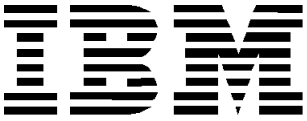
IBM® Storage

Business Continuity Solution with Red Hat OpenShift and IBM Spectrum Virtualize for Public Cloud on Microsoft Azure



Contents

Overview

The focus of this Blueprint is to facilitate the deployment of the hybrid cloud business continuity solution with Red Hat OpenShift Container Platform (RHOCP) on Microsoft Azure Cloud and Container Storage Interface (CSI) driver plug-in for IBM Block Storage and IBM® Spectrum Virtualize for Public Cloud (SV4PC) on Microsoft Azure Cloud.

This solution is designed to protect the data by using IBM Storage-based Global Mirror Replication, and the “volume replication” feature from IBM block storage CSI driver for IBM Storage.

For demonstration purposes, MySQL containerized database is installed on the persistent volume (PV) that is created on the on-premises IBM FlashSystem® Storage. This storage is connected to the RHOCP cluster in the vSphere environment.

CSI driver plug-in for IBM Block Storage (FS9100) and SV4PC on Azure is installed on Red Hat OCP on Azure and On-premises Red Hat OCP.

The volume or logical unit number (LUN) from on-premises IBM FlashSystem Storage (FS9100) is replicated to IBM SV4PC on Microsoft Azure Cloud by using the IBM storage global mirror replication feature and the IBM CSI volume replication feature.

The information in this document is distributed on an as-is basis without any warranty that is either expressed or implied. Support assistance for the use of this material is limited to situations where IBM Spectrum® Virtualize for Public Cloud is supported and entitled, and where the issues are specific to this Blueprint implementation.

Executive summary

In today's environment, many organizations use some form of cloud services, whether private, public, or hybrid multi-cloud. Storage infrastructure is a part of these services and deployments.

For the RHOCP that is deployed on Microsoft Azure Cloud, the RHOCP installation program offers you flexibility. You can use the installation program to deploy a cluster on infrastructure that the installation program provisions and the cluster maintains. You also can deploy a cluster on infrastructure that you prepare and maintain.

IBM released its open source CSI driver, which allows dynamic storage provisioning for containers on Kubernetes and RHOCP on Azure. The IBM Spectrum Virtualize family and IBM Spectrum Virtualize for Public Cloud (SV4PC on Azure) support clients in their IT architectural transformation and migration toward the cloud service model. This transformation enables hybrid cloud strategies while maintaining the benefits and advanced functions of sophisticated storage systems.

With IBM Spectrum Virtualize and IBM Spectrum Virtualize For Public Cloud on Azure, organizations can have multi-cloud environments with data replication between the following components:

- On-premises or private cloud to public cloud (Azure Cloud)
- Two public clouds (Azure Cloud)

IBM Spectrum Virtualize for Public Cloud enables data on heterogeneous storage systems to be replicated or migrated between on-premises and Azure or AWS.

IBM Spectrum Virtualize and IBM Spectrum Virtualize for Public Cloud together support mirroring between on-premises and cloud data center or between cloud data center.

These functions can be used to:

- Migrate data between on-premises and public cloud data center or between a public cloud data center. Data management is consistent between on-premises storage and the public cloud.
- Implement disaster recovery strategies between on-premises and public cloud data center.
- Enable cloud-based DevOps with easy replication of data from on-premises sources.

Scope

The focus of this document is to provide a business continuity solution for the containerized MySQL database running on RHOCP at on-premises data centers. The MySQL PV or LUN from the on-premises IBM FlashSystem Storage (FS9100) is replicated by using IBM Global mirror to the PV or LUN that is created on the IBM SV4PC on Microsoft Azure Cloud. The PV or LUN is created from IBM SV4PC on Microsoft Azure Cloud by using the IBM Block Storage CSI driver plug-ins on the RHOCP that is deployed on Microsoft Azure Cloud.

This document also describes a brief procedure about how to use IBM Block CSI driver volume replication function to create volume relationships between on-premises PV to the SV4PC PV. Configuration steps also are included for enabling hybrid cloud connectivity between the on-premises data center to Microsoft Azure Cloud

The solution that is described in this document relies on the following software components and related document links for the configuration:

- RHOCP 4.x on Microsoft Azure cloud and on-premises RHOCP.
- IBM Block Storage CSI driver for IBM Storages.
- IBM Spectrum Virtualize for Public Cloud on Microsoft Azure Cloud.
- IBM FlashSystem Storage FS9100 (on-premises).
- Hybrid Cloud connectivity on-premises to Azure Cloud with Virtual Private Network (VPN).
- MySQL containerized database on RHOCP.
- IBM Spectrum Virtualize for Public Cloud on Microsoft Azure Cloud implementation guide.
- Technical configuration steps for building an end-to-end solution.
- VPN connectivity, on-premises to public cloud. For more information, see *Solutions for Hybrid Cloud Networking Configuration Version 1 Release1*, REDP-5542.

Customers are encouraged to suitable proper data consistency mechanisms for the respective databases to ensure that consistent data is available across sites.

The use-case that is presented in this document is a sample disaster recovery scenario in the Hybrid Cloud environment.

This blueprint does not:

- Provide scalability and performance analysis from a user perspective
- Replace any official manuals and documents that are issued by IBM
- Describe the installation of RHOCP in the on-premises data center

Introduction

Combining the capabilities of Red Hat OCP and IBM SV4PC on Microsoft Azure Cloud with IBM Block Storage CSI driver for IBM Storages enables enterprises to build business continuity solutions. These solutions address various use cases and enables data on heterogeneous storage systems to be replicated or migrated between on-premises and Azure or AWS. IBM Spectrum Virtualize and IBM Spectrum Virtualize for Public Cloud together support mirroring between on-premises and the cloud data center or between two public cloud data center.

IBM Block Storage CSI driver

IBM block storage CSI driver is used by Kubernetes PVs to dynamically provision for block storage used with stateful containers.

IBM block storage CSI driver is based on an open source IBM project (CSI driver), which is included as a part of IBM storage orchestration for containers. IBM storage orchestration for containers enables enterprises to implement a modern, container-driven hybrid multi-cloud environment that can reduce IT costs and enhance business agility, while continuing to derive value from existing systems.

By using CSI drivers for IBM storage systems, Kubernetes PVs can be dynamically provisioned for block or file storage to be used with stateful containers, such as database applications (IBM Db2®, MongoDB, PostgreSQL, and so on) running in Red Hat OCP or Kubernetes clusters.

Storage provisioning can be fully automatized with more support of cluster orchestration systems to automatically deploy, scale, and manage containerized applications. For more information, see IBM Documentation web page.

IBM Spectrum Virtualize for Public Cloud on Microsoft Azure

IBM Spectrum Virtualize for Public Cloud is now available on Microsoft Azure. With IBM Spectrum Virtualize for Public Cloud 8.4.3 users, can deploy a highly available, two-node cluster running IBM Spectrum Virtualize for Public Cloud on supported Microsoft Azure virtual machines (VMs). This all-inclusive, bring your own license (BYOL) software offering virtualizes, optimizes, and provisions supported Azure Managed Disks to applications that require the performance of block storage in the cloud with the added efficiencies that IBM Spectrum Virtualize for Public Cloud brings to native infrastructure as a service (IaaS) provided by Microsoft Azure.

For more information, see *Implementation Guide for IBM Spectrum Virtualize for Public Cloud on Microsoft Azure Version 8.4.3*, SG24-8510.

For more information about product positioning, software requirements, and limitations, see the IBM Canada Software Announcement: *IBM Spectrum Virtualize for Public Cloud 8.4.3 on Microsoft Azure*, A21-0596.

Installing Red Hat OpenShift Container Platform on Azure

OpenShift Container Platform is used for developing and running containerized applications. It is designed to allow applications and the data centers that support them to expand from a few machines and applications to thousands of machines that serve millions of customers.

With its foundation in Kubernetes, OpenShift Container Platform incorporates the same technology that serves as the engine for massive telecommunications, streaming video, gaming, banking, and other applications. Its implementation in open Red Hat technologies lets you extend your containerized applications beyond a single cloud to on-premises and multi-cloud environments. For more information, see this Red Hat Documentation web page. Also, see the Red Hat OCP installation procedure for installing a cluster on Azure into a VNet.

Prerequisites

This section outlines prerequisites for the solution.

This blueprint assumes that the person who is implementing this solution has the basic knowledge of or access to the following information:

- IBM Spectrum Virtualize for Public Cloud on Microsoft Azure. For more information, see the following resources:
  - *Implementation Guide for IBM Spectrum Virtualize for Public Cloud on Microsoft Azure Version 8.4.3*, SG24-8510
  - This IBM Documentation web page
- IBM Storage Remote Replication (IBM Global Mirror). For more information, see this IBM Documentation web page.
- IBM Block Storage CSI driver plug-ins and RHOCP and Kubernetes.
- iSCSI basics and connectivity with IBM Storage. For more information, see this hIBM Documentation web page.
- Microsoft Azure Cloud portal login and required user rights and billing and cost approval.
- RHOCP 4.x on Microsoft Azure Cloud and on-premises RHOCP. For more information, see this Red Hat Documentation web page.
- Red Hat login credentials to download binaries, pull secret, tools. For more information, see this Red Hat Documentation web page (login required).
- VPN connectivity between on-premises data-center to Microsoft Azure Cloud. For more information, see the following resources:
  - This Microsoft Build tutorial
  - This VyOS Documentation web page
- Containerized MySQL database deployment on RHOCP.
- Bastion hosts on Microsoft Azure Cloud (Windows 2019 and Linux 7.x).
- User with administrator privileges and required roles that must be created on Microsoft Azure portal for creating resources on Azure and successful deployment.
- The firewall rules and network security groups that must be created on Microsoft Azure Cloud and on-premises data-centers for hybrid cloud connectivity and networking between various network components.
- Internet access from Microsoft Azure Cloud and on-premises data center for successful deployment of RHOCP.

Note: Consider the following points:

- Red Hat OpenShift installation on Azure and Azure Red Hat OpenShift (ARHO) feature different installation procedures. For more information, see this Red Hat Documentation web page.
- VPN connectivity between on-premises data centers to Microsoft Azure Cloud depends on the VPN and gateways devices that are available at on-premises. In this document, we used VyOS documentation.
- The yellow arrow that is outlined in blue in the figures in this document highlights areas for selecting options while configuring the solution.

Solution overview

The purpose of this document is to showcase the hybrid multi-cloud scenario for business continuity and data replication between on-premises IBM FlashSystem Storage FS9100 to IBM Spectrum Virtualize for Public Cloud on Microsoft Azure Cloud connected with iSCSI protocol for host mapping.

For demonstration purposes, MySQL containerized database is installed on the PV or LUN that was created on the on-premises IBM FlashSystem Storage that is connected with iSCSI protocol to the RHOCP (v4.8) worker nodes in the vSphere environment and by using the IBM block storage CSI driver (v1.8).

A 2-way IP partnership was created between the on-premises (FS9100) IBM FlashSystem Storage and IBM SV4PC on Azure Cloud. The VPN connectivity between the on-premises data center and Azure Cloud is created with the Site-to-Site VPN to Azure (BGP over IKEv2/IPsec).

The volume or LUN on IBM FlashSystem Storage FS9100 is replicated by IBM global mirror on IBM Spectrum Virtualize for Public Cloud on Azure. The replicated volume or PV is imported in the RHOCP that is deployed on Azure Cloud. For more information about importing a volume, see this IBM Documentation web page.

Figure 1 shows a typical infrastructure and the various components that are required and used to create a business continuity solution.

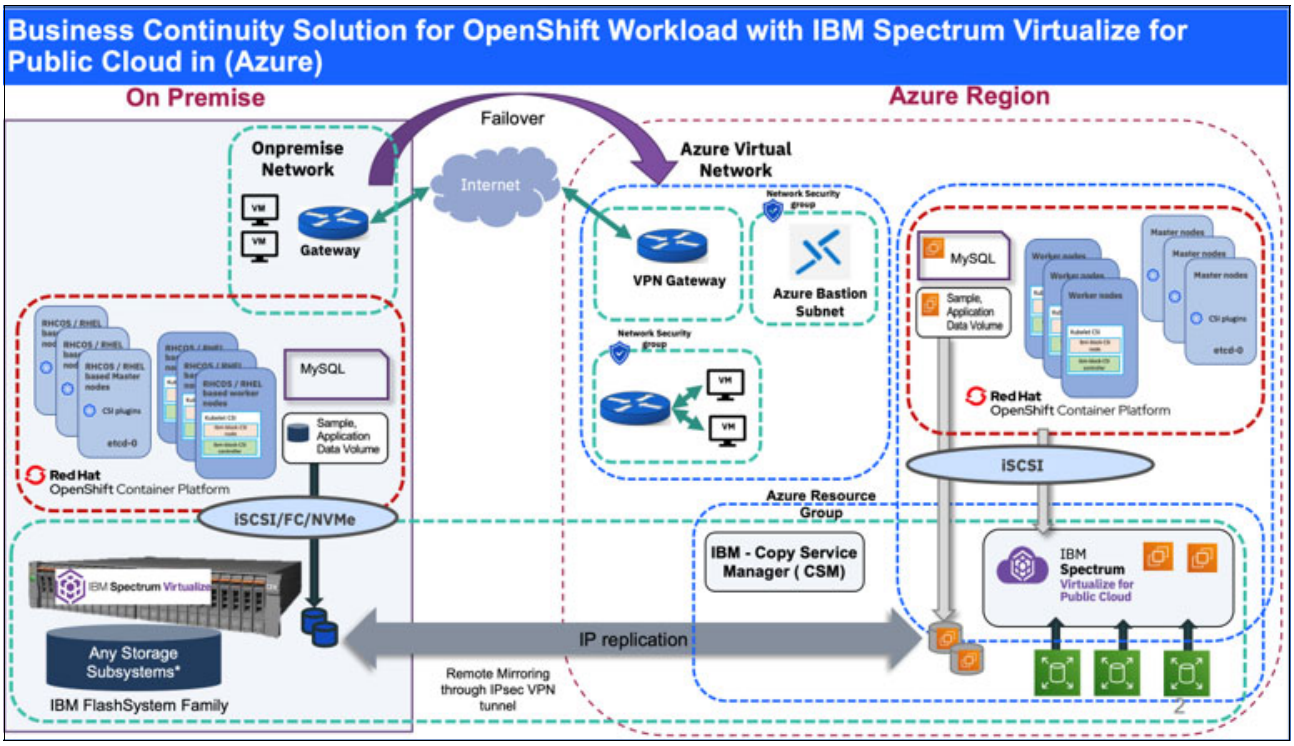


Figure 1 Solution overview

As part of the solution and the use case scenario and for data consistency, a sample database was created in the MySQL databases at the primary site (on-premises) and sample data is inserted in the table.

After the consistent copying status is completed to consistent synchronized, the consistency group is stopped and the replicated volume is opened for read/write access at the Azure Cloud. Also, the volume is imported by importing a volume in the RHOCP cluster and then, validating the sample data is available on the replicated volume to conclude the business continuity use-case.

Use cases demonstration methods

The following volume replication methods are described in this document for the use case demonstration:

- By using the IBM Storage global mirror feature
- By using IBM Block Storage CSI Volume Replication function

Lab setup

In this section, we describe the lab setup that was used for this use case.

Setting up Microsoft Azure Cloud and the on-premises data center

The following major components and software were deployed at the on-premises data center and Microsoft Azure Cloud for creating the lab setup:

- Microsoft Azure Cloud:
  - Red Hat OpenShift Container Platform v4.8 in the VNET
  - IBM Block Storage CSI driver v1.8 on RHOCP
  - IBM Spectrum Virtualize for Public Cloud v8.x with iSCSI connection
  - IBM Global mirror replication
  - Azure Cloud VPN Gateway device
  - Azure Site-Site VPN connection and local gateway
  - MySQL containerized database
  - Bastion hosts on Microsoft Azure (Windows 2019 and Linux 7.x)
  - SV4PC cluster IP: 40.10.1.4
  - Linux bastion host: `hybrid-cloud-linux-bastion-vm`
- On-premises data center:
  - Red Hat OpenShift Container Platform v4.8
  - IBM Block Storage CSI driver v1.8 on RHOCP
  - IBM FlashSystem Storage FS9100 with iSCSI connection
  - IBM Global mirror replication
  - On-premises VPN gateway devices (VyOS)
  - MySQL containerized database
  - RHOCP bastion hostname: `gw-10`
  - IBM FlashSystem storage IP: `10.0.240.30`

Steps to be performed on Microsoft Azure Cloud

The following steps must be completed on Microsoft Azure Cloud:

1. Create virtual networks.

   Log in to the Microsoft Azure portal at `https://portal.azure.com` and create a VNet by using the following settings (see Figure 2 - Figure 6 on page 12):

   - Resource group: Hybrid-Cloud-with-IBM-SV4PC
   - Name: Hybrid-Cloud-IBM-SV4PC-VNET
   - Region: Germany West Central
   - IPv4 address space: `40.10.0.0/16`
   - Subnet name: `Hybrid-Cloud-IBM-SV4PC-Cluster-snet`
   - Subnet address space: `40.10.1.0/24`
   - Subnet address space: `40.10.2.0/26`
   - AzureBastionSubnet: `40.10.3.0/24`

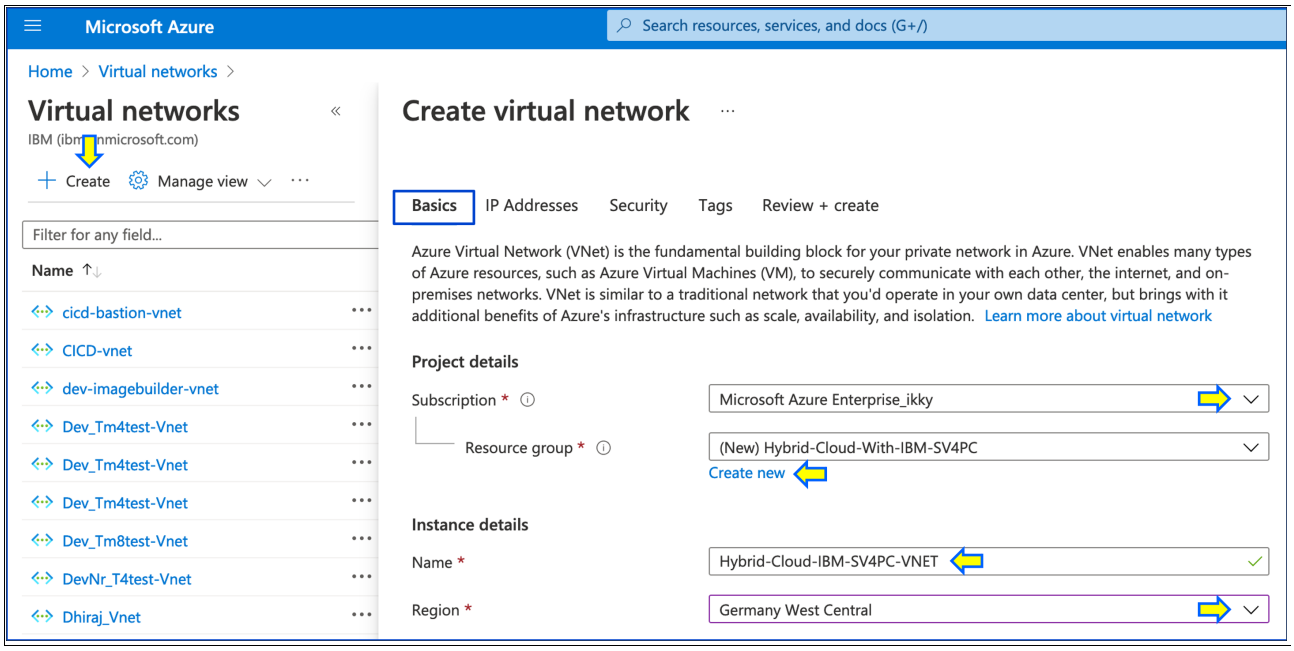


Figure 2 Creating virtual network: Basics

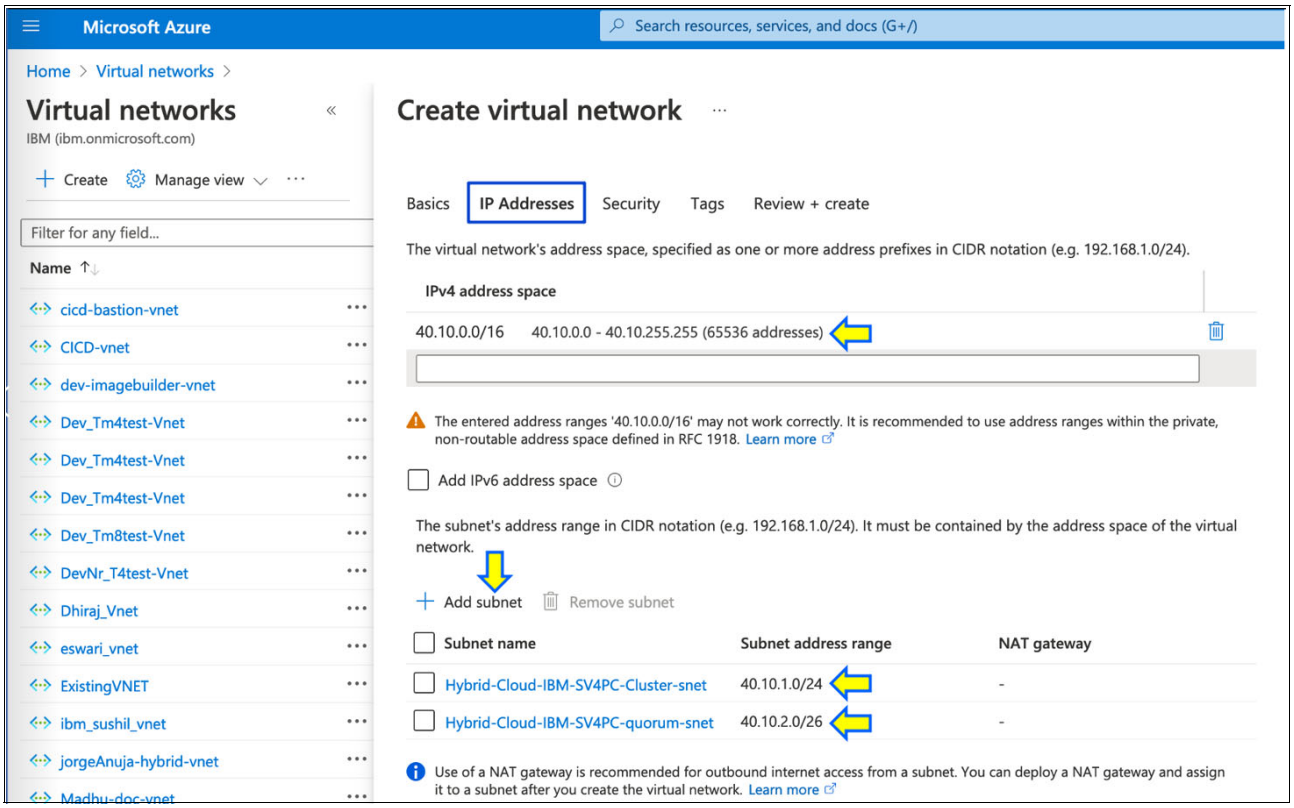


Figure 3 Creating VNet and adding subnet

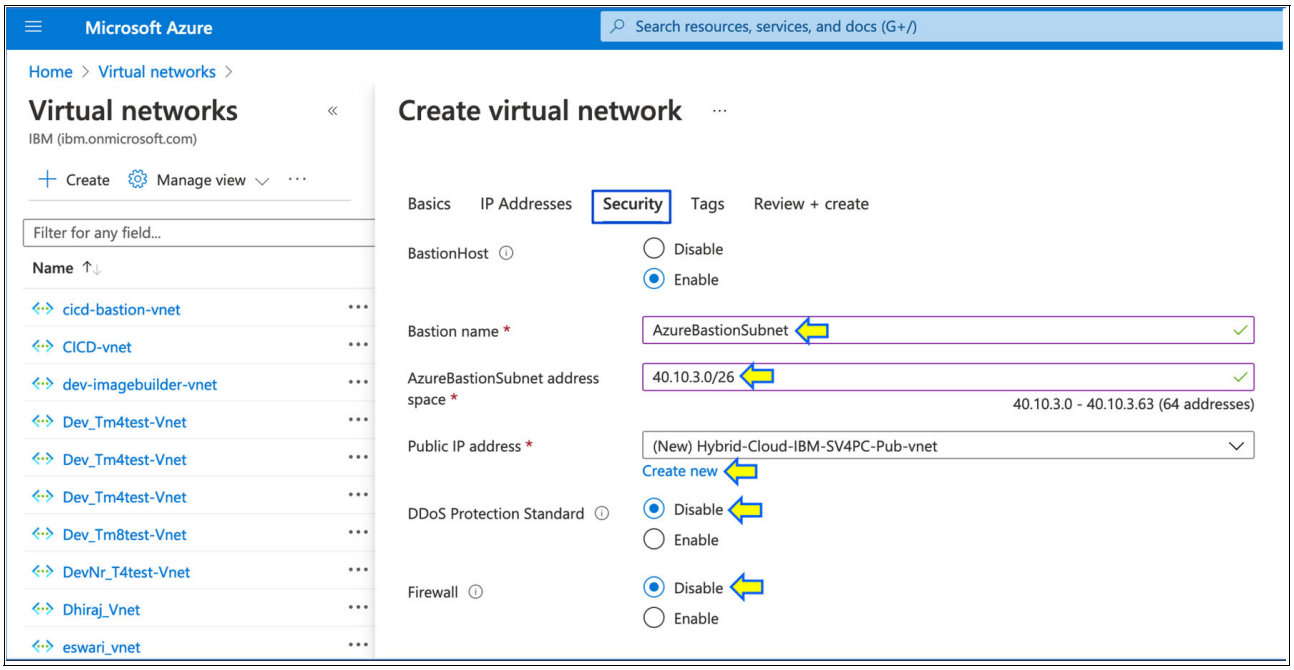


Figure 4 Creating VNet and AzureBastionSubnet

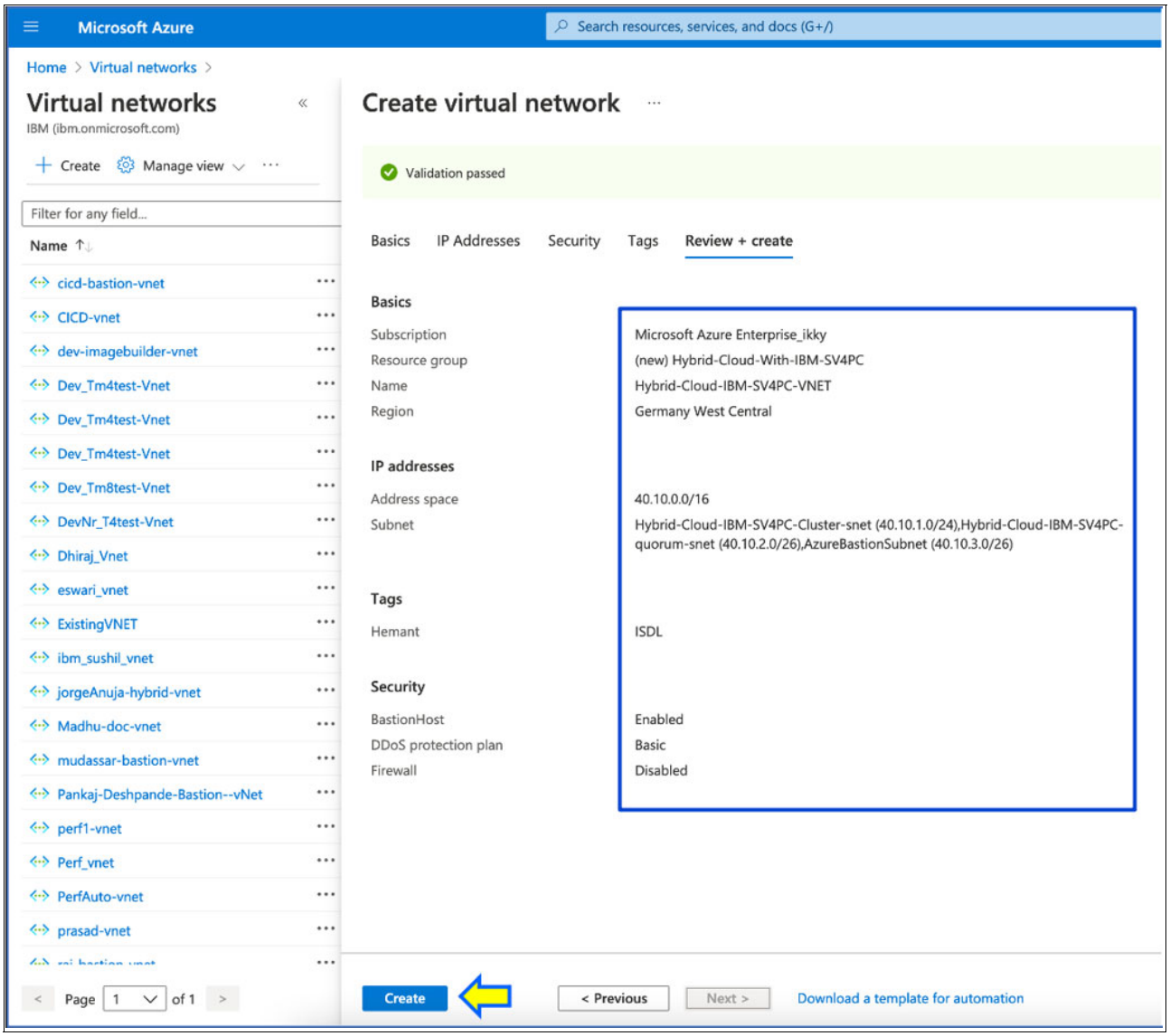


Figure 5 Creating resource

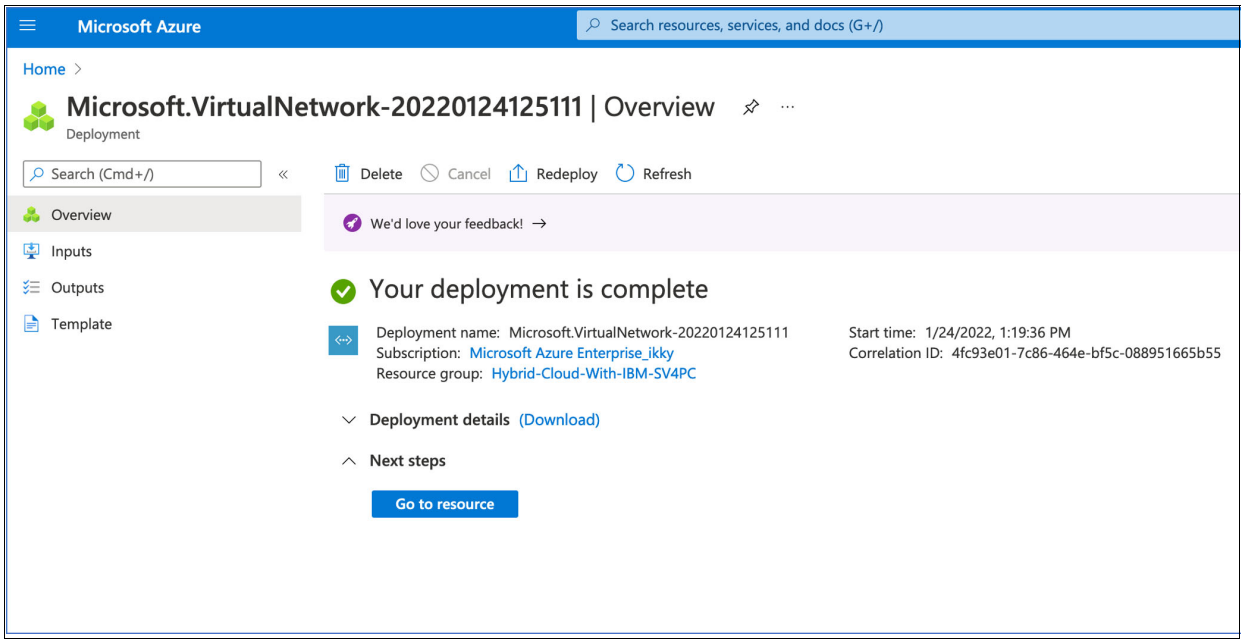


Figure 6 Checking deployment progress

2. Create the VPN gateway.

   Log in to the Microsoft Azure portal at `https://portal.azure.com` and create a VPN Gateway by using the following settings (see Figure 7 on page 13 - Figure 11 on page 16):

   - Name: `Hybrid-Cloud-IBM-SV4PC-Vnet-gateway`
   - Region: Germany West Central
   - Gateway type: VPN
   - VPN type: Route-based
   - SKU: VpnGw1
   - Generation: Generation 1
   - Virtual network: `Hybrid-Cloud-IBM-SV4PC-VNET`
   - Gateway subnet address range: `40.10.0.0/24`
   - Public IP address: Create new
   - Public IP address name: `Hybrid-Cloud-IBM- SV4PC-Public-IP`
   - ASN: `65515`

