Create and configure an Azure Active Directory Domain

Azure Active Directory Domain Services (Azure AD DS) provides managed domain services such as domain join, group policy, LDAP, Kerberos/NTLM authentication that is fully compatible with Windows Server Active Directory. You consume these domain services without deploying, managing, and patching domain controllers yourself.

Azure AD DS integrates with your existing Azure AD tenant. This integration lets users sign in using their corporate credentials, and you can use existing groups and user accounts to secure access to resources.

How does Azure AD DS work?

When you create an Azure AD DS managed domain, you define a unique namespace. This namespace is the domain name, such as *aaddscontoso.com*. Two Windows Server domain controllers (DCs) are then deployed into your selected Azure region. This deployment of DCs is known as a replica set.

You don't need to manage, configure, or update these DCs. The Azure platform handles the DCs as part of the managed domain, including backups and encryption at rest using Azure Disk Encryption.

A managed domain is configured to perform a one-way synchronization from Azure AD to provide access to a central set of users, groups, and credentials. You can create resources directly in the managed domain, but they aren't synchronized back to Azure AD. Applications, services, and VMs in Azure that connect to the managed domain can then use common AD DS features such as domain join, group policy, LDAP, and Kerberos/NTLM authentication.

In a hybrid environment with an on-premises AD DS environment, Azure AD Connect synchronizes identity information with Azure AD, which is then synchronized to the managed domain.

Azure AD DS features and benefits:

To provide identity services to applications and VMs in the cloud, Azure AD DS is fully compatible with a traditional AD DS environment for operations such as domain-join, secure LDAP (LDAPS), Group Policy, DNS management, and LDAP bind and read support. LDAP write support is available for objects created in the managed domain, but not resources synchronized from Azure AD.

Simplified deployment experience: Azure AD DS is enabled for your Azure AD tenant using a single wizard in the Azure portal.

•**Integrated with Azure AD:** User accounts, group memberships, and credentials are automatically available from your Azure AD tenant. New users, groups, or changes to attributes from your Azure AD tenant or your on-premises AD DS environment are automatically synchronized to Azure AD DS.

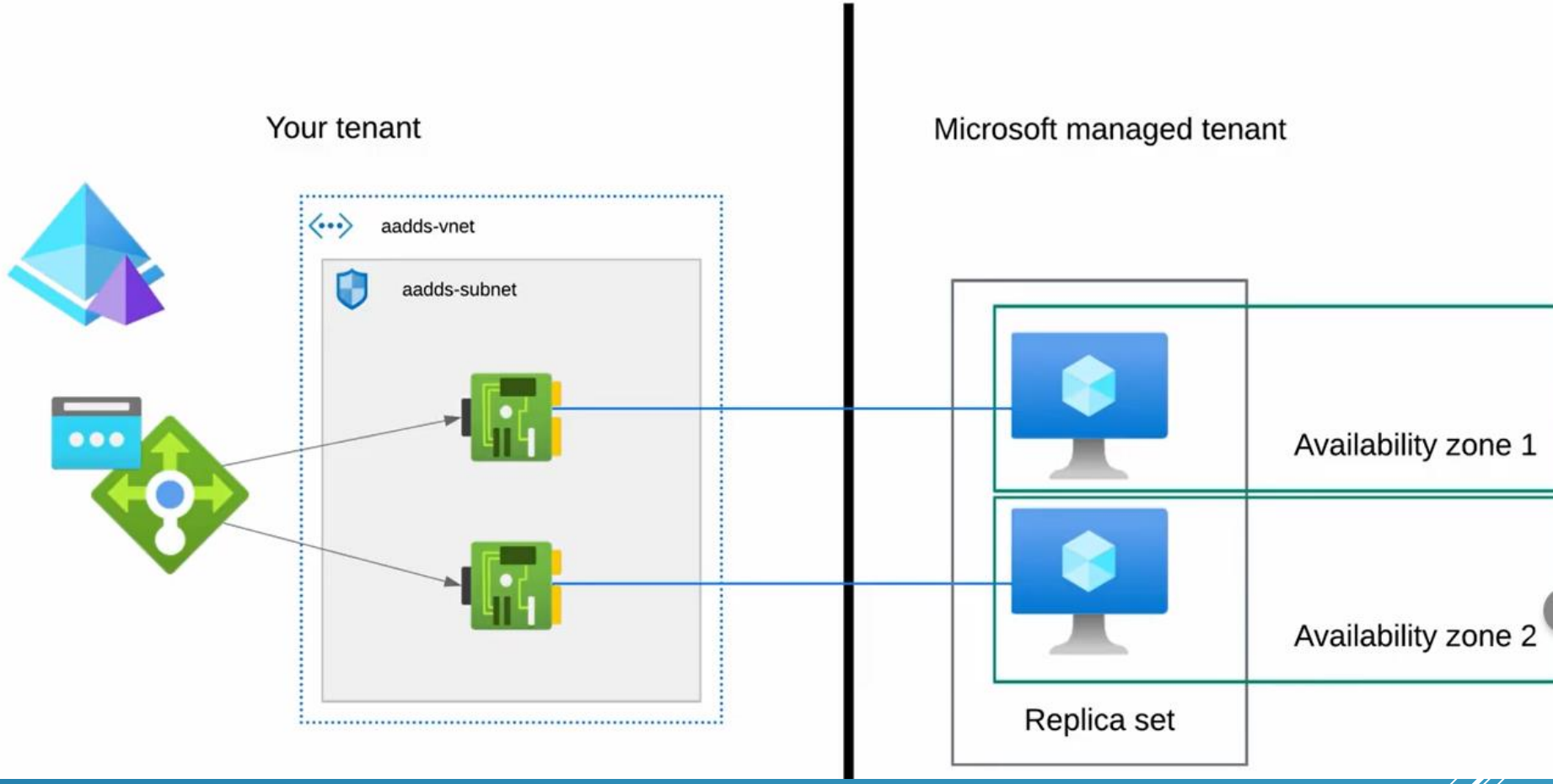
- Accounts in external directories linked to your Azure AD aren't available in Azure AD DS. Credentials aren't available for those external directories, so can't be synchronized into a managed domain.

