**BHF –VM Build Guide and Post deployment Steps**

**v1.0**

Contents

[1 Purpose 3](https://myoffice.accenture.com/personal/senthil_vel_murugan_accenture_com/Documents/refer/bright/bright/Guides/BHF%20-%20VM%20Build%20guide%20v1.0.docx#_Toc93703318)

[2 Scope 3](https://myoffice.accenture.com/personal/senthil_vel_murugan_accenture_com/Documents/refer/bright/bright/Guides/BHF%20-%20VM%20Build%20guide%20v1.0.docx#_Toc93703319)

[3 Azure Portal Pre-requisites 3](https://myoffice.accenture.com/personal/senthil_vel_murugan_accenture_com/Documents/refer/bright/bright/Guides/BHF%20-%20VM%20Build%20guide%20v1.0.docx#_Toc93703320)

[4 JSON template for deployment 3](https://myoffice.accenture.com/personal/senthil_vel_murugan_accenture_com/Documents/refer/bright/bright/Guides/BHF%20-%20VM%20Build%20guide%20v1.0.docx#_Toc93703321)

[5 Deployment using Cloud Shell 3](https://myoffice.accenture.com/personal/senthil_vel_murugan_accenture_com/Documents/refer/bright/bright/Guides/BHF%20-%20VM%20Build%20guide%20v1.0.docx#_Toc93703322)

[6 Scale Out Deployment 4](https://myoffice.accenture.com/personal/senthil_vel_murugan_accenture_com/Documents/refer/bright/bright/Guides/BHF%20-%20VM%20Build%20guide%20v1.0.docx#_Toc93703323)

[7 Post Deployment 8](https://myoffice.accenture.com/personal/senthil_vel_murugan_accenture_com/Documents/refer/bright/bright/Guides/BHF%20-%20VM%20Build%20guide%20v1.0.docx#_Toc93703324)

[8 Joining the VM to Domain 18](https://myoffice.accenture.com/personal/senthil_vel_murugan_accenture_com/Documents/refer/bright/bright/Guides/BHF%20-%20VM%20Build%20guide%20v1.0.docx#_Toc93703325)

[9 Backup onboarding 20](https://myoffice.accenture.com/personal/senthil_vel_murugan_accenture_com/Documents/refer/bright/bright/Guides/BHF%20-%20VM%20Build%20guide%20v1.0.docx#_Toc93703326)

[10 DNS Record creation 22](https://myoffice.accenture.com/personal/senthil_vel_murugan_accenture_com/Documents/refer/bright/bright/Guides/BHF%20-%20VM%20Build%20guide%20v1.0.docx#_Toc93703327)

1 Purpose

The purpose of this document is to showcase the steps involved in an Azure VM build/deployment. This document will serve as a guide for the BHF IO support team to perform future builds/deployments in the same manner.

2 Scope

The scope of this document is limited to Virtual Machines (VMs) within Azure under the BHF SAP subscription using JSON templates only.

Deployments In Scope

* Suse Linux Enterprise Server for SAP 12 SP4
* Microsoft Windows Server 2016

3 Azure Portal Pre-requisites

For the BHF subscription *BHF SAP*, one should have *Contributor* role in order to create and update objects within the subscription.

A screenshot of a computer

Description automatically generated

4 JSON template for deployment

VM deployment is carried out using JSON templates and a reference template is attached below. The same is to be reused for future deployments in accordance with the BOM sheet.

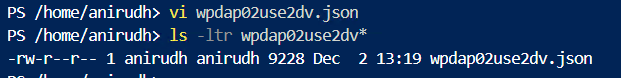


5 Deployment using Cloud Shell

Open cloud shell from the Azure portal.

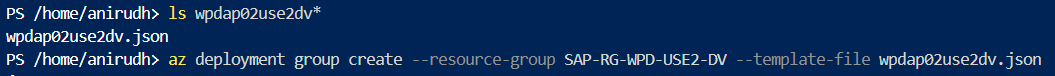
Icon to launch the Cloud Shell from the Azure portal

Create the deployment file with the hostname and the extension .json as below.

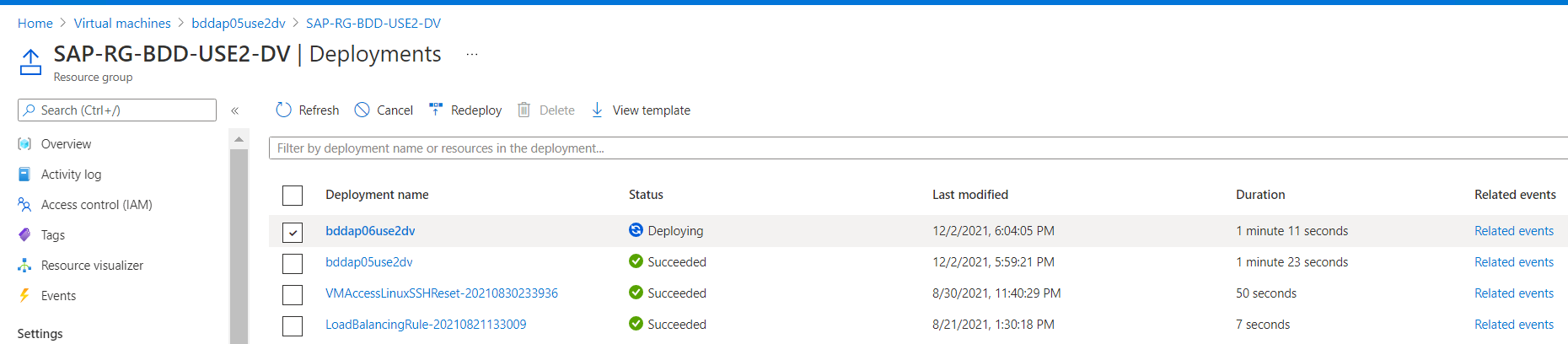


Execute the below command to begin the VM deployment.

