

## **LAB – Local Active Directory Synch to Azure Active Directory**

1. Create an Active Directory on Azure 2016
2. Login to the VM, and promote it as Domain Controller.
3. The Domain name should have already been configured and verified on the Azure portal as well.
4. Install the Azure AD connect on the VM and configure it.

### Pre-Requisite

1. Should have an domain either bought on the Azure custom domain, or anyother domain provider and verif the domain on Azure portal

# Azure-AD Sync to On Prem

## 1. Create an Active Directory on Azure 2016

Select the below image to create an VM on Azure for Active Directory.



## Ports to be opened on the Virtual Machine (Active Directory)

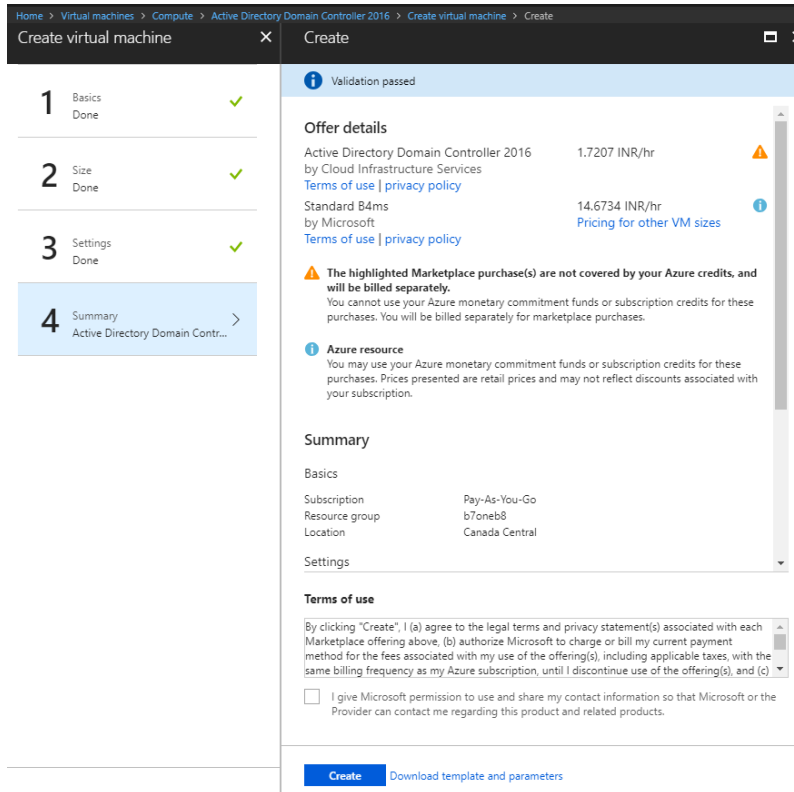
### INBOUND PORT RULES ⓘ

Network security group **VM01-nsg** (attached to network interface: [vm01604](#))  
Impacts 0 subnets, 1 network interfaces

[Add inbound port rule](#)