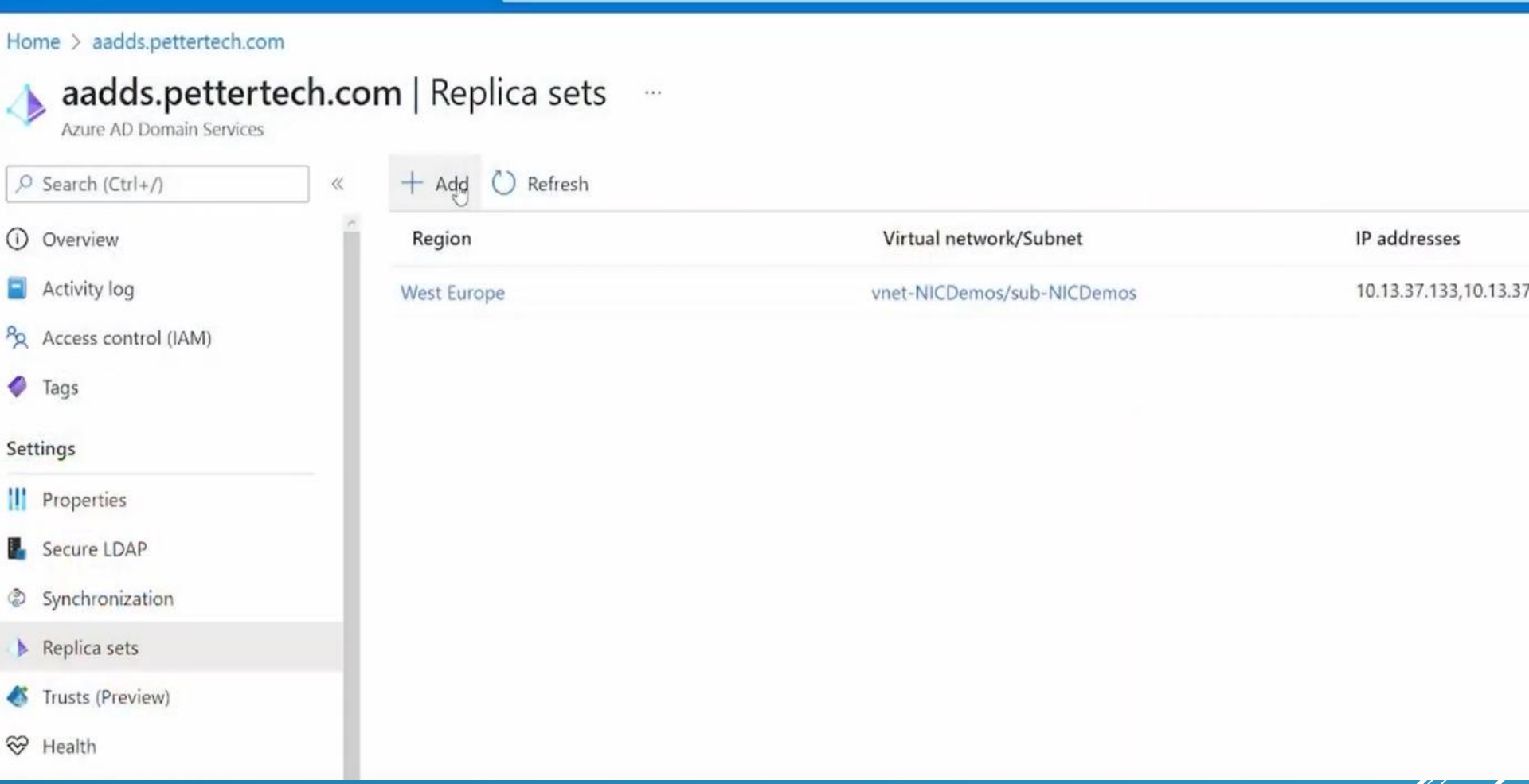
•**Use your corporate credentials/passwords:** Passwords for users in Azure AD DS are the same as in your Azure AD tenant. Users can use their corporate credentials to domain-join machines, sign in interactively or over remote desktop, and authenticate against the managed domain.