# az deployment group create --resource-group <resource group name> --template-file <file name>.json



The deployment could be monitored from the Azure portal



6 Scale Out Deployment

As per the SAP HANA Scale out Architecture on Azure, which follows SAP HANA network recommendations, three subnets are represented within one Azure virtual network:

For client communication – In BHF we are using the DB subnet

For communication with the storage system – In BHF we are using the Stor subnet

For internal HANA inter-node communication – In BHF we are using the Data subnet

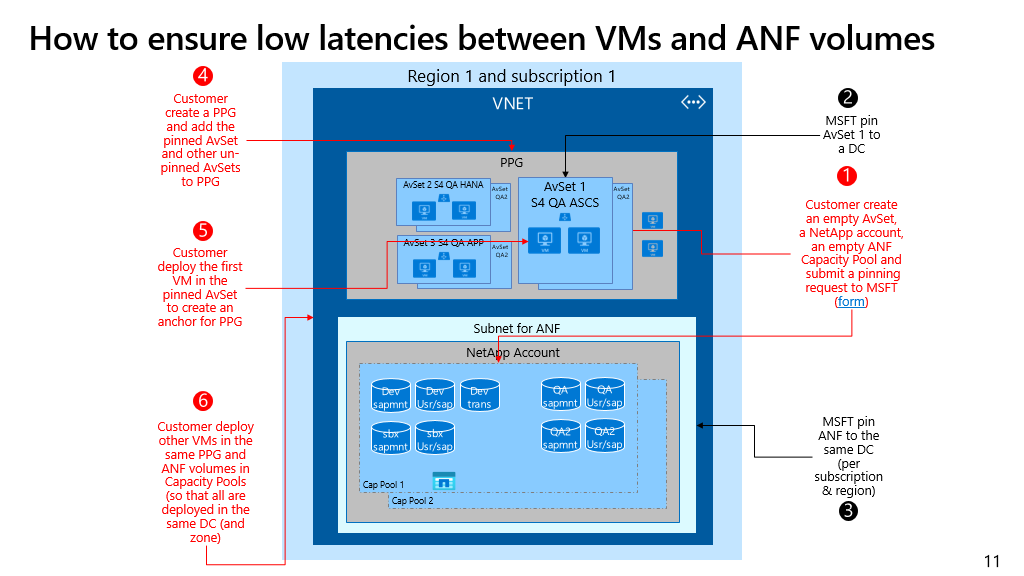
The Azure NetApp volumes are in separate subnet, delegated to Azure NetApp Files – In BHF we are using the Netapp subnet.

A screenshot of a computer

Description automatically generated

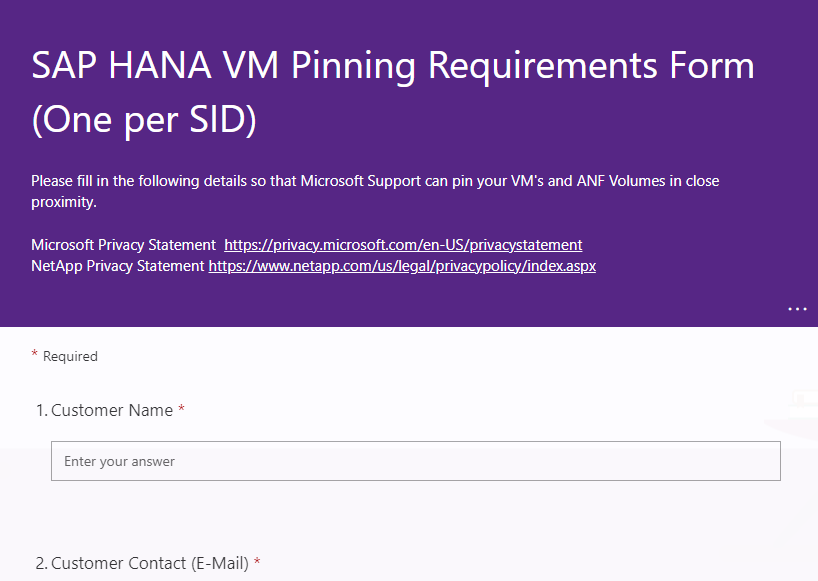
The pinning is needed only for HANA Scale deployments using ANF volumes for Data and Log volumes.

We can add the availability sets of additional HANA scale out cluster in the same PPG for future deployments, the pinning will apply by default



We need to submit the ANF pinning request to Microsoft for set it up.

<https://forms.office.com/Pages/ResponsePage.aspx?id=v4j5cvGGr0GRqy180BHbRxjSlHBUxkJBjmARn57skvdUQlJaV0ZBOE1PUkhOVk40WjZZQVJXRzI2RC4u>



Subscription ID:   
Using Zones (Yes/No):   
Region:

ANF Volume:

Resource Group AvSet:   
AvSet Name:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| VM for EIM | data | log | Backup | Shared |
| VM1 |  |  | Create |  |
| VM2 | VM1 | VM2, VM3 |  |  |
| VM3 | VM2, VM3 | VM1 |  | Create |



Please refer to the below link for the scale out deployment.

<https://docs.microsoft.com/en-us/azure/virtual-machines/workloads/sap/sap-hana-scale-out-standby-netapp-files-suse>

7 Post Deployment

**Linux:**

Post deployment tasks are automated using ansible and the following tasks are performed.

* Patching
* OS Hardening
* Installation of agents: Carbon Black, QRadar, Qualys and MyWizard
* Adding bhfworks.net to resolv.conf
* Client Interval time set to 3600 sec
* NTP sync
* kdump

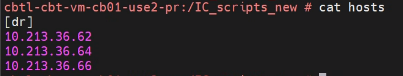
The ansible server 10.213.33.5 holds the post deployment ansible playbook under the /IC\_scripts\_new directory.



The directory houses the inventory file “hosts” to which the new build VM details should be saved under.

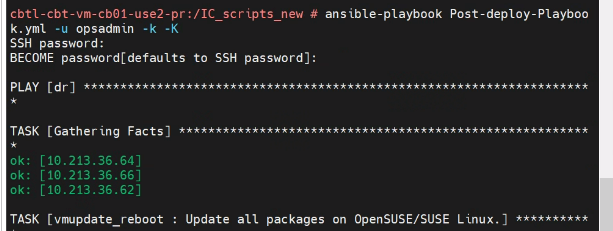


Carefully verify the IP addresses (Very Important!!)



