NetBackup™ Marketplace Deployment on Azure Cloud

Azure

VERITAS™

NetBackup™ Marketplace Deployment on Azure Cloud

Last updated: 2022-04-22

Legal Notice

Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies. For information about our support offerings and how to contact Technical Support, visit our website:

https://www.veritas.com/support

You can manage your Veritas account information at the following URL:

https://my.veritas.com

If you have questions regarding an existing support agreement, please email the support agreement administration team for your region as follows:

Worldwide (except Japan)	CustomerCare@veritas.com
Japan	CustomerCare_Japan@veritas.com

Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The latest documentation is available on the Veritas website:

https://sort.veritas.com/documents

Documentation feedback

Your feedback is important to us. Suggest improvements or report errors or omissions to the documentation. Include the document title, document version, chapter title, and section title of the text on which you are reporting. Send feedback to:

NB.docs@veritas.com

You can also see documentation information or ask a question on the Veritas community site:

http://www.veritas.com/community/

Veritas Services and Operations Readiness Tools (SORT)

Veritas Services and Operations Readiness Tools (SORT) is a website that provides information and tools to automate and simplify certain time-consuming administrative tasks. Depending on the product, SORT helps you prepare for installations and upgrades, identify risks in your datacenters, and improve operational efficiency. To see what services and tools SORT provides for your product, see the data sheet:

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

Contents

NetBackup marketplace deployment on Microsoft Azure

This chapter includes the following topics:

- About Veritas NetBackup Marketplace deployment on Microsoft Azure
- Before you begin the deployment

About Veritas NetBackup Marketplace deployment on Microsoft Azure

Veritas NetBackup provides the integrated deployment solution on the Azure Cloud Marketplace. The integrated offer facilitates an automated deployment of NetBackup and CloudPoint components on Azure.

Supported platforms:

- NetBackup deployment on Red Hat Enterprise Linux (RHEL) 7.x
- CloudPoint deployment on Red Hat Enterprise Linux (RHEL) 7.9, 8.5 and Ubuntu 20.04

The template lets you specify the following details for the NetBackup deployment:

- Installation type: You have the flexibility of configuring the NetBackup Primary server, Media server, CloudPoint server, and Cloud Recovery Server as independent components; or configuring a combination of two or all three of the components in a single deployment.
- NetBackup license key: To be used to validate your NetBackup entitlement.

- NetBackup Usage Insights customer registration key: To be used to track your license usage and entitlement.

- Proxy settings for CloudPoint server: You can configure the CloudPoint component to be accessible through a proxy server, if required.

- Other mandatory specifications such as, the Azure instance, the virtual environment and network, and the server-specific configuration details.

This document provides the instructions for deploying Veritas NetBackup on Azure by using a solution template. The intended audience for this document includes backup administrators, cloud administrators, architects, and system administrators.

Before you begin the deployment

Before you begin deploying the NetBackup on Azure, ensure the following:

- You have an Azure account with an active subscription.

- For CloudPoint deployment, make sure you have the 'Owner' role permissions for the Azure subscription.

- You have a valid NetBackup license key.

- You have a NetBackup Usage Insights Customer Registration key for your account.

- Meet system and instance requirements. Refer to the Compatibility lists and documentation.

- Make sure that the network is appropriately configured so that different components can communicate with each other. NetBackup deployment uses private DNS zone and links a virtual network with it. In case if you select an existing private DNS zone and existing virtual network then make sure to create a DNS-vNet link before starting the deployment. For more information refer: Virtual networks link.

Deploying NetBackup on Azure Cloud using the marketplace offer

This chapter includes the following topics:

- Deploying NetBackup on Azure Cloud using the marketplace offer

- NetBackup configuration parameters

- Accessing the NetBackup Web UI

Deploying NetBackup on Azure Cloud using the marketplace offer

To deploy NetBackup on Azure cloud

1 Visit the Azure Marketplace at link.

2 Locate and access the **Veritas NetBackup** offer.

3 On the offer page, select the latest version or the version you want to deploy and click **Create**. This opens the deployment template that has different tabs for providing the basic and server-specific configuration details.

4 Refer to the individual configuration sections that correspond to the installation type you will select in the Basics tab.

Refer to basics tab sectionBasics tab

> **Note:** The configuration parameters you are asked to provide under each tab, change based on the selections you make. For example, if you select any installation type other than the 'CloudPoint server only' option, the NetBackup license key and DNS zone fields are enabled for input. There are more such fields that change dynamically depending on your selection.