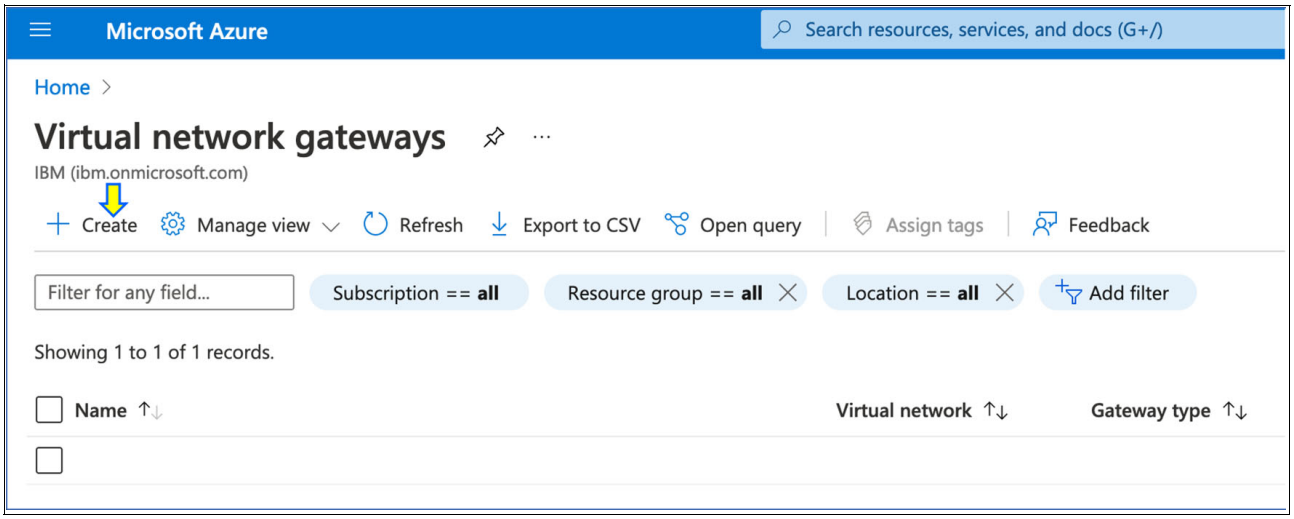


Figure 7 Selecting Create option

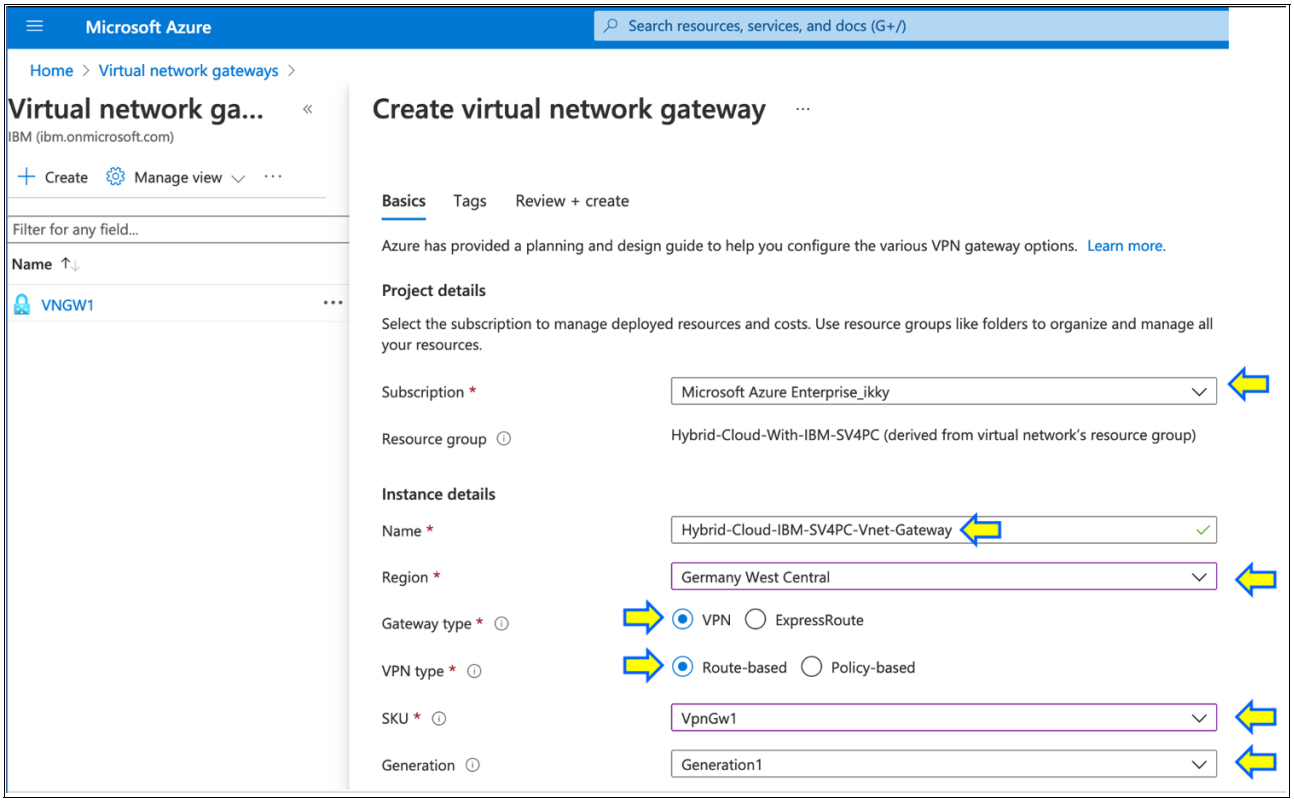


Figure 8 Creating VPN gateway: Basics page Part 1

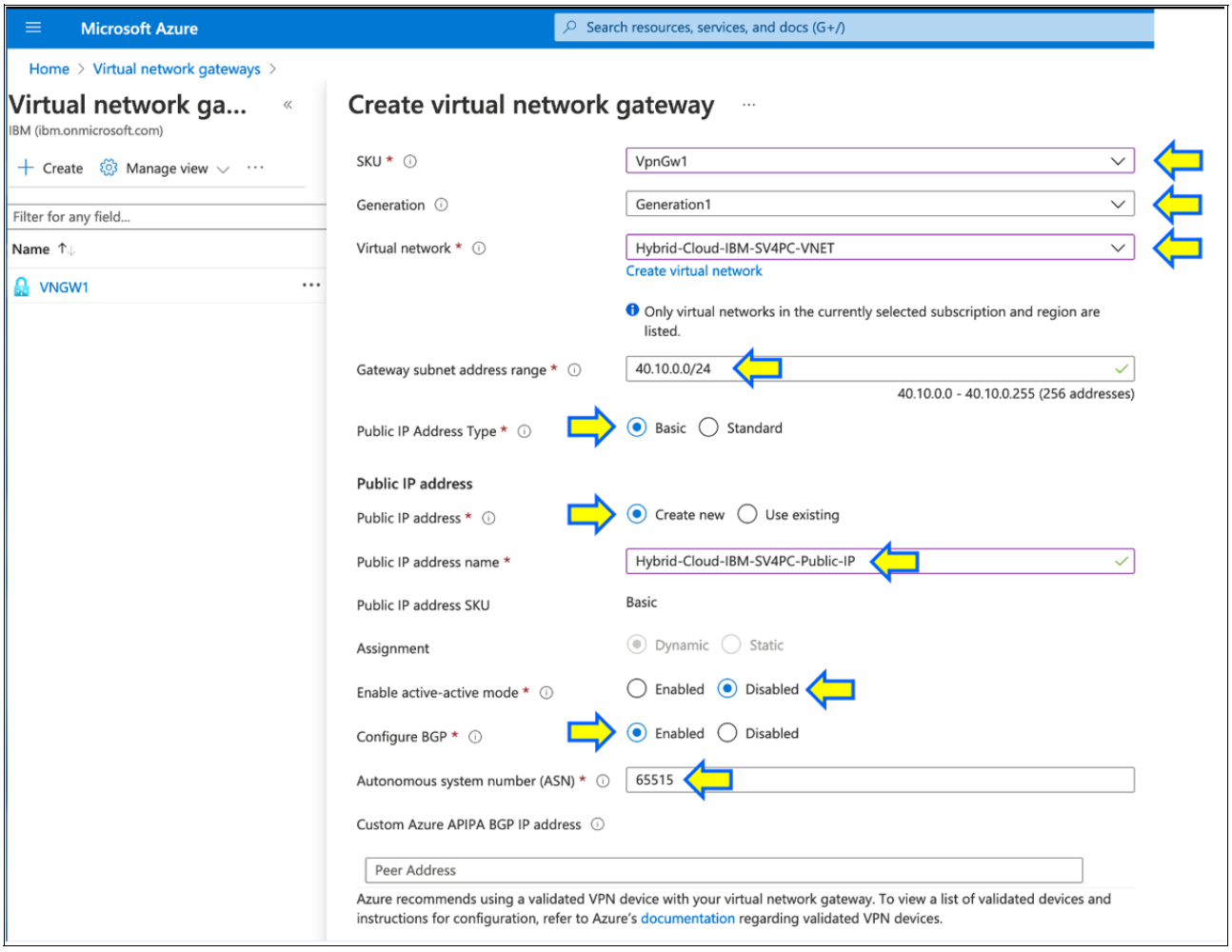


Figure 9 Creating VPN gateway: Basics page Part 2

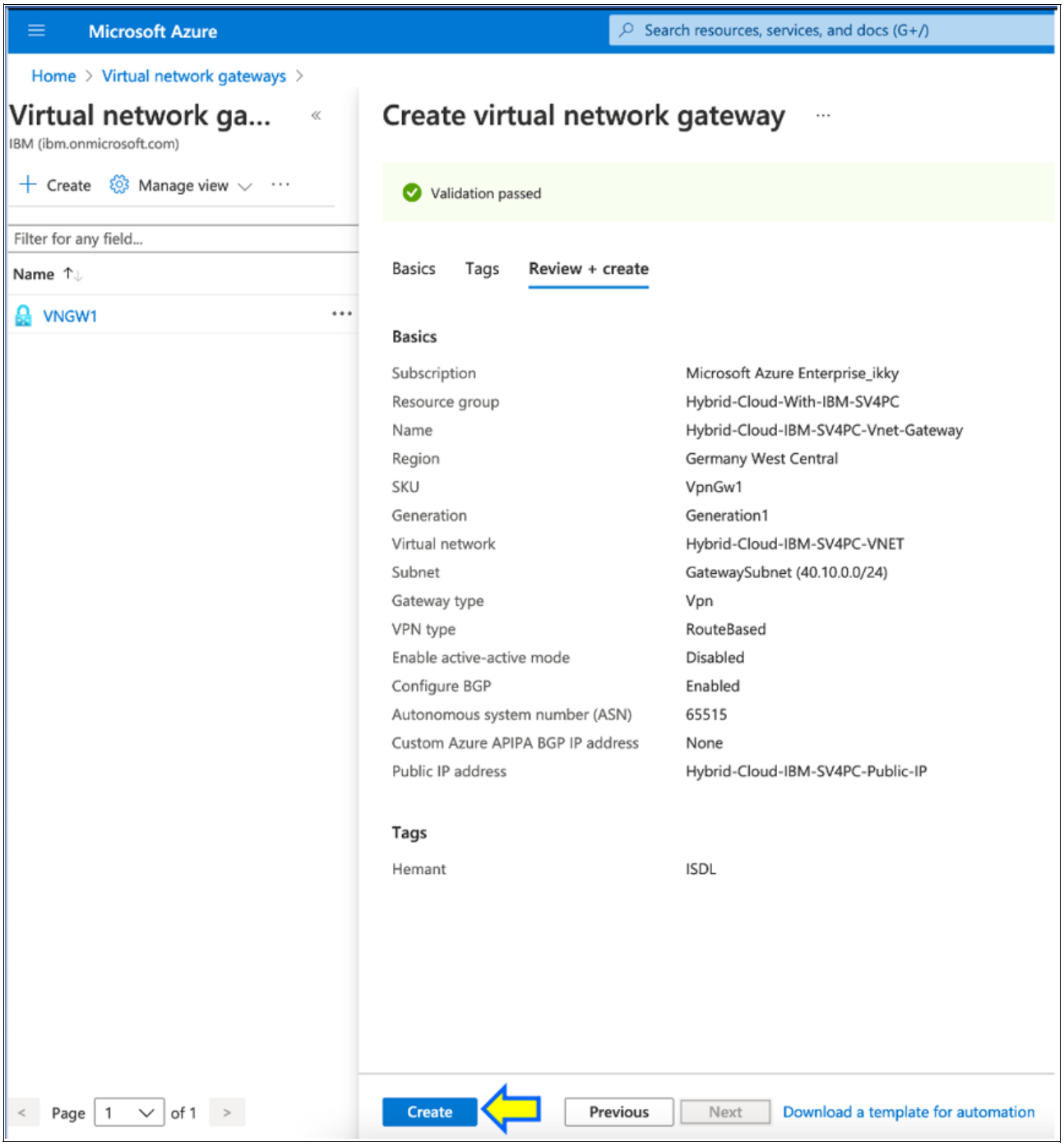


Figure 10 Selecting Create option on Review + create page

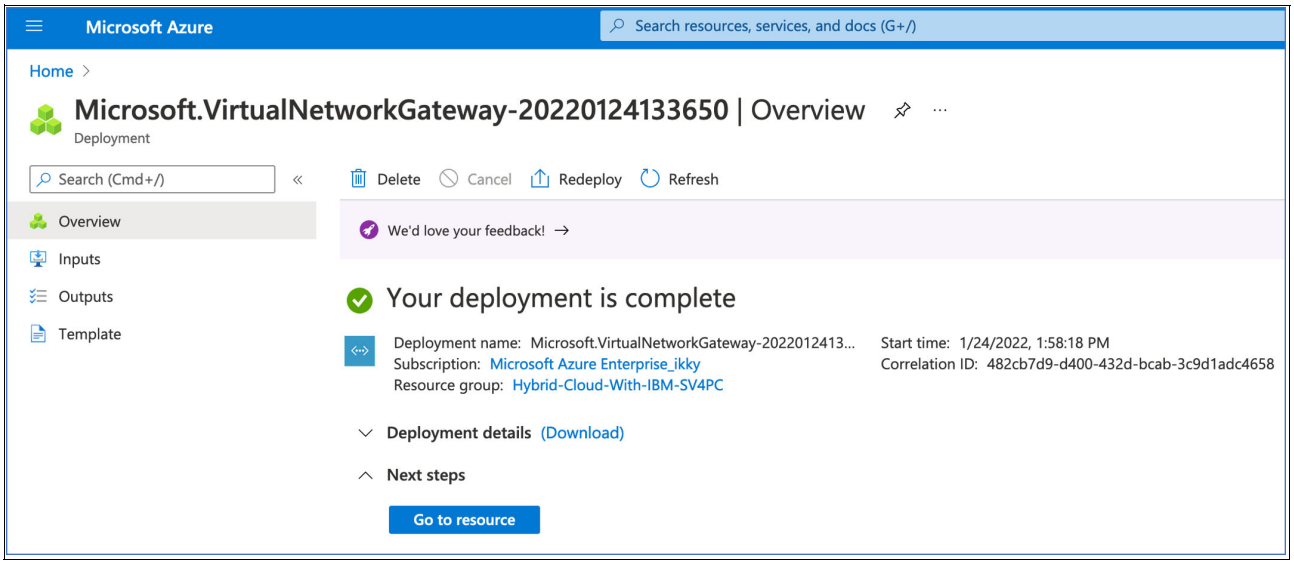


Figure 11 Checking that deployment is complete

3. Complete the following steps to create a site-to-site connection:

   a. Log in to the Microsoft Azure portal at `https://portal.azure.com` and create a site-to-site connection by using the values that are shown in Figure 12 - Figure 17 on page 19.

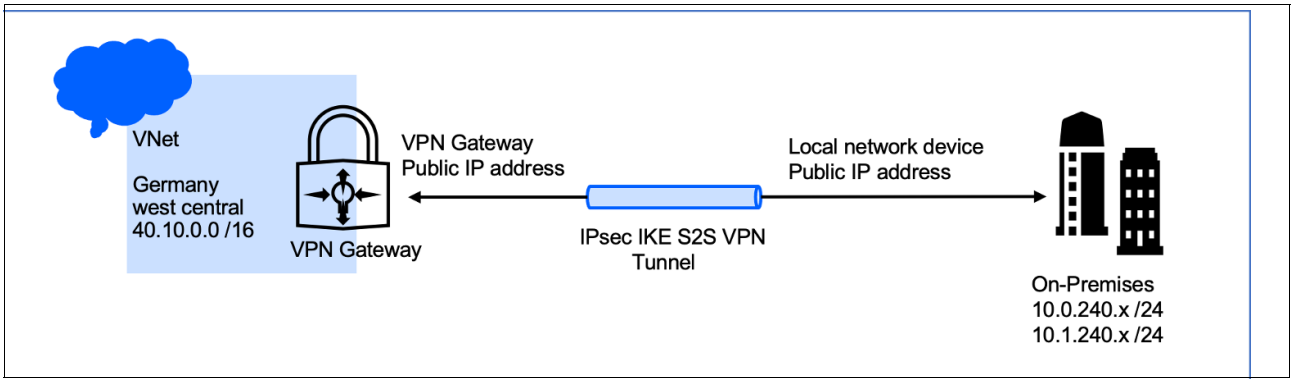


Figure 12 Hybrid cloud network connectivity

   b. Log in to the Microsoft Azure portal at `https://portal.azure.com` and create a Local Network Gateway to create a site-to-site connection. (A virtual network and VPN gateway were created in steps 1 and 2).

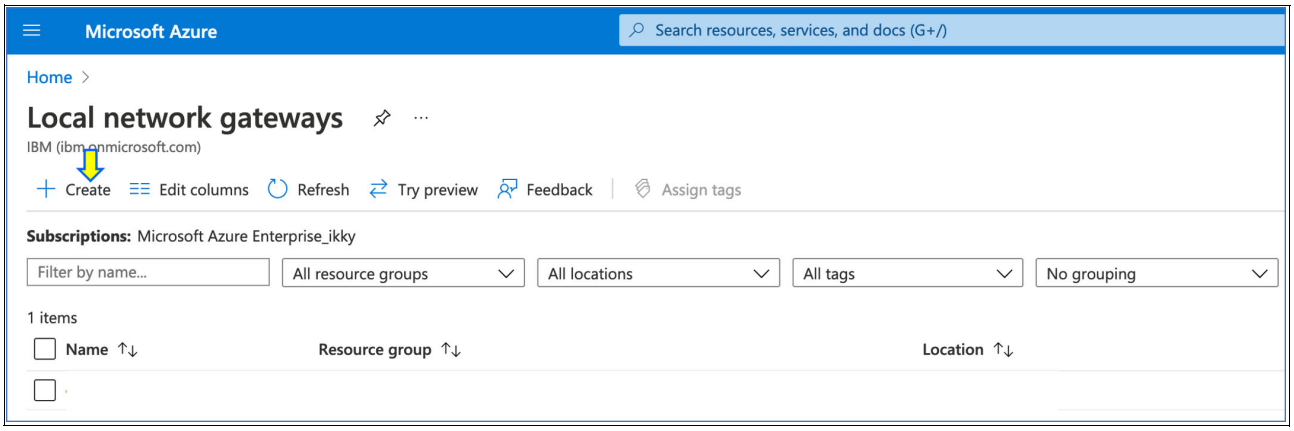


Figure 13 Selecting the Create option

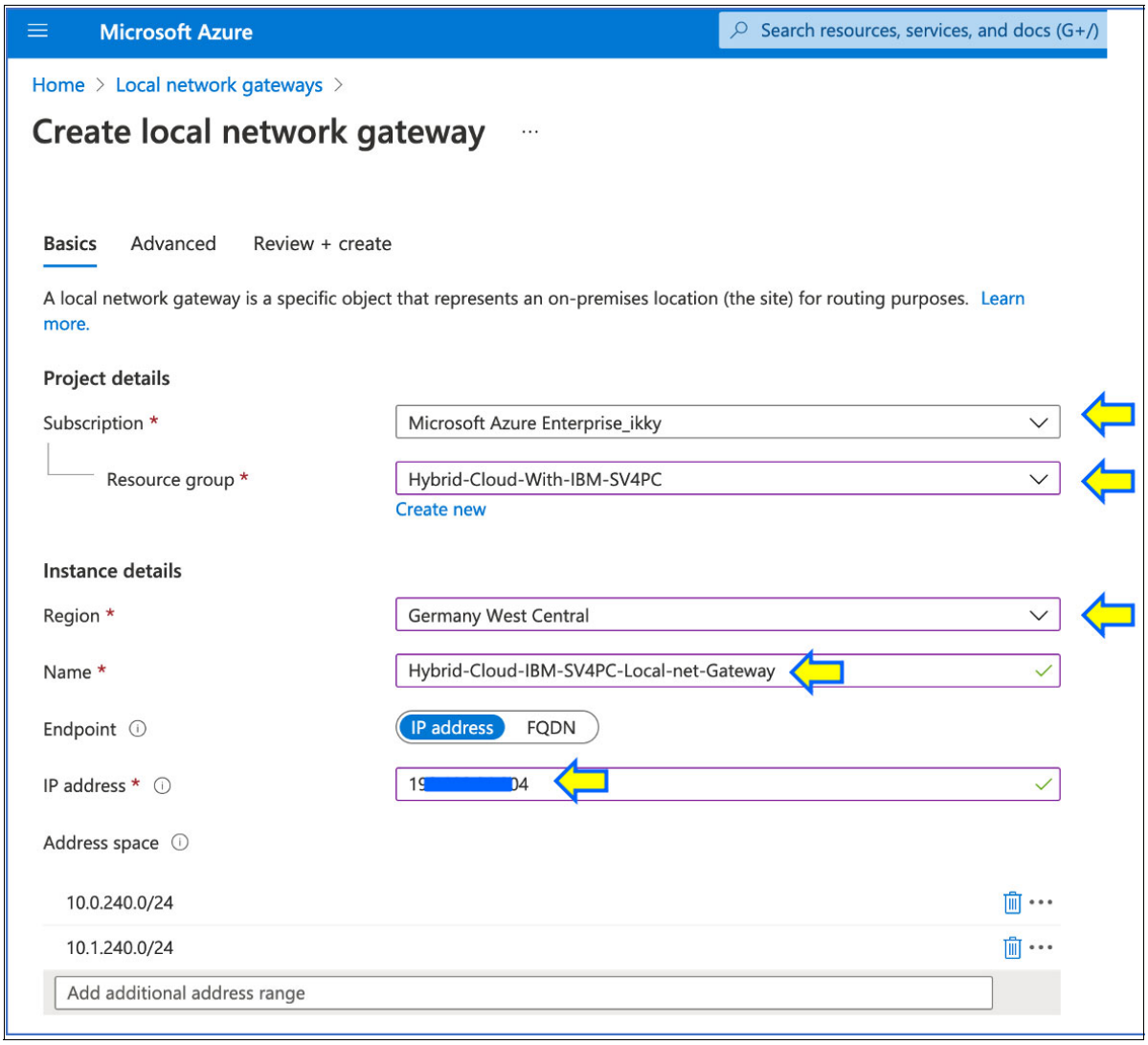


Figure 14 Create local network gateway: Basics page

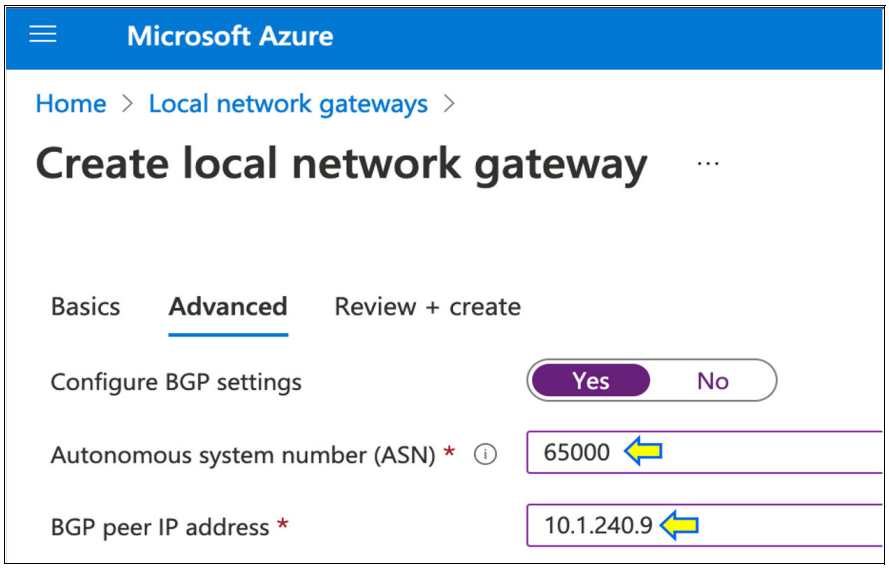


Figure 15 Create local network gateway: Advanced

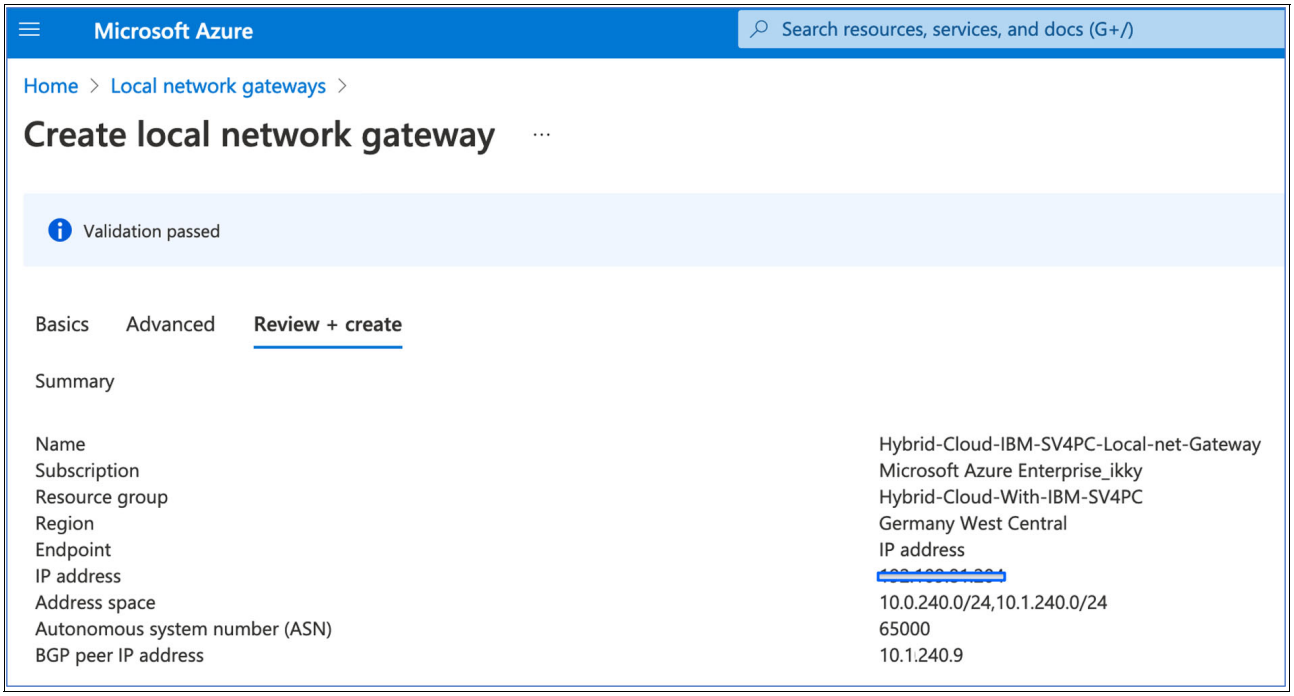


Figure 16 Creating local network gateway: Review + create page

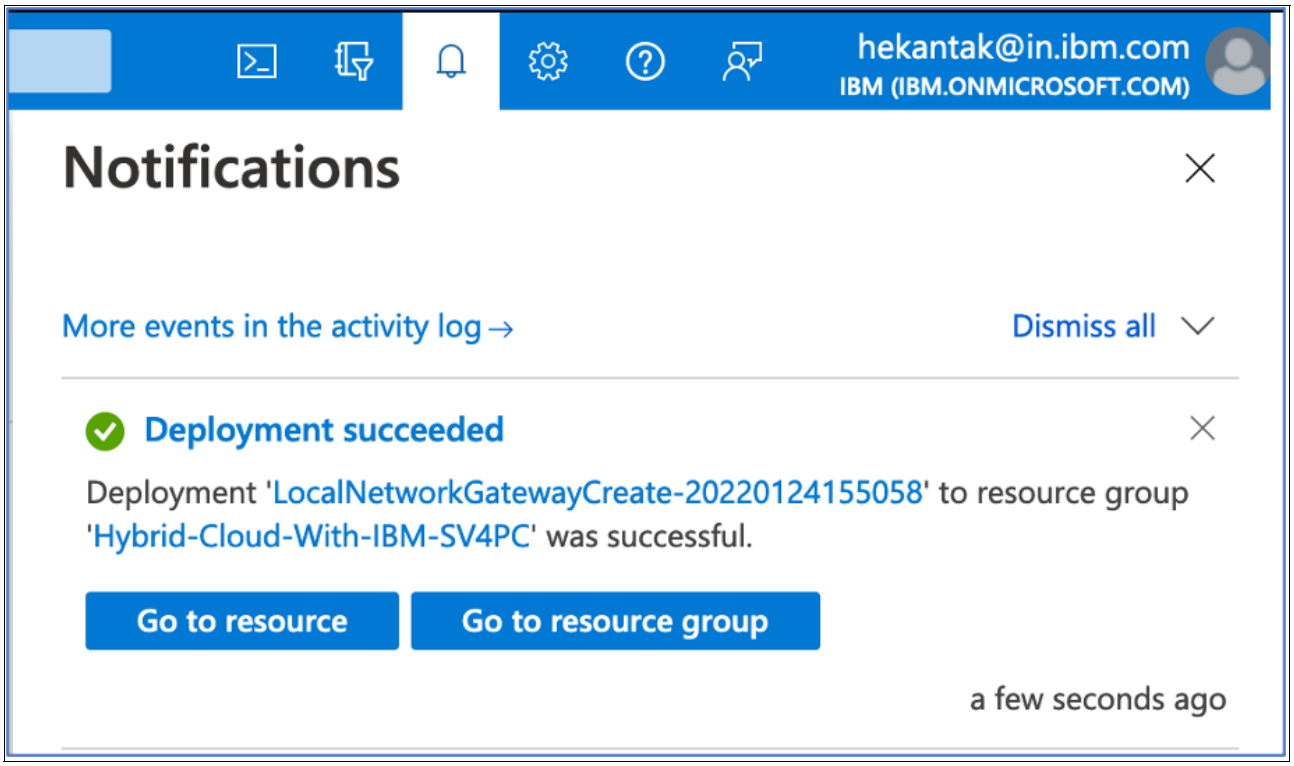


Figure 17 Deployment succeeded message

4. Configure the on-premises VPN gateway device.

   Log in to the on-premises VPN gateway device and configure the device for site-to-site VPN to Azure; that is, BGP over IKEv2/IPsec (see Figure 18 - Figure 20 on page 21). For more information, see this web page.

   Configure the device with the values as described in Appendix 18, “Configuring on-premises VPN device” on page 19.

```
WAN Interface                 eth0
On-premises address space     10.0.240.0/24
Azure address space           40.10.0.0
Vyos public IP                [On-premises Public IP address]
Vyos private IP               10.1.240.9
Azure VNet Gateway public IP  [Azure Public IP address] (Hybrid-Cloud-IBM-SV4PC-Public-IP)
Azure VNet Gateway BGP IP     40.10.0.254 (BGP peer IP address)
Pre-shared key                HybridCloudSV4PC
Vyos ASN                      65000
Azure ASN                     65515
```

Figure 18 Configuring on-premises VPN device

```
CONFIGURE ETHERNET INTERFACE
set interfaces ethernet eth0 address '10.1.240.9/24'
set interfaces ethernet eth0 description 'TRANSFER-NET'
set interfaces ethernet eth0 duplex 'full'
set interfaces ethernet eth0 hw-id 'e4:1f:13:6d:ea:58'
set interfaces ethernet eth0 smp_affinity 'auto'
set interfaces ethernet eth0 speed '1000'
set interfaces ethernet eth1 address '10.0.240.9/24'
set interfaces ethernet eth1 description 'YELLOW-ZONE'
set interfaces ethernet eth1 duplex 'full'
set interfaces ethernet eth1 hw-id 'e4:1f:13:6d:ea:5a'
set interfaces ethernet eth1 smp_affinity 'auto'
set interfaces ethernet eth1 speed '1000'
set interfaces loopback 'lo'

CONFIGURE THE IKE AND ESP SETTINGS TO MATCH A SUBSET OF THOSE SUPPORTED BY AZURE

set vpn ipsec esp-group AZURE compression 'disable'
set vpn ipsec esp-group AZURE lifetime '3600'
set vpn ipsec esp-group AZURE mode 'tunnel'
set vpn ipsec esp-group AZURE pfs 'dh-group2'
set vpn ipsec esp-group AZURE proposal 1 encryption 'aes256'
set vpn ipsec esp-group AZURE proposal 1 hash 'sha1'

set vpn ipsec ike-group AZURE dead-peer-detection action 'restart'
set vpn ipsec ike-group AZURE dead-peer-detection interval '15'
set vpn ipsec ike-group AZURE dead-peer-detection timeout '30'
set vpn ipsec ike-group AZURE key-exchange 'ikev1'
set vpn ipsec ike-group AZURE lifetime '28800'
set vpn ipsec ike-group AZURE proposal 1 dh-group '2'
set vpn ipsec ike-group AZURE proposal 1 encryption 'aes256'
set vpn ipsec ike-group AZURE proposal 1 hash 'sha1'

ENABLE IPSEC ON ETH0
set vpn ipsec ipsec-interfaces interface 'eth0'
set vpn ipsec nat-networks allowed-network '40.10.0.0/16'
set vpn ipsec nat-traversal 'enable'
```

Figure 19 Configuring on-premises VPN gateway device: Part 1

```
CONFIGURE A VTI WITH A DUMMY IP ADDRESS
set interfaces vti vti2 address '40.10.0.200/24'
set interfaces vti vti2 description 'Azure Tunnel'
set interfaces vti vti2 mtu '1436'


CONFIGURE THE VPN TUNNEL
set vpn ipsec site-to-site peer [Public IP address] authentication mode 'pre-shared-secret'
set vpn ipsec site-to-site peer [Public IP address] authentication pre-shared-secret 'HybridCloudSV4PC'
set vpn ipsec site-to-site peer [Public IP address] description 'AZURE PRIMARY TUNNEL'
set vpn ipsec site-to-site peer [Public IP address] ike-group 'AZURE'
set vpn ipsec site-to-site peer [Public IP address] local-address '10.1.240.9'
set vpn ipsec site-to-site peer [Public IP address] vti bind 'vti2'
set vpn ipsec site-to-site peer [Public IP address] vti esp-group 'AZURE'


CONFIGURE YOUR BGP SETTINGS
set protocols bgp 65000 neighbor 40.10.0.254 'disable-connected-check'
set protocols bgp 65000 neighbor 40.10.0.254 remote-as '65515'
set protocols bgp 65000 neighbor 40.10.0.254 soft-reconfiguration 'inbound'
set protocols bgp 65000 neighbor 40.10.0.254 timers holdtime '30'
set protocols bgp 65000 neighbor 40.10.0.254 timers keepalive '10'
set protocols bgp 65000 network '10.0.240.0/24'

ADD AN INTERFACE ROUTE TO REACH AZURE'S BGP LISTENER
set protocols static interface-route 40.10.0.254/32 next-hop-interface 'vti2'
```

Figure 20 Configuring on-premises VPN gateway device: Part 2

5. Add a connection to create the site-to-site VPN connection.

   Log in to the Microsoft Azure portal at `https://portal.azure.com` and add a connection to the VPN gateway to create the site-to-site connection (see Figure 21 on page 22 - Figure 23 on page 23).

