



## **Tech Data Windows Azure Active Directory Domain Services**

Below is a list of action items as part of the deployment process and post deployment recommendations to customize the Cloud Environment.

#### Technical Requirements: Parameters & Inputs

- ☐ **Resource Group Name** – Type the name of the resource group.
- ☐ **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** – Option to add a bastion host and the appropriate subnet to the AADDs deployment.

#### Post Deployment Steps:

- ☐ Enable Password has Synchronization on Azure Active Directory Domain Services Admin (AADDs). Detailed instructions can be found on Page #4 - 5 .

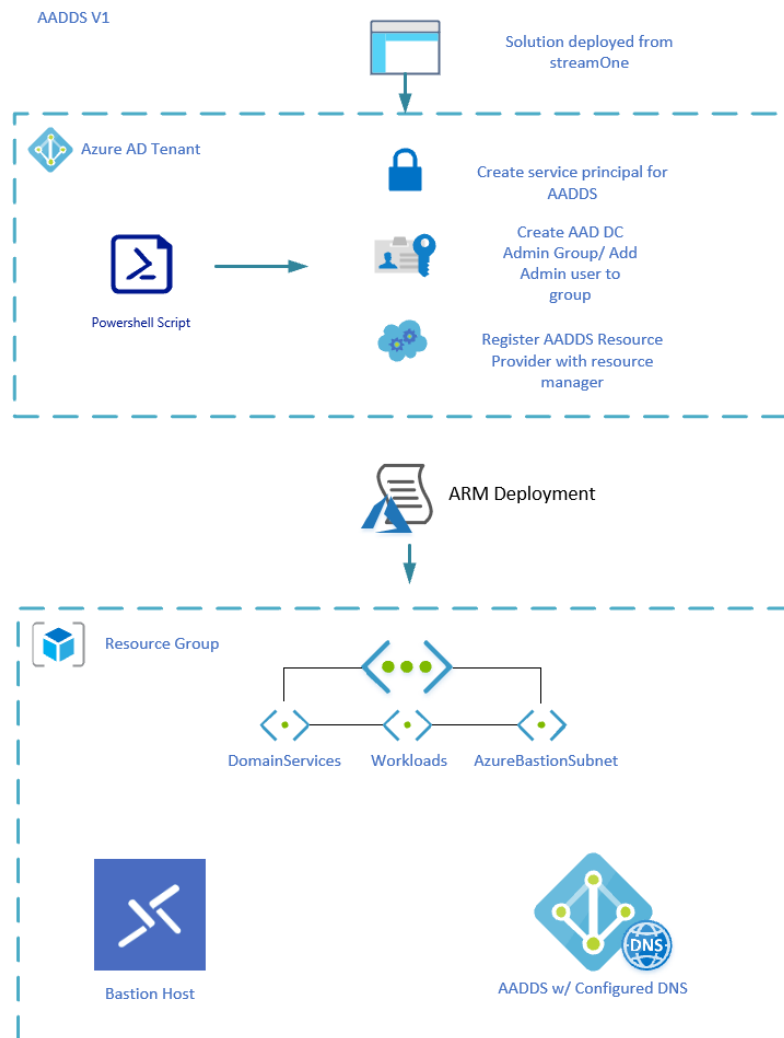
#### Solution Overview:

Azure Active Directory Domain Service is a cloud based managed domain service offered by Microsoft to facilitate many of the traditional Active Directory functions including group policy and authentication. It reduces or eliminates the need for managing, patching, and deploying domain controllers. It can integrate with your existing Azure Active Directory or existing Domain Controller in the cloud or on premise. Tech Data also includes the option to deploy a Bastion Host for secure and seamless RDP/SSH connectivity to virtual machines within Microsoft Azure. Use cases for this deployment include extending on premise directories to the cloud or shifting to a 100% cloud infrastructure.

#### Azure Active Directory Domain Services (AADDs) - Click to Run Solution Benefits:

- **Preconfigured VNet** - We provision the DomainServices, Workloads, and AzureBastion subnets.
- **DNS** - the solution configures the AADDs server as the primary DNS server IP addresses.
- **Azure Bastion** - Choose whether to deploy a Bastion Host to securely access hosts that will be joined to the AADDs instance. No user configuration or setup required.
- **AADDs Admin Group** – The solution creates the AAD DC Admins group in Azure Ad. The Admin user specified during deployment will be placed in this group by default.

