FALCONSTOR

FALCONSTOR® STORSAFE®

for IBM Power

Deployment Guide

FalconStor® StorSafe® for IBM Power Deployment Guide

FalconStor Software, Inc.
111 Congress Ave, Suite 500
Austin, TX 78701 USA
Phone: 631-777-5188
Website: www.falconstor.com

22224

Contents

Introduction

FalconStor StorSafe is an optimized backup and deduplication solution that provides Virtual Tape Library (VTL) emulation, high-speed backup/restore, data archival to supported S3 clouds for long-term storage, global data deduplication, and enterprise-wide replication, without requiring changes to the existing environment.

FalconStor StorSight is a single integrated platform that simplifies the management of data across legacy, modern, and virtual storage environments. StorSight gathers and consolidates information coming from different StorSafe servers into a scalable repository of services, tenants, users, predictive analytics, alert rules, reporting, and historical data. StorSight provides a web-based portal for centralized management and monitoring of multiple backup and deduplication servers.

This guide describes how to create and configure an IBM Power System Virtual Server running FalconStor StorSafe and StorSight software in IBM Cloud.

Intended audience

This guide is intended for the following individuals deploying the FalconStor StorSafe solution:

- Storage architects
- Consultants
- System Administrators

Individuals performing the deployment should have strong experience with the following products and technologies:

- IBM Cloud
- FalconStor StorSafe and StorSight solution
- Network design, configuration, and security
- Ethernet topologies, network routers, VPN, VLAN
- iSCSI technologies
- Fibre Channel SAN technologies (only if FC is used on-premises)

Resources and helpful links

Resource	Link
FalconStor Technical Support	https://www.falconstor.com/support/technical-support
FalconStor Sizing Calculator	http://ibmsizing.falconstor.com
FalconStor Certification Matrix	https://www.falconstor.com/support/certification-matrix
FalconStor license registration email	activate.keycode@falconstor.com
FalconStor StorSight SAK image for x-86 servers on-premises or on virtual servers for VPC	https://falconstor-download.s3.us-east.cloud-object-storage.appdomain.cloud/SAK-Install-8.8.32a-StorSight-10.16-4001-Linux8.iso
FalconStor StorSafe SAK image for on-premises Power servers	https://falconstor-download.s3.us-east.cloud-object-storage.appdomain.cloud/SAK-Install-8.8.22-StorSafe-11.13-12328-ppc64le-Linux8.iso
FalconStor SAK Image Installation Guide	https://falconstor-download.s3.us-east.cloud-object-storage.appdomain.cloud/FalconStor%20Server%20SAK%20ISO%20Image%20Installation%20Guide.pdf
FalconStor Server Virtual Appliance Installation Guide	https://falconstor-download.s3.us-east.cloud-object-storage.appdomain.cloud/FalconStor%20Server%20Virtual%20Appliance%20Installation%20Guide.pdf
FalconStor StorSafe with StorSight Release Notes	https://falconstor-download.s3.us-east.cloud-object-storage.appdomain.cloud/FalconStor%20StorSafe%20with%20StorSight%20Release%20Notes.pdf
FalconStor StorSafe with StorSight User Guide	https://falconstor-download.s3.us-east.cloud-object-storage.appdomain.cloud/FalconStor%20StorSafe%20with%20StorSight%20User%20Guide.pdf
FalconStor VTL 10.03 to StorSafe 11.13 Upgrade Patch	https://falconstor-download.s3.us-east.cloud-object-storage.appdomain.cloud/UpgradeVTL10.03ppc64letoStorSafe11.13Tile
FalconStor VTL 10.03 to StorSafe 11.13 Upgrade Guide	https://falconstor-download.s3.us-east.cloud-object-storage.appdomain.cloud/FalconStor%20VTL%2010.03%20to%20StorSafe%2011.13%20Upgrade%20Guide.pdf
IBM documentation for installation, configuration, and cloud connectivity	IBM Power Systems Virtual Server Guide for IBM https://www.redbooks.ibm.com/Redbooks.nsf/RedpieceAbstracts/sg248513.html?Open IBM Power Virtual Server Virtual Private Network Connectivity https://cloud.ibm.com/media/docs/downloads/power-iaas-tutorials/PowerVS_VPN_Tutorial_v1.pdf Modifying a Power Systems Virtual Server instance https://cloud.ibm.com/docs/power-iaas?topic=power-iaas-modifying-server

IBM documentation for IBM i Backups with IBM Power Virtual Server	IBM i Backups with IBM Power Virtual Server Tutorial https://cloud.ibm.com/media/docs/downloads/power-iaas-tutorials/PowerVS_IBMi_Backups_Tutorial_v1.pdf
IBM documentation for iSCSI clients	IBM i Support for Attaching an iSCSI VTL https://www.ibm.com/support/pages/system/files/inline-files/IBM%20i%20Support%20for%20iSCSI%20VTL%201.4.pdf IBM i 7.5 iSCSI Boot https://download4.boulder.ibm.com/sar/CMA/HMA/0b1ly/3/MF70433.readme.html?_gl=1*m2rnt0*_ga*MjExODMzNzI4NC4xNTc0NjQwNjE5*_ga_FYECCCS21D*MTY5NjI0OTMxNC40MTcuMS4xNjk2MjUxOTUzLjAuMC4w https://www.ibm.com/docs/en/linux-on-z?topic=server-boot-process
IBM documentation for Cloud Connections, Direct Link, and Proxy Server	Managing IBM Cloud connections https://cloud.ibm.com/docs/power-iaas?topic=power-iaas-cloud-connections Using IBM Cloud Direct Link to connect to IBM Cloud Object Storage https://cloud.ibm.com/docs/direct-link?topic=direct-link-using-ibm-cloud-direct-link-to-connect-to-ibm-cloud-object-storage Ordering Direct Link Connect for Power Systems Virtual Servers https://cloud.ibm.com/docs/power-iaas?topic=power-iaas-ordering-direct-link-connect

Deployment Scenarios

The following scenarios are examples of different deployment cases for StorSafe with IBM Cloud:

- Native backup in the cloud: StorSafe in IBM Cloud serves different IBM i host clients for backup.
- IBM cloud-to-cloud replication: StorSafe in IBM Cloud replicates data to another StorSafe.
- Hybrid Cloud: On-premises StorSafe replicates data to a StorSafe in IBM Cloud.
- Workload migration: On-premises StorSafe replicates data to a StorSafe in IBM Cloud, migrates backup client workload, and then removes the on-premises StorSafe.

Connectivity options

The network infrastructure can be very different for each customer, depending on their security, performance, and reliability requirements. Consult IBM networking references as additional connection options may become available for IBM Power Systems Virtual Servers (PowerVS). This section is meant for general considerations. In this document, some information and screenshot samples are provided as guidelines.

To configure connectivity between the components, you can use public IP addresses for cloud server access, but for higher security, it is better to use private IP addresses and Virtual Private Networks (VPNs) for a secure connection between machines in the primary site and machines in IBM Cloud.

You can order Direct Link (DL) Connect on Classic to allow your PowerVS to communicate with Linux/Window virtual servers in IBM Cloud and also with all other IBM Cloud services, such as Cloud Object Storage (COS) and VMware services.

For servers at on-premises sites, you need a physical router; for servers in the cloud, you need a Virtual Router Appliance (VRA), such as Vyatta or Juniper, that allows IBM Cloud users to selectively route private network traffic through firewall and VPN features. Optionally, you can use a transit gateway router and IBM Virtual Private Clouds (VPC). You can use IBM Deployable Architecture from the catalog to build a Power Systems Virtual Server workspace with VPC landing zone. Refer to the appendix in this guide for details.

If you make remote connections to IBM COS *Private* endpoints, you also need a reverse proxy server unless you use a VPC. A virtual router appliance can act as a proxy server. *Public* endpoints can accept requests from anywhere; in this case, you will also need to have a public IP for your server. There are also *Direct* endpoints, which accept requests coming within the virtual private cloud. With a proxy server, your StorSafe PowerVS will submit COS requests to the IP or URL of the proxy. Make sure the DNS settings are correct in `/etc/resolv.conf` of the StorSafe server to resolve the endpoint name. Use the system command `ping` to confirm connectivity with the endpoint.

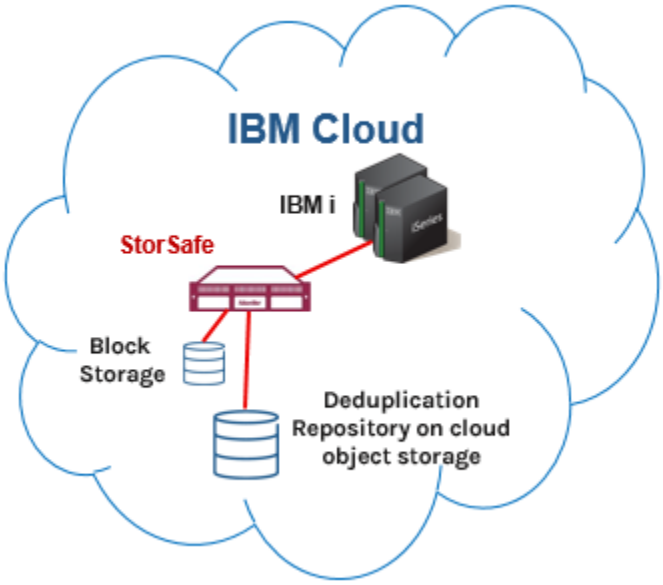
Optionally, you can use *Megaport*, which enables direct and dedicated connectivity between the primary site and IBM Cloud, to overcome the use of the public internet. Megaport is a software layer to manage network connections, allowing private point-to-point connectivity between any of the locations on the Megaport global network infrastructure. You can use a service key in your Megaport account to create a Virtual Cross Connect (VXC) from a port on a Megaport Cloud Router (MCR) to a port on the primary site. The key creator has control over limiting the bandwidth of the connection and can also specify the VLAN ID for a single-use key.

You can isolate the network traffic via different Virtual Local Area Networks (VLANs). For example, you may want to prevent access from the VLAN that gets bridged to Classic for COS from the VLAN for IBM i host clients. For better performance, you may want a different adapter for replication. You can set up VLANs to isolate the network traffic between:

- IBM i host clients and StorSafe for ingest data
- StorSafe and StorSight for management
- StorSafe and IBM COS for deduplicated data
- StorSafe source and replica servers for data replication

Native Backup Deployment

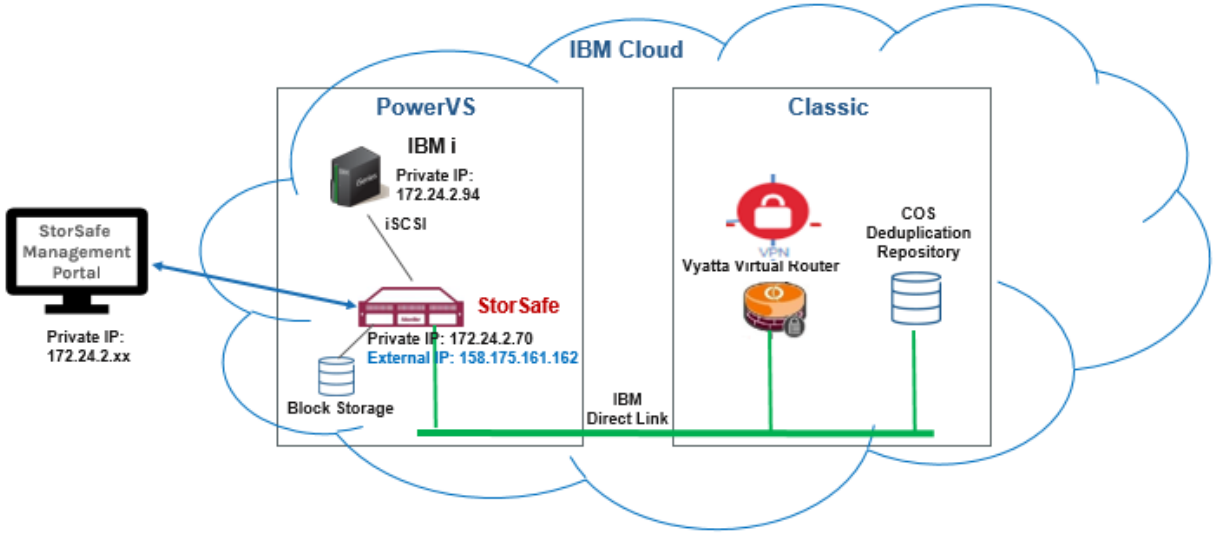
Several IBM i host clients are connected via iSCSI to StorSafe in the cloud to back up data via IBM Backup, Recovery & Media Services (BRMS) to virtual tape libraries. StorSafe uses IBM COS as the data devices for the deduplication repository via a Generic S3 object storage account.



Connectivity

The following connections are required:

- Network connections between StorSafe and the StorSight management portal
- iSCSI connections between StorSafe and IBM i host clients
- IBM Cloud Direct Link connection between StorSafe and the IBM COS in the IBM Cloud Classic environment
- Internet connection with the FalconStor license server for online registration (optional)



Example

Network default interface `eth0` has a public IP address and is used for all external connections.

Network interface `eth1` has a private IP address and is used to add routes to other networks.

The system command displays the network configuration on StorSafe as follows:

```
# ifconfig
  eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.150.162 netmask 255.255.255.248 broadcast
  192.168.150.167

  eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 9000
        inet 172.24.2.70 netmask 255.255.255.224 broadcast 172.24.2.95
```

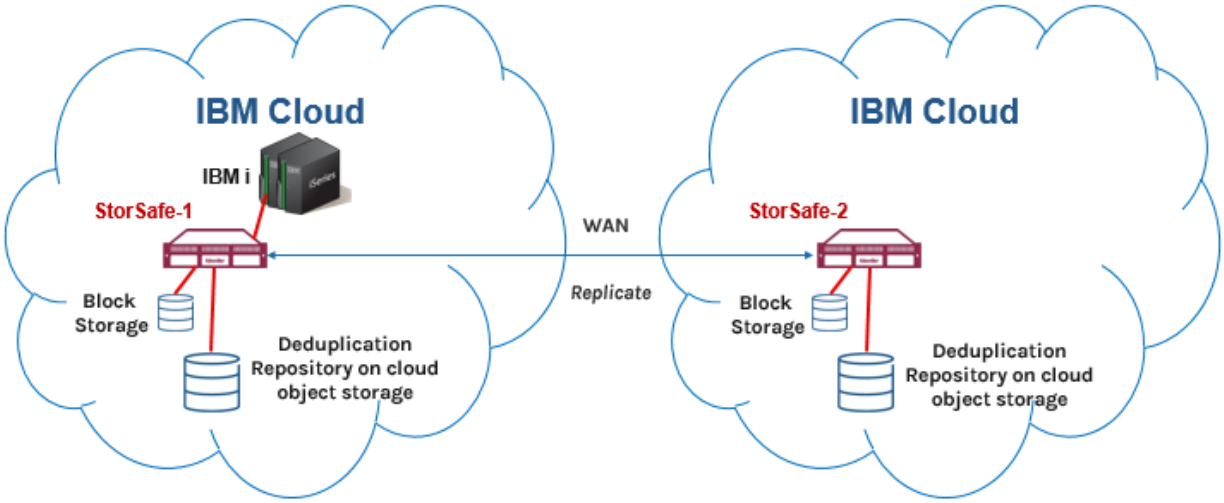
Create routes from the private IP to connect to the other networks. For example, `ADDRESS1=10.0.0.0` is for routing to the Classic infrastructure and `ADDRESS2=172.22.0.0` is added for routing to other private networks.

Any other customized networks to the route can be added using sequential numbers as a postfix.

```
# cat /etc/sysconfig/network-scripts/route-eth1
# Created by cloud-init on instance boot automatically, do not edit.
#
ADDRESS0=172.24.2.64
GATEWAY0=172.24.2.65
NETMASK0=255.255.255.224
ADDRESS1=10.0.0.0
GATEWAY1=172.24.2.65
NETMASK1=255.0.0.0
ADDRESS2=172.22.0.0
GATEWAY2=172.24.2.65
NETMASK2=255.255.0.0
```

Cloud-to-Cloud Replication Deployment

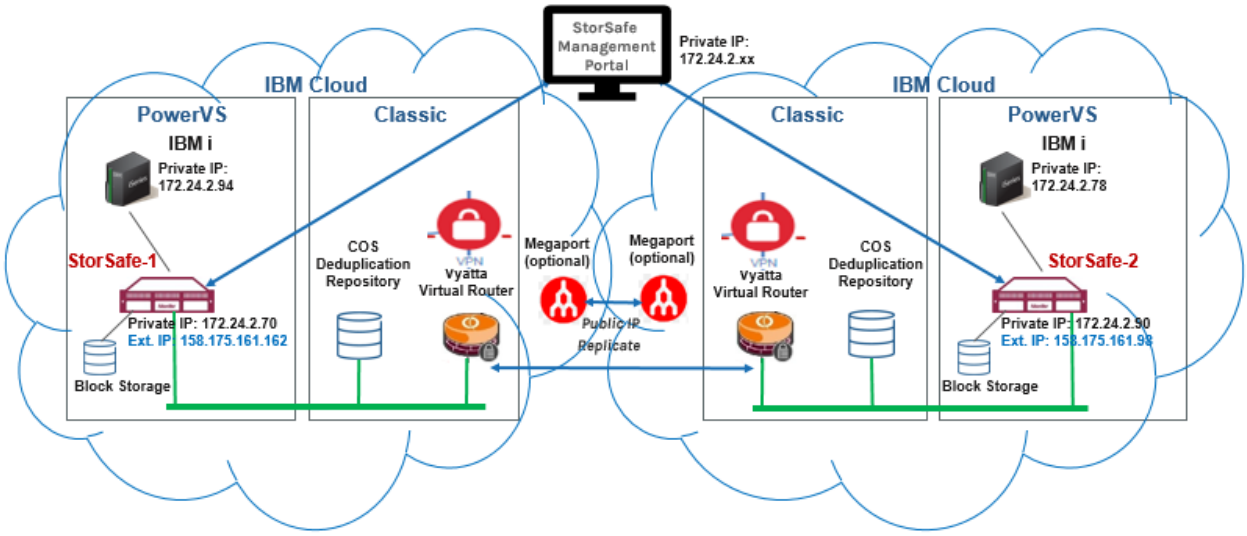
StorSafe in IBM Cloud replicates data over a WAN to another StorSafe in the cloud for data protection and disaster recovery. StorSafe source and replica servers use IBM COS as the data devices for the deduplication repository via Generic S3 object storage accounts.



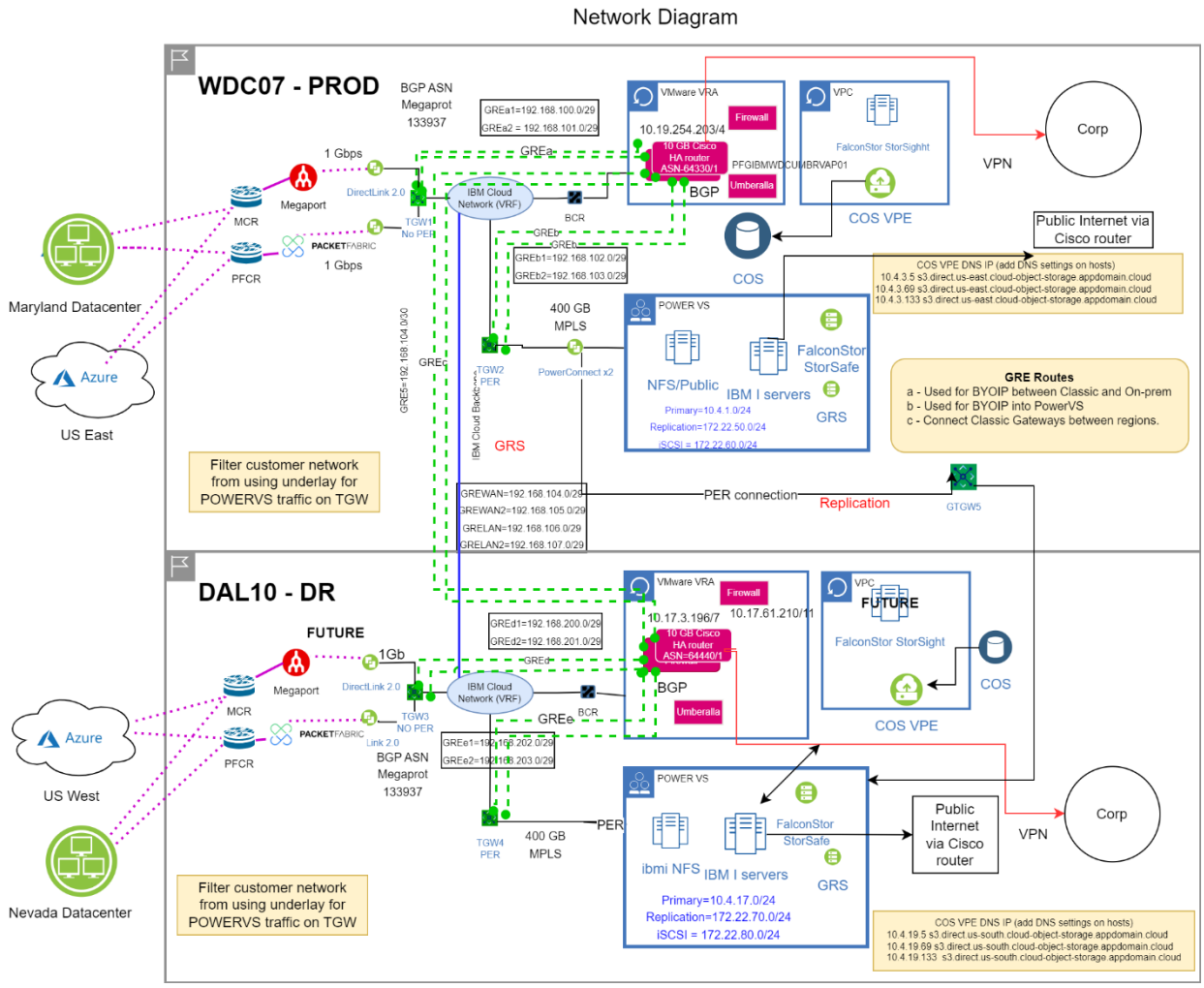
Connectivity

The following connections are required:

- Network connections between StorSafe and the StorSight management portal
- Network connection between the source and the replica StorSafe servers by virtual routers or Megaport
- iSCSI connections between StorSafe and IBM i host clients
- IBM Cloud Direct Link connection between StorSafe and the IBM COS in the IBM Cloud Classic environment
- Internet connection with the FalconStor license server for online registration (optional)