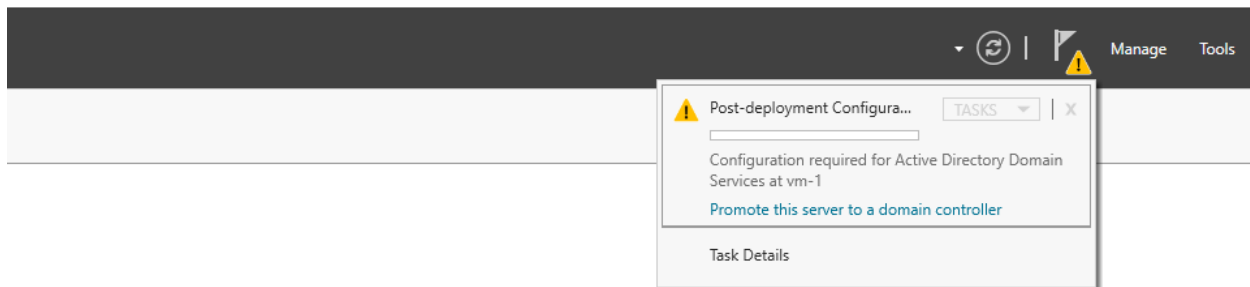
| PRIORITY | NAME                          | PORT | PROTOCOL | SOURCE            | DESTINATION    | ACTION  |     |
|----------|-------------------------------|------|----------|-------------------|----------------|---------|-----|
| 1010     | LDAP                          | 389  | TCP      | Any               | Any            | ✓ Allow | ... |
| 1020     | LDAP_SSL                      | 636  | TCP      | Any               | Any            | ✓ Allow | ... |
| 1030     | LDAP_GC                       | 3268 | TCP      | Any               | Any            | ✓ Allow | ... |
| 1040     | Kerberos                      | 88   | Any      | Any               | Any            | ✓ Allow | ... |
| 1050     | DNS                           | 53   | Any      | Any               | Any            | ✓ Allow | ... |
| 1060     | Replication                   | 445  | Any      | Any               | Any            | ✓ Allow | ... |
| 1070     | File_Replication              | 5722 | TCP      | Any               | Any            | ✓ Allow | ... |
| 1080     | Kerberos_PW_Change            | 464  | Any      | Any               | Any            | ✓ Allow | ... |
| 1090     | ⚠ default-allow-rdp           | 3389 | TCP      | Any               | Any            | ✓ Allow | ... |
| 65000    | AllowVnetInBound              | Any  | Any      | VirtualNetwork    | VirtualNetwork | ✓ Allow | ... |
| 65001    | AllowAzureLoadBalancerInBound | Any  | Any      | AzureLoadBalancer | Any            | ✓ Allow | ... |
| 65500    | DenyAllInBound                | Any  | Any      | Any               | Any            | ✗ Deny  | ... |

# Azure-AD Sync to On Prem



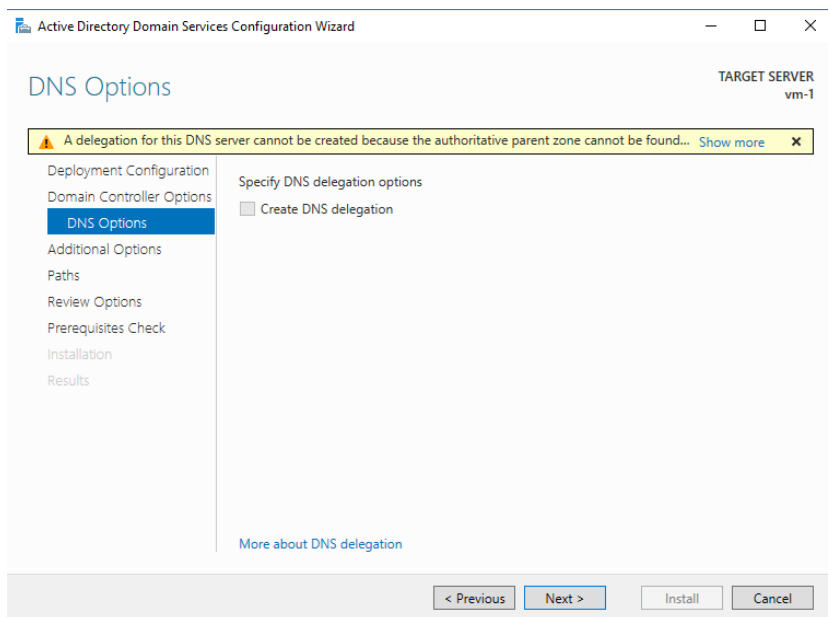
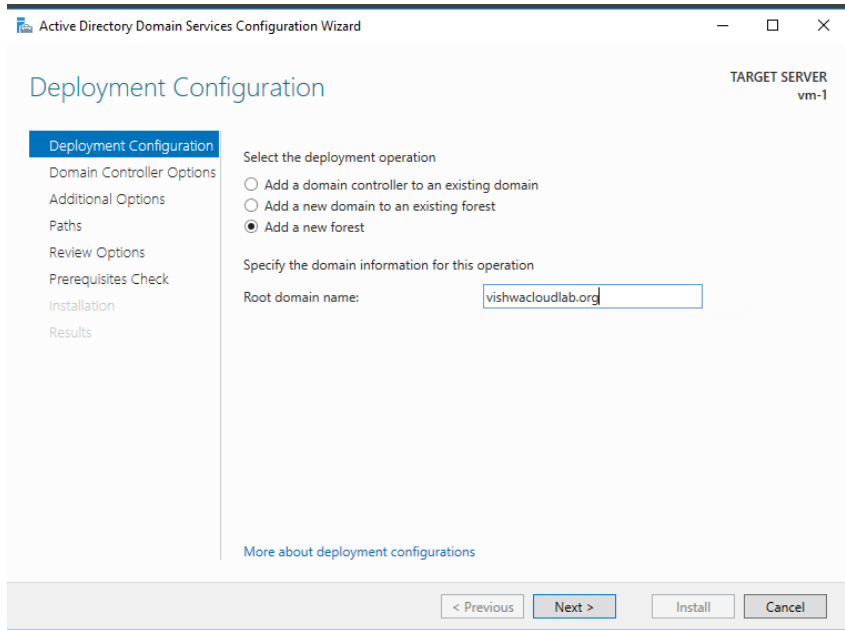
## 2. Configure the Active Directory on the Virtual Machine

