N-able On-Boarding Process

1. Open N-able portal

On top of the left side panel Select Client (Arvinas).

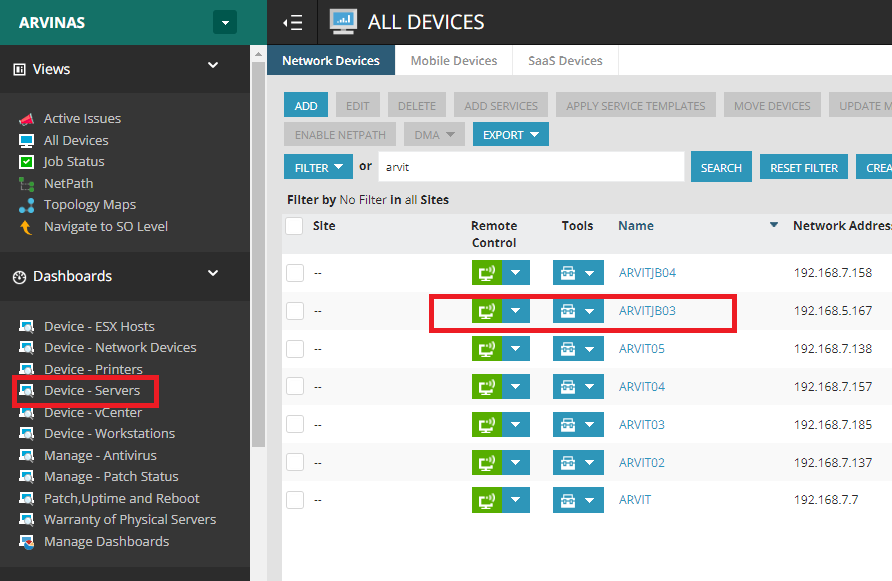
Note: - In this SOP we are taking Arvinas Client On-Boarding Example.

A screenshot of a computer

Description automatically generated

2. In the left side panel select Dashboard Navigate to Device-Servers

>> Login to Jump server (ARVIT03)



3. Open the CMD terminal run as administrator, and Ping the IP address of the server that we need to On-Board.

a. client may provide the IP address via mail

Go To CMD

>> ping IP

Ex- ping 10.5.128.49

A screenshot of a computer program

Description automatically generated

or

b. The client may provide the Server Name

From the Jump server open Google Chrome browser à open V-Center à Login V-center search Device name given by the client.

We can see the IP address of the server, Ping IP address from the jump server CMD  
  
  
 A screenshot of a computer program

Description automatically generated

4. We may get the issue that unable to ping the IP, Request timed out. The reason is due to the firewall on the server which we want to ping. The firewall may not allow IPV4 and IPV6 ping

A computer screen with white text

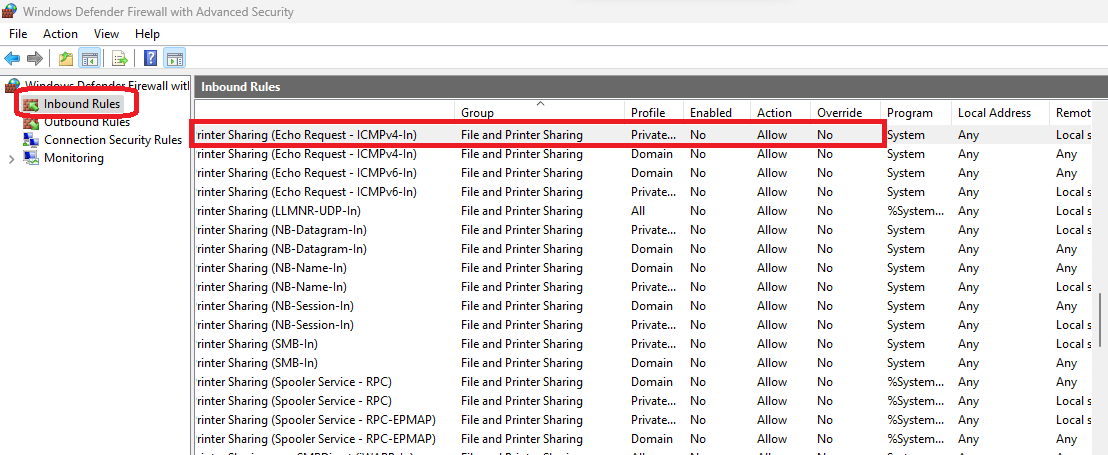
Description automatically generated

àIf we get a request timed out Then follow the below process.

