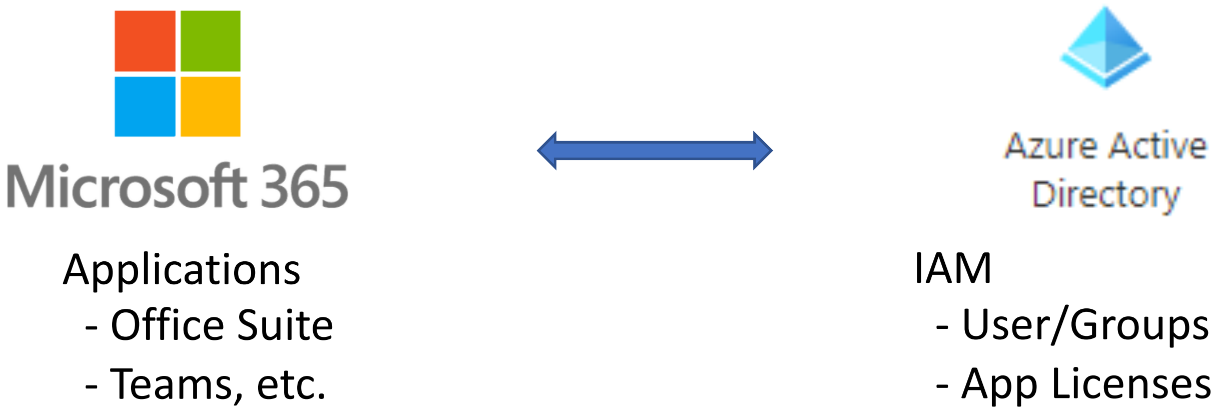
Morro Data Integration with Azure AD Domain

Step-by-Step using Azure AD as the Source of Identity

User management in Microsoft 365

- Microsoft 365 uses Azure Active Directory as Source of Identity
- If you have a Microsoft 365 account, then you can use Azure AD IAM (Identity and Access Management) for free

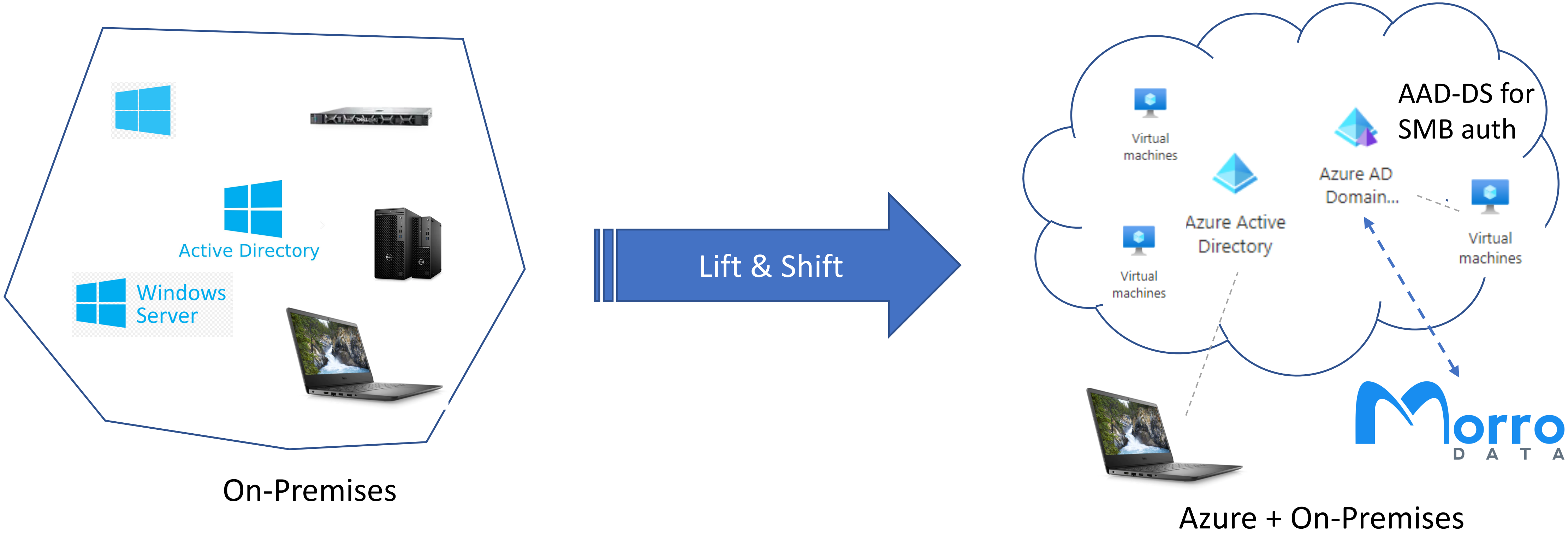


Applications
- Office Suite
- Teams, etc.