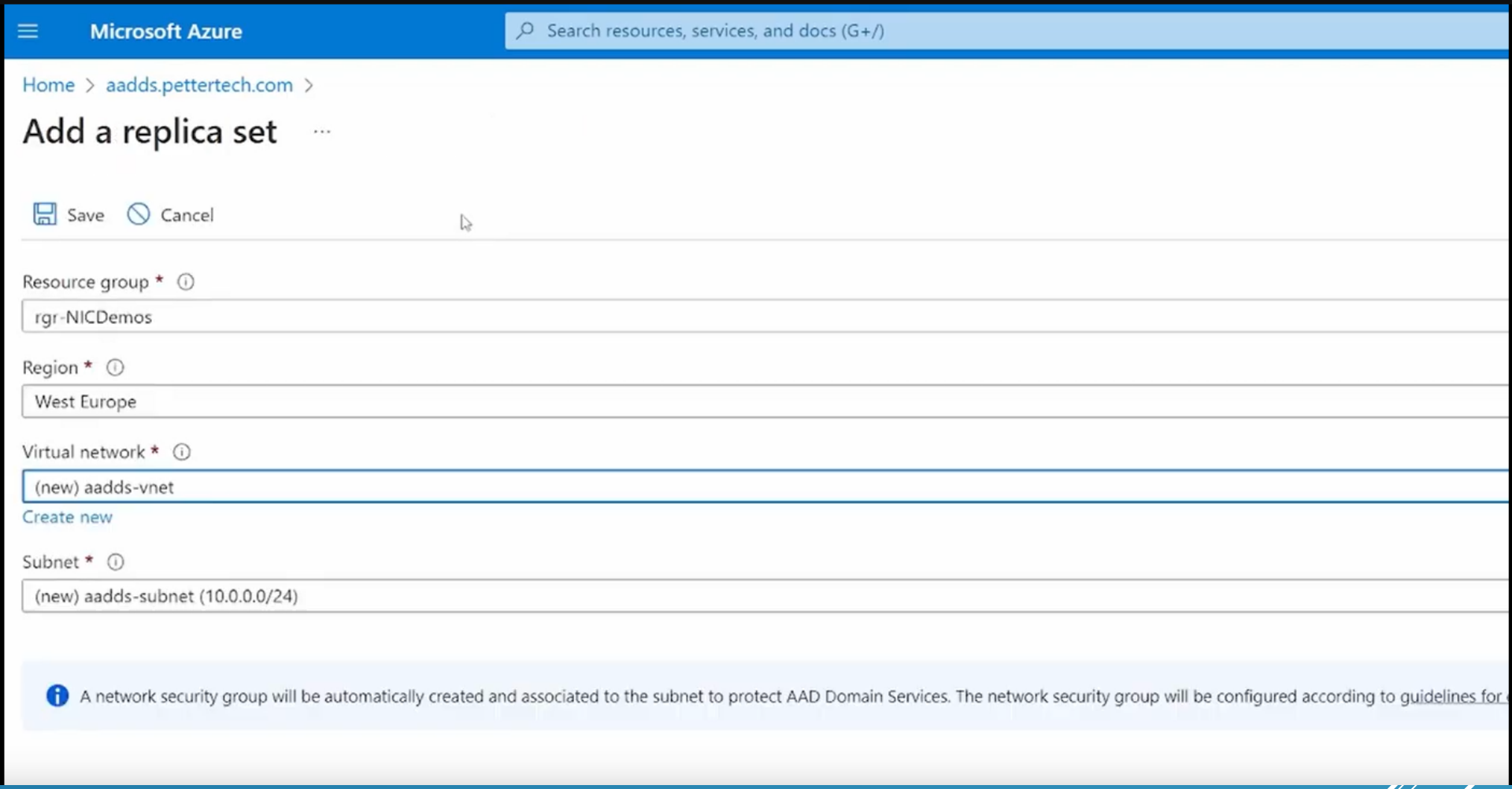
•**NTLM and Kerberos authentication:** With support for NTLM and Kerberos authentication, you can deploy applications that rely on Windows-integrated authentication.

