TD SYNNEX

AZURE ACTIVE DIRECTORY DOMAIN SERVICES

A Click-to-Run™ solution for

Managed Domain Services

Table of Contents

TD SYNNEX

Azure Active Directory Domain Services Guide

This guide was designed to provide channel partners with the deployment steps required to successfully deploy Azure Active Directory Domain Services (AADDS).

TD SYNNEX’s Azure Active Directory Domain Services (Azure ADDS) is a managed service that provides domain-related services such as user authentication, identity management, device management and group policy configuration.

This Click-to-Run solution delivers a simplified deployment of managed domain services, which offers alternatives for IT administrators that need to create VPN connections back to an on-premises AD DS environment or run and manage VMs in Azure to provide identity services. It reduces the complexity to create an integrated identity solution for both hybrid and cloud-only environments. It simplifies the ability to manage cloud identities – and therefore, is an important first step to operate in the cloud.

Infrastructure Requirements

This solution can be deployed using one of the following two approaches:

New Virtual Network

This option creates a new virtual network and subnet. There are no prerequisites for this option as all solution components are created during the deployment.

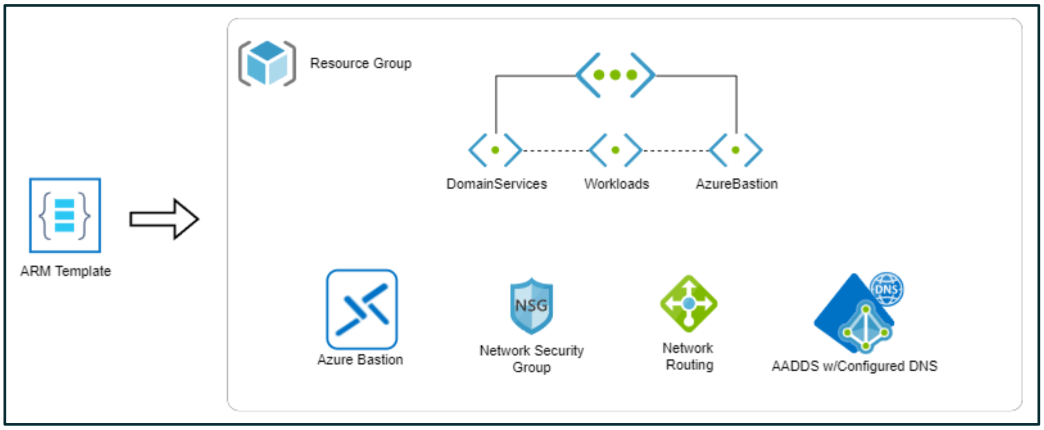


Figure 1. New virtual network architecture

Existing Virtual Network

You have the option to use an existing virtual network (VNet) and subnet, which will satisfy the networking requirements for this solution. Existing VNets and subnets will be presented in the solution user interface for you to select. When this option is selected, the Azure AD Domain Services managed domain will be created in a new resource group, alongside the required networking resources. Azure Bastion is not available as an option when selecting an existing virtual network.

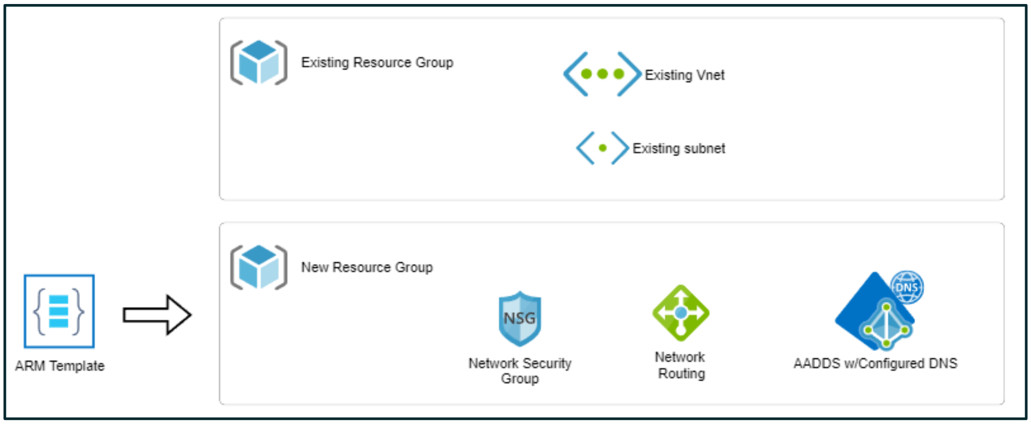


Figure 2. Existing VNet and Subnet architecture

Deployment - Step-by-Step Guide

Technical Requirements - Customer Inputs

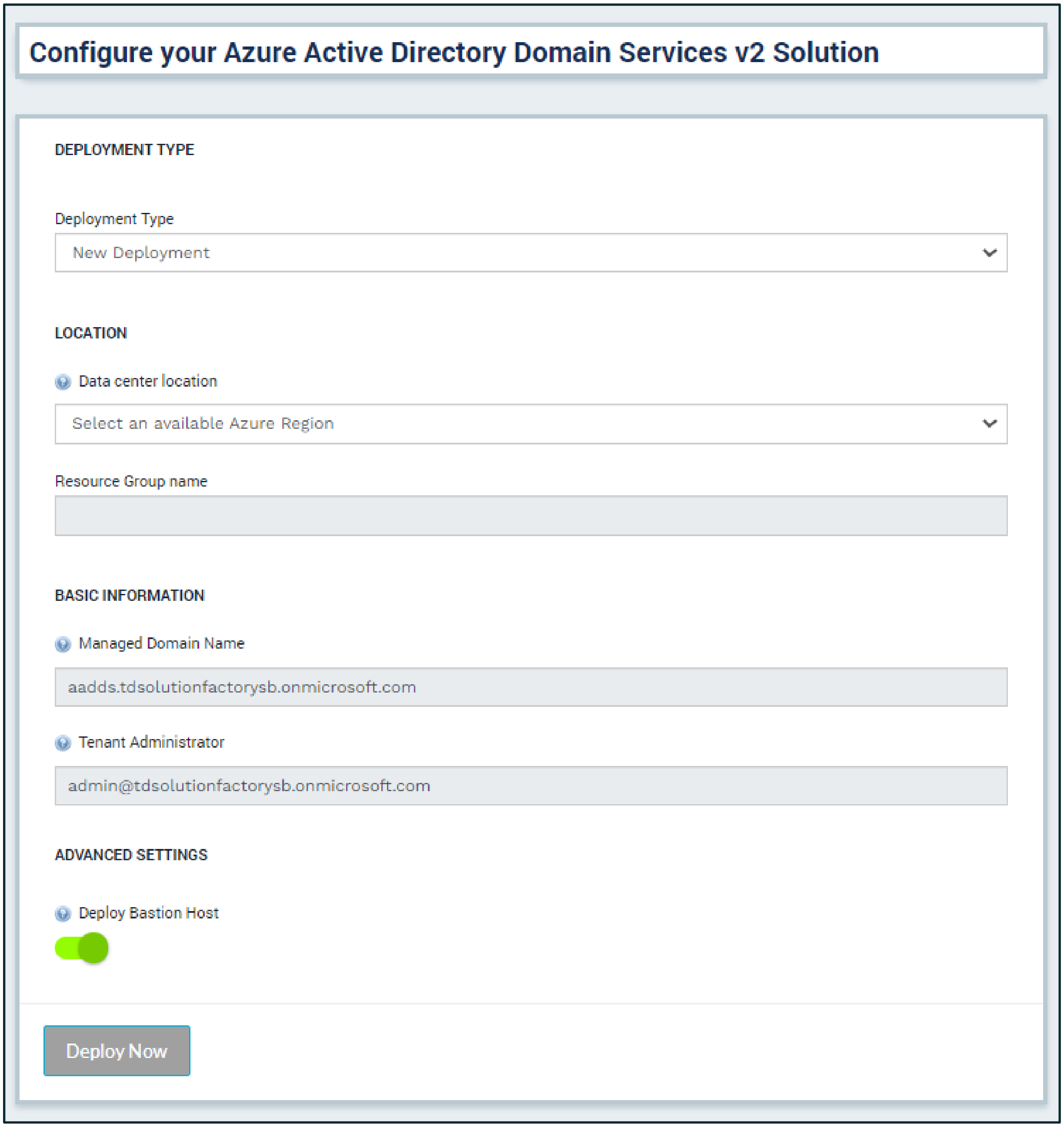
The following inputs will be required during the solution deployment:

- Resource Group Name - The name of the resource group to be used for deploying assets
- Tenant Administrator Name - The Azure AD user who will have administrative privileges on the AADDS resource.
- Managed Domain Name - The name of your AADDS Instance.
- Bastion Host Deployment - Possibility to add a bastion host and the appropriate subnet to the AADDS deployment.
- Existing Virtual Network vs. New Virtual Network - A decision should be made whether to use an existing virtual network, or whether a new virtual network should be created.

After the purchase of Azure Active Directory Domain Services v.2 solution in the StreamOne Marketplace, follow prompts to configure the solution. The following guide describes the solution configuration form and guides you through the deployment process.

Solution Deployment Instructions

On initial load, the solution form appears below. This section will provide instructions on completing this form.