Installation type 1: Primary, Media, and CloudPoint servers

Refer to this section if you are performing the full deployment that includes configuring the NetBackup Primary, Media, and CloudPoint servers, in a single deployment.

In case of full deployment, the servers are deployed in the following order:

1. Primary Server
2. Media Server
3. CloudPoint Server

The full deployment can take approximately 25 minutes.

Steps to configure:

1. Make sure that the appropriate details are provided in the Basics tab. Refer to Basics tab section.
2. Provide the Primary Sever Details. Refer to Primary Sever Details tab section.
3. Provide the CloudPoint Sever Details. Refer to CloudPoint Sever Details tab section.
4. Provide the Media Sever Details. Refer to Media Sever Details tab section.
5. Provide the Cloud Recovery Server Details. Refer to Cloud Recovery Sever Details tab section
6. Click **Review + Create** to review all the details and initiate the deployment

Installation type 2: Primary and Media servers

Refer to this section if you intend to configure the NetBackup Primary and Media servers both, in a single deployment.

Steps to configure:

1. Make sure that the appropriate details are provided in the Basics tab. Refer to Basics tabsection.
2. Provide the Primary Sever Details. Refer to Primary Sever Details tab section.
3. Provide the Media Sever Details. Refer to Media Sever Details tab section.

4. Click **Review + Create** to review all the details and initiate the deployment

Installation type 3: Primary server only

Refer to this section if you intend to configure the NetBackup Primary server only in a single deployment.

Steps to configure:

1. Make sure that the appropriate details are provided in the Basics tab. Refer to Basics tab section.

2. Provide the Primary Sever Details. Refer to Primary Sever Details tab section.

3. Provide only the Media Sever hostname. Refer to Media Sever Details tab section.

4. Click **Review + Create** to review all the details and initiate the deployment

Installation type 4: Media server only

Refer to this section if you intend to configure the NetBackup Media server only in a single deployment.

Steps to configure:

1. Make sure that the appropriate details are provided in the Basics tab. Refer to Basics tab section.

2. Provide only the Primary Sever hostname. Refer to Primary Sever Details tab section.

3. Provide the Media Sever Details. Refer to Media Sever Details tab section.

4. Click **Review + Create** to review all the details and initiate the deployment

Installation type 5: CloudPoint server only

Refer to this section if you intend to:

■ Configure the NetBackup CloudPoint server only in a single deployment.

■ Upgrade your existing CloudPoint server to the latest version.

Steps to configure:

1. Make sure that the appropriate details are provided in the Basics tab. Refer to Basics tabsection.

2. Provide the CloudPoint Sever Details. Refer to CloudPoint Sever Details tabsection.

3. Click **Review + Create** to review all the details and initiate the deployment.

Installation type 6: Cloud Recovery Server only

Refer to this section if you intend to configure the NetBackup Cloud Recovery Server only in a single deployment.

Steps to configure:

1. Make sure that the appropriate details are provided in the Basics tab. Refer to Basics tab section.

2. Provide the Cloud Recovery Sever Details. Refer to Cloud Recovery Sever Details tab section.

3. Click **Review + Create** to review all the details and initiate the deployment

NetBackup configuration parameters

Refer to the following tables and provide the configuration details depending on the type of installation you want to perform. Refer to the Installation type 1: Primary, Media, and CloudPoint servers.

Basics tab

On the Basics tab, provide the following details as required:

Table 2-1   Basics tab parameters

Parameter	Description
Project Details	
Subscription	Select the subscription ID using which you want to deploy NetBackup.
Resource group	Select from the existing resource groups under that subscription or create a new resource group
Instance Details	
Region	Select the region for the deployment.
Installation type	Select the type or a combination of NetBackup servers you want to deploy, based on the requirement.

Table 2-1   Basics tab parameters *(continued)*

Parameter	Description
Username	Provide the username that will be used for logging into the virtual instance. Same username will be used to log into the NetBackup Primary server Web UI.
Authentication type	Either select Password or SSH public key as the type of authentication. While deploying Primary server, you should use password authentication.
	If you have selected **Authentication type as SSH** while configuring the Primary server, you need to access the Primary server using SSH key and then set the password for the user to login to Web UI.
If Password is selected: ■ Password ■ Confirm password	Provide and confirm the password for the username previously provided.
SSH public key (if SSH public key is selected)	Provide a public SSH key to be used for authenticating the connection with the instance. Learn more about creating and using SSH keys in Azure
License key (not applicable for 'CloudPoint sever only' option)	Provide your NetBackup license key. When copy/pasting the license key, ensure that it is copied completely, including the hyphens. See NetBackup licenses
Use existing DNS zone	Select whether you want to use an existing DNS zone or create a new one to resolve hostnames of the deployment components.
	Note: This deployment uses/creates a private Azure DNS zone. So, to make the hostnames contained within the virtual networks inside a private DNS zone resolvable from the Internet, you must create a link between a private DNS zone and a virtual network. See About Virtual Network links
■ If Yes is selected above: Select existing private DNS zone ■ If No is selected above: Provide new DNS zone name	■ Select from the existing, private DNS zones. ■ Provide a name for the new DNS zone to be created.