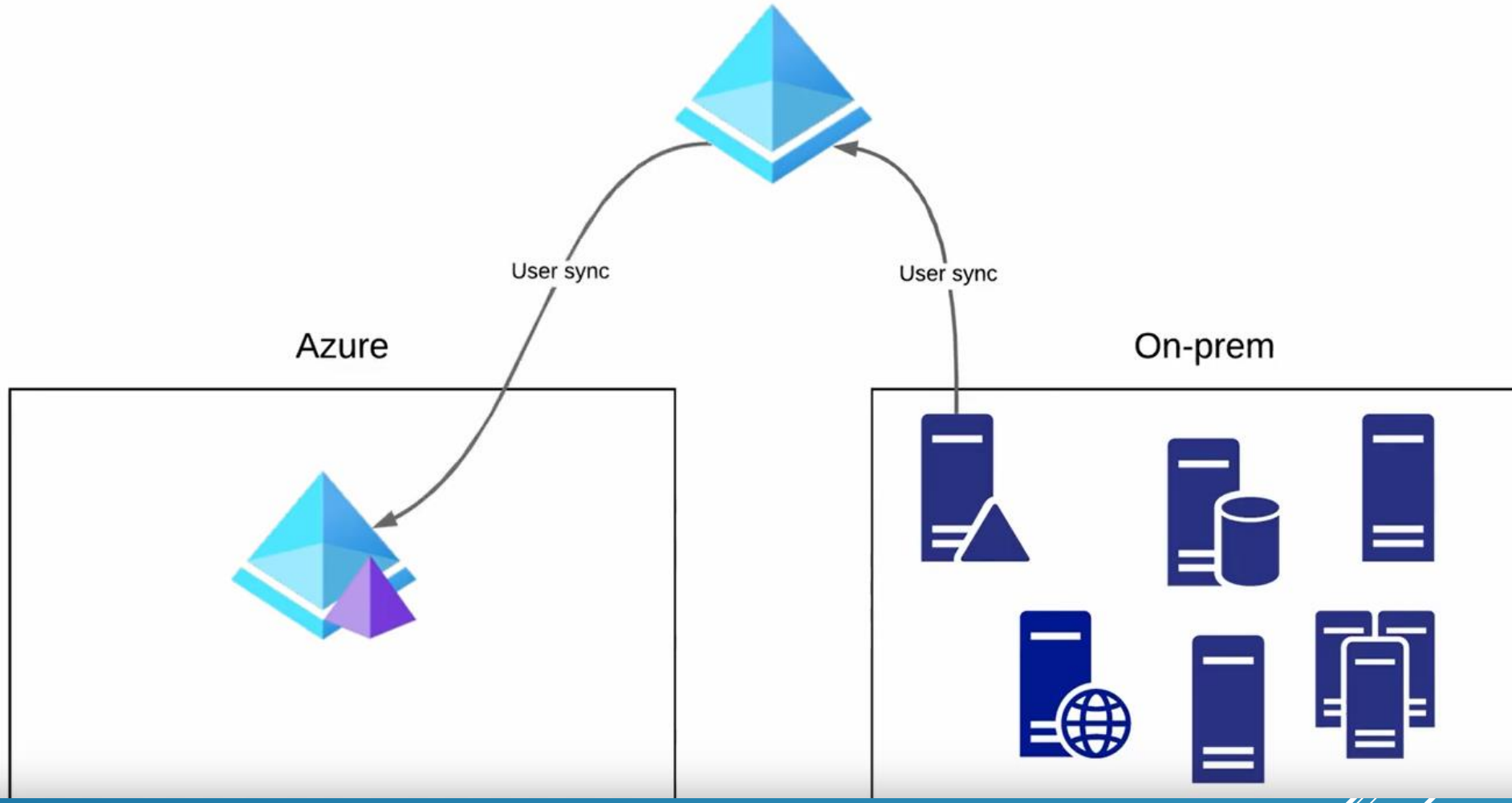
•**High availability:** Azure AD DS includes multiple domain controllers, which provide high availability for your managed domain. This high availability guarantees service uptime and resilience to failures.