Execute the playbook and wait for it to complete

# ansible-playbook Post-deploy-Playbook.yml -u opsadmin -k -K



The script execution starts the tasks in an order and one of the task is to reboot the VMs. This step would pause for an user intervention to approve a reboot. Press “enter” to continue with the VM reboot

A black background with a rectangular border

Description automatically generated with medium confidence

The entire process executes and exists with a summary of all succeeded and failed tasks.

**Windows:**

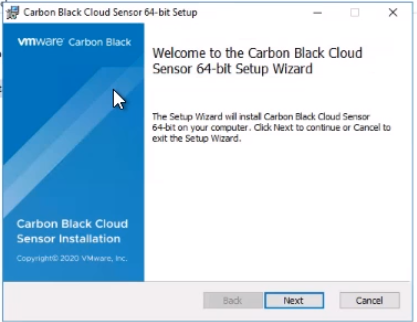
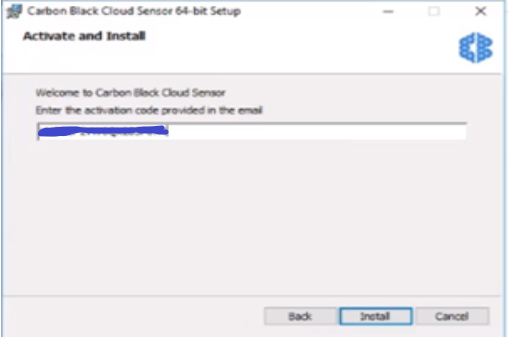
*Carbon Black:*

Before beginning with the Carbon Black (CB) sensor,

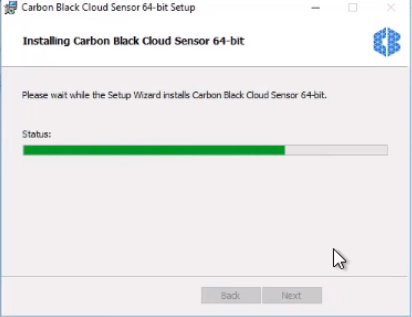
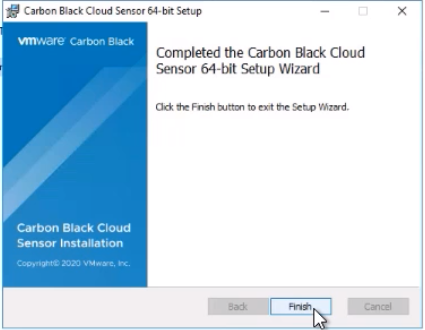
* Obtain the CB sensor kit (application)
* Obtain the Company Registration code

To get them, contact the application team as listed by end of this document.

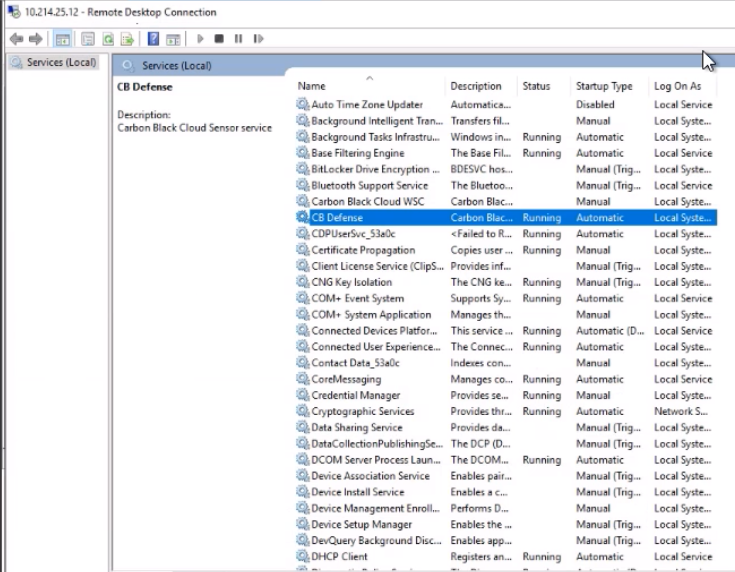
Run the Carbon Black agent executable file for windows and follow the wizard.

The activation code should be acquired from the POCs mentioned in this document.

Validate the Carbon Black service to be running.



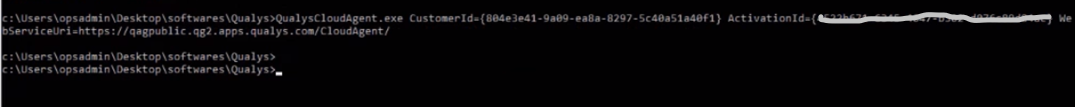
*Qualys:*

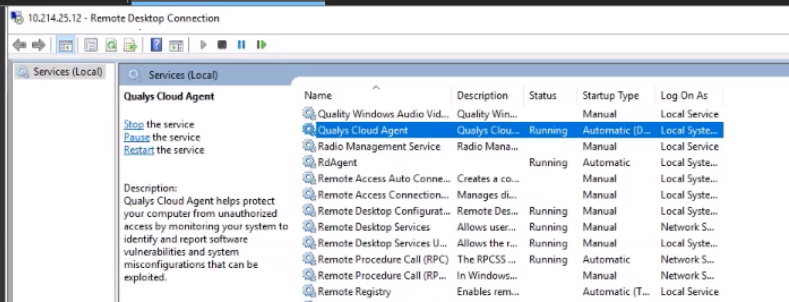
The software package for both Windows and Linux must be requested from the POCs at the end of the setup. Installation of Qualys is to be performed via command prompt.

Navigate to the directory where the agent software is placed. Run the command below.

***QualysCloudAgent.exe CustomerId={804e3e41-9a09-ea8a-8297-5c40a51a40f1} ActivationId={xxxxx-xxxxx-xxxx-xxxxx} WebServiceUri=https://qagpublic.qg2.apps.qualys.com/CloudAgent/***

Along with the softwarekit, the activation id will also be shared by the POCs.