Primary Sever Details tab

If you have chosen the installation type that includes the NetBackup Primary server deployment, provide the following details as appropriate.

Table 2-2   Primary Sever parameters

Parameter	Description
Primary server configuration details	
Hostname	Provide the hostname for the primary server.
Server size	Select size to be allocated for the primary server. The default size is 1x Standard DS4 v2, which you can change if required.
Usage Insights registration key	Upload a JSON file containing the NetBackup Usage Insights customer registration key. File name example: `veritas_customer_registration_key.json` See Veritas Usage Insights documentation.
Service username	Provide a 'service user' name. Most services on the server will run as this user. If a non-root username is provided, then the user will be created, and associated with the 'nbwebgrp' user group as the secondary group. Refer to "Running NetBackup services with non-privileged user (service user) account" in the "*Veritas NetBackup Security and Encryption Guide*"
Configure virtual networks	
Virtual network	Select an existing virtual network or create a new one.
Subnet	Select an existing subnet or create a new one, in which to deploy the primary server.
Public IP (optional)	Select an existing public IP or create a new one, if you want to access the primary server from outside the private network.

Media Sever Details tab

If you have chosen the installation type that includes the NetBackup Media server deployment, provide the following details as appropriate.

Table 2-3   Media Sever parameters

Parameter	Description
Media server Configuration Details	
Media server hostname	Provide the hostname for the Media server.
Server size	Select the size to be allocated for the media server. The default size is 1x Standard DS4 v2, which you can change if required.
Use same virtual network as primary server	Select from Yes or No. If Yes is selected, the Media server will be deployed in the same virtual network and subnet as that of the primary server and no additional network details are required.
	If No is selected, configure a new virtual network and subnet where the Media server should be deployed. See the next section.
Token for media server installation (applicable for 'Media server only' option)	Enter the NetBackup authorization token key for the media server generated from an existing primary server. See Creating authorization tokens.
Configure virtual networks	
Virtual network	Select an existing virtual network or create a new one.
Subnet	Select an existing Subnet or create a new one, in which to deploy the Media server.
Public IP (optional)	Select an existing public IP or create a new one, if you want to access the media server from outside the private network.

CloudPoint Sever Details tab

If you have chosen the installation type that includes the NetBackup CloudPoint server deployment, provide the following details as appropriate.

Table 2-4   CloudPoint Sever parameters

Parameter	Description
System settings	
Virtual machine name	Provide the name for the Azure VM that is being provisioned, on which the CloudPoint server will be deployed. The VM name will be used as a short hostname of the instance.

Table 2-4   CloudPoint Sever parameters *(continued)*

Parameter	Description
Virtual machine OS type	Select the OS that should be configured on the VM
Virtual machine size	Select the size of the VM to be provisioned. The default size is 1x Standard B2ms, which you can change if required.
Upgrade from an existing CloudPoint instance? (applicable only for 'CloudPoint server only' option) If Yes is selected: CloudPoint data disk	Select Yes only in case of an upgrade. Provide the name of an existing CloudPoint data volume, which has the /cloudpoint directory and its contents.
Data disk size	Specify the data disk size to be provisioned, in GB. Minimum required size is 64 GB.
Network settings section	
Use same virtual network as primary server (not applicable for CloudPoint only deployments)	Select from Yes or No. If Yes is selected, the CloudPoint server will be deployed in the same virtual network and subnet as that of the primary server and no additional network details are required. If No is selected, configure a new virtual network and subnet where the CloudPoint server should be deployed. See the next section.
Configure virtual networks	
Virtual network	Select an existing virtual network or create a new one.
Subnet	Select an existing Subnet or create a new one, in which to deploy the CloudPoint server.
Public IP (optional)	Select an existing public IP or create a new one, if you want to access the CloudPoint server from outside the private network.
Domain name label (if Public IP is provided)	Provide a globally unique domain name label to resolve with the public IP provided above
Inbound access CIDR (optional)	If the CloudPoint server is deployed in a network which is different from NetBackup's network, then you may provide the CIDR block from which the CloudPoint server can access NetBackup.