Configure your Azure Active Directory Domain Services v2 Solution

DEPLOYMENT TYPE

Deployment Type: New Deployment

LOCATION

Data center location: Select an available Azure Region

Resource Group name:

BASIC INFORMATION

Managed Domain Name: aadds.tdsolutionfactorysb.onmicrosoft.com

Tenant Administrator: admin@tdsolutionfactorysb.onmicrosoft.com

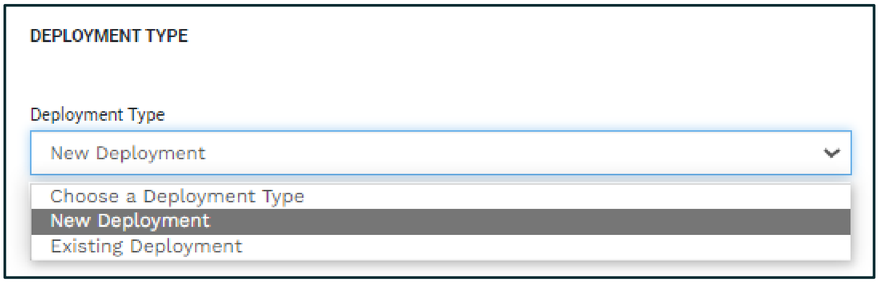
ADVANCED SETTINGS

Deploy Bastion Host: ●

Figure 3. Solution deployment form

Step 1. Select deployment type

Select the deployment type to perform, as it relates to virtual networks. Either a new deployment or existing deployment must be selected.



DEPLOYMENT TYPE

Deployment Type

New Deployment

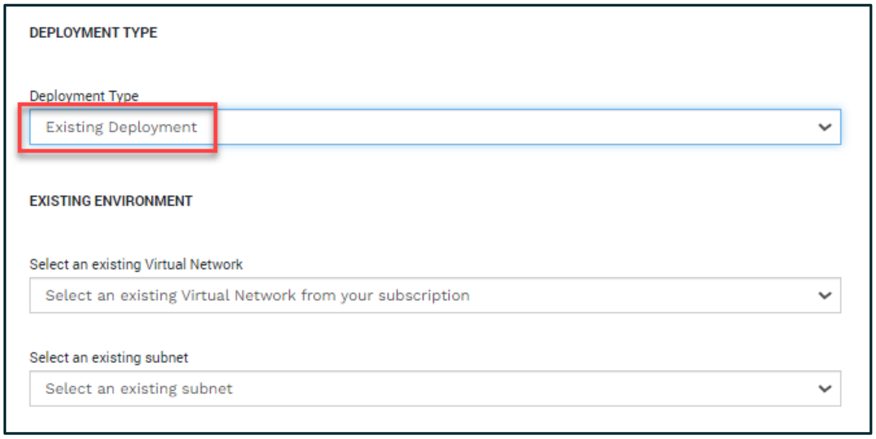
New Deployment: Creates a new virtual network and multiple subnets into which the solution is deployed. Select this option when you desire a new virtual network. Refer back to Figure 1 for a model of the resulting deployment.

Existing Deployment: Deploys the solution into an existing virtual network. If this option is selected, virtual network and subnet data will be loaded into the form, and you must select one of each. See Figure 2 for a diagram of the "existing virtual network" deployment.

If you selected "New Deployment", skip to Step 3. If you selected "Existing Deployment", proceed to the next step (Step 2.)

Step 2. Select Virtual Network and subnet

Selecting "Existing Deployment" will generate two new form fields that prompt you to select a Virtual Network and a subnet.



DEPLOYMENT TYPE

Deployment Type

Existing Deployment

EXISTING ENVIRONMENT

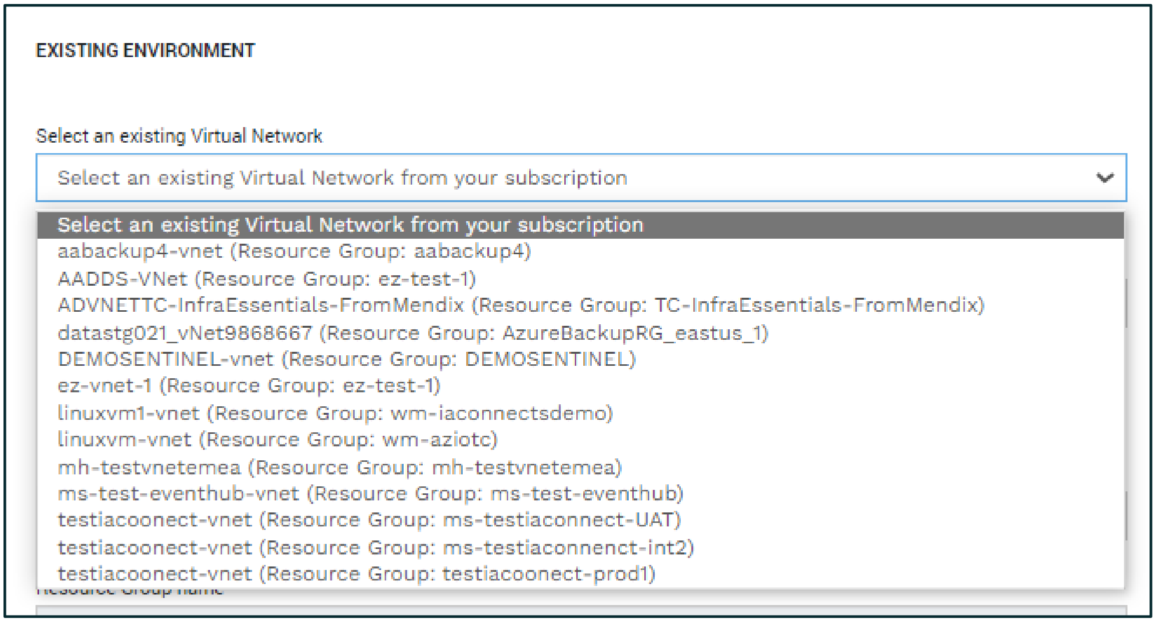
Select an existing Virtual Network

Select an existing Virtual Network from your subscription

Select an existing subnet

Select an existing subnet

Selecting the dropdown titled "Select an existing Virtual Network" will display all of the available Virtual Networks in the Azure subscription.



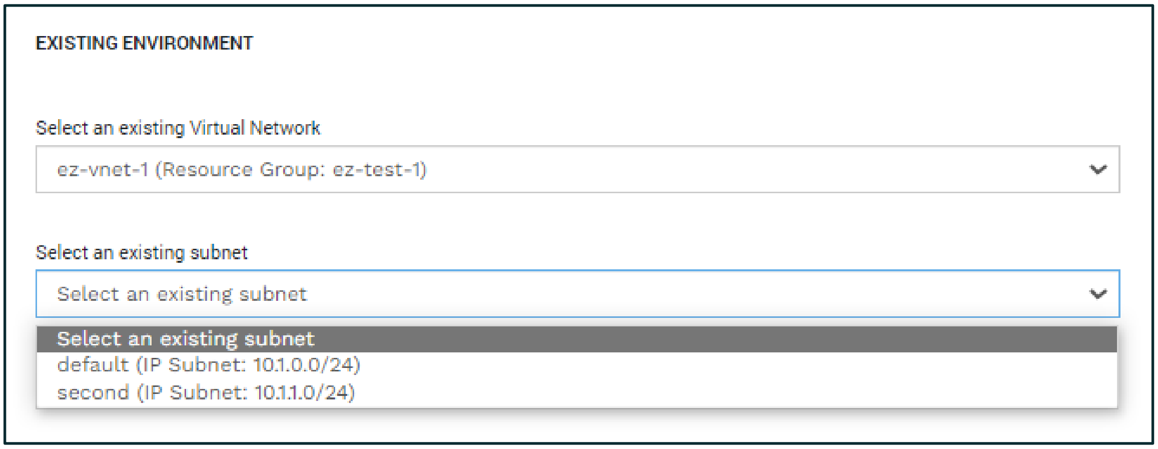
EXISTING ENVIRONMENT

Select an existing Virtual Network

Select an existing Virtual Network from your subscription

Select an existing Virtual Network from your subscription
aabackup4-vnet (Resource Group: aabackup4)
AADDS-VNet (Resource Group: ez-test-1)
ADVNETTC-InfraEssentials-FromMendix (Resource Group: TC-InfraEssentials-FromMendix)
datastg021_vNet9868667 (Resource Group: AzureBackupRG_eastus_1)
DEMOSENTINEL-vnet (Resource Group: DEMOSENTINEL)
ez-vnet-1 (Resource Group: ez-test-1)
linuxvm1-vnet (Resource Group: wm-iaconnectsdemo)
linuxvm-vnet (Resource Group: wm-aziotc)
mh-testvnetemea (Resource Group: mh-testvnetemea)
ms-test-eventhub-vnet (Resource Group: ms-test-eventhub)
testiacoonect-vnet (Resource Group: ms-testiaconnect-UAT)
testiacoonect-vnet (Resource Group: ms-testiaconnenct-int2)
testiacoonect-vnet (Resource Group: testiacoonect-prod1)

Select the appropriate virtual network. In the example below, we've select "ez-vnet-1" as the target Virtual Network. Once we've made this selection, the "Select an existing subnet" dropdown will be populated with a list of the subnets contained within the selected virtual network. In our example, there are two subnets (one called "default" and one called "second").