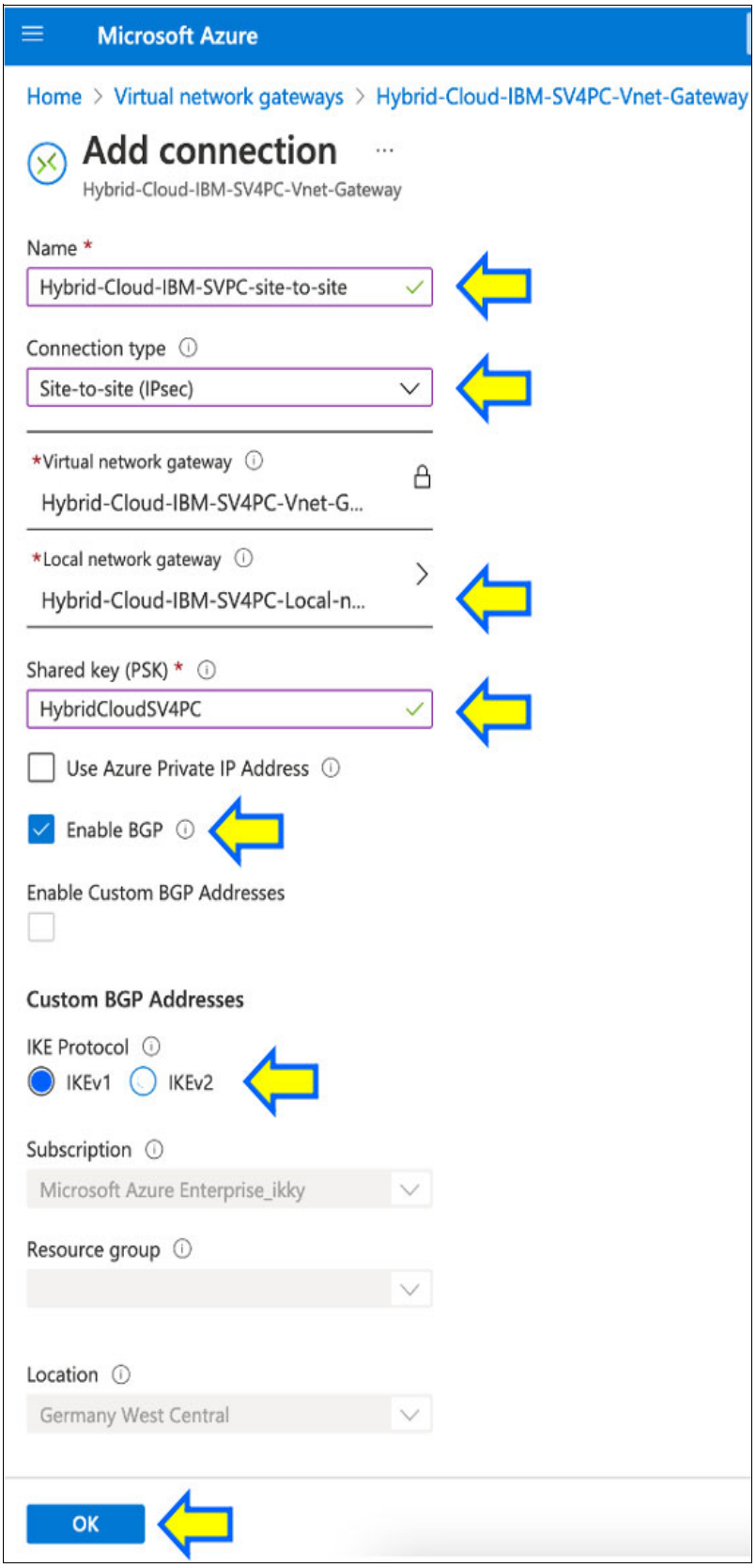


Figure 21 Adding connection

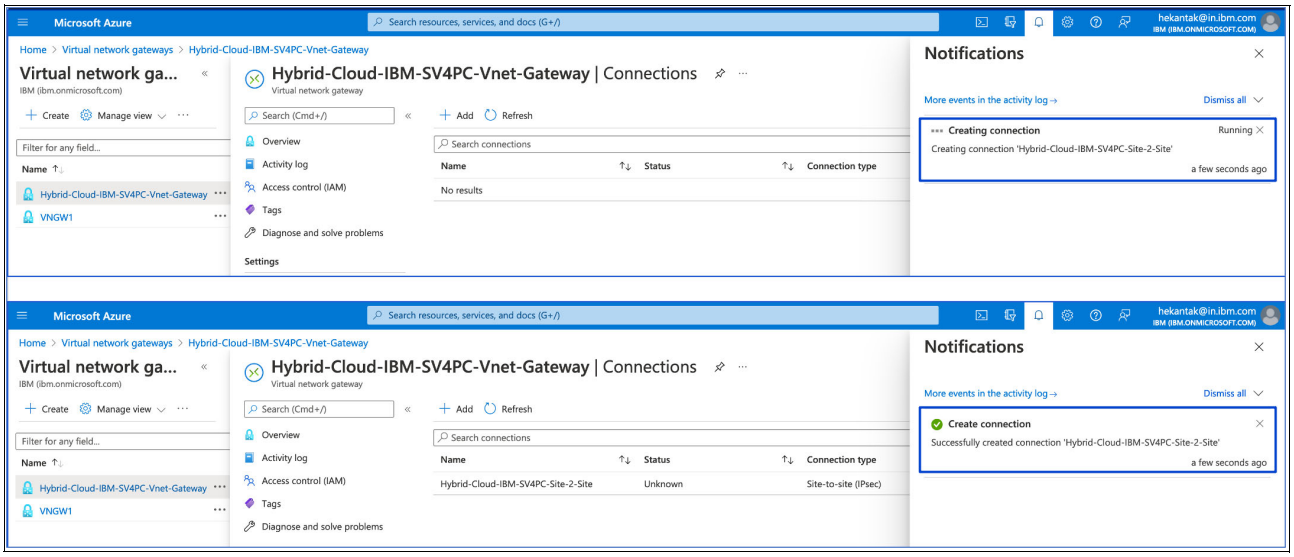


Figure 22 Checking the status of the deployment

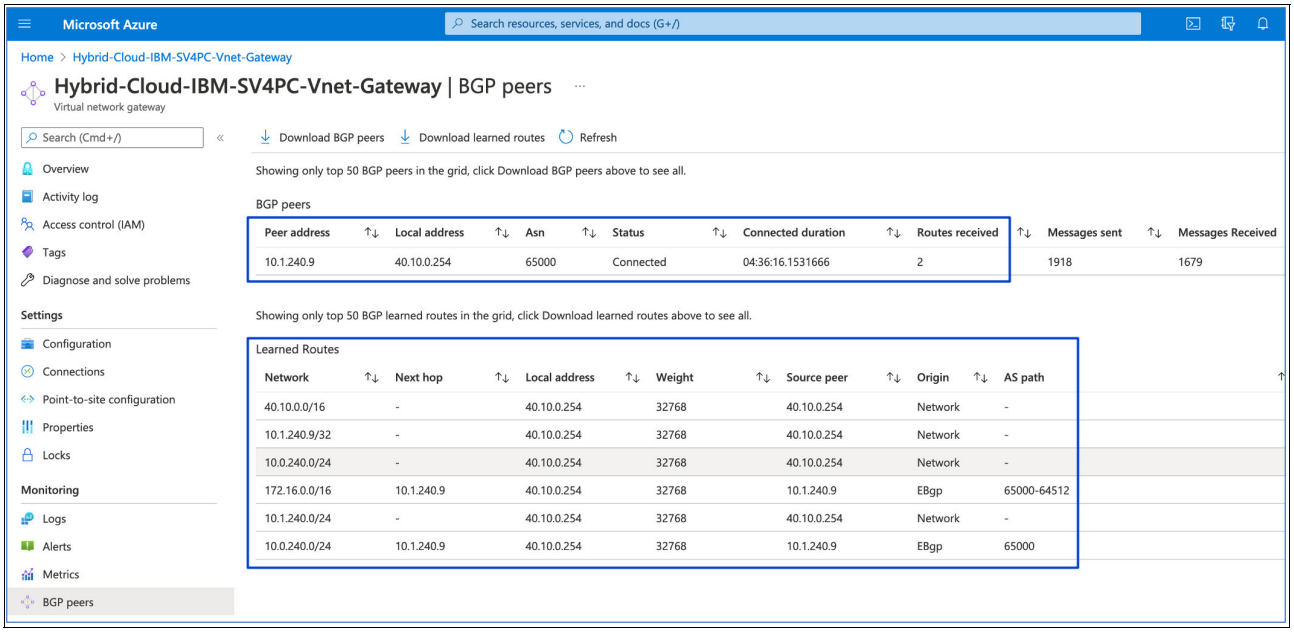


Figure 23 Checking the status of devices that are connected on-premises to Azure Cloud

6. Complete the following steps to install Linux VM as the Bastion host for the RHOCP cluster on Microsoft Azure Cloud:

   a. Log in to the Microsoft Azure portal at `https://portal.azure.com` and create the Linux virtual machine (see Figure 24).

   b. Enter the Disk, Networking, Management, Advance, Tags information.

   c. Review and create the virtual machine.

      Ensure that the existing Resource Group, which was configured with Virtual networks (VNET), was selected.

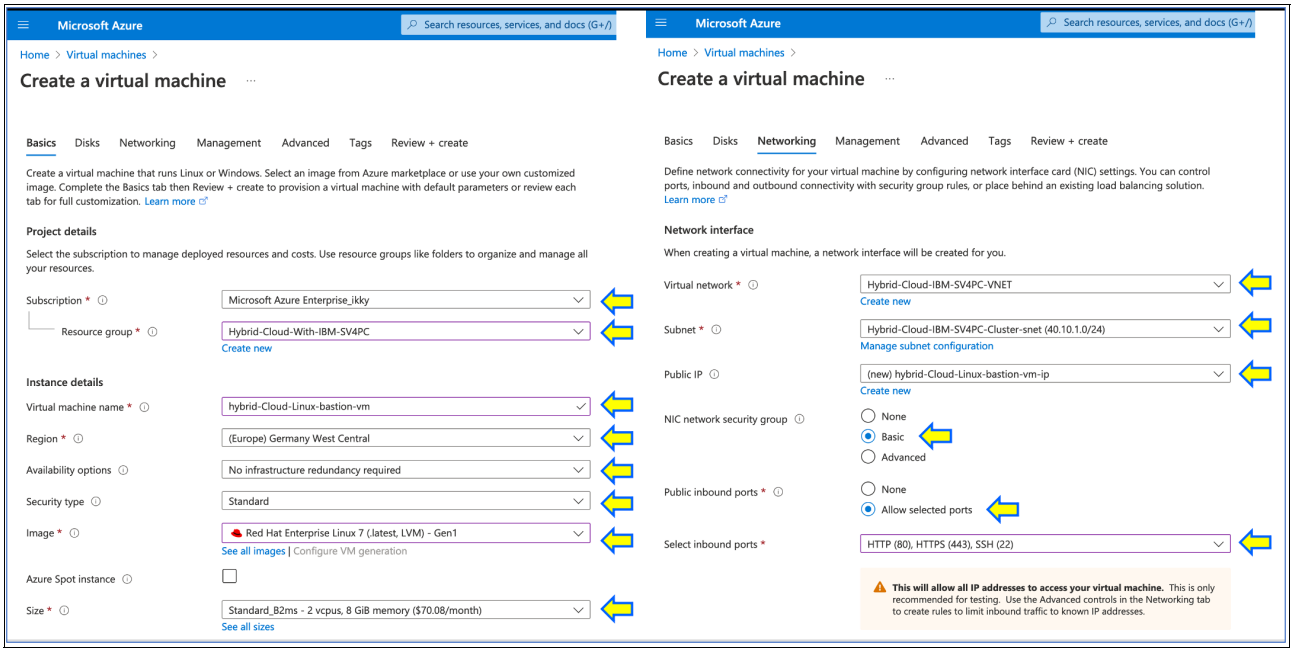


Figure 24 Creating Linux virtual machine

7. Complete the following steps to install Red Hat OpenShift Container Platform on Microsoft Azure Cloud:

   a. Log in to the Microsoft Azure portal at `https://portal.azure.com`.

   b. Log in to the Linux VM by using `azureuser` and the SSH key that uses the Bastion service or by using SSH and configuring the Azure Account that is required for the RHOCP deployment (see this Red Hat Documentation web page), as shown in Figure 25 on page 25 - Figure 28 on page 26).

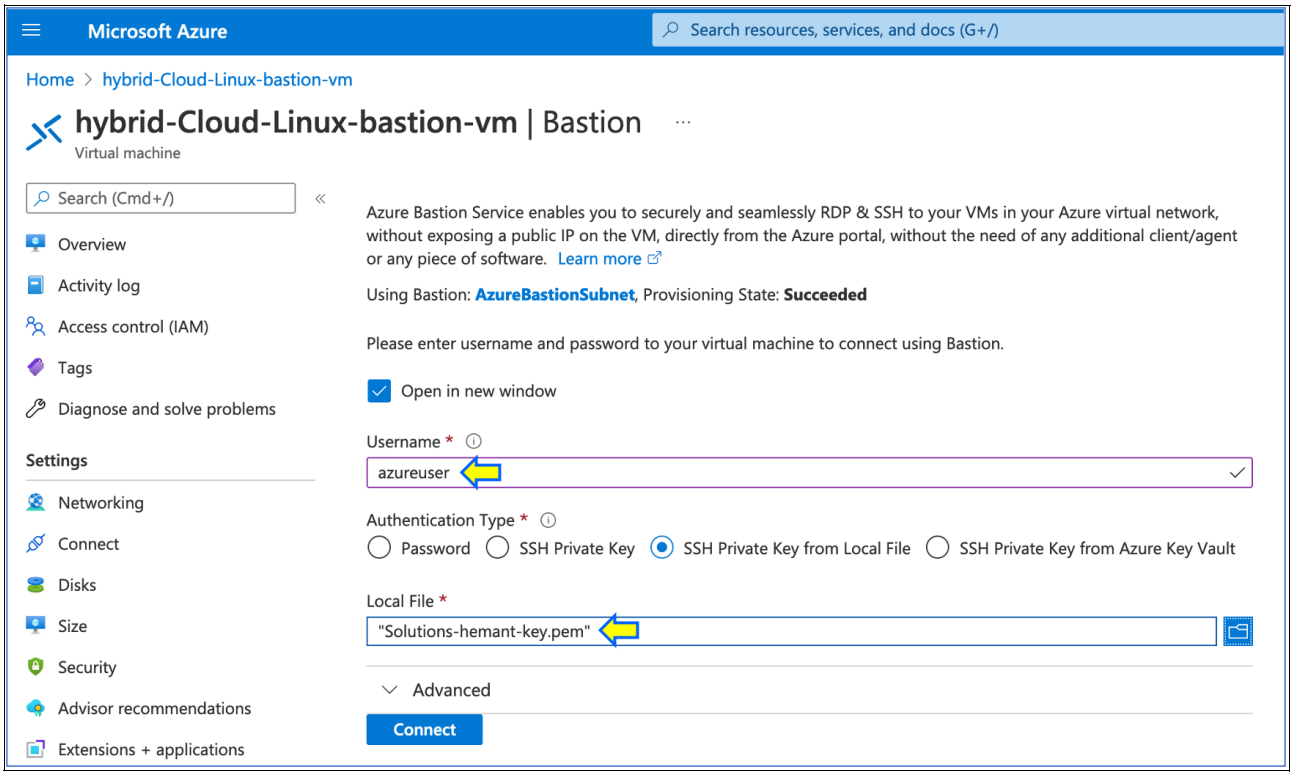


Figure 25 Logging in to Linux VM host

```
[root@hybrid-Cloud-Linux-bastion-vm ~]# az login
To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the code DDSQBZTJN to authent
icate.
The following tenants don't contain accessible subscriptions. Use 'az login --allow-no-subscriptions' to have tenant lev
el access.
7d684505-f7d4-4f7c-8f93-c8e54ea36510 'Microsoft Partner Events'
[
  {
    "cloudName": "AzureCloud",
    "homeTenantId": "[redacted]9e9",
    "id": "[redacted]3a0",
    "isDefault": true,
    "managedByTenants": [],
    "name": "[redacted]y",
    "state": "Enabled",
    "tenantId": "[redacted]",
    "user": {
      "name": "hekantak@in.ibm.com",
      "type": "user"
    }
  }
]
[root@hybrid-Cloud-Linux-bastion-vm ~]#
```

Figure 26 Creating Azure Account

```
[root@hybrid-Cloud-Linux-bastion-vm ~]# az account show
{
  "environmentName": "AzureCloud",
  "homeTenantId": "[redacted]",
  "id": "[redacted]",
  "isDefault": true,
  "managedByTenants": [],
  "name": "[redacted]",
  "state": "Enabled",
  "tenantId": "[redacted]",
  "user": {
    "name": "hekantak@in.ibm.com",
    "type": "user"
  }
}
[root@hybrid-Cloud-Linux-bastion-vm ~]#
```

Figure 27 Azure account show

```
[root@hybrid-Cloud-Linux-bastion-vm ~]# az ad sp create-for-rbac --role Contributor --name hybrid-cloud-service_principal
Creating 'Contributor' role assignment under scope '/subscriptions/994c6fdf-6182-4da4-b701-dad9da3c23a0'
The output includes credentials that you must protect. Be sure that you do not include these credentials in your code or check the credent
ials into your source control. For more information, see https://aka.ms/azadsp-cli
{
  "appId": "f386e929-e84c-4abb-ad68-3cf921bffaa9",
  "displayName": "hybrid-cloud-service_principal",
  "password": "[redacted]",
  "tenant": "fcf67057-50c9-4ad4-98f3-ffca64add9e9"
}
[root@hybrid-Cloud-Linux-bastion-vm ~]#

[root@hybrid-Cloud-Linux-bastion-vm ~]#
[root@hybrid-Cloud-Linux-bastion-vm ~]# az role assignment create --role "User Access Administrator" --assignee-object-id $(az ad sp list
--filter "appId eq 'f386e929-e84c-4abb-ad68-3cf921bffaa9'" | jq '.[0].objectId' -r)
RBAC service might reject creating role assignment without --assignee-principal-type in the future. Better to specify --assignee-principal
-type manually.
{
  "canDelegate": null,
  "condition": null,
  "conditionVersion": null,
  "description": null,
  "id": "/subscriptions/994c6fdf-6182-4da4-b701-dad9da3c23a0/providers/Microsoft.Authorization/roleAssignments/bee77d02-d031-4a08-a479-792
29e0ae0eb",
  "name": "bee77d02-d031-4a08-a479-79229e0ae0eb",
  "principalId": "86355021-591e-4e9f-91bb-083db774f57d",
  "principalType": "ServicePrincipal",
  "roleDefinitionId": "/subscriptions/994c6fdf-6182-4da4-b701-dad9da3c23a0/providers/Microsoft.Authorization/roleDefinitions/18d7d88d-d35e
-4fb5-a5c3-7773c20a72d9",
  "scope": "/subscriptions/994c6fdf-6182-4da4-b701-dad9da3c23a0",
  "type": "Microsoft.Authorization/roleAssignments"
}
[root@hybrid-Cloud-Linux-bastion-vm ~]#
```

Figure 28 Adding role and assignment and creating service principal

8. Complete the following steps to create the Public DNS Zone in Microsoft Azure:
   a. Log in to the Microsoft Azure portal at https://portal.azure.com and create the DNS zone (see Figure 29 on page 27 - Figure 32 on page 28).

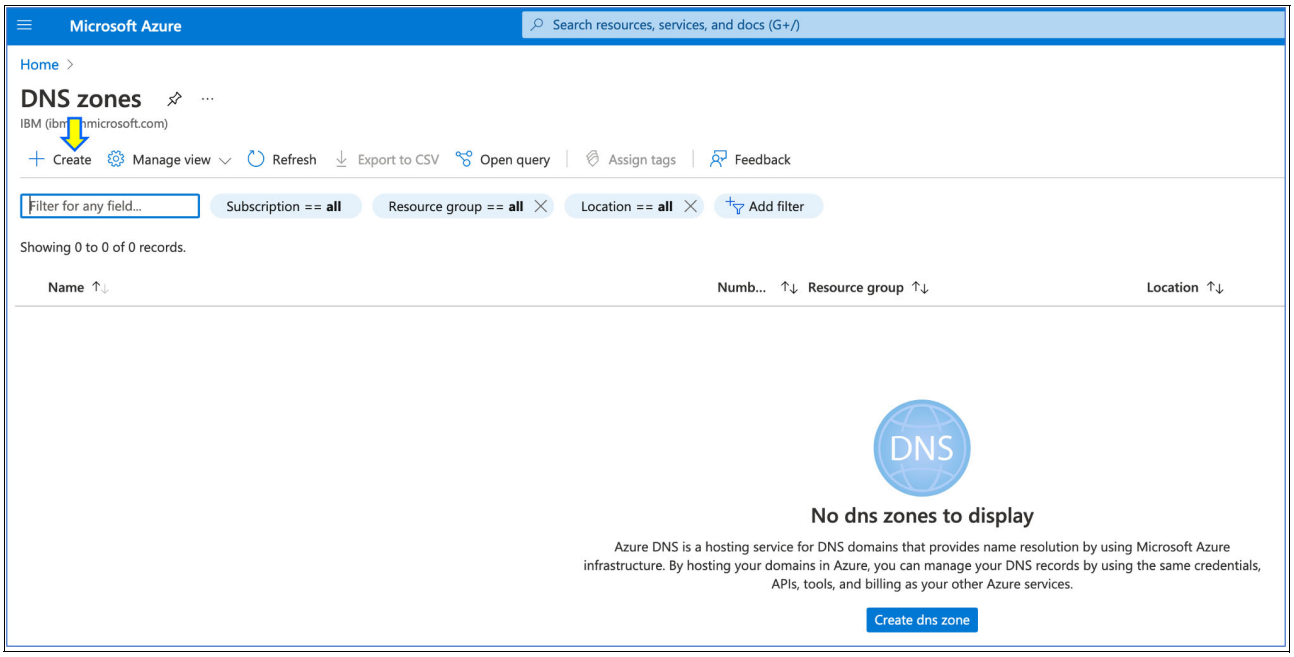


Figure 29 Selecting the Create option

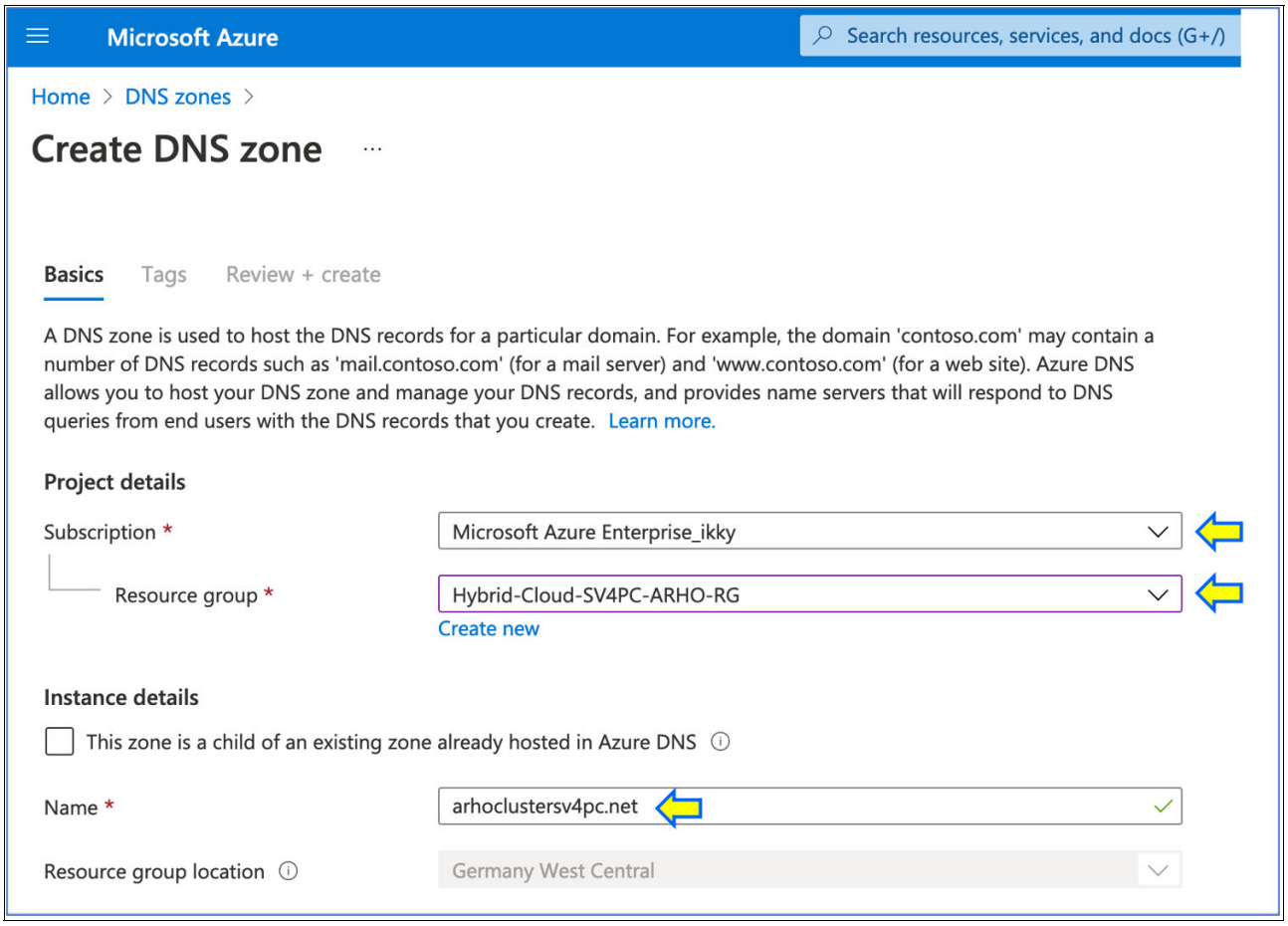


Figure 30 Creating DNS zones: Basics page

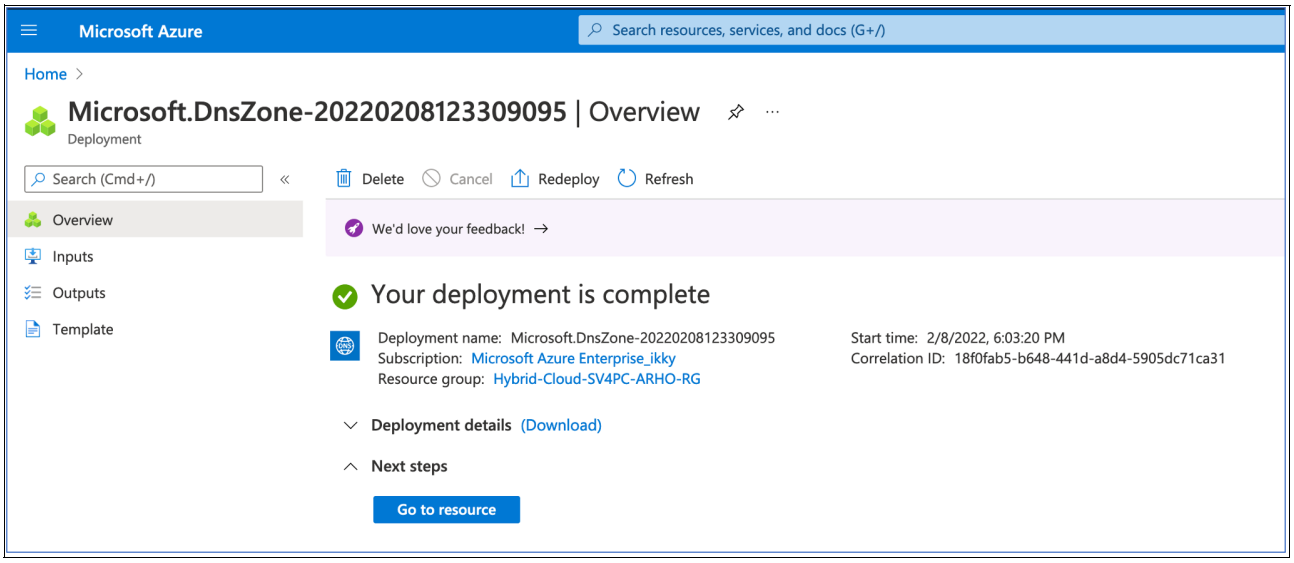


Figure 31 Checking the deployment

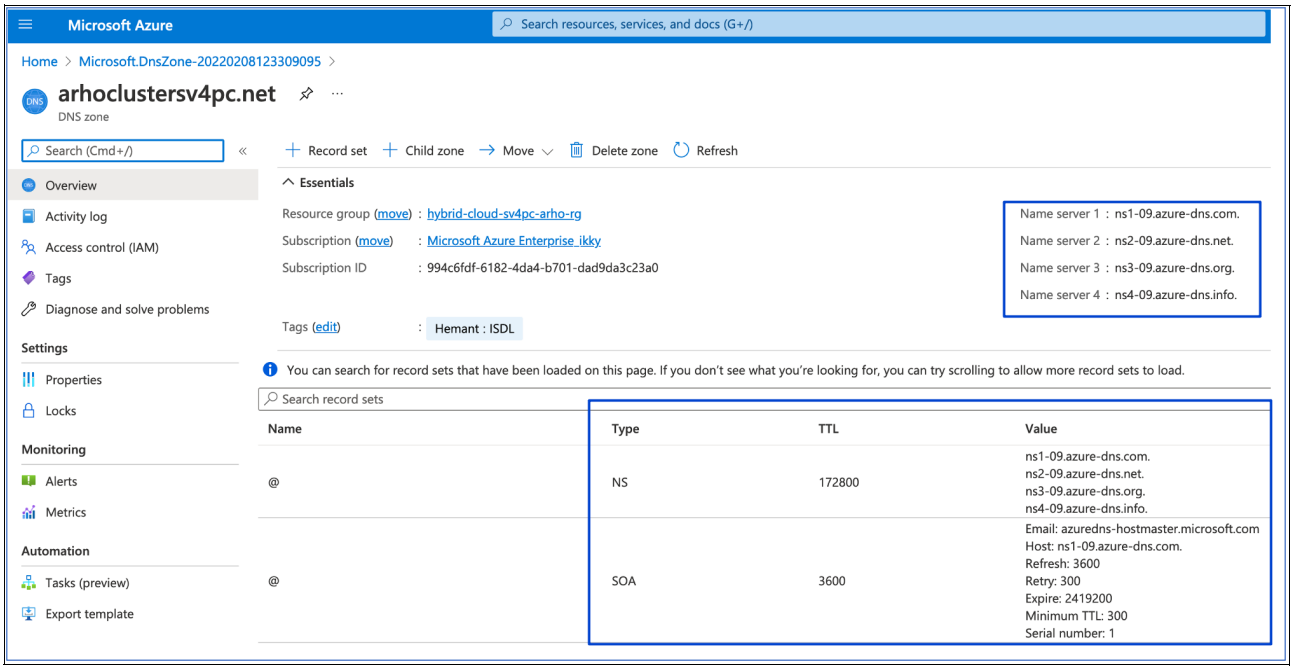


Figure 32 Checking the name server details

b. Log in to the Microsoft Azure portal at `https://portal.azure.com`.

c. Log in to the Linux VM by using `azureuser` and the SSH key.

d. Create the `install-config.yaml` file and the RHOCP cluster (see Figure 33 on page 29 - Figure 37 on page 31).

```
[root@hybrid-Cloud-Linux-bastion-vm ocp4.8]# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:GXYWBVQrxmcQD2UwpvVeTWz0pynpTLdh+ONJqdHtnBQ root@hybrid-Cloud-Linux-bastion-vm
The key's randomart image is:
+---[RSA 2048]----+
|          .%B=  oo|
|          = O . o+|
|         + * * ..+|
|        . * = + o.|
|         S   * *E |
|            + * =.|
|             + B..|
|              =.=.|
|             . o.o|
+----[SHA256]-----+
[root@hybrid-Cloud-Linux-bastion-vm ocp4.8]#
```

Figure 33 Creating SSH key with ssh-keygen

```
[root@hybrid-Cloud-Linux-bastion-vm bin]# ./openshift-install create install-config --dir /root/ocp4.8/config/
? SSH Public Key /root/.ssh/id_rsa.pub
? Platform azure
? azure subscription id 99[redacted]3a0
? azure tenant id fcf6[redacted]9e9
? azure service principal client id f3[redacted]faa9
? azure service principal client secret [? for help] **********************************
? Region germanywestcentral
? Base Domain arhoclustersv4pc.net
? Cluster Name arhocluster1sv4pc
? Pull Secret [? for help] ********************************************************************************************************************
********************************************************************************************************************
********************************************************************************************************************
********************************************************************************************************************
********************************************************************************************************************
********************************************************************************************************************
********************************************************************************************************************
********************************************************************************************************************
********************************************************************************************************************
********************************************************************************************************************
********************************************************************************************************************
********************************************************************************************************************
********************************************************************************************************************
********************************************************************************************************************
********************************************************************************************************************
********************************************************************************************************************
********************************************************************************************************************
********************************************************************************************************************
********************************************************************************************************************
********************************************************************************************************************
**********
INFO Saving user credentials to "/root/.azure/osServicePrincipal.json"
INFO Credentials loaded from file "/root/.azure/osServicePrincipal.json"
```