>>From the Jump server take RDP and connect to a new server which we need to Onboard (10.5.128.49).  
>> Search Windows Defender Firewallà Advanced Settingsà Inbound Rules



àselect file and printer sharing (Echo request-ICMpv4-In and ICMpv6) >> Click on Enabled YES



5. After this again check Ping 10.5.128.49

A close up of a line

Description automatically generated  
  
   
  
A screenshot of a computer program

Description automatically generated

6. After Completion of the above process follow the below steps to On-board the Machine into the N-able portal.

>> Navigate to Configurations à Asset Discoveryà Discovery Jobà Click on Add

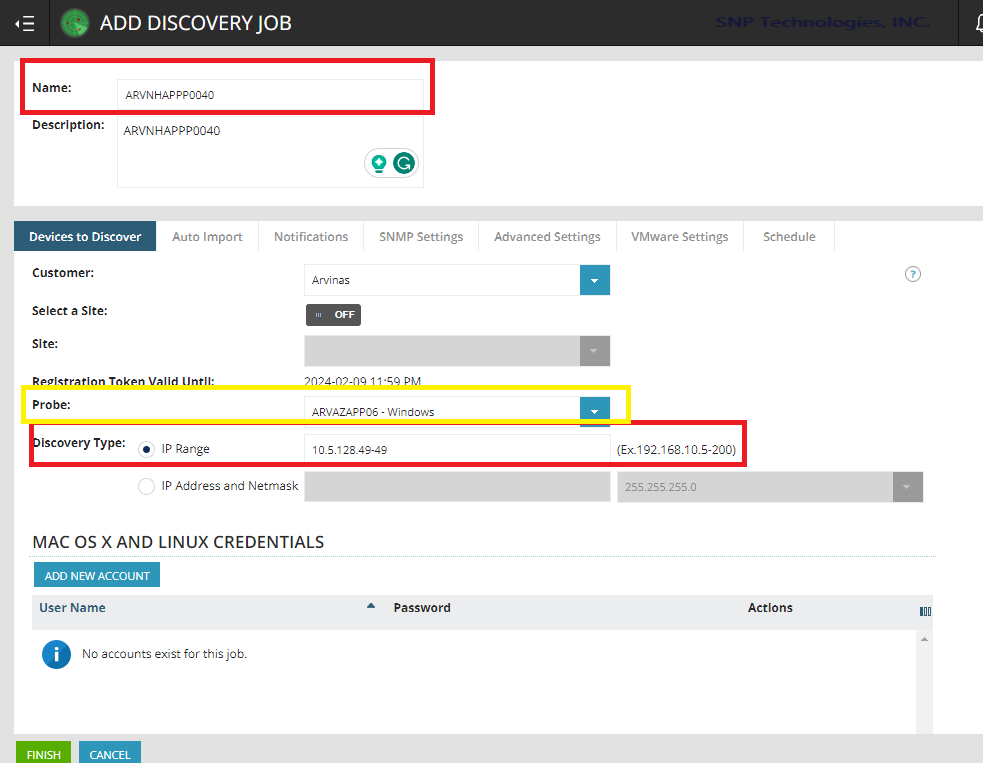
A screenshot of a computer

Description automatically generated

7. Provide Details based on client requirements such as device name (The name for the device) device IP.

Note: Device IP should be the IP-last pointer of the IP, so that it will create one IP for the server or else it may take IP range of 256.

Ex: 10.5.128.49-49  
  >>We can select prob as Jump server name



* Go to the Auto import option and deselect all

A screenshot of a computer

Description automatically generated

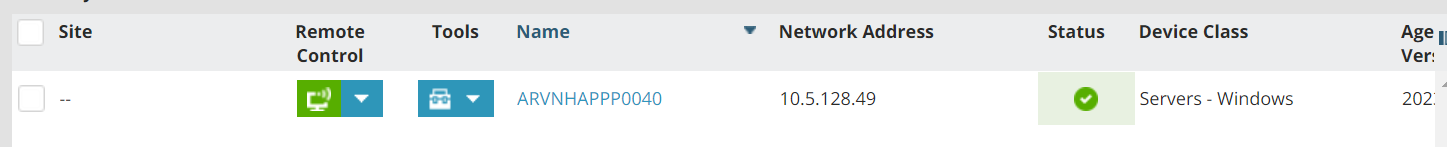
>> Click on Finish.