- In regions that support Azure Availability Zones, these domain controllers are also distributed across zones for additional resiliency.
- Replica sets can also be used to provide geographical disaster recovery for legacy applications if an Azure region goes offline.


Your tenant
Microsoft managed tenant
aadds-vnet
aadds-subnet
Availability zone 1
Availability zone 2
Replica set


Home > aadds.pettertech.com
aadds.pettertech.com | Replica sets
Azure AD Domain Services
Search (Ctrl+/)
Add
Refresh
Region
Virtual network/Subnet
IP addresses
West Europe
vnet-NICDemos/sub-NICDemos
10.13.37.133,10.13.37
Overview
Activity log
Access control (IAM)
Tags
Settings
Properties
Secure LDAP
Synchronization
Replica sets
Trusts (Preview)
Health


Microsoft Azure
Search resources, services, and docs (G+/)
Home > aadds.pettertech.com >
Add a replica set
Save
Cancel
Resource group *
rgr-NICDemos
Region *
West Europe
Virtual network *
(new) aadds-vnet
Create new
Subnet *
(new) aadds-subnet (10.0.0.0/24)
A network security group will be automatically created and associated to the subnet to protect AAD Domain Services. The network security group will be configured according to guidelines for


User sync
User sync
Azure
On-prem

Azure AD DS Limitations

No Hybrid Azure AD Join

A client computer can be joined to AD DS (Windows or Azure) or to Azure AD. For client computers joined to Windows AD, Azure AD Connect Sync can hybrid join them to Azure AD. Azure AD Connect Sync does not support Azure AD DS and, therefore, client computers cannot be Hybrid Azure AD Joined if a member of an Azure AD DS domain. These client computers cannot be part of services that require Azure AD Join or Hybrid Azure AD join, such as Universal Print or Conditional Access Policies.

No Enterprise or Domain Admin

There are no Enterprise or Domain admin accounts in Azure AD DS. Instead, there is a group called AAD DC Administrators used to manage Azure AD DS. Accounts in this group have rights such as local administrator on member servers and administrative rights required to manage Azure AD DS. The Domain and Enterprise Administrator permissions are reserved for the Azure AD DS service.

No Active Directory Certificate Services Support

The first requirement for installing Active Directory Certificate Services is to log in as a member of the Enterprise Admin Group. As stated, these accounts do not exist in Azure AD DS, and therefore, AD Certificate Service is not supported in Azure AD DS. That rules out certificate-based features such as smart card authentication.

Schema cannot be Extended

Azure AD DS does not support extending the schema. Lack of schema extension rules out any applications, both Microsoft and 3rd party, that require a schema extension.

Limited Group Policy Support

Azure AD DS is a PaaS offering, meaning customers don't have to log in and manage the Domain Controllers. With that said, there is no access to server resources such as the sysvol folder. Azure AD DS does support a default set of group policies. However, it is not possible to add ADMX files to the sysvol folder.

Also, there is a default policy for account lockouts applied to all Azure AD DS users. You can create a new policy with more restrictive settings, but you can't change the default policy.