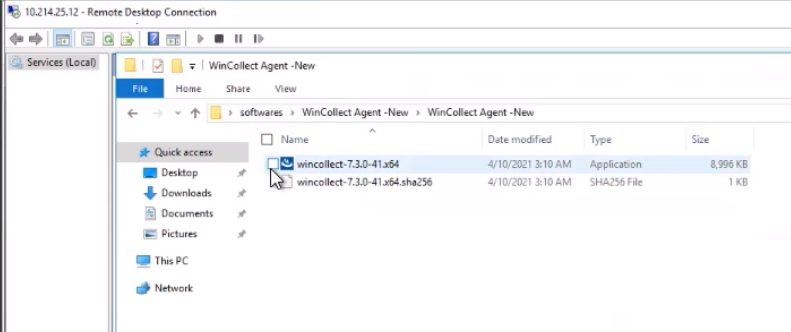


Verify the Qualys service to be running as below.

*QRadar:*

The software kit for QRadar Win Collect agent should be acquired from the POCs listed at the end of this setup.

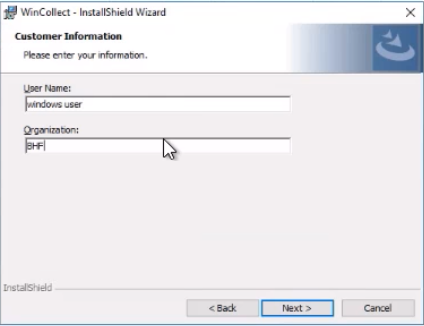
Copy the file to the target server and click to run the 64-bit version and follow the wizard.



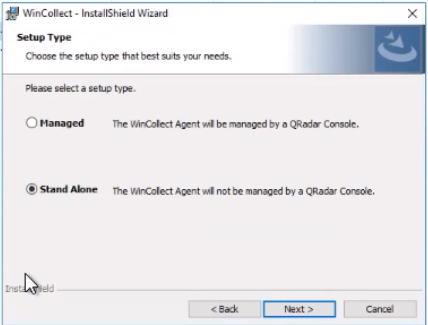
A screenshot of a computer

Description automatically generated

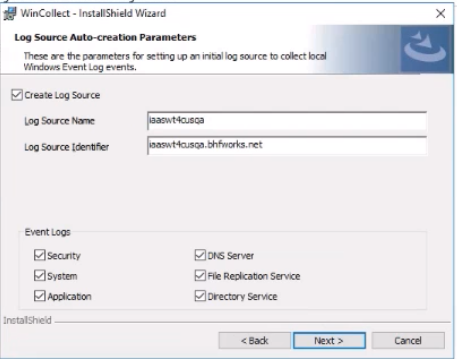
Input the details for the username and Org. as below



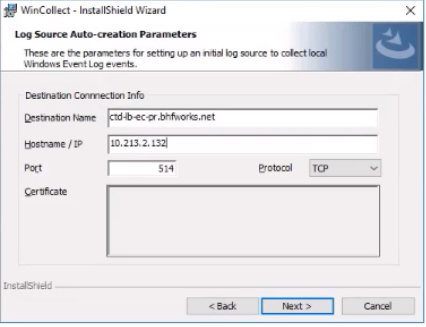
Choose standalone mode for the installation to proceed.



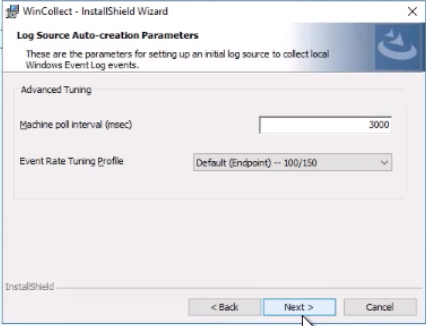
Log source name will be auto populated based on the hostname of the virtual machine. Input the identifier as below including the domain name as below. Choose the logs as below.

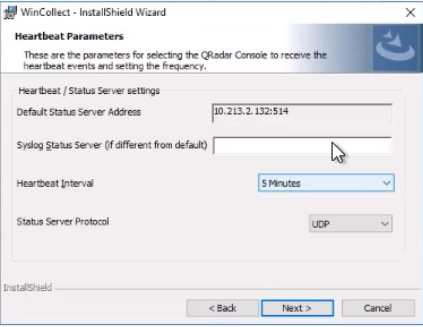


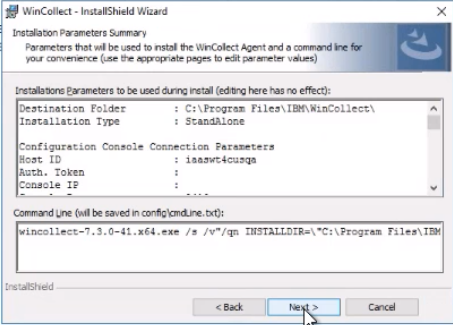
Wincollect destination Ips and DNS name is to be entered as below.

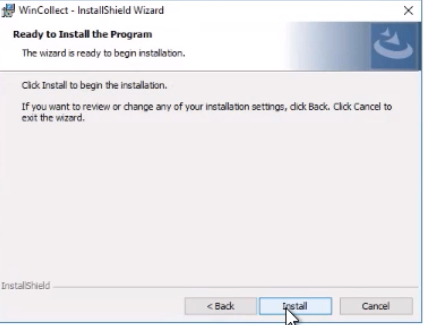


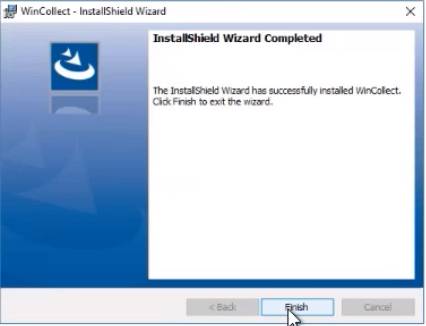
Rest of the wizard is to be followed with the default entries as below



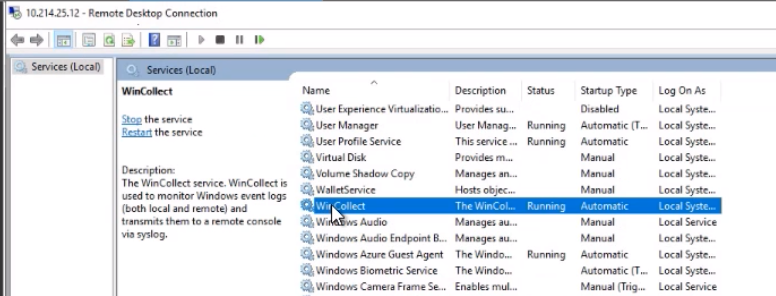








The WinCollect service shall be validated as below.