EXISTING ENVIRONMENT

Select an existing Virtual Network

ez-vnet-1 (Resource Group: ez-test-1)

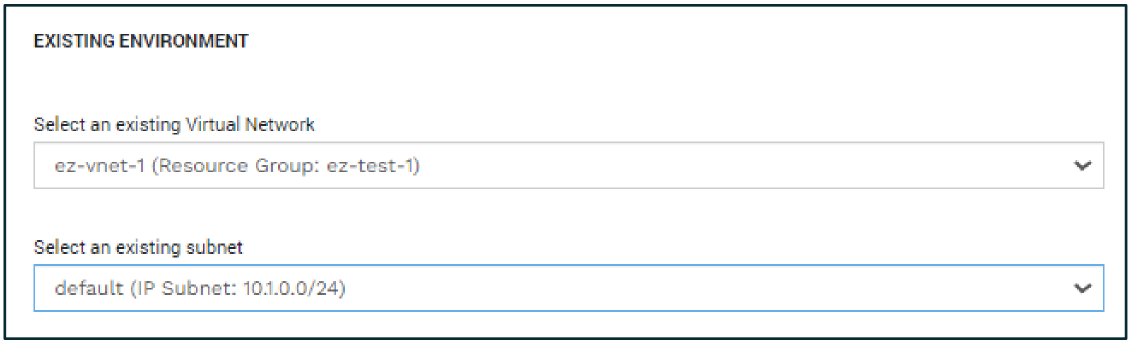
Select an existing subnet

Select an existing subnet

Select an existing subnet
default (IP Subnet: 10.1.0.0/24)
second (IP Subnet: 10.1.1.0/24)

Select the appropriate subnet. In our case we will select the subnet called "default".

We've now completed the "Existing Environment" section. Proceed to Step 3.



EXISTING ENVIRONMENT

Select an existing Virtual Network

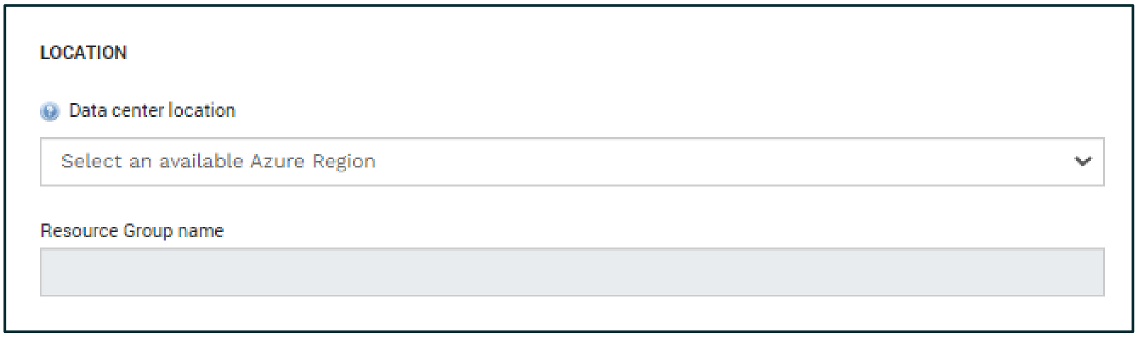
ez-vnet-1 (Resource Group: ez-test-1)

Select an existing subnet

default (IP Subnet: 10.1.0.0/24)

Step 3. Specify Location and Resource Group Name

You will now select the Azure Region and provide a Resource Group name in which to deploy the solution artifacts.



LOCATION

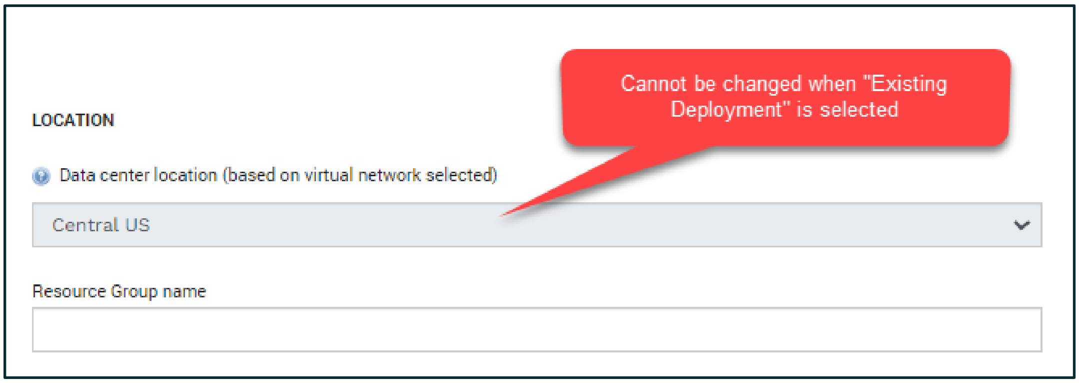
Data center location

Select an available Azure Region

Resource Group name

⚠ Attention

If you select “Existing Deployment” for Deployment Type in Step 1, you will not be able to change the Data center location. The location will be pre-selected based on the location of the Virtual Network that was selected in Step 2 (example shown below):



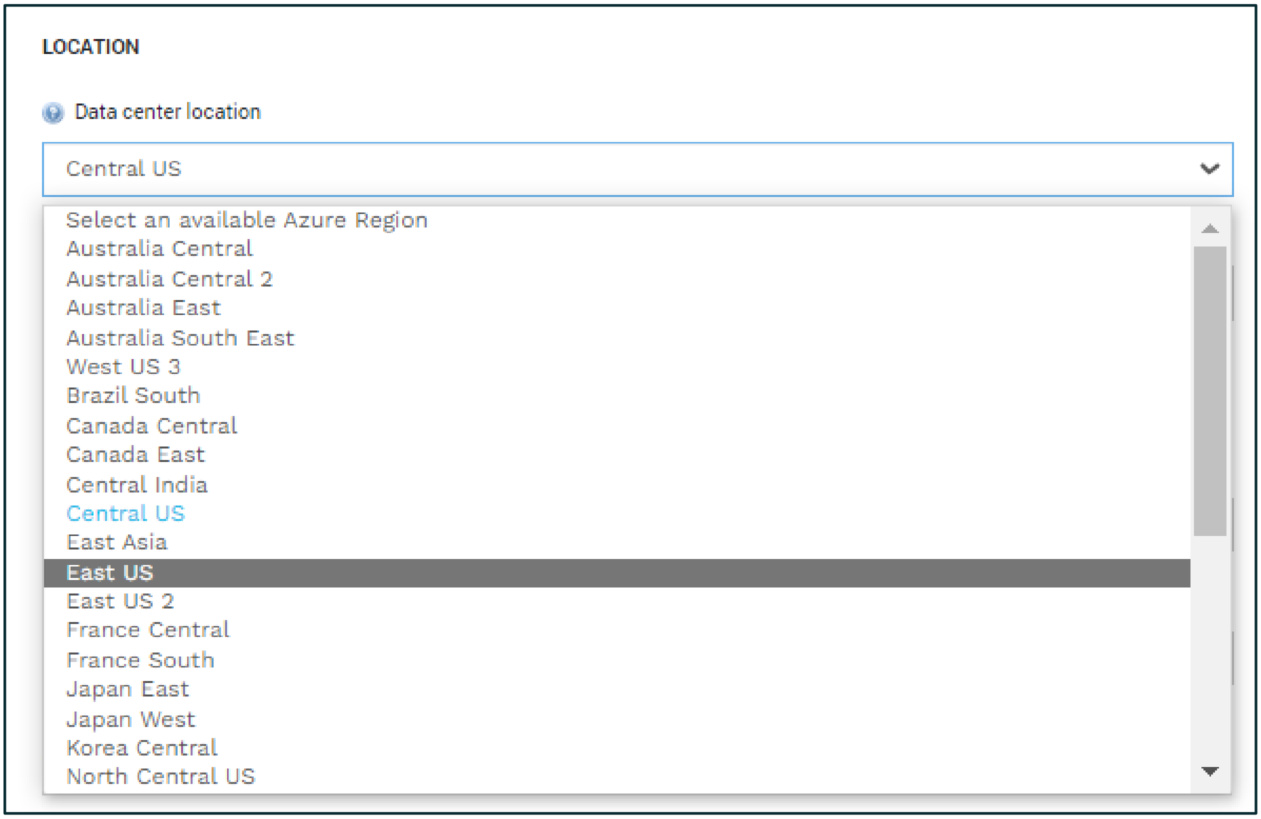
LOCATION

Data center location (based on virtual network selected)

Central US

Resource Group name

To select a region, select the “Data center location” dropdown. You will see a list of Azure regions. Select the desired region:



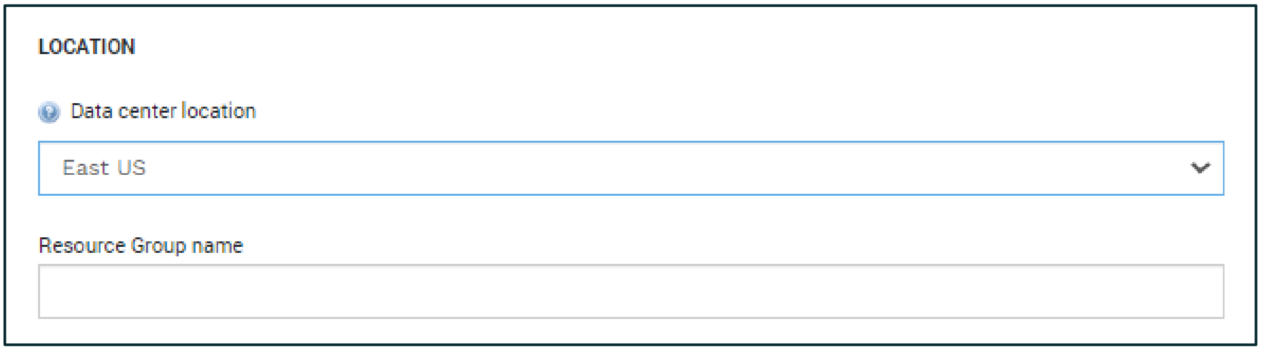
LOCATION

Data center location

Central US

- Select an available Azure Region
- Australia Central
- Australia Central 2
- Australia East
- Australia South East
- West US 3
- Brazil South
- Canada Central
- Canada East
- Central India
- Central US
- East Asia
- East US
- East US 2
- France Central
- France South
- Japan East
- Japan West
- Korea Central
- North Central US

In our example, we’ve selected the “East US” region:



LOCATION

Data center location

East US

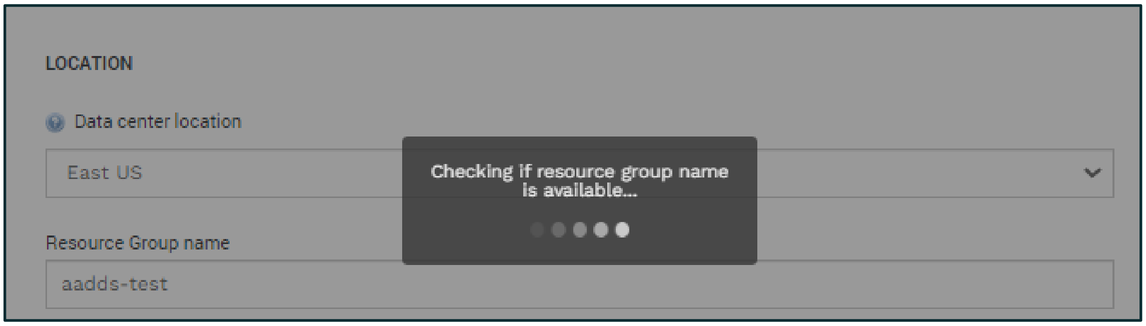
Resource Group name

Next, input a name into the Resource Group name field. The field is required, and you must input a valid name*.

** Resource group names only allow alphanumeric characters, periods, underscores, hyphens and parentheses. Resource group names cannot end with a period. The length cannot be over 90 characters.*

After providing a name in the field, the system will verify that the name is valid and available. It must not match the name of a resource group already contained within your subscription.

In the image below, we've input "adds-test" into the Resource Group name field and the system is now validating our input.



LOCATION

Data center location

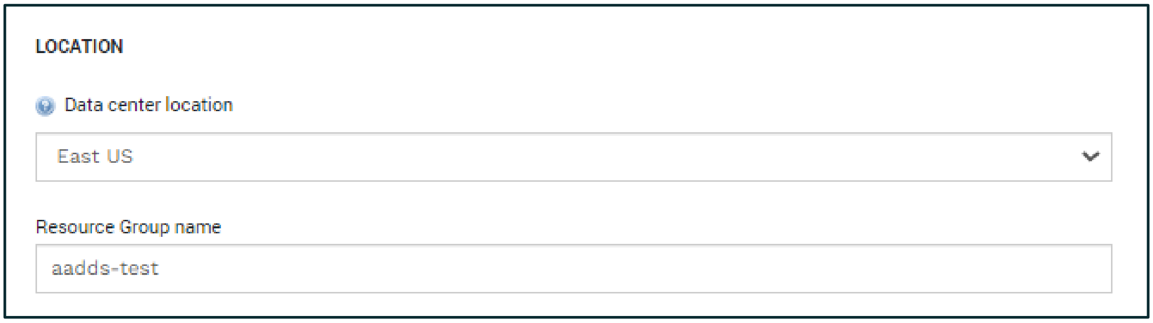
East US

Resource Group name

aadds-test

Checking if resource group name is available...

If the provided name is of a valid format and is not already used, control will be returned to the user and no errors will display. If no errors display, proceed to Step 4.



LOCATION

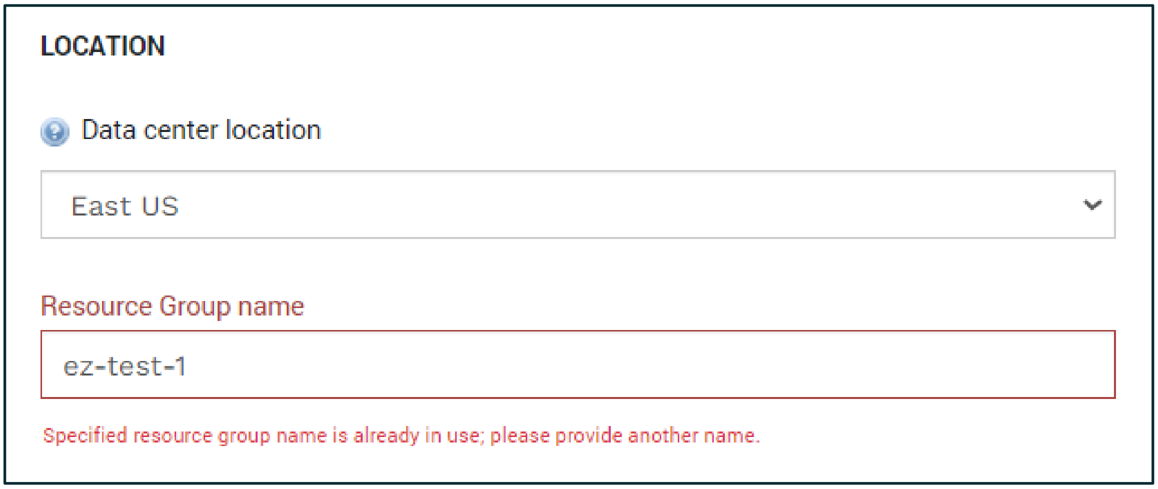
Data center location

East US

Resource Group name

aadds-test

If an issue was found with the provided name, an error will display:



LOCATION

Data center location

East US

Resource Group name

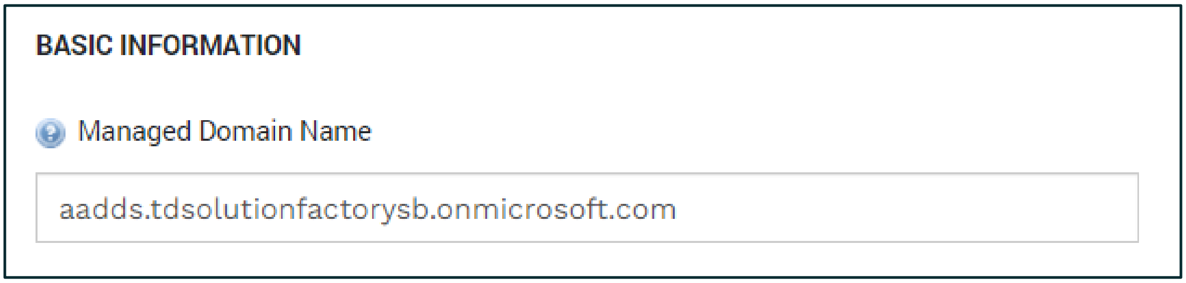
ez-test-1

Specified resource group name is already in use; please provide another name.

If an error is detected, please resolve the indicated error and proceed to Step 4.

Step 4. Define the Managed Domain Name

The next form field, “Managed Domain Name” requests configuration information related to your Azure Active Directory Domain Service. You are prompted to input a domain name that will uniquely represent your managed service.



BASIC INFORMATION

Managed Domain Name

aadds.tdsolutionfactorysb.onmicrosoft.com

This field is prefilled with the customer tenant domain, prefixed with "aadds.". In our example, the tenant domain name is "tdsolutionfactorysb.onmicrosoft.com". Thus, the generated domain name is "aadds.tdsolutionfactorysb.onmicrosoft.com". This is a suggested domain name that will uniquely identify the managed domain service that will be created during the deployment. You can change this value if desired.

When you specify your own Managed Domain Name, you must specify a DNS name. The following are some considerations when you choose this DNS name:

- Built-in domain name: By default, the built-in domain name of the directory is used (a .onmicrosoft.com suffix). If you wish to enable secure LDAP access to the managed domain over the internet, you can't create a digital certificate to secure the connection with this default domain. Microsoft owns the .onmicrosoft.com domain, so a Certificate Authority (CA) won't issue a certificate.

- Custom domain names: The most common approach is to specify a custom domain name, typically one that you already own and is routable. When you use a routable, custom domain, traffic can correctly flow as needed to support your applications.

