Integrating Active Directory with Azure Active Directory

Johnathan Reinhart

This manual is to be used as a jumping-off point for any skill level between Support Level 1 and 2 when integrating AD into an Azure AD environment. This is not a comprehensive guide but rather a manual on best practices when engaging in integration for the first time. I recommend you follow this manual as you proceed. However, Microsoft Help Center is also extremely useful, as this is, in fact, a Microsoft product. Thus, they have quite a bit of literature on the topic that you might find helpful. If you are a Level 1 specialist and still need help, you can email Jonathan at: [Removed for public distribution].

Additionally, every Thursday at Room 3B, there is a skills-building seminar that we will be hosting. Come in during lunch if you like.

Table of Contents

1.1 Overview of Active Directory and Azure Active Directory

Hello! Welcome to the first chapter of our comprehensive guide on integrating Active Directory (AD) with Azure Active Directory (Azure AD). This integration represents a strategic step forward for organizations aiming to bridge their on-premises and cloud-based identity management systems. Before delving into the technicalities of integration, let's first understand the core components of this process.

Active Directory is a directory service developed by Microsoft for Windows domain networks. It provides a variety of network services, including authentication and authorization, user and computer management, and policy administration. AD is typically used within an on-premises environment, where it plays a critical role in managing the organization's IT infrastructure.

Azure Active Directory, on the other hand, is Microsoft's multi-tenant, cloud-based directory and identity management service. It offers a broad range of capabilities focused on managing users and providing access to cloud applications, including Microsoft's own services like Microsoft 365, and a vast number of third-party SaaS applications.

Integrating these two systems allows organizations to enjoy the best of both worlds: the robust, tried-and-tested management capabilities of AD, and the modern, flexible, and globally accessible services provided by Azure AD

1.2 Benefits of Integrating AD with Azure AD

Integrating Active Directory with Azure Active Directory unlocks numerous benefits for organizations, enhancing both operational efficiency and security posture. Key advantages include:

- **Unified Identity Management:** Streamline the management of user identities and access by having a single identity for each user across both on-premises and cloud environments. This simplification reduces administrative overhead and improves user experience.

- **Seamless Single Sign-On (SSO)**: Users can access both on-premises and cloud applications using the same set of credentials, minimizing password fatigue and reducing the likelihood of security breaches due to weak or reused passwords.
- **Enhanced Security Features:** Leverage Azure AD's advanced security features, such as Conditional Access policies and Multi-Factor Authentication (MFA), to protect both on-premises and cloud resources. These features help in building a more robust defense against cybersecurity threats.
- **Scalability and Flexibility:** Azure AD's cloud-based nature allows organizations to scale their identity management capabilities as needed without significant upfront investment in on-premises infrastructure. This scalability supports organizational growth and adaptation to changing business requirements.
- **Cost Efficiency:** By reducing the reliance on physical infrastructure and streamlining identity management processes, organizations can achieve significant cost savings. The integration also enables more efficient use of IT resources, allowing teams to focus on strategic initiatives rather than routine maintenance.

As we proceed through this manual, we will explore the technical aspects of achieving such integration, starting with preparing your environment, choosing the right integration method, and implementing best practices to ensure a successful deployment.

Our journey begins with understanding the prerequisites for integration, setting the stage for a smooth transition to a hybrid identity framework. Let's turn the page to Chapter 2, where we delve into the essential preparations and considerations before embarking on the integration process.

2.1 System Requirements

To begin, let's ensure your systems are ready:

- **Active Directory Environment:** Ensure that your on-premises Active Directory is running on a supported Windows Server version. It's recommended to have your domain controllers on the latest or at least a supported Windows Server version to ensure compatibility and security.
- **Azure Subscription:** You need an active Azure subscription. If you don't have one, you can sign up for a free account or a pay-as-you-go subscription to get started.
- **Azure AD Tenant:** An Azure AD tenant is required to integrate with your on-premises AD. If your organization already uses Microsoft 365 or other

Microsoft services, you likely have an Azure AD tenant set up. If not, setting up a new tenant is a straightforward process that we'll cover la

2.2 Necessary Permissions

Permissions play a critical role in the setup process:

- **On-Premises:** You'll need an account with domain admin privileges in your on-premises Active Directory. This account will be used for configuring components like Azure AD Connect and modifying schema settings if necessary.
- **Azure:** In Azure AD, you must have global administrator privileges. This level of access is required to configure integration settings, manage user syncing, and set up features like SSO and Conditional Access.