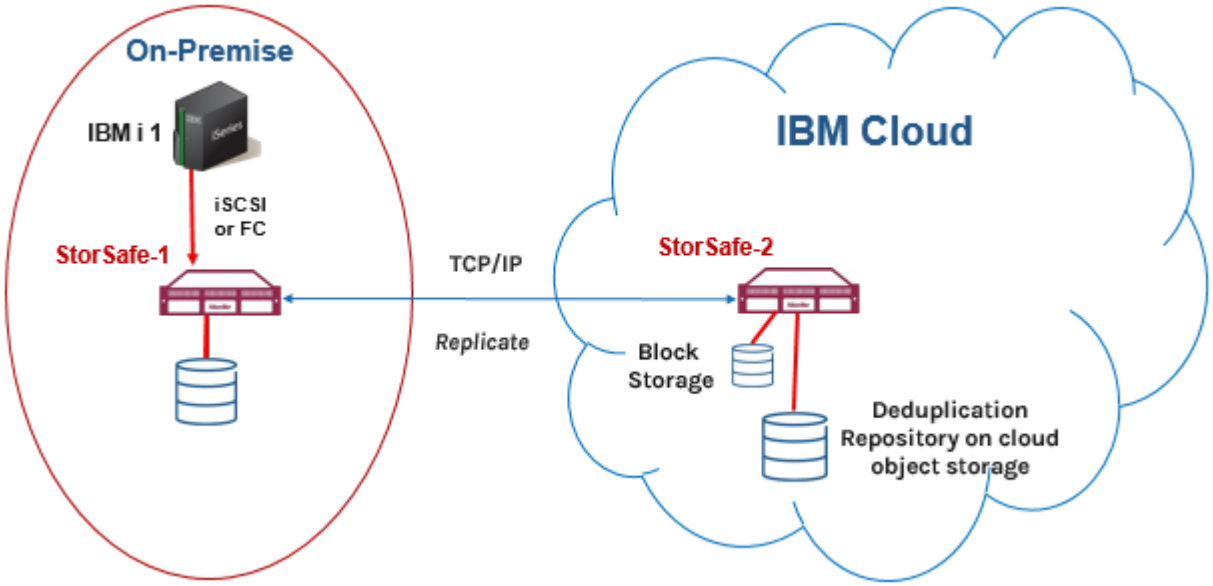


Deployment Network Example



Hybrid Cloud Deployment

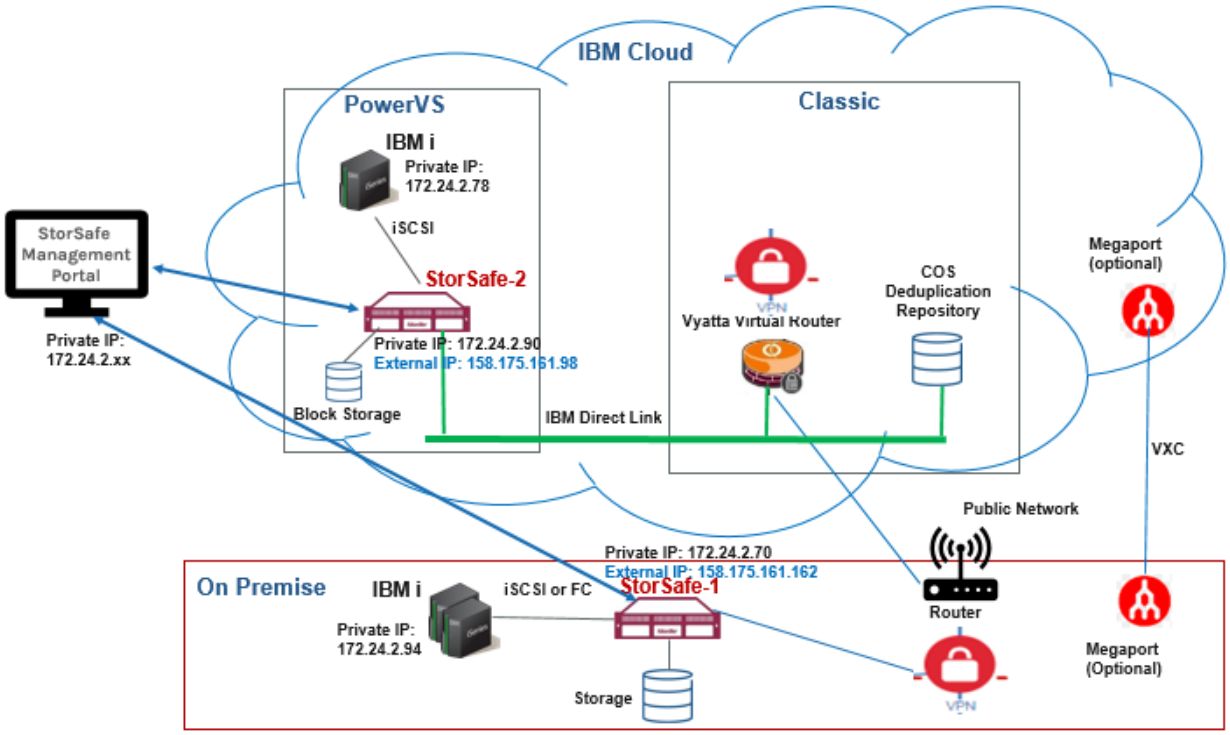
An on-premises StorSafe server deduplicates data and replicates to a StorSafe server in IBM Cloud for data protection and disaster recovery purposes. The on-premises StorSafe uses SCSI devices for the deduplication repository. The StorSafe target server in the cloud uses IBM COS as the data devices for the deduplication repository via a Generic S3 object storage account.



Connectivity

The following connections are required:

- Network connection between the on-premises StorSafe and the PowerVS StorSafe in IBM Cloud
- Network connection between StorSight in the classic infrastructure and the on-premises StorSafe
- Network connections between StorSight in the classic infrastructure and the PowerVS StorSafe in IBM Cloud
- iSCSI or Fibre Channel connection between IBM i host clients and the on-premises StorSafe
- iSCSI connections between IBM i host clients and the PowerVS StorSafe in IBM Cloud
- IBM Cloud Direct Link connection between the PowerVS StorSafe and the IBM Cloud Classic environment, if IBM COS is used for the deduplication repository
- Internet connection with the FalconStor license server for online registration


IBM Cloud
PowerVS
IBM i
Private IP:
172.24.2.78
iSCSI
StorSafe-2
Private IP: 172.24.2.90
External IP: 158.175.151.98
Block Storage
IBM Direct Link
Classic
Vyatta Virtual Router
COS
Deduplication
Repository
Megaport
(optional)
VXC
StorSafe
Management
Portal
Private IP:
172.24.2.xx
Public Network
Router
On Premise
IBM i
Private IP:
172.24.2.94
iSCSI or FC
Private IP: 172.24.2.70
External IP: 158.175.161.162
StorSafe-1
Storage
Megaport
(Optional)

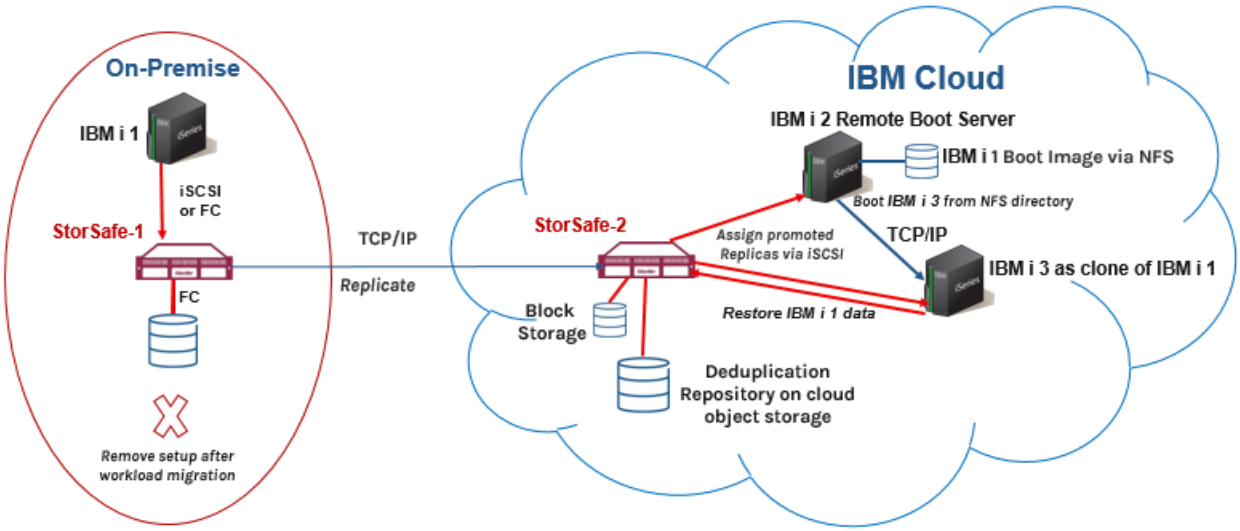
Workload Migration Deployment

IBM i backup clients of on-premises StorSafe servers are to be moved to the cloud via StorSafe data replication. StorSafe in the cloud uses IBM COS as the data devices for the deduplication repository via a Generic S3 object storage account.

The following describes how IBM Cloud can be used for workload migration:

1. IBM BRMS running at the primary site on an IBM i host client performs I/O to a FalconStor StorSafe server via iSCSI to back up the OS boot image and application data on virtual tapes. The IBM i host client needs to be prepared for migration; two virtual tapes are needed; the first tape will contain the base operating system for the initial remote boot and the second tape will contain the remaining data of the host machine image.
2. The primary StorSafe server deduplicates data and replicates both tapes to another StorSafe server in IBM Cloud.
3. On the replica site, the replica virtual tapes are promoted; the first tape is assigned to an IBM i remote boot server via iSCSI.
4. The IBM i remote server in the cloud mounts the OS image on the first promoted tape on an NFS share, then it boots another IBM i virtual server from the NFS boot directory running the same OS as the IBM i of the primary site.
5. The second tape is assigned to the new IBM i via iSCSI. This new server will read data from this second tape to complete the workload migration and become the clone of the IBM i on the primary site.

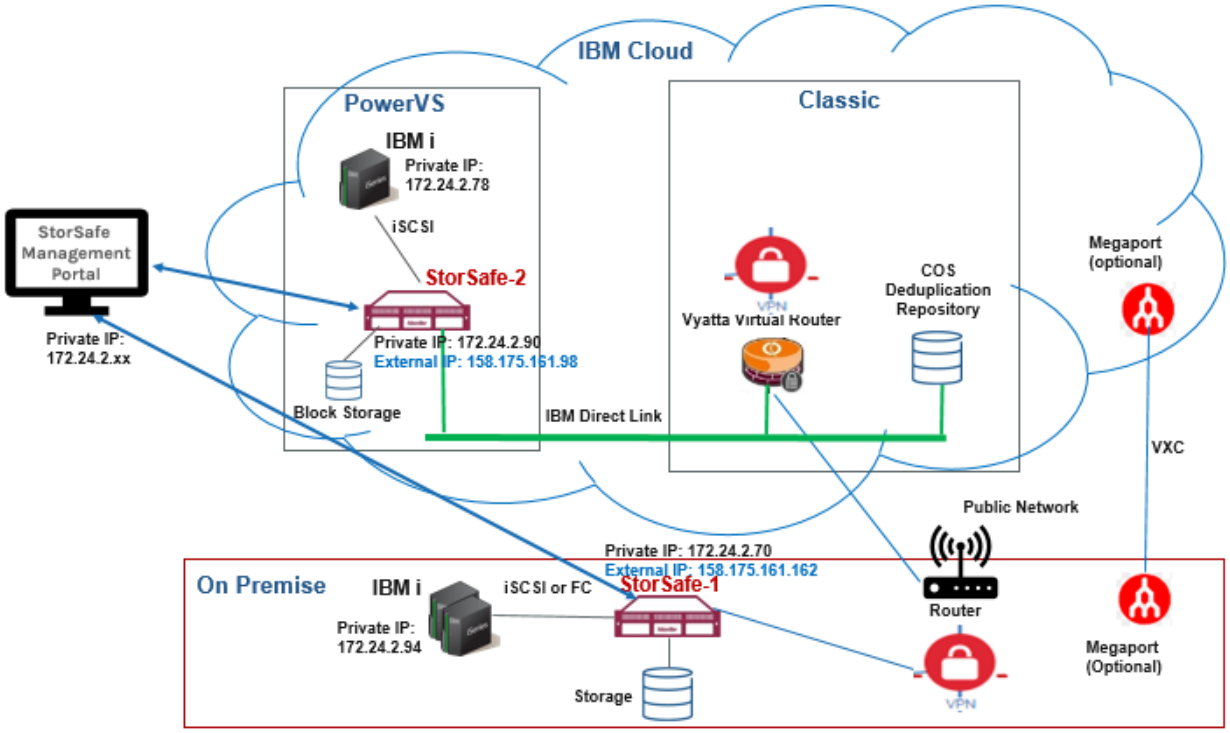
Refer to FalconStor knowledge base article 2162, which contains custom scripts developed for migration of IBM i/AIX workloads from on-premises Power to the PowerVS Cloud.



Connectivity

The following connections are required:

- Network connection between the on-premises StorSafe and the PowerVS StorSafe in IBM Cloud
- Network connection between StorSight in the classic infrastructure and the on-premises StorSafe
- Network connections between StorSight in the classic infrastructure and the PowerVS StorSafe in IBM Cloud
- iSCSI or Fibre Channel connection between IBM i host clients and the on-premises StorSafe
- iSCSI connections between IBM i host clients and the PowerVS StorSafe in IBM Cloud
- IBM Cloud Direct Link connection between the PowerVS StorSafe and the IBM Cloud Classic environment, if IBM COS is used for the deduplication repository
- Internet connection with the FalconStor license server for online registration (optional)
- When an IBM i host client is used for a workload migration scenario, it needs to be an NFS server to use the boot image for the cloned machine. Refer to IBM documentation for more information.



Prepare Deployment

This section contains information and deployment guidelines for FalconStor StorSafe in IBM Cloud.

Outline of steps

The following highlights the steps you need to perform; for each step, detailed information is provided in sections below:

1. Obtain an IBM cloud account with adequate access rights.
2. Identify the solution sizing.
3. Create worksheets to plan and record your deployment configuration.
4. Create or use an existing Power Systems Virtual Server service that represents your datacenter.
5. Create at least one subnet in your Power Systems Virtual Server service. You can create two more subnets to isolate traffic via VLANs for backup data and replication data.
6. Create SSH keys in the Power Systems Virtual Server service for secure remote connections.
7. Use the *FalconStor* StorSafe *for PowerVS* tile in the IBM catalog to create a power virtual server running the FalconStor software.
8. If you use COS for the deduplication data repository, create an object storage bucket on IBM Cloud. Note the access key, password, endpoint specifying the full URI/URL path to the object storage, region, and bucket name.
9. Install the FalconStor StorSight management portal.
10. Obtain a FalconStor license keycode for product usage.
11. Configure FalconStor StorSafe via the StorSight management portal.
12. Create power servers running backup software that will be attached as iSCSI clients to FalconStor StorSafe.
13. Configure iSCSI clients to be attached to the FalconStor StorSafe iSCSI target to perform backups.

Verify the following components before starting the deployment:

- Network connectivity
- Storage connectivity and integrity
- While you should have the current, generally available version of the software product at the time of deployment, you should always check the FalconStor Portal for the latest revisions and patches.

Access rights

Verify that you have Manager service access role for IBM Cloud Schematics.

Review and verify the Identity and Access Management (IAM) information to confirm you have adequate rights to create resources.

Sizing and licensing

To identify the required system resources, such as the amount of memory, CPU cores, and storage capacity for your FalconStor servers, you need to follow the sizing guidelines. StorSafe sizing depends on the amount of data to retain based on the size of ingest data, deduplication ratio, and backup parameters.

Refer to the FalconStor Solution Sizing page to get the sizing information about the deduplication repository, backup cache, memory, CPU, and the machine type.

Refer to the IBM Cost Estimation page. Click *Estimate costs* on the top right-side panel, select *Virtual Tape Library* as the operating system, enter values for usage parameters based on the Solution Sizing tool results, and then click *Calculate cost* and *Save* to see the cost. Click *Review estimate* to go to the *Cost estimator* page. Additional costs may apply based on extra capacity for the COS, or additional network and infrastructure components. For the COS capacity, go to *Catalog*, type *Object Storage* in the Search box, and select the *Standard* plan. Click *Estimate costs*, enter a value for *Monthly average capacity*, and click *Calculate cost* again.

The FalconStor StorSafe license will be activated as soon as it is added to StorSight for management. StorSafe servers do not require individual licenses. A global unique license is provided for StorSight that manages all StorSafe servers. After you create a StorSafe PowerVS, look for an email from FalconStor to receive a license keycode to enter into FalconStor StorSight.

Required storage

Besides the operating system (OS) disk, there are four classes of storage resources:

- Tapes – For storing virtual tapes and virtual index tapes
- Configuration Repository and Database - A small resource used for reporting and configuration management
- Deduplication Repository – For storing unique blocks of data
- Deduplication index/folder and configuration repository - For storing metadata

The following storage types are required for StorSafe. Only the deduplication repository can use cloud object storage; others use block storage:

- OS boot disk: 200 GB
- Configuration repository and tape database disk: 20 GB
- Deduplication repository: Amount of data to retain based on the size of ingest data, deduplication ratio, and backup parameters; the deduplication ratio is an estimated value based on the nature of the data. To estimate the deduplication repository size, you can divide the amount of data by the deduplication ratio.
- Storage for deduplication index and folder disks: 4.3% of the deduplication repository size
- Storage as backup cache to hold virtual tape data: Sum of:
    a. Amount of data to be moved to the deduplication repository. If the input rate is high, the cache must be large enough to buffer data for several days. To be safe, you can estimate the amount as one week's worth of data, considered as *weekly ingest data*.
    b. Size of virtual tape indexes, which is estimated as 3% of *weekly ingest data* multiplied by the number of weeks to retain data
    c. Size of replica tape indexes in case of incoming replication, which is estimated as 6% of *weekly ingest data* multiplied by the number of weeks to retain data
    d. Size of largest dataset to restore

Object Storage

If you use Cloud Object Storage (COS) for the StorSafe deduplication repository data disks, get an S3 object storage bucket with "**Object Writer**" access, with service credentials including HMAC. Note the bucket name, location, access key ID, and secret access key. Create an IBM COS bucket with the service credentials, including HMAC for the deduplication repository.

Required memory

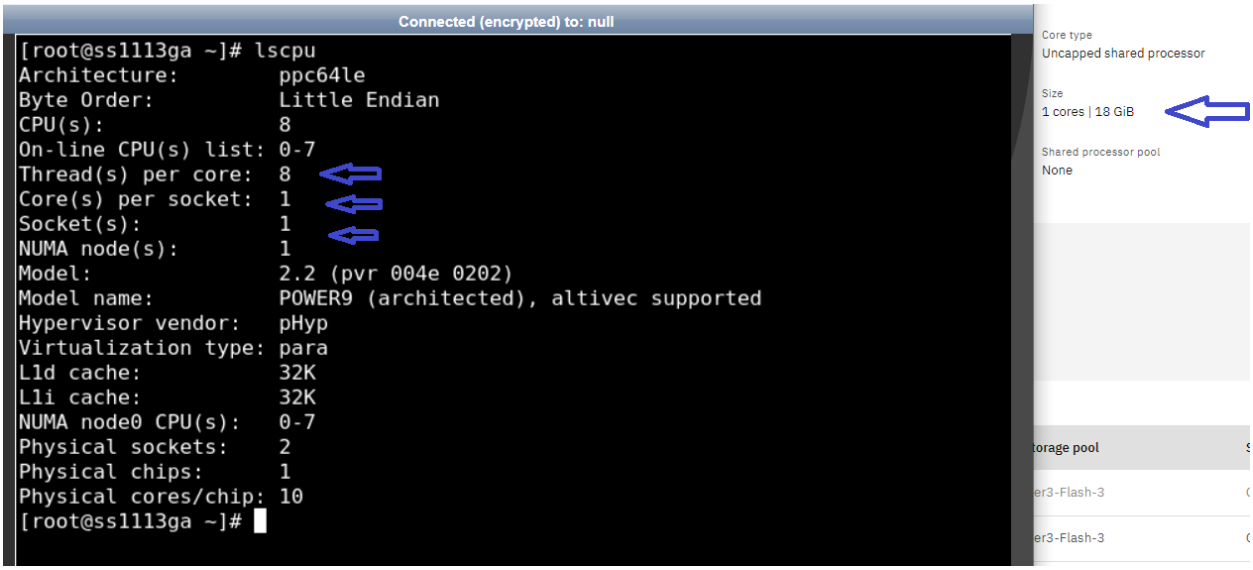
The memory reserved for deduplication depends on the size of the deduplication repository, where 2 GB memory is used for each 1 TB of deduplication repository capacity.

You will need at least 16 GB of base memory plus 2 GB for each TB of deduplication repository.

Required CPU cores

A core is a physical unit of a Central Processing Unit (CPU) that acts as a separate processing unit. Basically, a core can be considered as a small processor built into the main processor that is connected to a socket. A virtual CPU (vCPU), also known as a virtual processor, represents the central processing unit used in a virtual machine (VM). Each vCPU in a VM operating system represents one physical CPU core. Since there is a core-to-vCPU ratio of 1:1, for shared processors, fractional cores round up to the nearest whole number. For example, 1.25 cores equal 2 vCPUs. Note that with hyper-threading the OS detects a single-core processor as a processor with more logical cores (not physical cores).

For example, the `lscpu` command shows the following output for a VM with one core:



For large systems requiring a high amount of memory based on the deduplication repository size, use more CPU cores:

- Deduplication repository up to 10 TB: 1 CPU core
- Deduplication repository up to 50 TB: 2 CPU cores
- Deduplication repository up to 100 TB: 4 CPU cores
- Deduplication repository over 100 TB: 8 CPU cores

Network connections

The StorSafe instance can have public and private networks for remote access. The public network hosts an external IP address. You can either connect to the instance using the IBM **Open console** option or connect to the StorSafe public IP via a remote SSH session using the pre-installed SSH key. Once you are connected you can configure required routing to private IP interfaces for private routes.

The traffic with the StorSight management portal, IBM COS for deduplication repository, iSCSI clients, and tape replication goes through the private IP addresses. Perform the following steps:

- Configure network routers with a VPN configuration and firewall settings.
- Check network settings for speed and Maximum Transmission Unit (MTU) values on network devices and routers. For example, network devices can have an MTU value of 1500 bytes but tunnel interfaces, as used in the cloud, can have **1476** or lower bytes, since they use some bytes for IP headers. You can use the system command `ping` to confirm the maximum transmission size value for a network device (default `eth0`) does not display any errors:
  `# ping [-I <NetWork device>] -s <MTU value> -M do <IP address>`
- If IBM COS is used for the deduplication repository, set up cloud connections.
- Make sure the DNS settings are correct in `/etc/resolv.conf` of the StorSafe and StorSight servers to resolve the host names. Use the system command `ping` to confirm connectivity with the name servers and FalconStor servers.

Required network ports

Make sure network firewalls allow StorSafe access through the following ports.
Refer to the *Appendix* section in the *FalconStor StorSafe with StorSight User Guide* for more details:

- TCP port 22 for remote connection via Secure Standard Shell (SSH)
- TCP/UDP port 25 for email alerts via SMTP
- TCP port 80 for internet connection to the FalconStor license server (*register.falconstor.com*), for online registration of license keycodes. If this cannot be set up for security reasons, offline registration can be used.
- UDP port 123 for time synchronization via NTP
- TCP port 3260 for communication between StorSafe and iSCSI clients
- TCP port 11576 for secure RPC communication between StorSafe and StorSight
- TCP/UDP port 11577 for incoming data replication (if replication is configured)
- TCP/UDP port 11579 for replication authentication (if replication is configured)
- TCP port 11581 for StorSight statistics gathering
- TCP port 11582 for CLI commands (if applicable)
- TCP port 11584 for replication of deduplicated data (if replication is configured)
- TCP port 11583 for report requests
- TCP ports 11781 and 11782 for replication encryption (if applicable)
- TCP port 18651 for non-encrypted replication (if applicable)
- TCP port 18652 for encrypted replication (if applicable)

StorSight ports

- HTTP port 80 for internet connection
- HTTPS port 443 for secure internet connection
- LDAP port 636 for LDAP and Active Directory authentication (if applicable)
- TCP port 11753 for retrieving StorSafe configuration

Deployment Worksheets

Use the following worksheets to plan and record your deployment configuration.

