FALCONSTOR

FALCONSTOR STORSAFE ™

VTL for IBM PowerVS
Deployment Guide

FalconStor StorSafe™ VTL for IBM PowerVS Deployment Guide

FalconStor Software, Inc.
701 Brazos Street, Suite 400
Austin, TX 78701 USA
Phone: 631-777-5188
Website: www.falconstor.com

33023

Contents

Introduction

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

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

Intended audience

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

- Storage architects
- Consultants
- System Administrators

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

- IBM Cloud
- FalconStor VTL 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

Site	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 Java GUI Console	https://falconstor-download.s3.us-east.cloud-object-storage.appdomain.cloud/VTL-Console-10.03-11072-01.exe
FalconStor VTL User Guide	https://falconstor-download.s3.us-east.cloud-object-storage.appdomain.cloud/FalconStor%20VTL%20for%20IBM%20User%20Guide.pdf
FalconStor USB image for on-premises physical appliances	https://falconstor-download.s3.us-east.cloud-object-storage.appdomain.cloud/gUSB3850MB-Install-7.6.282a-Dedupe-10.03-11072-OEL7U6.img.zip

FalconStor USB image installation guide	https://falconstor-download.s3.us-east.cloud-object-storage.appdomain.cloud/FalconStor%20Server%20Physical%20Appliance%20Installation%20Guide.pdf
FalconStor VA image for on-premises virtual appliances on VMware	https://falconstor-download.s3.us-east.cloud-object-storage.appdomain.cloud/Install-7.6.282-VA-Dedupe-10.03-11072.OEL7U6.VMDK.zip
FalconStor VA image installation guide	https://falconstor-download.s3.us-east.cloud-object-storage.appdomain.cloud/FalconStor%20Server%20Virtual%20Appliance%20Installation%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 documentation for 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 VTL with the IBM Cloud:

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

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) that allows IBM Cloud users to selectively route private network traffic through firewall and VPN features. IBM VRA incorporates elements of Vyatta OS, which is a router software component. Optionally you can use a transit gateway router and Power Virtual Clouds (VPC).

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, like Vyatta or Juniper, 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 VTL PowerVS will submit COS requests to the IP or URL of the proxy. Make sure the DNS settings are right in `/etc/resolv.conf` of the VTL server to resolve the endpoint name. Use the system command `ping` to confirm connectivity with the endpoint.

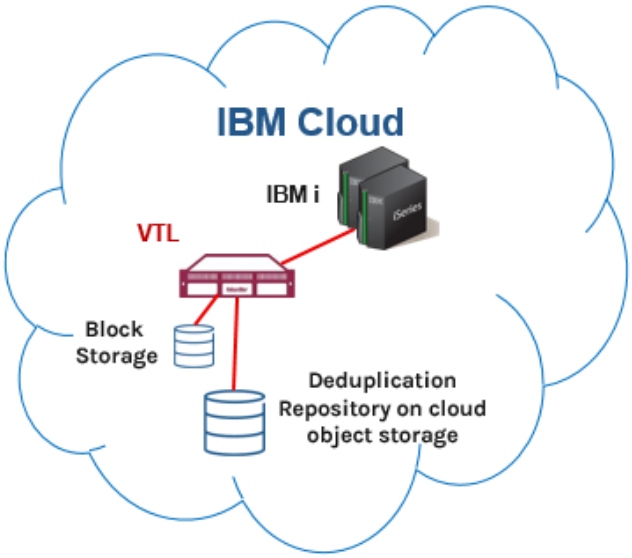
Optionally, you can use *Megaport*, which enables direct and dedicated connectivity between the primary site and IBM Cloud, to overcome the use of the public internet. Megaport is a software layer to manage network connections, allowing private point-to-point connectivity between any of the locations 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 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 VTL for ingest data,
- between the VTL console and VTL for management,
- between VTL and IBM COS for deduplicated data,
- between VTL source and replica servers for data replication.

Native Backup Deployment

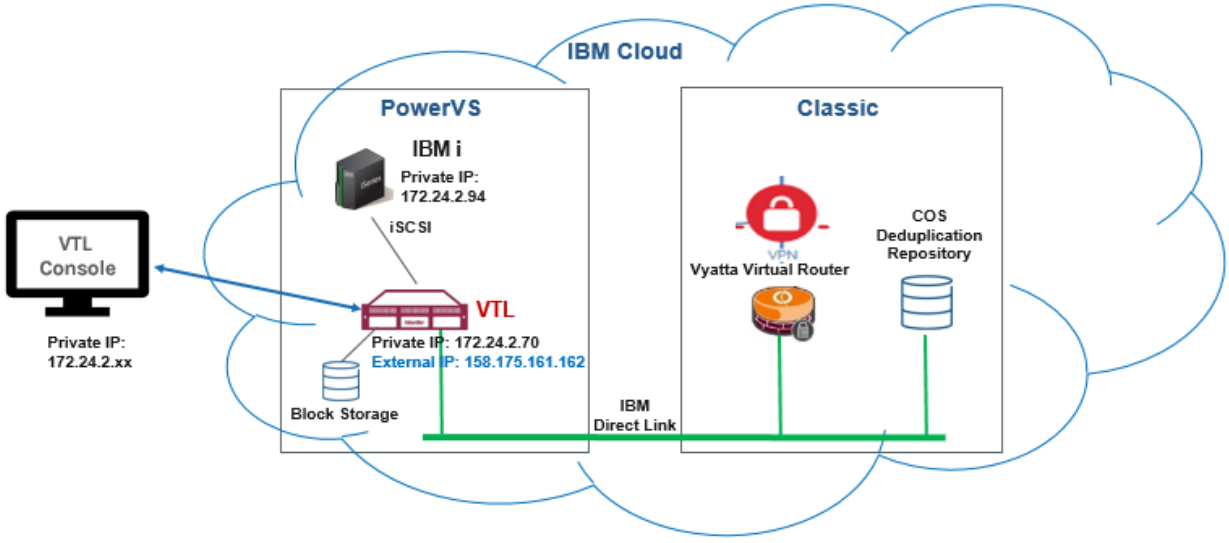
Several IBM i host clients are connected via iSCSI to VTL in the cloud to back up data via IBM Backup, Recovery & Media Services (BRMS) to virtual tape libraries. VTL uses IBM COS as the data devices for the deduplication repository via a Generic S3 object storage account.