Table 2-4 CloudPoint Sever parameters *(continued)*

Parameter	Description
Proxy settings (optional)	
HTTP proxy	Provide the HTTP proxy value to configure CloudPoint with proxy server.
HTTPS proxy	Provide the HTTPS proxy value to configure CloudPoint with proxy server.
No proxy	Specify the hosts that should be allowed to bypass the proxy server. You can mention multiple, comma-separated values. Eexample: `localhost,mycompany.com,192.168.0.10:80`
Configuration details (not applicable if upgrading from an older CloudPoint version)	
Enable HA for CloudPoint	Select Yes, if you want to take the snapshot of the CloudPoint server once daily and store the snapshot in the same resource group, the stored snapshots can be used for recovering or upgrading CloudPoint. In this option CloudPoint will be deployed in a vVM scale set. If you select yes, provide Tenant ID, Client ID, and Secret Key values of the subscription where CloudPoint is being deployed.
CloudPoint Username	Specify a username for the CloudPoint administrator user account to be created.
CloudPoint Password	Specify a password for the CloudPoint administrator user.
Confirm CloudPoint Password	Confirm the administrator user password.
Port	Select the port through which the CloudPoint server can communicate. Default is port 443.
Tenant ID	Specify the ID of the AAD directory in which you created the application.
Client ID	Specify the application ID.
Secret key	Specify the secret key of the application.
Primary server details (Applicable only if you choose to freshly install a 'CloudPoint server only'. Not applicable for upgrading a CloudPoint server.)	

Table 2-4 CloudPoint Sever parameters *(continued)*

Parameter	Description
Need to register with existing Primary?	Select if you want to register the CloudPoint server with the primary server during the deployment. If selected, then provide further details.
Primary server FQDN	Provide a Fully Qualified Domain Name of the existing primary server to which the CloudPoint server needs to be associated. Configuration fails if the FQDN is not resolvable from this CloudPoint server.
Primary server API key	As a NetBackup user, provide a valid API key generated from the existing primary server to validate the communication between the Primary server and the CloudPoint server. The user who generates API keys must have the permission to add the CloudPoint server. See "Creating and managing API keys for users (Administrators)" and "Adding and managing your API key (Users)" in the *NetBackup Web UI Administrator's Guide*.

Cloud Recovery Sever Details tab

If you have chosen the installation type that includes the NetBackup Cloud Recovery Server deployment, provide the following details as appropriate.

Table 2-5 Cloud Recovery Server parameters

Parameter	Description
Hostname	Provide the short hostname of the Cloud Recovery Server. Hostname must be entered in lower case and must not start with '-' or digit.
Server size	Select Cloud Recovery Server size. Enter URL of Primary Data disk available in a storage account.
Data Disk Size in GB	Enter the desired size for the attached data disk (in GB). Minimum is 200GB.
Usage Insights registration key	Upload a JSON file containing the NetBackup Usage Insights customer registration key for the Server installation.

Table 2-5   Cloud Recovery Server parameters *(continued)*

Parameter	Description
Service username	Provide a 'service user' name. If a non-root user is provided, then a user will be created and added in nbwebgrp as the secondary group.
Storage Account Name	Provide name of the Storage Account where MSDP images are stored.
Access Key	Provide Access key for the Storage Account.
Container Name	Provide name of the Container where MSDP images are stored.
Sub-Folder Name	Provide name of the sub folder inside the container where MSDP images are stored.
Configure virtual networks	
Virtual network	Select an existing Virtual Network or create a new one.
Subnet	Select an existing Subnet or create a new one.
Public IP (Optional)	Select or create a public IP if you want to access the server from outside the private network, otherwise choose 'None'. (Optional)

Accessing the NetBackup Web UI

After the successful deployment, you can access the NetBackup Web UI if you are an authorized user.

1. Open a web browser and enter the following URL with an appropriate hostname.

    https://<primaryserver>/webui/login

    The Web UI *primaryserver* can only be accessed using the hostname of the NetBackup Primary server that you have deployed.

2. Enter the username and password (Authentication Type field) provided on Basic tab to login to NetBackup web UI.

    Refer to Basic tab for more details. Basics tab

There are more ways to access the NetBackup Web UI. Refer to section "Sign in to the NetBackup web UI" in the latest version of *NetBackup Web UI Administrator's Guide*, and start managing and protecting your assets.

Managing CloudPoint deployment

This chapter includes the following topics:

- Upgrading CloudPoint
- Migrating CloudPoint from RHEL 7.x to RHEL 8.x
- Recovering CloudPoint VM

Upgrading CloudPoint

For upgrading the CloudPoint server, you will need to perform the steps from the Azure portal and the Azure marketplace deployment template.