8 Joining the VM to Domain

BHF uses CyberArk for enterprise privileged access management for their IAM requirements. The domain admin id is CyberArk\_DA11 and the password must be generated every time whenever there is a requirement to join a VM to the BHF domain: BHFWORKS.NET.

The password once generated will be active for 12 hours post which a new password has to be generated for new objects that are to be joined to the domain.

**Linux:**

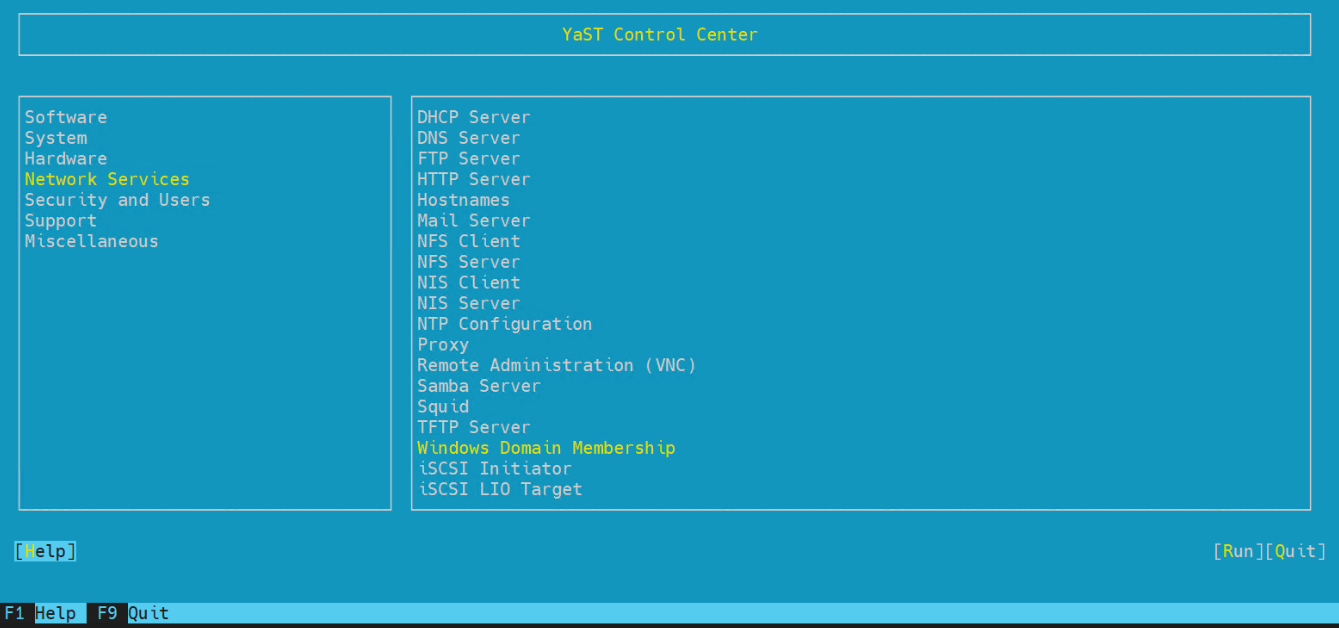
From the terminal, execute the below command to initiate domain join.

#sudo yast samba-client joindomain domain=bhfworks.net user=CyberArk\_DA11 password=<admin password>

