**SOP - Hybrid Identity**

**Implementation Guide**

Hybrid identity implementation is performed when extending identity and offload authentications from on-premises windows active directory domain controller to domain controller in Azure. Upon extending identity to Azure cloud, organizations building applications in azure can easily serve authentication requests without any VPN or connection issues.

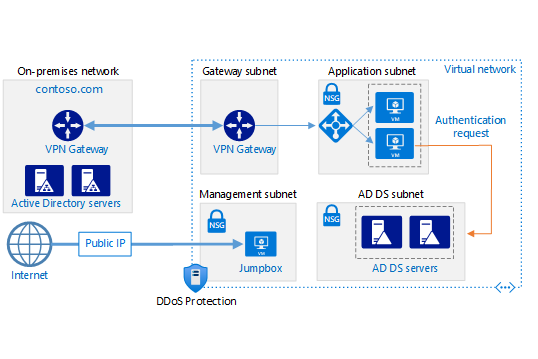
As per requirements & implementation planning, virtual machine(s) will be deployed in prod subscription. Before proceeding with the implementation, the following details needs to thoroughly revised and ready.

Permissions:

1. Domain account to on-premises environment.
2. Contributor role on subscription

Notable points:

1. Azure Vnet should not overlap with on-premises network (address spaces).
2. Public IP or inbound public inbound ports should not be opened.
3. Line of sight to on-premises network either using VPN tunnel or ExpressRoute to your azure network.
4. No spot VMs will be used for DCs in Azure.



**Domain Controller Details**

Size of VM:

CPU:

Memory:

Redundancy option (Ex: Zones):

Region to deploy production DC(s):

Region to deploy Disaster Recovery DC(s):

Number of Production DCs:

Number of DR DCs:

**Configurations on on-premises DC:**

1. Create two sites for Azure prod and Azure DR.
2. Configure network address spaces for both sites.

**Deploy 1st Production Domain Controller:**

1. Login into Azure portal (<https://portal.azure.com>)
2. Subscription: Select the subscription you want to use for the VM.
3. Resource group: Select an existing or create a new resource group.
4. Virtual machine name: Give your VM a name (AZ-DC01)
5. Region: Choose the first region to deploy 1st production-based DC.
6. Availability options: Select Zone 1 (and Zone 2).
7. Security Type: Choose Trusted Launch Virtual Machine.
8. Image: Choose “Windows Server 2019 Datacenter”.
9. Size: For default choice, choose Azure VM size of “Standard\_D2s\_v5” which will have 2 Cores and 8 GB of RAM.
10. Username and password: This will be the local administrator account for the VM.
11. Public inbound ports: you want this set to “none”.
12. Licensing: If you have an existing license, you can use select the box, this can save money on each VM.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