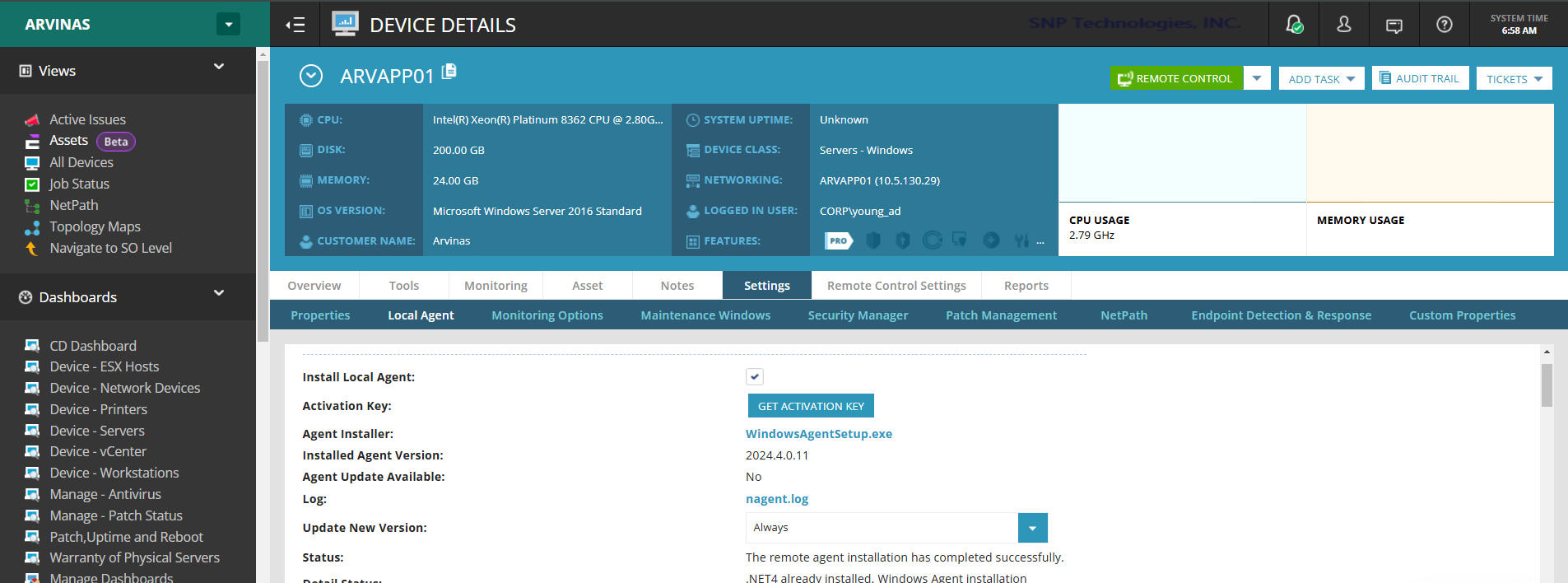
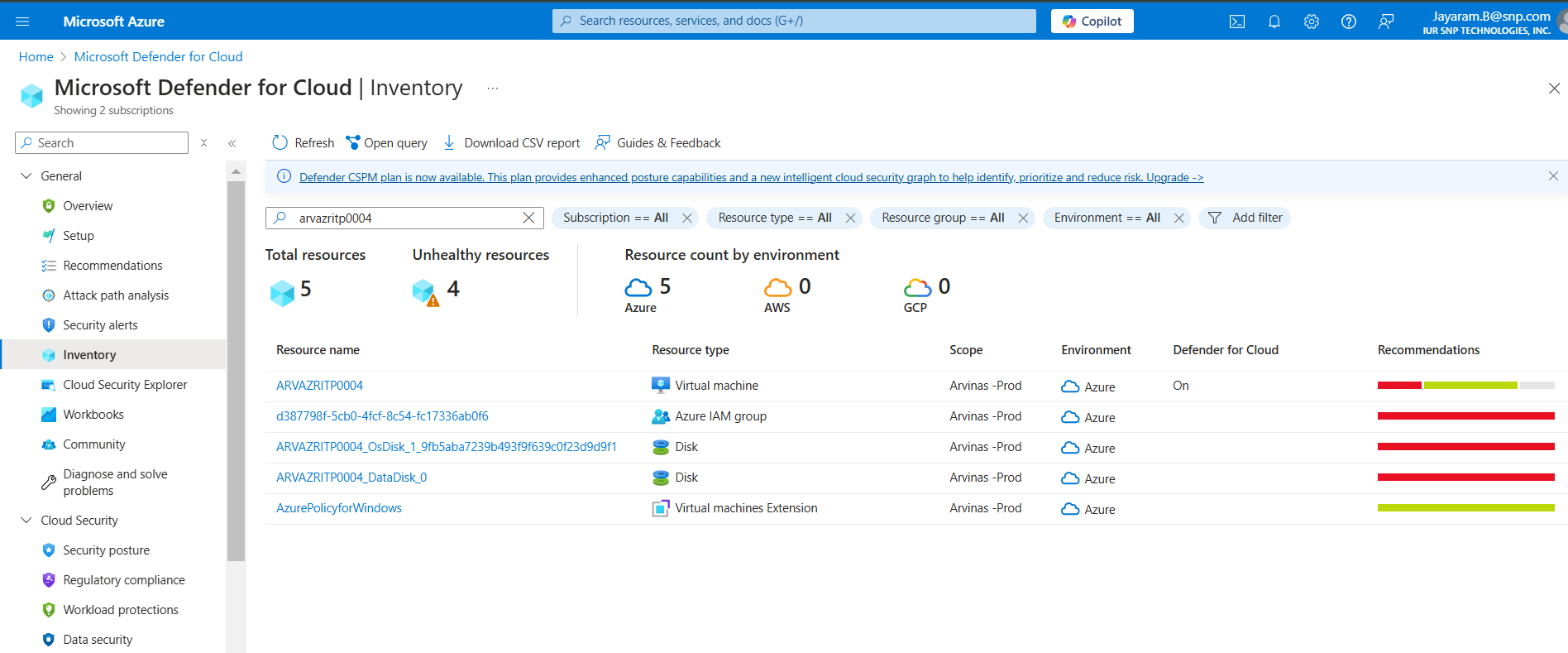
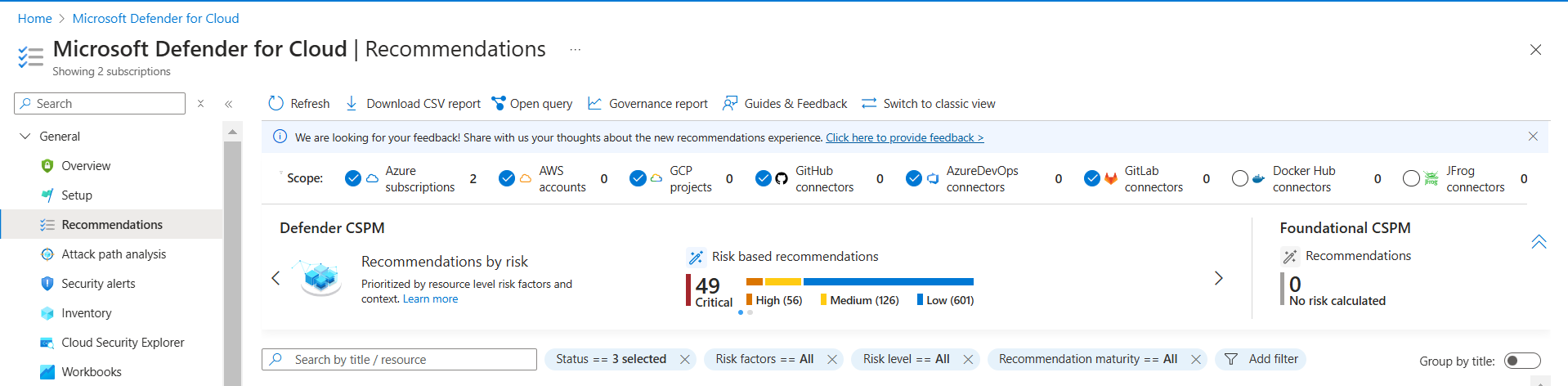
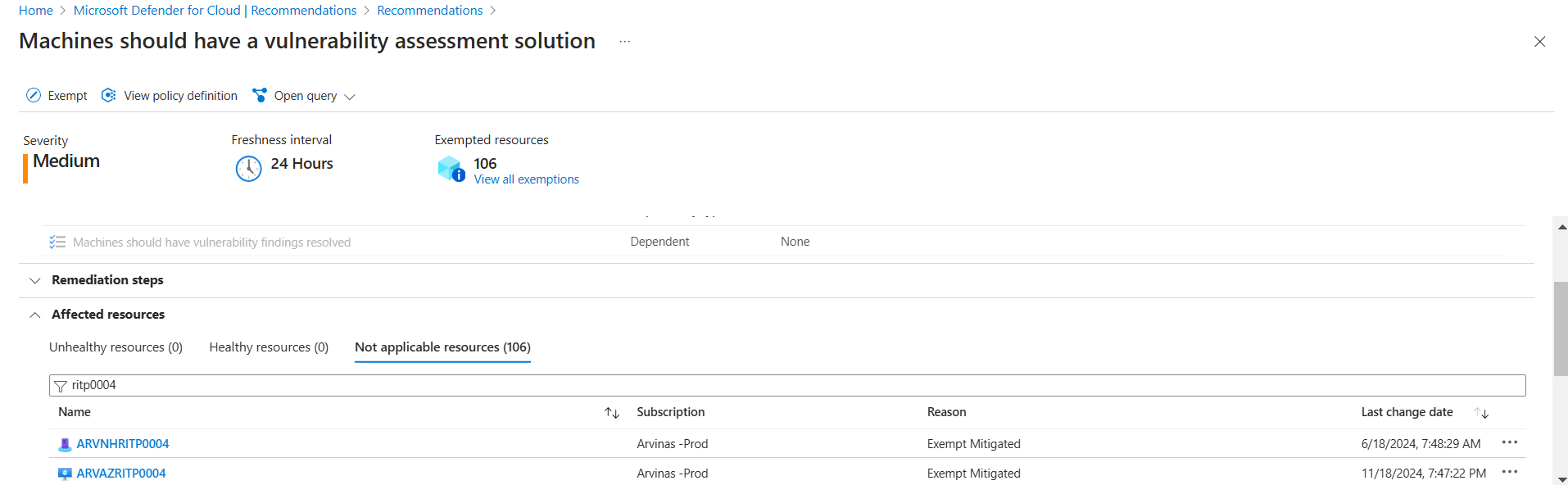
8. After the above process the newly added server will be discovered in **Discovered Assets** option under the **configuration**.