Limited Redundancy

A best practice with Windows AD was to put a DC as close to users as possible. It is common to do this by deploying Domain Controllers in branch locations to process logins locally and provide login services if WAN connectivity failed. An Azure AD DS instance is limited to two domain controllers in a single region. If that region goes down or the network connectivity is disrupted, login processing would become unavailable.

Azure AD DS has a Different DNS Name

Azure AD DS requires a publicly routable domain when deployed. The domina name is a different domain from the on-premises domain and the Azure AD domain. User replicated from the source Azure AD domain can log in with their Azure AD UPN, but any users provisioned from Azure AD DS will use the Azure AD DS domain suffix. This situation is manageable but confusing for users and support.

No Forest Trusts

There are two types of Azure AD DS forests. A User forest synchronizes all objects from Azure AD. Included are users accounts sourced from Windows AD, providing Azure AD Connect Sync is in place between Windows AD and Azure AD. This forest type does not support forest trusts. Forest trusts are common for larger organizations, or during merger and acquisition activities that require sharing resources across disjoined forests.

Technically, the second Azure AD DS forest type, a resource forest, does support trusts relationships. It does not, however, synchronize objects from Azure AD. Instead, it's used for resources that rely on a trust relationship with a Windows AD domain for access.

Not Publicly Available

One frequent question I see is a version of "now that I have Azure AD DS, how do I join my laptop to it?" Joining a client to Azure AD DS requires a private network connection, VPN, or ExpressRoute, for the same reason joining a Windows AD domain requires one. There are significant security risks to exposing Active Directory Domain Services to the internet.

Prerequisites :

An active Azure subscription.

An Azure Active Directory tenant associated with your subscription, either synchronized with an on-premises directory or a cloud-only directory.

You need *global administrator* privileges in your Azure AD tenant to enable Azure AD DS.

You need *Contributor* privileges in your Azure subscription to create the required Azure AD DS resources.

Create an instance

To launch the **Enable Azure AD Domain Services** wizard, complete the following steps:

1. On the Azure portal menu or from the **Home** page, select **Create a resource**.
2. Enter *Domain Services* into the search bar, then choose *Azure AD Domain Services* from the search suggestions.
3. On the Azure AD Domain Services page, select **Create**. The **Enable Azure AD Domain Services** wizard is launched.
4. Select the Azure **Subscription** in which you would like to create the managed domain.
5. Select the **Resource group** to which the managed domain should belong. Choose to **Create new** or select an existing resource group.

Create Azure AD Domain Services

Basics * | Networking * | Administration | Synchronization | Review + create

Azure AD Domain Services provides managed domain services such as domain join, group policy, LDAP, and Kerberos/NTLM authentication. You can use Azure AD Domain Services without needing to manage, patch, or service domain controllers in the cloud. For ease and simplicity, defaults have been specified to provide a one-click deployment. Learn more

Project details

When choosing the basic information needed for Azure AD Domain Services, keep in mind that the subscription, resource group, DNS domain name, and location cannot be changed after creation.