Figure 34 Creating install-config file

```
[root@hybrid-Cloud-Linux-bastion-vm bin]#
[root@hybrid-Cloud-Linux-bastion-vm bin]#
[root@hybrid-Cloud-Linux-bastion-vm bin]# ./openshift-install create cluster --dir /root/ocp4.8/config/ --log-level=info
INFO Credentials loaded from file "/root/.azure/osServicePrincipal.json"
INFO Consuming Install Config from target directory
INFO Creating infrastructure resources...
INFO Waiting up to 20m0s for the Kubernetes API at https://api.arhocluster1sv4pc.arhoclustersv4pc.net:6443...
INFO API v1.21.6+bb8d50a up
INFO Waiting up to 30m0s for bootstrapping to complete...
INFO Destroying the bootstrap resources...
INFO Waiting up to 40m0s for the cluster at https://api.arhocluster1sv4pc.arhoclustersv4pc.net:6443 to initialize...
INFO Waiting up to 10m0s for the openshift-console route to be created...
INFO Install complete!
INFO To access the cluster as the system:admin user when using 'oc', run 'export KUBECONFIG=/root/ocp4.8/config/auth/kubeconfig'
INFO Access the OpenShift web-console here: https://console-openshift-console.apps.arhocluster1sv4pc.arhoclustersv4pc.net
INFO Login to the console with user: "kubeadmin", and password: "ii3B5-AbFPa-ujRfg-ntkYX"
INFO Time elapsed: 35m43s
[root@hybrid-Cloud-Linux-bastion-vm bin]#
```

Figure 35 Creating cluster

```
[root@hybrid-Cloud-Linux-bastion-vm auth]#
[root@hybrid-Cloud-Linux-bastion-vm auth]# export KUBECONFIG=/root/ocp4.8/config/auth/kubeconfig
[root@hybrid-Cloud-Linux-bastion-vm auth]#
[root@hybrid-Cloud-Linux-bastion-vm auth]#
[root@hybrid-Cloud-Linux-bastion-vm auth]# oc get nodes
NAME                                                STATUS   ROLES    AGE   VERSION
arhocluster1sv4pc-9w2gw-master-0                    Ready    master   31m   v1.21.6+bb8d50a
arhocluster1sv4pc-9w2gw-master-1                    Ready    master   30m   v1.21.6+bb8d50a
arhocluster1sv4pc-9w2gw-master-2                    Ready    master   31m   v1.21.6+bb8d50a
arhocluster1sv4pc-9w2gw-worker-germanywestcentral1-244l7   Ready    worker   22m   v1.21.6+bb8d50a
arhocluster1sv4pc-9w2gw-worker-germanywestcentral2-rzjm7   Ready    worker   22m   v1.21.6+bb8d50a
arhocluster1sv4pc-9w2gw-worker-germanywestcentral3-kk4rv   Ready    worker   22m   v1.21.6+bb8d50a
[root@hybrid-Cloud-Linux-bastion-vm auth]#
[root@hybrid-Cloud-Linux-bastion-vm auth]#
[root@hybrid-Cloud-Linux-bastion-vm auth]# oc get nodes -o wide
NAME                                                STATUS   ROLES    AGE   VERSION           INTERNAL-IP   EXTERNAL-IP   OS-IMAGE
                                KERNEL-VERSION                CONTAINER-RUNTIME
arhocluster1sv4pc-9w2gw-master-0                    Ready    master   31m   v1.21.6+bb8d50a   40.10.4.6     <none>        Red Hat Enterprise Linux
 CoreOS 48.84.202201241104-0 (Ootpa)   4.18.0-305.34.2.el8_4.x86_64   cri-o://1.21.4-9.rhaos4.8.gitaebb17b.el8
arhocluster1sv4pc-9w2gw-master-1                    Ready    master   31m   v1.21.6+bb8d50a   40.10.4.5     <none>        Red Hat Enterprise Linux
 CoreOS 48.84.202201241104-0 (Ootpa)   4.18.0-305.34.2.el8_4.x86_64   cri-o://1.21.4-9.rhaos4.8.gitaebb17b.el8
arhocluster1sv4pc-9w2gw-master-2                    Ready    master   31m   v1.21.6+bb8d50a   40.10.4.7     <none>        Red Hat Enterprise Linux
 CoreOS 48.84.202201241104-0 (Ootpa)   4.18.0-305.34.2.el8_4.x86_64   cri-o://1.21.4-9.rhaos4.8.gitaebb17b.el8
arhocluster1sv4pc-9w2gw-worker-germanywestcentral1-244l7   Ready    worker   23m   v1.21.6+bb8d50a   40.10.5.4     <none>        Red Hat Enterprise Linux
 CoreOS 48.84.202201241104-0 (Ootpa)   4.18.0-305.34.2.el8_4.x86_64   cri-o://1.21.4-9.rhaos4.8.gitaebb17b.el8
arhocluster1sv4pc-9w2gw-worker-germanywestcentral2-rzjm7   Ready    worker   23m   v1.21.6+bb8d50a   40.10.5.5     <none>        Red Hat Enterprise Linux
 CoreOS 48.84.202201241104-0 (Ootpa)   4.18.0-305.34.2.el8_4.x86_64   cri-o://1.21.4-9.rhaos4.8.gitaebb17b.el8
arhocluster1sv4pc-9w2gw-worker-germanywestcentral3-kk4rv   Ready    worker   23m   v1.21.6+bb8d50a   40.10.5.6     <none>        Red Hat Enterprise Linux
 CoreOS 48.84.202201241104-0 (Ootpa)   4.18.0-305.34.2.el8_4.x86_64   cri-o://1.21.4-9.rhaos4.8.gitaebb17b.el8
[root@hybrid-Cloud-Linux-bastion-vm auth]#
```

Figure 36 Logging in and checking the node status

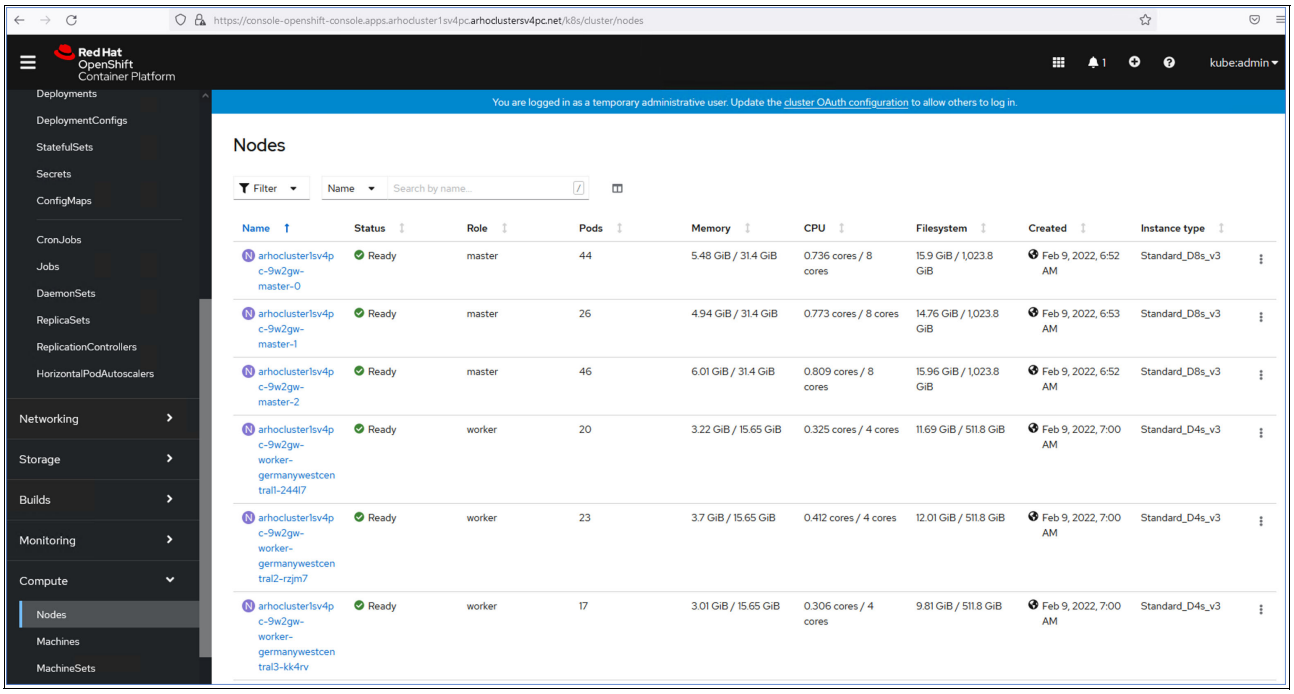


Figure 37 Checking the cluster status with web console

9. Install the IBM Block Storage CSI driver on RHOCP on Microsoft Azure Cloud.

   As shown in Figure 38, Open the RHOCP console URL from the browsers of your choice and log in by using `kubeadmin`. Click the **Operator** hub and install the IBM Block Storage CSI driver. For more information, see this IBM Documentation web page.

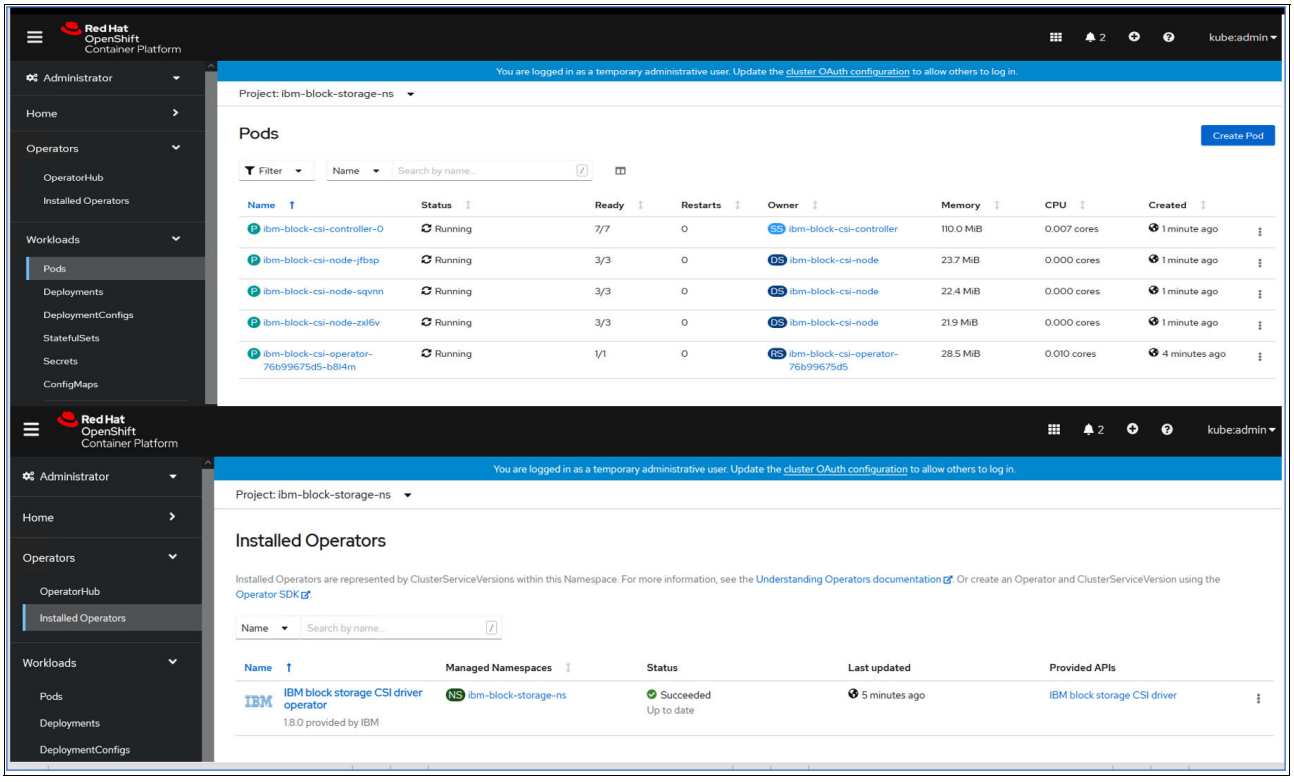


Figure 38 Installing IBM Block storage CSI driver

10. Complete the following steps to install IBM Spectrum Virtualize for Public Cloud on Microsoft Azure Cloud:
    a. Log in to the Microsoft Azure portal at `https://portal.azure.com`.
    b. Select **market place** → **Private Products** → **IBM Spectrum Virtualize for Public Cloud**.
    c. Click **Create** (see Figure 39 - Figure 47 on page 38).

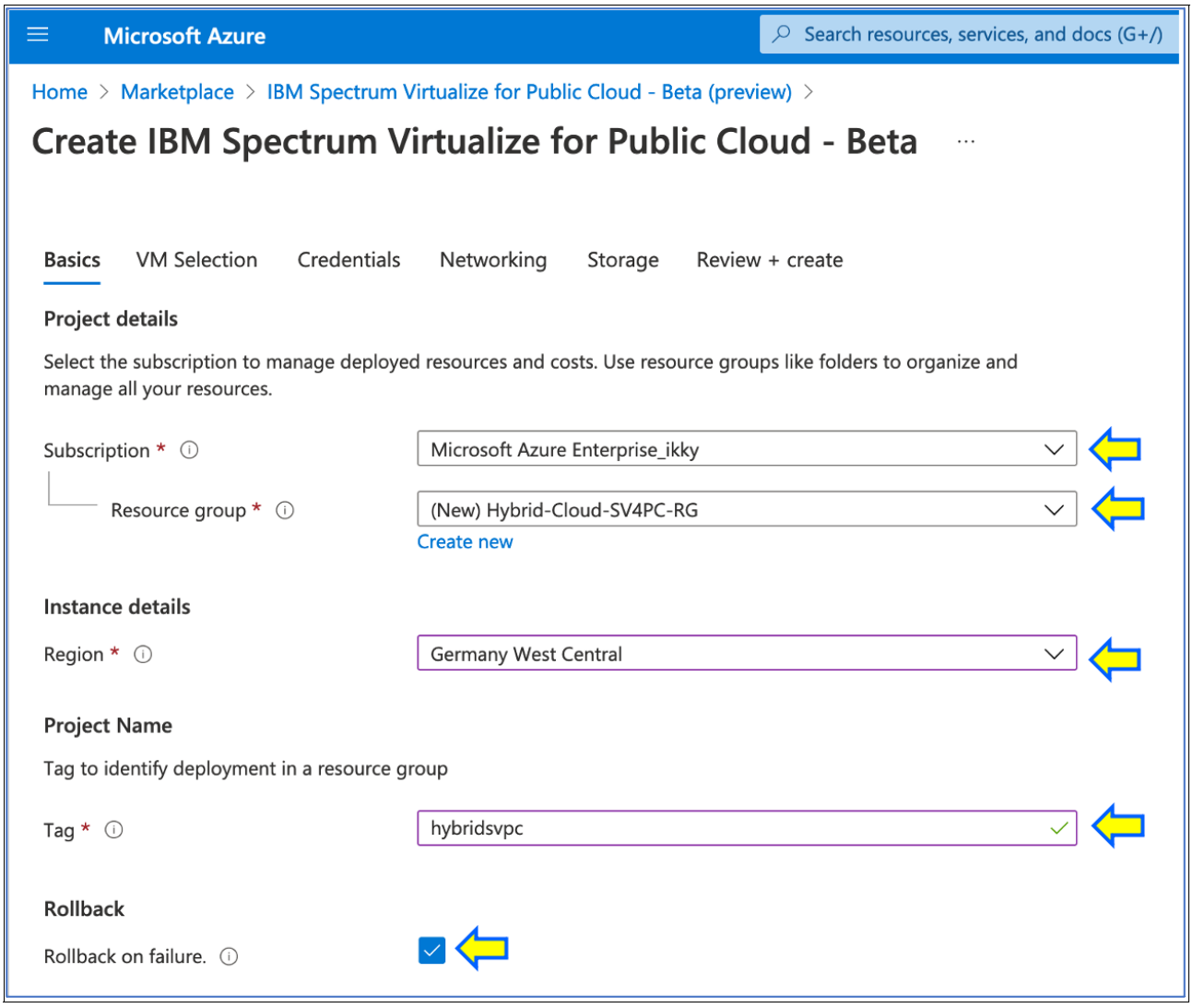


Figure 39 Basic product details

Figure 40 Selecting VM to create SV4PC on Azure

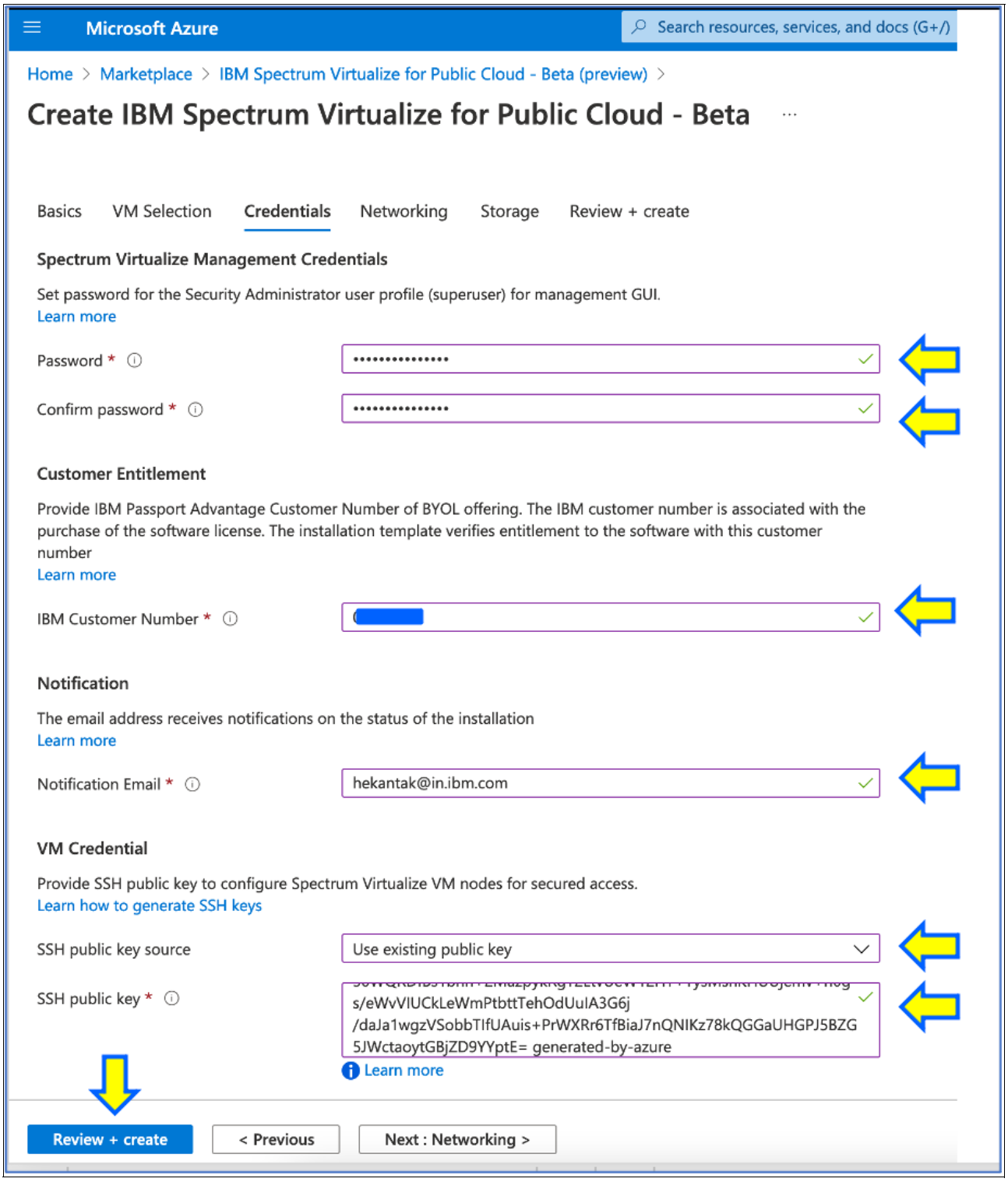


Figure 41 Providing credentials to create SV4PC on Azure

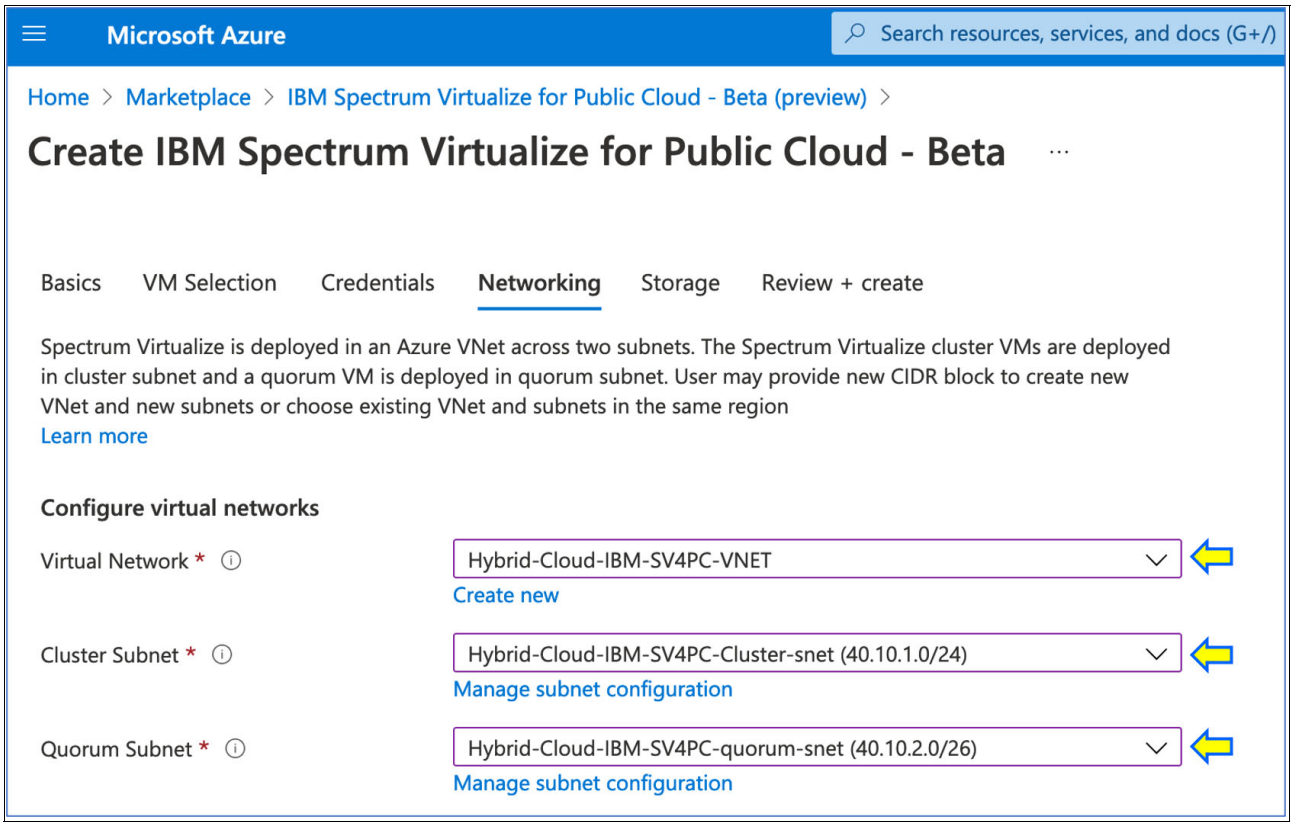


Figure 42 Networking details

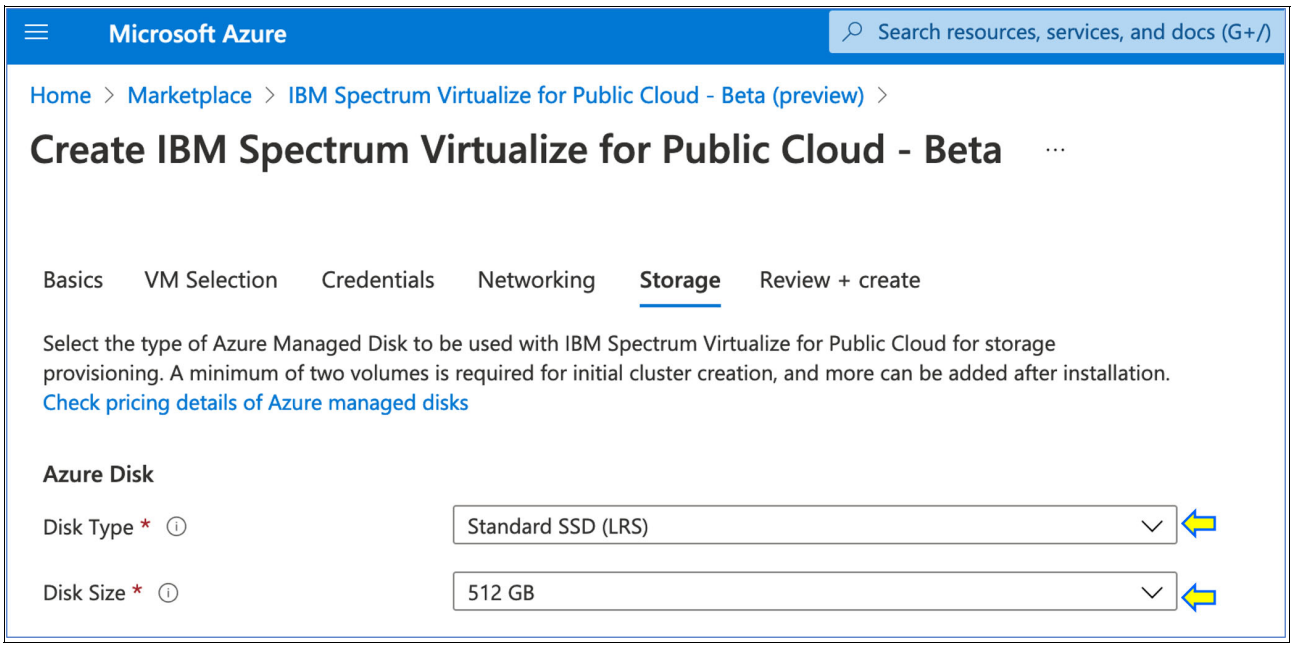


Figure 43 Storage details

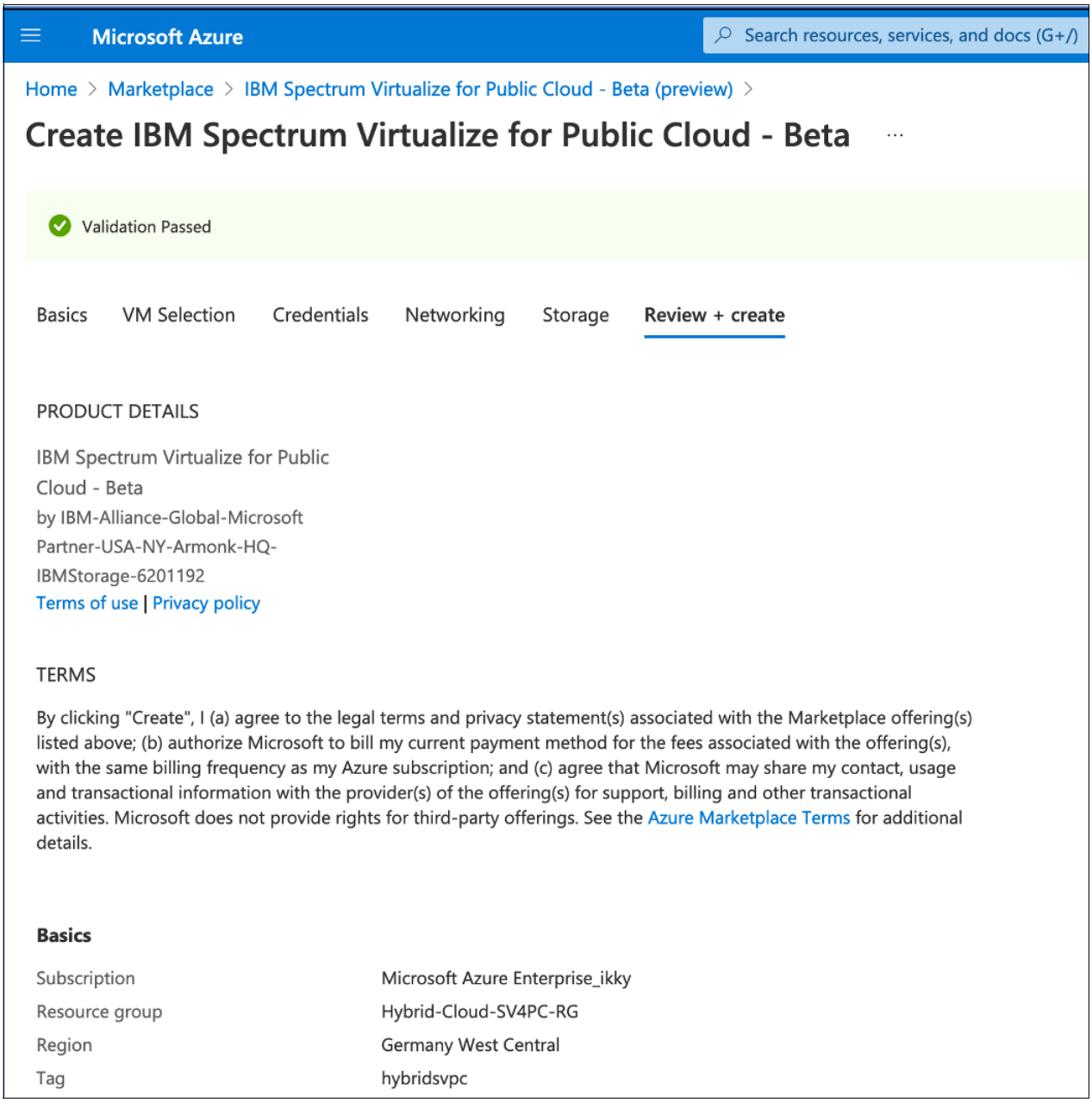


Figure 44 Review + create option

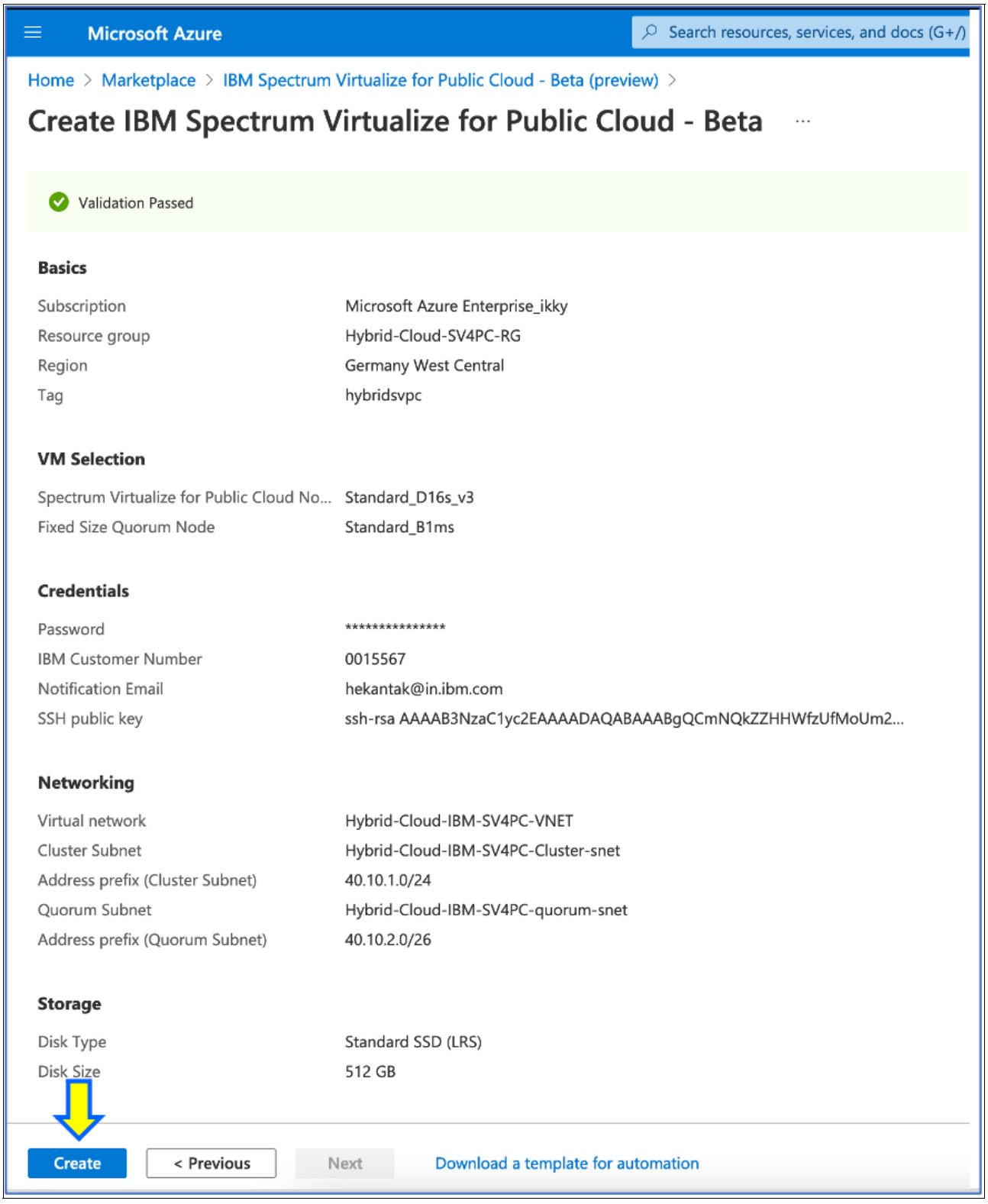


Figure 45 Creating SV4PC

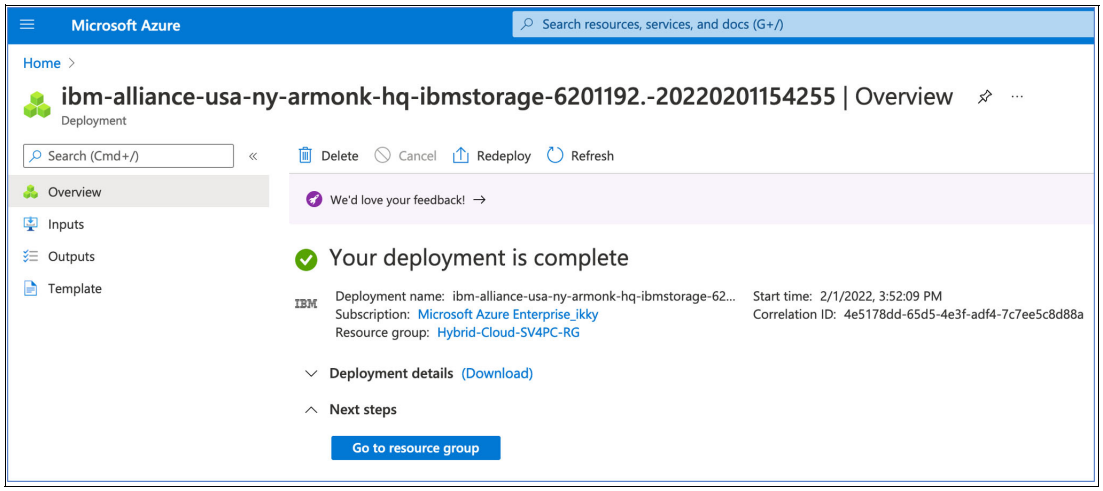


Figure 46 Checking the deployment

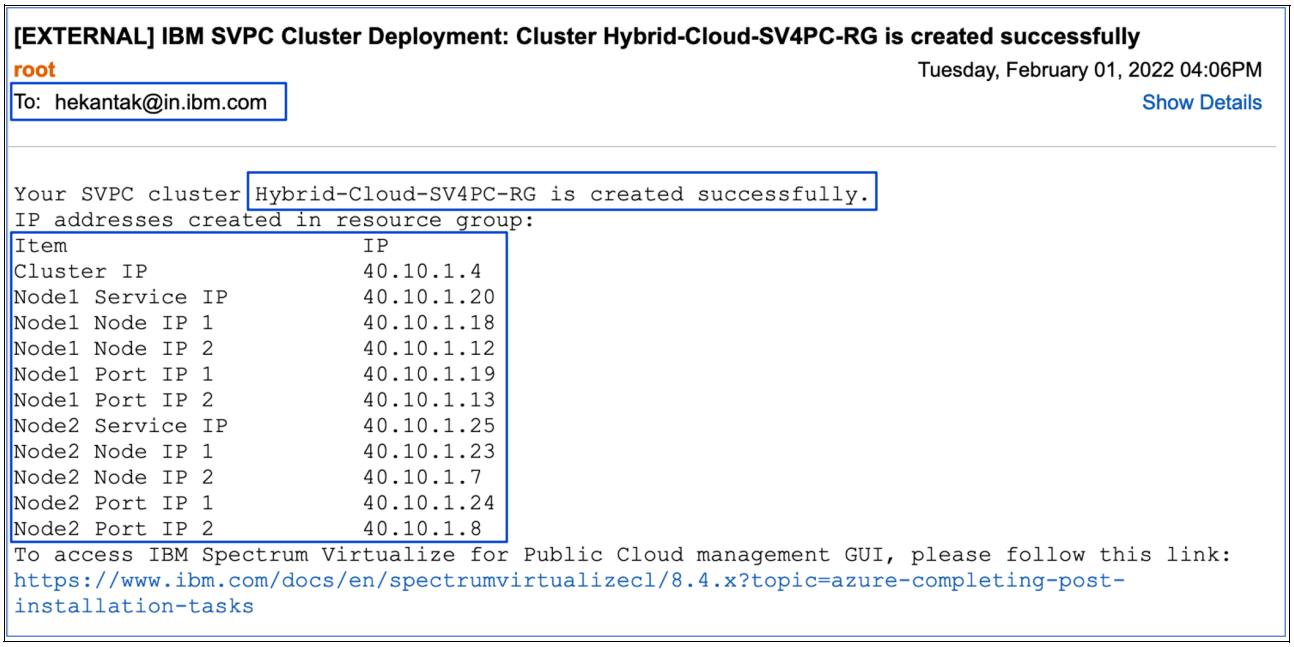


Figure 47 Checking email for cluster IP details

11. Create a Windows 2019 VM on Microsoft Azure Cloud or log in to the Windows VM from your on-premises Windows host and open the web browser of your choice to configure the newly deployed SV4PC storage on Azure Cloud.
12. Log in to the cluster IP at `https://40.10.1.4:8443/login` to complete the configuration for the newly deployed SV4PC (see Figure 47).
13. Click **Next**. Select **Agree with the terms in the License agreement**. Enter the password and then, click **Apply**. Then, click **Next**.
14. Enter the following information:
    - Name of the system
    - External Virtualization
    - Capacity in TB
    - DNS
    - Storage IBM Insight®

