new Password Settings Object (PSO), open the Active Directory Administrative Center and navigate to the Password Settings Container (PSC), which is located in the System Container of the domain. From the **Tasks** menu, select **New**, and then select **Password Settings**. The PSC enables you to view the precedence of PSOs. Password settings with lower precedence values override password settings with higher precedence values.

CONFIGURING PASSWORD SETTINGS OBJECTS

A Password Settings Object (PSO) contains settings for both password policy and account lockout policy. A PSO applies to the groups and users specified in the Directly Applies To area. If a PSO applies to a user account, either directly or indirectly through group membership, that PSO overrides the existing password and account lockout policies configured at the domain level.

PSOs contain the following options:

- **Name** Enables you to configure a name for the PSO.
- **Precedence** When multiple PSOs apply to an account, the PSO with the lowest precedence value has priority.
- **Enforce Minimum Password Length** Minimum password length that can be used by users subject to the policy.
- **Enforce Password History** The number of passwords remembered by Active Directory. Remembered passwords can't be reused.
- **Password Must Meet Complexity Requirements** A password must contain a mix of numbers, symbols, and uppercase and lowercase letters.
- **Store Password Using Reversible Encryption** Provides backward compatibility with older software and is rarely used in Windows Server 2012 environments.
- **Protect From Accidental Deletion** The user account can't be accidentally deleted. Although this setting is not available in Group Policy password or account lockout settings, you can edit an object directly to configure it.
- **Enforce Minimum Password Age** The minimum length of time users must have a password before they are eligible to change it.
- **Enforce Maximum Password Age** The maximum number of days that users can go without changing their password.