IAM
- User/Groups
- App Licenses

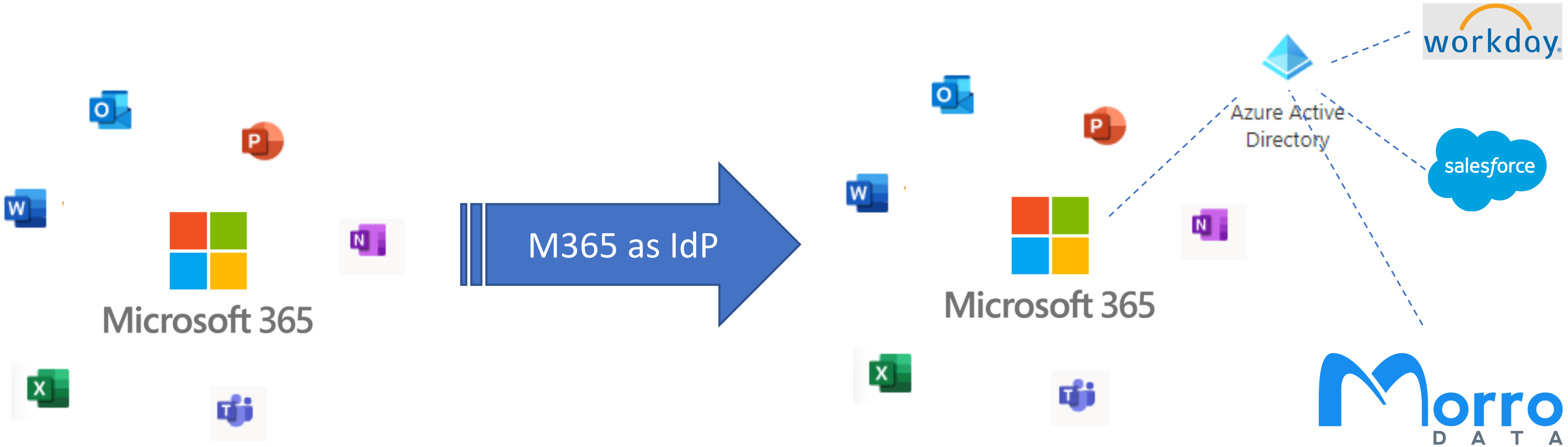
Who should consider Azure AD as IdP (Identity Provider)

- Company using on-premises Active Directory but wants to lift and shift on-premises resources.



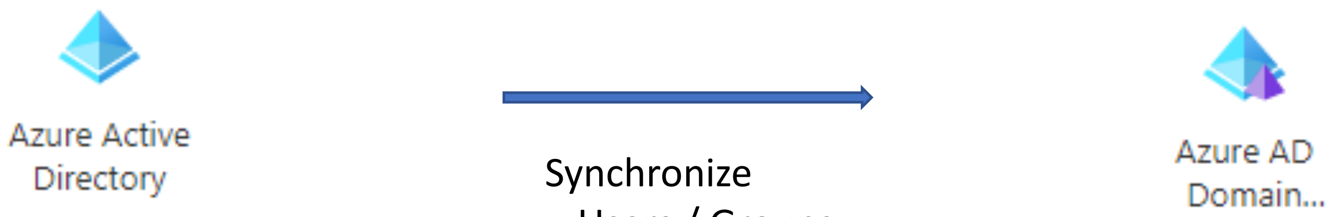
AAD as IdP (cont'd)