15. Click **Finish** to complete the setup.

16. Log in to the Storage at `https://40.10.1.4:8443/login` and check the status (see Figure 48).

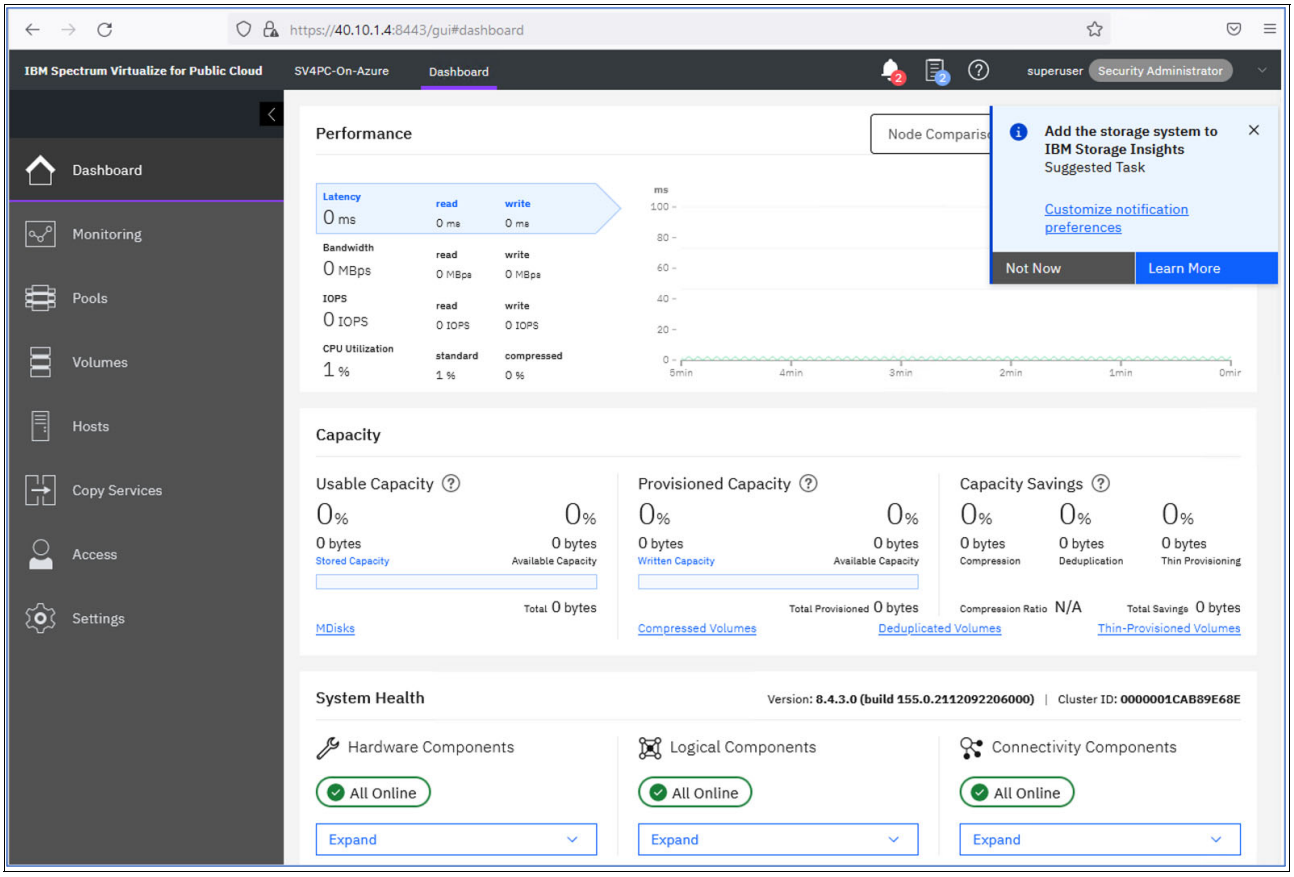


Figure 48 Checking the status of storage

17. Complete the following steps to create host mapping in SV4PC Storage for RHOCP Worker nodes with iSCSI connection:

    a. Log in to the Microsoft Azure portal at `https://portal.azure.com`.

    b. Log in to the Linux VM by using `azureuser` and the SSH key that uses the Bastion service or by using SSH and get the initiator name from the RHOCP worker nodes.

    c. Create the host mapping for the worker nodes, as shown in Figure 49 on page 40 - Figure 52 on page 41.

    d. Repeat the same procedure for all the worker nodes in the cluster. Then, run **`iscsiadm`** commands for the iSCSI login.

```
[root@hybrid-Cloud-Linux-bastion-vm yaml]#
[root@hybrid-Cloud-Linux-bastion-vm yaml]# oc get nodes
NAME                                                STATUS   ROLES    AGE     VERSION
arhocluster1sv4pc-9w2gw-master-0                    Ready    master   6h22m   v1.21.6+bb8d50a
arhocluster1sv4pc-9w2gw-master-1                    Ready    master   6h21m   v1.21.6+bb8d50a
arhocluster1sv4pc-9w2gw-master-2                    Ready    master   6h22m   v1.21.6+bb8d50a
arhocluster1sv4pc-9w2gw-worker-germanywestcentral1-24417   Ready    worker   6h13m   v1.21.6+bb8d50a
arhocluster1sv4pc-9w2gw-worker-germanywestcentral2-rzjm7   Ready    worker   6h13m   v1.21.6+bb8d50a
arhocluster1sv4pc-9w2gw-worker-germanywestcentral3-kk4rv   Ready    worker   6h13m   v1.21.6+bb8d50a
[root@hybrid-Cloud-Linux-bastion-vm yaml]#
[root@hybrid-Cloud-Linux-bastion-vm yaml]# ssh core@arhocluster1sv4pc-9w2gw-worker-germanywestcentral1-24417 cat /etc/iscs
i/initiatorname.iscsi
InitiatorName=iqn.1994-05.com.redhat:402e6796fb6e
[root@hybrid-Cloud-Linux-bastion-vm yaml]#
[root@hybrid-Cloud-Linux-bastion-vm yaml]# ssh core@arhocluster1sv4pc-9w2gw-worker-germanywestcentral2-rzjm7 cat /etc/iscs
i/initiatorname.iscsi
InitiatorName=iqn.1994-05.com.redhat:25dd27569eb1
[root@hybrid-Cloud-Linux-bastion-vm yaml]#
[root@hybrid-Cloud-Linux-bastion-vm yaml]# ssh core@arhocluster1sv4pc-9w2gw-worker-germanywestcentral3-kk4rv cat /etc/iscs
i/initiatorname.iscsi
InitiatorName=iqn.1994-05.com.redhat:113148c0f72e
[root@hybrid-Cloud-Linux-bastion-vm yaml]#
```

Figure 49 Getting iSCSI initiator name

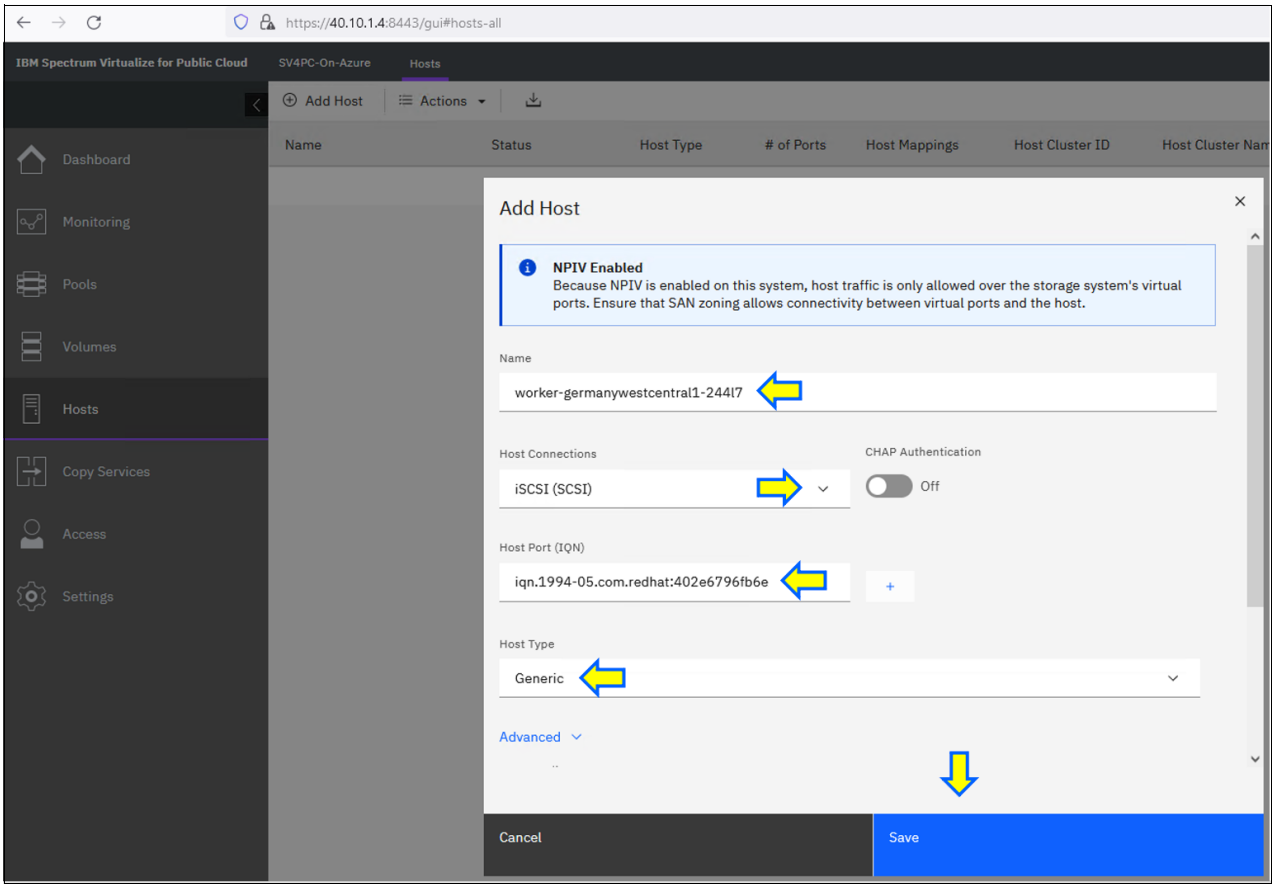


Figure 50 Defining host mapping

```
[root@arhocluster1sv4pc-9w2gw-worker-germanywestcentral1-24417 ~]#
[root@arhocluster1sv4pc-9w2gw-worker-germanywestcentral1-24417 ~]# iscsiadm -m discoverydb -t st -p 40.10.1.13:3260 --disc
over
40.10.1.19:3260,1 iqn.1986-03.com.ibm:2145.sv4pc-on-azure.node1
40.10.1.13:3260,1 iqn.1986-03.com.ibm:2145.sv4pc-on-azure.node1
[root@arhocluster1sv4pc-9w2gw-worker-germanywestcentral1-24417 ~]#
[root@arhocluster1sv4pc-9w2gw-worker-germanywestcentral1-24417 ~]# iscsiadm -m discoverydb -t st -p 40.10.1.8:3260 --discover
40.10.1.24:3260,1 iqn.1986-03.com.ibm:2145.sv4pc-on-azure.node2
40.10.1.8:3260,1 iqn.1986-03.com.ibm:2145.sv4pc-on-azure.node2
[root@arhocluster1sv4pc-9w2gw-worker-germanywestcentral1-24417 ~]#
[root@arhocluster1sv4pc-9w2gw-worker-germanywestcentral1-24417 ~]# iscsiadm -m node -p 40.10.1.13 --login
Logging in to [iface: default, target: iqn.1986-03.com.ibm:2145.sv4pc-on-azure.node1, portal: 40.10.1.13,3260]
Login to [iface: default, target: iqn.1986-03.com.ibm:2145.sv4pc-on-azure.node1, portal: 40.10.1.13,3260] successful.
[root@arhocluster1sv4pc-9w2gw-worker-germanywestcentral1-24417 ~]#
[root@arhocluster1sv4pc-9w2gw-worker-germanywestcentral1-24417 ~]# iscsiadm -m node -p 40.10.1.8 --login
Logging in to [iface: default, target: iqn.1986-03.com.ibm:2145.sv4pc-on-azure.node2, portal: 40.10.1.8,3260]
Login to [iface: default, target: iqn.1986-03.com.ibm:2145.sv4pc-on-azure.node2, portal: 40.10.1.8,3260] successful.
[root@arhocluster1sv4pc-9w2gw-worker-germanywestcentral1-24417 ~]#


[root@arhocluster1sv4pc-9w2gw-worker-germanywestcentral2-rzjm7 ~]#
[root@arhocluster1sv4pc-9w2gw-worker-germanywestcentral2-rzjm7 ~]# iscsiadm -m discoverydb -t st -p 40.10.1.13:3260 --discover
40.10.1.19:3260,1 iqn.1986-03.com.ibm:2145.sv4pc-on-azure.node1
40.10.1.13:3260,1 iqn.1986-03.com.ibm:2145.sv4pc-on-azure.node1
[root@arhocluster1sv4pc-9w2gw-worker-germanywestcentral2-rzjm7 ~]# iscsiadm -m discoverydb -t st -p 40.10.1.8:3260 --discover
40.10.1.24:3260,1 iqn.1986-03.com.ibm:2145.sv4pc-on-azure.node2
40.10.1.8:3260,1 iqn.1986-03.com.ibm:2145.sv4pc-on-azure.node2
[root@arhocluster1sv4pc-9w2gw-worker-germanywestcentral2-rzjm7 ~]# iscsiadm -m node -p 40.10.1.13 --login
Logging in to [iface: default, target: iqn.1986-03.com.ibm:2145.sv4pc-on-azure.node1, portal: 40.10.1.13,3260]
Login to [iface: default, target: iqn.1986-03.com.ibm:2145.sv4pc-on-azure.node1, portal: 40.10.1.13,3260] successful.
[root@arhocluster1sv4pc-9w2gw-worker-germanywestcentral2-rzjm7 ~]# iscsiadm -m node -p 40.10.1.8 --login
Logging in to [iface: default, target: iqn.1986-03.com.ibm:2145.sv4pc-on-azure.node2, portal: 40.10.1.8,3260]
Login to [iface: default, target: iqn.1986-03.com.ibm:2145.sv4pc-on-azure.node2, portal: 40.10.1.8,3260] successful.
[root@arhocluster1sv4pc-9w2gw-worker-germanywestcentral2-rzjm7 ~]#
```

Figure 51 Running iscsiadm commands

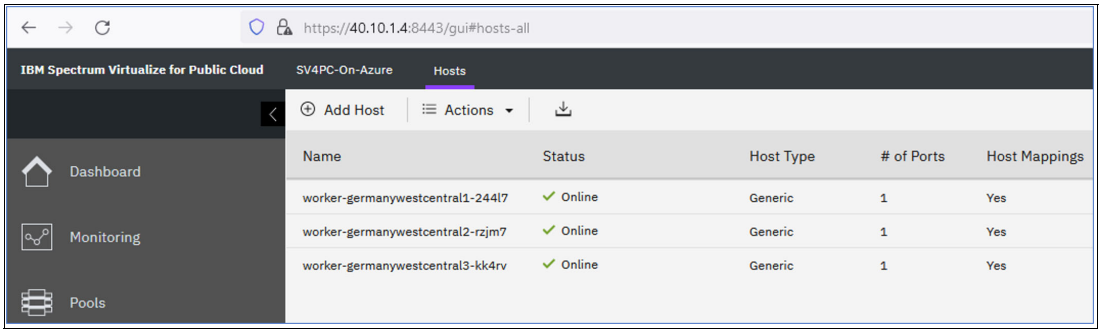


Figure 52 Checking the host status

18. Complete the following steps to create the Storage secret and Storage class on RHOCP on Microsoft Azure Cloud:

    a. Log in to the Microsoft Azure portal at https://portal.azure.com.

    b. Log in to the Linux VM by using azureuser and the SSH key that uses the Bastion service or by using SSH.

    c. Create the Storage secret and Storage class (see Figure 53 and Figure 54).

```
[root@hybrid-Cloud-Linux-bastion-vm yaml]# cat ibm-sv4pc-storage-secret.yaml
kind: Secret
apiVersion: v1
metadata:
  name: ibm-sv4pc-storage-secret
  namespace: ibm-block-storage-ns
type: Opaque
stringData:
  management_address: 40.10.1.4
  username: superuser
data:
  password: SWJtU3Y0cGNvbkF6dXJlCg==
[root@hybrid-Cloud-Linux-bastion-vm yaml]#
[root@hybrid-Cloud-Linux-bastion-vm yaml]# oc create -f ibm-sv4pc-storage-secret.yaml
secret/ibm-sv4pc-storage-secret created
[root@hybrid-Cloud-Linux-bastion-vm yaml]#
[root@hybrid-Cloud-Linux-bastion-vm yaml]#
```

Figure 53 Creating Storage secret

```
[root@hybrid-Cloud-Linux-bastion-vm yaml]# cat ibm-sv4pc-storage-class.yaml
kind: StorageClass
apiVersion: storage.k8s.io/v1
metadata:
  name: ibm-block-storage-class-sv4pc
  annotations:
    description: ibm-block-storage-class-sv4pc
provisioner: block.csi.ibm.com
parameters:
  pool: CloudPool0
  SpaceEfficiency: thin
  volume_name_prefix: SV4PC-AZ
  csi.storage.k8s.io/fstype: xfs
  csi.storage.k8s.io/secret-name: ibm-sv4pc-storage-secret
  csi.storage.k8s.io/secret-namespace: ibm-block-storage-ns
reclaimPolicy: Delete
allowVolumeExpansion: true
volumeBindingMode: Immediate

[root@hybrid-Cloud-Linux-bastion-vm yaml]# oc create -f ibm-sv4pc-storage-class.yaml
storageclass.storage.k8s.io/ibm-block-storage-class-sv4pc created
[root@hybrid-Cloud-Linux-bastion-vm yaml]#
```

Figure 54 Creating Storage class

19. Install the following components:
    - Red Hat OpenShift container Platform. For more information, see the following resources:
        - *IBM Storage for Red Hat OpenShift*, REDP-5565
        - This Red Hat Documentation web page
    - IBM Block storage CSI driver v1.8. For more information, see this IBM Documentation web page.
    - IBM FlashSystem Storage FS9100 and Create host mapping and iSCSI connection for on-premises RHOCP worker nodes and host, as described in Step 17 on page 39.

With these steps completed, the hardware, software, and hybrid cloud networking setup process is complete and the use case demonstration is available.

Use case demonstration

This use case demonstration shows how the on-premises data can be made available to remote sites and Microsoft Azure Cloud by using the following methods:

- Volume replication by using IBM Storage Global mirror
- Data replication by using IBM Block Storage CSI driver volume replication

These methods are described next.

Volume replication by using IBM Storage Global Mirror feature

Note: In this use case demonstration we did *not* use the Global Mirror with Change Volumes (GMCV) replication method. The customer can use this method if wanted.

The steps in this demonstration show how the on-premises data can be made available to remote sites and public clouds by using the components that are described in this Blueprint.

For more information about steps that can be taken to ensure database data consistency, see the specific product documentation.

Complete the following steps:

1. Log in to the on-premises RHOCP bastion hosts or the host from where the RHOCP cluster can be accessed by using **`oc cli`** command tools.
2. Create the Storage secret and Storage class, as shown in Figure 55 on page 44 and Figure 56 on page 44.

```
[root@gw-10 yaml]#
[root@gw-10 yaml]# oc project
Using project "ibm-flashsystem-csi" on server "https://api.sha.spp-mcm.kb.stglabs.ibm.com:6443".
[root@gw-10 yaml]#
[root@gw-10 yaml]# ls -l
total 24
-rw-r--r--. 1 root root  212 Feb 12 07:51 01-ibm-block-storage-secret.yaml
-rw-r--r--. 1 root root  490 Feb 12 07:53 02-ibm-block-storageclass.yaml
-rw-r--r--. 1 root root 4135 Jan 27 04:01 install-config.yaml
-rw-r--r--. 1 root root 4135 Jan 27 04:07 install-config.yaml.orig
drwxr-xr-x. 2 root root   62 Jan 27 13:01 MySQL
[root@gw-10 yaml]# cat 01-ibm-block-storage-secret.yaml
apiVersion: v1
data:
  management_address: MTAuMC4yNDAuMzA=
  password: cGFzc3cwcmQ=
  username: c3VwZXJ1c2Vy
kind: Secret
metadata:
  name: ibm-block-storage-secret
  namespace: ibm-flashsystem-csi
type: Opaque
[root@gw-10 yaml]# oc create -f 01-ibm-block-storage-secret.yaml
secret/ibm-block-storage-secret created
[root@gw-10 yaml]#
[root@gw-10 yaml]# oc get secrets ibm-block-storage-secret
NAME                       TYPE     DATA   AGE
ibm-block-storage-secret   Opaque   3      15s
[root@gw-10 yaml]#
```

Figure 55 Creating Storage secret

```
[root@gw-10 yaml]# oc project
Using project "ibm-flashsystem-csi" on server "https://api.sha.spp-mcm.kb.stglabs.ibm.com:6443".
[root@gw-10 yaml]#
[root@gw-10 yaml]# ls
01-ibm-block-storage-secret.yaml  02-ibm-block-storageclass.yaml  install-config.yaml  install-config.yaml.orig  MySQL
[root@gw-10 yaml]#
[root@gw-10 yaml]# cat 02-ibm-block-storageclass.yaml
allowVolumeExpansion: true
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  annotations:
    description: ibm-block-storage-class
  name: ibm-block-storage-class
parameters:
  SpaceEfficiency: thin
  csi.storage.k8s.io/fstype: xfs
  csi.storage.k8s.io/secret-name: ibm-block-storage-secret
  csi.storage.k8s.io/secret-namespace: ibm-flashsystem-csi
  pool: SVPC Pool
  volume_name_prefix: hybrid
provisioner: block.csi.ibm.com
reclaimPolicy: Delete
volumeBindingMode: Immediate
[root@gw-10 yaml]#
[root@gw-10 yaml]# oc create -f 02-ibm-block-storageclass.yaml
storageclass.storage.k8s.io/ibm-block-storage-class created
[root@gw-10 yaml]#
[root@gw-10 yaml]# oc get sc
NAME                      PROVISIONER                    RECLAIMPOLICY   VOLUMEBINDINGMODE   ALLOWVOLUMEEXPANSION   AGE
ibm-block-storage-class   block.csi.ibm.com              Delete          Immediate           true                   <invalid>
thin (default)            kubernetes.io/vsphere-volume   Delete          Immediate           false                  15d
[root@gw-10 yaml]#
```

Figure 56 Creating Storage class

3. Create a project and namespace and then, create the yaml files for the PV claim and MySQL deployment yaml file, as shown in Figure 57.

```
[root@gw-10 MySQL]# oc project
Using project "mysql" on server "https://api.sha.spp-mcm.kb.stglabs.ibm.com:6443".
[root@gw-10 MySQL]#
[root@gw-10 MySQL]# ls
01-mysqlpvc.yaml  02-mysql-deployment.yaml
[root@gw-10 MySQL]#
[root@gw-10 MySQL]# cat 01-mysqlpvc.yaml
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: mysql-pvc
spec:
  accessModes:
  - ReadWriteOnce
  resources:
    requests:
      storage: 20Gi
  storageClassName: ibm-block-storage-class
[root@gw-10 MySQL]#
[root@gw-10 MySQL]# oc create -f 01-mysqlpvc.yaml
persistentvolumeclaim/mysql-pvc created
[root@gw-10 MySQL]#
[root@gw-10 MySQL]# oc get pv,pvc
NAME                                                        CAPACITY   ACCESS MODES   RECLAIM POLICY   STATUS   CLAIM               STORAGECLASS
  REASON   AGE
persistentvolume/pvc-96a829c2-db25-48bc-8ad8-6d334e19323c   20Gi       RWO            Delete           Bound    mysql/mysql-pvc     ibm-block-storage-class
           5s

NAME                                STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS              AGE
persistentvolumeclaim/mysql-pvc     Bound    pvc-96a829c2-db25-48bc-8ad8-6d334e19323c   20Gi       RWO            ibm-block-storage-class   8s
[root@gw-10 MySQL]#
```

Figure 57 Creating PVC pvc for mysql

4. Confirm that the volume was created on the on-premises IBM FlashSystem storage FS9100, as shown in Figure 58.

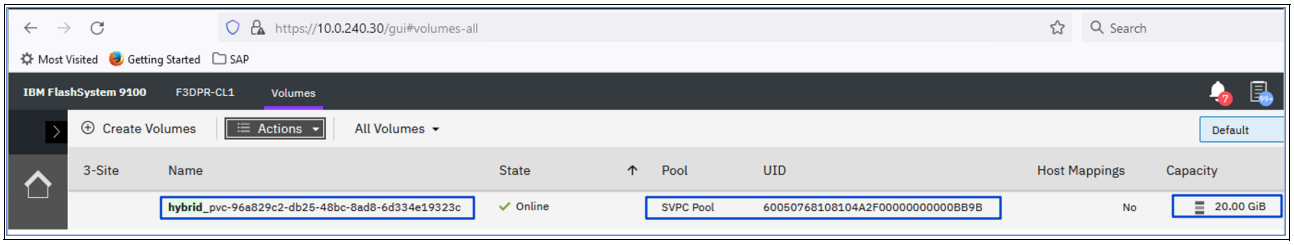


Figure 58 Checking that the volume and LUN are created on storage

5. Create the MySQL deployment yaml file and the MySQL containerized database, as shown in Figure 59 on page 46.

```
01-mysqlpvc.yaml  02-mysql-deployment.yaml
[root@gw-10 MySQL]#
[root@gw-10 MySQL]# cat 02-mysql-deployment.yaml
---
apiVersion: v1
kind: Service
metadata:
  name: mysql
spec:
  ports:
  - port: 3306
  selector:
    app: mysql
  clusterIP: None
---
apiVersion: apps/v1 # for versions before 1.9.0 use apps/v1beta2
kind: Deployment
metadata:
  name: mysql
spec:
  selector:
    matchLabels:
      app: mysql
  strategy:
    type: Recreate
  template:
    metadata:
      labels:
        app: mysql
    spec:
      containers:
      - image: mysql:5.6
        name: mysql
        env:
          # Use secret in real usage
        - name: MYSQL_ROOT_PASSWORD
          value: password
        ports:
        - containerPort: 3306
          name: mysql
        volumeMounts:
        - name: mysql-persistent-storage
          mountPath: /var/lib/mysql
      volumes:
      - name: mysql-persistent-storage
        persistentVolumeClaim:
          claimName: mysql-pvc
[root@gw-10 MySQL]#
[root@gw-10 MySQL]# oc create -f 02-mysql-deployment.yaml
service/mysql created
deployment.apps/mysql created
[root@gw-10 MySQL]#
```

Figure 59 Creating mysql yaml file and deploying mysql

6. Log in to the MySQL pod and check whether the MySQL deployment was successful, as shown in Figure 60.

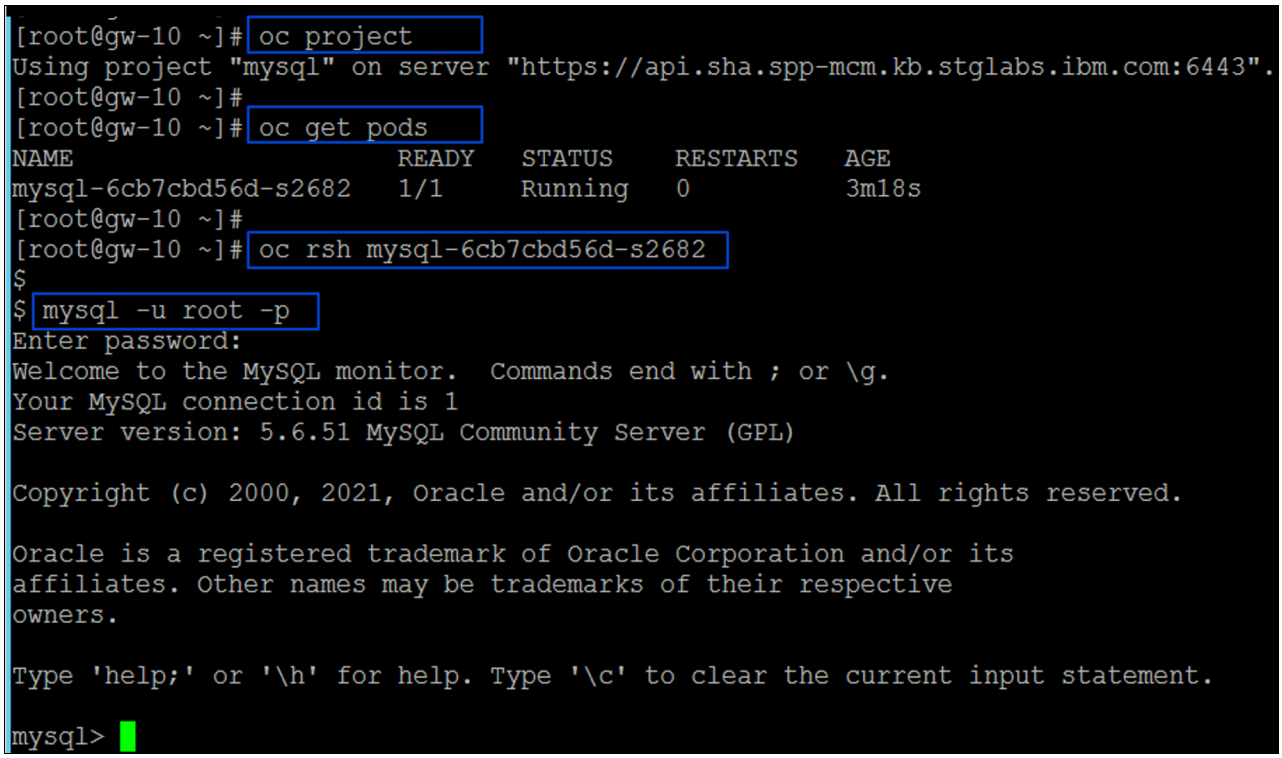


Figure 60 Logging in to mysql pod

7. Create the sample database and table and then, insert data into table and show the table contents (see Figure 61).

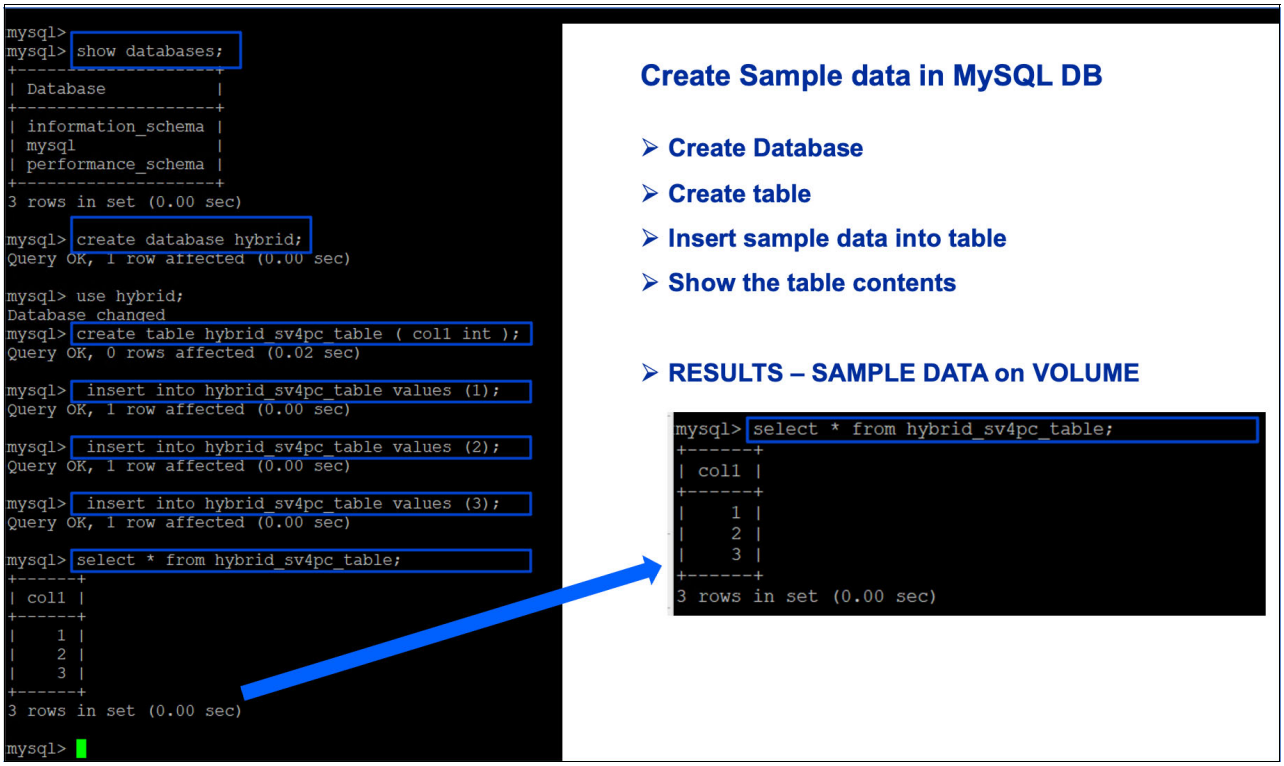


Figure 61 Creating database and insert sample data

The next part of the process involves replicating the on-premises storage volume or LUN with the equal sized volume or LUN on the SV4PC storage that is deployed on Microsoft Azure Cloud. The data replication is performed by using IBM Global mirror replication.