2.3 Preparing Your Active Directory for Integration

Preparation is key to ensuring that your Active Directory is ready for integration:

- **Clean Up AD Data:** Ensure that user accounts are in good standing, with accurate, up-to-date attributes. Duplicate entries, outdated information, or incorrect configurations can lead to sync issues later on.
- **Network Configuration:** Verify that your network and firewall settings allow communication between your on-premises environment and Azure AD. This includes ensuring that the necessary endpoints and ports are open and accessible.
- **Install Necessary Updates:** Apply the latest updates to your domain controllers and any servers involved in the integration process. This reduces the risk of compatibility issues and exploits.
- **Review AD Schema:** Consider extending your AD schema if you're using advanced features or custom attributes that you plan to sync with Azure AD. This step may not be necessary for all organizations but can be crucial for those with complex setups.
- **Plan for High Availability:** If your organization requires uninterrupted access to both on-premises and cloud resources, plan for high availability and disaster recovery. This may involve setting up additional domain controllers or considering staging environments for Azure AD Connect.

With these prerequisites addressed, you're well on your way to beginning the integration process. The next step is to choose the right method for integrating your Active Directory with Azure Active Directory, which we will explore in Chapter 3. This decision will shape the path forward, impacting how users are managed and authenticated across your hybrid environment.

3.1 Creating an Azure AD Tenant

An Azure AD tenant represents a dedicated instance of Azure AD that your organization receives and owns. Here's how to set one up:

- **Sign Up for Azure:** If you haven't already, sign up for an Azure account. You can start with a free account which provides you with access to most services for a limited period or a number of resources.
- **Access the Azure Portal:** Once your Azure account is active, log in to the Azure Portal.
- **Create a New Tenant:** Navigate to the Azure Active Directory section and select "Create a new tenant." Follow the prompts, providing information about your organization, including the organization's name and initial domain name. The domain name will be in the form of `<yourdomain>.onmicrosoft.com`, which you can later customize with your organization's domain.
- **Configure Basic Tenant Settings:** After creating your tenant, configure the basic settings, such as country/region, preferred language, and organizational details. These settings can impact certain compliance and data residency configurations.

3.2 Configuring Azure AD Basic Settings

With your Azure AD tenant created, you’ll need to configure some basic settings to tailor the directory to your organization's needs:

- **Custom Domain Name:** By default, your Azure AD instance will use a domain like `<yourdomain>.onmicrosoft.com`. Most organizations prefer to use their domain, such as `@yourcompany.com`. To do this, navigate to the "Custom domain names" section in Azure AD, add your domain, and verify it by updating DNS records as instructed.
- **User Accounts:** Start creating user accounts or prepare for user synchronization if you plan to integrate with your on-premises AD. At this stage, you might only create accounts for administrators or test users.
- **Company Branding:** Personalize the sign-in and access panel experiences by adding your company branding to Azure AD. This includes logos, custom color schemes, and sign-in page text, enhancing the user experience and reinforcing security by making phishing attempts easier to identify.
- **Security Defaults:** Azure AD offers security defaults that provide pre-configured security settings covering common attacks. Consider enabling these defaults initially, especially Multi-Factor Authentication (MFA) for admin accounts, to protect your organization.
- **License Assignments:** Depending on the services your organization plans to use (e.g., Microsoft 365, Azure services), assign licenses to user accounts. This ensures that users have access to the necessary resources and applications.

3.3 Understanding Azure AD Editions

Azure AD comes in several editions: Free, Office 365 apps, Premium P1, and Premium P2. Each edition offers different features, such as advanced security, identity protection, and governance capabilities. Evaluate your organization's needs to select the appropriate edition. Upgrading is always an option as your requirements evolve.

3.4 Planning for Integration

With your Azure AD tenant established and basic configurations set, the groundwork is laid for integrating with your on-premises Active Directory. The integration process, which will be detailed in the upcoming chapters, involves choosing an integration method, setting up directory synchronization, and configuring single sign-on (SSO), among other tasks.

By completing the steps in this chapter, you have taken a critical stride towards enabling a robust, cloud-based identity and access management solution for your organization. The next chapter will delve into the various integration options available and guide you in selecting the most suitable approach for your organizational needs and objectives.

4.1 Overview of Integration Options

Integrating AD with Azure AD can be achieved through several methods, each with its unique advantages and suited for different organizational needs. The main options include:

- **Azure AD Connect:** The most commonly used tool for integrating on-premises AD with Azure AD. It synchronizes user accounts, groups, and other AD objects to Azure AD, enabling users to access Microsoft cloud services with their existing credentials. It supports various sign-in options, including Password Hash Synchronization (PHS), Pass-through Authentication (PTA), and Federation.
- **Pass-through Authentication (PTA):** A feature of Azure AD Connect that allows users to sign in using the same passwords as on-premises without storing those passwords in the cloud. Authentication requests are passed back to the on-premises AD.
- **Federation (with AD FS or third-party identity providers):** Ideal for organizations with complex authentication requirements or those that require additional customization. Federation uses a claims-based authentication method, allowing users to access both on-premises and cloud applications with a single set of credentials.
- **Azure AD Application Proxy**: Enables users to access on-premises web applications through Azure AD, leveraging its security and conditional access policies without changing the network infrastructure.