- Cloud-Only organization using Microsoft 365 but does not use on-prem AD



Azure AD & Azure AD Domain Services

- Azure AD Domain Services supports SMB and legacy authentication while Azure AD does not. In a domain environment, Morro uses SMB authentication.
- Synchronize Identity from Azure AD to AAD DS
  - Users/Groups
  - User credentials when set/change password
- Multiple AAD DS can be deployed for different geographical regions



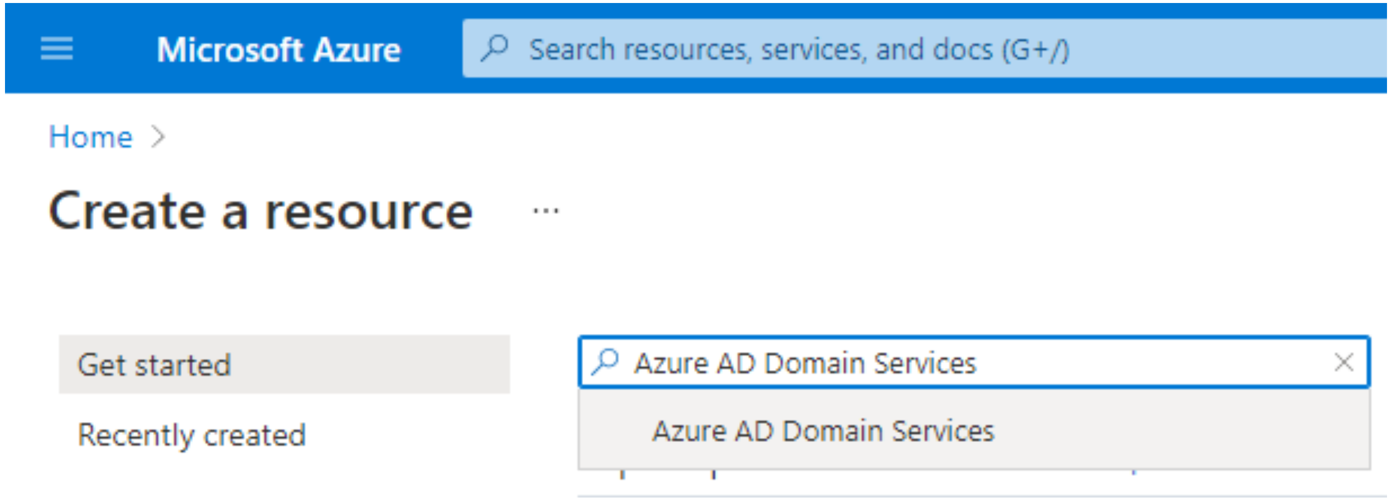
AAD provides Auth for web apps using SAML/OIDC

Synchronize
- Users / Groups
- Credentials

AAD DS provides Auth for SMB and legacy applications

Step 1: Create Azure AD Domain Services

- Assume identity is already migrated from on-prem AD to Azure AD
- Assume Microsoft 365 and/or Azure AD is already set up
- Create Azure AD Domain Services
  - Start Wizard by selecting Azure AD Domain Services from Create a resource