Perform the following steps from the Azure portal:

1. Note the OS of the CloudPoint VM. This would be required later in step 10.

2. Stop the existing CloudPoint VM. While stopping the VM select the option to reserve the public IP address, if associated.

3. Disassociate the public IP address of the CloudPoint VM, if associated. Also note the IP address name as it would be required later in step 14.

4. Detach the data disk. Note the data disk name as it would be required later in step 12.

5. Delete the CloudPoint VM. Note the VM name as it would be required later in step 9.

6. Delete and purge the associated CloudPoint's key vault if it exists. Ensure that you purge the key vault after deletion as it would be in soft-delete state after deletion and may cause failure while upgrading.

Perform the following steps from the NetBackup 10.0 deployment template:

7. Select the **CloudPoint only** deployment.

8. Select the same Resource Group and Region as that of the older CloudPoint deployment.

9. Use the same CloudPoint VM name as that of the older CloudPoint VM. This is the same VM name as noted in step 5.

10. Select the same OS as that of the older CloudPoint VM that was noted in step 1.

11. Select **Yes** for the **Upgrade from an existing CloudPoint instance** option.

12. Provide the data disk name that was detached in step 4.

13. Perform the deployment in the same Virtual Network and Subnet as that of the older CloudPoint VM.

14. Assign the same public IP, if there was any IP associated earlier and was dissociated in step 2.

15. Click **Review and create** to start the CloudPoint upgrade process.

Note: If CloudPoint was registered with NetBackup using the private IP or an internal FQDN before upgrade, then ensure the same private IP address and internal FQDN are associated with the upgraded CloudPoint VM.

Migrating CloudPoint from RHEL 7.x to RHEL 8.x

CloudPoint can be migrated only from RHLE 7.x to RHEL 8.x. For migration, follow the same steps as described in the Upgrading CloudPoint section, except that in step 10, select the OS as RHEL 8.

Recovering CloudPoint VM

To enable High Availability (HA) for CloudPoint you must configure the plugin at the time of deployment, by providing TenantID, ClientID and SecretKey of CloudPoint Application. HA for CloudPoint performs regular snapshot of CloudPoint meta data disk for the instance deployed through marketplace.

This internally creates a CloudPoint policy *backupsnapmgr*. It creates a disk level snapshots (daily once) and keeps three of the most recent copies. Hence, the disk snapshots created as a part of this policy run would have its name start with *backupsnapmgr**.

If you want to restore your CloudPoint server using these snapshots, you can search the snapshots with the string *backupsnapmgr**, sort the filtered snapshots based on their **Creation Time** and identify the one that you want to use for restoring the CloudPoint.

Once you identify the snapshot in the cloud, you can follow the steps mentioned below.

Recovering CloudPoint using Azure Marketplace deployment

◆ Recover theCloudPoint deployed from Azure Marketplace with HA enabled in 10.0.

In this case, the CloudPoint is deployed on a VM Scale Set (VMSS) and regular snapshots of CloudPoint are taken once daily and snapshot copies are maintained up to last 3 days.

- **If you want to recover from the latest CloudPoint Snapshot:**
  Delete the CloudPoint instance in the VMSS which you want to recover. This would automatically create a new CloudPoint instance in the VMSS which would have the CloudPoint data disk, created from the latest snapshot (*backupsnapmgr**).

- **If you want to recover from an older CloudPoint Snapshot:**
  - a. Create a disk from the CloudPoint Snapshot you want to recover.
  - b. Note the operating system of the CloudPoint VM.
  - c. Stop the existing CloudPoint VM. While stopping the VM, select the option to reserve the public IP address, if associated.
  - d. Disassociate the public IP address of the CloudPoint VM, if associated and note the IP address name.
  - e. Note the VM name and delete the CloudPoint VM.
  - f. Delete and purge the associated CloudPoint's key vault if it exists. Ensure that you purge the key vault after deletion as it would be in soft-delete state after deletion and may cause failure while upgrading.
  - g. Launch the Veritas NetBackup 10.0 Cloud Marketplace Deployment in Azure.
  - h. Select the CloudPoint only deployment.
  - i. Select the same **Resource Group** and **Region** as that of the older CloudPoint deployment.
  - j. Use the same CloudPoint VM name as that of the older CloudPoint VM. This is the same VM name as noted in step e.
  - k. Use the existing DNS zone name, which was used in the original CloudPoint deployment.
  - l. Select the same OS as that of the older CloudPoint VM that was noted in step b.
  - m. Select **Yes** for the Upgrade from an existing CloudPoint instance option.