4.2 Choosing the Right Integration Option for Your Organization

Selecting the right integration method depends on various factors, including your organization's security requirements, infrastructure complexity, and specific needs for customization. Here’s a brief guideline:

- **Azure AD Connect with Password Hash Synchronization:** Best for organizations looking for a straightforward, easy-to-manage solution that doesn't require complex authentication mechanisms.
- **Azure AD Connect with Pass-through Authentication:** Suitable for organizations that prefer not to store password hashes in the cloud but still want a simple integration.
- **Federation with AD FS or Third-party Identity Providers:** ideal for organizations with advanced security and compliance requirements, needing the flexibility to customize authentication and authorization processes.
- **Azure AD Application Proxy:** A perfect choice for extending access to on-premises web applications to remote users while maintaining control over authentication and access.

4.3 Preparing for Integration

Before proceeding with the chosen integration method, ensure the following preparatory steps are completed:

- **Review and Clean Up AD Objects:** Ensure that the user accounts and groups in your on-premises AD are correctly configured, with up-to-date and standardized attributes. This will prevent synchronization issues and ensure a smooth integration process.
- **Network and Connectivity:** Verify that your network infrastructure is ready for integration. This includes ensuring proper connectivity between your on-premises AD and Azure AD and configuring any required firewall rules.
- **Decide on Synchronization Features:** Depending on the chosen method, decide which features you will enable, such as password synchronization, filtering, or write-back capabilities. This decision impacts how data flows between on-premises AD and Azure AD.
- **Plan for High Availability:** If continuous access to cloud services is critical for your organization, plan for high availability of the integration components, such as deploying multiple Azure AD Connect instances or configuring a highly available AD FS infrastructure.

With a clear understanding of the integration options and having prepared your environment accordingly, you're now ready to embark on the actual integration process. The following chapters will delve deeper into each integration method, providing step-by-step guidance on setting up Azure AD Connect, implementing federation, and leveraging Azure AD Application Proxy to achieve a seamless and secure integration between your on-premises Active Directory and Azure Active Directory.

5.1 Installing AD Connect

Before installing AD Connect, ensure that you meet the system and permission requirements as outlined in Chapter 2. Once ready, follow these steps to install AD Connect:

Download Azure AD Connect: Download Azure AD Connect V2 from Official Microsoft Download Center Navigate to the official Azure AD Connect download page and download the latest version of the tool.

Launch the Installer: Run the Azure AD Connect installer on a server that can communicate with your on-premises AD. The server doesn't need to be a Domain Controller, but it should meet the tool's system requirements.
Express Settings vs. Customized Installation: For a straightforward setup, you can choose the Express Settings, which is suitable for most small to medium-sized organizations. It configures Password Hash Synchronization (PHS) as the default sign-in method. If you require more control over the synchronization process, such as filtering specific AD objects or configuring other sign-in methods like Pass-through Authentication (PTA) or federation, select the customized installation.
Enter Admin Credentials: You'll be prompted to provide Azure AD Global Administrator credentials and on-premises AD Enterprise Admin credentials. These are required to configure the synchronization settings and permissions.
Configure Sign-In Options: If you chose the customized installation, select your preferred sign-in method. The options include Password Hash Synchronization, Pass-through Authentication, and federation with AD FS.
Configure Synchronization Options: Select the AD forests and domains you want to synchronize. You can also configure filtering to exclude certain objects or OU (Organizational Units) from synchronization.
Install: Proceed with the installation. After installation, the synchronization process will begin, copying AD objects to Azure AD based on the configured settings.

5.2 Configuring Synchronization Options

After installing AD Connect, you might want to tweak the synchronization settings to better fit your organization's needs:

- **Synchronization Schedule:** By default, AD Connect synchronizes every 30 minutes. You can adjust this frequency based on your requirements.
- **Filtering:** Filtering allows you to control which objects (users, groups, etc.) are synchronized to Azure AD. This is useful for excluding test accounts or objects that are not needed in the cloud.
- **Attribute Mapping:** Customize how on-premises AD attributes map to Azure AD attributes. This is particularly important for organizations that use custom attributes or have specific identity requirements.

5.3 Scheduling Synchronization

The AD Connect synchronization process is scheduled to run at regular intervals automatically. However, you might need to perform a manual sync during initial setup or when significant changes are made in your on-premises AD:

Initial Sync: After installation, it's recommended to monitor the initial synchronization closely to ensure that all intended objects are successfully synchronized and that there are no errors.
Forcing a Manual Sync: If you need to force a manual synchronization, you can do so by using PowerShell commands on the server where AD Connect is installed.