Login to the VM. Click on the notification in the "Server Manager"



Click on "promote this server to Domain Controller"

# Azure-AD Sync to On Prem



# Azure-AD Sync to On Prem

Active Directory Domain Services Configuration Wizard

Additional Options

TARGET SERVER  
vm-1

Deployment Configuration  
Domain Controller Options  
DNS Options  
**Additional Options**  
Paths  
Review Options  
Prerequisites Check  
Installation  
Results

Verify the NetBIOS name assigned to the domain and change it if necessary

The NetBIOS domain name:

[More about additional options](#)

< Previous Next > Install Cancel

Active Directory Domain Services Configuration Wizard

Paths

TARGET SERVER  
vm-1

Deployment Configuration  
Domain Controller Options  
DNS Options  
Additional Options  
**Paths**  
Review Options  
Prerequisites Check  
Installation  
Results

Specify the location of the AD DS database, log files, and SYSVOL

Database folder:  ...

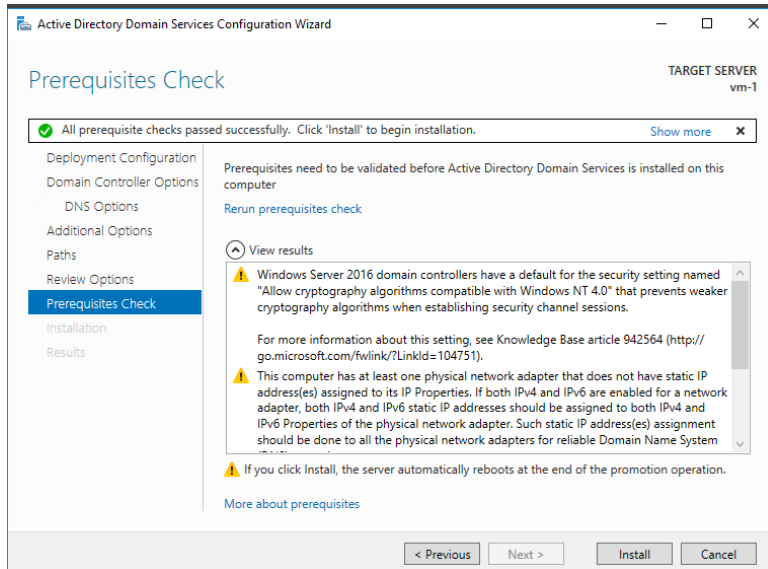
Log files folder:  ...

SYSVOL folder:  ...

[More about Active Directory paths](#)

< Previous Next > Install Cancel

# Azure-AD Sync to On Prem



Note:-- The VM would restart, this would take 5 to 10 min for AD to be ready.

### 3. The Domain name should have already been configured on the Azure portal as well.

The "Domain" has to be bought by you.

And should be **verified** on the Azure portal.

And the same "Domain" should be configured on the Active Directory VM as well.

| NAME               | STATUS     |
|--------------------|------------|
| n                  | Unverified |
| rosoft.com         | Unverified |
| :rosoft.com        | Available  |
| vishwacloudlab.org | Verified   |

### 4. Install the Azure AD connect on the VM and configure it.

Note:-- Create an **user** on the Azure portal for the **Domain** that is created with “**Global Adminsitrator**” Role.