Connectivity

The following connections are required:

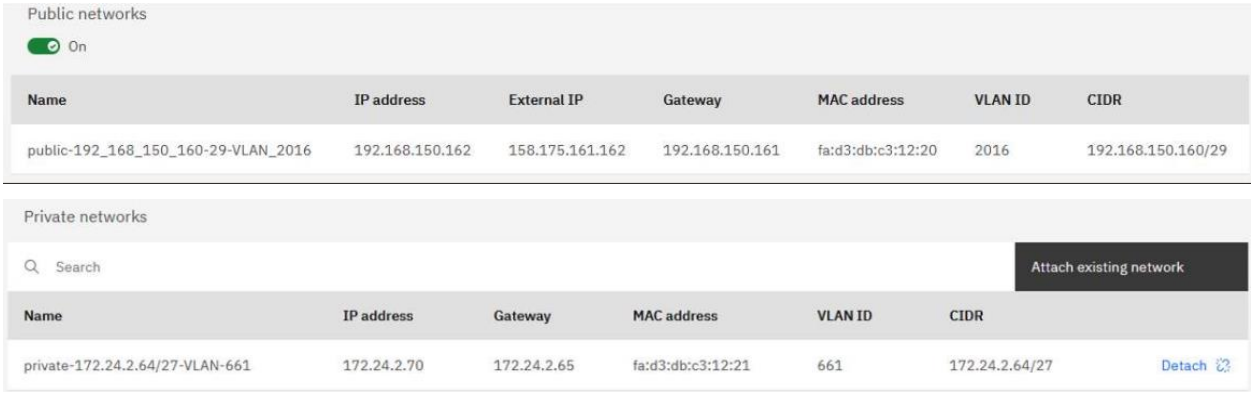
- Network connections between VTL and the management console
- iSCSI connections between VTL and IBM i host clients
- IBM Cloud Direct Link connection between VTL and the IBM Cloud Object Storage (COS) in the IBM Cloud Classic environment
- Internet connection with the FalconStor license server for online 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 VTL 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
```

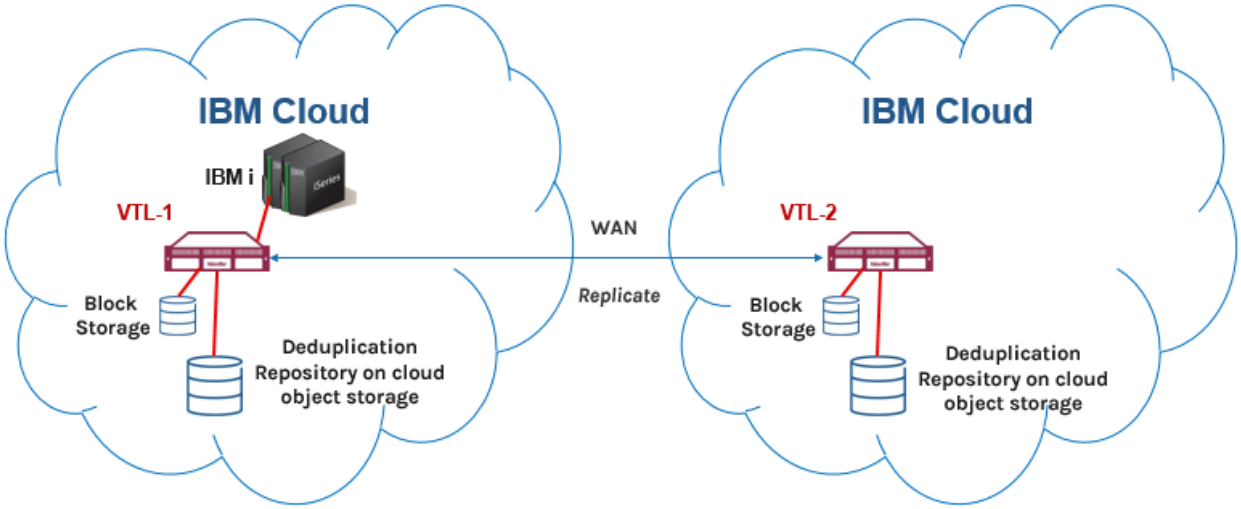
Create routes from the private IP to connect to the other networks. For example, `ADDRESS1=10.0.0.0` is for routing to the Classic infrastructure and `ADDRESS2=172.22.0.0` is added for routing to other private networks.

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

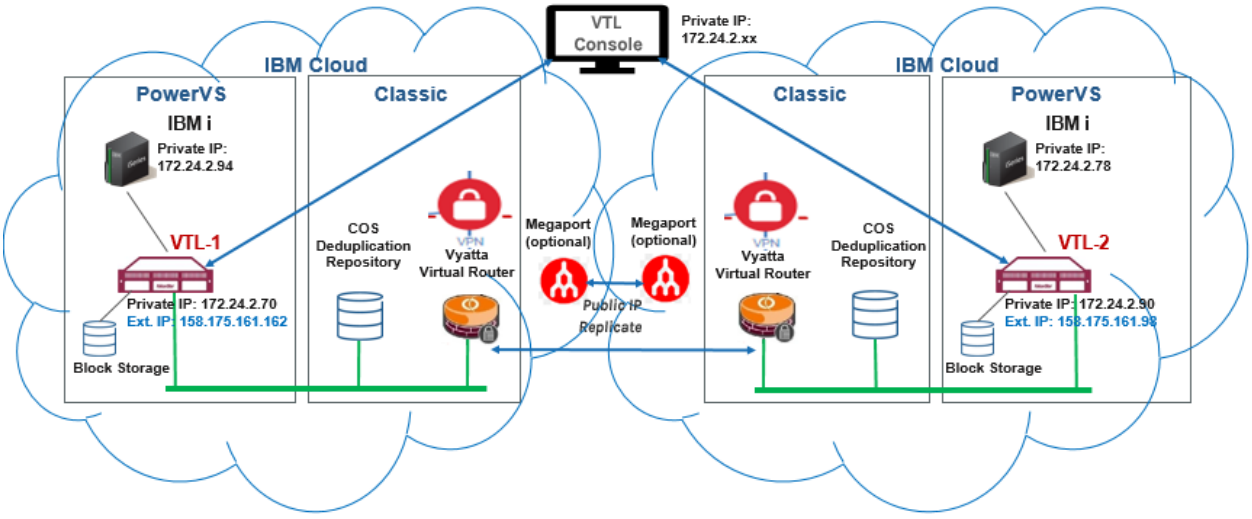
VTL in IBM Cloud replicates data over a WAN to another VTL in the cloud for data protection and disaster recovery. VTL source and replica servers use IBM COS as the data devices for the deduplication repository via Generic S3 object storage accounts.



Connectivity

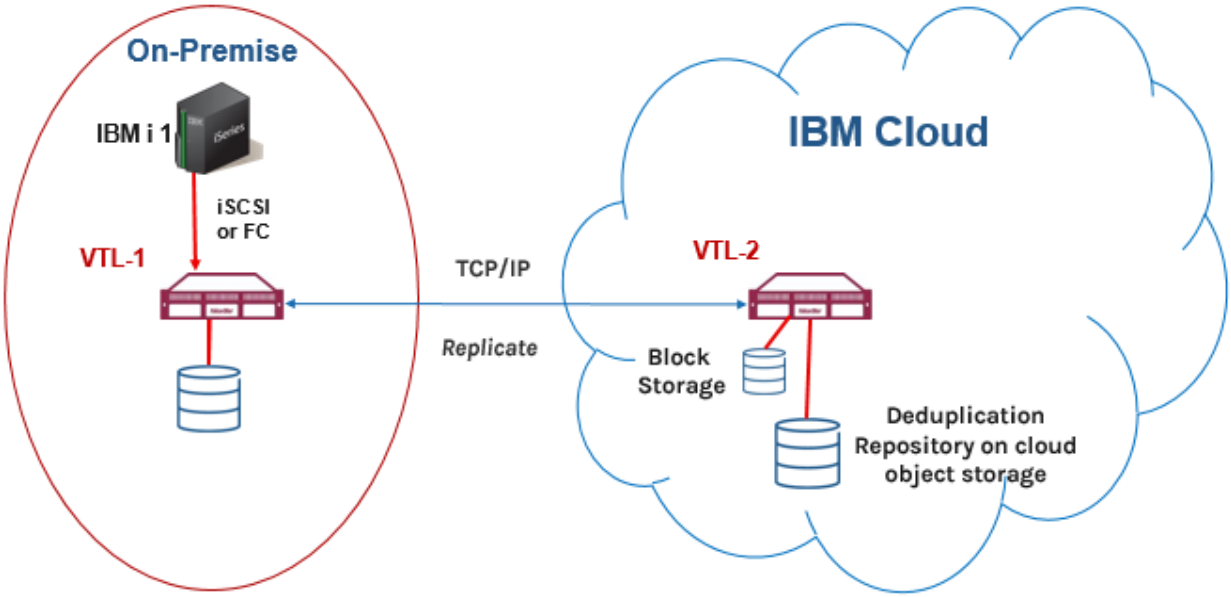
The following connections are required:

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



Hybrid Cloud Deployment

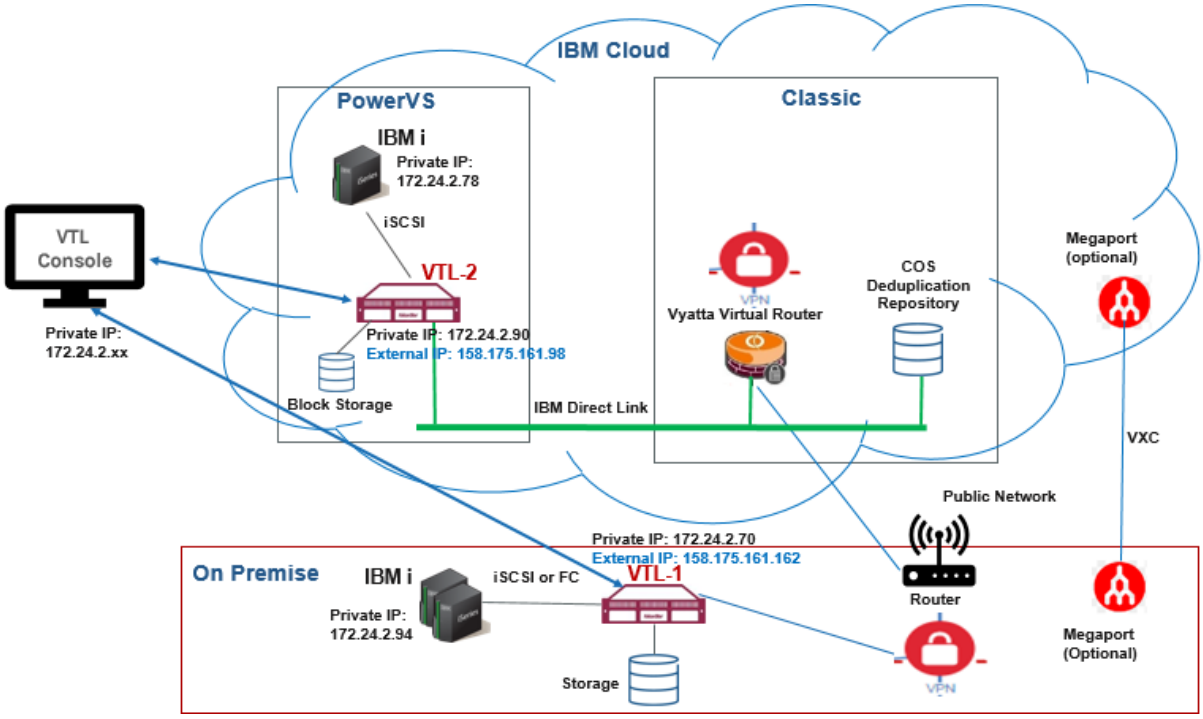
An on-premises VTL server deduplicates data and replicates to a VTL server in IBM Cloud for data protection and disaster recovery purposes. The on-premises VTL uses SCSI devices for the deduplication repository. The VTL target server in the cloud uses IBM COS as the data devices for the deduplication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



Connectivity

The following connections are required:

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

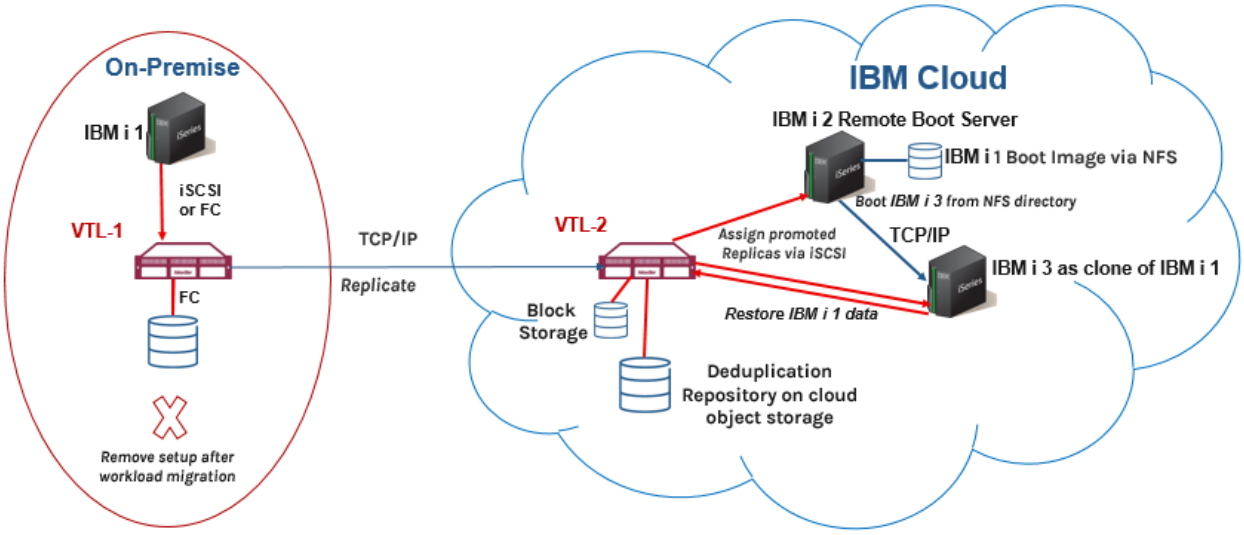

IBM Cloud
PowerVS
IBM i
Private IP:
172.24.2.78
iSCSI
VTL-2
Private IP: 172.24.2.90
External IP: 158.175.161.98
Block Storage
IBM Direct Link
Classic
VPN
Vyatta Virtual Router
COS
Deduplication
Repository
Megaport
(optional)
VXC
VTL
Console
Private IP:
172.24.2.xx
Public Network
Private IP: 172.24.2.70
External IP: 158.175.161.162
On Premise
IBM i
iSCSI or FC
VTL-1
Private IP:
172.24.2.94
Router
Storage
VPN
Megaport
(Optional)

Workload Migration Deployment

IBM i backup clients of on-premises VTL servers are to be moved to the cloud via VTL data replication. VTL 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:

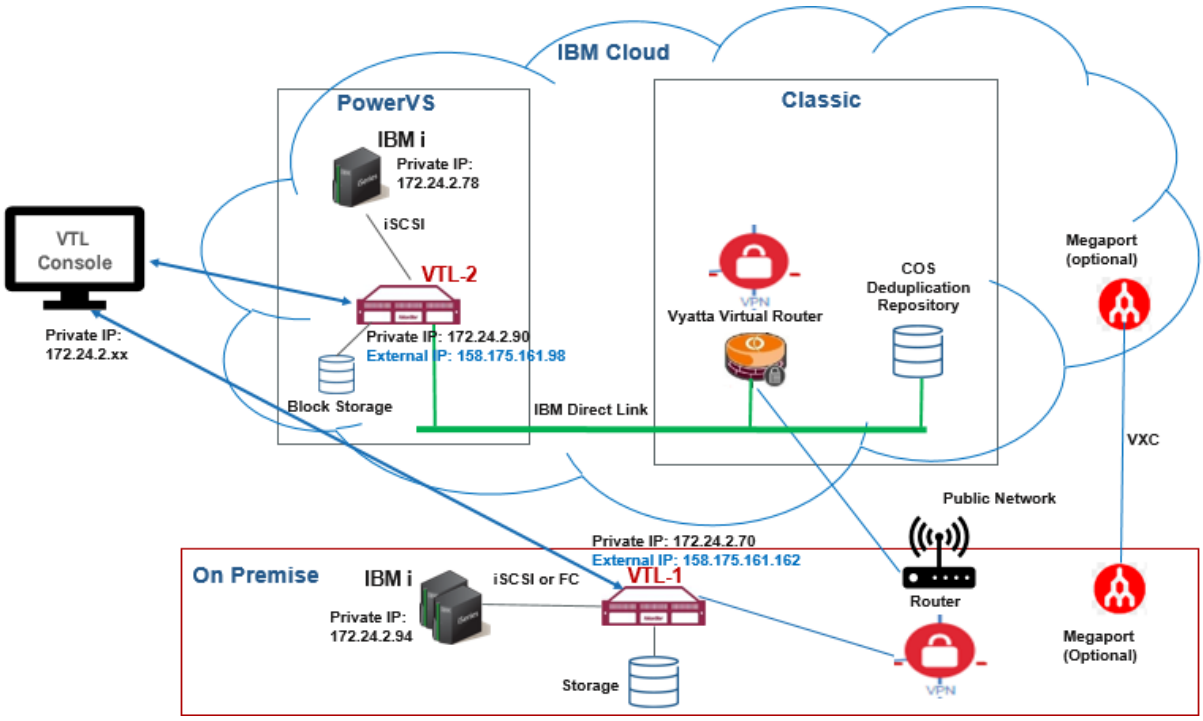