Complete the following steps:

1. Log in to the SV4PC storage on the Azure Cloud and the, create the 20Gi volume, as shown in Figure 62 and Figure 63 on page 50.

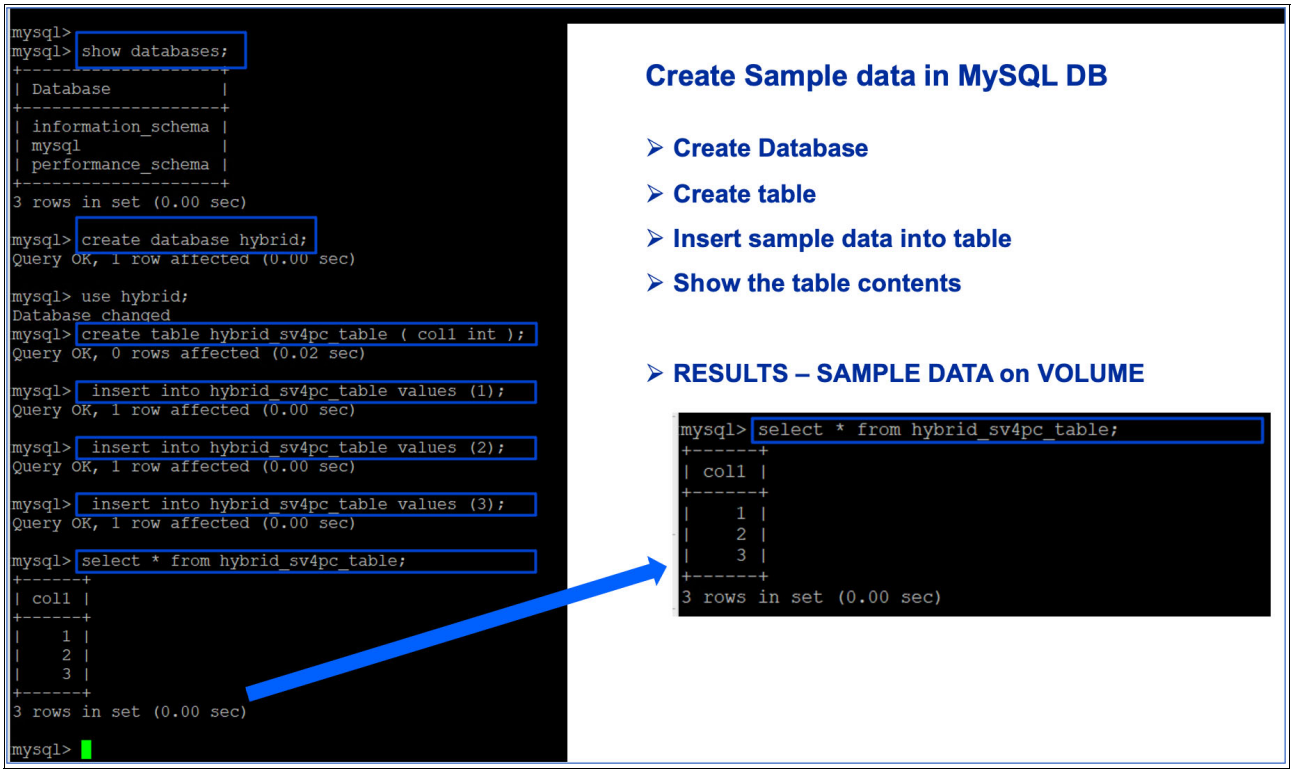


Figure 62 Creating 20gi volume on sv4pc on Azure

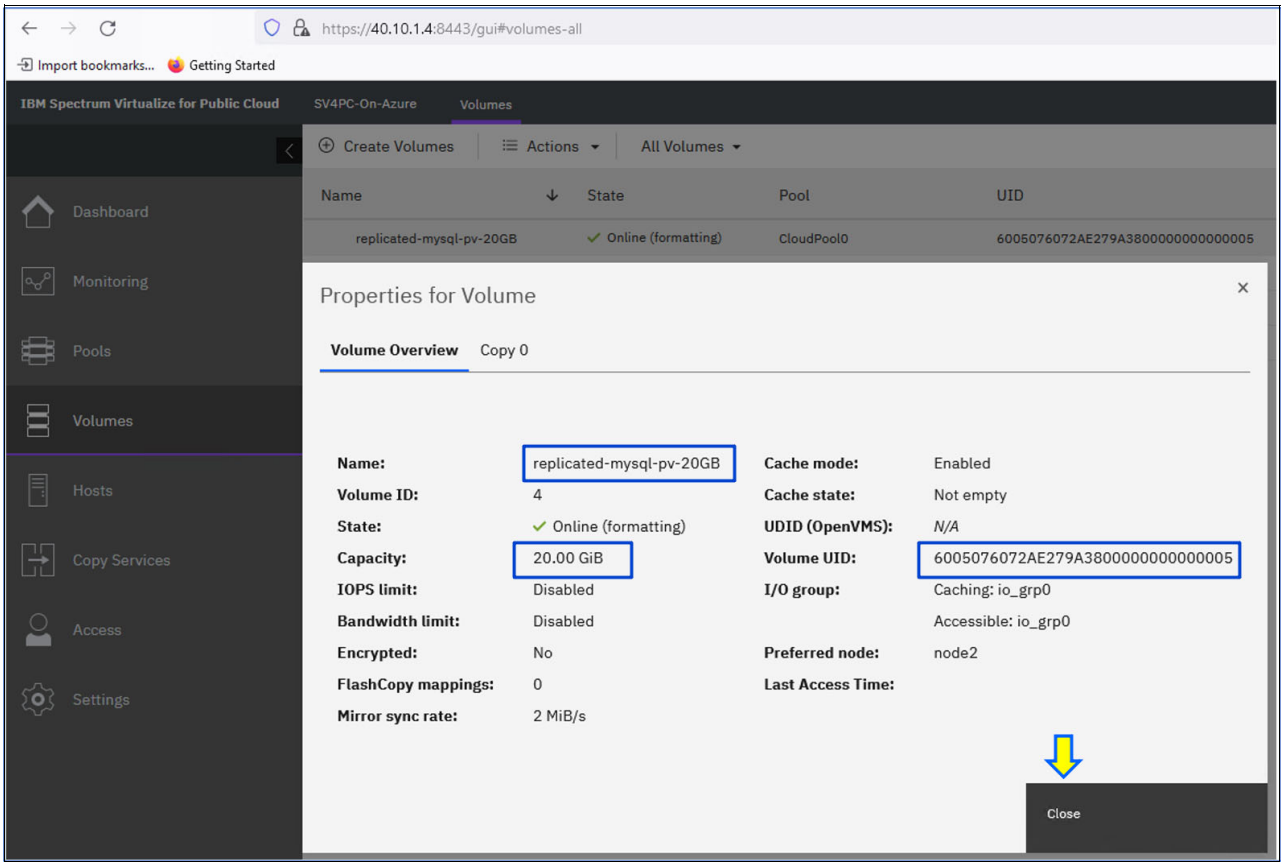


Figure 63 Checking the volume properties

2. Log in to the IBM FlashSystem FS9100 storage (on-premises) and SV4PC storage on Azure and complete the following steps to replicate the data on the volume, as shown in Figure 64 on page 51 - Figure 74 on page 55):

   a. Create a partnership from on-premises storage.
   b. Create a partnership from SV4PC storage on Azure Cloud.
   c. Add a Consistency Group.
   d. Create a relationship and start copying the data that is on the volume.
   e. Stop the Remote-copy Consistency Group.

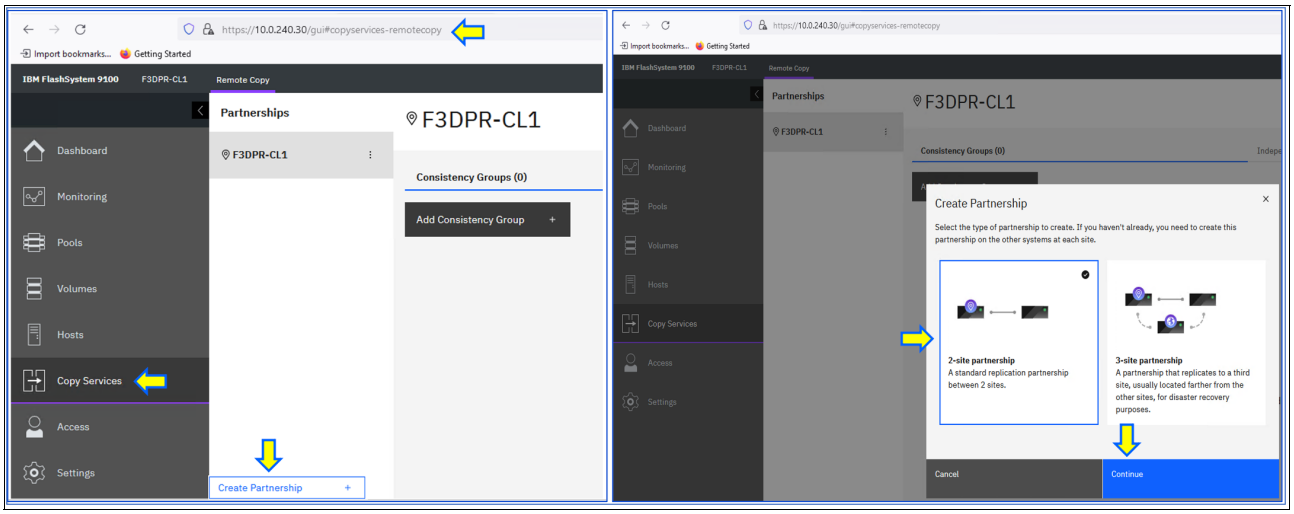


Figure 64 Creating partnership: On-premises storage, Part 1

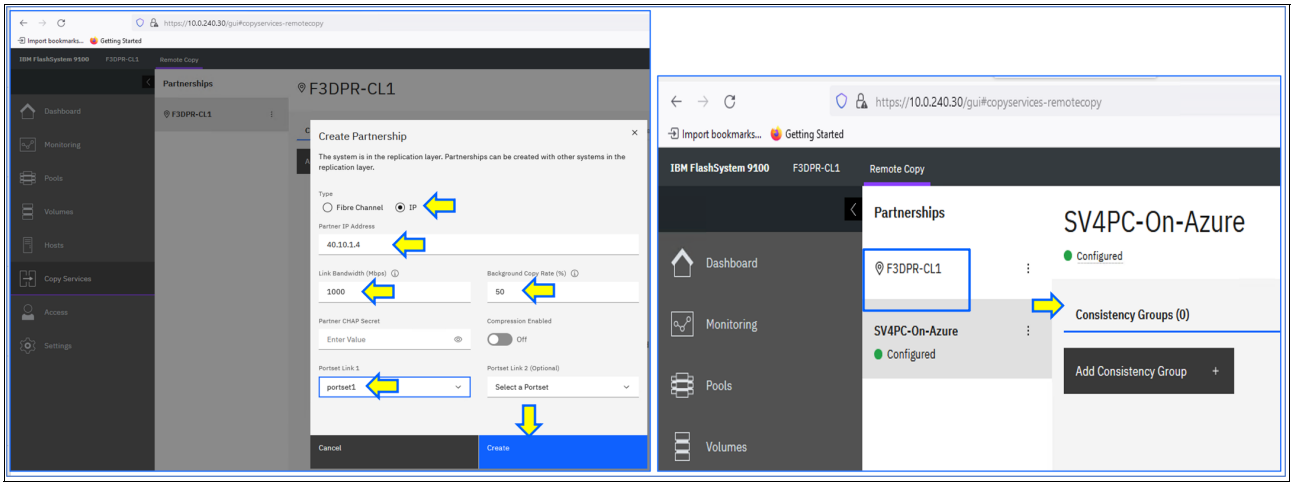


Figure 65 Creating partnership: On-premise storage, Part 2

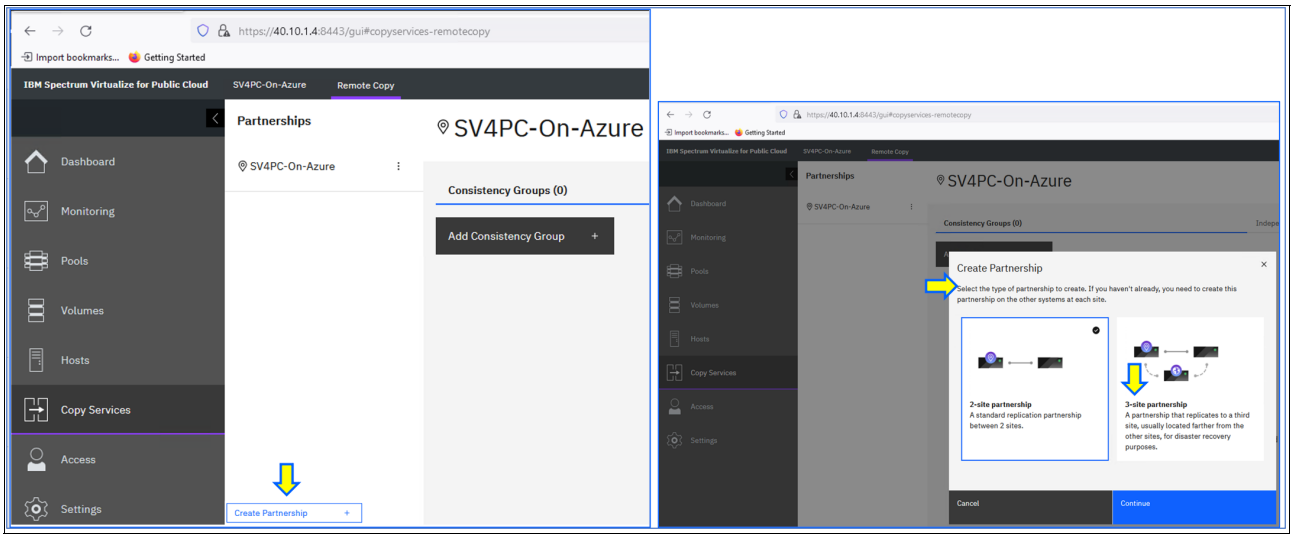


Figure 66 Creating partnership: sv4pc on Azure, Part 1

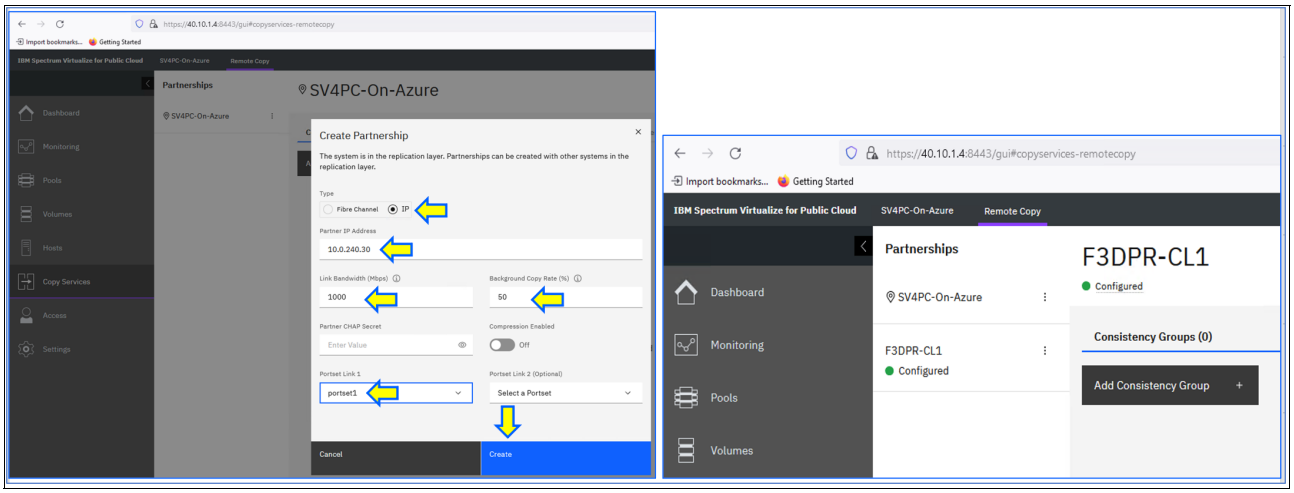


Figure 67 Creating partnership: sv4pc on Azure, Part 2

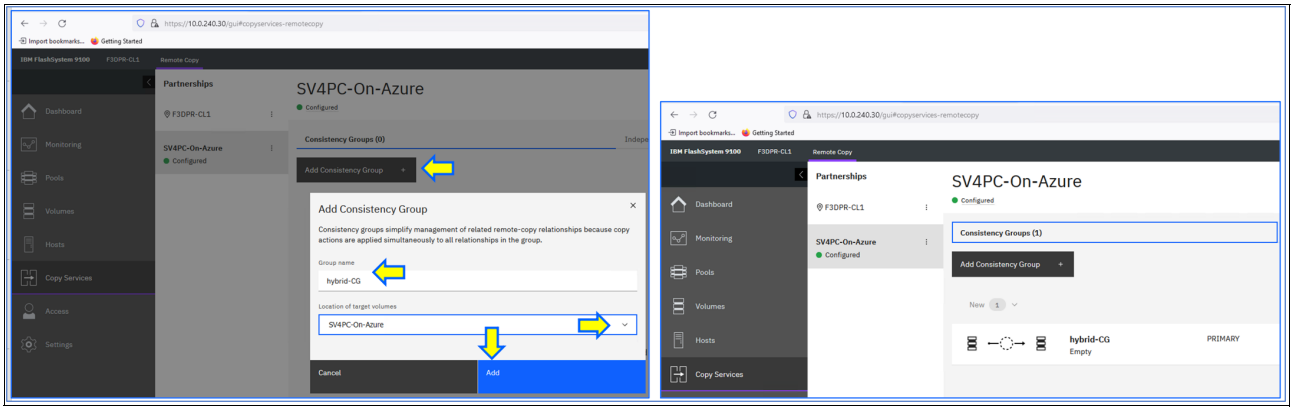


Figure 68 Adding consistency group: On-premises storage

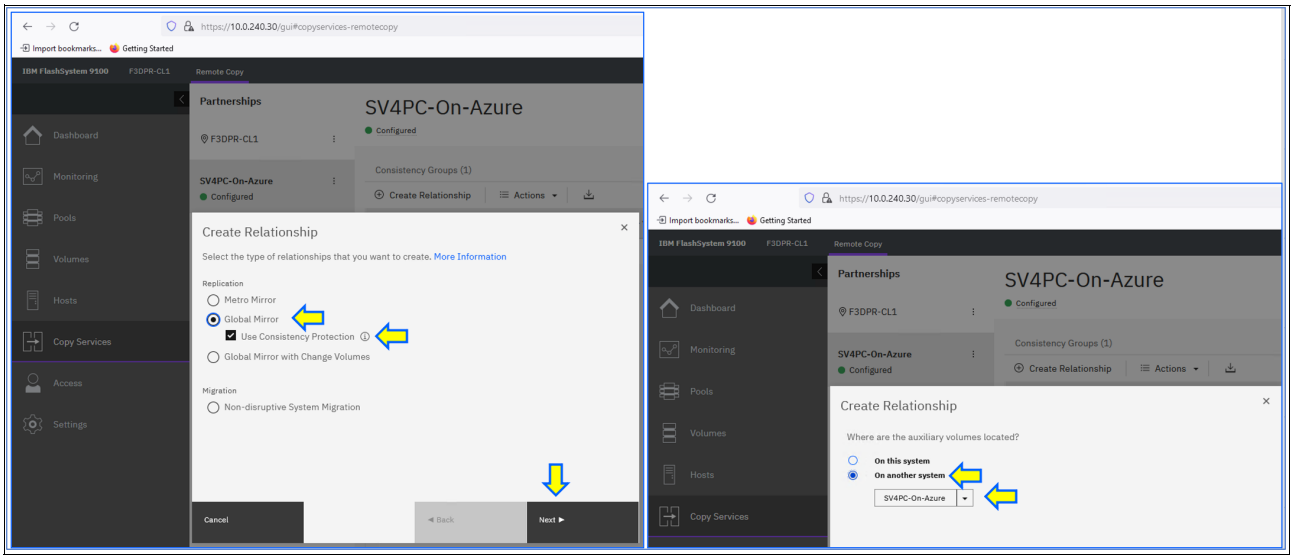


Figure 69 Creating relationship: On-premises storage Part 1

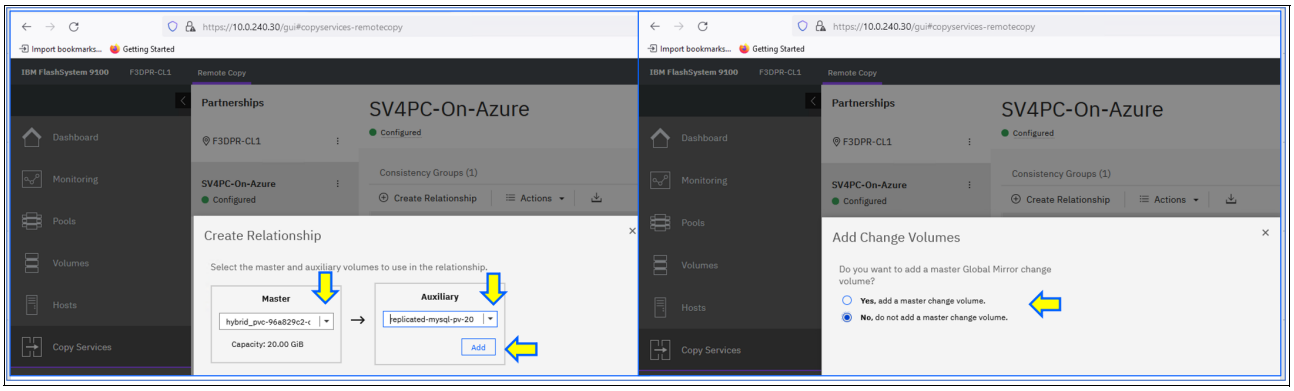


Figure 70 Creating relationship: On-premises storage Part 2

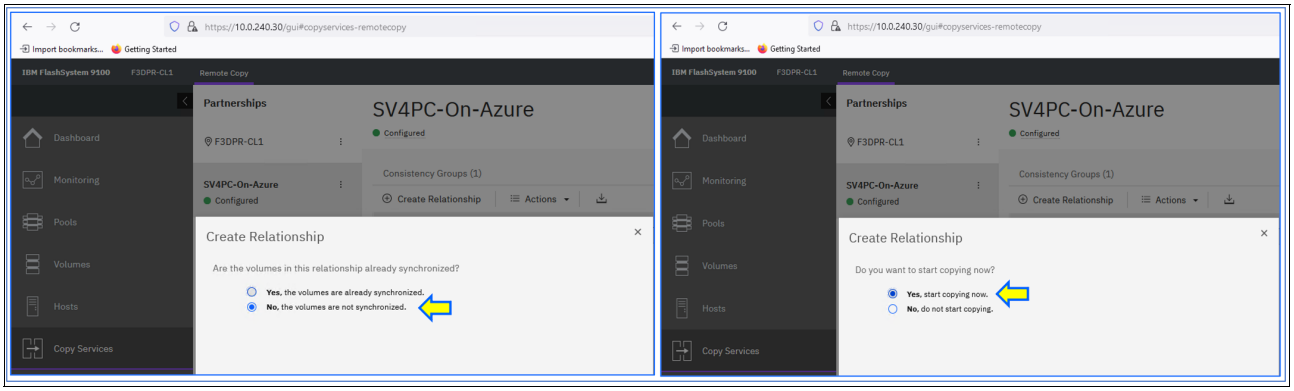


Figure 71 Creating relationship: On-premises storage Part 3

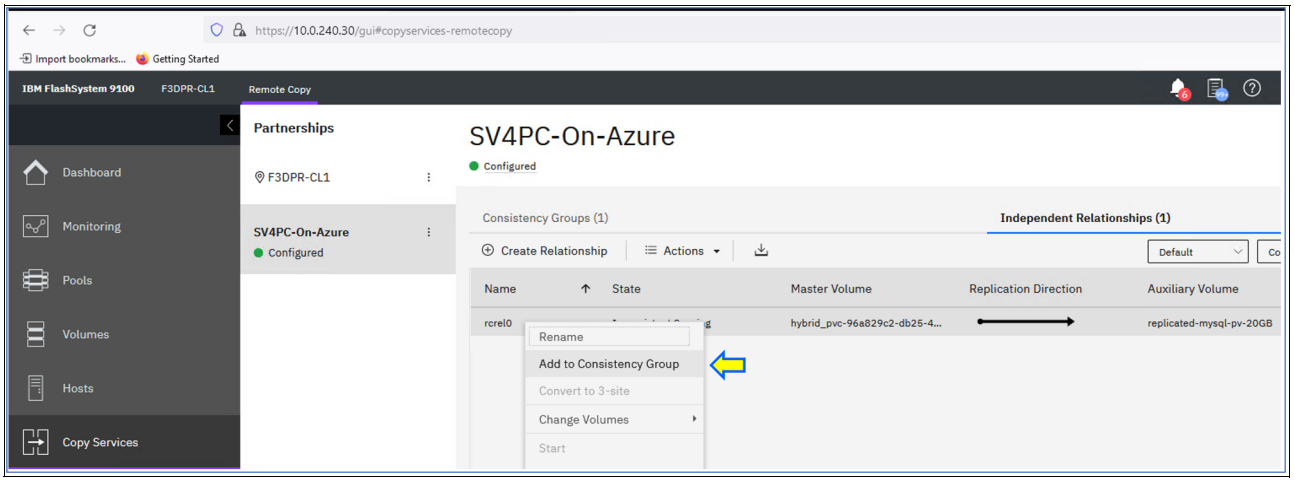


Figure 72 Adding consistency group: On-premises storage

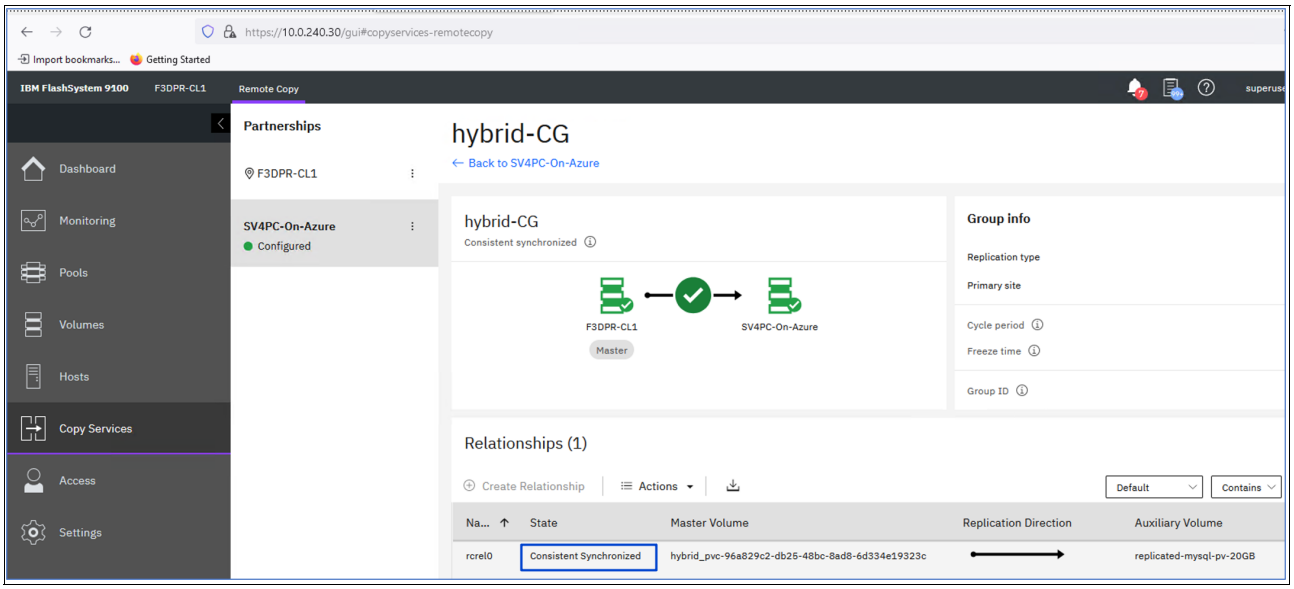


Figure 73 Checking status: Consistent synchronized

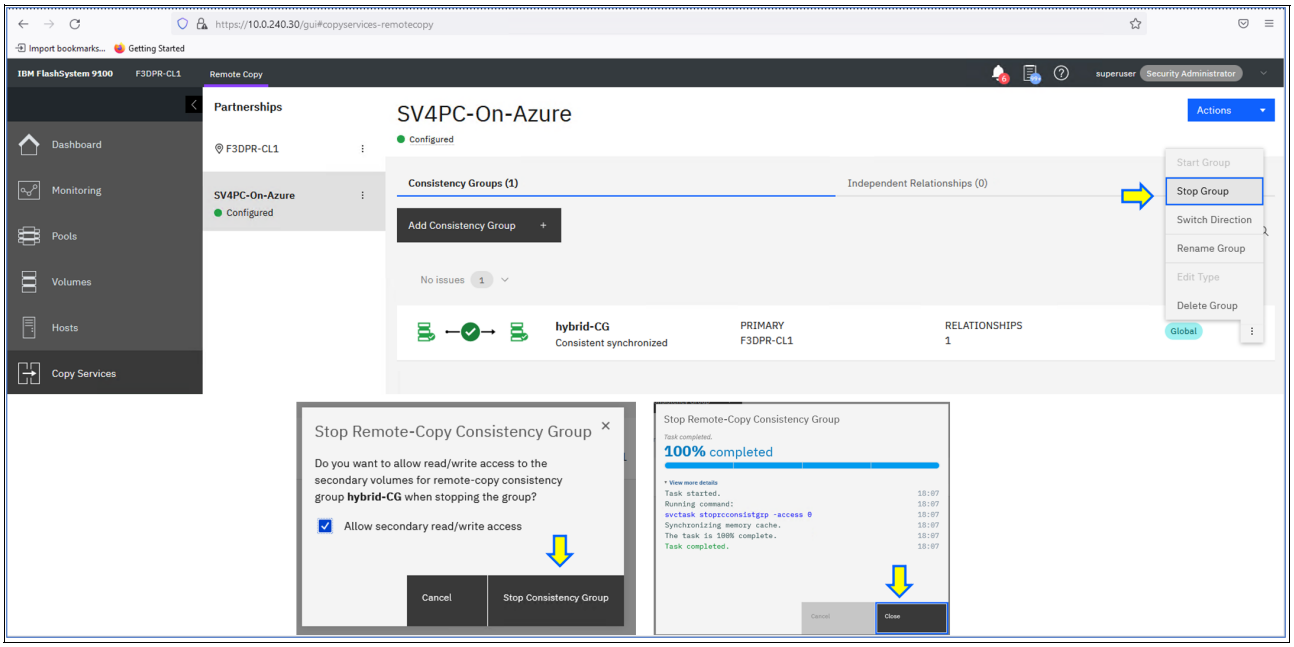


Figure 74 Stopping remote-copy consistency group

3. Log in to the Microsoft Azure portal at `https://portal.azure.com` and then, log in to the Linux VM by using `azureuser` and the SSH key that uses the Bastion service or by using SSH and creating the persistent volume claim (PVC) and PV by using the procedure that is described at this IBM Documentation web page (see Figure 75 on page 56 - Figure 82 on page 60).

```
root@hybrid-Cloud-Linux-bastion-vm:~/ocp4.8/yaml/MySQL
[root@hybrid-Cloud-Linux-bastion-vm MySQL]# oc project mysql-cloud
Already on project "mysql-cloud" on server "https://api.arhocluster1sv4pc.arhoclustersv4pc.net:6443".
[root@hybrid-Cloud-Linux-bastion-vm MySQL]#
[root@hybrid-Cloud-Linux-bastion-vm MySQL]# cat 01-replicated-existing-mysql-pv.yaml
apiVersion: v1
kind: PersistentVolume
metadata:
  annotations:
    pv.kubernetes.io/provisioned-by: block.csi.ibm.com
  finalizers:
  - kubernetes.io/pv-protection
  - external-attacher/block-csi-ibm-com
  name: replicated-mysql-pv-20gb
spec:
  accessModes:
  - ReadWriteOnce
  capacity:
    storage: 20Gi
  csi:
    controllerExpandSecretRef:
      name: ibm-sv4pc-storage-secret
      namespace: ibm-block-storage-ns
    controllerPublishSecretRef:
      name: ibm-sv4pc-storage-secret
      namespace: ibm-block-storage-ns
    driver: block.csi.ibm.com
    fsType: xfs
    nodePublishSecretRef:
      name: ibm-sv4pc-storage-secret
      namespace: ibm-block-storage-ns
    nodeStageSecretRef:
      name: ibm-sv4pc-storage-secret
      namespace: ibm-block-storage-ns
    volumeAttributes:
      array_address: 40.10.1.4
      pool_name: CloudPool0
      storage.kubernetes.io/csiProvisionerIdentity: 1644399157645-8081-block.csi.ibm.com
      storage_type: SVC
      volume_name: replicated-mysql-pv-20gb
    volumeHandle: SVC:4;6005076072AE279A3800000000000005
  persistentVolumeReclaimPolicy: Delete
  storageClassName: ibm-block-storage-class-sv4pc
  volumeMode: Filesystem
[root@hybrid-Cloud-Linux-bastion-vm MySQL]#
```

