Existing Domain Integration Guide (Hybrid AD)

A guide for connecting a Nerdio WVD deployment to an existing Active Directory domain

Purpose

When provisioning a Nerdio WVD environment in Azure, a new “greenfield” Active Directory is created. This enables safe testing of WVD in a non-production Active Directory environment. However, most production deployments need to utilize the existing AD user objects and join newly created WVD sessions hosts to an existing AD domain. This guide outlines the steps for connecting a Nerdio deployment to an existing AD environment to accomplish this goal.

Audience

This guide is geared towards technical staff and IT administrators that are familiar with Active Directory, Azure AD, Azure AD Connect, NAP, Azure and WVD in general. Some experience managing virtual desktops, networking infrastructure and IT systems is assumed.

Nerdio Hybrid AD guide

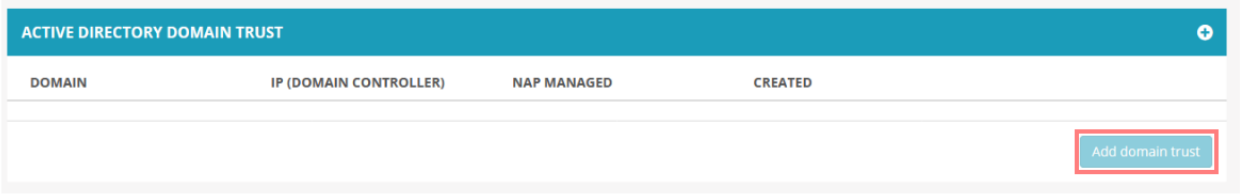
The process to connect a Nerdio deployment to an existing AD environment and extend it into Azure consists of 3 steps. This functionality is referred to as Nerdio “Hybrid AD”.

Step I – Enable network connectivity between Nerdio and existing AD environment

1. Utilize site-to-site IPSec VPN, ExpressRoute or vNet peering to connect the subnet that contains DC01 to the network that contains a domain controller of the existing AD.
    a. If utilizing site-to-site VPN go to NAP>Network>VPN connections, enable VPN and add a new connection

Step II – Add domain trust between Nerdio AD and existing AD domains

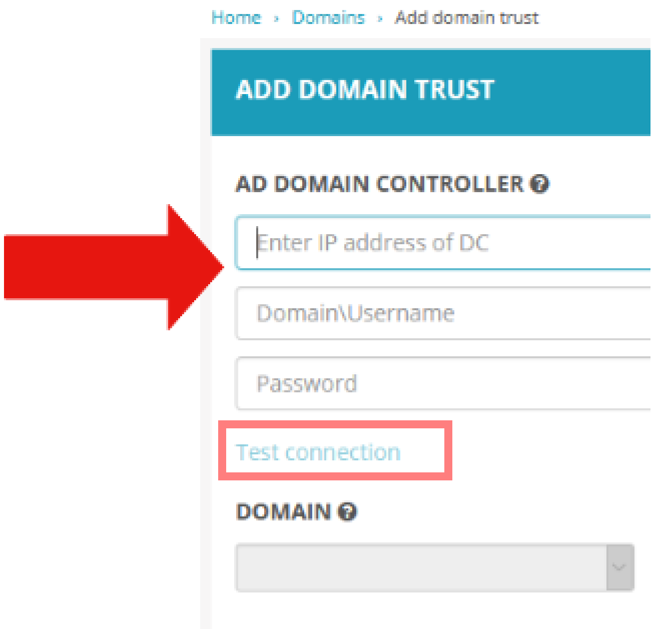
1. Log in to NAP as an administrator.
2. From the main menu on the left side, click Onboard>Domains.
3. Scroll down to "Active Directory Domain Trust" section and click "Add domain trust" button.