5.4 Monitoring and Managing AD Connect

Regular monitoring of AD Connect is essential to ensure ongoing synchronization health:

- **Azure AD Connect Health:** Use Azure AD Connect Health for monitoring the health and performance of your AD Connect synchronization. It provides alerts and insights into synchronization issues and overall health.
- **Troubleshooting:** Familiarize yourself with common synchronization issues and their resolutions. The Azure AD Connect Health dashboard and the AD Connect synchronization service manager are valuable tools for identifying and resolving issues.

6.1 Overview of Federation

Federation uses standards-based secure identity authentication mechanisms, such as SAML and OAuth, to allow users to access multiple applications using a single set of credentials. This method is particularly useful for organizations with complex authentication requirements or those looking for greater control over the login experience.

6.2 Setting Up AD FS

Install AD FS Role: Begin by installing the AD FS role on a Windows Server within your on-premises environment.
Configure AD FS: After installation, configure AD FS by creating a Federation Service, defining a federation server, and setting up a trust relationship between AD FS and Azure AD.
Certificate Requirements: Ensure you have a valid SSL certificate from a trusted Certificate Authority (CA) for the AD FS server.

6.3 Configuring AD FS for Azure AD

Connect AD FS with Azure AD: Use the Azure AD Connect tool to establish a federation trust between your on-premises AD FS and Azure AD. During this process, you'll specify the AD FS server as the authentication method.
Relying Party Trust: Configure a Relying Party Trust on the AD FS server for Azure AD, allowing Azure AD to trust tokens issued by AD FS.
Claim Rules: Define claim rules to determine how user attributes are passed from AD FS to Azure AD during the authentication process.

6.4 Managing Federation Trust

Regularly monitor and maintain the federation trust to ensure seamless authentication experiences. This includes monitoring AD FS server performance, updating SSL certificates before they expire, and adjusting claim rules as necessary to meet evolving organizational needs.

Federation with AD FS provides a robust way to extend on-premises authentication mechanisms to cloud services, offering enhanced security and a seamless user experience. However, it requires careful planning and ongoing management to ensure optimal performance and security.

7.1 Synchronizing Users and Groups

- **Azure AD Connect:** Utilize Azure AD Connect to synchronize your on-premises AD objects with Azure AD. This includes users, groups, and other AD objects, ensuring that your cloud and on-premises environments are aligned.

- **Synchronization Rules:** Customize synchronization rules to control which objects are synchronized to Azure AD, based on attributes, group memberships, or organizational units (OUs).

7.2 Managing Azure AD Group Memberships from AD

- **Group-Based Management:** Learn how to manage group memberships directly from your on-premises AD. Changes to group memberships in AD will automatically reflect in Azure AD, simplifying access management for cloud resources.
- **Dynamic Groups in Azure AD:** Explore the use of dynamic groups in Azure AD, which automatically update memberships based on user attributes, reducing the administrative overhead of managing user access.

7.3 Handling User Attributes and Custom Mappings

- **Attribute Customization:** Tailor how user attributes are synchronized from AD to Azure AD. This includes modifying attribute flows in Azure AD Connect and using expressions for custom mappings.
- **Directory Extensions:** Extend your Azure AD schema with custom attributes from your on-premises AD. This is particularly useful for applications that require specific user attributes not present in the default schema.

Best Practices:

- Regular Review: Periodically review your synchronization settings and group memberships to ensure they meet your organization's access and security requirements.
- Monitor Synchronization Health: Utilize tools like Azure AD Connect Health to monitor the health of your synchronization process, ensuring that user and group data remain consistent across environments.

8.1 Configuring SSO with AD Connect

- **Overview:** Simplify user access to both on-premises and cloud resources by enabling Single Sign-On (SSO) using Azure AD Connect. This method allows users to utilize their existing on-premises AD credentials to access Azure AD services without additional logins.
- Steps:

    Install Azure AD Connect: Ensure Azure AD Connect is installed with the 'Password Hash Synchronization' or 'Pass-through Authentication' option selected, depending on your organization's preference.

    Enable SSO: In the Azure AD Connect setup wizard, choose the option to enable SSO and follow the prompts to configure it.

8.2 Setting Up SSO with Federation

- **Overview:** For organizations requiring advanced authentication scenarios, setting up federation with services like Active Directory Federation Services (AD FS) offers customizable authentication flows, integrating with Azure AD for SSO.

    Configure AD FS: Install and configure AD FS in your environment, establishing a trust relationship with Azure AD.

    Federate with Azure AD: Use Azure AD Connect or the Azure portal to create a federated trust between your AD FS and Azure AD, enabling SSO for users.

Best Practices:

- Regular Validation: Regularly test and validate the SSO experience from various user endpoints to ensure seamless access.
- Monitor Authentication Logs: Keep an eye on authentication logs for any failed SSO attempts and address issues promptly to maintain uninterrupted service.