## Deployment Architecture:



## AADDs Resource Health Status

After deploying the AADDs solution, it takes some time for the AADDs core services to become fully useable (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 7 of 7 records.
☐ Show hidden types

<input type="checkbox"/> Name ↑↓	Type ↑↓	Location ↑↓
<input type="checkbox"/> aadds-681f3704fd5a437f9730ade399f04cc6-nic	Network interface	West Europe
<input type="checkbox"/> aadds-d164855962074b4c937671dc11297613-lb	Load balancer	West Europe
<input type="checkbox"/> aadds-d164855962074b4c937671dc11297613-pip	Public IP address	West Europe
<input type="checkbox"/> AADDs-NSG	Network security group	West Europe
<input type="checkbox"/> AADDs-VNet	Virtual network	West Europe
<input type="checkbox"/> aadds.tdsolutionfactorysb.onmicrosoft.com	Azure AD Domain Services	West Europe
<input type="checkbox"/> bastionHost-pip	Public IP address	West Europe

The AADDs Deployment is ready for use if the health status is shown as "Running."



aadds.tdsolutionfactorysb.onmicrosoft.com

 Running

View health

More Information on AADDs Health can be found [here](#).

## 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.

✓ **Configure your Azure Active Directory Domain Services Solution**

Location

Select data center location  
 West Europe

Resource Group Name  
 TC-AADDs-2

Basic Information

👤 Tenant Administrator

tony@tdsolutionfactorysb.onmicrosoft.com
 

←

👤 Managed Domain Name

aadds.tdsolutionfactorysb.onmicrosoft.com

Advanced settings

👤 Deploy Bastion Host

Deploying...

TD Solution Factory Sandbox Sign out

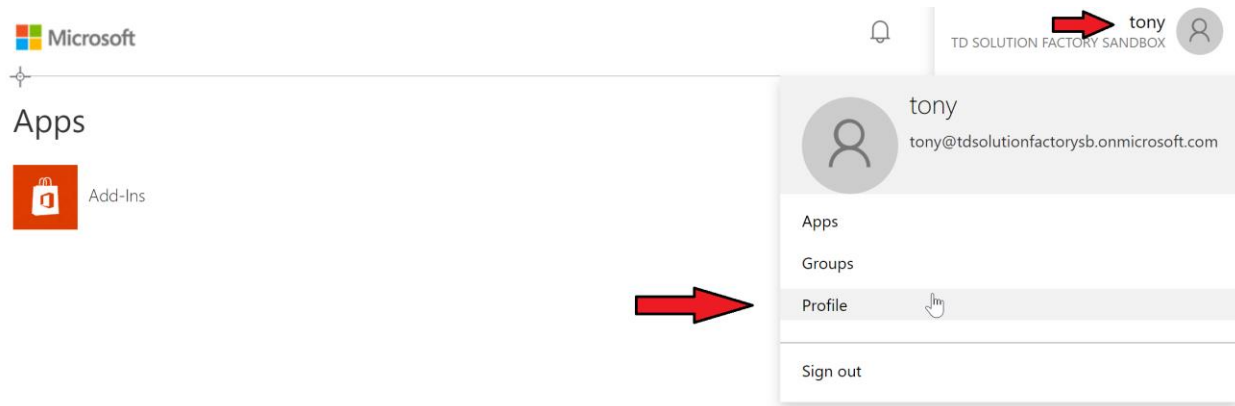
→

tony

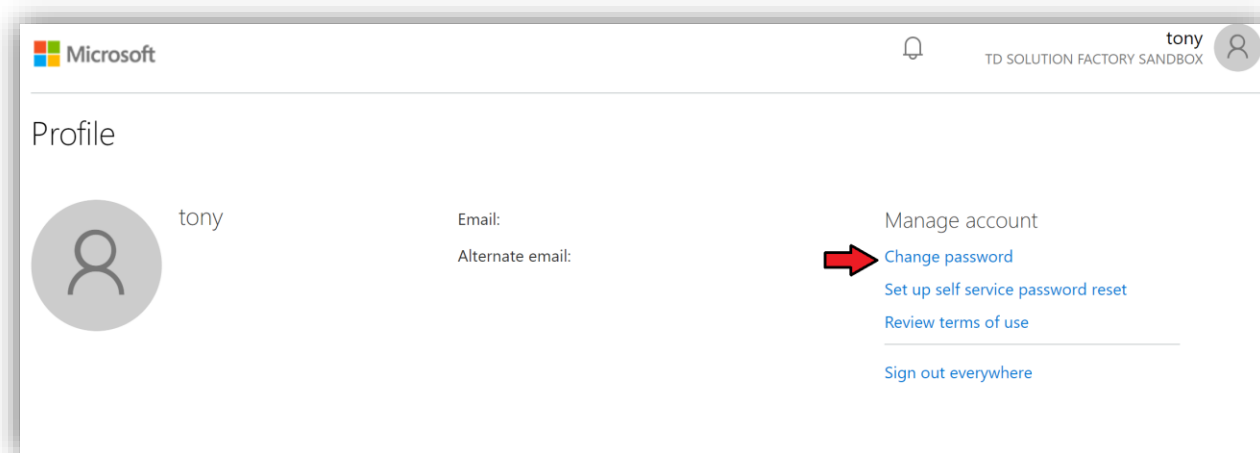
tony@tdsolutionfactorysb.on...

View account
Switch directory
...

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.



On the **Profile** page, select **Change password**.



----- Continue to the next page -----

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




Select **Submit**. *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](#).

## 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 achieving this can be found [here](#).

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