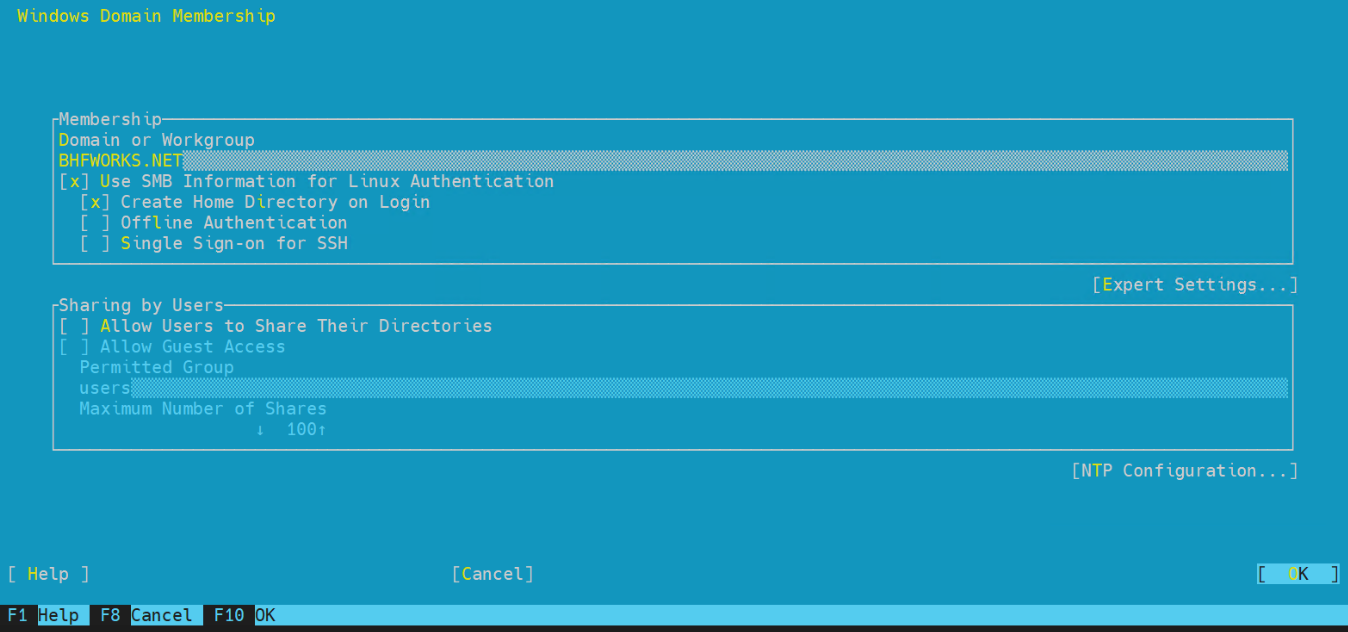
Or,

Use YAST to domain join the VM to BHFWORKS.NET

GO to yast and navigate to -> Network Services -> Windows Domain Membership

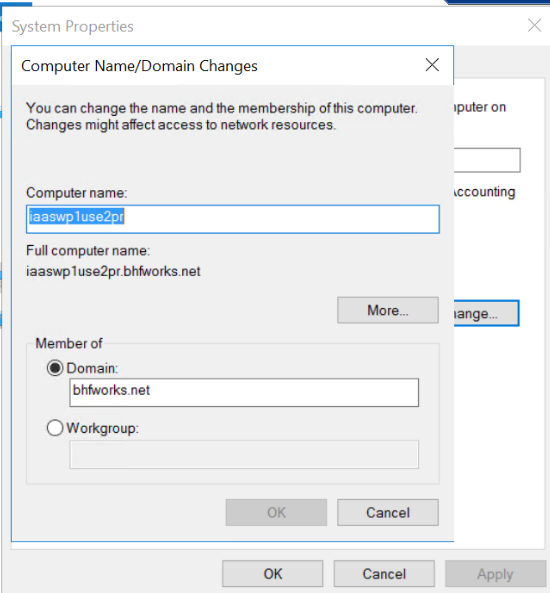


Specify the domain in the field below and save the settings. Upon saving, admin id and password prompt would appear. Key in the user id as CyberArk\_DA11 and the generated password as mention above. A reboot is to be done after the settings are saved.



**Windows:**

For Windows VMs to be joined to domain, open system properties and click on Change to see the below window. The domain is to be mentioned in the field as below and save the settings. It will prompt for the domain admin ID and password for which the id is CyberArk\_DA11 and the password is to be generated by the admin console which will be set with an expiry time of 12hours.