1. IBM BRMS running at the primary site on an IBM i host client performs I/O to a FalconStor VTL server via iSCSI to back up the OS boot image and application data on virtual tapes. The IBM i host client needs to be prepared for migration; two virtual tapes are needed; the first tape will contain the 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 VTL server deduplicates data and replicates both tapes to another VTL 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.



Connectivity

The following connections are required:

- Network connection between the on-premises VTL and the PowerVS VTL in IBM Cloud
- Network connection between the VTL console in the classic infrastructure and the on-premises VTL
- Network connections between the VTL console in the classic infrastructure and the PowerVS VTL in IBM Cloud
- iSCSI or Fibre Channel connection between IBM i host clients and the on-premises VTL
- iSCSI connections between IBM i host clients and the PowerVS VTL in IBM Cloud
- IBM Cloud Direct Link connection between the PowerVS VTL and the IBM Cloud Classic environment, if the IBM Cloud Object Storage (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 chapter contains information and deployment guidelines for FalconStor VTL in IBM Cloud.

The following highlights 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 three subnets in your Power Systems Virtual Server service to isolate traffic via VLANs.
6. Create SSH keys in the Power Systems Virtual Server service for secure remote connections.
7. Use the *FalconStor* StorSafe *VTL for PowerVS* tile in the IBM catalog to create a power virtual server running the FalconStor software.
8. If you use COS for deduplication data repository, create an object storage bucket on the IBM Cloud. Note the access key, password, endpoint specifying the full URI/URL path to the object storage, region, and bucket name.
9. Set up storage resources in the IBM Cloud to attach to FalconStor VTL.
10. Create power servers running backup software that will be attached as iSCSI clients to FalconStor VTL.
11. Configure FalconStor VTL via the FalconStor management console.
12. Configure iSCSI clients to be attached to the FalconStor VTL 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. VTL 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 OS, enter values for usage parameters based on the Solution Sizing tool results, click *Calculate cost* and *Save* to see the cost. Click *Review estimate* to go the *Cost estimator* page. Additional costs may apply based on extra capacity for the Cloud Object Storage (COS), or additional network and infrastructure components. For the COS capacity go to *Catalog*, type *Object Storage* in the