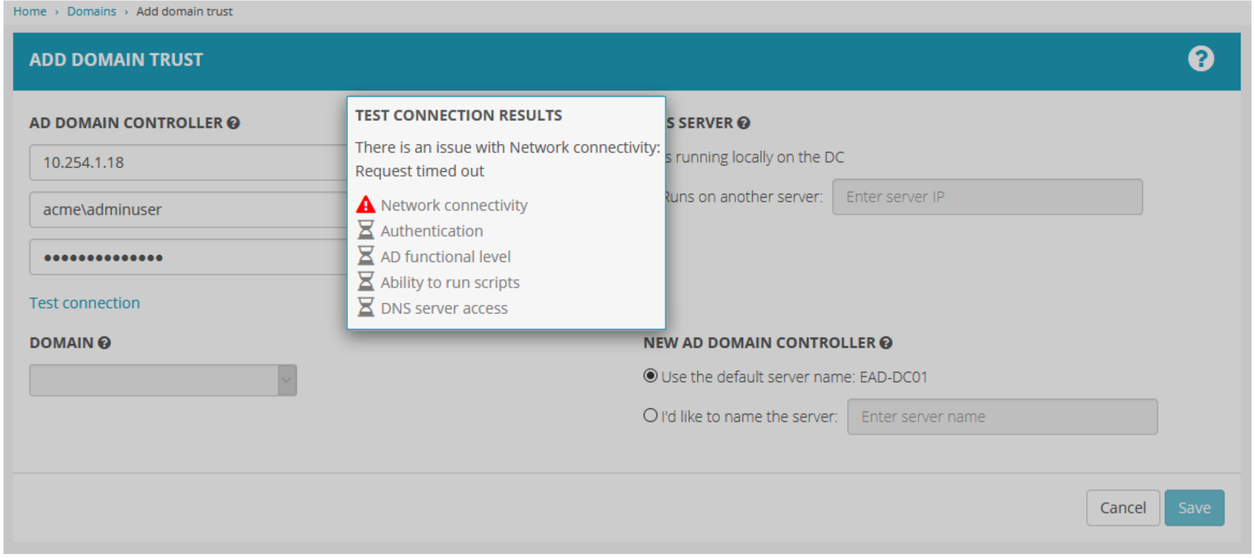
ACTIVE DIRECTORY DOMAIN TRUST

DOMAIN	IP (DOMAIN CONTROLLER)	NAP MANAGED	CREATED

4. On the "Add Domain Trust" screen, first enter information about the on-prem domain controller, and then click "Test connection".



Note: if NAP is unable to connect to the domain controller, you will see an error message like this:



10.254.1.18

acme\adminuser

••••••••••••••

○ I'd like to name the server:

● Use the default server name: EAD-DC01

TEST CONNECTION RESULTS

There is an issue with Network connectivity: Request timed out

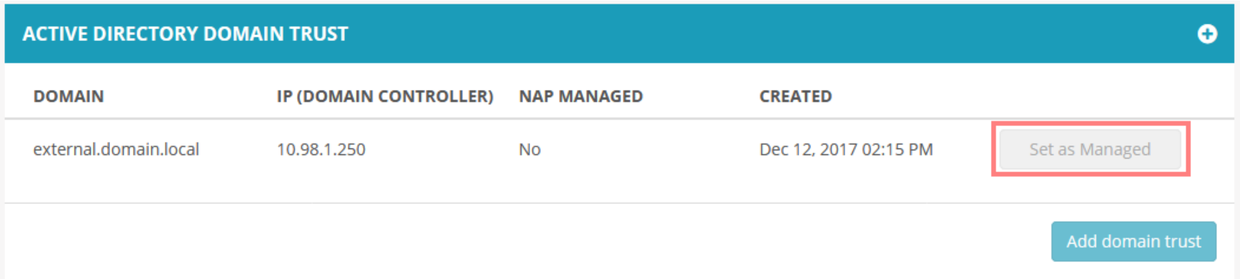
- ⚠ Network connectivity
- ⌛ Authentication
- ⌛ AD functional level
- ⌛ Ability to run scripts
- ⌛ DNS server access

5. If NAP is able to connect to domain controller, continue filling out rest of the fields on screen.
6. Click Save.

Step III – Setting external (trusted) AD domain as "NAP Managed"

1. Login to Azure management portal.
2. From the main menu on the left side, click Onboard>Domains.
3. Scroll down to "Active Directory Domain Trust" section, locate the domain you want to manage.