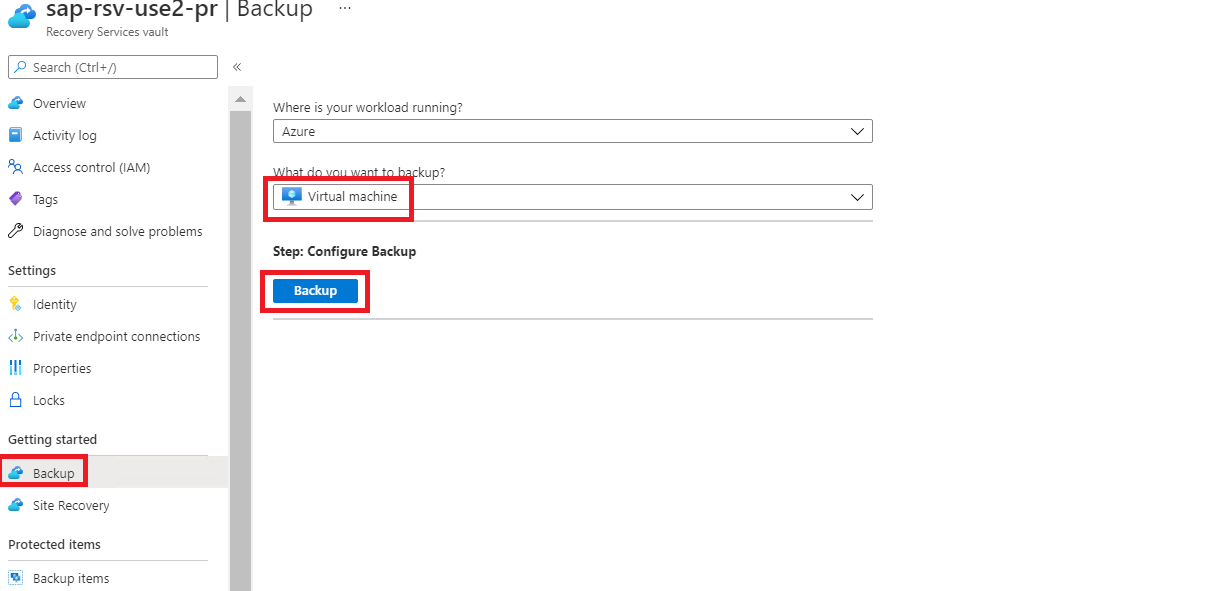


9 Backup onboarding

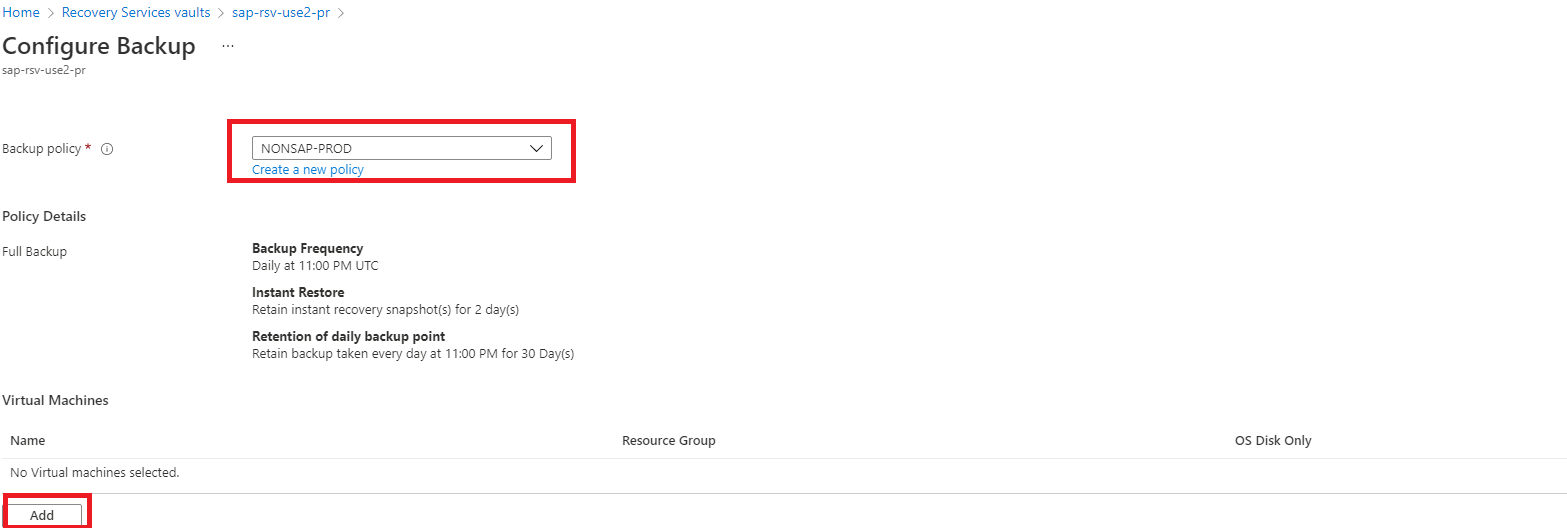
Azure recovery service Vault is solution for azure file storage backup of Virtual Machine. The data is typically copies of data, or configuration information for virtual machines (VMs), workloads, servers, or workstations. We can use Recovery Services vaults to hold backup data for various Azure services such as IaaS VMs (Linux or Windows).

**Configuration Steps:**

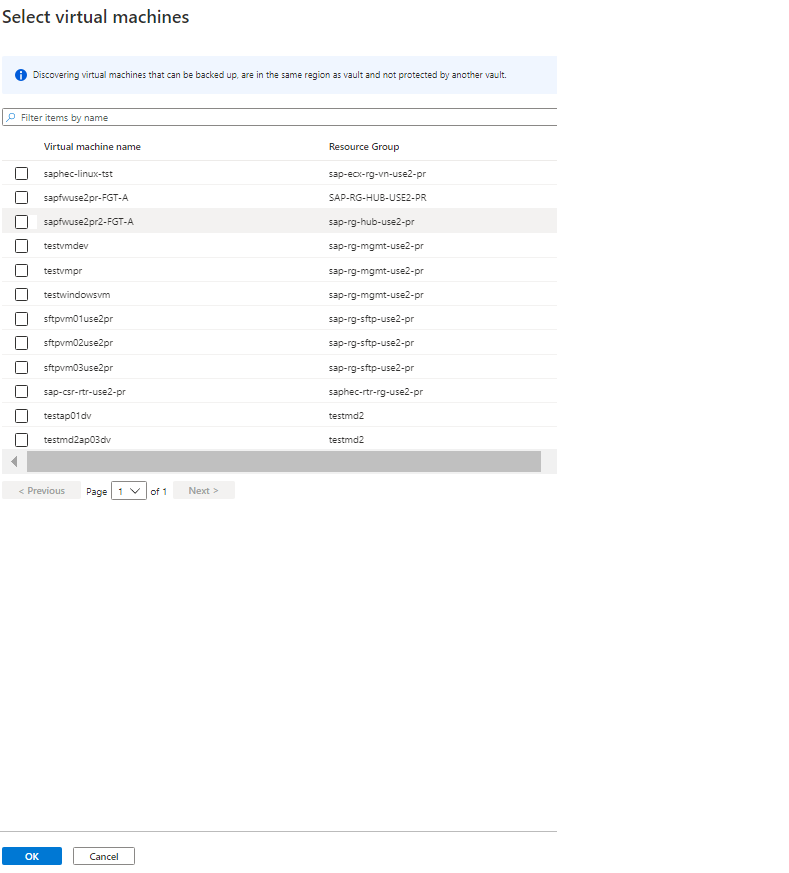
Step 1: Select The Recovery Services which you want to configure VM Backup then Click on Backup and select the Virtual machine in drop down and hit on Backup.



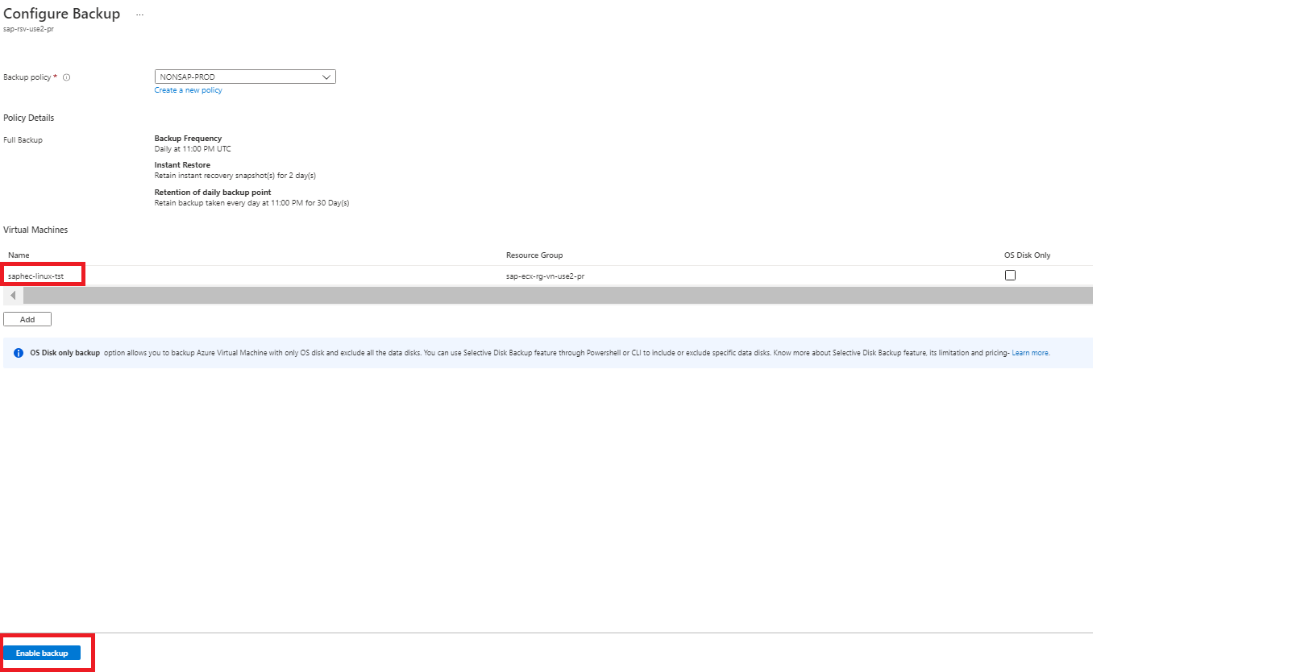
Step 2: Select the Backup Policy and click on Add button.