The default Admin userID for the Azure Portal will not work to add the active directory to the Azure.



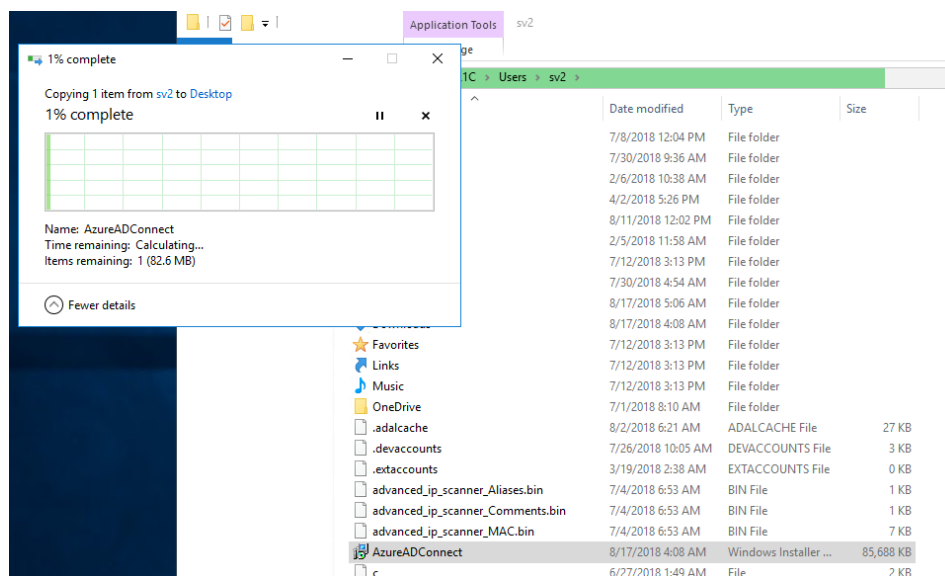
The userID would say “Created on Azure Active Directory”.

Download the below link on the Virtual Machine for “azure AD Connect”

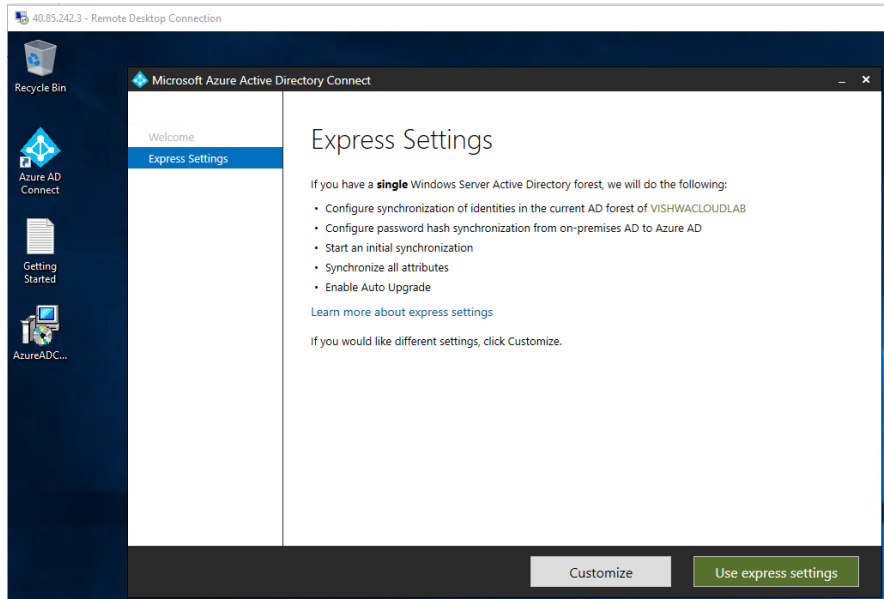
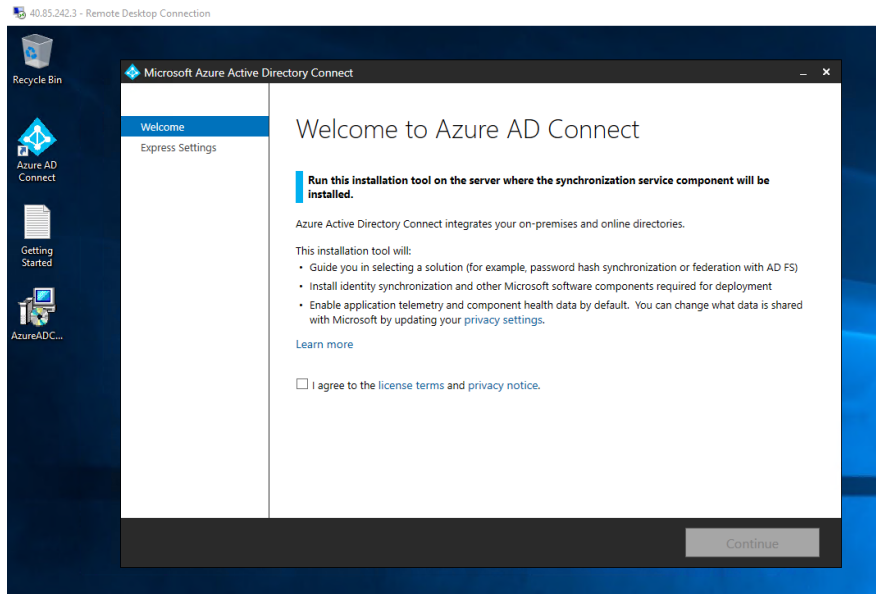
<https://www.microsoft.com/en-us/download/details.aspx?id=47594>