Network IP addresses

The table below describes information about IP addresses needed on each StorSafe server:

- **Name** represents a meaningful label to identify the network usage
- **Port** represents a network device, *ethn*
- **Type** can be
  - *Private* (for private subnets and VLANs)
  - *Public* (for outside communication)
- **Usage** identifies what the network will be used for, such as:
  - StorSight management portal and *COS* access
  - *iSCSI clients* in different areas
  - *Replication* traffic with a remote server
  - *Outside* communication via a public IP address

Name	Port	IP Address	Type	Usage

iSCSI clients

The table below describes information about iSCSI clients.

Client Name	IP Address	iSCSI Initiator IQN	iSCSI Target IQN

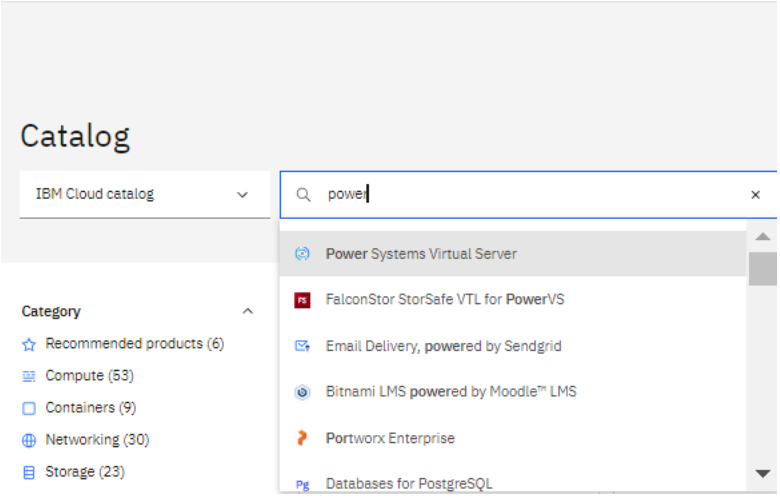
Data replication

Source Site Location	
Target Site Location	
WAN Link Type	
WAN Length	
WAN Bandwidth	
Cross Replication or not	
Dedicated or Shared	

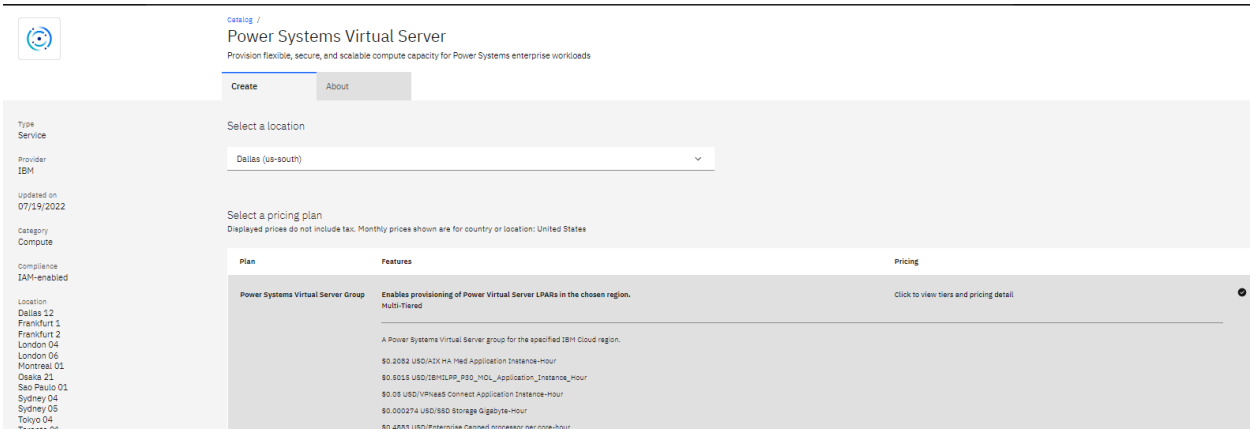
Create a Power Systems Virtual Server service

Before deploying a StorSafe PowerVS instance, you need to have a Power Systems Virtual Server service that represents a datacenter with adequate networking and infrastructure for your deployment scenario. If you do not have a Power Systems Virtual Server service, follow the instructions below to create one.

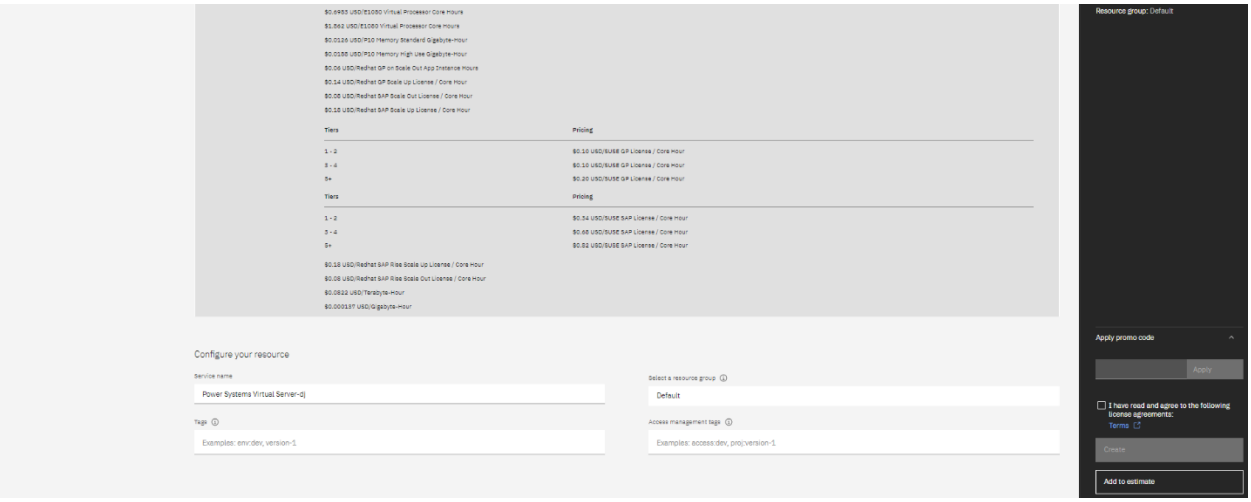
1. Connect to IBM Cloud using your credentials.
2. Click *Catalog* in the menu bar, type *Power* in the search box, and select *Power System Virtual Servers.*



3. Select a *location* that matches your region. You are limited to only one service per region.



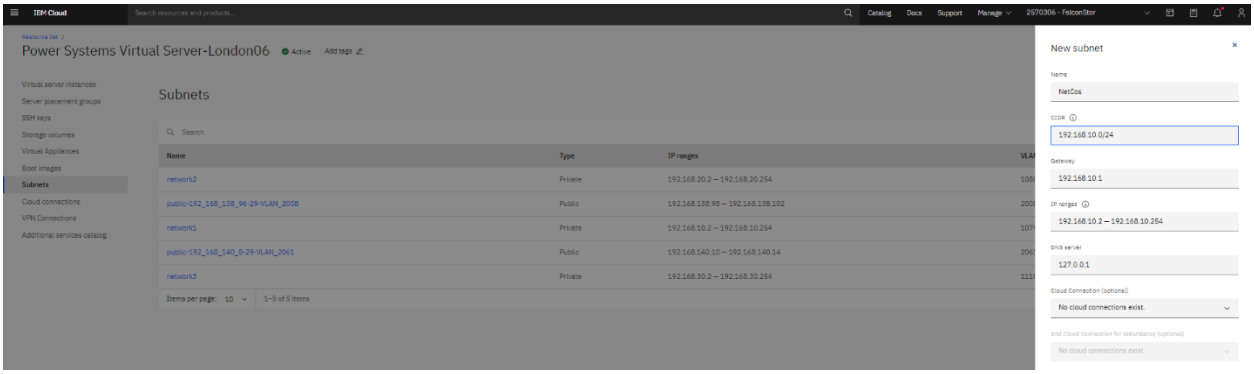
4. Update the *Service name* or leave the default name and press *Create*.



Create network subnets

To isolate traffic via VLANs, create at least three subnets in your Power Systems Virtual Server service for different usage, such as *StorSight Portal* and *COS* access, *iSCSI clients* in different areas, and *Replication* traffic with a remote server. You can have as many subnets as you require in each Power Systems Virtual Server service. Once you specify the networks, IBM *cloud-init* configures the IP addresses.

1. Click *Resource list*, select *Services and software*, and select your Power Systems Virtual Server service.
2. Select *Subnets* and click *Create subnet*.
3. Enter a meaningful label to identify the network usage.
4. Enter the IP address range and click *Create a subnet*.



Add SSH keys

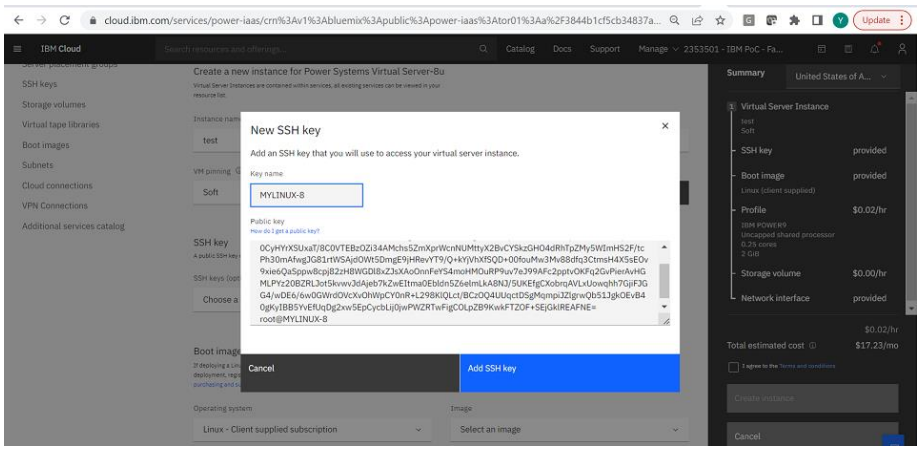
SSK keys are used for secure remote connections to StorSafe.

A public key can be created by using the `ssh-keygen` command available in the *OpenSSH Client* application to generate the RSA public key file `id_rsa.pub`:

```
# ssh-keygen
# cat /root/.ssh/id_rsa.pub
ssh-rsa
AAAAB4NzaC1yc2EAAAADAQABAAABgGzx4Z8z8AskuIgVOGBJ+psPbmOOHCAApR3bfoOHDztyG36rt
0CyHYrXSUxaT/8C0VTEBzOZi34AMchs5ZmXprWcnNUMttyX2BvCYSkzGHO4dRhTpZMy5WImHS2F/t
cPh30mAfwgJG81rtWSAjdOWt5DmgE9jHRevYT9/Q+kYjVhXfSQD+00fouMw3Mv88dfq3CtmsH4X5s
EOv9xie6QaSppw8cpj82zH8WGDl8xZJsXAoOnnFeYS4moHMOuRP9uv7eJ99AFc2pptvOKFq2GvPie
rAvHGMLPYz20BZRLJot5kvwvJdAjeb7kZwEItma0Ebldn5Z6elmLkA8NJ/5UKEfgCXobrqAVLxUow
qhh7GjiFJGG4/wDE6/6w0GWrdOVcXvOhWpCY0nR+L298KlQLct/BCzOQ4UUqctDSgMqmpiJZlgrwQ
b51JgkOEvB40gKyIBB5YvEfUqDg2xw5EpCycbLij0jwPWZRTwFigCOLpZB9KwkFTZOF+SEjGklREA
FNE= root@MYLINUX-8
```

To add your SSH key to the Power Systems Virtual Server service, perform the following steps:

1. Click *Resource list*, select *Services and software*, and select your Power Systems Virtual Server service.
2. Select *SSH keys* and click *Add SSH key*.
3. Enter a *Key name* and copy and paste your SSH key file contents in the *Public key area*. Click *Add SSH key*.

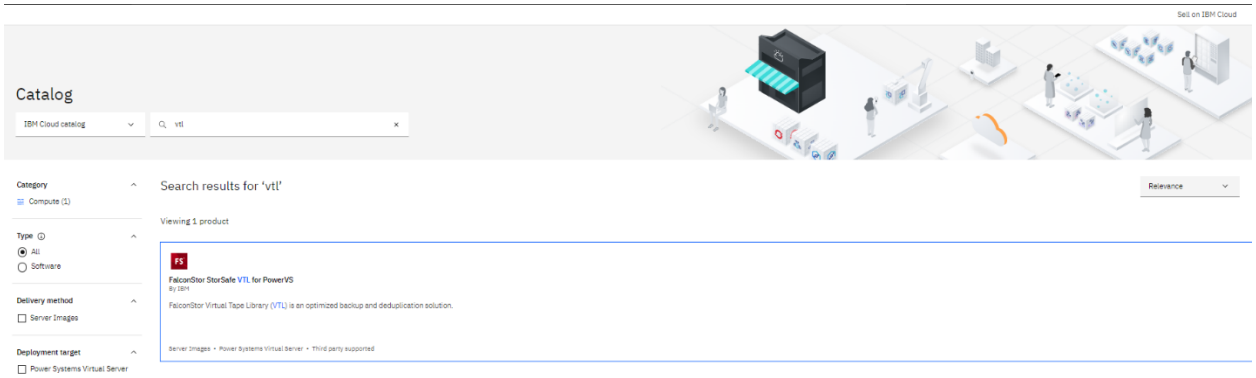


Create StorSafe Power Virtual Server

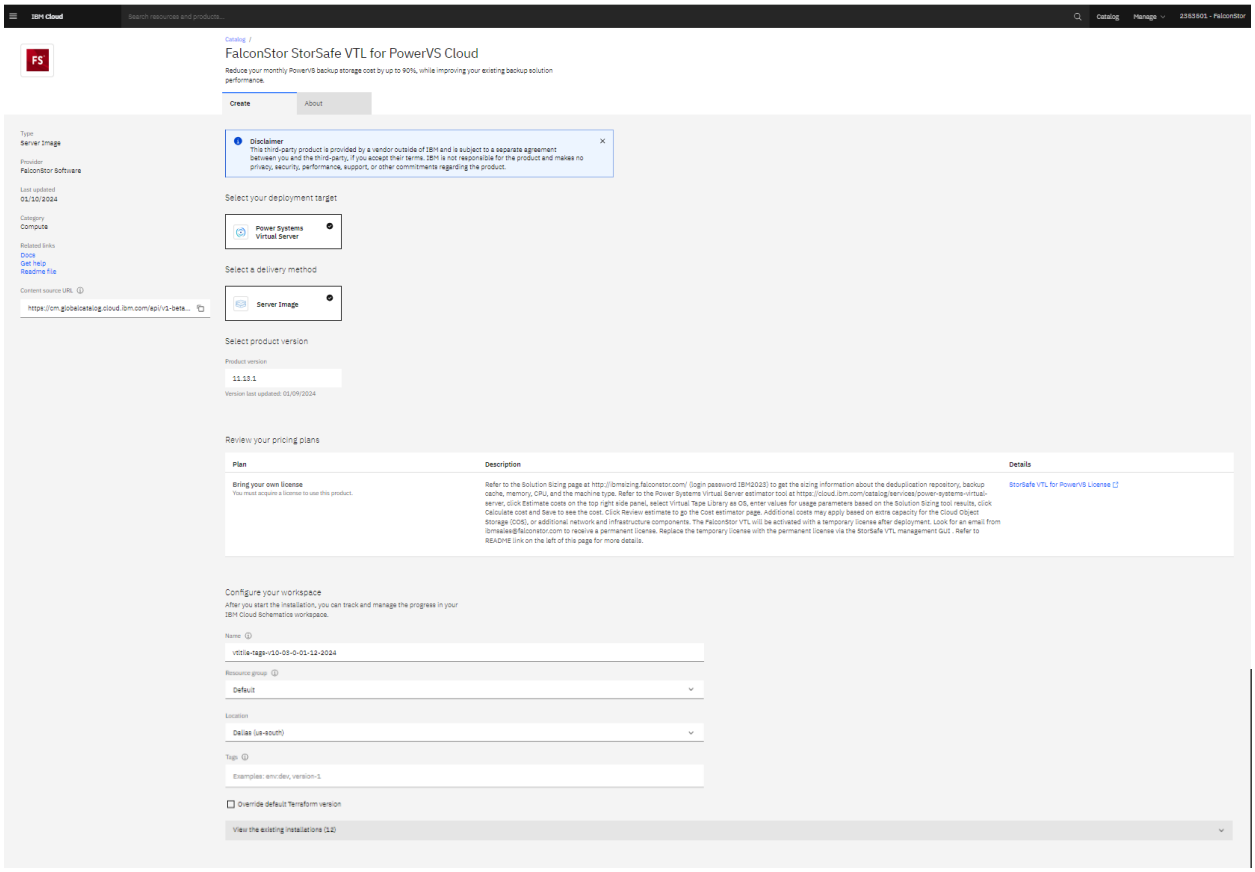
This section explains how to create a power virtual server running the FalconStor StorSafe software product in IBM Cloud. The FalconStor Open Virtual Appliance (OVA) package contains the Linux OS image and FalconStor StorSafe software.

Follow the instructions below to access the software from the IBM catalog tile:

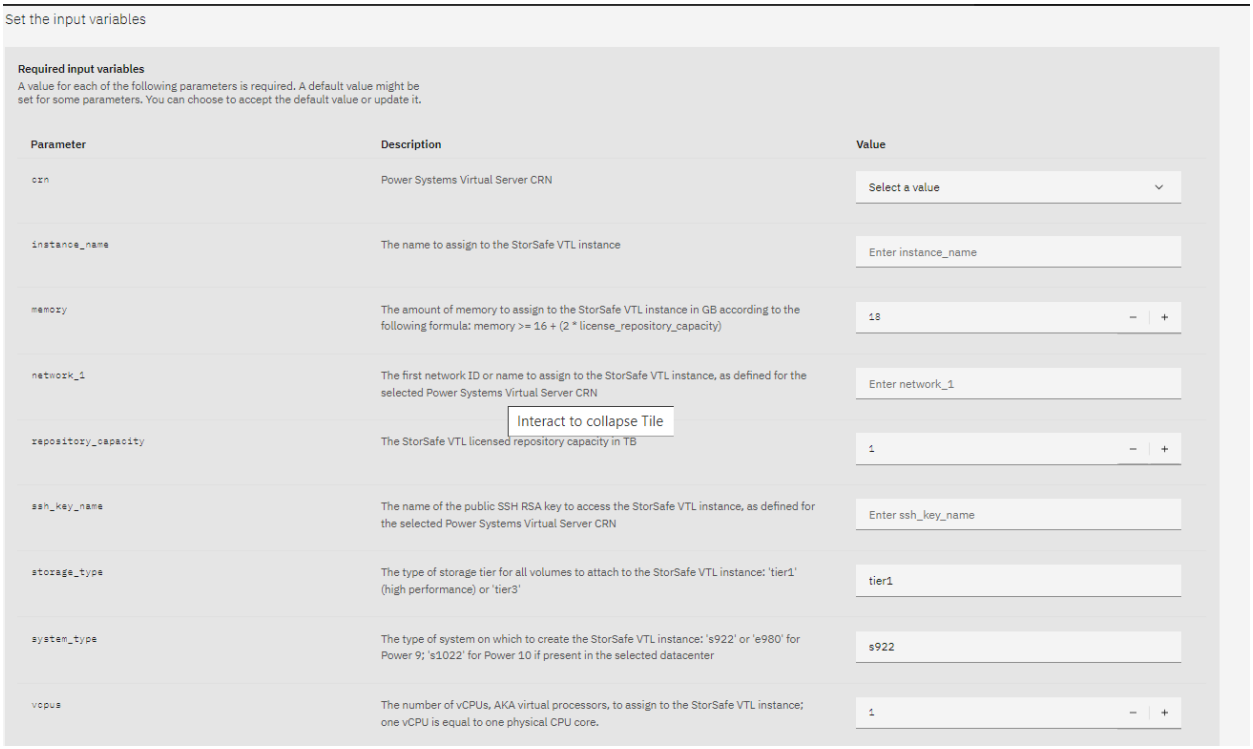
1. Connect to IBM Cloud using your credentials.
2. Click *Catalog* in the menu bar, type *vtl* in the search box, and select the *FalconStor* StorSafe *for PowerVS* tile.



3. Use *Power Systems Virtual Server* as the deployment target, use *Server Image* as the delivery method, and select the version. Leaver other settings as default.

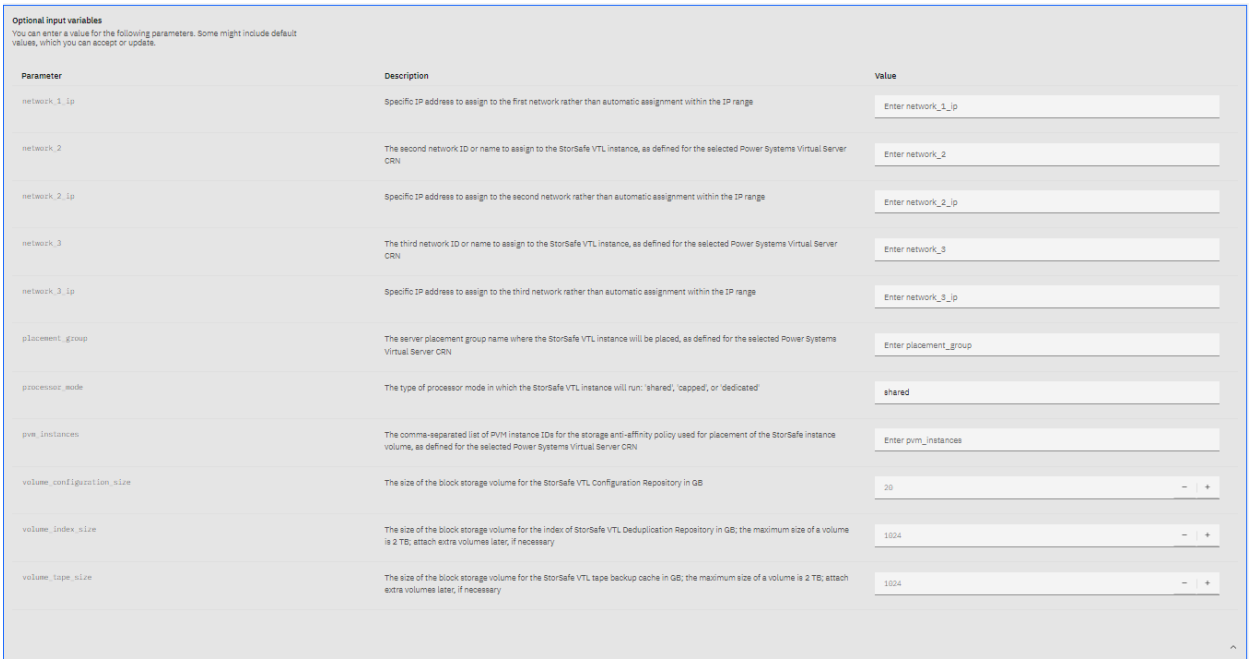


4. Set the server required values:
   a. Select the Power Systems Virtual Server Cloud Resource name (CRN) that represents your data center.
   b. Enter a name for your StorSafe instance.
   c. Set the memory size, according to the sizing calculator tool results.
   d. Enter one network name that you want to use, as defined for the selected Power Systems Virtual Server CRN. Refer to the Network IP addresses worksheet that has been prepared for this deployment.
   e. Set the size of your license repository capacity.
   f. Enter the SSH key name, as defined for the selected Power Systems Virtual Server CRN.
   g. Choose the storage type; *Tier 3* is cheaper than *Tier 1* but *Tier 1*provides better I/O performance. Make sure you choose the same storage type for all attached storage devices; do not use mix storage types.
   h. Select the type of the system on which to create the StorSafe VTL VM based on the server sizing: *s922* or *e980* for Power 9 and *s1022* for Power 10. For *s1022* make sure a Power10 machine exists on the datacenter that you selected in CRN. The system type *e980* should be used for a large system that requires more memory to hold a deduplication repository of around 400 TB.
   i. Set the number of vCPU cores, according to the sizing calculator tool results.