Figure 75 Creating a volume yaml file

```
[root@hybrid-Cloud-Linux-bastion-vm MySQL]# oc create -f 01-replicated-existing-mysql-pv.yaml
persistentvolume/replicated-mysql-pv-20gb created
[root@hybrid-Cloud-Linux-bastion-vm MySQL]#
[root@hybrid-Cloud-Linux-bastion-vm MySQL]# oc get pv,pvc
NAME                                                        CAPACITY   ACCESS MODES   RECLAIM
                    STORAGECLASS                    REASON   AGE
persistentvolume/pvc-016db124-d744-4e5c-a74e-4919ee05ff28   5Gi        RWO            Delete
test-claim-on-sv4pc   ibm-block-storage-class-sv4pc            3d5h
persistentvolume/replicated-mysql-pv-20gb                   20Gi       RWO            Delete
                    ibm-block-storage-class-sv4pc            5s
[root@hybrid-Cloud-Linux-bastion-vm MySQL]#
```

Figure 76 Checking the status of pv,pvc

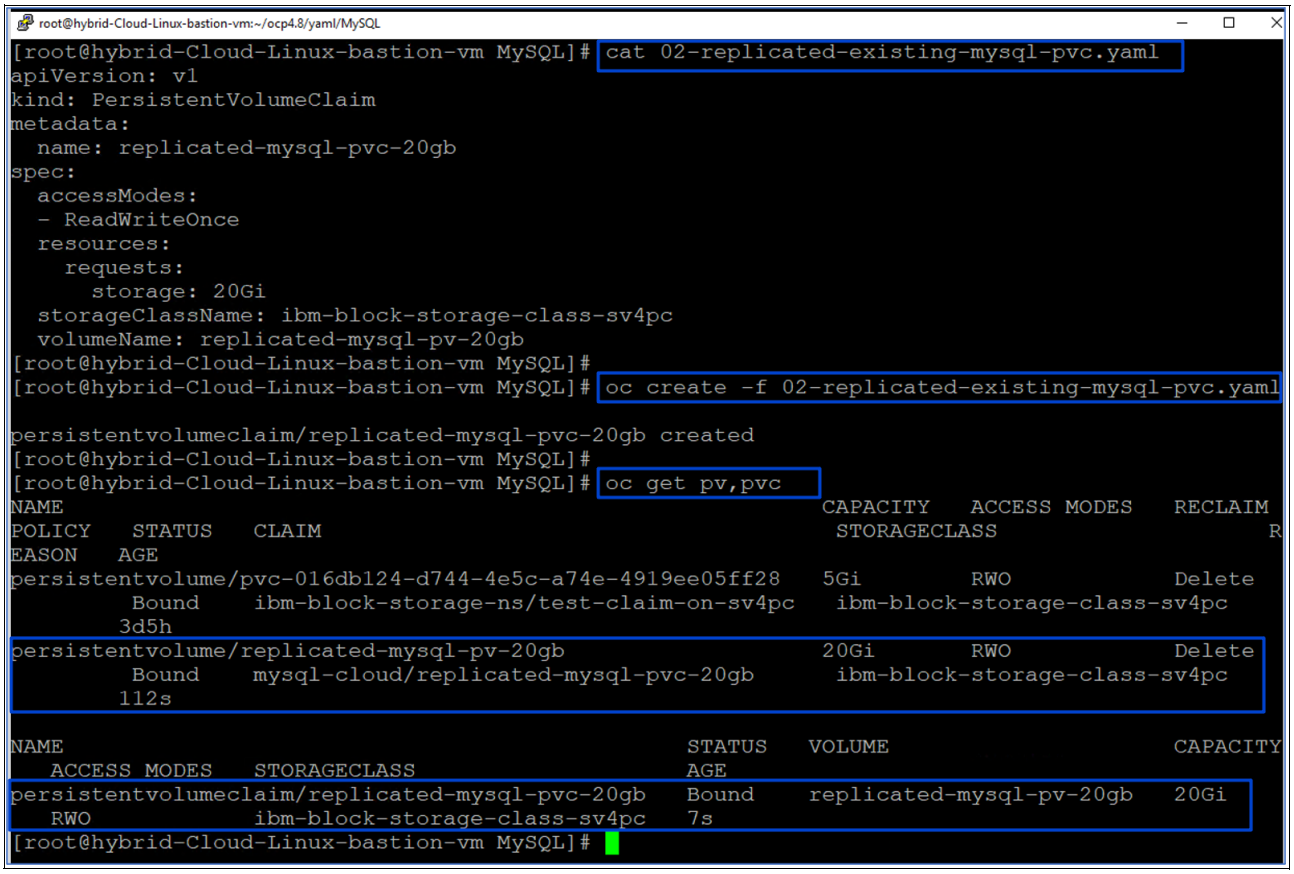


Figure 77 Creating mysql pvc

```
[root@hybrid-Cloud-Linux-bastion-vm MySQL]# cat 03-Cloud-mysql-deployment.yaml
---
apiVersion: v1
kind: Service
metadata:
  name: mysql
spec:
  ports:
  - port: 3306
  selector:
    app: mysql
  clusterIP: None
---
apiVersion: apps/v1 # for versions before 1.9.0 use apps/v1beta2
kind: Deployment
metadata:
  name: mysql
spec:
  selector:
    matchLabels:
      app: mysql
  strategy:
    type: Recreate
  template:
    metadata:
      labels:
        app: mysql
    spec:
      containers:
      - image: mysql:5.6
        name: mysql
        env:
          # Use secret in real usage
        - name: MYSQL_ROOT_PASSWORD
          value: password
        ports:
        - containerPort: 3306
          name: mysql
        volumeMounts:
        - name: mysql-persistent-storage
          mountPath: /var/lib/mysql
      volumes:
      - name: mysql-persistent-storage
        persistentVolumeClaim:
          claimName: replicated-mysql-pvc-20gb
```

Figure 78 Creating mysql yaml file

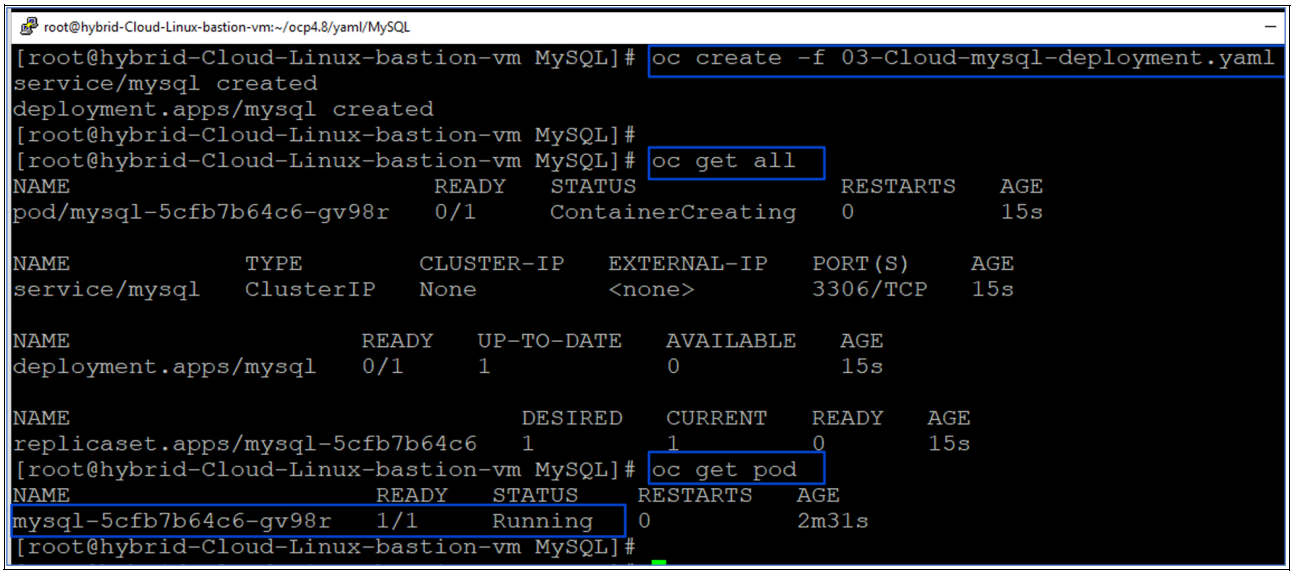


Figure 79 Deploying mysql

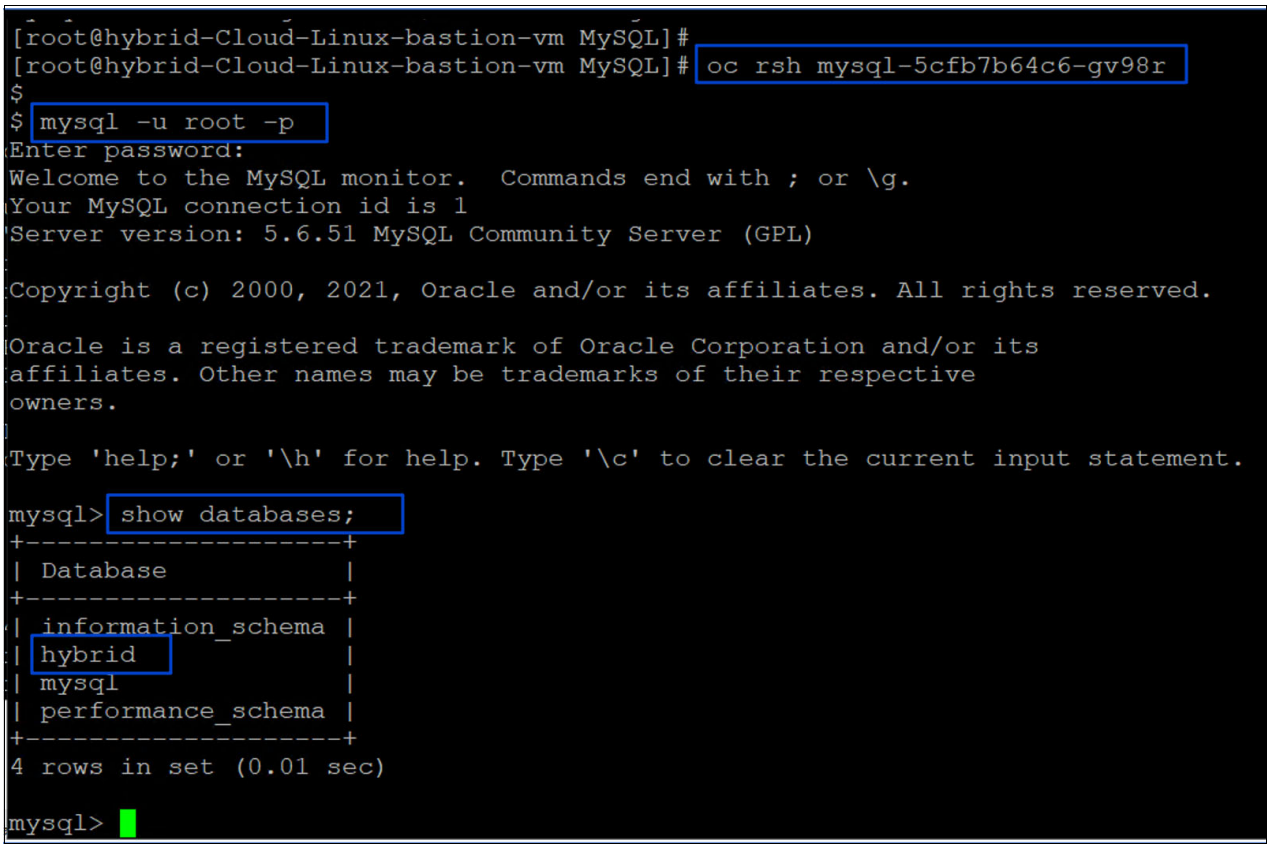


Figure 80 Logging in to mysql pod

```
mysql>
mysql> use hybrid;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql>
mysql> select * from hybrid_sv4pc_table;
+------+
| col1 |
+------+
|    1 |
|    2 |
|    3 |
+------+
3 rows in set (0.00 sec)

mysql>
```

Figure 81 Validating the replicated data

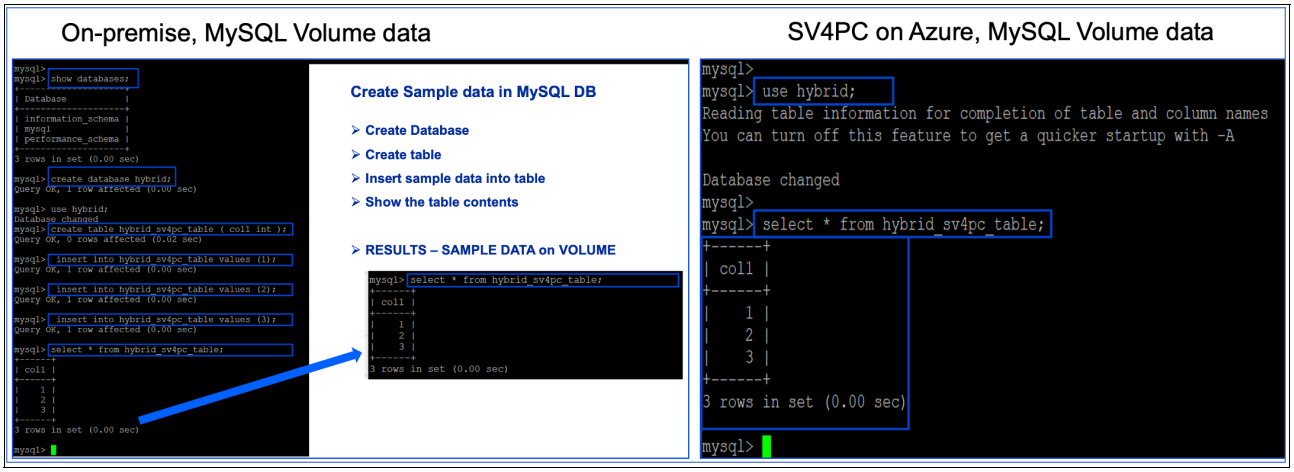


Figure 82 Validating replicated data

Now, the volume replication and business continuity use case is complete by using IBM Storage Global Mirror.

Replication by using IBM Block Storage CSI driver volume replication

Complete the following steps:

1. Log in to the on-premises RHOCP bastion hosts or the host from where RHOCP cluster can be accessed by using **`oc cli`** command tools and deploy MySQL, as shown in Figure 83 - Figure 87 on page 63.

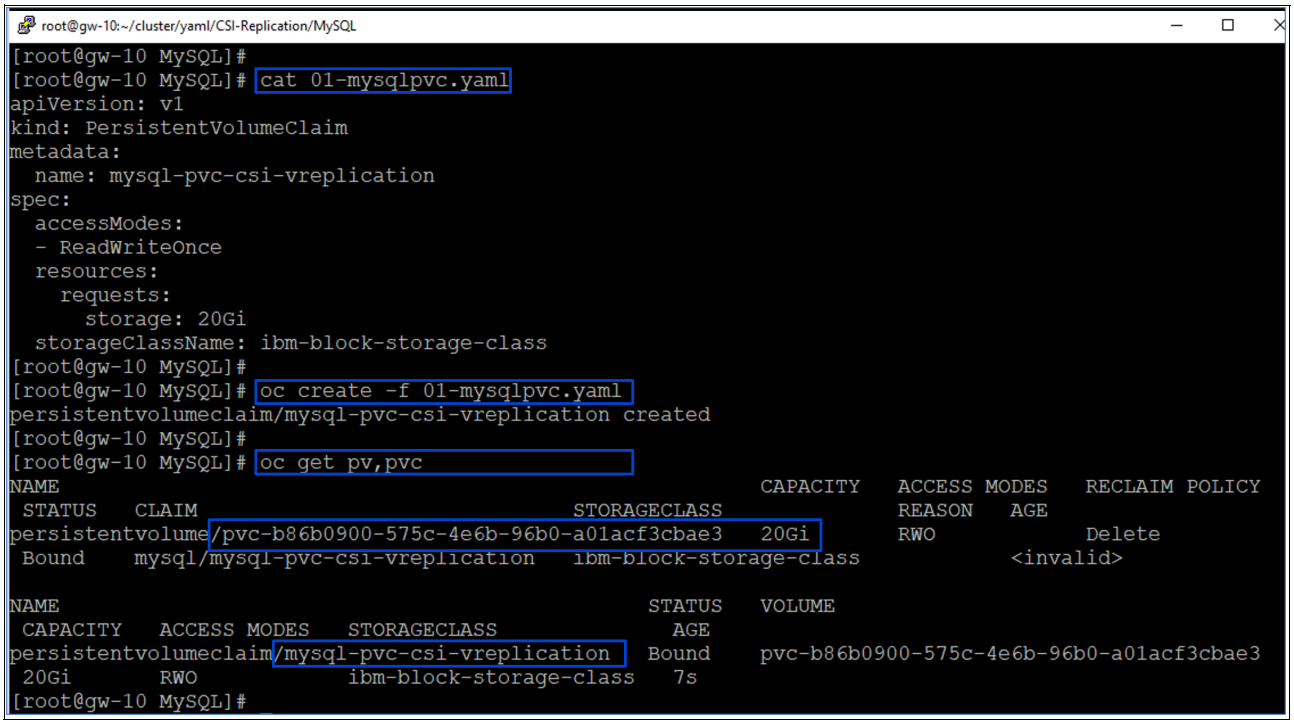


Figure 83 Creating mysql pvc yaml file

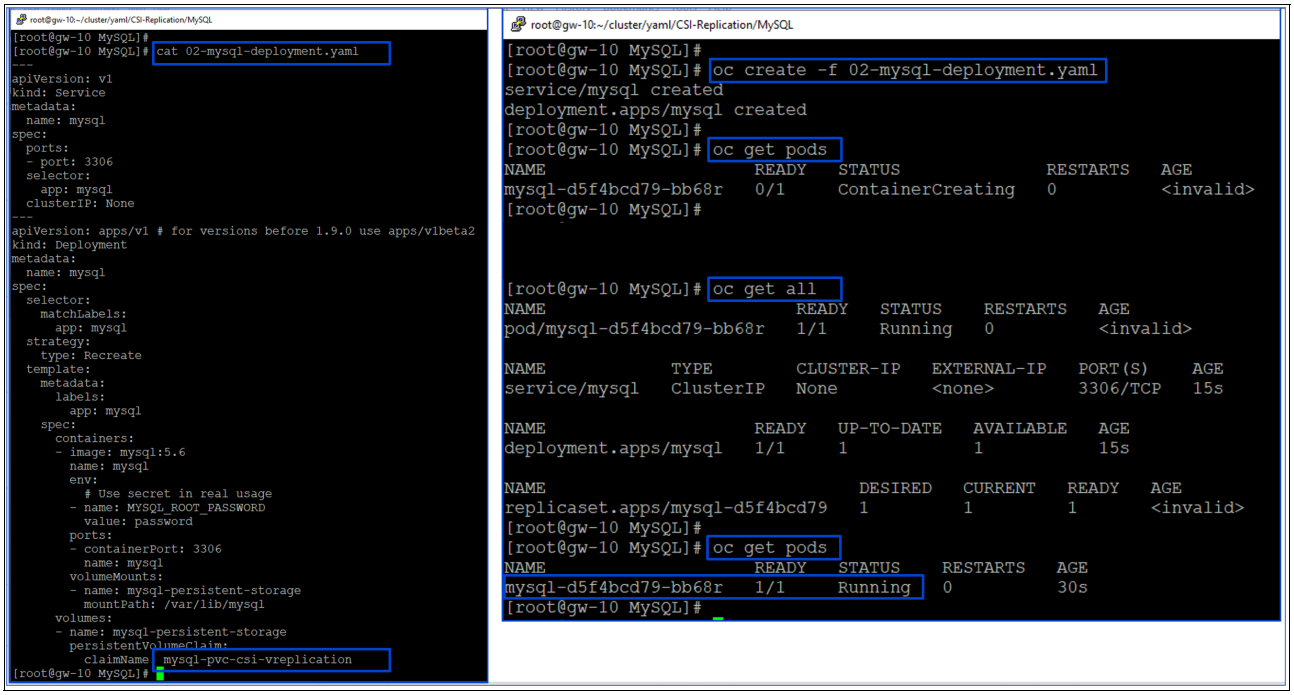


Figure 84 Deploying mysql

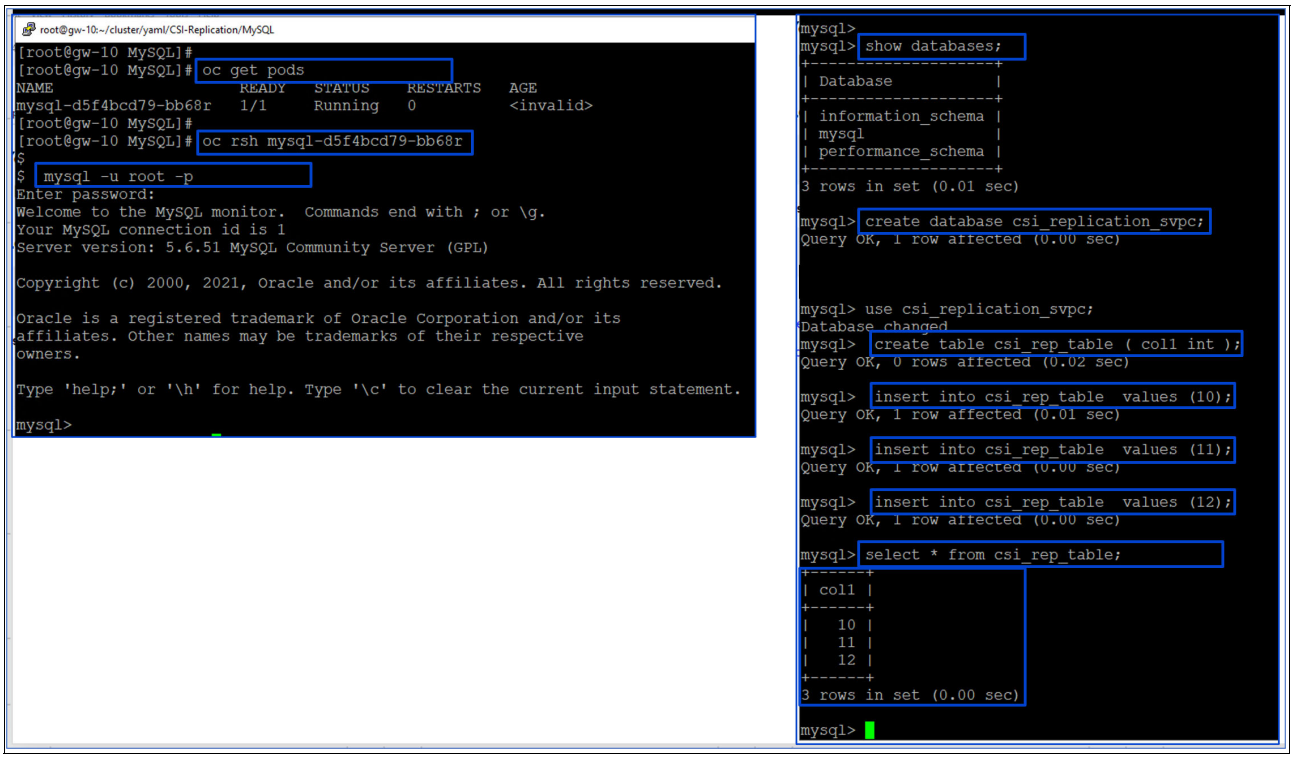


Figure 85 Logging in to the mysql pod and inserting sample data

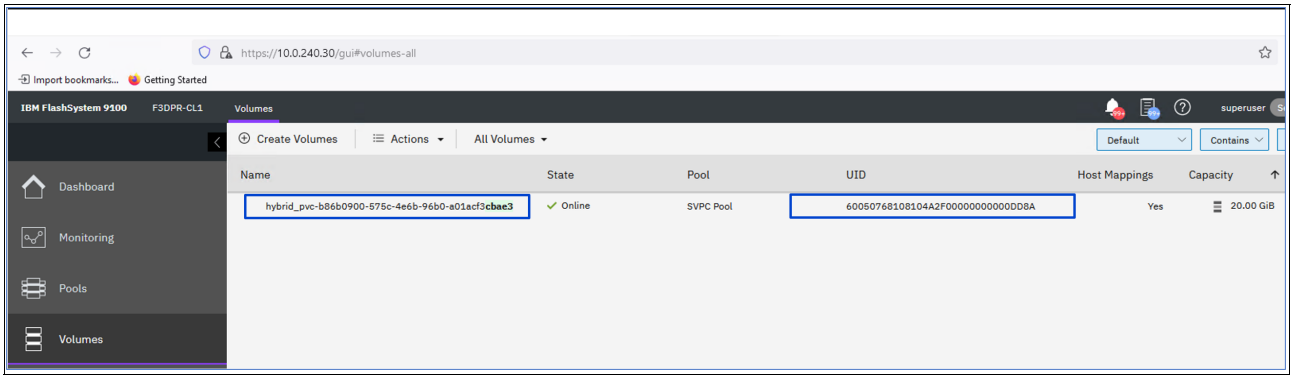


Figure 86 Checking that the volume is created in storage

2. Log in to the SV4PC on Azure and create equal-sized storage LUNs for CSI-based volume replication (see Figure 87).

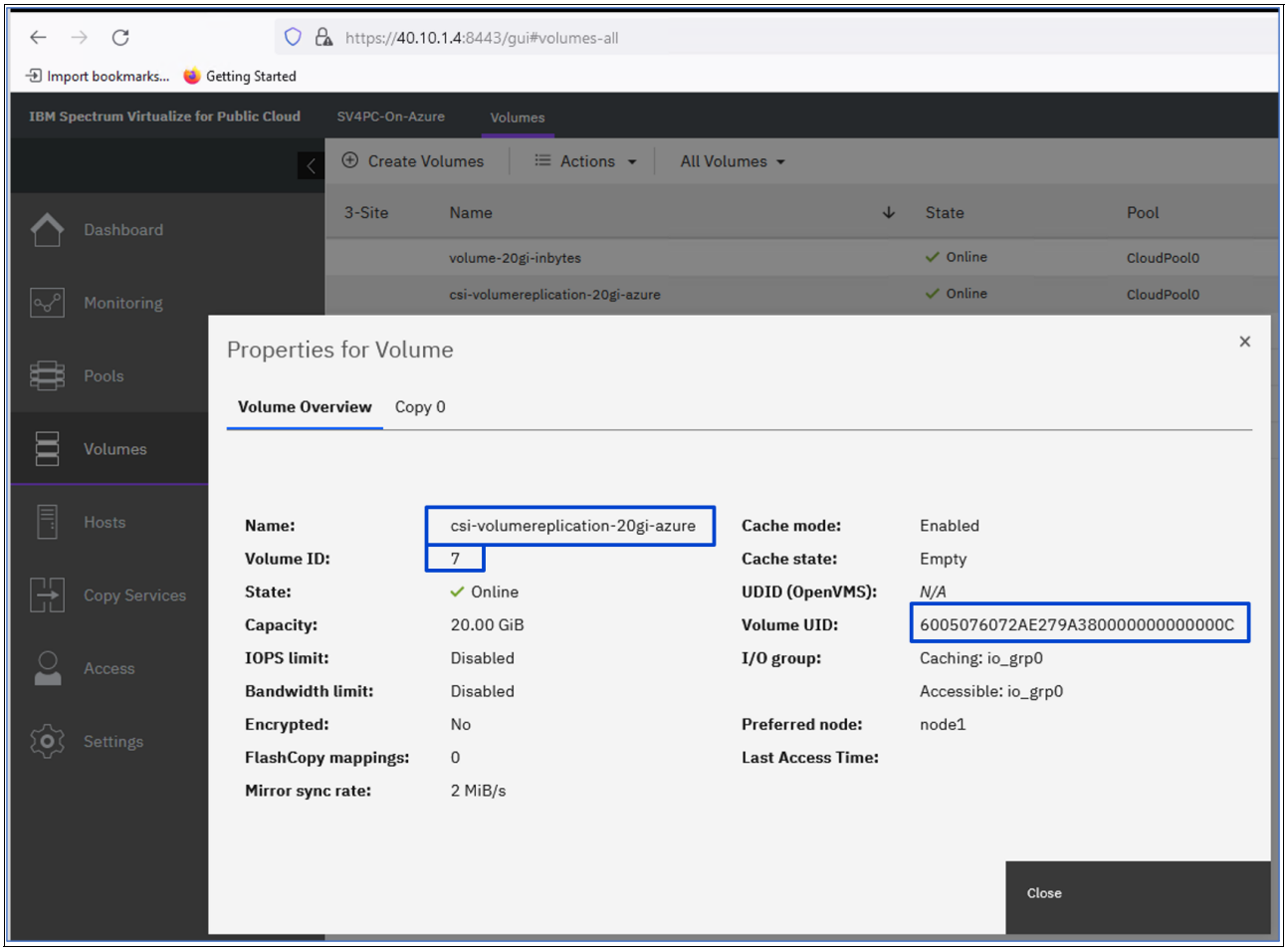


Figure 87 Creating a same size (20gi) volume on sv4pc storage

3. Using volume replication (remote copy function), enable support on your orchestration platform cluster and the storage system.

   To enable support on your Kubernetes or Red Hat OpenShift cluster, install the following replication CRDs once per cluster as shown in Figure 88 on page 64 and Figure 90 on page 65.