- Non-routable domain suffixes: We recommend that you avoid a non-routable domain name suffix, such as contoso.local. The .local suffix isn't routable and can cause issues with DNS resolution.

Tip

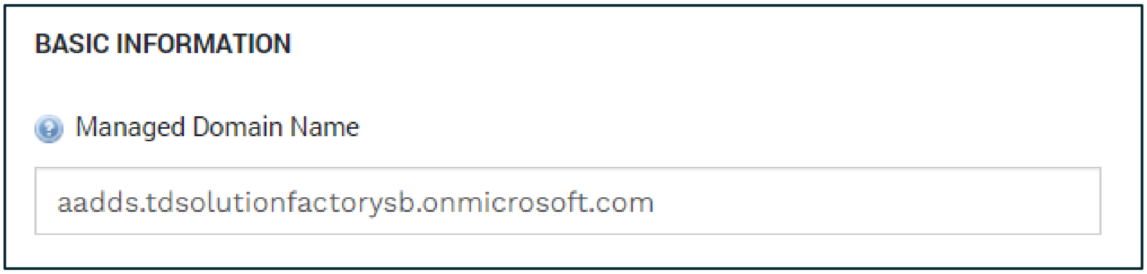
If you create a custom domain name, take care with existing DNS namespaces. It’s recommended to use a domain separate from any existing Azure or on-premises DNS name space.

For example, if you have an existing DNS name space of contoso.com, create a managed domain with the custom domain name of aaddscontoso.com. If you need to use secure LDAP, you must register and own this custom domain name to generate the required certificates.

The following DNS name restrictions also apply:

- **Domain prefix restrictions:** You can't create a managed domain with a prefix longer than 15 characters. The prefix of your specified domain name (such as aaddscontoso in the aaddscontoso.com domain name) must contain 15 or fewer characters.
- **Network name conflicts:** The DNS domain name for your managed domain shouldn't already exist in the virtual network. Specifically, check for the following scenarios that would lead to a name conflict:
  - If you already have an Active Directory domain with the same DNS domain name on the Azure virtual network.
  - If the virtual network where you plan to enable the managed domain has a VPN connection with your on-premises network. In this scenario, ensure you don’t have a domain with the same DNS domain name on your on-premises network.
  - If you have an existing Azure cloud service with that name on the Azure virtual network.

For this guide, we will leave the value of the Managed Domain Name that was pre-filled.



BASIC INFORMATION

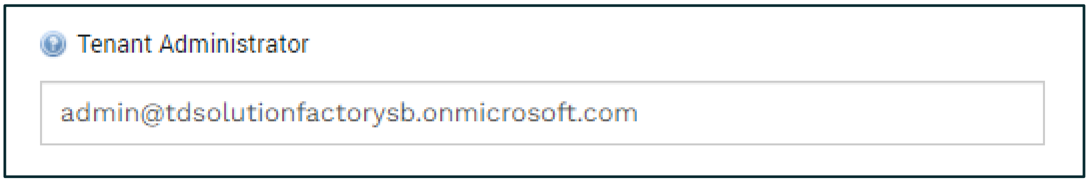
Managed Domain Name

aadds.tdsolutionfactorysb.onmicrosoft.com

Once you’ve completed this field, proceed to Step 5.

Step 5. Define the Tenant Administrator

Input a valid Azure Active Directory account. This account will be assigned administrative privileges for the new Azure AD DS domain. Note: The provided user must already exist in the Azure Active Directory within the customer’s Azure subscription.



Tenant Administrator

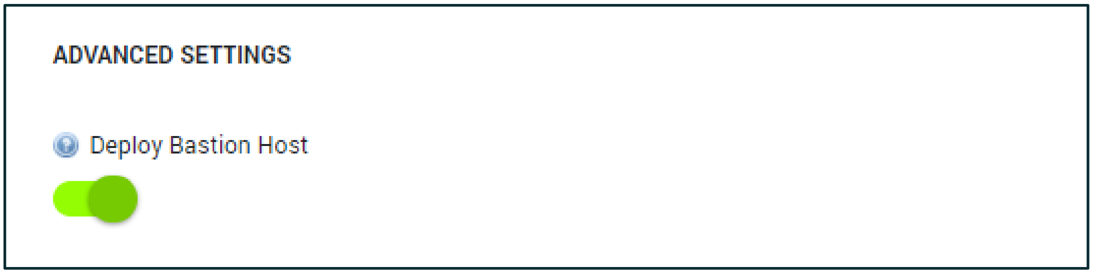
admin@tdsolutionfactorysb.onmicrosoft.com

The specified user will be added to the “AAD DC Administrators” group. This group is used for management of the Azure AD DS domain. Members of this group are granted administrative permissions on virtual machines (VMs) that are domain-joined to the managed domain. On domain-joined VMs, this group is added to the local administrators group. Members of this group can also use Remote Desktop to connect remotely to domain-joined VMs.

Step 6. Bastion Host configuration (New Deployment type only)

ⓘ Note

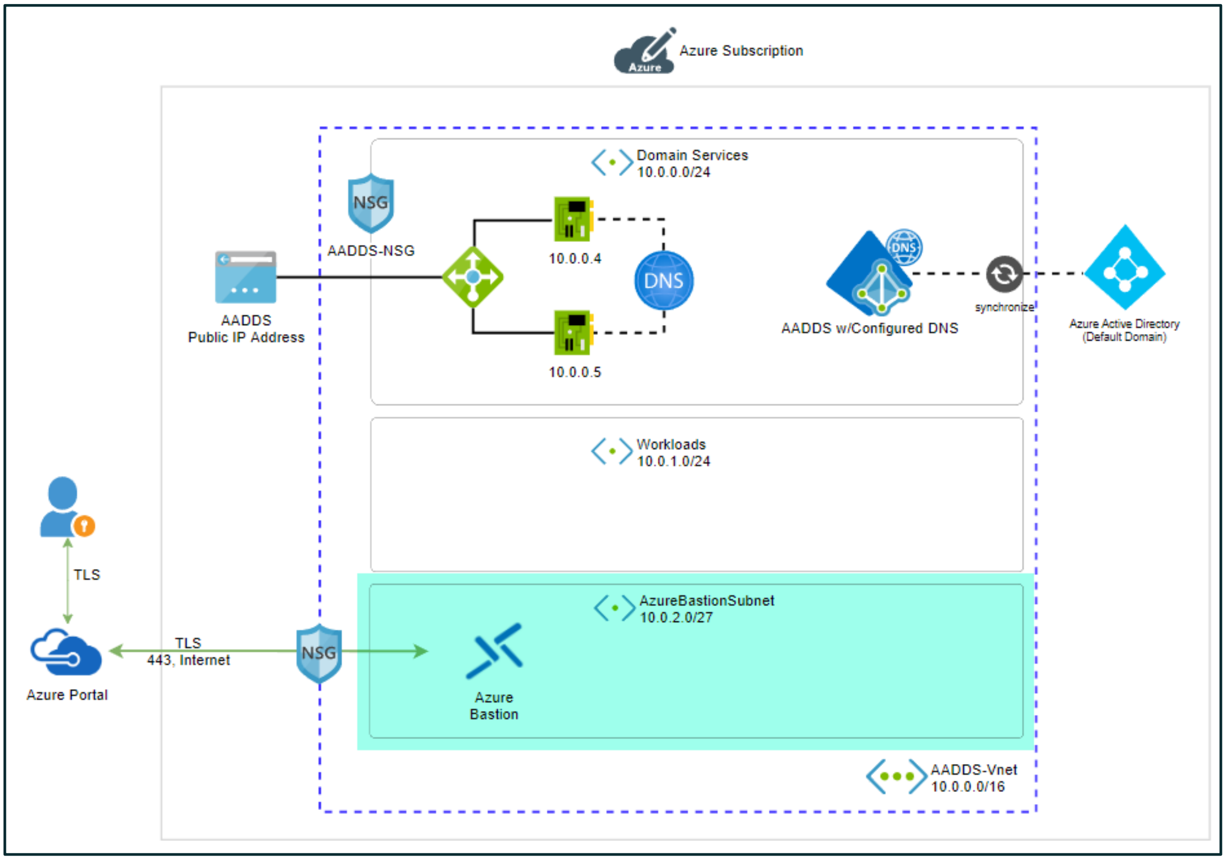
The Bastion Host option is only available when "New Deployment" is selected as the Deployment Type, due to the relative simplicity of configuring Bastion in a net new virtual network.