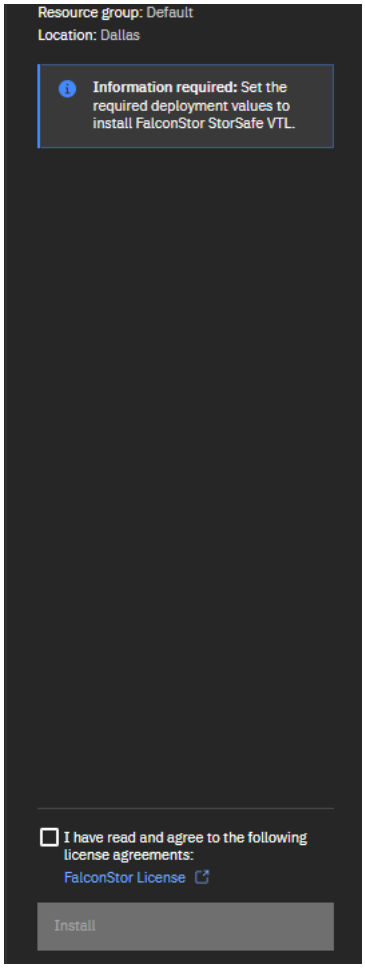


5. Expand the *Optional input values* to check other deployment values.
   a. You can enter two extra network names that you want to use for traffic isolation.
   b. You can enter a specific IP address for each network. This is useful when you perform an A-to-B upgrade scenario, where you want the network configuration of source machine A be preserved on target machine B.
   c. If applicable, enter the name of a server placement group where the StorSafe instance should be placed, as defined for the selected Power Systems Virtual Server CRN.
   d. Set the processor mode: *Shared*, *Dedicated*, or *Shared Capped*. *Shared* is less expensive.
   e. To place the StorSafe volume on storage controllers, according to a storage anti-affinity policy, enter the PVM ID of other server instances, as defined on the selected Power Systems Virtual Server CRN. The ID is displayed in the server details. This can be useful when other VMs exist in your environment and StorSafe is not the first VM to be added. An anti-affinity rule places a group of virtual machines across different storage controllers, which prevents all VMs from failing at once in case a single controller fails.

      NOTE: For both storage affinity and server placement group, we recommend that StorSafe not be on the same server or storage box as other machines it will be backing up.
   f. Accept or update block storage size values for the configuration repository, tape cache, deduplication repository index and folder disks.



6. Check all parameters, click the license agreement box on the right, and click *Install* to continue. Once installation is complete, the StorSafe instance will appear in the list of *Virtual Appliances*.



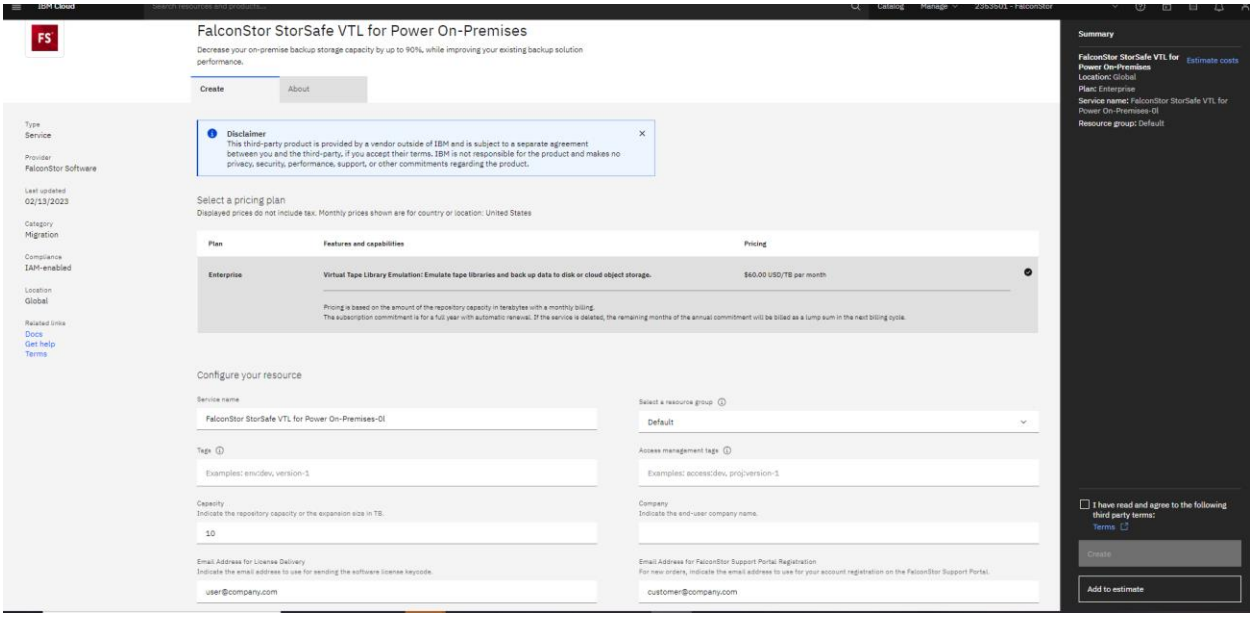
7. Click *Virtual Appliances* and select your instance.
8. Click StorSafe *actions* and select *Open console*. Connect to the instance using the *root* user account and the default password *IPStor101*. The system will then prompt you to enter a new password for the root account, since the default password expires after installation.
   You can also connect to the IP address via *ssh* with the SSH key using the *centos* user account (`ssh centos@<StorSafe IP Address>`), become *root* by the `sudo su –` command and then run the `passwd` command to enter a new password for the *root* account, to replace the expired password. Alternatively, you can use the `sudo -i` command to enter a new password.
9. Check the network IP addresses with the `ifconfig` command, check the default gateway with the `ip -route` command, and the routing table with the `netstat -nr` command.
   The default gateway is set based on the first assigned IP subnet that is used for management and can be reached from outside. When there are multiple subnets, you can set the system to use a specific subnet for backup and another subnet for replication.
10. When you deploy a VM on Power, an IPV6 private network connection gets configured in order to manage the VM. If that connection is down, the server may remain in the 'Warning' state and adding disks or changing memory/vCPU cannot be performed. If this occurs, run the following commends to reset the configuration:

```
/usr/sbin/rsct/install/bin/uncfgct -n
sleep 5
```

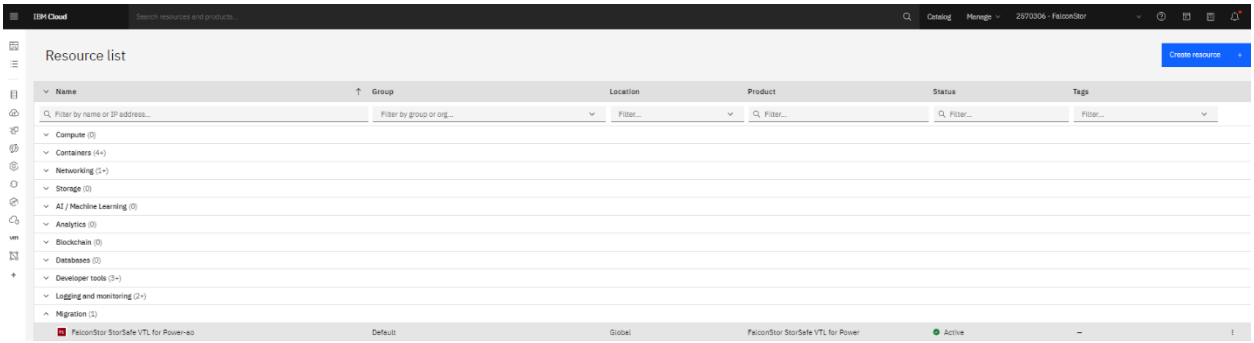
```
/usr/sbin/rsct/install/bin/cfgct
sleep 5
/usr/sbin/rsct/bin/rmcctrl -z
/usr/sbin/rsct/bin/rmcctrl -A
/usr/sbin/rsct/bin/rmcctrl -p
```

Deploy StorSafe On-Premises

If you need to deploy an on-premises StorSafe VTL server, select the *FalconStor StorSafe VTL for Power On-Premises* service from the IBM catalog. It can take about 15 minutes to complete.



After you create the StorSafe VTL software service, a new resource appears in the IBM *Resource list* under the *Migration* category:



Follow the steps below to deploy an on-premises server:

1. Click the StorSafe VTL service to display download links for FalconStor software and documentation.
2. Download the Software Appliance Kit (SAK) installation packages for FalconStor StorSafe and FalconStor StorSight.
3. Refer to *Sizing and licensing* and the StorSafe and StorSight release notes for sizing and requirements.
4. Refer to the FalconStor Server SAK ISO Image Installation Guide to install the FalconStor software.
5. Look for an email from FalconStor to receive a license keycode to enter in the FalconStor StorSight.

Install StorSight Management Portal

FalconStor StorSight is a web-based portal for centralized management and monitoring of multiple backup and deduplication servers.

For StorSight installations on a physical or virtual appliance where a supported Linux operating system has already been installed, use the FalconStor Software Appliance Kit (SAK) image, which installs StorSight and configures the Linux operating system for use with StorSight. This section describes the installation procedure and how to run configuration scripts.

For StorSight installations on a physical appliance where no operating system exists, use the FalconStor USB bootable image, which contains the operating system, chassis management utilities, and StorSight software. Refer to the *FalconStor Physical Appliance Installation Guide* for details.

Create a virtual server

1. Connect to the IBM cloud using your credentials.
2. Click *Catalogue* in the menu bar and select *Virtual Server for Classic* or *Virtual Server for VPC*.
3. Change the default *Hostname*, if desired.
4. Set the *Location* to match your region.
5. Select *View all profiles* to define system resource, for example, select *bx2d-4x16* for 16 GB RAM and 4 vCPU or *M1.4x32* for 32 GB RAM and 4 vCPU and click *Save profile*.
6. Add a SSH key for easy secure access to the virtual server.
7. For *Operating system*, select Vendor RedHat or Rocky and Version *8.x - Minimal Install (64 bit)*.
8. For *Attached storage disks*, set the size of the Boot disk to 100 GB.
9. Click Add new to add Disk1 for the StorSight database with a size of 100 GB.
10. Check the *'I read*…' box to confirm the configuration and click Create to complete virtual server creation.
11. If using *Virtual Server for VPC*, remotely log in to your new virtual server from a server having the SSH key. Set up the root password.
12. If using *Virtual Server for VPC*, retrieve the server password. Click the *IBM Cloud Navigation Menu* icon on the top right, select *Classic Infrastructure -> Device List*. Select your device. Click *Passwords*, click the view icon to see the default root password for server connection.

Start StorSight installation

1. Download the FalconStor StorSight SAK image to the server having the SSH key and then copy it to your virtual server via the system command `scp`.
2. Log in to the virtual server.
3. Mount the FalconStor StorSight installation ISO file:

```
mount -o loop SAK-Install-….iso  /mnt
```

4. Navigate to the mounted directory:

```
cd /mnt
```

5. Run the following command to adjust the Linux kernel and to rename the Ethernet ports to `eth`*x*:

```
./OSupdate
```

6. At the prompt, after successful completion of the OS update, press the *Enter* key to reboot.
7. After reboot, navigate to the SAK image directory, mount the FalconStor StorSight installation ISO again, and navigate to the mounted directory, following the steps described above.
8. Execute the StorSight installation script to update dependency RPMs.

```
./freestorinstall
```

9. Navigate to the previous directory:

```
cd -
```

10. Unmount the FalconStor StorSight installation ISO file:

```
umount /mnt
```

Configure StorSafe via StorSight

You need to run FalconStor StorSight to configure StorSafe. The StorSight web portal allows you to connect to each server for management and monitoring purposes.

Refer to the *FalconStor StorSafe with StorSight User Guide* for more details.

The following highlights the configuration steps for StorSafe:

- Open any HTML5-capable browser and type the IP address of your FalconStor StorSight Server. Enter your username, domain, and password to log in. The default login is:
    - Username: *superadmin*
    - Domain: <blank>
    - Password: *freestor*
- Agree to the End User License Agreement (EULA) that appears the first time that the StorSight management portal is launched.
- Select *Administration -> StorSight*. Click *License*, and the "+" icon to add your license keycode received from FalconStor. Register your license.
- Select *Administration -> Servers* from the menu bar and click the "+" icon to add your StorSafe server. Enter the IP address or hostname of the StorSafe server. Enter the root user and password for the StorSafe server. Click *Add*.
- In the *Manage* tab select your StorSafe server.
- Select the *Physical Resources –> Physical Devices* tab to virtualize storage devices. Select unassigned physical devices, click the *Manage* icon, and select *Prepare*. Set the category as *Virtual* and the appropriate reservation type: *Configuration* for the 20 GB device to be used as the Configuration Repository and tape database, *Deduplication* for index and folder devices of the Deduplication Repository, or *Tapes* for backup cache devices. Click *Prepare*.
- Select the *Object Storage* tab and click the "+" icon to add the object storage account to be used for deduplication. Select the *Generic S3* provider, enter the IBM Cloud access account information noted above, and enable the "*Use for Deduplication Repository*" option. If you use a reverse proxy server to make remote connections to IBM COS private endpoints, enter the proxy IP address and user/password.
- Select the *Settings* tab.
    - Click the *Configuration Repository* icon. Click *Create Configuration Repository*. Select the physical device reserved for Configuration and click *Create* to enable the Configuration Repository using 10 GB of the reserved device.
    - Click the *Tape Database* icon. Click *Create Tape Database*. Select the physical device reserved for the configuration and click *Create* to enable the tape database using 10 GB of the reserved device.
    - Click the *Deduplication Repository* icon. Click *Create Deduplication Repository*. Select *Object Storage* for the Deduplication Repository data disks. select the object storage account that you had created with the "*Use for Deduplication Repository"* option. Select the physical devices reserved for Deduplication that will be used for the deduplication index and folder and click *Create* to enable the Deduplication Repository.
    - Enable iSCSI target mode to enable host clients running backup software to communicate with StorSafe via the iSCSI protocol.

- Select the *Virtual Libraries* tab and click the "+" icon to create virtual tape libraries with IBM drives:
    - For IBM i host clients, select the virtual tape library type as *FalconStor FALCON TS3500L32 (03584L32)* or *FALCON TS3500L32 (03584L32)* and the media type as *ULTRIUM3 (LT03)* or newer. By using Falcon library types, you get the *3584-403* device types to configure on IBM i host clients.
    - Set the library name, the drive name prefix, number of drives, barcode range for tapes, and set the number of Import/Export slots to 1.
    - Enable Tape Capacity On demand (COD) to create small resources for your tapes and then automatically allocate additional space when needed. The minimum value for the incremental size is (Maximum Capacity – Initial Tape Size) / 63.
    - Leave default settings and do not enable any service options.
- Configure iSCSI from the client side according to the *Configure an iSCSI client* section below.
- Select the *Host Clients* tab and click the "+" icon to add host clients to which virtual tape libraries will be assigned for backup:
    - Specify the client name and select *iSCSI* as the communication protocol.
    - Click the *iSCSI* tab to select the initiators that this client will use. If the initiator does not appear, you may need to rescan by clicking *Rescan Initiators*. The client iSCSI initiator name is the same as the one configured on the client side, for example, *iqn.1994-05.com.ibm:apacibmi74falcon*.
    - Do not enable CHAP, to allow unauthenticated access.
- Select the newly created host client to create an iSCSI target for the client. Click the *Manage* icon and select *Create iSCSI Target*. Enter the iSCSI target name as the one configured on the client side, for example, *iqn.2000-03.com.falconstor:h21-47.ibmi94*. Select the IP address of the adapter on the StorSafe server. Leave the starting LUN as 0. One iSCSI target should be created for each iSCSI client initiator. Refer to "Configure an iSCSI client" for more information.
- Select the newly created host client to assign virtual tape libraries to the new iSCSI target. Click the *Assign* icon. Select available libraries to assign.
- On the client side, to discover assigned devices, run the IPL I/O processor option to send a login request. You can run the IPL using a SQL command or the Start System Service Tools command (STRSST):

  SQL Command

    - Run the SQL command with the IPL I/O processor option:
      `CALL QSYS2.CHANGE_IOP(IOP=>'ISCSI', OPTION=>'IPL');`

  STRSST Command

    - Run `STRSST` on the client to check the system bus resource and execute a bus reset to the iSCSI bus resource:

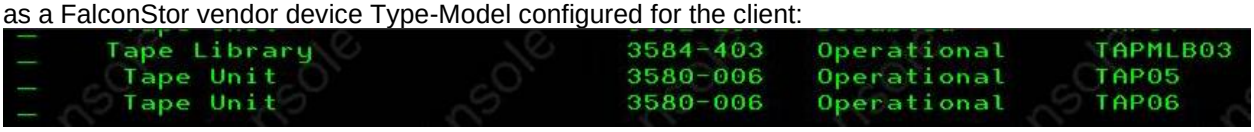
I/O debug to 298A-001 IOP resource (option 6):

Run the IPL I/O processor option that will send a login request from the client iSCSI initiator to the StorSafe server with a nonexistent target:

If everything is successful, the StorSafe server receives the iSCSI login request with the following sample messages in the system log:

```
May 30 14:34:23 h21-47 fsiscsid[9033]: IPSTOR||1653892463||I||0x0000c351||Login
to the target %1 from the initiator %2||iqn.2000-03.com.falconstor:h21-
47.ibmi94||iqn.1994-05.com.ibm:apacibmi74falcon
May 30 14:34:23 h21-47 kernel: FSISCSI client 14 initiator iqn.1994-
05.com.ibm:apacibmi74falcon type 2 login request to target iqn.2000-
03.com.falconstor:h21-47.ibmi94 from 172.24.2.94, conn 4020293, new tcp session
May 30 14:34:23 h21-47 kernel: FSISCSI conn 4020293 create new session 62603.
May 30 14:34:24 h21-47 kernel: svdp_get_cpu: vdev 536 cpu 31.
May 30 14:34:24 h21-47 kernel: svdp_get_cpu: vdev 537 cpu 32.
May 30 14:34:25 h21-47 kernel: svdp_get_cpu: vdev 538 cpu 33.
May 30 14:34:25 h21-47 kernel: [vtl_tde_537|4018142] TLE_INFO: VDrive 537
bPowerOnReset is set to 1, CDB[0]=0h vtape=-1 [n/a]
May 30 14:34:25 h21-47 kernel: IOCORE1 [kworker/31:1|3523459] release_vdev,
releasing vdev 536 without a reservation
May 30 14:34:26 h21-47 kernel: [vtl_tde_538|4018147] TLE_INFO: VDrive 538
bPowerOnReset is set to 1, CDB[0]=0h vtape=-1 [n/a]
```

- Confirm the iSCSI device is now available to the client. For example, the 3584-403 is displayed as a FalconStor vendor device Type-Model configured for the client:



- Select the *Deduplication* tab to use the default deduplication policy or create a new policy. For a new policy, enter a name and select the *Inline* deduplication trigger. Leave default priority and retry settings.
- If applicable, on the primary StorSafe server, designate the replica server as the target server and create deduplication/replication policies.
- On the IBM i host client, start your backup software to write data on virtual tapes.

Configure an iSCSI client

This section provides an example of configuring an IBM i host client with StorSafe via iSCSI. You need to create a power server running IBM I and install IBM iSCSI packages and required PTF files on that server.

One iSCSI target is created in StorSafe for each iSCSI client initiator. The StorSafe PowerVS instance is running Ethernet under an IBM Cloud private network that belongs to a VLAN subnet; no extra VLAN is set on the StorSafe server.

Check Type-Model

Confirm the IBM PTF is installed on the client by checking the *Type-Model,* which should display as `298A-001`. This indicates that the iSCSI bus IOP resource is operational on the client. If it does not exist, contact IBM to install the required PTF file.

Create an iSCSI target

For IBM i version 7.3 or higher, use the IBM Navigator for i GUI to create an iSCSI target. Select *System Services –> iSCSI* Tab *–> Action –> Create iSCSI Target –>* Enter target iSCSI Qualified Name (IQN), target IP address, or hostname.

For older IBM i versions, use the SQL service commands as described below.

SQL commands

1. Confirm the SQL service is operational by running the run `STRSQL` command. This service is used for configuring communication between the client iSCSI initiator and StorSafe iSCSI target.

2. Run the SQL command to add the iSCSI target and the initiator information on the client; you can set the target to any value matching IQN patterns, for example:

```
CALL QSYS2.ADD_ISCSI_TARGET(
TARGET_NAME=>'iqn.2000-03.com.falconstor:h21-47.ibmi94',
TARGET_HOST_NAME=>'172.22.21.47',
INITIATOR_NAME=>'iqn.1994-05.com.ibm:apacibmi74falcon');
```

   The iSCSI target name does not exist on StorSafe yet. After the SQL command completes, you will use the same target name on StorSafe, when configuring the iSCSI client.

3. Run the SQL command with the IPL I/O processor option that will send a login request from the client iSCSI initiator to the StorSafe server with a nonexistent target:
   ```
   CALL QSYS2.CHANGE_IOP(IOP=>'ISCSI', OPTION=>'IPL');
   ```
4. Confirm the IPL I/O processor successfully completes by checking the StorSafe system log, `/var/log/messages`. Make a note of the target name in the log; you will need to use it when configuring the iSCSI target in StorSight. You will see a message similar to the following:
   ```
   May 30 14:31:36 h21-47 fsiscsid[9033]:
   IPSTOR||1653892296||E||0x0000c352||Login request to nonexistent target %1
   from initiator %2||iqn.2000-03.com.falconstor:h21-47.ibmi94 (ip
   172.22.21.47)||iqn.1994-05.com.ibm:apacibmi74falcon
   ```

Add Server Resources

This section describes the configuration changes you can make to add system resources to an operational StorSafe server.

Add block storage

Follow the steps below if you need to attach additional block storage to a StorSafe server:

1. From the IBM Cloud portal, select your power system from the *Resource list -> Services and software* menu.
2. Click *Virtual Appliances* and select your instance.
3. Click *Create volume* for a new volume or click *Attach volume* for an existing volume.
4. Set values for related parameters.
5. Acknowledge and submit changes.
6. From the StorSight portal, select *Rescan* on the *Physical Devices* tab to detect new devices.

Expand object storage for the deduplication repository

Follow the steps below if you need to increase the size of COS for deduplication repository data:

1. Complete the FalconStor online form at http://ibmexpansion.falconstor.com/ to get a new license keycode for the new required space.
2. From the IBM Cloud portal, select your power system from the *Resource list -> Services and software* menu.
3. Click *Virtual Appliances* and select your instance.
4. Click *Edit details* to increase the licensed repository capacity of object storage.
5. From the StorSight portal, select *Administration -> StorSight*. Click *License*, and the "+" icon to add your new license keycode received from FalconStor. Register your license.
6. In the *Manage* tab, click the *Settings* tab, click the *Deduplication Repository* icon, click the *Manage* icon, and select *Add Deduplication Data Storage*. Specify the expansion size of object storage in GB. You must have enough object storage capacity; the system cannot check whether there is sufficient free space.
7. Check sizing guidelines to see if you also need additional system resources, such as CPU cores, memory, or block storage. If applicable, follow related steps in this section.