ShortCut—Download the “Azure AD Connect” on your laptop and copy it into the Virtual machine.

As the link does not open up in the new VM , properly.

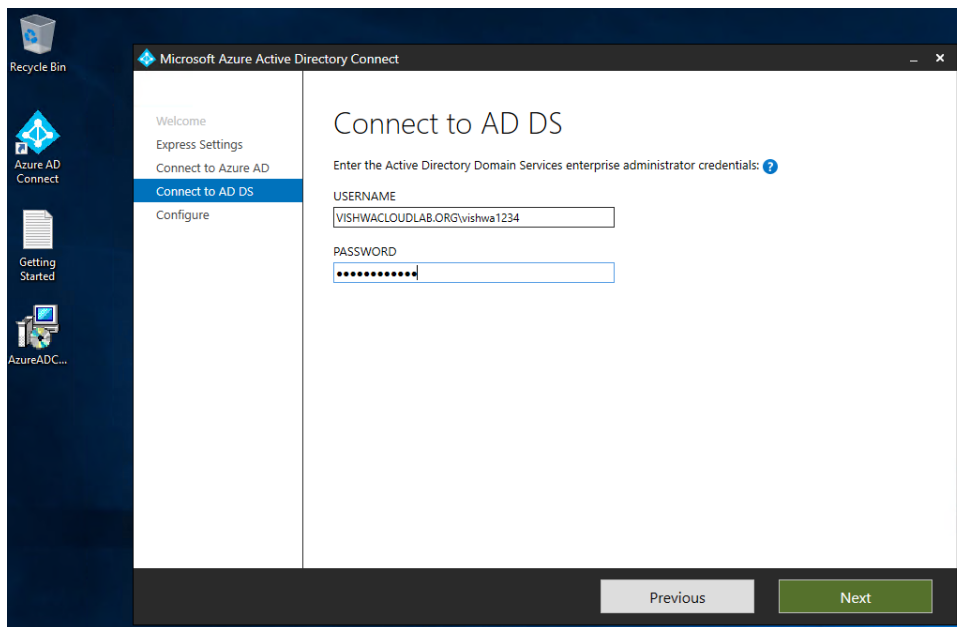
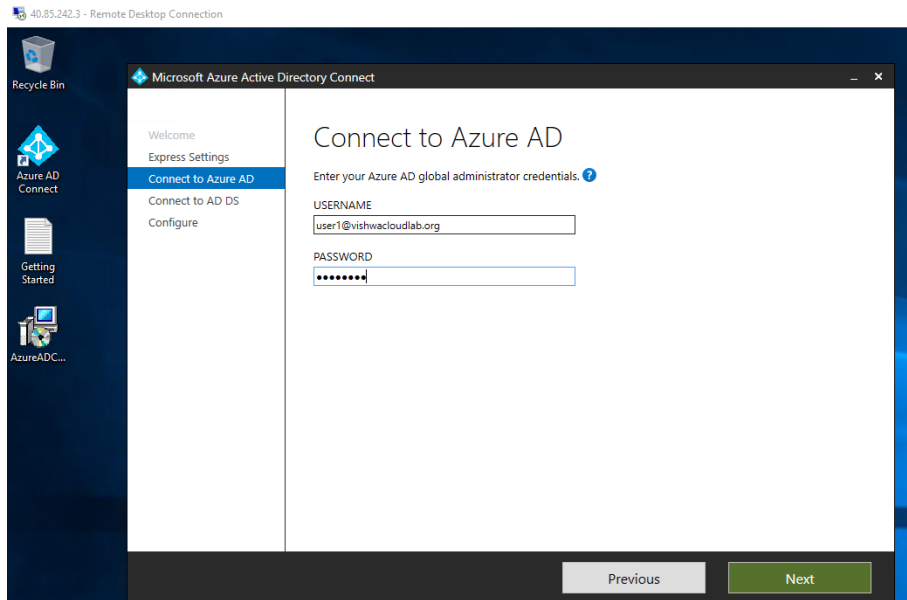