Search box, Select the *Standard* plan. Click *Estimate costs*, enter a value for *Monthly average capacity*, and the *Calculate cost* again.

The FalconStor VTL will be activated with a temporary license after deployment. Once deployment is complete, look for an email from ibmsales@falconstor.com to receive a permanent license and then replace the temporary license with the permanent license via the VTL management GUI.

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 VTL. 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 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 data to restore

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 processor. A virtual CPU (vCPU) also known as a virtual processor, is a physical central processing unit that is assigned to a virtual machine. One vCPU is equal to one physical CPU core.

For large systems requiring 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 VTL 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 VTL 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 management console, 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.

Required network ports

Make sure network firewalls allow VTL access through the following ports. Refer to the *Appendix* section in the *FalconStor VTL 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
- UDP port 123 for time synchronization via NTP
- TCP port 3260 for communication between VTL and iSCSI clients
- TCP port 11576 for secure RPC communication between VTL and the Management Console
- TCP/UDP 11577 port for incoming data replication (if replication configured)
- TCP/UDP 11579 port for replication authentication (if replication configured)
- TCP port 11582 for CLI commands (if applicable)
- TCP port 11583 for report requests to VTL
- TCP ports 11781 and 11782 for replication encryption (if applicable)
- TCP port 18651 for communication between severs for non-encrypted replication (if applicable)
- TCP port 18652 for communication between severs for encrypted replication (if applicable)
- TCP port 80 for internet connection to the FalconStor license server (*register.falconstor.com*) for online registration of license keycodes. If for security reasons, this cannot be set up, offline registration can be used.

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 VTL 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:
  - *Management Console* 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

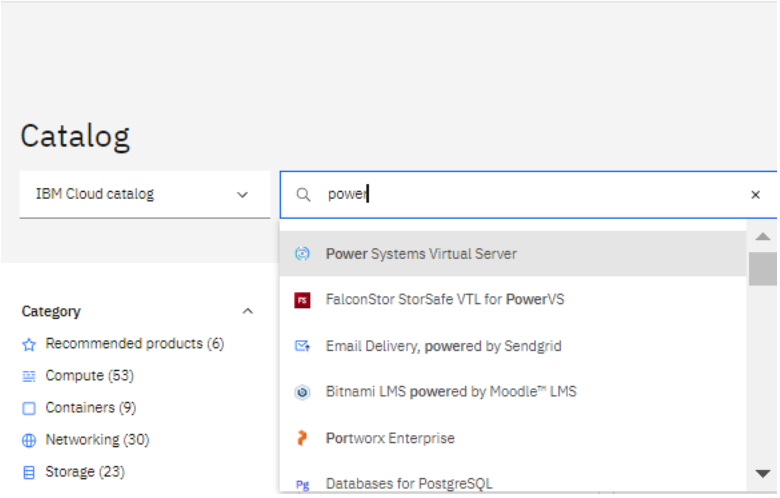
Data replication

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

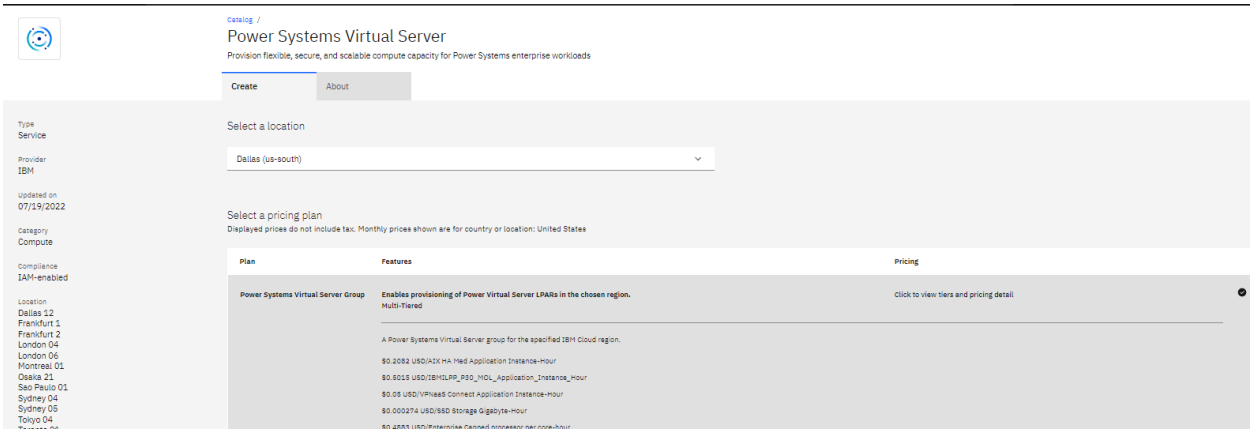
Create a Power Systems Virtual Server service