Add memory

Follow the steps below if you need to change the amount of memory of a StorSafe instance. For example, when you increase the size of object storage for the deduplication repository, you may also need to increase memory to be used for deduplication.

1. From the IBM Cloud portal, select your power system from the *Resource list -> Services and software* menu.
2. Click *Virtual Appliances* and select your instance.
3. Stop StorSafe services and shut down the instance.
4. Click *Edit details* to enter a new value for memory.
   For details, refer to the following IBM document "Modifying a Power Systems Virtual Server instance" https://cloud.ibm.com/docs/power-iaas?topic=power-iaas-modifying-server.
5. Power on the instance and restart StorSafe services for the changes to take effect.

Add CPU

Follow the steps below if you need to change the number of CPU cores of a StorSafe instance. For example, when you increase the size of object storage for the deduplication repository, you may also need to increase the number of CPU cores.

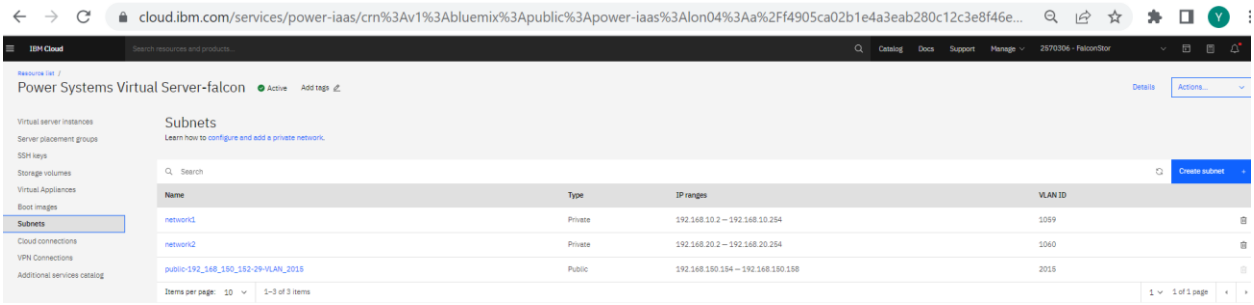
1. From the IBM Cloud portal, select your power system from the *Resource list -> Services and software* menu.
2. Click *Virtual Appliances* and select your instance.
3. Make sure it is in an *Active* or *Stopped* state, and click *Edit details* to enter new values for CPU cores.
   For details, refer to the following IBM document “Modifying a Power Systems Virtual Server instance” https://cloud.ibm.com/docs/power-iaas?topic=power-iaas-modifying-server
4. Restart the StorSafe services for the changes to take effect.

Add network

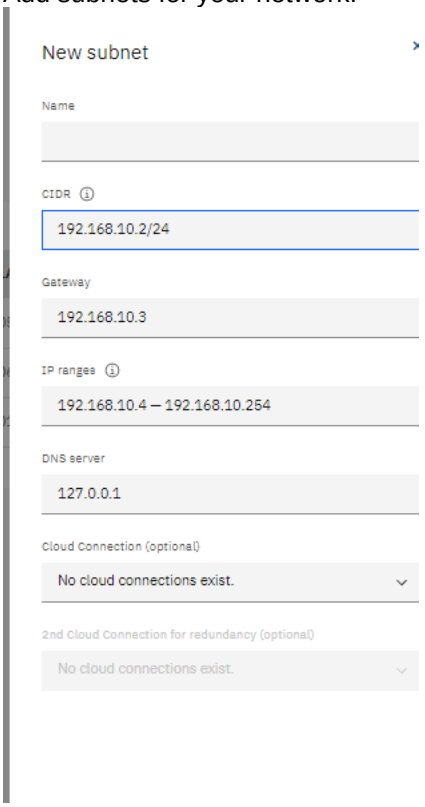
Private network

Follow the steps below if you need to add a private network interface to a StorSafe instance:

1. From the IBM Cloud portal, select your power system from the *Resource list -> Services and software* menu.
2. Select *Subnets* and click *Create subnet*.

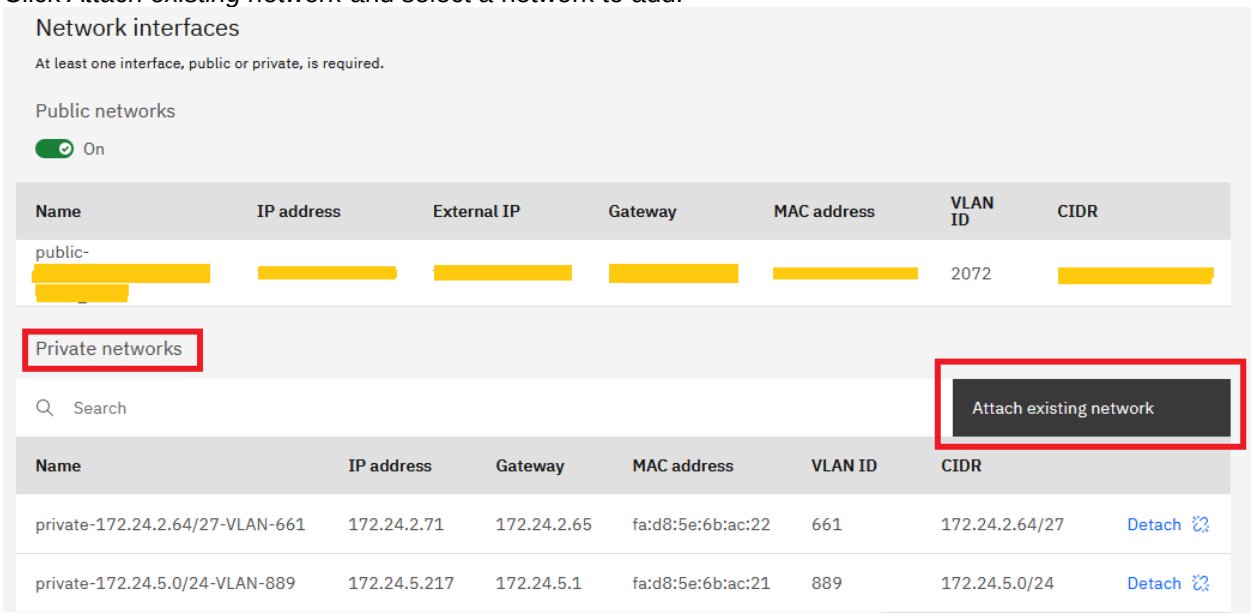


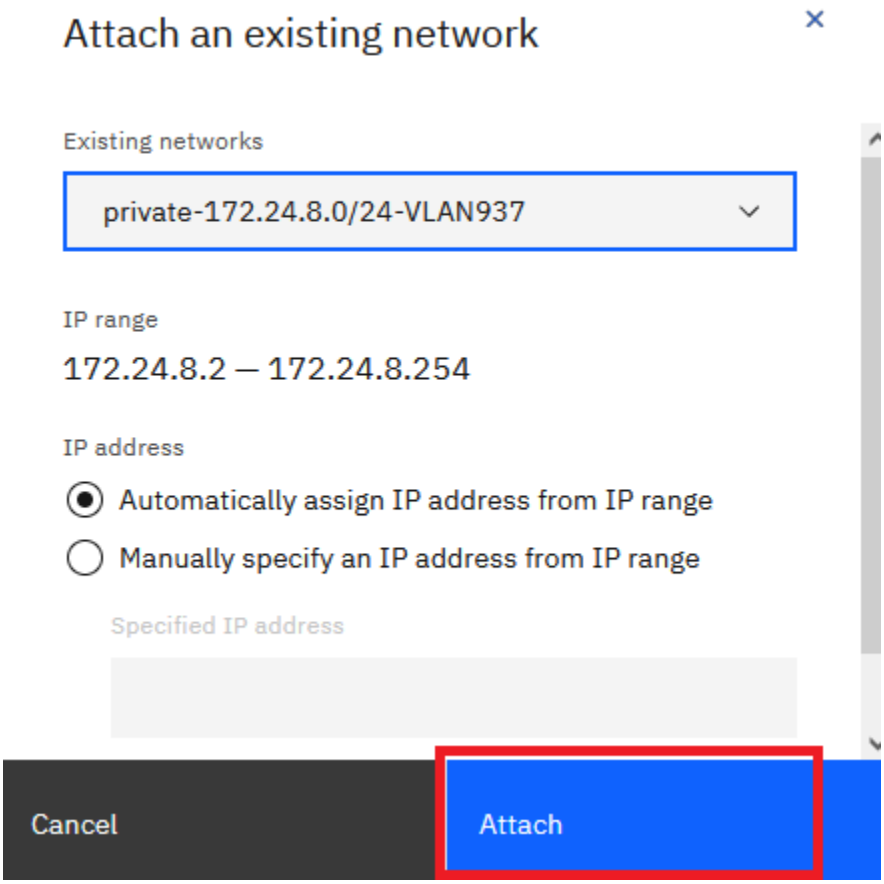
3. Add subnets for your network.



4. Select your Power StorSafe instance.
5. Stop StorSafe services.

6. Click *Attach existing network* and select a network to add.





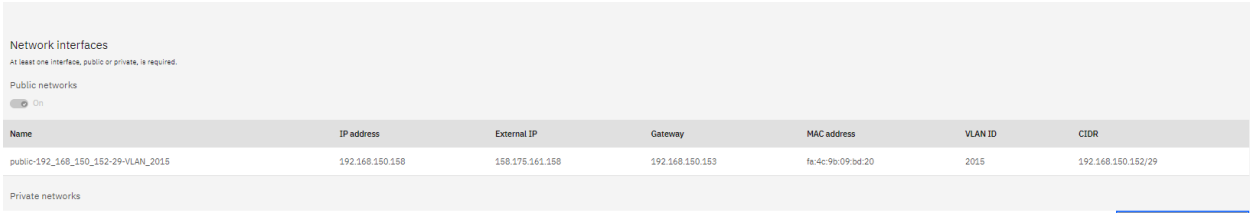
7. Make sure network routers are configured properly for the traffic in your network infrastructure.

8. Open a Linux shell on the StorSafe server and type the following commands to complete the network device configuration:
    a. # `systemctl restart NetworkManager` (to restart the network)
    b. # `ls /sys/class/net` (to see the new interface device `eth`*n*, for example eth3)
    c. # `cat /sys/class/net/eth`*3*`/address` (to get the HW MAC address of the new network device)
    d. # `cd /etc/sysconfig/network-scripts`
    # `cp ifcfg-eth0 ifcfg-eth3` (to copy one network file, for example, ifcfg-eth0, to the new one, for example ifcfg-eth3)
    e. # `vi ifcfg-eth3` (to set related parameters for the new interface file, such as the following)
        i. DEVICE=eth3
        ii. HWADDR=
        iii. IPADDR=
        iv. NETMASK=

Public network

You can have only one public network. Follow the steps below if you need to add a public IP address for a StorSafe instance:

1. From the IBM Cloud portal, select your power system from the *Resource list -> Services and software* menu.
2. Click *Virtual Appliances* and select your instance.
3. Check the *Public networks* box.



Network considerations

1. You can only disable a public IP address while deduplication has not been enabled on the StorSafe server. After disabling the public IP address, you must restart StorSafe services. If deduplication is already enabled while the public interface is in effect, contact FalconStor Technical Support for help.
2. If you need to remove any network interfaces on the StorSafe server, contact FalconStor Technical Support for help.

APPENDIX 1 -

Measures for Security Threats

This section describes the security policy implemented for the underlying operating system (OS) and FalconStor StorSafe software product.

OS packaging

The FalconStor software image contains a scaled down version of the Linux operating system, which contains only required packages. Only a subset of Linux support modules is included, to keep unneeded services from being available for malicious entry points. The hardening of OS packaging is a controlled process and does not use an automated update program such as `yum` in order to avoid adding or updating unnecessary files. At each product release, FalconStor makes sure the OS packages in the product USB image are up-to-date and do not contain any security vulnerabilities. If any major vulnerability is fixed in newer minor versions of the kernel used in the current USB, the USB kernel is also updated to that newer version. FalconStor will perform tests to ensure OS patches do not cause any issue to the software.

FalconStor regularly checks for vulnerabilities using the using the following methods:

- Vulnerability updates/newsletters from the Red Hat Security Response Team and Red Hat General Advisories web page for upcoming OS updates
- Security Content Automation Protocol (SCAP) reports
- Reports from vulnerability scanners such as Nessus® by Tenable Network Security from customers. FalconStor focuses on the ‘High’ and ‘Medium’ reported vulnerabilities to evaluate whether an OS patch is needed.

OS security options

The following security options are enabled during installation:

- OS (`Grand Unified Bootloader`) GRUB security features allow setting a password so users cannot edit any grub entries or pass arguments to the kernel from the grub command line without entering the password.
- The Linux Audit framework can log system calls, such as, opening a file, killing a process, or creating a network connection. These audit logs can be used to monitor systems for suspicious activity.
- The Linux Advanced Intrusion Detection Environment (AIDE) can be configured with predefined rules to check the integrity of files and directories in the Linux operating system.
- The OpenSCAP scanner packages are included for the Security Content Automation Protocol (SCAP). SCAP content is based on the Security Technical Implementation Guide (STIG) published by the Department of Defense Cyber Exchange (DoD), which is sponsored by the Defense Information Systems Agency (DISA). It contains guidance on how to configure systems to defend against potential threats. The OpenSCAP scanner can be regularly run in order to apply required fixes and bring the system to a compliant state.

Authentication

The following measures are taken in order to maintain a high level of security among services for authentication:

- Linux secure login with shadow passwords is used to access the server terminal console.
- Remote SSH access is disabled for the 'root' account on all StorSafe servers.
- A shared secret mechanism based on the Diffie-Hellman algorithm is used for authentication between:
    - Source and replica servers
    - Management portal and server
    - Host clients and server

The Diffie-Hellman key exchange sets a shared secret of 48 bytes between primary and target components. When a communication session starts, the primary authenticates itself with the target and generates two symmetric keys following the TLS 1.2 standard, one for sending and one for receiving data.

- The FalconStor StorSafe NAS feature provides two security modes to authenticate users/groups trying to access NAS shares:
    - Domain mode, where authentication is controlled by a Windows Active Directory Domain Controller; POSIX Access Control Lists (ACLs) can be set on files and folders.
    - User mode, where authentication is controlled by passwords that are set for each Windows user.
- FalconStor StorSight uses the Spring framework, where the security module is a flexible and powerful authentication and access control framework to secure Spring-based Java web applications.
- FalconStor StorSight offers the option to use an Active Directory or LDAP server for authenticating and authorizing users.
- FalconStor StorSight offers the Multi-Factor Authentication (MFA) option. MFA is a multi-step account login process that requires users to enter more information than just a password. Along with the password, users will be asked to enter a verification code sent to their email in order to validate their identity.

Communication

The following measures are taken in order to maintain a high level of security for communication between software modules:

- Most of the standard communication ports are disabled and only those required for FalconStor software are left open. Although you may temporarily open some ports during initial setup of the FalconStor appliance, such as the telnet port (23) and FTP ports (20 and 21), you should shut them down after your work is complete.
- Non-standard dedicated communication ports are used by the software modules for internal communication. The list of used ports is available in an appendix in the user guide.
- The management portal and host clients use a secured RPC link to communicate with FalconStor servers.
- The web-based StorSight GUI can use an SSL certificate for secure https communication with the StorSight management module.

Encryption

Replication traffic

Encryption provides an additional layer of security during replication by securing data transmission over open, public networks. Initial key distribution is accomplished using the authenticated Diffie-Hellman exchange protocol. Subsequent session keys are derived from the master shared secret, making it very secure. The available replication encryption methods are ARC4 (128-bit), AES (128-bit), and AES (256-bit).

128-bit ARC4 stream cipher usage is fully licensed by the U.S. government for export to countries outside of North America, other than specifically restricted areas.

AES encryption is compliant with Federal Information Processing Standard (FIPS) 140-2; all cryptographic code/algorithms are located in a single FIPS 140-2 compliant software module.

iSCSI traffic

The Mutual CHAP level of security allows the target and the initiator to authenticate to each other. A separate secret is set for each target and for each initiator in the storage area network (SAN).

Strong password management

The system checks whether the password meets the following complexity requirements in the default configuration:

- The password contains at least 14 characters
- The password meets at least two of the following conditions:
  - Contains at least one lower-case letter
  - Contains at least one upper-case letter
  - Contains at least one digit
  - Contains at least one space or one of the following special characters:
  - [mailto:~!@#$%^&*()-_=+\|[{}];:'",<.>/]~!@#$%^&*()-_=+\|[{}];:'",<.>/?
- The password is not the same as the account or its reverse order.
- There are at least 5 different characters between an old and new password.

The system provides one of the following mechanisms for locking user accounts:

- The system locks the account if the user enters a wrong password for a number of times more than the threshold specified during product configuration; the default value is three times.
- The system allows setting the account locking duration for user accounts locked due to more than *n* login attempts with wrong passwords. The recommended locking duration is five minutes.
- When the account locking duration elapses, the account is unlocked automatically. The security administrator can also unlock the user accounts manually.
- When an account is locked, only the security administrator can unlock the account manually.

Password encryption rules are as follows:

- Passwords are encrypted with AES 256.
- The password must be entered in encrypted text. That is, the entered password is presented by asterisks * on the user interface. The password cannot be displayed in plain text in terminals or logs.
- A password without encryption in memory (for example, at login) must be overwritten right after being used.
- The password cannot be saved in log files, configuration files, cookies, or buffers without encryption.

- Access control is implemented for password files and common users cannot read or copy the encrypted content.
- A password in a text box cannot be copied.
- The old password is required for a password change.
- Users (except for administrators) cannot change the passwords of other user accounts.
- GUI console login authentication uses SHA 512.

SNMP traffic

SNMP user authentication uses the MD5 or SHA algorithm.

SNMP data traffic uses AES or DES for encryption of data sent over the network. A passphrase (8-127 characters) is used.

Data security

Data encryption

Encryption can be enabled for:

- Virtual libraries to encrypt virtual tape data using an encryption key defined by the user
- Migrating tape data to an object storage account in-flight and at-rest (end-to-end) using an encryption key obtained for each tape from the Network Security Service (NSS) internal key management system
- Deduplication repository using an internal encryption key

Data structure

All data are stored as disaggregated without a file system construct; data layout is not discoverable outside the FalconStor server or across user accounts to provide the first “air-gap” security layer.

WORM tapes

On a virtual tape library or drive, the Write-Once-Read-Many (WORM) property can be enabled for tapes that support ULTRIUM5 media type and above. WORM tapes cannot be overwritten. WORM allows non-rewriteable and non-erasable data to be written and provides extra data security by prohibiting accidental data erasure. Since tapes are written once, they cannot be altered or overwritten by some virus/ransomware/other malicious software.

Immutable Cloud Object Storage

The immutable option can be enabled for tape migration to IBM Cloud Object Storage (COS). Immutable object storage locks data to provide a safe backup and to maintain data integrity. You can enable an object lock at the bucket level to get secure backups and long-term data retention. Retention policies ensure that data is stored in a non-erasable and non-rewritable manner for a specified time frame. Data cannot be changed until the retention period has expired. Once the retention period is over, data can be unlocked for further actions, according to your company policies.

From the IBM COS management GUI, you can configure the retention policy of your bucket and set the minimum and default values to zero, and the maximum retention period to the number of days you want to lock the bucket data.

From the FalconStor portal, you can set a tape migration policy for a virtual tape library or drive. At the end of each backup job, the tape is ejected to the vault, where the tape data gets packaged and migrated to the object storage of a cloud provider.

This copy of data remains intact during the retention period and is protected from malicious activity or accidental deletion.

Tape shredding

Just as deleting a file from your hard drive does not completely destroy the file, deleting a virtual tape does not completely destroy the data on the tape. If you want to ensure that the data is unrecoverable, you must shred the tape. Shredding a virtual tape destroys all data on the tape, making it impossible to recover the data. Tape shredding uses a military standard to destroy data on virtual tapes by overwriting it with a random pattern of bits, rendering the data unreadable.

Data Isolation for multi-tenancy

StorSight provides a secure multi-tenant architecture that allows Managed Service Providers (MSPs) and large enterprises to offer data protection as a service to their customers, called tenants. Each tenant (a business or organization) has its own secure computing environment, called a domain (i.e., *companyA.com*). While all storage and network resources are shared among domains, StorSight logically isolates data by restricting visibility of storage resources to specific customers. Therefore, customers only see their own data and are not aware of other tenants.

The landlord in a multi-tenant environment is a Super Administrator, the master role that does not belong to any domain. By default, there is one Super Administrator account per StorSight server; however, the Super Administrator can create additional Super Administrator accounts.

The Super Administrator creates an administrator account for each company or organization, associating each tenant's domain with the account.

The Administrator for each domain then creates user accounts within their organization. Typically, the Administrator will create Administrator accounts for departments within their organization, possibly creating one Administrator for each department. Each Administrator will then create other user accounts as needed for their department.

For privacy, access to downstream storage can be isolated via storage pools, access to Fibre Channel targets via separate Fibre Channel zones, and access to networks via separate private subnets.

StorSafe Servers can be assigned to a customer domain in exclusive or shared mode:

- In exclusive mode, the server is only available to the users in that customer domain.
- In shared mode, the server is available to users of multiple customers. Data isolation among those customers is by assigning different storage pools to each single customer so they can only see resources created from storage pools assigned to them.

A hierarchy of user account types is used to control access to the system:

- **Superadmin**: A master role that does not belong to any domain with full access to StorSight who can create customer domains, add and assign StorSafe servers, virtualize physical resources, reserves resources for specific usages (configuration, tapes, deduplication, NAS), create storage pools of virtualized storage, perform global configuration and maintenance of servers, configure failover, and create the single instance deduplication repository.
- **Admin**: The administrator for a customer domain who can create User or Viewer accounts and assign these accounts to specific storage pools, virtual resources, and clients. An Administrator can also create and manage virtual resources for their domain.
  An Administrator of a server in exclusive mode has the same rights as the superadmin (root) user on the server.
- **User**: A tenant user with read-write access to resources that have been created by that user or assigned to that user by the domain admin.
- **Viewer**: A tenant user with read-only access to resources withing a domain who can view configuration and reports as well as receive alerts but cannot make any configuration changes.

Accounts with a higher or equal role can change the properties of other accounts. For example, Superadmin can change the password of other Superadmin, Admin, User, or Viewer accounts; Admin can change the password of other Admin, User, and Viewer accounts. Users and Viewers can only change their own passwords.

Event logging

- The Linux Audit framework can log system calls, such as, opening a file, killing a process or creating a network connection. These audit logs can be used to monitor systems for suspicious activity.
- The Linux Advanced Intrusion Detection Environment (AIDE) can be configured with predefined rules to check the integrity of files and directories in the Linux operating system.
- Any operation performed via the management portal or command line interface that changes the current state/configuration is recorded in the event log.
- Any user login and logout are recorded in the event log.

General Security Guidelines

FalconStor recommends the following general guidelines to ensure security:

- Place FalconStor appliances in a secure location protected by firewalls and accessible only by trusted people since these appliances are service units and not general-purpose computers.
- Do not create any shares on appliances.
- Do not install any unauthorized software.
- Do not open any unnecessary communication ports.
- Apply only OS patches certified by FalconStor.