Subscription * : Azure

Resource group * : (New) myResourceGroup

Create new

Help me choose the subscription and resource group

DNS domain name * : aadds.contoso.com

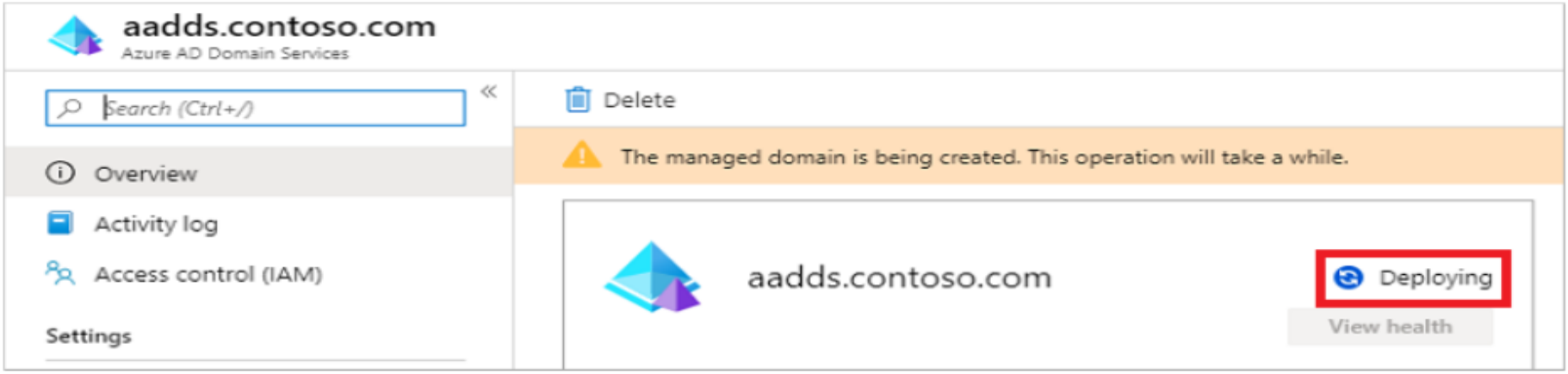
Help me choose the DNS name

Location * : (US) West US

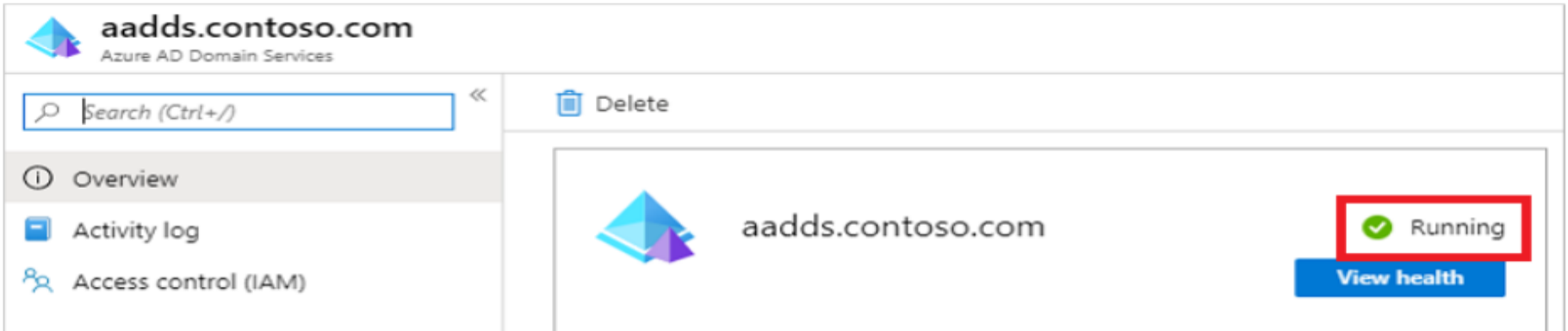
Forest type * : User

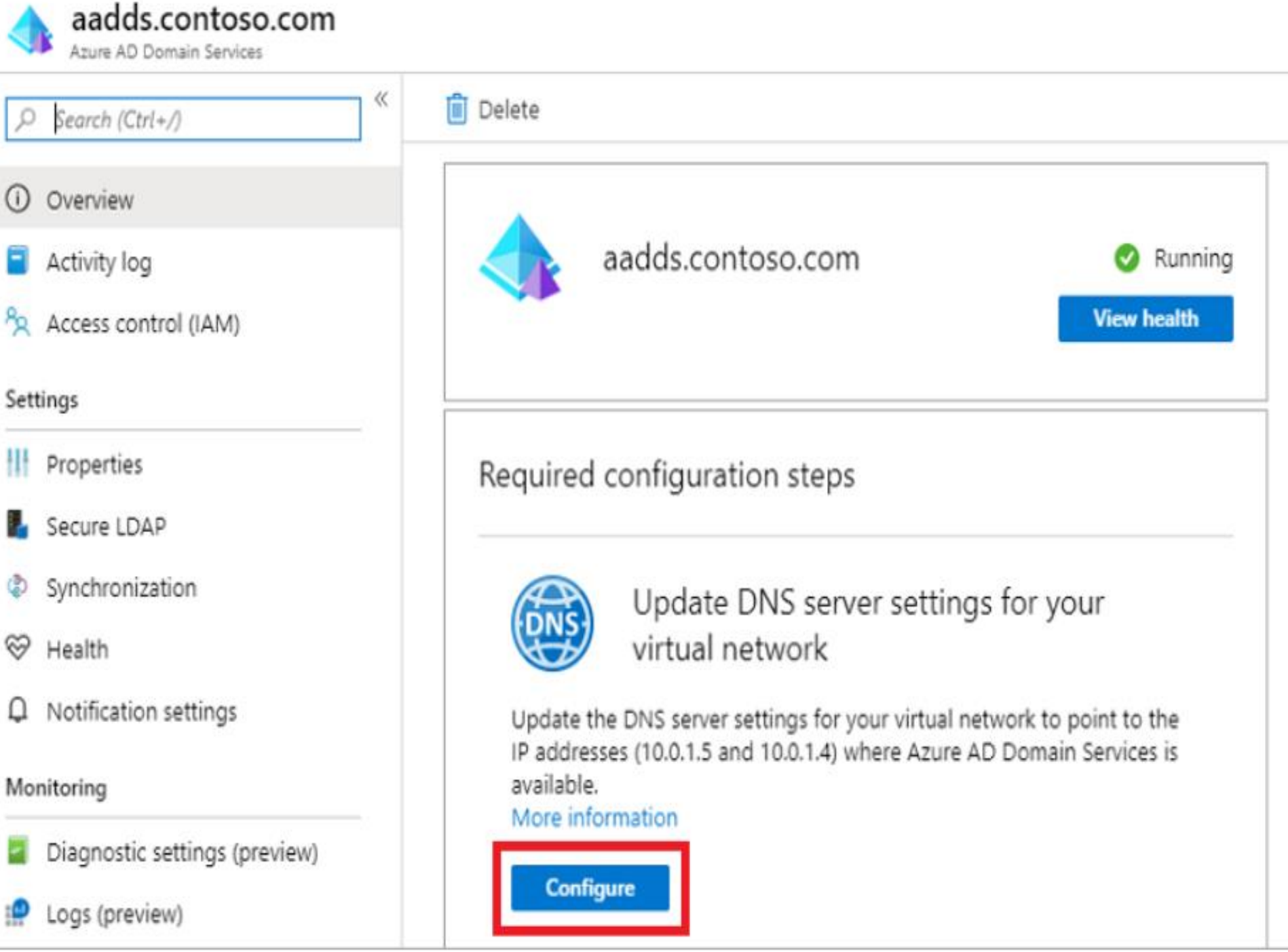
Help me choose a forest type

4. Select your resource group, such as *myResourceGroup*, then choose your Azure AD DS instance from the list of Azure resources, such as *aadds.contoso.com*. The **Overview** tab shows that the managed domain is currently *Deploying*. You can't configure the managed domain until it's fully provisioned.



5. When the managed domain is fully provisioned, the **Overview** tab shows the domain status as *Running*.




aadds.contoso.com
Azure AD Domain Services
Search (Ctrl+/)
Delete
Overview
Activity log
Access control (IAM)
Settings
Properties
Secure LDAP
Synchronization
Health
Notification settings
Monitoring
Diagnostic settings (preview)
Logs (preview)
aadds.contoso.com
Running
View health
Required configuration steps
DNS
Update DNS server settings for your virtual network
Update the DNS server settings for your virtual network to point to the IP addresses (10.0.1.5 and 10.0.1.4) where Azure AD Domain Services is available.
More information
Configure

Region: South Central US

Currency: Indian Rupee (₹)

Display pricing by: Hour

Pricing details

Azure Active Directory Domain Services usage is charged per hour, based on the total number of objects in your Active Directory Domain Services managed domain, including users, groups and domain-joined computers. Azure Active Directory is available in User Forest and Resource Forest Enterprise tiers (currently in preview). While in preview, Resource Forest Enterprise pricing includes a preview pricing discount. Prices listed in the table below include the preview discount.

TIER/NUMBER OF DIRECTORY OBJECTS [1]	PRICE
User Forest with less than 25,000	₹9.92/hour
User Forest with 25,001 to 1,00,000	₹26.44/hour
User Forest with 1,00,001 to 5,00,000	₹105.76/hour
User Forest with greater than 5,00,000	Contact us
Resource Forest Enterprise - PREVIEW [2]	₹26.44/hour

GPO
=====

https://docs.microsoft.com/en-us/azure/active-directory-domain-services/manage-group-policy

https://learn.microsoft.com/en-us/azure/active-directory-domain-services/join-windows-vm