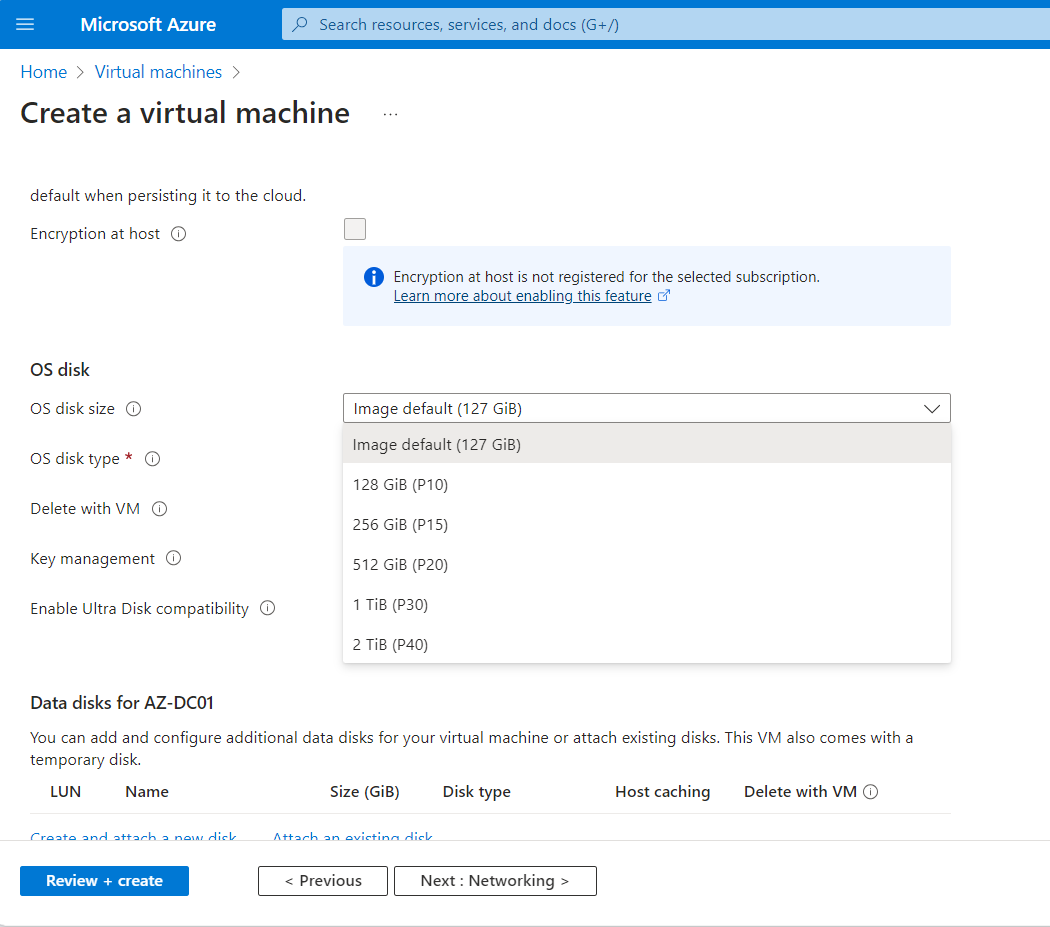
Description automatically generated

A screenshot of a computer

Description automatically generated

Disk Configuration:

1. OS Disk Type: choose image default (127 GiB)



1. OS disk type: choose Standard HDD.
2. Key Management: choose “Platform-managed key”.

A screenshot of a computer

Description automatically generated

Network Configuration:

A screenshot of a computer

Description automatically generated

1. Virtual network: choose the Vnet from the available list.
2. Subnet: choose the subnet from the available list.
3. Public IP: Do not provide Public IP.

A screenshot of a computer

Description automatically generated

Management Configuration:

A screenshot of a computer

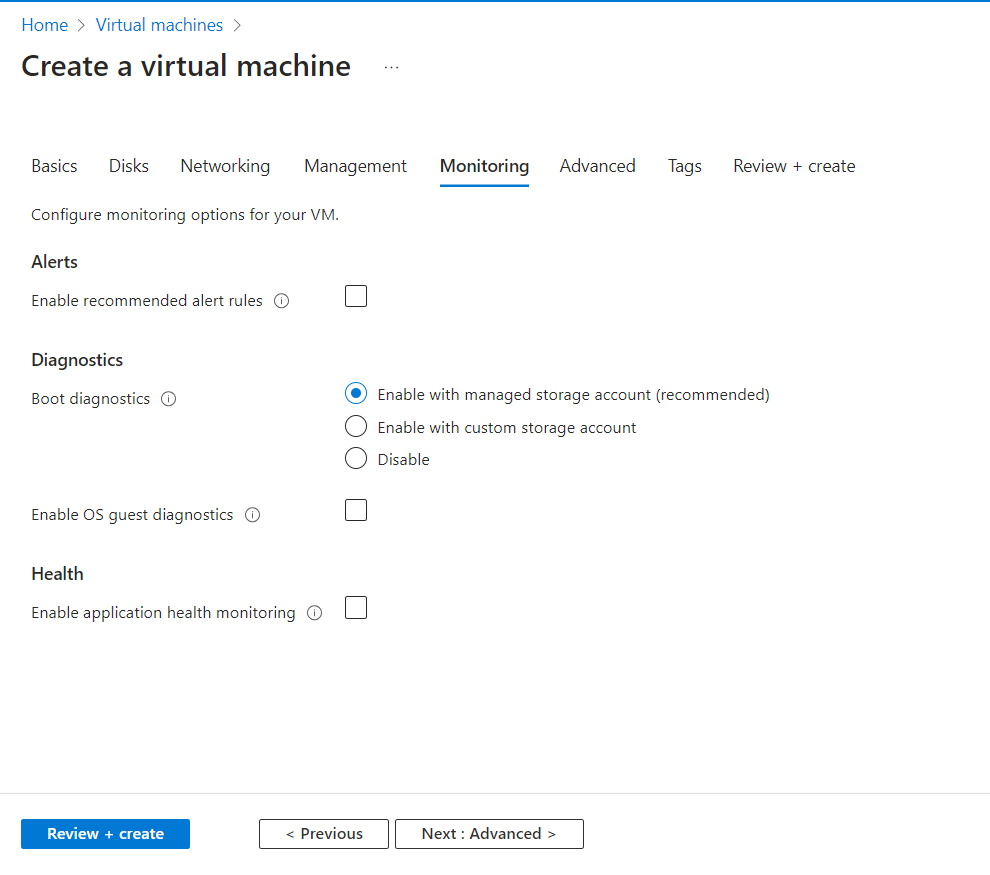
Description automatically generated

1. Patch Orchestration Options: Choose the appropriate option.
2. Backup: Enable backup with existing backup policy and recovery service vault.