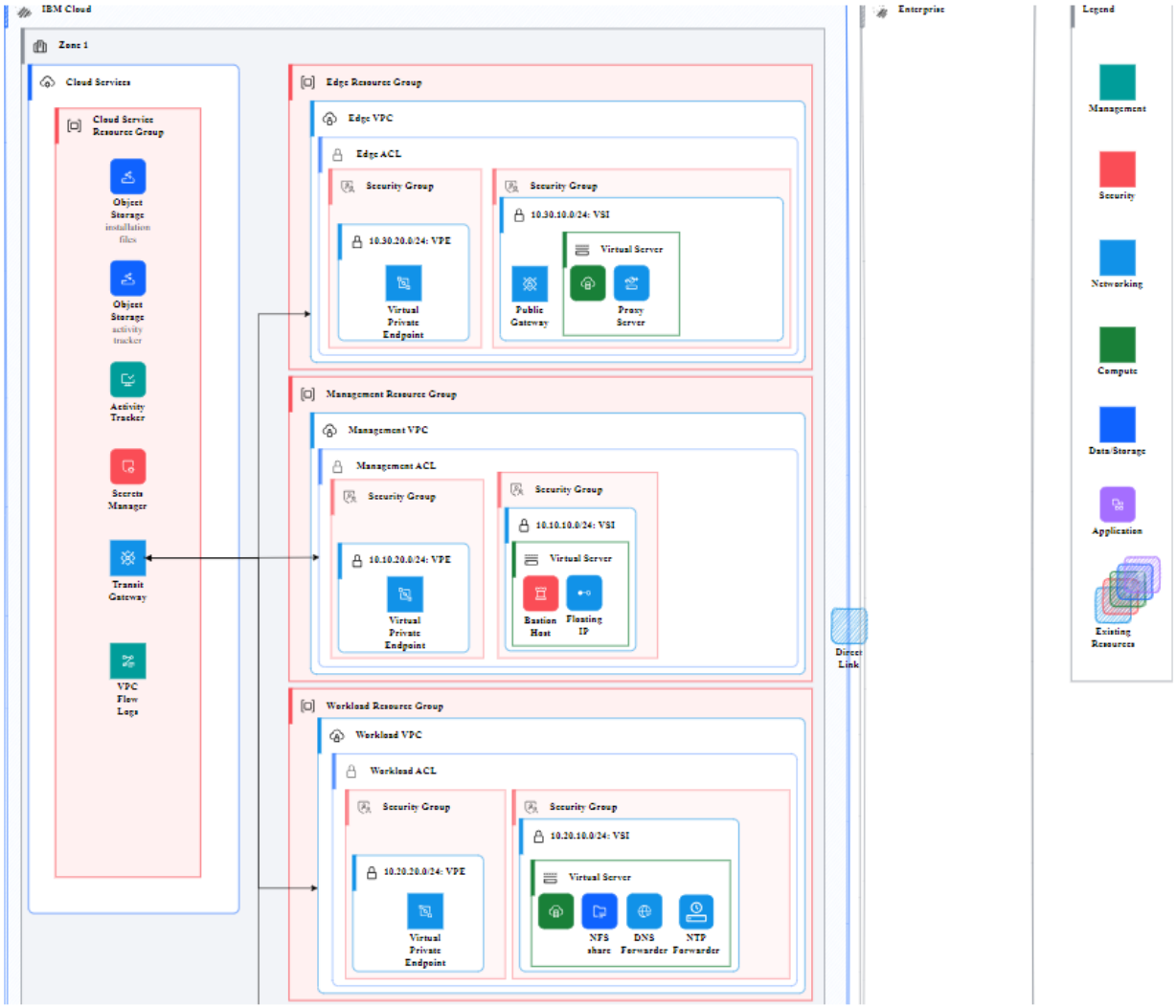
APPENDIX 2 -

IBM Deployable Architecture Workspace

This section describes the steps to use the IBM Deployable Architecture from the catalog to build a Power Systems Virtual Server (PowerVS) workspace with a Virtual Private Cloud (VPC) landing zone. Then, you can select the CRN of this workspace when you deploy a FalconStor StorSafe VTL tile.

The deployable architecture for PowerVS workspace provides:

- Three separate VPCs for service isolation
- Three Intel Virtual Server Instances (VSI) in the classic environment:
    - Server running DNS, NTP, and NFS services
    - Server running Squid proxy server to access the public Internet
    - Server with a floating IP address acting as a jump box to access other servers
- Two cloud connections for a transient gateway to access the classic environment
- Two networks, one for management and one for backup
- Two Cloud Object Storage (COS), one for management and one for workload



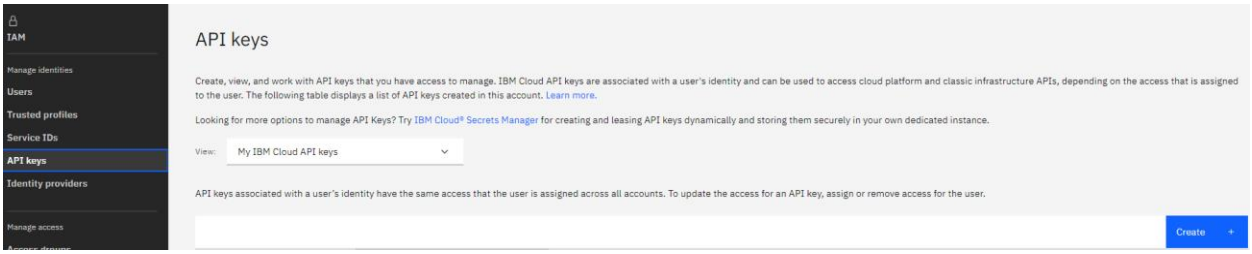
Prerequisites

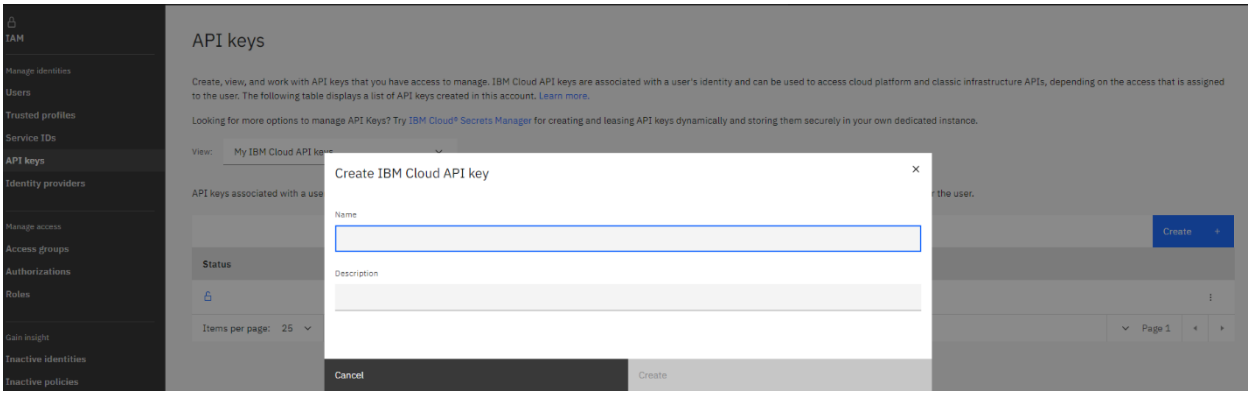
To set up a deployable architecture workspace, you will need to:

1. Create your API key.
2. Generate your SSH private and public keys on your machine that will access resources in the workspace.
3. Add IBM Secrets Manager service that will hold your keys for a centralized management.
4. Create an IBM project to manage code-based deployments across accounts, collaborate with team members, and maintain compliance.

Create your API key

Select Access (IAM) in the menu bar Manage option. Select *API keys* in the left panel, click *Create* and give a name to your key.





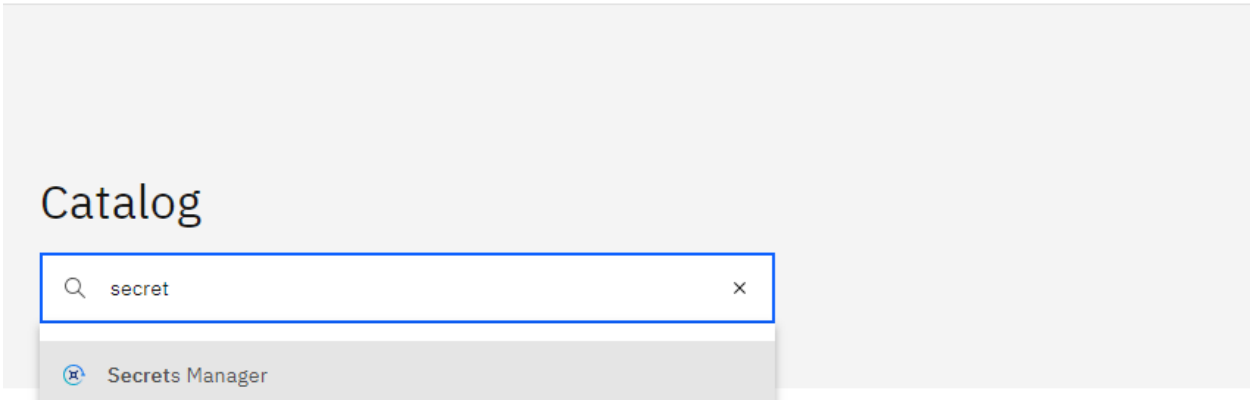
Generate your SSH keys

From the machine you want to access resources in the workspace, run the following command to generate an SSH public key in `.ssh/id_rsa.pub` and a private key in `.ssh/id_rsa`:
`ssh-keygen`

Add IBM Secrets Manager service

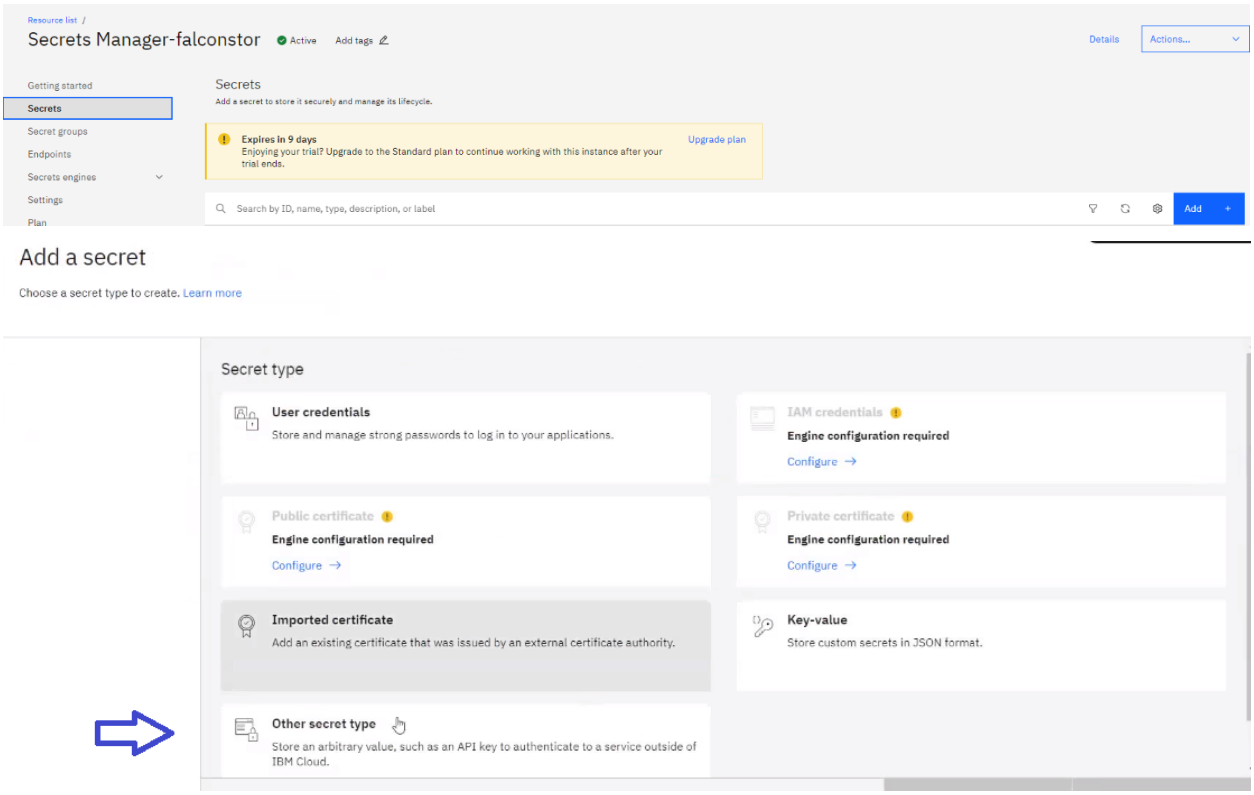
You can create one Secrets Manager service for your company or create several per tenant in a multi-tenancy environment.

In the IBM catalog, type 'secrets' and select *Secrets Manager*. You can use all default options. For clarity, create three groups for secret keys, for example, *'apikeys', 'private_ssh', 'public_ssh'*.

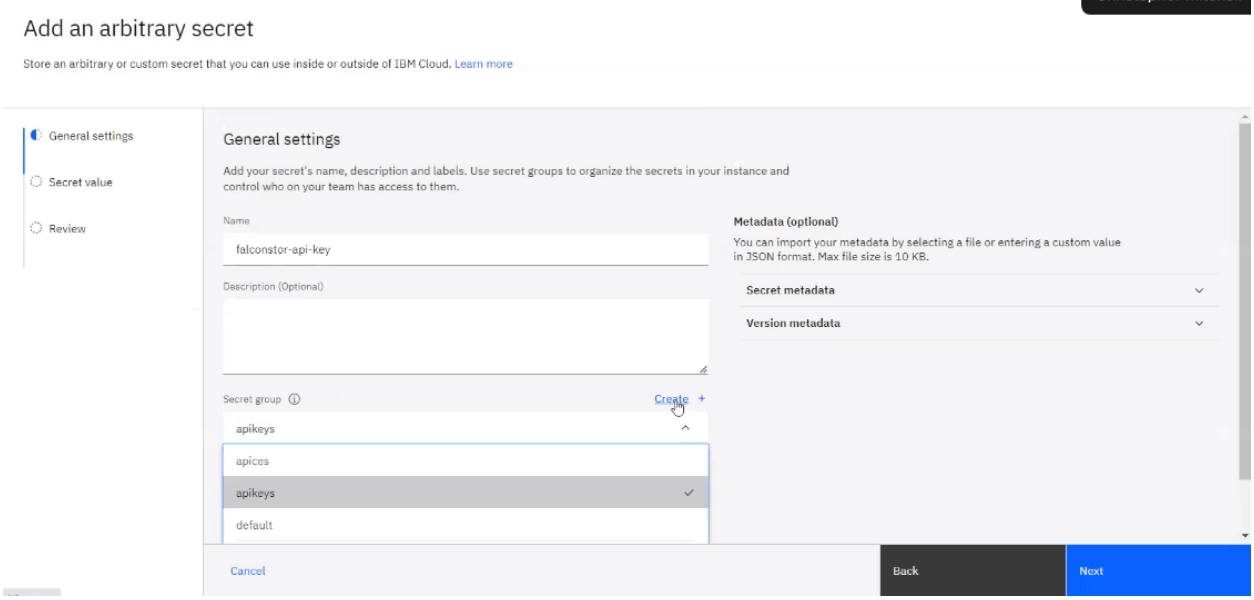


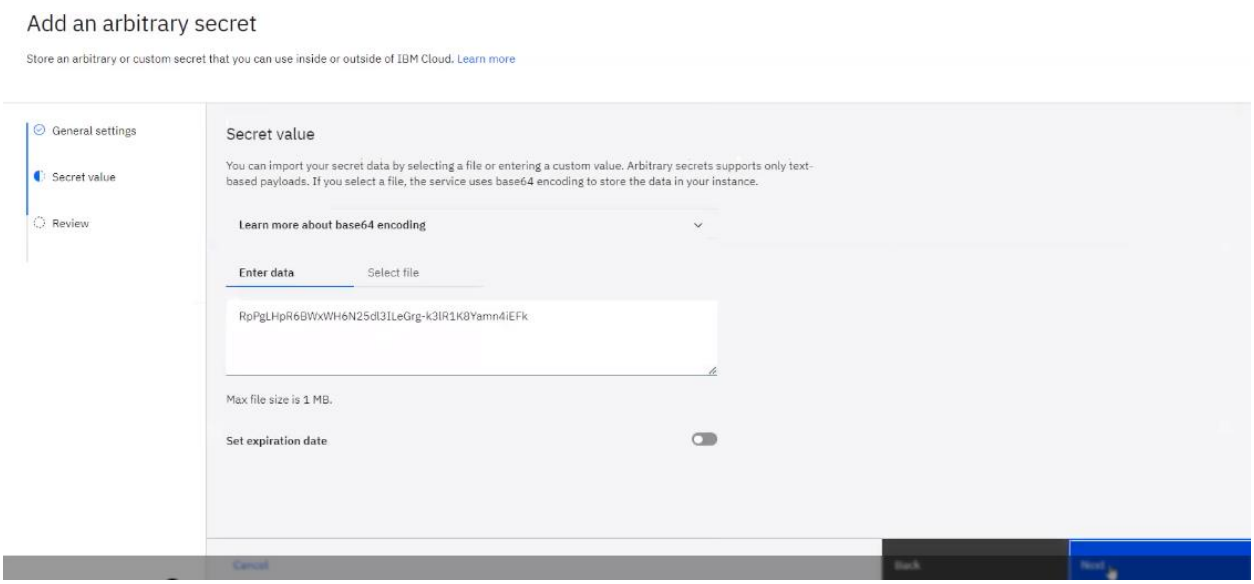
Go back to your API key and copy the key.

Select your Secrets Manager in the *Security* section of the Resource list, select *Secrets* in the left panel, and click *Add* to add your keys to the Secrets Manager. Then, select *Other secret type*.

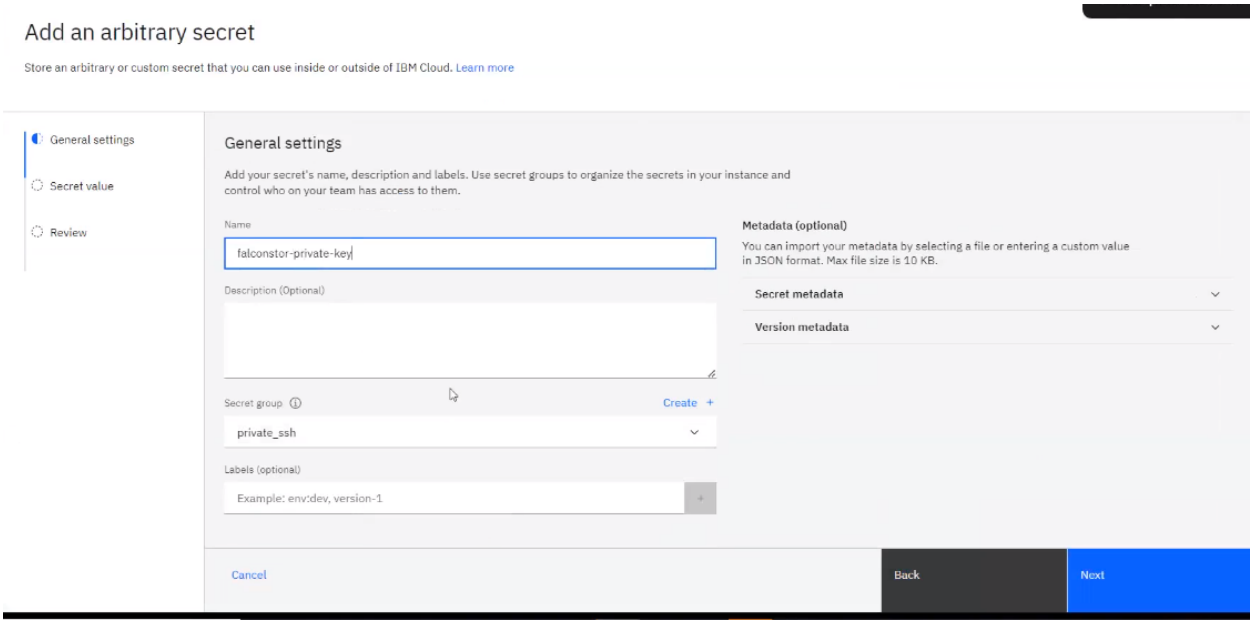


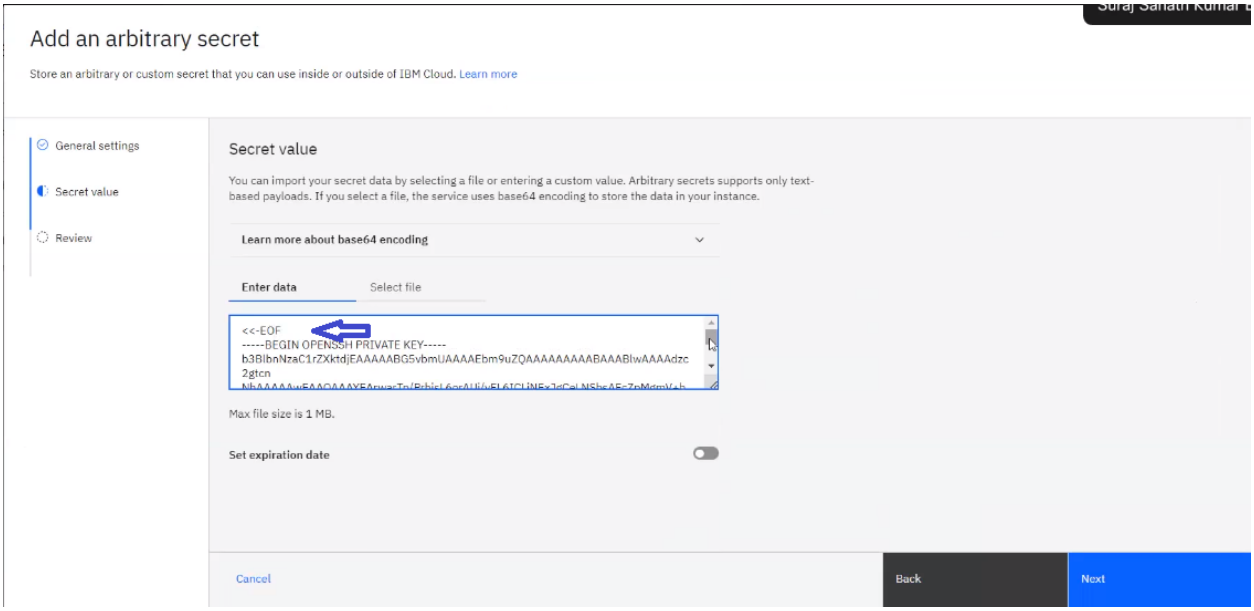
Select the *apikeys* group and paste your copied API key.