ADVANCED SETTINGS

Deploy Bastion Host

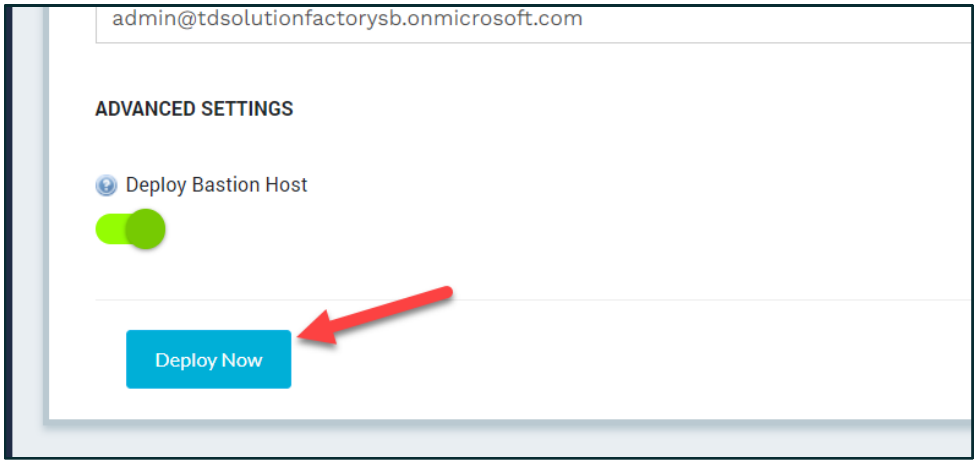
Enabling the toggle-button will include the deployment of a Bastion host within the new virtual network. The following diagram shows the deployment architecture for a “New Environment” deploy, with the Bastion infrastructure highlighted in green.



For more information on Azure Bastion, please refer to the following Microsoft documentation: [Azure Bastion]

Step 7. Launch the Deploy

Once you complete all of the form requirements, click on “Deploy New” to start the deployment of the solution.

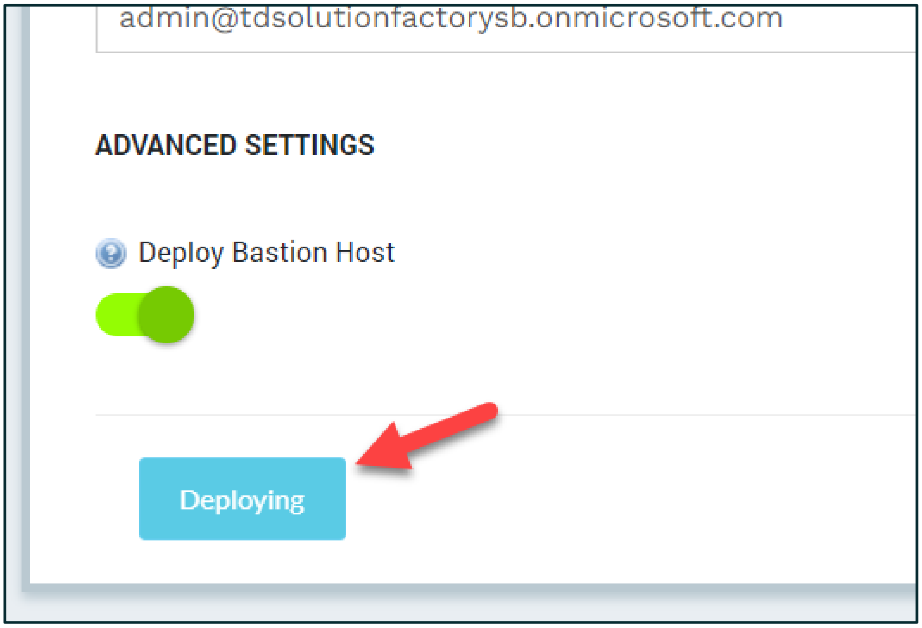


admin@tdsolutionfactorysb.onmicrosoft.com

ADVANCED SETTINGS

Deploy Bastion Host

The deployment begins. The status label on the button will change to “Deploying”. At this point, the process is working in the background and you can safely close the application as the deployment will proceed. You can also leave the application open

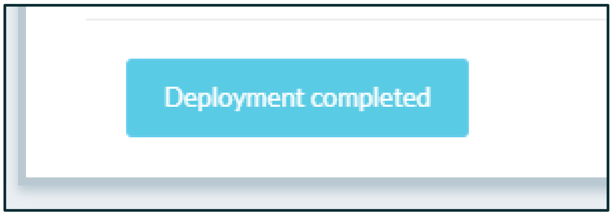


admin@tdsolutionfactorysb.onmicrosoft.com

ADVANCED SETTINGS

Deploy Bastion Host

The deployment process can take up to one hour to complete. Upon successful completion of the deployment, the status label on the button changes to “Deployment Completed”.



Post-Deployment Activities

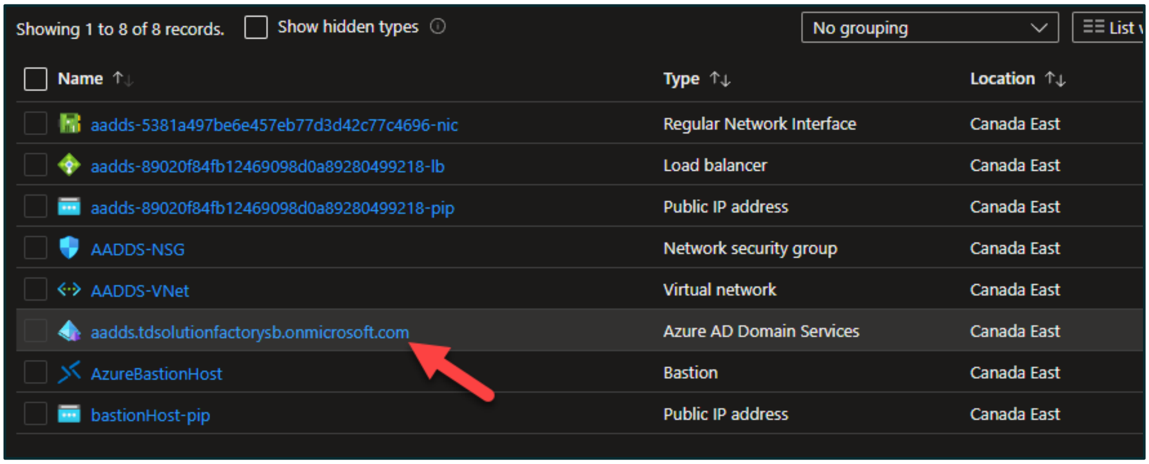
Please review the below post-deployment activities that may need to be performed prior to using the new managed domain.

Verify AADDS health status

After deploying the AADDS solution, it takes some time for the AADDS core services to become fully usable (10-15 minutes).

AADDS runs some background tasks to keep the managed domain healthy and up-to-date. After deployment, the health status will be displayed as “Deploying.” *You cannot work with your AADDS instance until the resource shows a health status of “Running”.* Follow the steps below to verify this:

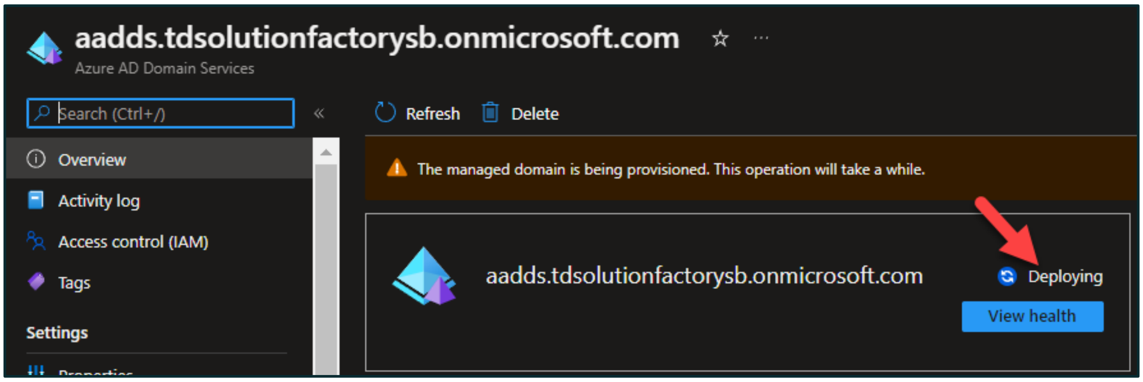
Select the AADDS resource that you have just deployed.



Showing 1 to 8 of 8 records. □ Show hidden types

Name ↑↓	Type ↑↓	Location ↑↓
aadds-5381a497be6e457eb77d3d42c77c4696-nic	Regular Network Interface	Canada East
aadds-89020f84fb12469098d0a89280499218-lb	Load balancer	Canada East
aadds-89020f84fb12469098d0a89280499218-pip	Public IP address	Canada East
AADDS-NSG	Network security group	Canada East
AADDS-VNet	Virtual network	Canada East
aadds.tdsolutionfactorysb.onmicrosoft.com	Azure AD Domain Services	Canada East
AzureBastionHost	Bastion	Canada East
bastionHost-pip	Public IP address	Canada East

Immediately after the deployment completes, the managed domain will start provisioning. While this is in process, you will see a health status of “Deploying”.



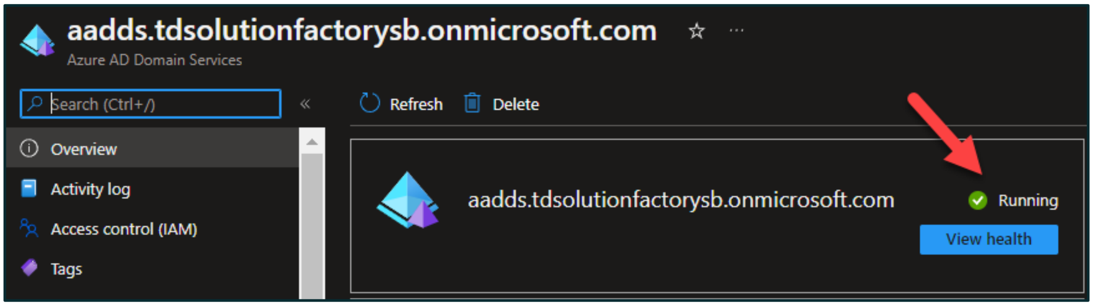
aadds.tdsolutionfactorysb.onmicrosoft.com

Azure AD Domain Services

The managed domain is being provisioned. This operation will take a while.

aadds.tdsolutionfactorysb.onmicrosoft.com — Deploying

When the process completes, the health status will change to "Running". This can take up to an hour to complete. Once this is complete, the service is ready to be used.