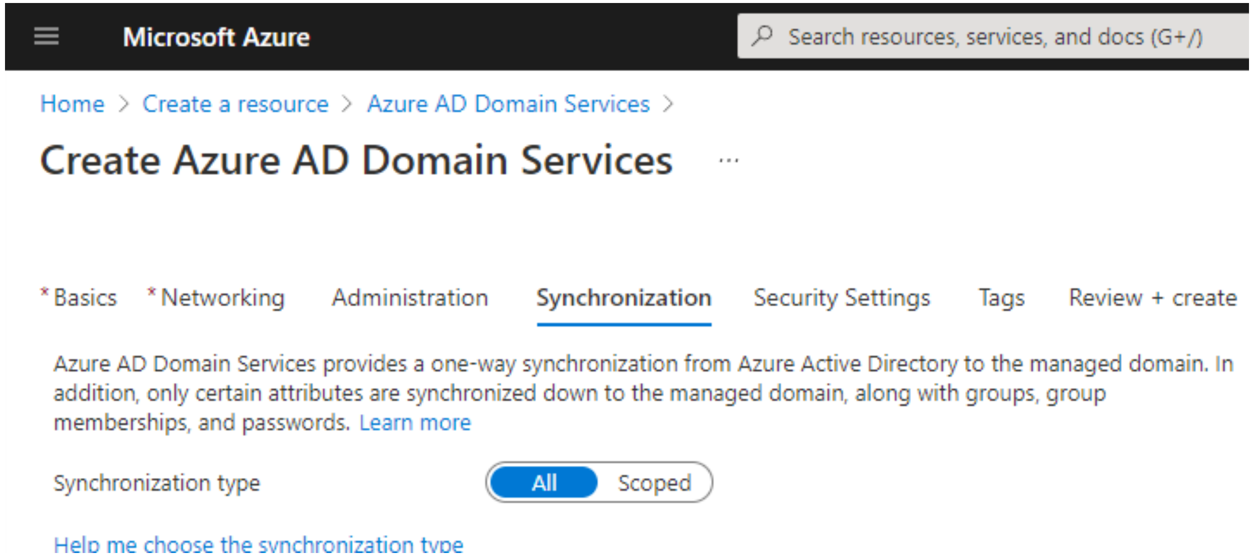


Azure AD Domain Services

Azure AD Domain Services

Step 2: Configure Azure AD Domain Services

- Follow the Wizard. Some configurations cannot be modified later.
- Consider Scoped Sync for large directory
- Enable “NTLM Password Synchronization” to use SMB authentication



Home > Create a resource > Azure AD Domain Services >

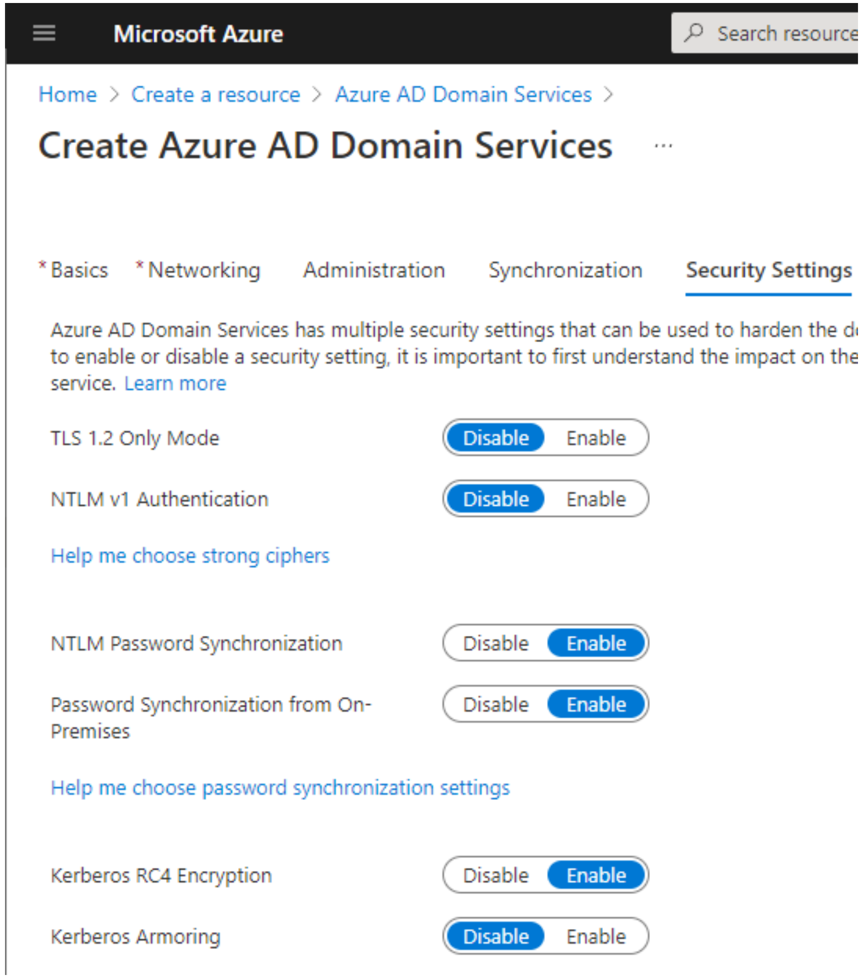
Create Azure AD Domain Services ...