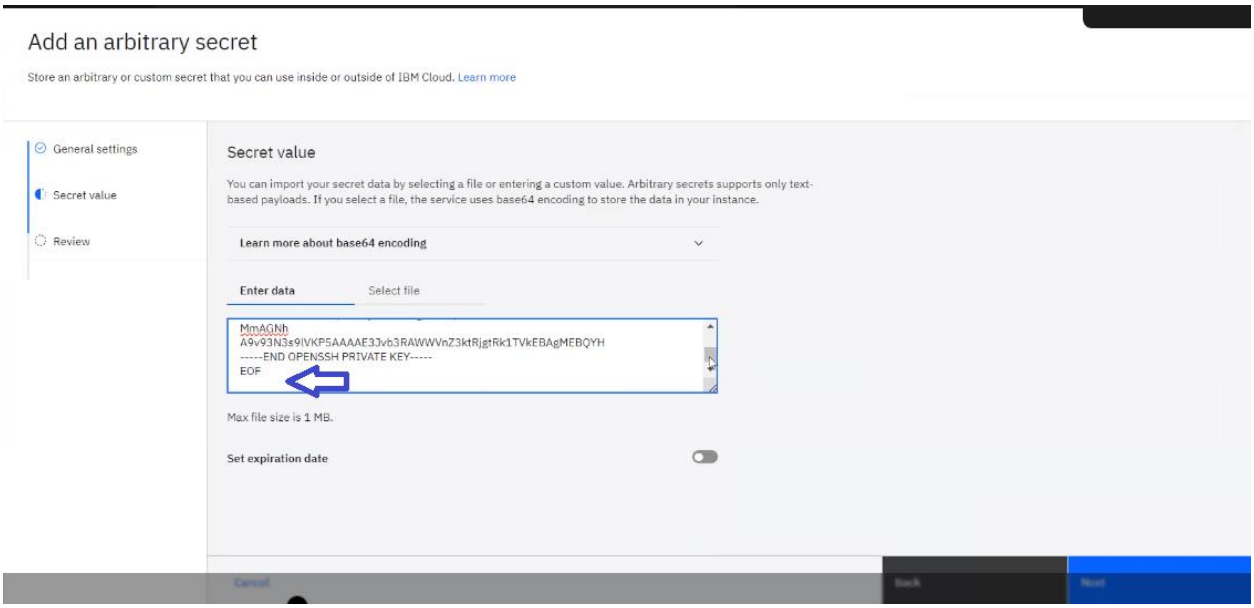




In the same way, add your SSH public and private keys. Copy contents of `.ssh/id_rsa.pub` for the public key and `.ssh/id_rsa` for the private key.
When copying the private key, you will need to enter a line on the top with `<< EOF` and a line at the end with `EOF` and a line break.

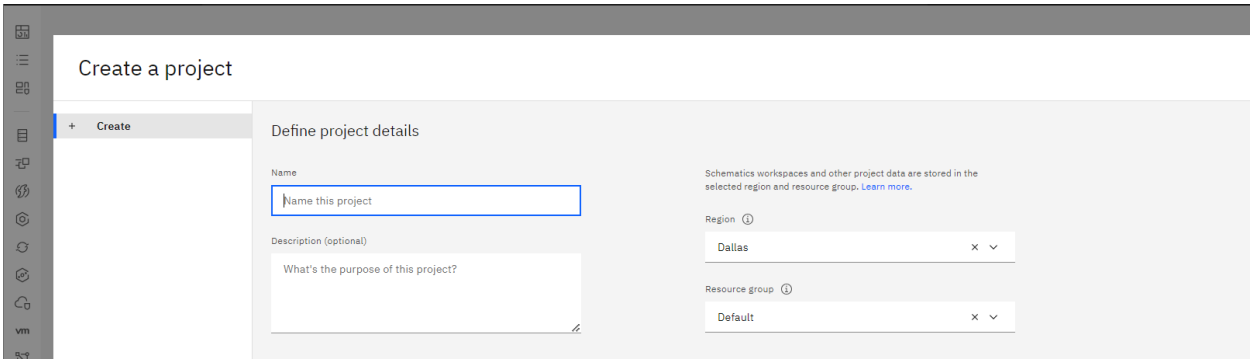






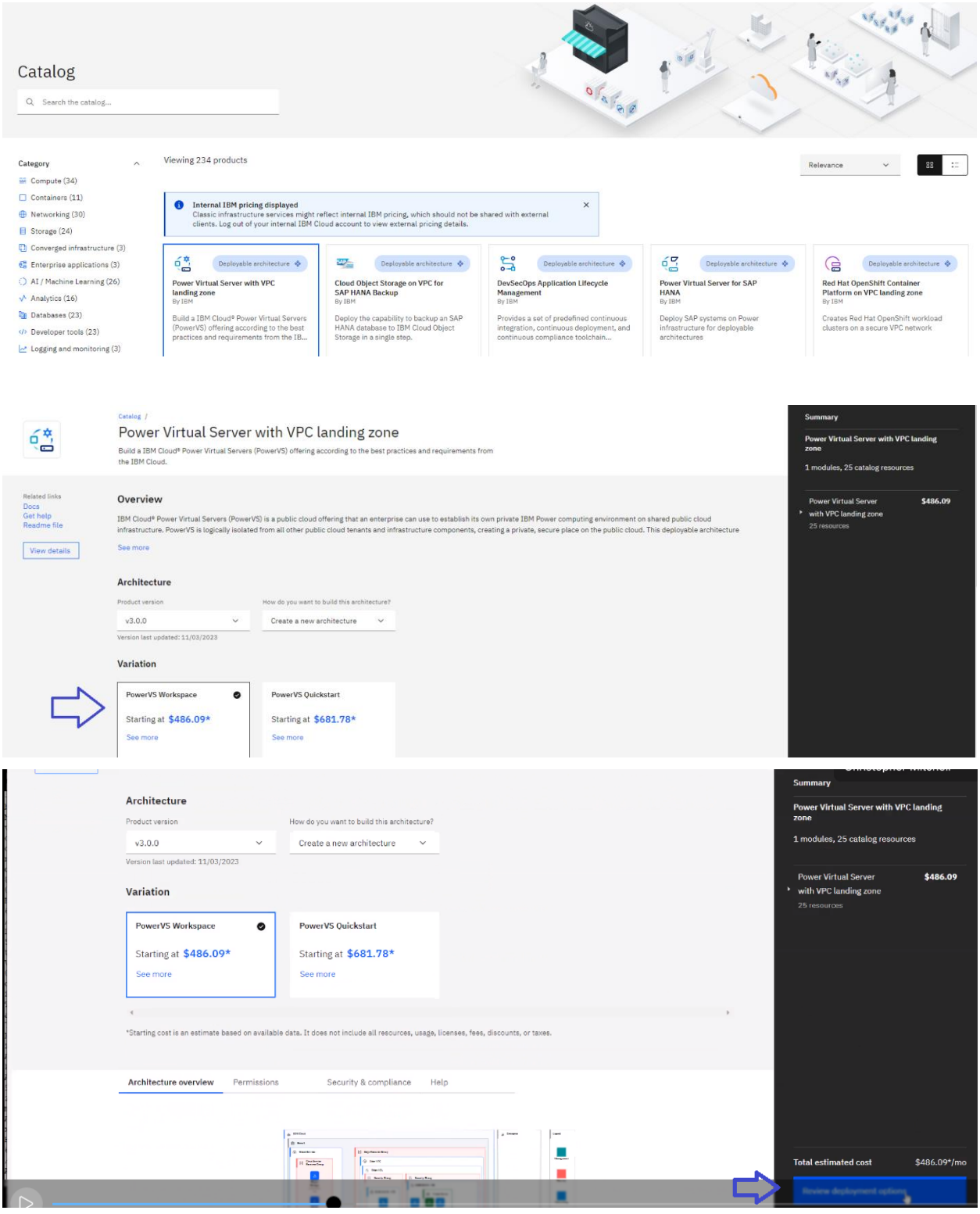
Create an IBM Project

Select *Projects* in the *Resource* list to create a project to manage your deployments across accounts.

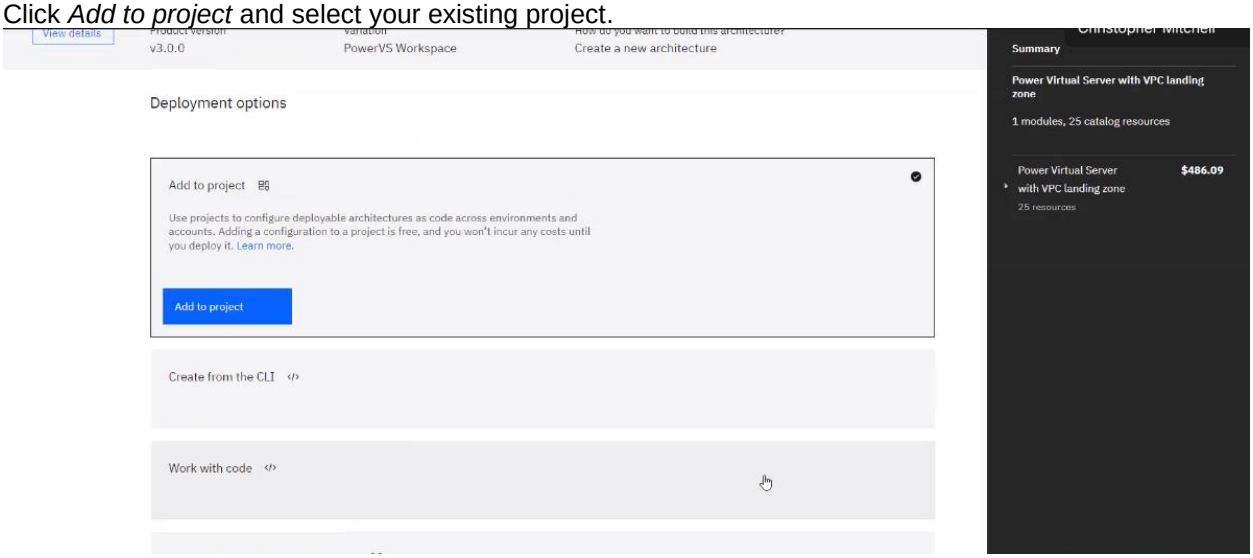


Create a Deployable Architecture workspace

From the IBM catalog, select the *Power Virtual Server with VPC landing zone* tile. Then, select the *PowerVS workspace* option. Click *Review deployment options* in the right panel.

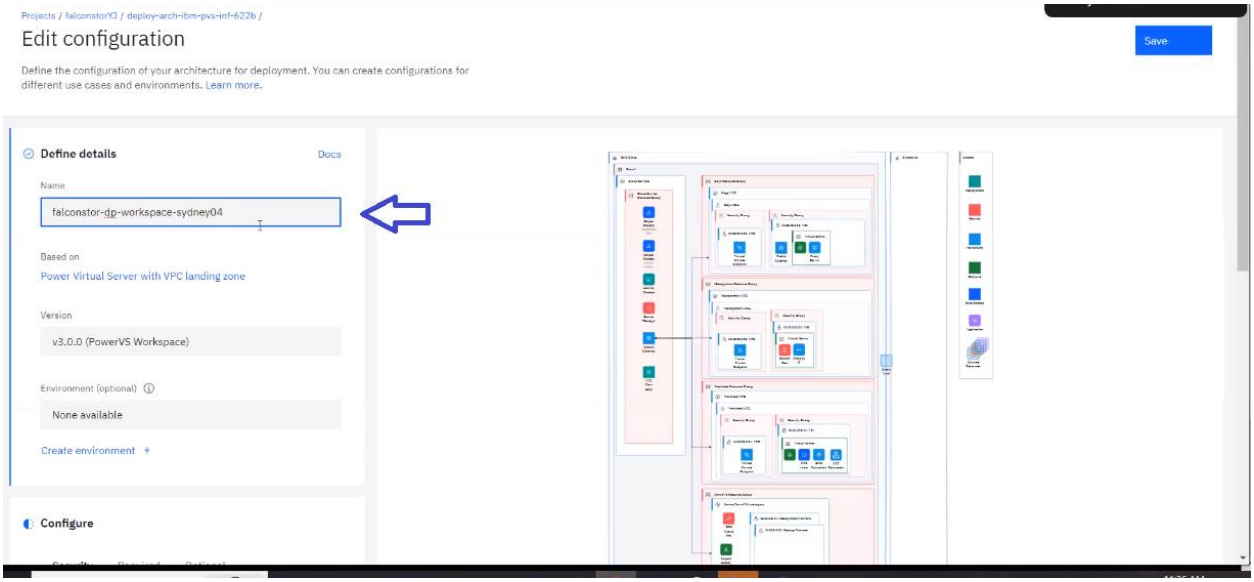


Click *Add to project* and select your existing project.

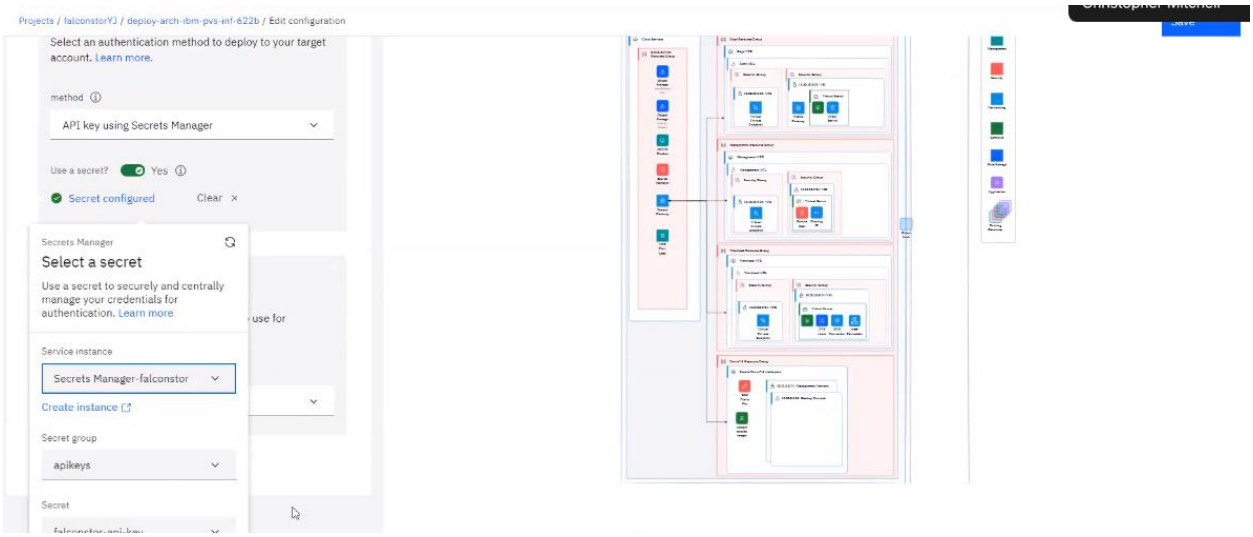


Configure this instance of the deployable architecture. Enter a name for the configuration of the deployable architecture; include the deployment site region in the name for clarification.

Note that this workspace requires two cloud connections for the transient gateway to access the classic environment. Since there is a limit of two cloud connections per data center; make sure you select a site that does not have any cloud connections, so no direct link resource is used on that site.



Scroll down to the *Security* section and select the authentication method as *API key* using the Secrets Manager. Select your Secrets Manager service and select the group of API keys, *apikeys,* in this example. Then select your API key. You need to click somewhere in the white space area to close the popup after entering keys.

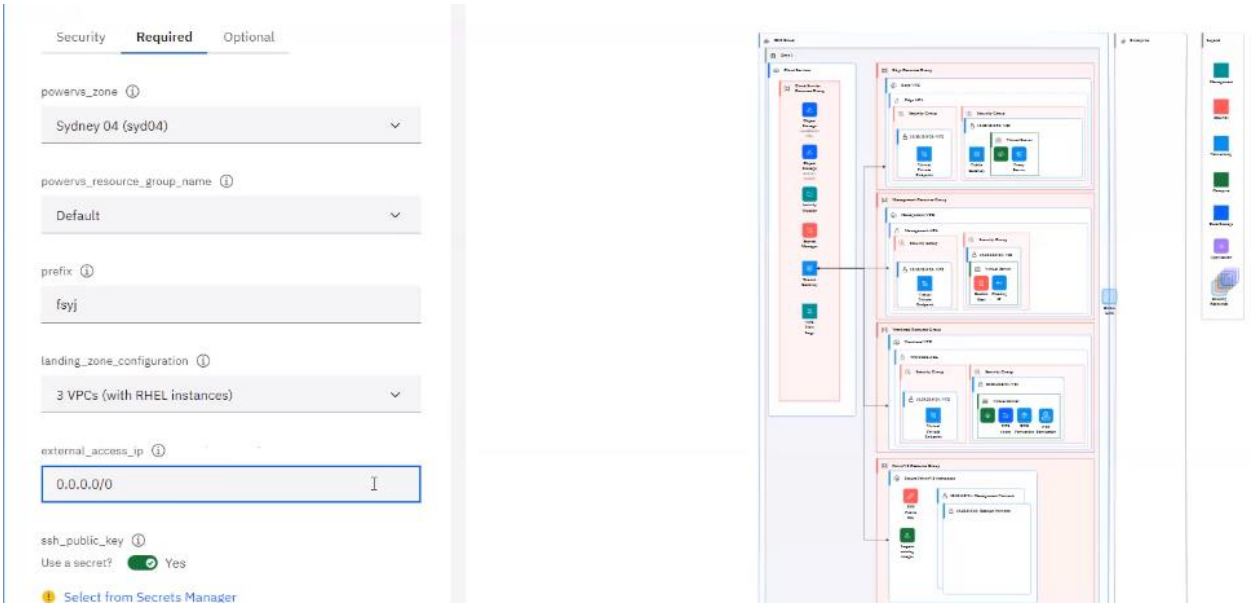


Click the *Required* tab and select a PowerVS region that does not have any cloud connections.

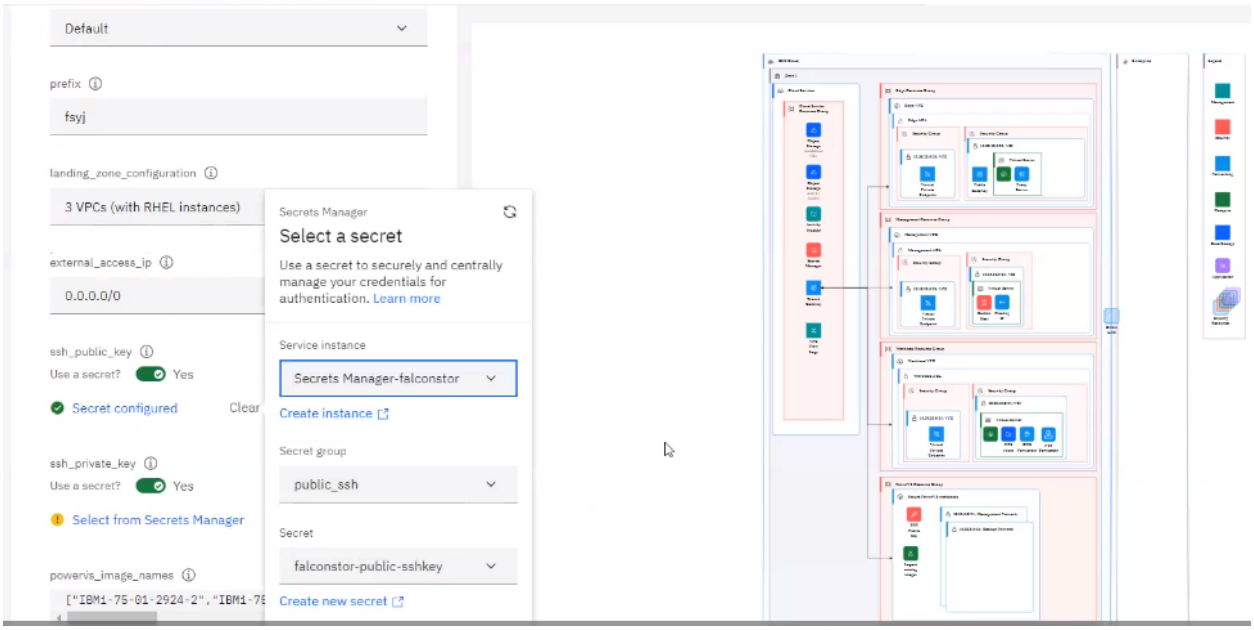
Enter a string in lowercase that will be used as a prefix for all resource names that will be created in this workspace. This allows you to easily list all these resources.

The three VSIs for DNS Server, NTP server, and NFS server can run RedHat or SUSE.

In the *external-access-ip*, enter a specific IP or a range of IP addresses that can access resources from outside. This can emulate a VPN that is not configured in the deployable architecture workspace. Enter 0.0.0.0/0 if you want all IP addresses to be able to access.

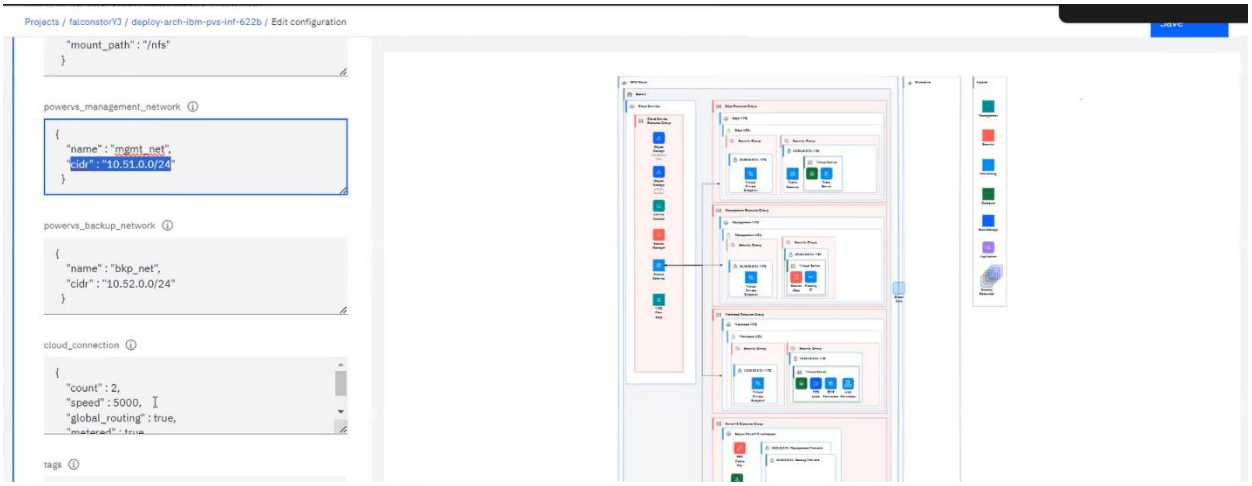


In a similar way to above, add your public and private keys.



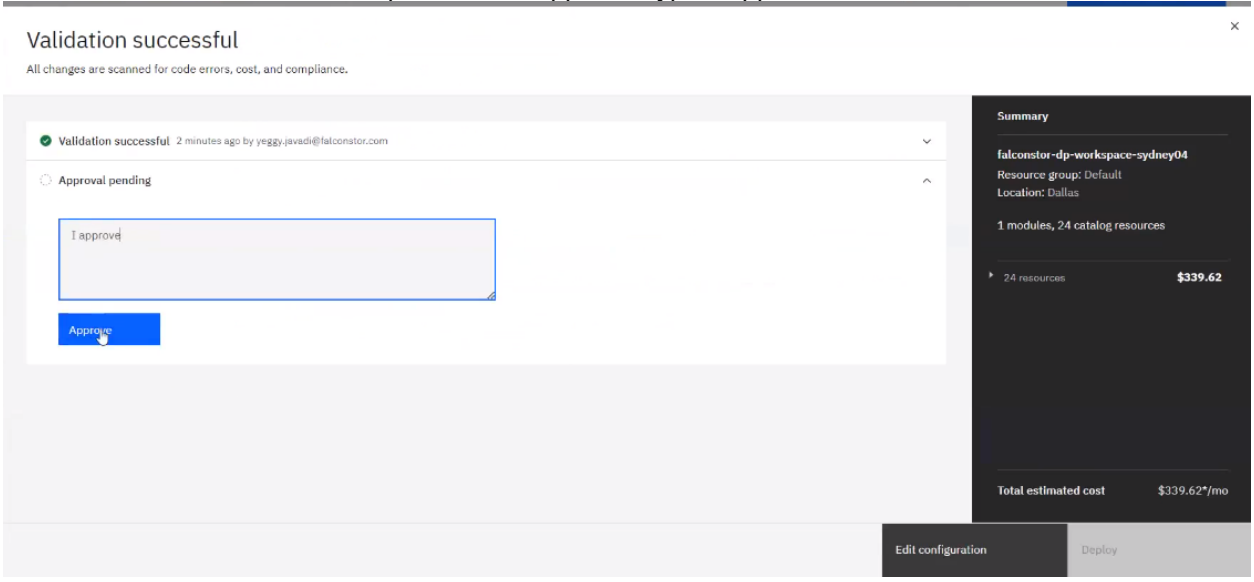
Click the *Optional* tab to review default selections.