More information on Azure AD Domain Services Health can be found here:

https://learn.microsoft.com/en-us/entra/identity/domain-services/check-health

Enabling Password Hash Synchronization

After the AADDS Resource health is shown as "Running", you must enable password-hash synchronization before authenticating users to the managed domain. ***This is a manual step that must be performed by the partner post-deployment.***

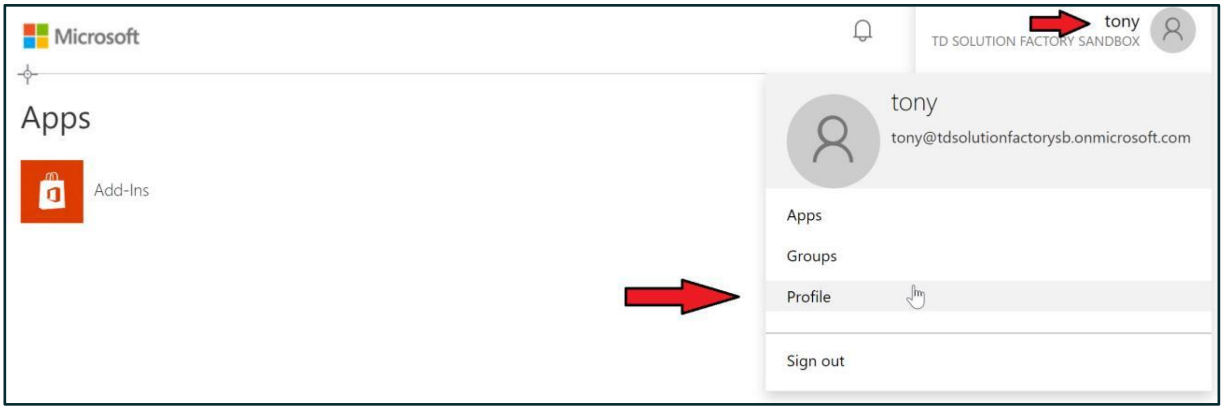
According to Microsoft documentation:

"Azure *AD DS needs password hashes in a format that's suitable for NT LAN Manager (NTLM) and Kerberos authentication. Azure AD doesn't generate or store password hashes in the format that's required for NTLM or Kerberos authentication until you enable Azure AD DS for your tenant.*"

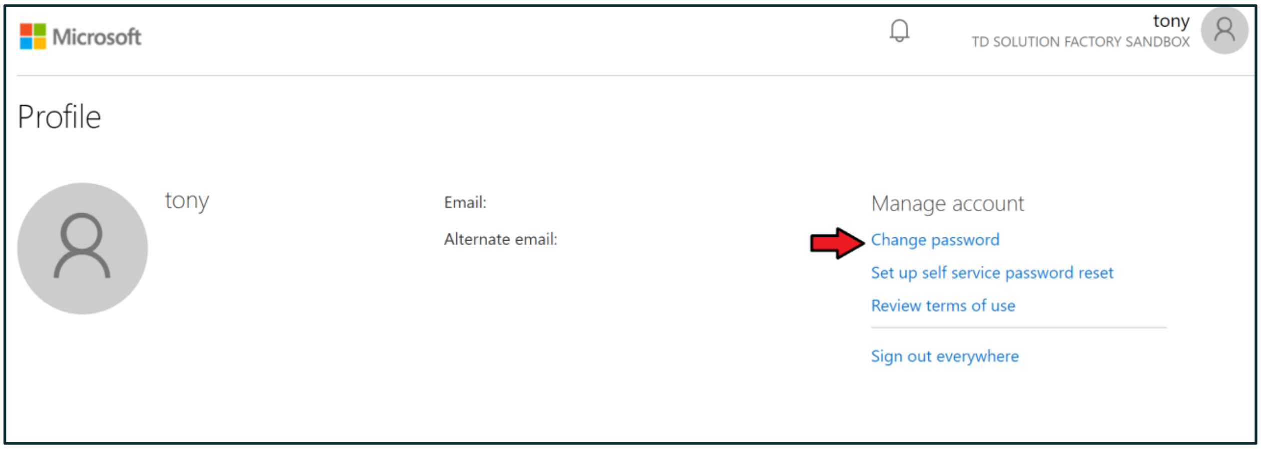
This can simply be done by resetting the password of the "Tenant Administrator" account specified when configuring your solution. Follow the steps below to reset the password:

Make sure you are signed into your tenant with the Tenant Administrator Account you specified during the deployment of the AADDS solution.

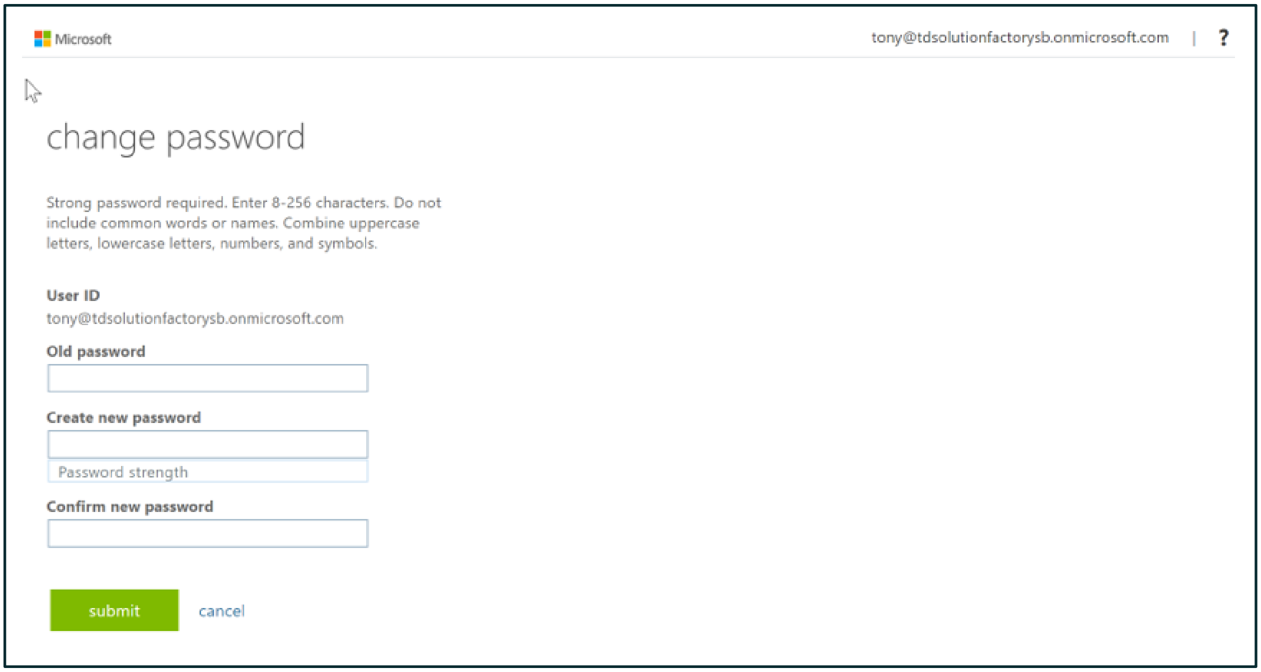
Go to the Azure AD Access Panel page at https://myapps.microsoft.com. In the top-right corner, select your name, then choose "Profile" from the drop-down menu.


Microsoft
tony
TD SOLUTION FACTORY SANDBOX
Apps
Add-Ins
tony
tony@tdsolutionfactorysb.onmicrosoft.com
Apps
Groups
Profile
Sign out

On the Profile page, select “Change password”.



On the “Change Password” page, enter your existing (old) password, then enter and confirm a new password.



change password

Strong password required. Enter 8-256 characters. Do not include common words or names. Combine uppercase letters, lowercase letters, numbers, and symbols.

User ID
tony@tdsolutionfactorysb.onmicrosoft.com

Old password

Create new password

Password strength

Confirm new password

Click on the “Submit” button. *Make sure to log out of the Azure portal and log in with your updated password.* It takes a few minutes after you've changed your password for the new password to be usable in AADDS. More information on password hash synchronization can be found here.