*Basics *Networking Administration **Synchronization** Security Settings Tags Review + create

Azure AD Domain Services provides a one-way synchronization from Azure Active Directory to the managed domain. In addition, only certain attributes are synchronized down to the managed domain, along with groups, group memberships, and passwords. Learn more

Synchronization type [✓ All] Scoped

Help me choose the synchronization type



Home > Create a resource > Azure AD Domain Services >

Create Azure AD Domain Services ...

*Basics *Networking Administration Synchronization **Security Settings**

Azure AD Domain Services has multiple security settings that can be used to harden the d to enable or disable a security setting, it is important to first understand the impact on the service. Learn more

TLS 1.2 Only Mode [✓ Disable] Enable

NTLM v1 Authentication [✓ Disable] Enable

Help me choose strong ciphers

NTLM Password Synchronization Disable [✓ Enable]

Password Synchronization from On-Premises Disable [✓ Enable]

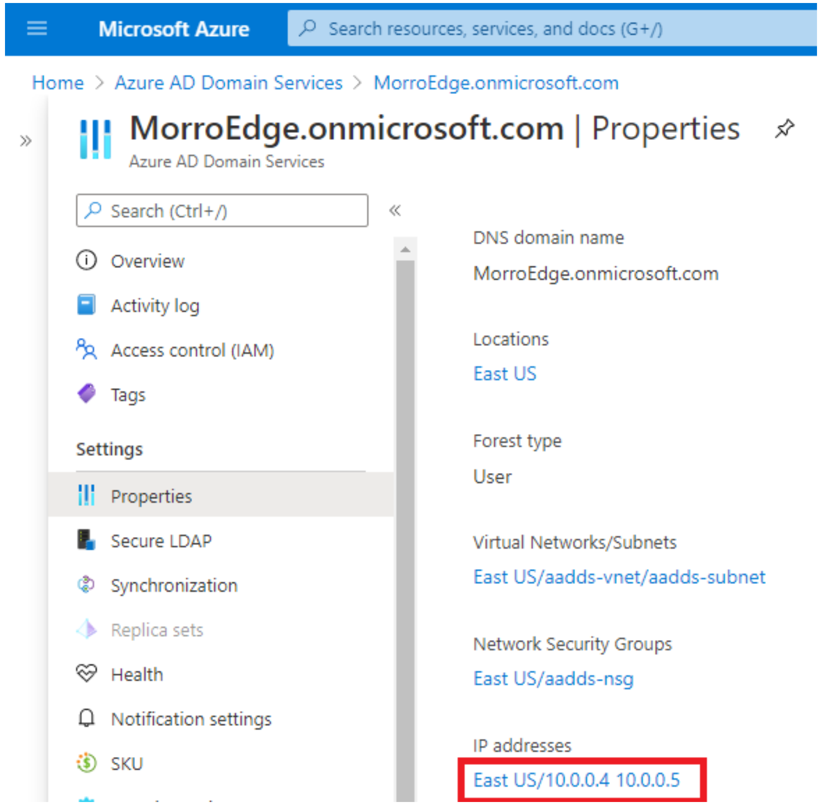
Help me choose password synchronization settings

Kerberos RC4 Encryption Disable [✓ Enable]

Kerberos Armoring [✓ Disable] Enable

Step 3: Configure Azure VNet

- Set up DNS server to look up domain-joined devices by name
  - Copy IP Addresses of AAD DS into VNet DNS servers configuration.