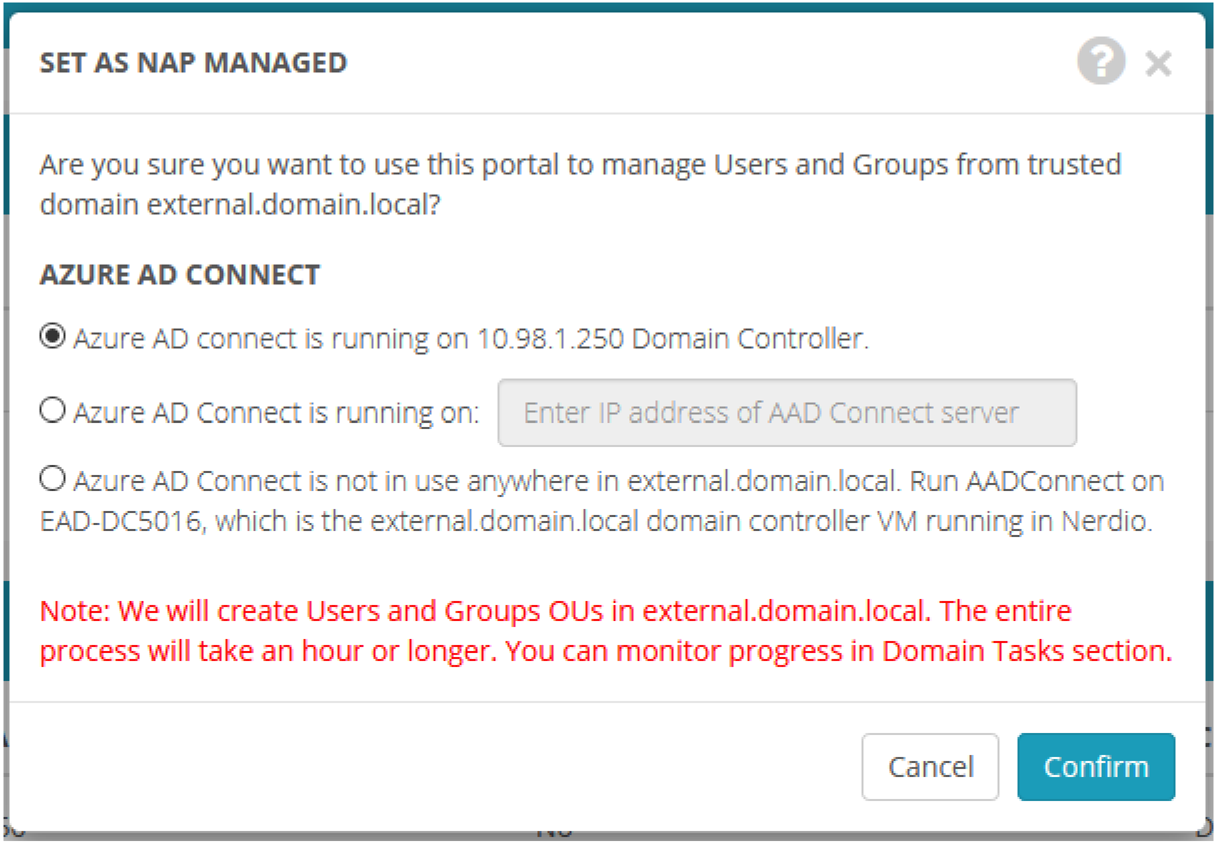
4. Click "Set as managed" button.



ACTIVE DIRECTORY DOMAIN TRUST

DOMAIN	IP (DOMAIN CONTROLLER)	NAP MANAGED	CREATED	
external.domain.local	10.98.1.250	No	Dec 12, 2017 02:15 PM	Set as Managed

5. Indicate if Azure AD Connect is already running on a server in existing AD or if you want to have it run on the new domain controller that was spun up when domain trust was established (step II above).



SET AS NAP MANAGED

Are you sure you want to use this portal to manage Users and Groups from trusted domain external.domain.local?

AZURE AD CONNECT

● Azure AD connect is running on 10.98.1.250 Domain Controller.

○ Azure AD Connect is running on: Enter IP address of AAD Connect server

○ Azure AD Connect is not in use anywhere in external.domain.local. Run AADConnect on EAD-DC5016, which is the external.domain.local domain controller VM running in Nerdio.

Note: We will create Users and Groups OUs in external.domain.local. The entire process will take an hour or longer. You can monitor progress in Domain Tasks section.

6. Click Confirm button to confirm the action the action you are taking.

Once the above steps are completed and Nerdio Hybrid AD is enabled users from the existing AD domain can be imported into Nerdio and assigned to WVD resources. To import users, navigate to NAP>Onboard>Domains and click on **Import users** button next to the existing AD domain.

A few items to consider once you have completed the setup:

- You will notice that an "Active Directory" field has been added to most modules in NAP (for example Users, Groups, Servers, etc.). This indicates which AD the objects resides in: Nerdio AD or Existing AD

- Existing objects created in NAP prior to enabling Hybrid AD reside in the Nerdio AD. Objects cannot be moved automatically from one AD to the other.
- When you create new objects (e.g. WVD host pool, personal desktops, users, groups, new servers, etc.), the object will be created in existing AD by default. You can override the default and create the object in Nerdio AD (this could be used for testing purposes).
- Any WVD session host objects you may have provisioned prior to enabling Hybrid AD reside in Nerdio AD. As a result, when you assign desktops to users from existing domain, there won't be a WVD desktop pool to assign them to from the same AD domain. Simply add a new WVD desktop pool and select the existing pool as the template source. Then delete the original WVD pool once the new one is successfully created. This will allow users from existing AD to be assigned to the newly provisioned WVD session host pool.

An in-depth overview of Nerdio Hybrid AD can be found in this Nerdio Knowledge Base article.