Requirements

Tailwind Traders is doing very well and is expanding their workforce. They have successfully bought an online retailer in the sports apparel space. The company has also found a partner to outsource marketing literature. Tailwind Traders is using Azure Active Directory for user and groups accounts. Here are two specific initiatives the IT department would like you to help with.

* 1. • New user accounts. ▪ The online retailer acquisition will add 75 employees to Tailwind Traders. All the new users have on-premises Active Directory Domain Services accounts in the retailer’s existing domain.
  2. ▪ The new marketing partner will initially have 15 employees who will need corporate access. These employees already have Azure AD accounts in the partner’s AAD tenant.
  3. ▪ The new employees are located at various geographic locations and will need account privileges for their new job roles. Some changes to existing employee roles are expected.
  4. ▪ The IT department wants to take this opportunity to include new identity security features.
  5. • **New application access.** The business development team has an application running on Azure VM and data stored in an Azure SQL database. They need to securely allow the VM to query the Azure SQL database. They also need an on-premises server to be able to securely access the SQL database without storing credentials in the application code or configuration files.

Tasks

1. New user accounts. • Diagram the process for bringing in the acquired user accounts.

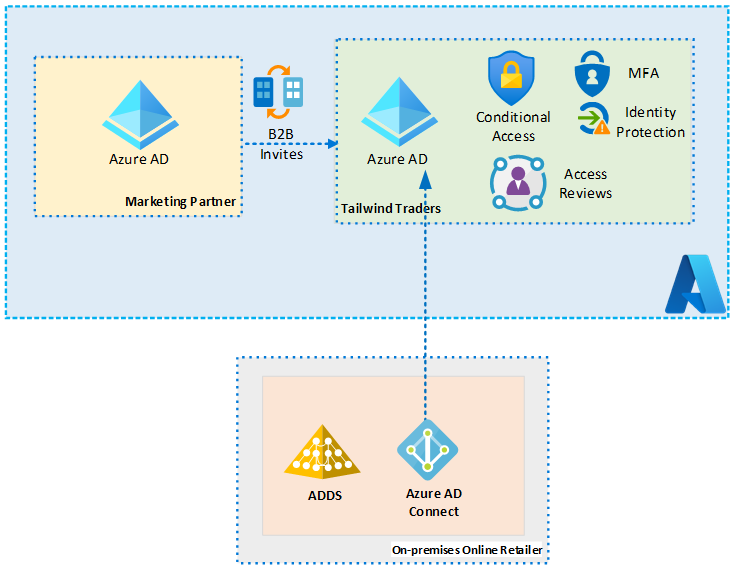
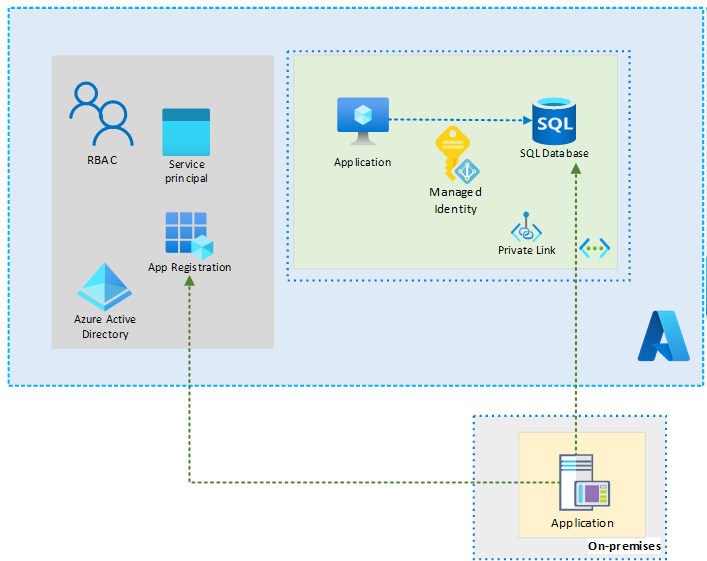
• Diagram the process for adding the new partner accounts.

• For the above 2 requirements, be sure to include any tools that will be used. List at least three benefits of your suggested solution.

• Provide at least three recommendations for improving Tailwind Traders user identity solutions. Rank the recommendations in order of importance. Include your reasons for making these suggestions.

2. New application access • Provide an access solution for the business development application.

* + Provide an access solution for the on-premises resources.

1. **Solution**
2. 1. New employee user accounts.
3. 
4. The on-premises users can be synced using Azure AD Connect. Are new groups needed in Azure AD? How will you decide which Azure AD groups to use? Are the permissions for existing groups appropriate? Use password hash for synchronization? Advantages include centralized management, synchronized changes, and ease of administration.
5. The partner users can be added using Azure B2B. These external identities will be added as guest users. What new Azure AD groups will be needed? What permissions will these users need? Who will issue the invites? Advantages include established processes, centralized management, and ease of administration.
6. 2. **New identity solution features.** Here are some recommendations to discuss and review. Discuss the order of importance.
7. 

• Use MFA for privileged roles like administrators. Consider MFA for the partner accounts.

• Use access reviews to ensure users changing jobs still have the correct permissions.

• Use RBAC to ensure permissions are correct. Design at the group level.

• Require users to access applications only from managed devices.

• Block access from untrusted sources, such as access from unknown or unexpected locations.

• Establish user and sign-in risk policies.

* 1. 3. New application access • Access solution for the business development application: Use a Windows VM system-assigned managed identity to access Azure SQL. Managed Service Identities are automatically managed by Azure and enable you to authenticate to services that support Azure AD authentication, without needing to insert credentials into your code.

• Access solution for the on-premises resources: Register the application with Azure AD and assign an application service principal. With Azure AD, you can use

* 1. Azure role-based access control (Azure RBAC) to grant permissions to a security principal, which may be a user, group, or application service principal. The security principal is authenticated by Azure AD to return an OAuth 2.0 token. The token can then be used to authorize a request against the Blob service.