- n. Provide the disk name created from snapshot in step a.

- o. Perform the deployment in the same Virtual Network and Subnet as that of the older CloudPoint VM.

- p. Assign the same public IP, if there was any IP address associated earlier and was dissociated in step d.

- q. Click **Review and create** to start the CloudPoint upgrade process.

Regenerate CloudPoint certificates

To regenerate the CloudPoint certificates with the new IP address / hostname, perform the following steps.

Regenerate the certificate

1 Execute the certificate regeneration script:

```
# docker run -it --rm -v /cloudpoint:/cloudpoint --entrypoint
"/cloudpoint/scripts/cp_regenerate_certs.sh"
veritas/flexsnap-cloudpoint:10.0.0.0.9818 -i
<new-ip-address-1>,<new-ip-address-2> -h
<cloudpoint-hostname-1>,<cloudpoint-hostname-2>
```

Note: 1. Here, *10.0.0.0.9818* represents the CloudPoint version. Replace it as per your currently installed product version.

Note: 2. This is a single command. Ensure that you enter the command without any line breaks.

Note: 3. Note the change in the entrypoint in the above command.

Note: 4. Also note that you can pass multiple comma-separated IP addresses using '-i' argument and multiple comma-separated hostnames using '-h' argument.

---

2 Restart the CloudPoint services:

```
# docker run -it --rm -v /cloudpoint:/cloudpoint -v
/var/run/docker.sock:/var/run/docker.sock
veritas/flexsnap-cloudpoint:10.0.0.0.9818 restart
```

When the installation completes, re-register the CloudPoint Instance with NetBackup Primary with the existing CloudPoint credentials.

Recovering the CloudPoint using manually provisioned virtual machine

You can also recover the CloudPoint using manually provisioned virtual machines.

Recover the CloudPoint manually

1   Using your Azure Portal, create a disk from the snapshot identified earlier, in the region where you want to create the CloudPoint instance.

2   Create a new virtual machine with specifications equal to or higher than your previous CloudPoint server.

3   Install docker on the new server. Docker and other system related requirements can be found in the CloudPoint 9.1.2 Install Guide.

4   Attach the newly created volume to this CloudPoint server instance.

5   Create the `/cloudpoint` mount directory on this server using the command:`#`
    `mkdir /cloudpoint`

6   Login to the newly created CloudPoint instance. After identifying the device path of the newly attached volume in Step 1, mount the same to the `/cloudpoint` directory you just created by using the command: `# mount <device-path> /cloudpoint`

7   Verify that all CloudPoint related configuration data are in the directory by using the command:`# ls -l /cloudpoint`

8   Download or copy the CloudPoint installer binary to the newly created CloudPoint server instance.

9 Install the CloudPoint using the following command:

```
# sudo docker run -it --rm -v /cloudpoint:/cloudpoint -v
/var/run/docker.sock:/var/run/docker.sock
veritas/flexsnap-cloudpoint:10.0.0.0.9818 install
```

10.0.0.0.9818 represents the CloudPoint version. Replace it as per your currently installed product version.

Note: This is a single command. Ensure that you enter the command without any line breaks. The installation program detects an existing version of CloudPoint and re-installs all theCloudPoint services without overwriting existing content.

Following message is displayed on the command prompt: `Configuration started at time Sun May 30 22:20:47 UTC 2021`

10 In the case where a static external IP address is not assigned to the newly created instance, the IP address changes after creating a new machine. You need to regenerate the certificates.

To regenerate the CloudPoint certificates with the new IP address / hostname, perform the following steps.

- **Run the certificate regeneration script:**

```
# docker run -it --rm -v /cloudpoint:/cloudpoint --entrypoint
"/cloudpoint/scripts/cp_regenerate_certs.sh"
veritas/flexsnap-cloudpoint:10.0.0.0.9818 -i
<new-ip-address-1>,<new-ip-address-2> -h
<cloudpoint-hostname-1>,<cloudpoint-hostname-2>
```

Note: i. Note the change in the entrypoint in the above command.

Note: ii. Note that you can pass multiple comma-separated IP addresses using '-i' argument and multiple comma-separated hostnames using '-h' argument.