# Azure-AD Sync to On Prem





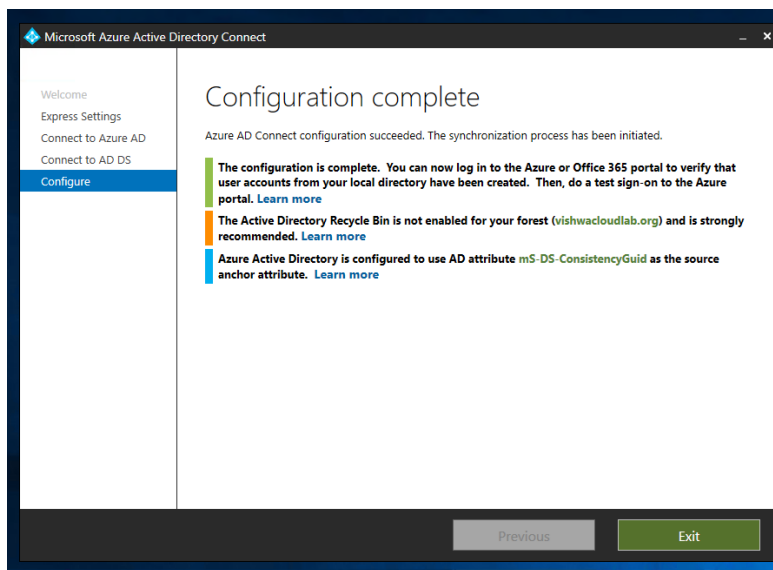
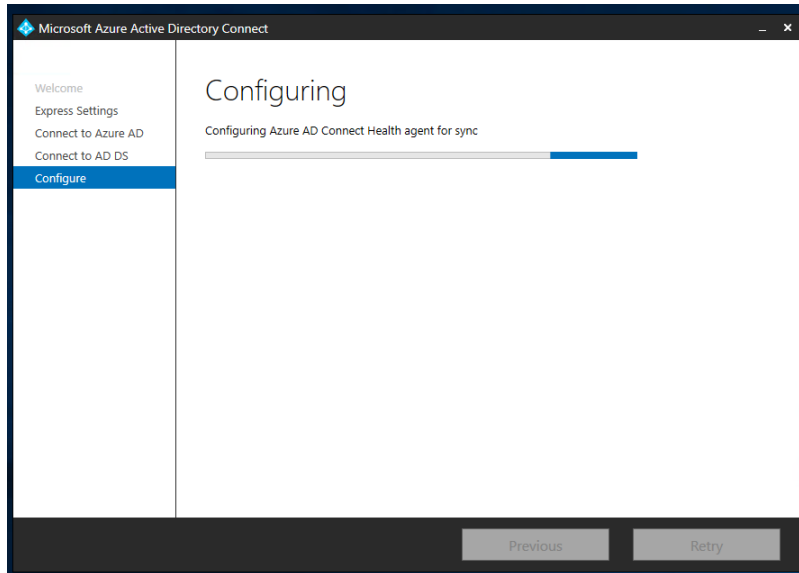
# Azure-AD Sync to On Prem



The above usr and pwd is the local user/pwd on the Active Directory server.