A screenshot of a computer

Description automatically generated

Monitoring Configuration:



Advance Configuration:

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Step 2: Configure VM with static IP address

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Go to DNS settings,

A screenshot of a computer

Description automatically generated

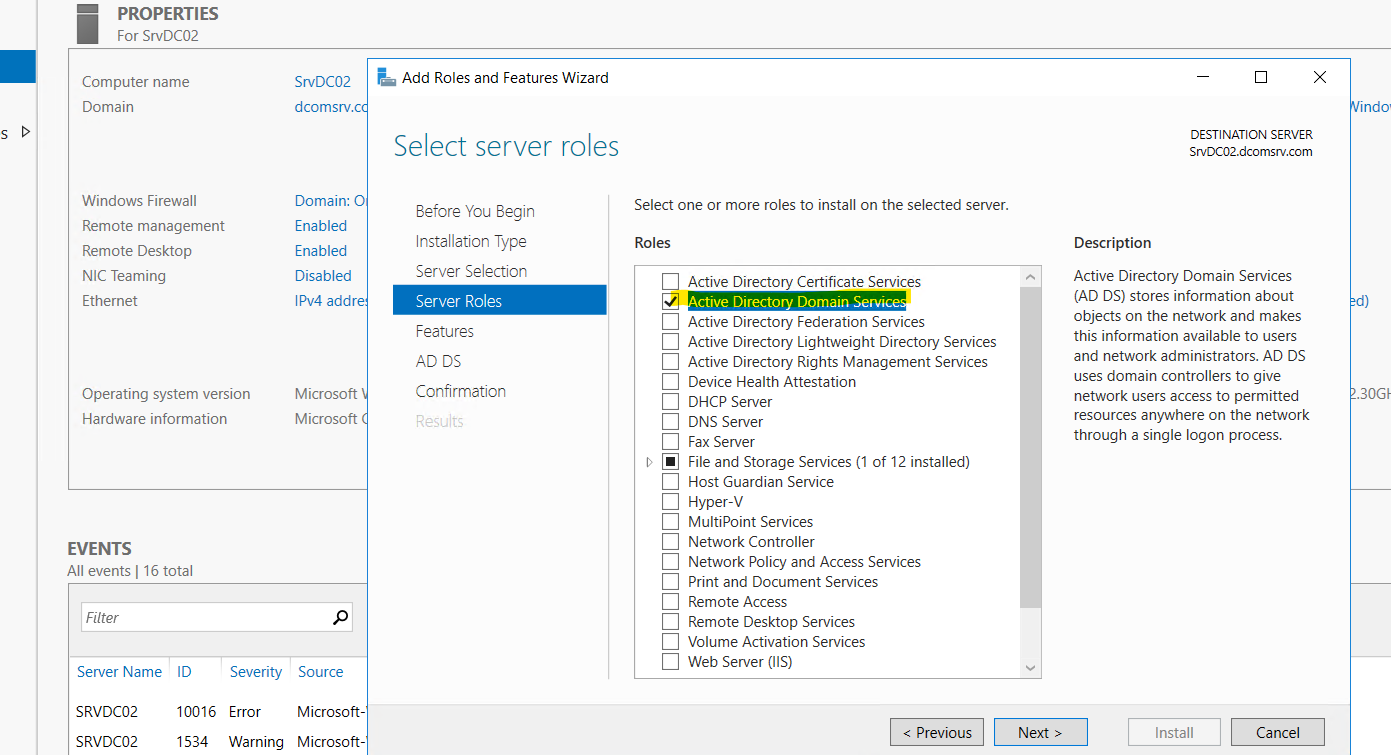
**Note: make sure no other VMs are affected with DNS settings.**

ADDS Pre-Configuration Settings:

1. Login into the Server that is created with admin credentials.
2. Run ipconfig /all in cmd and verify the custom DNS settings.
3. If clients are following managing separate disk to store database, SYSVOL and logs. Follow below steps to create new data disk.
4. Initialize and format the data disk as F:
5. Open the Start menu and browse to Computer Management
6. Browse to Storage > Disk Management
7. Initialize the disk as MBR.
8. Create a New Simple Volume and Assign the drive letter ‘F’ (you can provide a Volume label if you wish)

AD DS Configuration:

1. Launch server manager.
2. Install AD DS server role.



1. Promote the server to Domain controller.