   Before the volume replication function is used, ensure that a partnership is created, and a consistency group is added to configure correctly.

```
[root@gw-10 CSI-Replication]#  curl -O https://raw.githubusercontent.com/csi-addons/volume-replication
-operator/v0.2.0/config/crd/bases/replication.storage.openshift.io_volumereplicationclasses.yaml
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  2747  100  2747    0     0   7027      0 --:--:-- --:--:-- --:--:--  7043
[root@gw-10 CSI-Replication]#
[root@gw-10 CSI-Replication]# oc apply -f ./replication.storage.openshift.io_volumereplicationclasses.
yaml
customresourcedefinition.apiextensions.k8s.io/volumereplicationclasses.replication.storage.openshift.i
o configured
[root@gw-10 CSI-Replication]#
[root@gw-10 CSI-Replication]#  curl -O https://raw.githubusercontent.com/csi-addons/volume-replication
-operator/v0.2.0/config/crd/bases/replication.storage.openshift.io_volumereplications.yaml
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  8935  100  8935    0     0  16291      0 --:--:-- --:--:-- --:--:-- 16275
[root@gw-10 CSI-Replication]#
[root@gw-10 CSI-Replication]# oc apply -f ./replication.storage.openshift.io_volumereplications.yaml
customresourcedefinition.apiextensions.k8s.io/volumereplications.replication.storage.openshift.io conf
igured
[root@gw-10 CSI-Replication]#
```

Figure 88 Enabling volume replication support (on-premises)

4. Log in to the on-premises RHOCP Bastion hosts or the host from where the RHOCP cluster can be accessed by using **`oc cli`** command tools and create the volume replication class (see Figure 89). Ensure to add the correct `system_id` in the yaml file (see Figure 89).

```
root@gw-10:~/cluster/yaml/CSI-Replication
[root@gw-10 CSI-Replication]# cat 01-create-volumereplicationclass
apiVersion: replication.storage.openshift.io/v1alpha1
kind: VolumeReplicationClass
metadata:
  name: csi-volumereplicationclass
spec:
  provisioner: block.csi.ibm.com
  parameters:
    system_id: 0000001CAB89E68E
    copy_type: async  # Optional. Values sync/async. The default is sync.

    replication.storage.openshift.io/replication-secret-name: ibm-block-storage-secret
    replication.storage.openshift.io/replication-secret-namespace: ibm-flashsystem-csi
[root@gw-10 CSI-Replication]#
[root@gw-10 CSI-Replication]# oc create -f 01-create-volumereplicationclass
volumereplicationclass.replication.storage.openshift.io/csi-volumereplicationclass created
[root@gw-10 CSI-Replication]#
[root@gw-10 CSI-Replication]# oc get volumereplicationclasses.replication.storage.openshift.io
NAME                          PROVISIONER
csi-volumereplicationclass    block.csi.ibm.com
[root@gw-10 CSI-Replication]#
[root@gw-10 CSI-Replication]#
```

Storage System ID
SV4PC on Azure

Figure 89 Creating volume replication class (on-premises)

```
[root@hybrid-Cloud-Linux-bastion-vm csi-replication]# curl -O https://raw.githubusercontent.com/
csi-addons/volume-replication-operator/v0.2.0/config/crd/bases/replication.storage.openshift.io_
volumereplicationclasses.yaml
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  2747  100  2747    0     0  17974      0 --:--:-- --:--:-- --:--:-- 17954
[root@hybrid-Cloud-Linux-bastion-vm csi-replication]#
[root@hybrid-Cloud-Linux-bastion-vm csi-replication]#  oc apply -f ./replication.storage.openshi
ft.io_volumereplicationclasses.yaml
customresourcedefinition.apiextensions.k8s.io/volumereplicationclasses.replication.storage.opens
hift.io configured
[root@hybrid-Cloud-Linux-bastion-vm csi-replication]#
[root@hybrid-Cloud-Linux-bastion-vm csi-replication]# curl -O https://raw.githubusercontent.com/
csi-addons/volume-replication-operator/v0.2.0/config/crd/bases/replication.storage.openshift.io_
volumereplications.yaml
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  8935  100  8935    0     0  61025      0 --:--:-- --:--:-- --:--:-- 61620
[root@hybrid-Cloud-Linux-bastion-vm csi-replication]#
[root@hybrid-Cloud-Linux-bastion-vm csi-replication]# oc apply -f ./replication.storage.openshif
t.io_volumereplications.yaml
customresourcedefinition.apiextensions.k8s.io/volumereplications.replication.storage.openshift.i
o configured
```

Figure 90 Enabling volume replication support (sv4pc on Azure)

5. Log in to the Microsoft Azure portal at https://portal.azure.com.
6. Log in to the Linux VM by using `azureuser` and the SSH key by using the Bastion service or use SSH and create the volume replication class (see Figure 91).

```
root@hybrid-Cloud-Linux-bastion-vm:~/ocp4.8/yaml/csi-replication
[root@hybrid-Cloud-Linux-bastion-vm csi-replication]# cat 04-create-volumereplicationclass
apiVersion: replication.storage.openshift.io/v1alpha1
kind: VolumeReplicationClass
metadata:
  name: csi-volumereplicationclass-sv4pc
spec:
  provisioner: block.csi.ibm.com
  parameters:
    system_id: 00000204204128BC
    copy_type: async  # Optional. Values sync/async. The default is sync.

    replication.storage.openshift.io/replication-secret-name: ibm-sv4pc-storage-secret
    replication.storage.openshift.io/replication-secret-namespace: ibm-blockstorage-ns

[root@hybrid-Cloud-Linux-bastion-vm csi-replication]#
[root@hybrid-Cloud-Linux-bastion-vm csi-replication]# oc create -f 04-create-volumereplicationcl
ass
volumereplicationclass.replication.storage.openshift.io/csi-volumereplicationclass-sv4pc created
[root@hybrid-Cloud-Linux-bastion-vm csi-replication]#
[root@hybrid-Cloud-Linux-bastion-vm csi-replication]# oc get volumereplicationclasses.replicatio
n.storage.openshift.io
NAME                              PROVISIONER
csi-volumereplicationclass-sv4pc   block.csi.ibm.com
[root@hybrid-Cloud-Linux-bastion-vm csi-replication]#
[root@hybrid-Cloud-Linux-bastion-vm csi-replication]#
```

Storage System ID - on-premise, IBM FS9100 storage

Figure 91 Creating volume replication class (sv4pc on Azure)

7. Create the volume replication yaml file as shown in Figure 92. Then, create volume replication and check the status of volume replication.

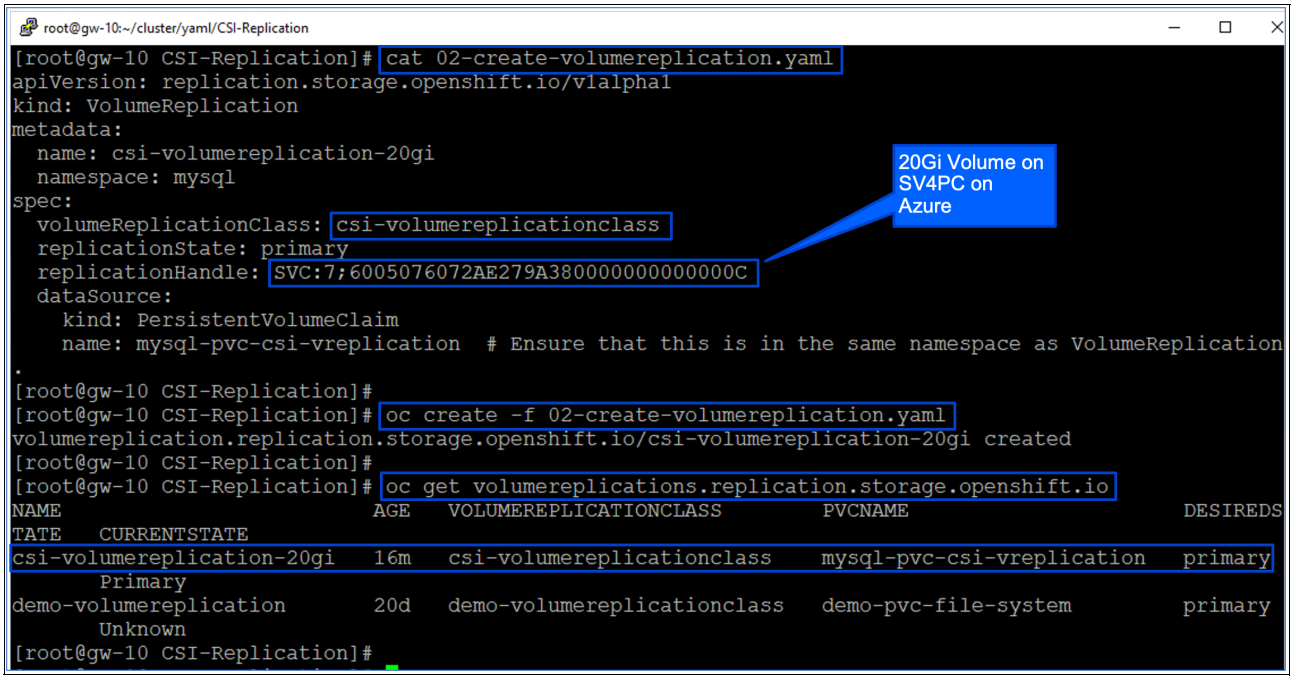


Figure 92 Creating volume replication (on-premises)

8. Log in to the on-premises storage and check the status of volume relationship (see Figure 93). The status should be `consistent synchronized`.

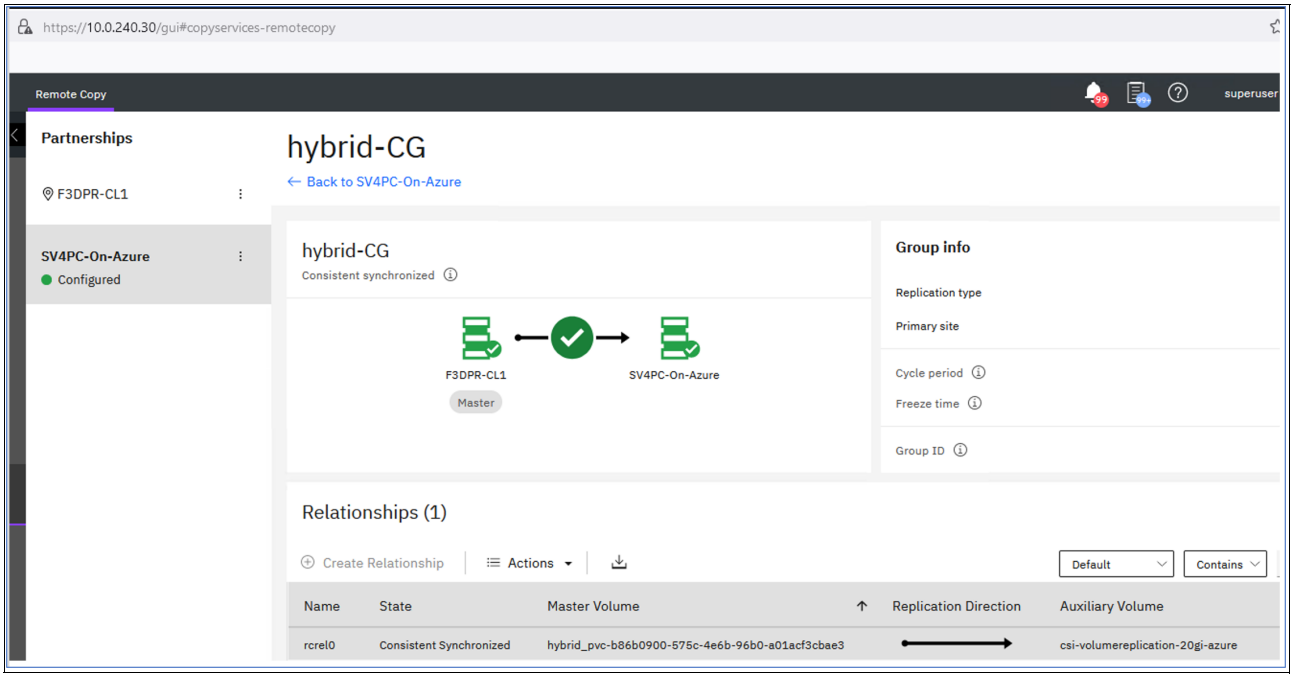


Figure 93 check status consistent synchronized

9. Stop the Remote-copy consistency group and allow secondary read/write access (see Figure 94).

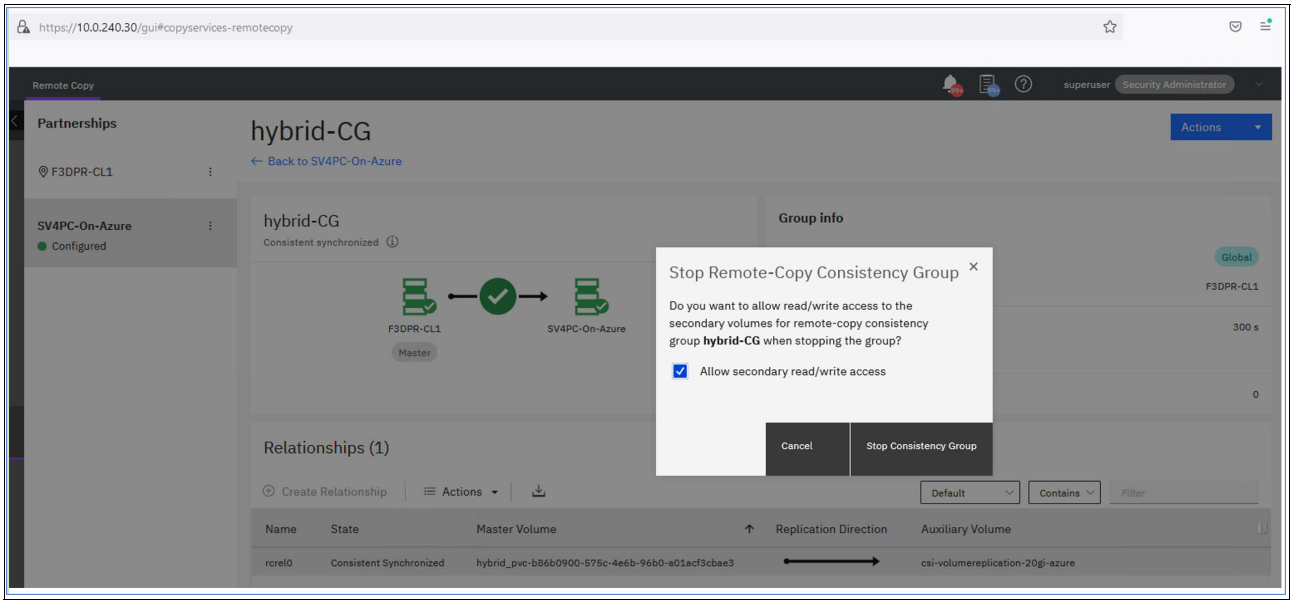


Figure 94 Stopping remote-copy consistency group

10. Log in to the Microsoft Azure portal at `https://portal.azure.com`.
11. Log in to the Linux VM by using `azureuser` and the SSH key that uses the Bastion service or by using SSH and deploying MySQL and validating the data (see Figure 95 - Figure 100 on page 71).

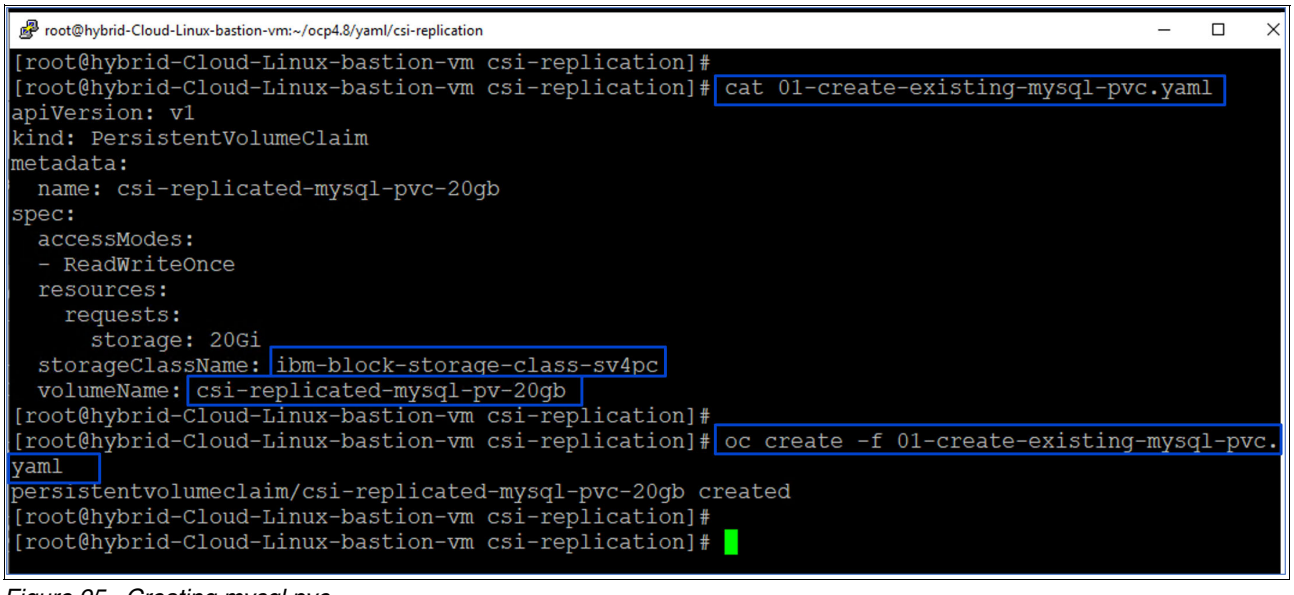


Figure 95 Creating mysql pvc

12. Create the PVC and PV by using the procedure that is described at this IBM Documentation web page (see Figure 96 and Figure 97).

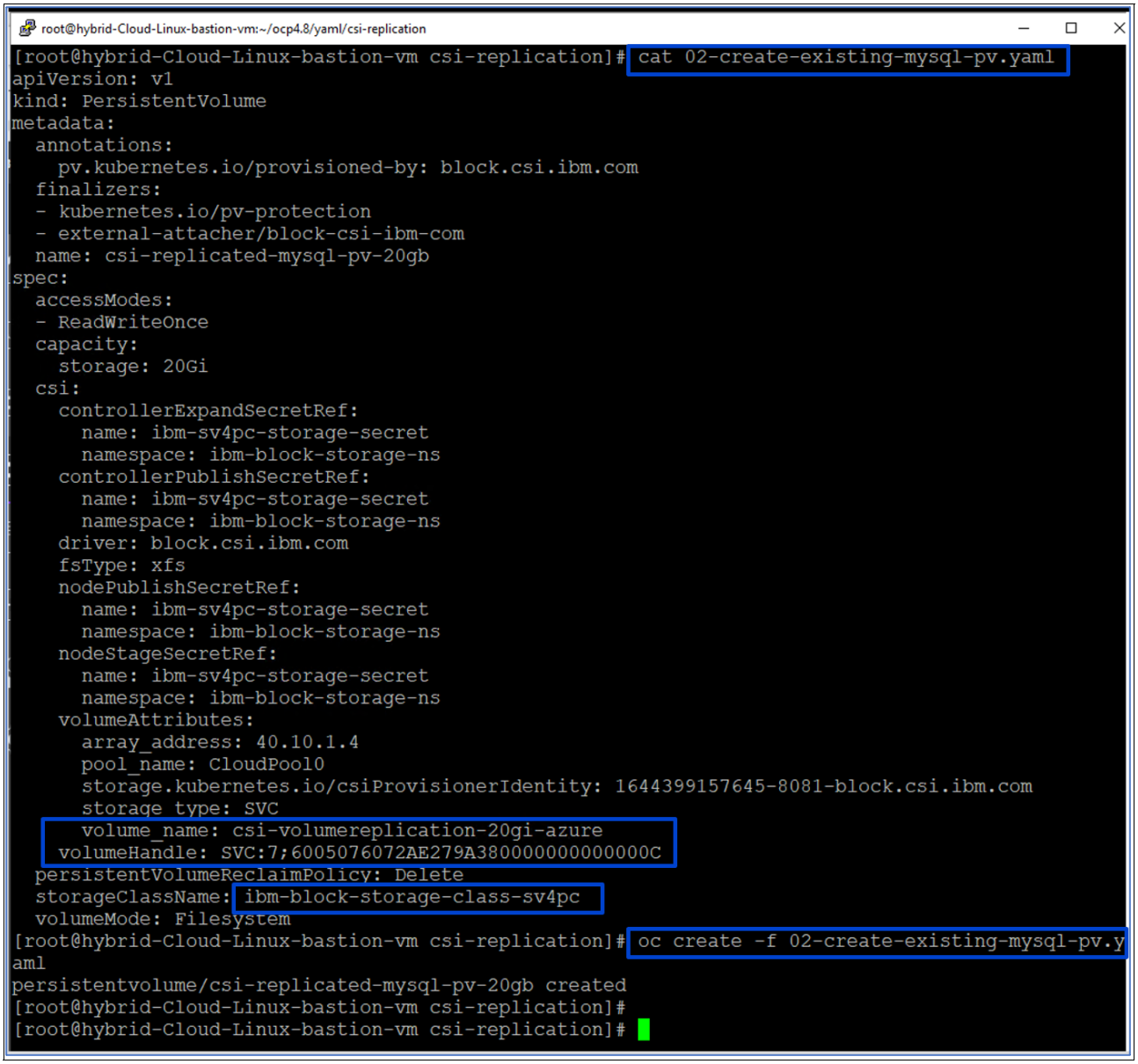


Figure 96 Importing a volume

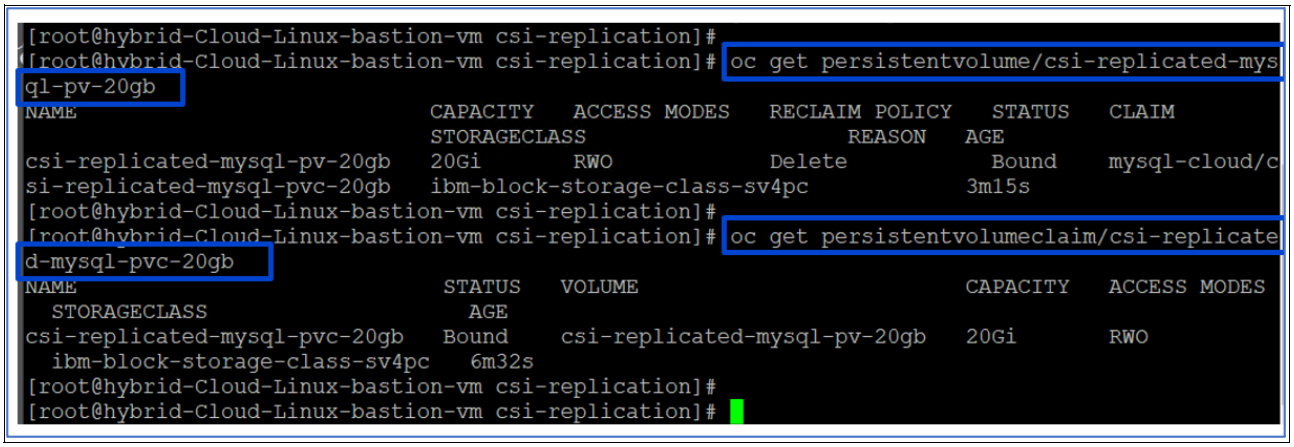


Figure 97 Checking the status of the volume

13. Create the MySQL deployment yaml file and the MySQL deployment (see Figure 98 on page 70 and Figure 99 on page 71).

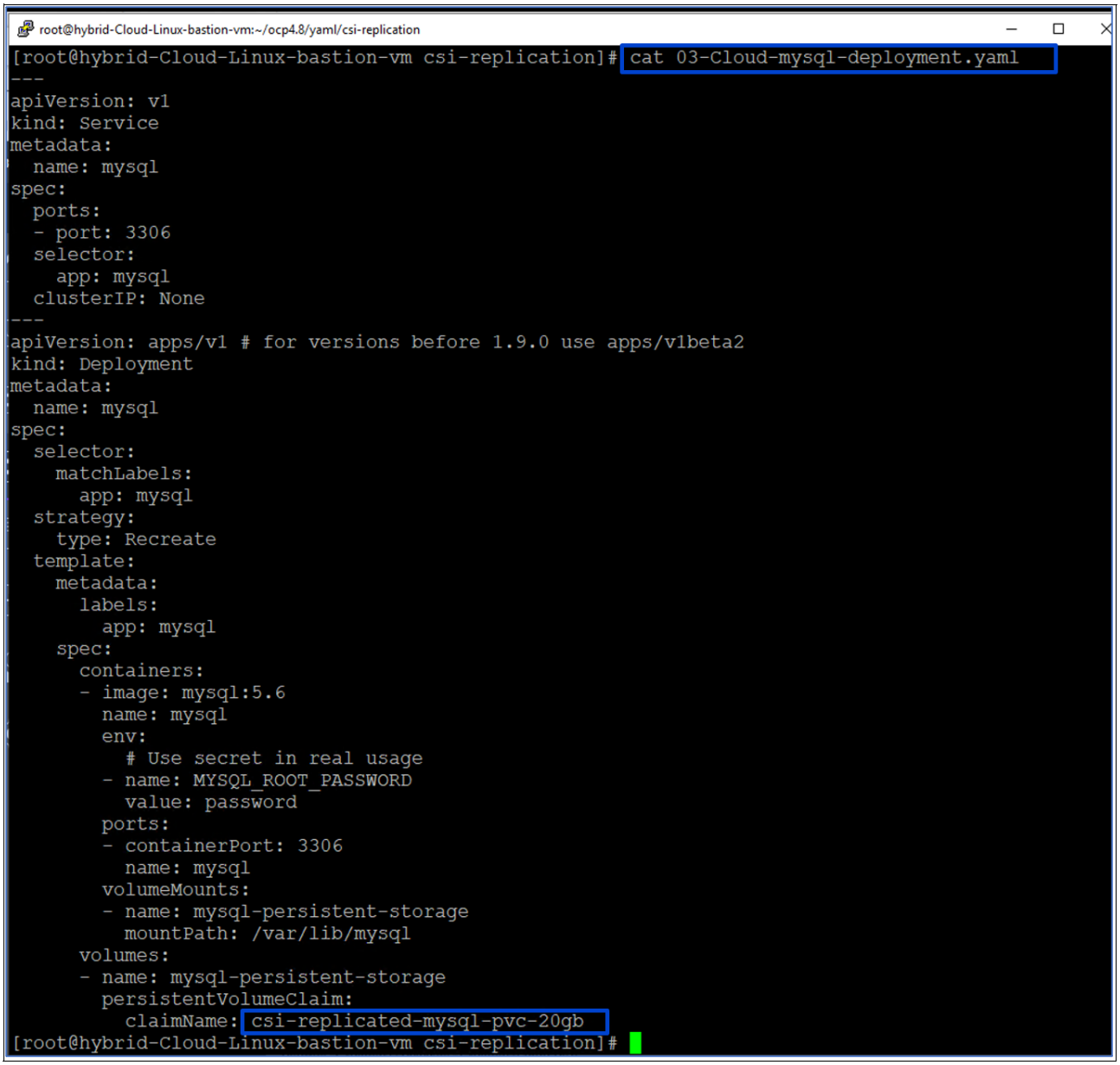


Figure 98 Deploying mysql

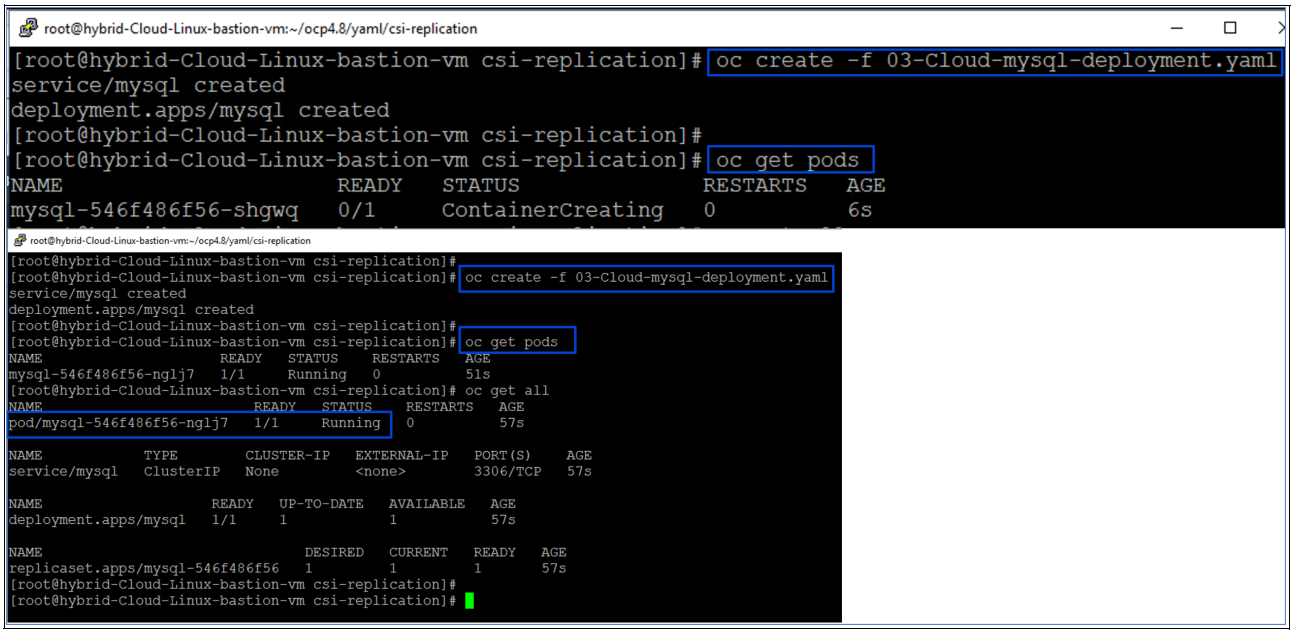


Figure 99 Creating mysql deployment

14. Log in to the MySQL pod and validate the data, as shown in Figure 100.

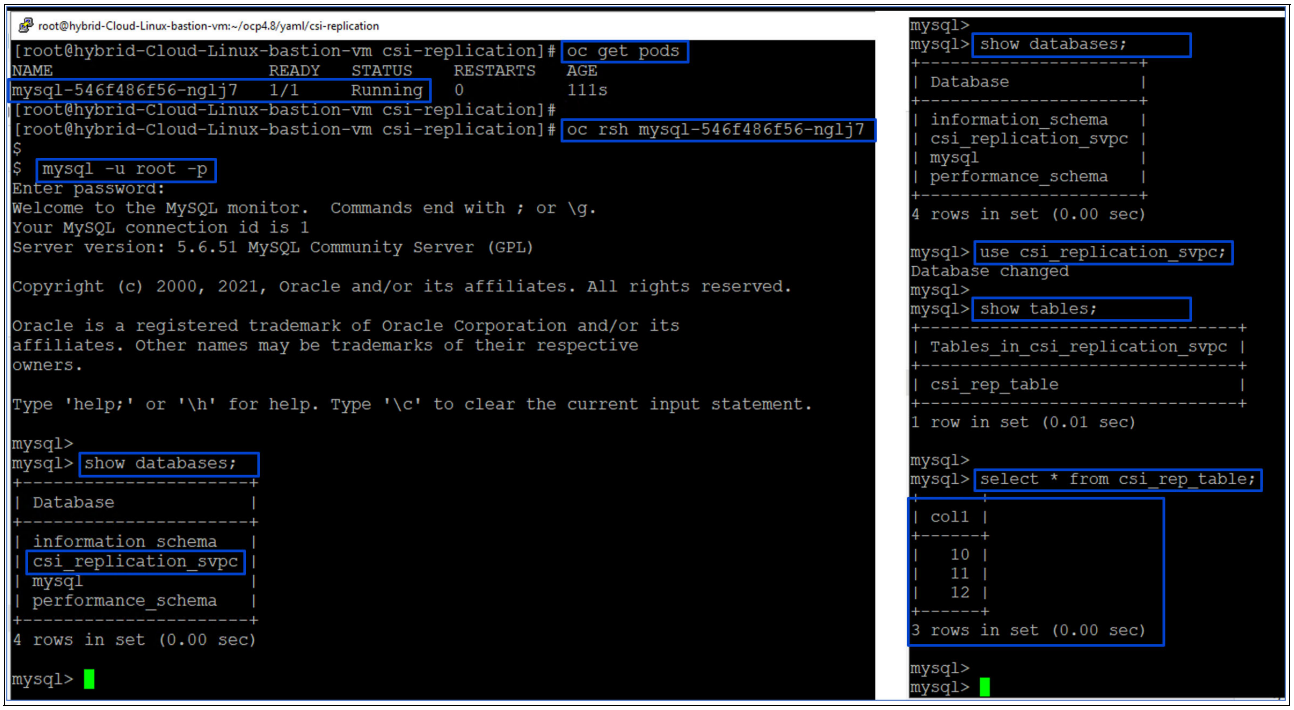


Figure 100 validate the data

Now, the volume replication and business continuity use case that uses the IBM block storage CSI volume replication feature is complete.

Summary

This solution is designed to protect the data by using IBM Storage-based Global Mirror Replication and the volume replication feature from IBM block storage CSI driver for IBM Storage.

The use case that is described in this document is designed for the business continuity solution for containerized workload for Red Hat OpenShift on Microsoft Azure with IBM Spectrum Virtualize for Public Cloud on Azure.

The steps in this demonstration show how the on-premises data can be made available to remote sites and public clouds by using the components that are described in this Blueprint.

For more information about steps that can be taken to ensure database data consistency, see the specific product documentation.

Author

This blueprint guide was produced by a team of specialists from around the world working at IBM Redbooks, Poughkeepsie Center.

Hemant Kantak is a Storage Solutions Architect with IBM® Systems, ISDL Lab Pune, India, for past 12 years in IBM. He designs and deploys storage and backup, virtualization, and Cloud technologies solutions across various platforms, including AWS, IBM Cloud®, and Microsoft Azure. He designs and deploys Hybrid Cloud Solutions with Red Hat OpenShift Container Platform, IBM Cloud Paks, and VMware Solutions/Tanzu. As an IBM Systems TechU speaker, he has demonstrated solutions to IBM customers and the IBM Sales team. He also is the author of several Blueprints and other IBM Redbooks® publications.

Thanks to Michelle Tidwell, IBM Storage, Program Director, IBM Spectrum Virtualize Hybrid Cloud Product Management, for her contributions to this project.

Resources

For more information, see the following resources:

- IBM block storage CSI driver 1.8.0:

  https://www.ibm.com/docs/en/stg-block-csi-driver/1.8.0

- Preparing to install on Azure:

  https://docs.openshift.com/container-platform/4.8/installing/installing_azure/preparing-to-install-on-azure.html

- Microsoft tutorial: Create a site-to-site VPN connection in the Azure portal:

  https://docs.microsoft.com/en-us/azure/vpn-gateway/tutorial-site-to-site-portal

- Route-Based Site-to-Site VPN to Azure (BGP over IKEv2/IPsec):

  https://docs.vyos.io/en/latest/configexamples/azure-vpn-bgp.html

- *Implementation Guide for IBM Spectrum Virtualize for Public Cloud on Microsoft Azure Version 8.4.3*, SG24-8510:

  https://www.redbooks.ibm.com/Redbooks.nsf/RedpieceAbstracts/sg248510.html?Open

Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive, MD-NC119, Armonk, NY 10504-1785, US

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at http://www.ibm.com/legal/copytrade.shtml

The following terms are trademarks or registered trademarks of International Business Machines Corporation, and might also be trademarks or registered trademarks in other countries.

Redbooks (logo)  ®	IBM Cloud®	Insight®
Db2®	IBM FlashSystem®	Redbooks®
IBM®	IBM Spectrum®	

The following terms are trademarks of other companies:

The registered trademark Linux® is used pursuant to a sublicense from the Linux Foundation, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis.

Microsoft, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

OpenShift, Red Hat, are trademarks or registered trademarks of Red Hat, Inc. or its subsidiaries in the United States and other countries.

VMware, and the VMware logo are registered trademarks or trademarks of VMware, Inc. or its subsidiaries in the United States and/or other jurisdictions.

Other company, product, or service names may be trademarks or service marks of others.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Privacy policy considerations

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user, or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM's Privacy Policy at http://www.ibm.com/privacy and IBM's Online Privacy Statement at http://www.ibm.com/privacy/details in the section entitled "Cookies, Web Beacons and Other Technologies," and the "IBM Software Products and Software-as-a-Service Privacy Statement" at http://www.ibm.com/software/info/product-privacy.

May 2022

Please recycle

ISBN 0738460559

REDP-5682-00