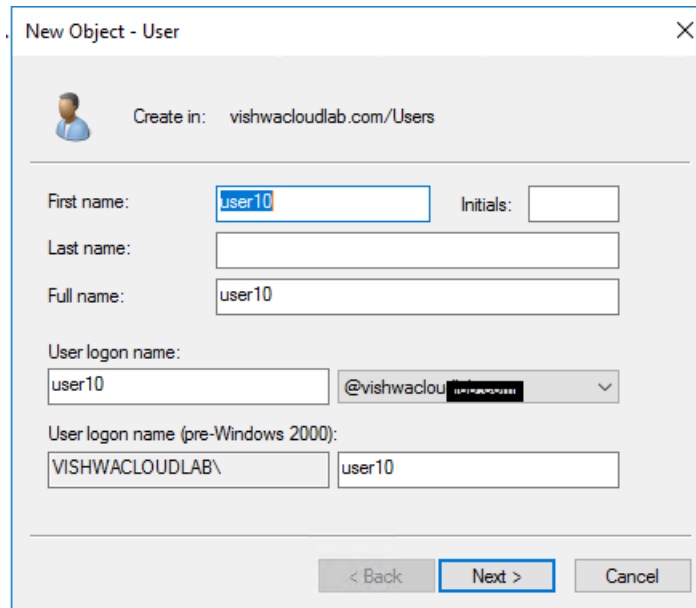
# Azure-AD Sync to On Prem

---



Create an user in the Active Directory on the Virtual Machine AD.



## Azure-AD Sync to On Prem




|   |                   |
|---|-------------------|
|  Schema Admins | Security Group... |
|  user10        | User              |
|  vishwa123     | User              |

After the Active Directory is connected to the Azure AD connect

The below is the screen short after 1 hr on the Azure portal.

 Troubleshoot  Refresh



SYNC STATUS

Sync Status

Enabled

Last Sync

Less than 1 hour ago

Password Hash Sync

Enabled

The users that was created in the active directory on the onprem has been listed automatically in the azure active directory

# Azure-AD Sync to On Prem

The Above users are created on the active directory

The below same users are synced to Azure.

| NAME  | USER NAME                              | USER TYPE | SOURCE                 |
|---|--|-----------|------------------------|
| 623b7d48-0e5a-4feb-a2bd-6a030e3f934f 5c03   | vishwaawsac@gmail.com                  | Member    | Microsoft Account      |
| On-Premises Directory Synchronization Service Sync_VM01_bac95bf4eabb@vishwaawsacgmail.onmicr... |  | Member    | Windows Server AD      |
| user1   | user1@vishwacloudlab.org               | Member    | Azure Active Directory |
| user1   | user1@vishwaawsacgmail.onmicrosoft.com | Member    | Azure Active Directory |
| user10  | user10@vishwacloudlab.org              | Member    | Windows Server AD      |
| user2   | user2@vishwaawsacgmail.onmicrosoft.com | Member    | Azure Active Directory |
| vishwa123   | vishwa123@vishwacloudlab.org           | Member    | Windows Server AD      |
| vishwanath.murthy   | vishwanath.murthy@gmail.com            | Guest     | Microsoft Account      |

Synced from Previous Active Directory server

|           |  |        |                        |
|-----------|--|--------|------------------------|
| user10    | user10@vishwacloudlab.org              | Member | Windows Server AD      |
| user2     | user2@vishwaawsacgmail.onmicrosoft.com | Member | Azure Active Directory |
| vishwa123 | vishwa123@vishwacloudlab.org           | Member | Windows Server AD      |

## Objective:

There is no need to create users in the Azure AD

This is very usefull for the IT admins in an organization, where in they will hve single sign on for their local systems and Azure portal.