Before deploying a VTL 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.

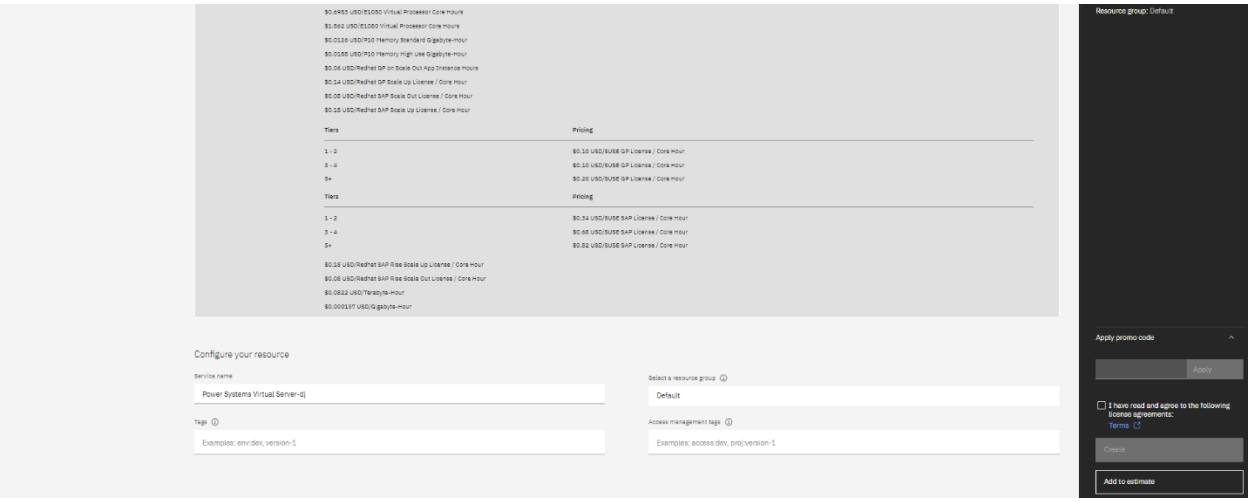
1. Connect to IBM Cloud using your credentials.
2. Click *Catalog* in the menu bar, type *Power* in the search box and select *Power System Virtual Servers.*



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



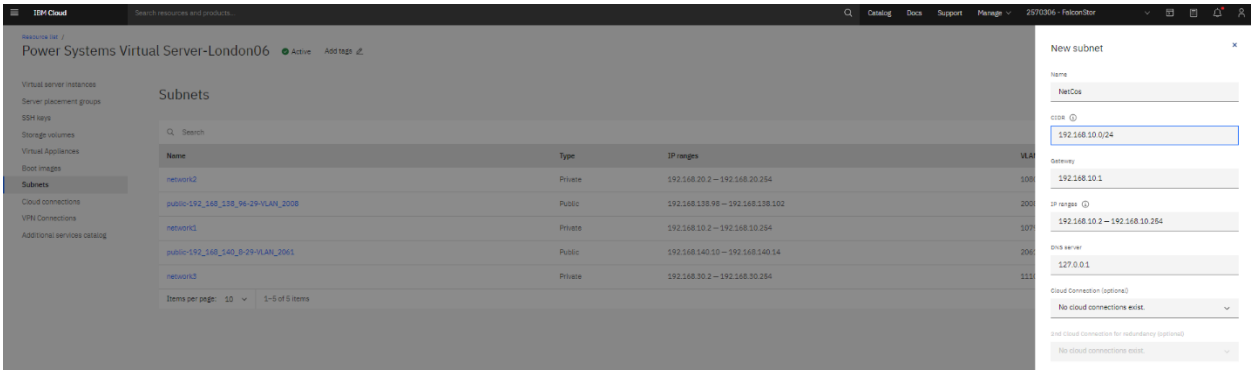
4. Update the *Service name* or leave the default name and press *Create*.



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 *Management Console* and *COS* access, *iSCSI clients* in different areas, *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*, 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

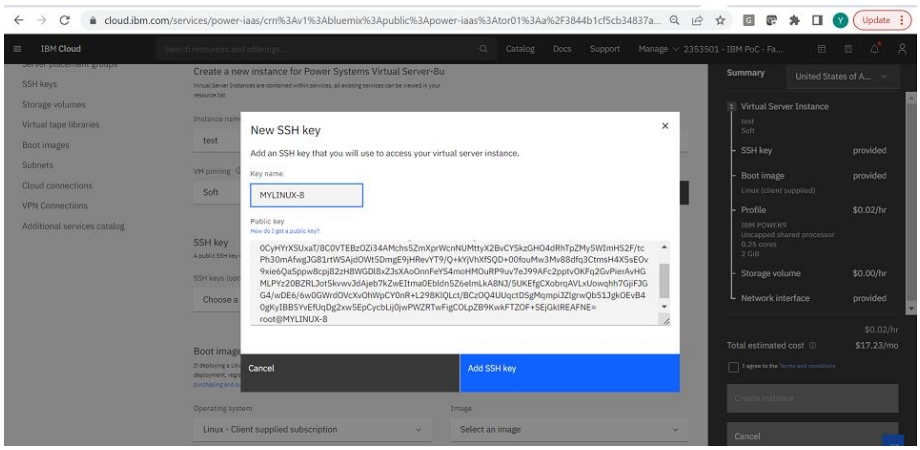
SSK keys are used for secure remote connections to VTL.

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*, 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*.

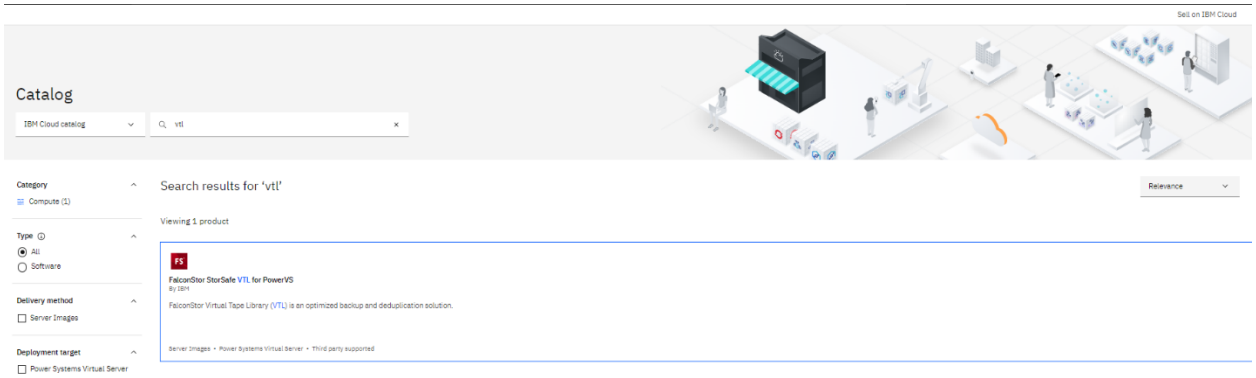


Create VTL Power Virtual Server

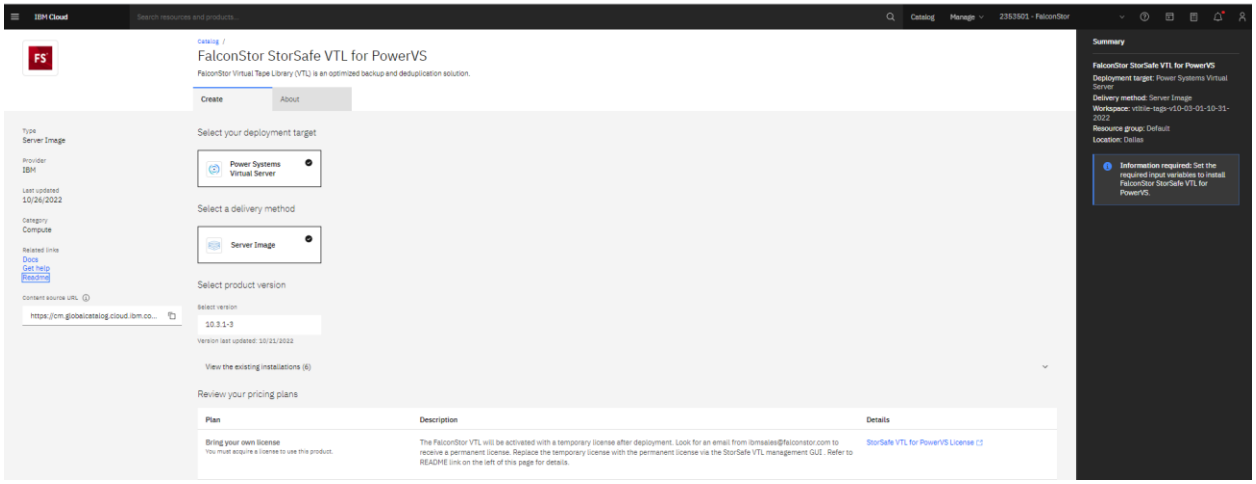
This chapter explains how to create a power virtual server running the FalconStor VTL software product in IBM Cloud. The FalconStor Open Virtual Appliance (OVA) package contains the Linux OS image and FalconStor VTL software.

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

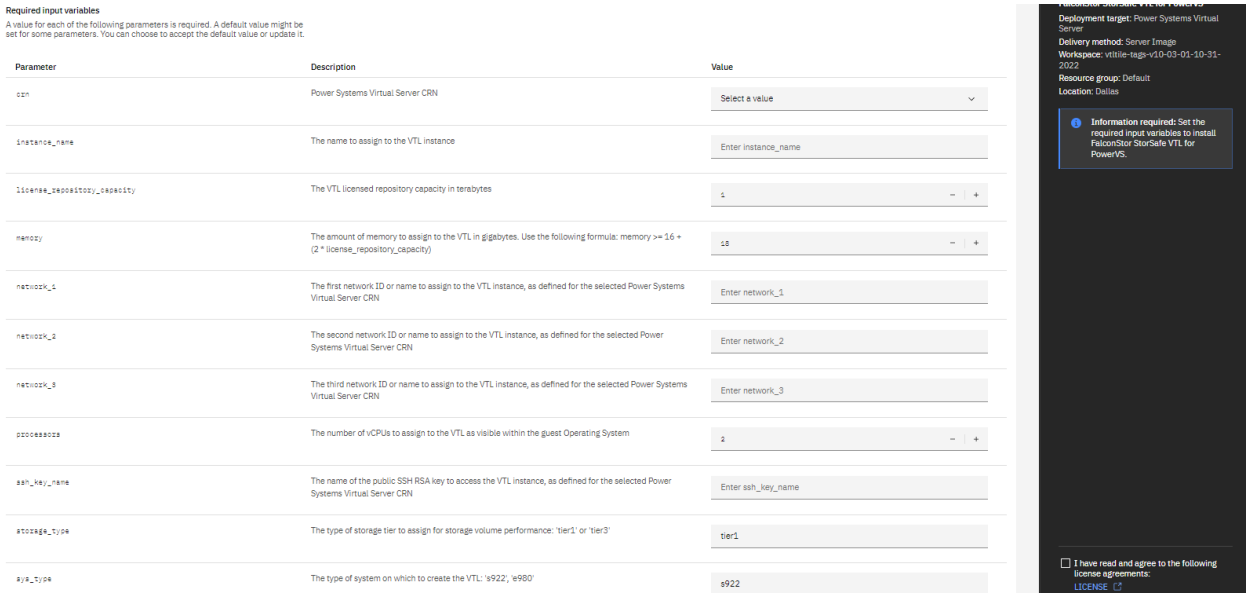
1. Connect to IBM Cloud using your credentials.
2. Click *Catalog* in the menu bar, type *vtl* in the search box, and then select *FalconStor* StorSafe *VTL for PowerVS* tile.



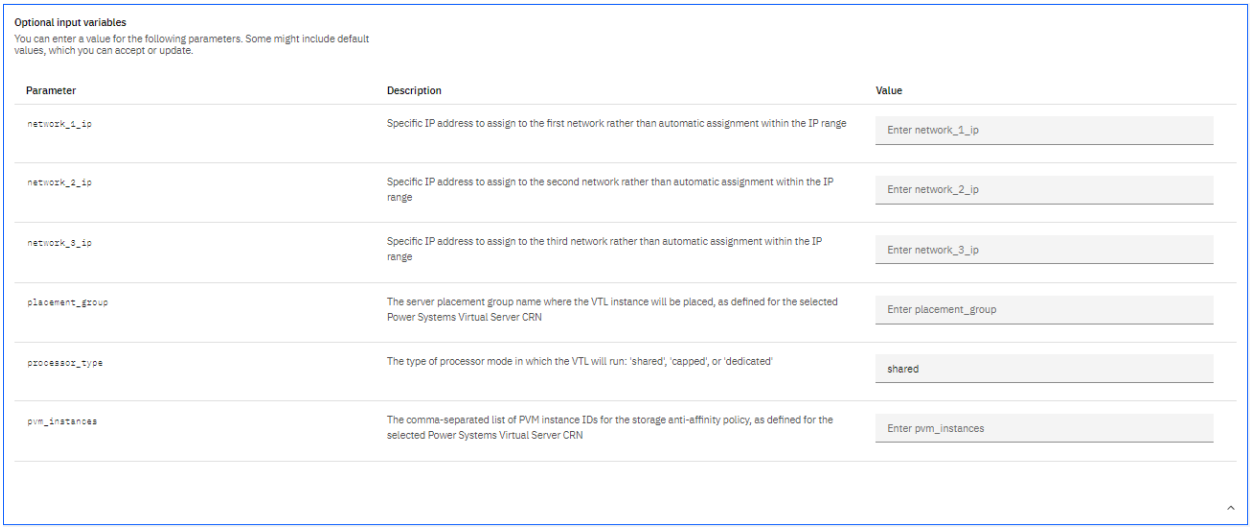
3. Use *Power Systems Virtual Server* as the deployment target, use *Server Image* as delivery method, select the version.



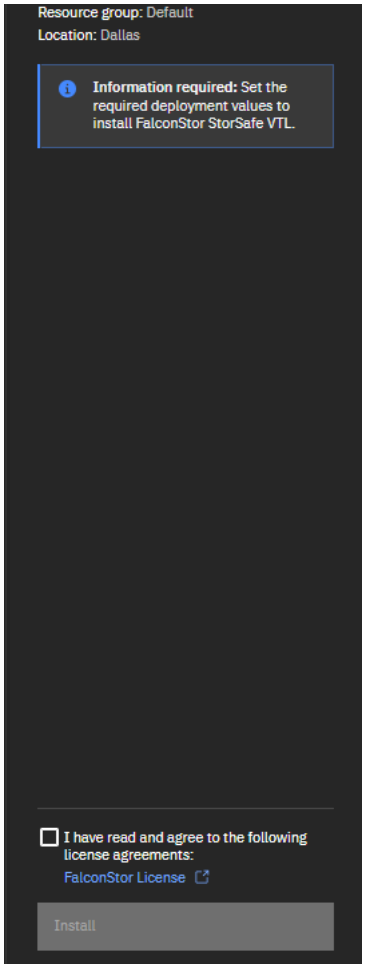
4. Set the server deployment values:
   a. Select the Power Systems Virtual Server Cloud Resource name (CRN) that represents your data center.
   b. Enter a name for your VTL instance.
   c. Set the size of your license repository capacity.
   d. Set the memory size according to the sizing calculator tool results.
   e. Enter the network names 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.
   f. Set the number of CPU cores according to the sizing calculator tool results.
   g. Enter the SSH key name as defined for the selected Power Systems Virtual Server CRN.
   h. Choose *Tier 1* for the storage type for better I/O performance.
   i. Select the machine type, *s922* or *e980*, based on the server sizing. Type *e980* is to be used for a large system that requires more memory to hold a deduplication repository of around 400 TB.



5. Expand the *Optional input values* to check other deployment values.