- **Restart CP services:**

```
# docker run -it --rm -v /cloudpoint:/cloudpoint -v
/var/run/docker.sock:/var/run/docker.sock
veritas/flexsnap-cloudpoint:10.0.0.0.9818 restart
```

Troubleshooting NetBackup Deployment

This chapter includes the following topics:

■ Troubleshooting scenarios

Troubleshooting scenarios

1. Deployment fails with the error:

```
"{"code":"InvalidResourceLocation","message":"The resource 'CPVnet'
already exists in location 'westus2' in resource group 'CP_dev'. A
resource with the same name cannot be created in location 'centralus'.
Please select a new resource name."}".
```

Explanation:

When you select an existing RG for deployment and existing VNet which is from another RG but has a same name as a Vnet in this RG then, validation fails with conflicts. For example:

■ You choose to deploy in CP_dev which is an existing RG which has CP_VNet as a virtual network in West US 2

■ Then in the region parameter you choose region as Central US, so all your resources are deployed in central US and are linked to RG: CP_dev

■ In the networking section you choose an existing VNet, i.e. CP_VNet from another RG: demoRG, which is in Central US (as this the location selected in above step, so all VNets in central US region are listed).

In the above scenario the validation fails with conflicts saying it cannot create a VNet with same name as existing VNet CP_VNet in another region.

Solution:

Try to deploy in an RG which does not have a VNet with the same name as the existing VNet that you want to select.

2. Deployment fails with the error:

```
"{"code":"InvalidResourceLocation","message":"The resource 'PublicIp'
already exists in location 'centralindia' in resource group 'CP_dev'.
A resource with the same name cannot be created in location
'centralus'. Please select a new resource name."}".
```

Explanation:

When you select an existing RG for deployment which has a public IP address as 'publicIP' (i.e. default public IP address of arm template) and you select to deploy without any public IP address then validation fails with conflicts. For example:

- You select to deploy in CP_dev which is an existing RG which has publicIP as a public IP address in centralindia.

- Then in the region parameter you select region as Central US, so all your resources are deployed in central US and are linked to RG: CP_dev

- In the networking section you select 'none' for public IP, so that deployment would not have any public IP address.

In the above scenario the validation fails with conflicts saying it cannot create a public IP address with same name as existing public IP "publicIP" in another region.

```
"{"code":"InvalidResourceLocation","message":"The resource 'PublicIp'
already exists in location 'centralindia' in resource group 'CP_dev'.
A resource with the same name cannot be created in location
'centralus'. Please select a new resource name."}".
```

Solution:

Try to deploy in an RG which does not have an IP address whose name is PublicIP.

3. Deployment fails with the error:

```
"{"code":"InvalidResourceLocation","message":"The resource 'CPIP'
already exists in location 'centralindia' in resource group 'CP_dev'.
A resource with the same name cannot be created in location
'centralus'. Please select a new resource name."}".
```

Explanation:

When you select an existing RG for deployment and existing public IP address which is from another RG, but has a same name as a public IP address in this RG then, validation fails with conflicts. For example:

- You select to deploy in CP_dev which is an existing RG which has CP_IP as a public IPaddress.

- Then in the region parameter you select region as Central US, so all your resources are deployed in central US and are linked to RG: CP_dev

- In the networking section you select an existing public IP, i.e. CP_IP from another RG: demoRG, which is in Central US (as this the location you selected in the above step, so all IPs in central US region are listed).

In the above scenario the validation fails with conflicts saying it cannot create an IP address with same name as existing IP address CP_IP in another region.

```
"{"code":"InvalidResourceLocation","message":"The resource 'CPIP'
already exists in location 'centralindia' in resource group 'CP_dev'.
A resource with the same name cannot be created in location
'centralus'. Please select a new resource name."}".
```

Solution:

Try to deploy in an RG which does not have an IP address with same name as the existing IP address that you want to select.

4. Deployment fails with the error:

```
{ "status": "Failed", "error": { "code": "DeploymentFailed",
"message": "At least one resource deployment operation failed. Please
list deployment operations for details. Please see
https://aka.ms/DeployOperations for usage details.", "details": [ {
"code": "Conflict", "message": "{ \r\n \"status\": \"Failed\",\r\n
\"error\": {\r\n \"code\": \"ResourceDeploymentFailure\",\r\n
\"message\": \"The resource operation completed with terminal
provisioning state 'Failed'.\",\r\n \"details\": [\r\n { \r\n
\"code\": \"VMExtensionProvisioningTimeout\",\r\n \"message\":
\"Provisioning of VM extension ExtensionForConfiguringCP has timed
out. Extension provisioning has taken too long to complete. The
extension last reported \\\"Plugin enabled\\\".\\r\\n\\r\\nMore
information on troubleshooting is available at
https://aka.ms/VMExtensionCSELinuxTroubleshoot\"\r\n } \r\n ]\r\n
}\r\n}" }, { "code": "NotFound", "message": "{ \r\n \"error\": {\r\n
\"code\": \"ParentResourceNotFound\",\r\n \"message\": \"Can not
perform requested operation on nested resource. Parent resource
'cpzbxyjundfpwc2-kv' not found.\"\r\n }\r\n}" } , { "code":
"Conflict", "message": "{\r\n \"error\": { \r\n \"code\":
\"ConflictError\",\r\n \"message\": \"Exist soft deleted vault with
the same name. \"\r\n }\r\n} " } ] }}
```