Configure DNS settings (*Existing Virtual Network deployment only)

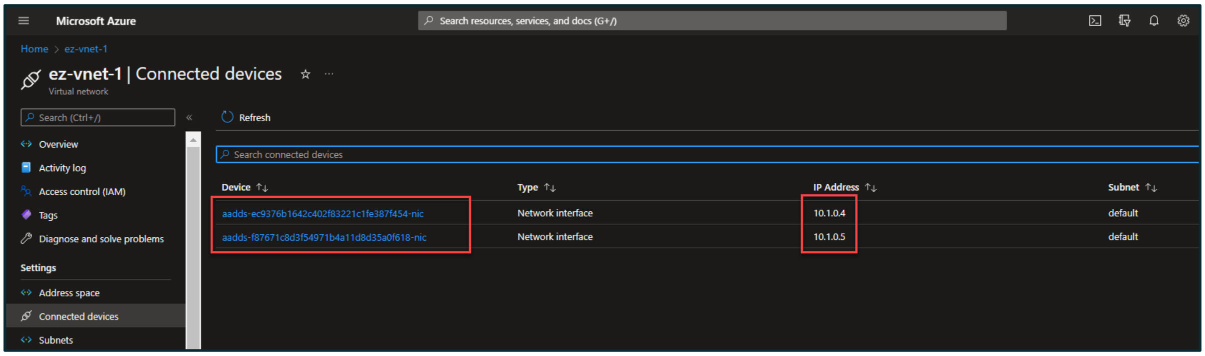
**

**Because of the limitations with Password Hash Synchronization and Health status, we are unable to include this in the AADDS deployment.*

For a deployment into an existing virtual network, there is an additional configuration step that is required. When the Azure portal shows that the managed domain has finished provisioning, you must configure your DNS so that virtual machines can find the managed domain for a domain join or authentication.

To configure the DNS, perform the following actions in Azure Portal:

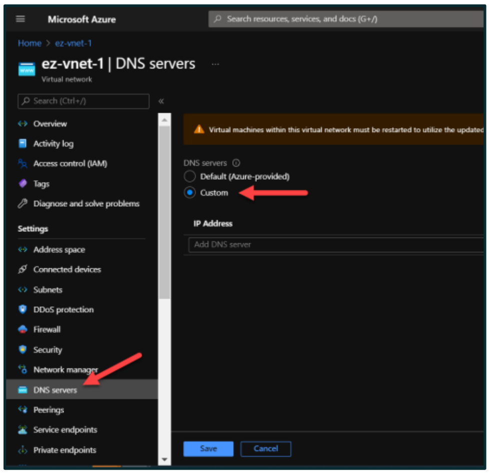
1. Navigate to the Virtual Network that was selected during the deployment. Click on “Connected Devices”In the Overview screen, find the two IP Addresses that start with a Device name of “aadds-“. Make note of the IP addresses.



ez-vnet-1 | Connected devices
Virtual network

Device	Type	IP Address	Subnet
aadds-ec9376b1642c402f83221c1fe387f454-nic	Network interface	10.1.0.4	default
aadds-f87671c8d3f54971b4a11d8d35a0f618-nic	Network interface	10.1.0.5	default

2. Select “DNS Servers” and select ”Custom”.



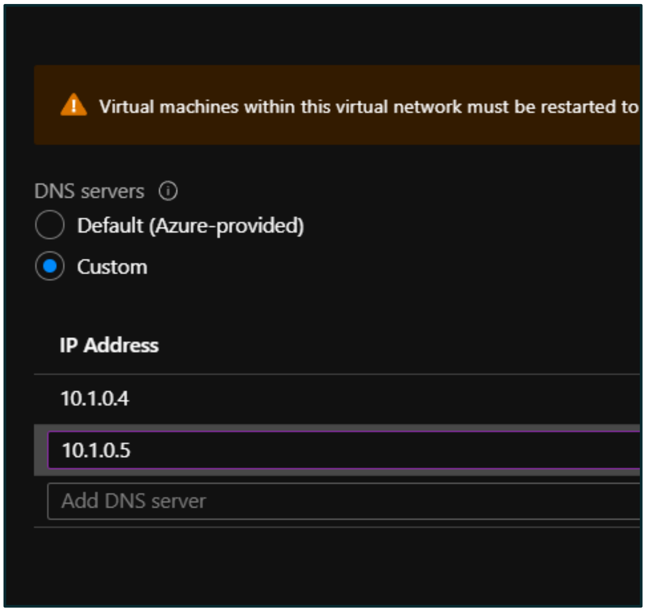
ez-vnet-1 | DNS servers
Virtual network

Virtual machines within this virtual network must be restarted to utilize the updated

DNS servers
○ Default (Azure-provided)
● Custom

IP Address
Add DNS server

3. In the IP Address section, find the field labeled “Add DNS server”. Add the two IP addresses that you noted in step 1.



Virtual machines within this virtual network must be restarted to

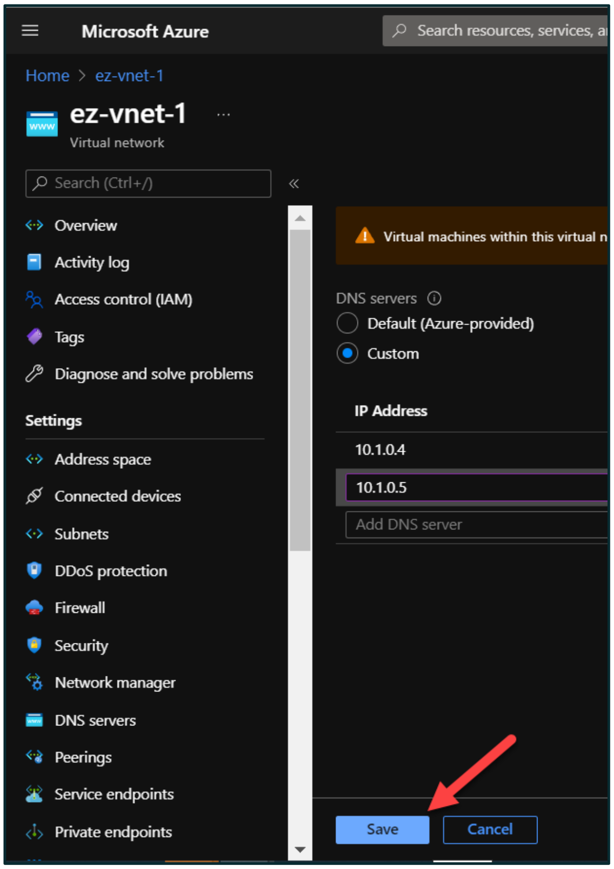
DNS servers ⓘ

○ Default (Azure-provided)

● Custom

IP Address
10.1.0.4
10.1.0.5
Add DNS server

4. Click the Save button to apply your changes.



Virtual machines within this virtual n

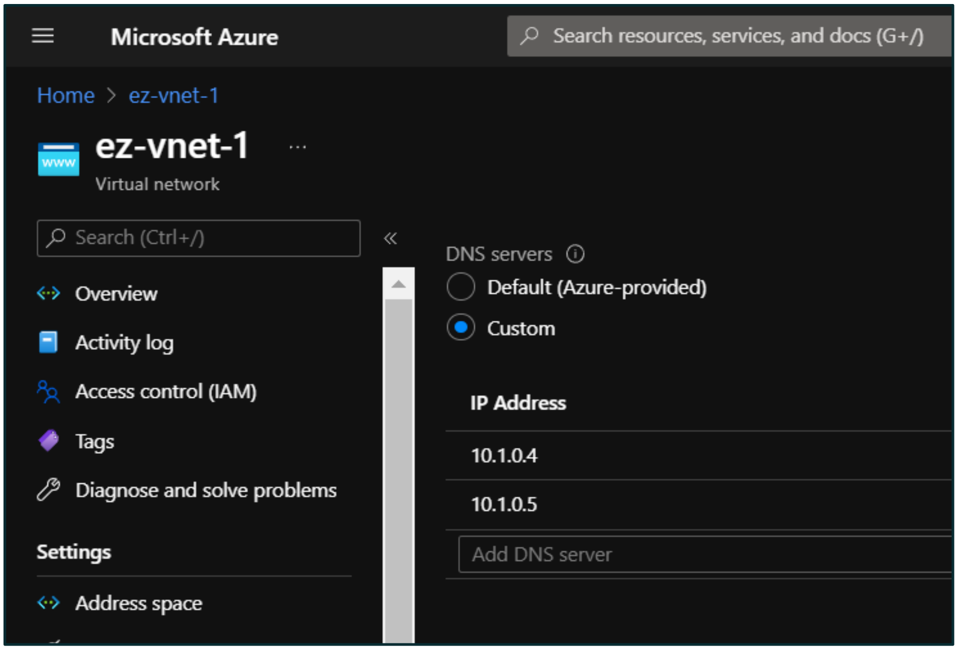
DNS servers ⓘ

○ Default (Azure-provided)

● Custom

IP Address
10.1.0.4
10.1.0.5
Add DNS server

Your DNS setting are now successfully saved:



DNS servers

○ Default (Azure-provided)

● Custom

IP Address
10.1.0.4
10.1.0.5
Add DNS server

Add a management Server

Microsoft recommends that you deploy a management server installed with Remote Server Administration tools to further manage your AADDS environment and identities. You can leverage a management server for User Management, Device Management, and Group Policy configuration. Full documentation for creating the management server can be found here.

Join a Windows Server Virtual Machine to an Azure AD Domain Services Managed 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. With an Azure AD DS managed domain, you can provide domain join features and management to virtual machines (VMs) in Azure. This tutorial shows you how to create a Windows Server VM and then join it to a managed domain.