MorroEdge.onmicrosoft.com | Properties

Azure AD Domain Services

DNS domain name
MorroEdge.onmicrosoft.com

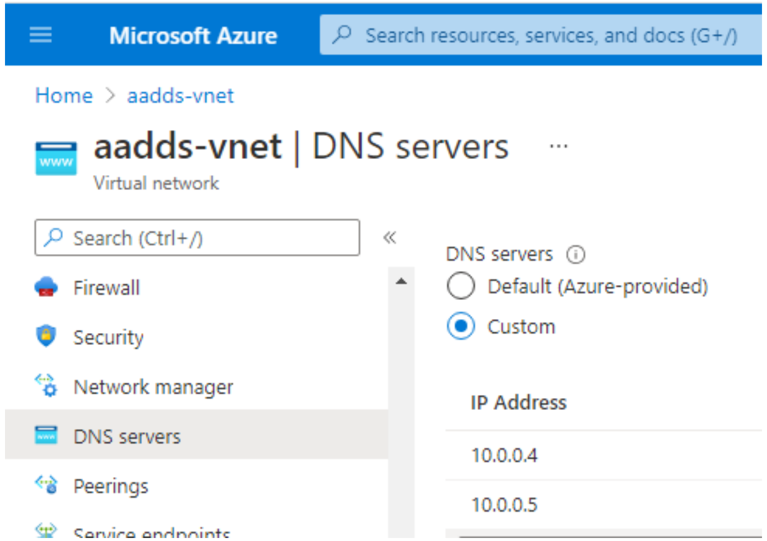
Locations
East US

Forest type
User

Virtual Networks/Subnets
East US/aadds-vnet/aadds-subnet

Network Security Groups
East US/aadds-nsg

IP addresses
East US/10.0.0.4 10.0.0.5



aadds-vnet | DNS servers

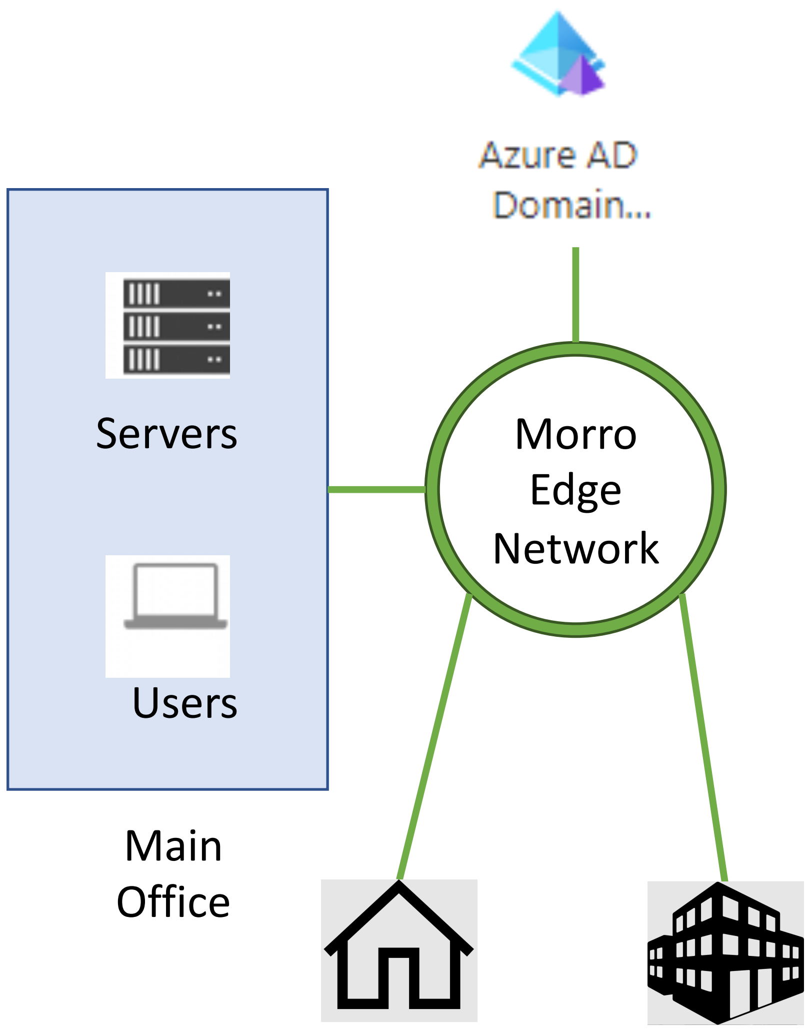
Virtual network

DNS servers
○ Default (Azure-provided)
● Custom

IP Address
10.0.0.4
10.0.0.5

Step 4: Enable Morro Edge

- Now that Azure AD Domain Services is up. How to connect it to on-prem offices and/or home offices?
- VPN or SDN connection is needed
- As an integrated function of Morro Global File Services, Morro Edge WAN Network securely connects all sites that do not have VPN or SDN, including the AAD DS VNet.


Azure AD
Domain...
Servers
Users
Main
Office
Morro
Edge
Network