Step 3: Select the Virtual machine and then hit ok.



Step 4: Finally click on Enable Button to onboard the VM for Backup.



10 DNS Record creation

Generally, DNS Records are creating for Physical Host name, Virtual Host name. BHF Follows the below procedure to create the DNS Entries.

Step1:

Go to the service now link (<https://brighthouse.service-now.com/ssp?id=home>)

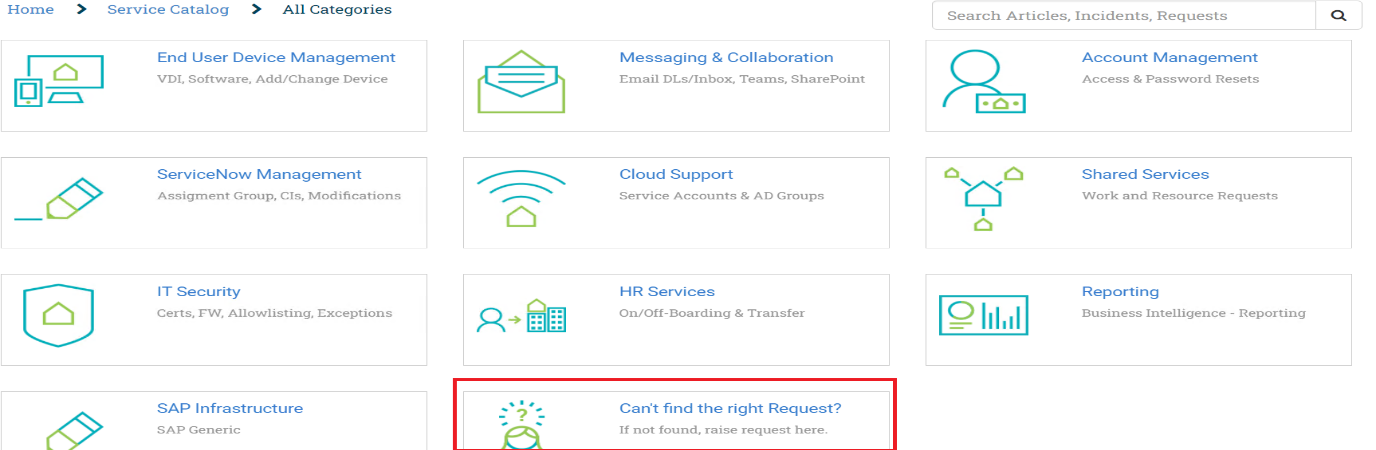
A screenshot of a computer

Description automatically generated

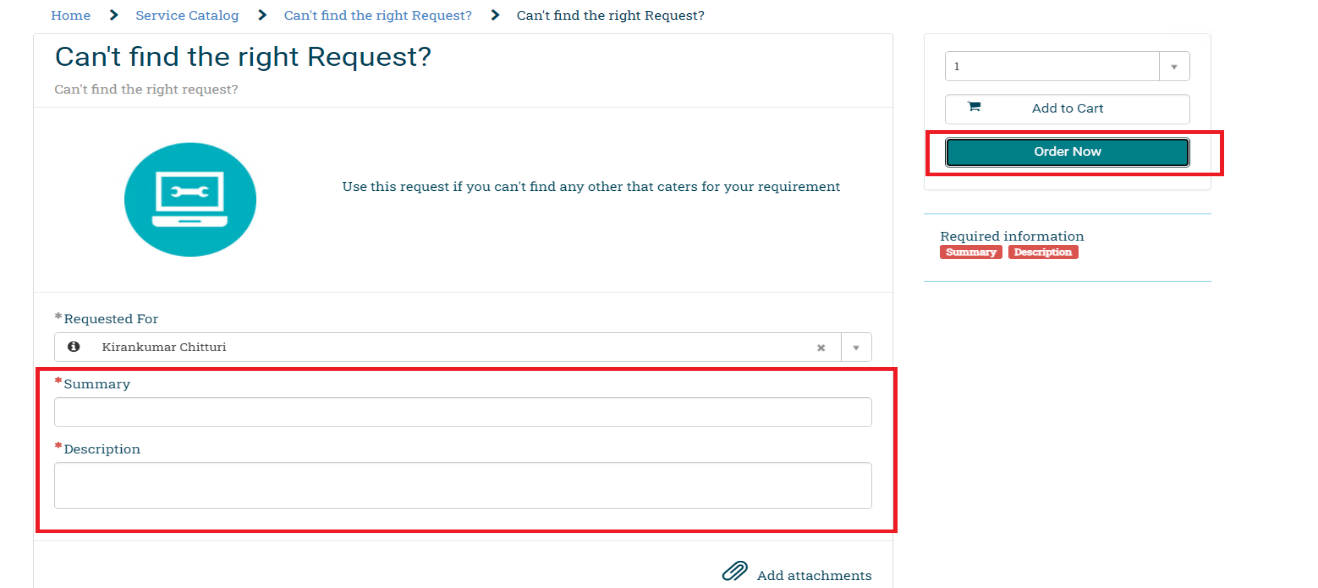
Step 2: Click on Request something.



Step 3: Then click on “Can’t find the right Request?”



Step 4: Provide the IP address and FQDN details in the ticket **description** and then hit on **Order Now**



Sample Request details:

A screenshot of a computer

Description automatically generated