Check your network range for the two networks that can be used for management interface and backup application servers.



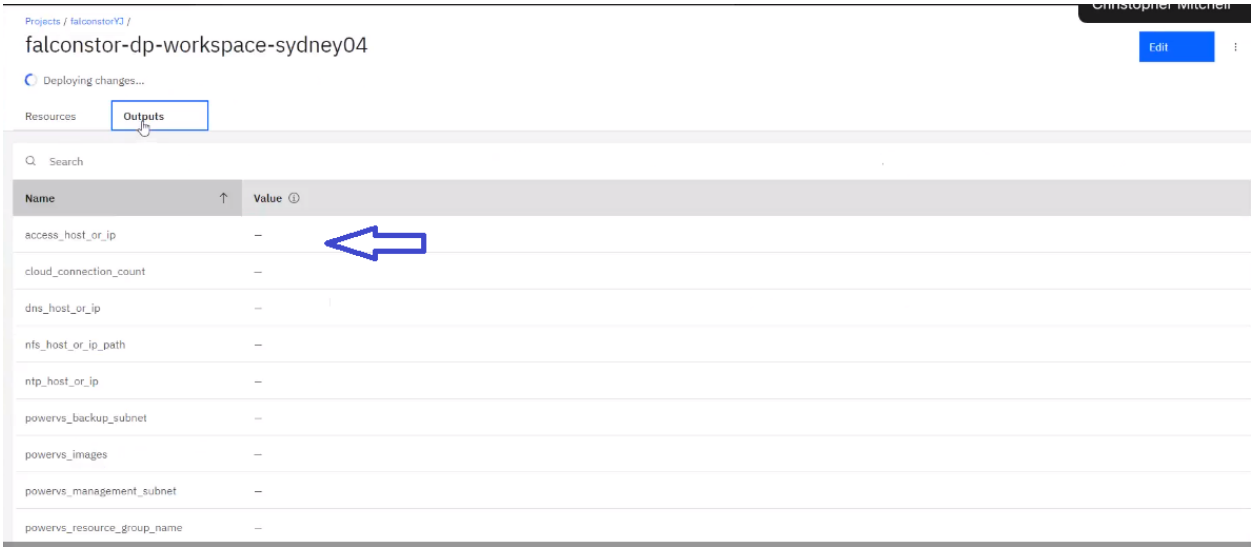
Click *Save* and then click *Validate* to start the terraform execution. It can take about 30 minutes to deploy terraform.

Once terraform execution is completed, click *Approve*, type 'I approve' and submit.

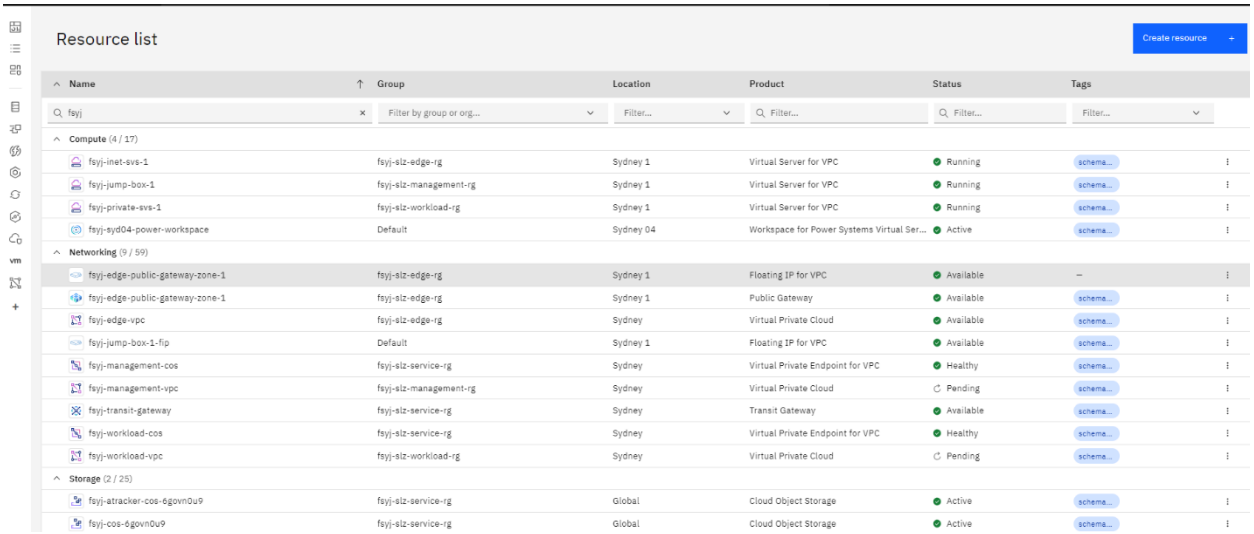


Output of Deployable architecture workspace

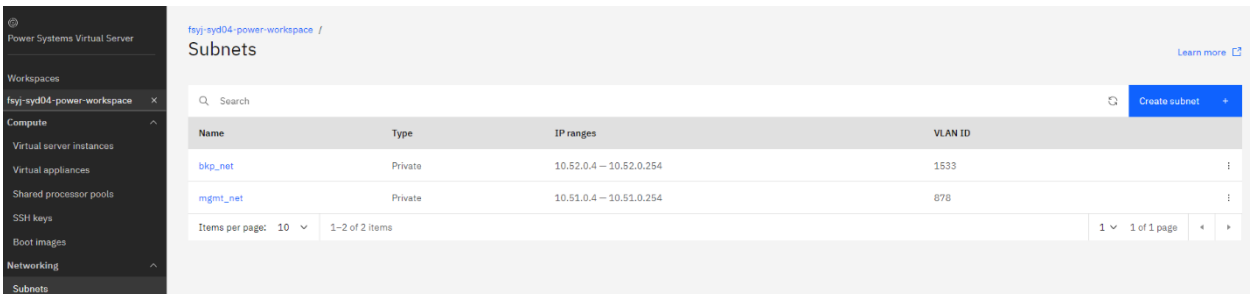
Click the deployable architecture workspace and check the results in the *Output* tab.



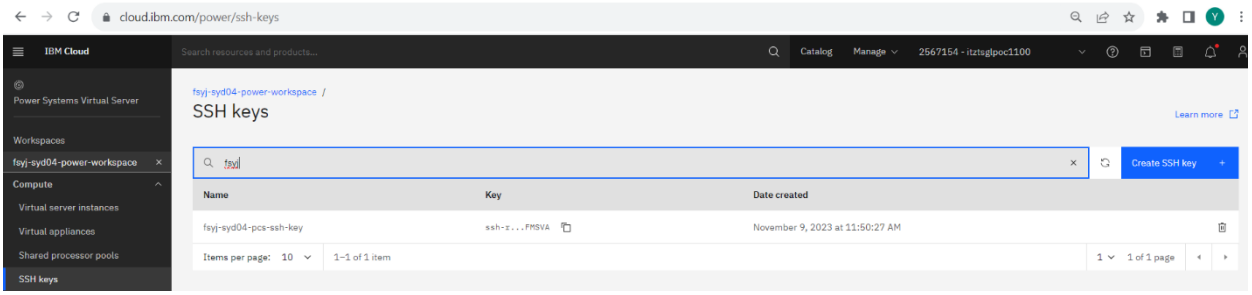
In the *Resource* list, enter your prefix to list all created resources in the workspace.



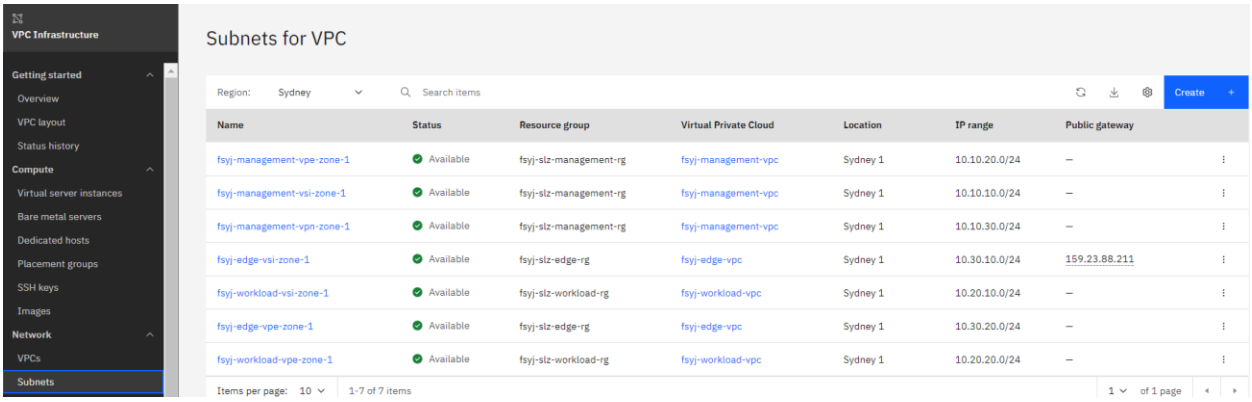
Identify two network subnets created for management and backup.



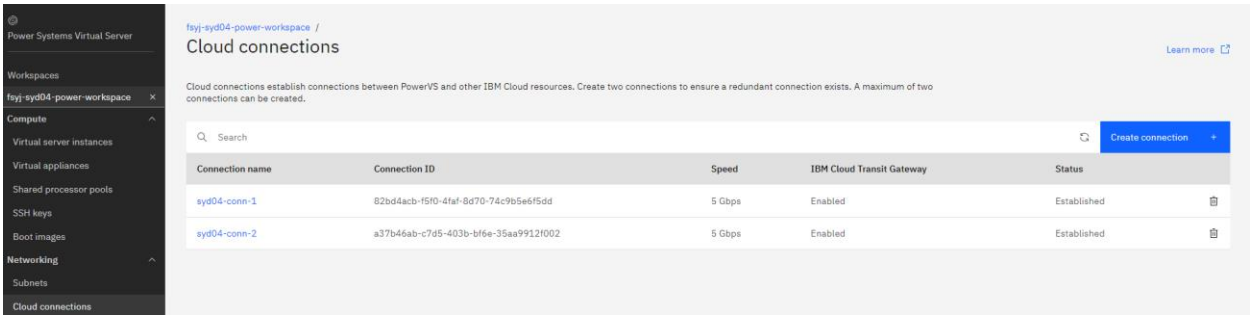
Identify the SSH key created for secure remote connections.



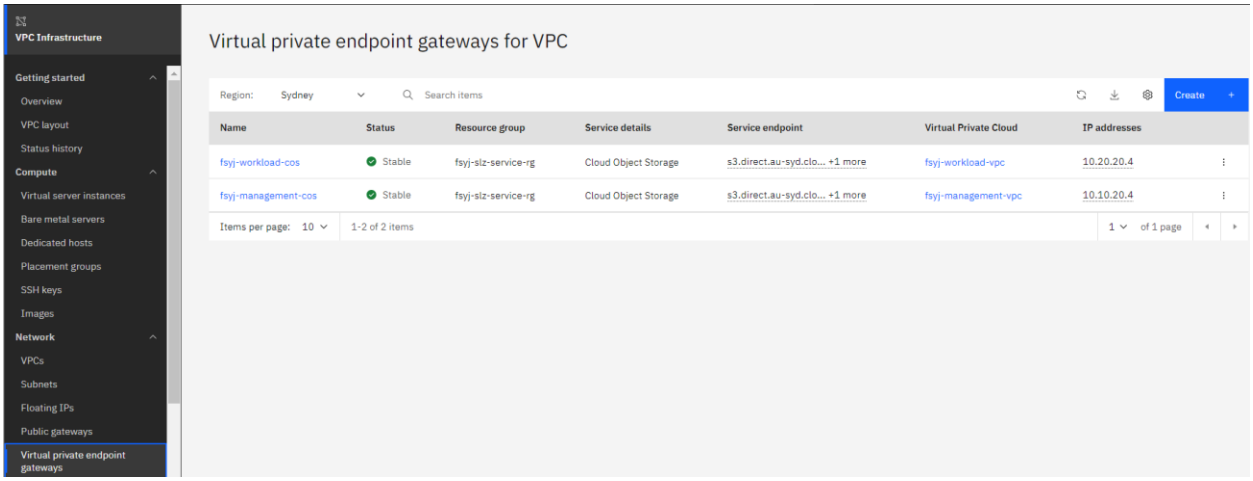
Check VPC subnets.



Check cloud connections.



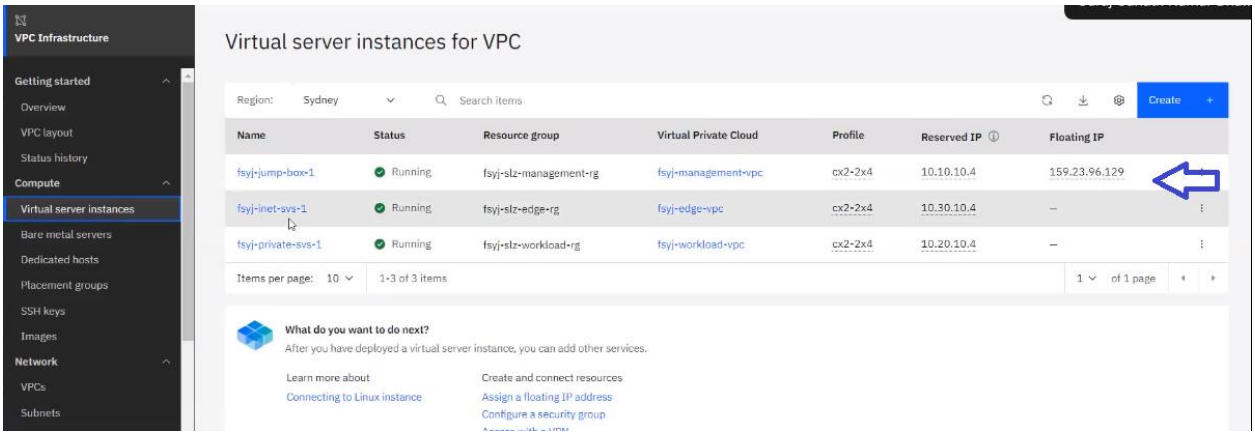
Check Cloud Object Storage.



Access to other servers via jump box

To remotely access other servers via SSH, run the following command, where `access_host_or_ip` is the jump box IP address and `vpc_instance_ip` is the server IP that you want to access:

```
ssh -A -o ServerAliveInterval=60 -o ServerAliveCountMax=600 -o ProxyCommand=\"ssh -W
%h:%p root@\<access_host_or_ip\>\" root@\<vpc_instance_ip\>
```



In this example, *fsyj-jump-box-1* is the jump box host with a public floating IP, *fsyj-inet-svs-1* is the proxy server, and *fsyj-private-sys-1* is the DNS/NTP/NFS server.

For example, to access the DNS/NTP/NFS server with IP 10.20.10.4, run:

```
# ssh -A -o ServerAliveInterval=60 -o ServerAliveCountMax=600 -o ProxyCommand="ssh -W
%h:%p root@159.23.96.129" root@10.20.10.4


Activate the web console with: systemctl enable --now cockpit.socket
Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
Last login: Wed Nov 15 12:25:24 2023 from 10.10.10.4
# exit
logout
Connection to 10.20.10.4 closed.
```

For example, to access the proxy server with IP 10.30.10.4, run:

```
# ssh -A -o ServerAliveInterval=60 -o ServerAliveCountMax
=600 -o ProxyCommand="ssh -W %h:%p root@159.23.96.129" root@10.30.10.4
The authenticity of host '10.30.10.4 (<no hostip for proxy command>)' can't be e
stablished.
ECDSA key fingerprint is SHA256:mY+dkcNTBIZeb/c0JnKBf+/ipaPUBapXFl4dnWAOzDc.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.30.10.4' (ECDSA) to the list of known hosts.
Activate the web console with: systemctl enable --now cockpit.socket

Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
Last login: Thu Nov  9 11:58:39 2023 from 10.10.10.4
```

You can ping the gateways to confirm connectivity.

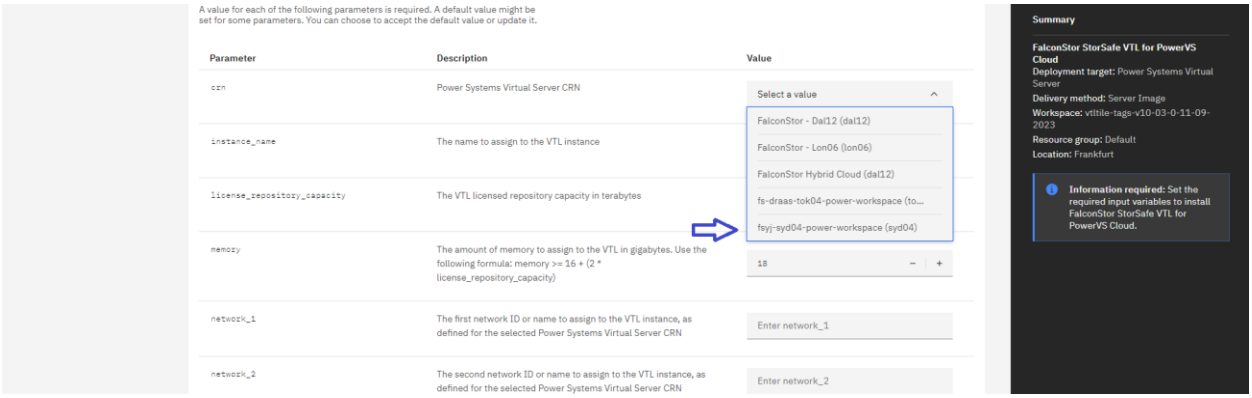
```
[root@fsyj-private-svs-1 ~]# ping 10.51.0.1
PING 10.51.0.1 (10.51.0.1) 56(84) bytes of data.
64 bytes from 10.51.0.1: icmp_seq=1 ttl=53 time=1.76 ms
64 bytes from 10.51.0.1: icmp_seq=2 ttl=53 time=1.100 ms
64 bytes from 10.51.0.1: icmp_seq=3 ttl=53 time=1.81 ms
--- 10.51.0.1 ping statistics ---
```

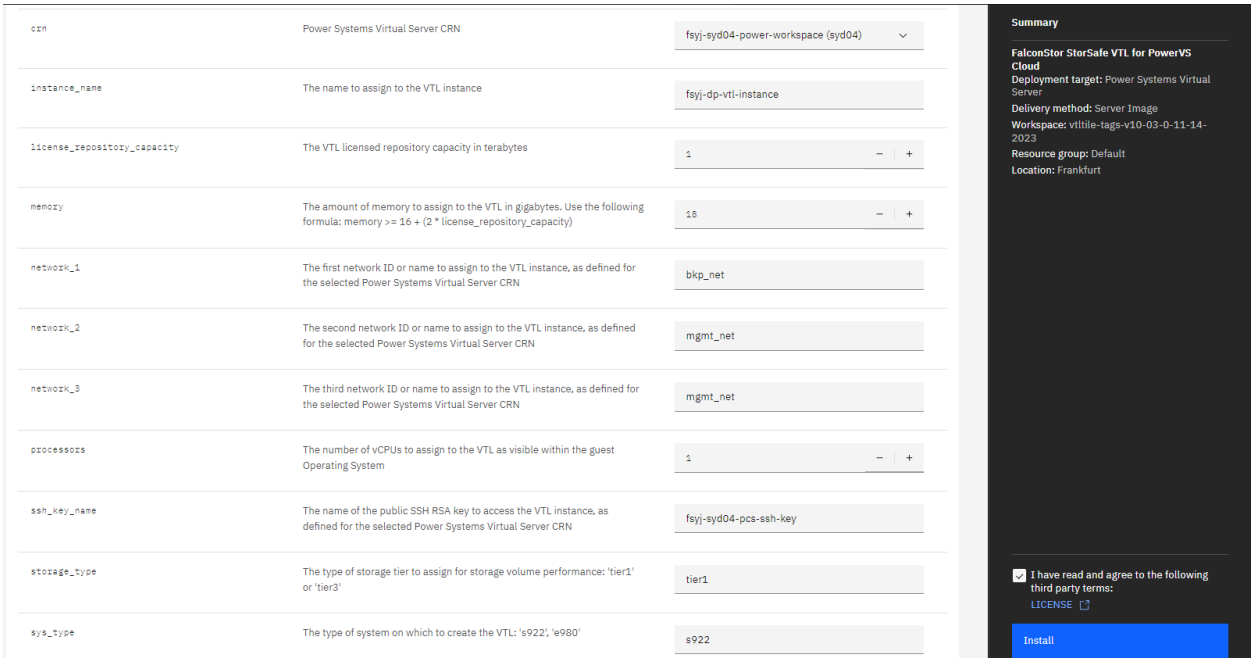
```
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.758/1.856/1.998/0.102 ms

[root@fsyj-private-svs-1 ~]# ping 10.52.0.1
PING 10.52.0.1 (10.52.0.1) 56(84) bytes of data.
64 bytes from 10.52.0.1: icmp_seq=1 ttl=53 time=1.79 ms
64 bytes from 10.52.0.1: icmp_seq=2 ttl=53 time=1.86 ms
64 bytes from 10.52.0.1: icmp_seq=3 ttl=53 time=2.04 ms
--- 10.52.0.1 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8016ms
rtt min/avg/max/mdev = 1.753/1.802/1.867/0.057 ms
```

Use deployable architecture workspace for the FalconStor StorSafe VTL tile

Once your workspace is ready, you can run the FalconStor StorSafe VTL tile and just select that workspace for your CRN. Then, enter the two network names and the SSH key name created in that workspace. Follow your deployment according to steps provided earlier in this document.





Once FalconStor StorSafe VTL tile deployment is completed, you can the related virtual appliance instance in the workspace.

Run the SSH command to connect to FalconStor StorSafe VTL with the *centos* user account from the jump box:

```
ssh -A -o ServerAliveInterval=60 -o ServerAliveCountMax=600 -o
ProxyCommand="ssh -W %h:%p root@159.23.96.129" centos@10.52.0.76

##########################################################################
##                      AUTHORIZED USERS ONLY                           ##
##                                                                      ##
##         The information on this computer is protected by             ##
##         intellectual property rights. You activity may be            ##
##         monitored and recorded.                                      ##
##                                                                      ##
##########################################################################

##########################################################################
##                      AUTHORIZED USERS ONLY                           ##
##                                                                      ##
##         The information on this computer is protected by             ##
##         intellectual property rights. You activity may be            ##
##         monitored and recorded.                                      ##
##                                                                      ##
##########################################################################

=====================================================
  IBM Service and Productivty Tools for Linux on Power

   IBM value-added software for Linux on Power servers
   is available to be installed.
   You can set up IBM remote repositories at any time
   by running as root:

   # /opt/ibm/lop/configure

=====================================================

[centos@fsyj-dp-vtl-instance ~]$
```