Explanation:

If you delete an old CloudPoint deployment and its resources and immediately start a new deployment with the same VM name for CloudPoint as earlier, you face this issue as the Keyvault created in the earlier deployment is in soft-delete state, and the new deployment tries to create a key-vault with same name.

Solution:

Purge the Key-vault and attempt again. Or try the deployment with a new VM name for CloudPoint.

5. Unable to add Azure provider, when CloudPoint is deployed behind a Proxy

Explanation:

CloudPoint is unable to access azure.com, microsoftonline.com

Solution:

Set azure.com, microsoftonline.com values for noproxy during CloudPoint deployment.

6. Provisioning of VM extension NB-Primary timed out

```
Installation has timed out. Extension provisioning has taken too long
to complete.
```

Explanation:

Installation of primary or media server failed because of some issue. To check the issue, login to the instance and switch to the root user using commaNetBackupnd 'sudo su'. You can check logs at location /root/NBSetup/userdata.log.

7. component upgrade failure

Explanation:

If you are trying to upgrade a NetBackup component till version 9, which was deployed through Azure marketplace then, you may get a following error:

```
Unable to configure target host.

ERROR: bpnbaz failed with status [68]. The authentication broker
could not be configured. Review the NetBackup Security and Encryption
Guide for more information.
```

Solution:

Add an entry in the /etc/hosts file for 'private_ip' 'short_hostname' mapping. This happens when the server cannot resolve a short hostname while upgrade. After adding an entry restart the upgrade.

8. Deployment fails with the error:

```
{ "status": "Failed", "error": { "code": "PrincipalNotFound",
"message": "Principal 55535faac7f748a2b8a1b080518b3df3 does not exist
in the directory fc8e13c0-422c-4c55-b3ea-ca318e6cac32." } }
```

Explanation:

This error may happen when Azure is speedily processing the template and tries to assign authorization to the VM to access key vault when the VM is not yet completely formed.

Solution:

Delete the resources formed in the deployment, purge the key vault if formed, and retry the deployment.

9. Backup from Snapshot job fails with errors:

Jun 10, 2021 2:17:48 PM - Error mqclient (pid=1054) SSL Connection failed with string, broker:<hostname> Jun 10, 2021 2:17:48 PM - Error mqclient (pid=1054) Failed SSL handshake, broker:<hostname> Jun 10, 2021 2:19:16 PM - Error nbcs (pid=29079) Invalid operation for asset: <asset_id> Jun 10, 2021 2:19:16 PM - Error nbcs (pid=29079) Acknowledgement not received for datamover <datamover_id>

and/or

```
Jun 10, 2021 3:06:13 PM - Critical bpbrm (pid=32373) from client
<asset_id>: FTL - Cannot retrieve the exported snapshot details for
the disk with UUID:<disk_asset_id> Jun 10, 2021 3:06:13 PM - Info
bptm (pid=32582) waited for full buffer 1 times, delayed 220 times
Jun 10, 2021 3:06:13 PM - Critical bpbrm (pid=32373) from client
<asset_id>: FTL - cleanup() failed, status 6
```

Explanation:

This can happen when the inbound access to CloudPoint on port 5671 and 443 port gets blocked at the OS firewall level (firewalld). Hence, from the datamover container (used for the Backup from Snapshot jobs), communication to CloudPoint gets blocked. This results in the datamover container not being able to start the backup.

Solution:

Modify the rules in OS firewall to allow the inbound connection from 5671 and 443 port.

10. Discovery fails after CloudPoint has been recovered by deleting instance in VM scale set

Explanation:

A manual entry in NetBackup Primary and Media's `/etc/hosts` folder with private IP address of CloudPoint for Backup from Snapshot to work is made. Since the new CloudPoint came up with a new private IP address, NetBackup is not able to find CloudPoint at the old IP address that it has in its `/etc/hosts`.

Solution:

Update `/etc/hosts` on both NetBackup Primary and Media with CloudPoint' s new private IP address.