A screenshot of a computer

Description automatically generated

>> Click on that Device à Set License Modeà Professional & SET DEVICE CLASS/OS TO RESPECTIVE OS.  
>> Click on Import   
 >> **Successfully onboard the Machine in N-able**



Check the agent version == if it displays in N-able then it is successful otherwise we need to manually install the agent .  
For this open n-able link in new VM and download agent locally provide by activation key.  
  
  
  
  
For enabling Azure defender for cloud == Actually Defender for cloud is enabled at subscription level. So once the VM is added under any prod subscription it automatically applies.  
  
U need to cross verify from portal == go to defender for cloud == inventor == search for new VM name.  
  
  
  
  
  
For Excempt from Qualys Vulnerability Assessment Tool  
  
  
Go to Microsoft defender for cloud == Recommendations == switch to classic view === Remediate vulnerabilities == click on Machines should have a vulnerability assessment solution == Affected Resources == under not applicable resources check for new VM. If it is there then the new VM is exempted.  
  
  
  
  
NEXT: - After the above process the server will be added to the N-able portal, we can manage the server configuration and monitor alerts on the server, etc.  
To Extend more operations on the server such as applying Azure policies, and governance, and enable more security (cloud defender) we can onboard the server to Azure.

To onboard the server to Azure we use Azure ARC.   
go to portal == login with Arvinas creds on portal == Azure arc – configure new VM give details like RG & region == depends on the OS it will provide u the script. Run that script on the new vm PowerShell ISE. After few mins it will pop up the dialog box & enter Arvinas credentials   
  
Ref document—” Azure Arc”