   a. 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 the source machine A be preserved on the target machine B.
   b. If applicable, enter the name of a server placement group where the VTL instance should be placed, as defined for the selected Power Systems Virtual Server CRN.
   c. Set the processor type: *Shared*, *Dedicated*, or *Shared Capped*. *Shared* is less expensive.
   d. To place the VTL volume on storage controllers according to a storage anti-affinity policy, enter the 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 virtual machines (VMs) exist in your environment and VTL is not the first VM to add. 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.
   For both storage affinity and server placement group we recommend the VTL to not be on the same server or storage box as other machines it is backing up.



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



7. Click *Virtual Appliances* and select your instance.
8. Click *VTL 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@VTL 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.

Set up Resources in IBM Cloud

The following highlights the storage volumes in IBM Cloud that you will need to attach to VTL:

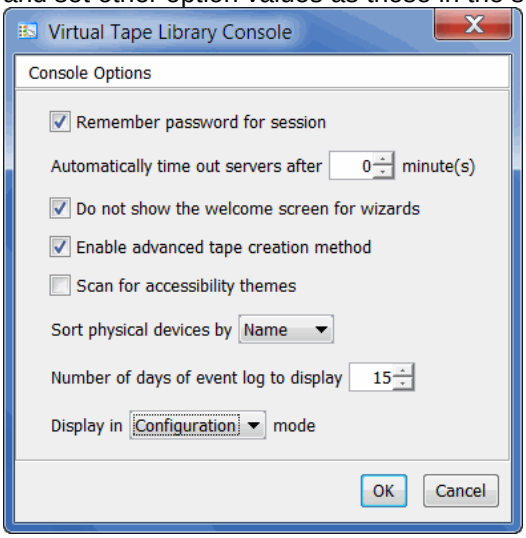
- Set block storage for the configuration repository, tape cache, deduplication repository index and folder disks.
- If you use COS for VTL deduplication repository data disks, get an S3 object storage bucket with "Object Writer" access, with service credential including HMAC. Note the bucket name, location, access key ID, and secret access key. Create an IBM COS bucket with service credential including HMAC for the deduplication repository.
- Add block storage and COS (if applicable) to the VTL instance.
- Create power servers as backup VTL clients running IBM i. Install IBM iSCSI packages and required PTF files on IBM i host clients.

Configure VTL

You need to run the FalconStor management console to configure VTL. The console is the graphical administration tool that enables you to manage your VTL servers.
Refer to the *FalconStor VTL User Guide*.

The following highlights the configuration steps for VTL:

- Download the FalconStor VTL management console from the link above in this document.
- Install the management console as a Power User or Administrator on a Windows machine.
- Launch the console from your machine.
- Confirm the End-User License Agreement (EULA) that appears the first time that the console is launched.
- Open the GUI Console and navigate to *Tools - Console Options*. Select the *Configuration* mode and set other option values as those in the screenshot below:



- Add VTL servers. Right-click the *Servers* object and click *Add*.
- Connect to your server with the *root* user account and the related password. The default password *IPStor101* expires after installation, and you need to set a new password the first time you log in to the server, the configuration wizard launches.
- Check items below in the configuration wizard that appears after connecting to a server. Click *Configure* for each item that applies and click *Skip* for items that do not apply:
    - Set up network parameters and hostname.
    - Skip Fiber Channel for virtual servers. Enable it only for an on-premises VTL server that is using Fibre Channel protocol to communicate with backup clients.
    - Prepare devices by selecting all devices and setting an appropriate reservation type for each block storage: *Configuration repository* for the 20 GB device, *Deduplication repository* for index and folder devices, *Tapes* for backup cache devices.
    - Enable Configuration Repository using 10 GB of the reserved device.
    - Create Virtual Tape Library database using another 10 GB of the reserved device, select the *Express* method, enable virtual tape library software compression, accept default thresholds, and do not create a mirror for the database.

  - Skip virtual tape encryption.
  - Skip physical tape libraries/drives assignment.
  - 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.
    Leave default settings and do not enable any service options.
    Set the barcode range for tapes, adjust current settings, if desired, set the number of Import/Export slots to 1. The number of slots in a virtual tape library can be larger than the supported number of its equivalent physical library of the same model. Skip the warning that may be displayed based on the library model.
    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 Incremental size is (Maximum Capacity – Initial Tape Size) / 63.
    You can create virtual tapes at this time or later.
  - Skip assigning virtual tape library to clients
  - Skip the item to enable deduplication.
  - Exit the wizard after selecting the option *Don't show this next time*.

- Optionally, create storage pools for tape allocation: Expand the *Physical Resources* object, right click *Storage Pools* and select *New*.
- Right-click the server and add a Generic S3 object storage account using IBM Cloud access account information noted above and enable the "Reserved for SIR" option.
  If you use a reverse proxy server to make remote connections to IBM COS private endpoints, use the CLI command `object-storage-add` to enter the proxy IP address and user/password:

```
# iscon object-storage-add -s <VTL server name> -u <username>
-p <password> -On <object storage name> -Ot GENERIC_S3
-Oi <HMAC access key ID> -Os <HMAC secret key> -Ob <bucket name>
-Op <true (for https)|false (for http)> -Ou <Full URI/URL path>
-Oe false -Ol true [-Oc <optional comments>]
-Ps <Proxy server to access object storage> -Pp <Proxy port number>
-Ph <true (proxy access via https)|false (proxy access via http)>
-PU <Proxy username> -PP <Proxy password>
```

- Enable deduplication from the *Options* menu to create a deduplication cluster. Follow the Single Instance Repository wizard. Select *Object Storage* for data. Select *Generic S3* as provider. Select the Generic S3 object storage account that you had created. Set the SIR data repository size according to the licensed capacity. Select index devices for the deduplication repositories.
- Enable iSCSI target mode from the *Options* menu for connection to backup application servers that access virtual resources.
- Configure iSCSI from the client side according to the *Configure an iSCSI client* section below.
- Create iSCSI host clients to represent your backup application servers. Right-click the *Clients* object and click *Add*. Enter a name, enter client iSCSI initiator name as the one configured on the client side, for example, *iqn.1994-05.com.ibm:apacibmi74falcon*, and allow unauthenticated access.
- Create an iSCSI target for the client: Right-click the newly created client under *iSCSI Clients* object and click *Create 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 VTL server IP address. One iSCSI target should be created for each iSCSI client initiator.

- Assign virtual tape libraries to the new iSCSI target: Select the iSCSI client under *iSCSI Clients*, click the *Resources* tab. Right-click the newly created iSCSI target and click *Assign*. 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

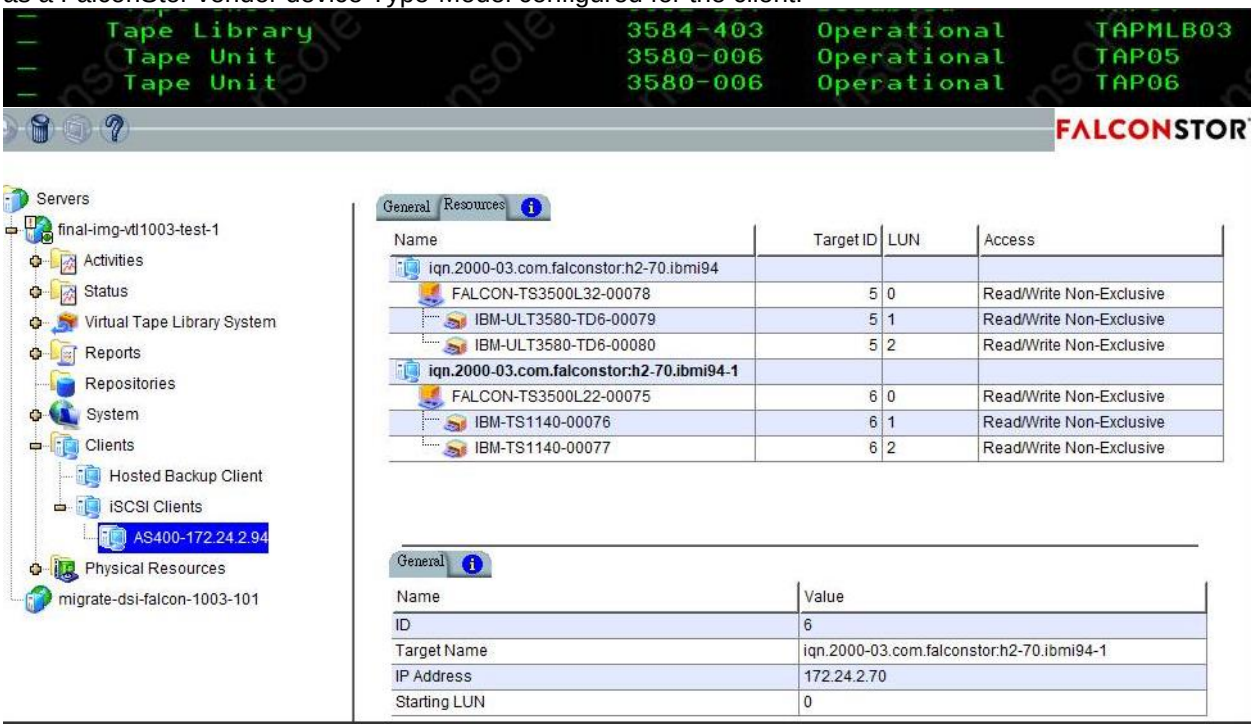
  - Run `STRSST` on the client to check the system bus resource and execute a bus reset to the iSCSI bus resource:
    I/O debug to 298A-001 IOP resource (option 6)

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

If everything is successful, the VTL 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:



- User the default deduplication policy or create deduplication policies: Expand the *VTL Library System* object, right-click *Deduplication Policies*, and select *New*. Enter a name for the policy. Select the deduplication cluster that was previously created. Select *Inline Deduplication* trigger with the option to switch to post-processing. Leave default priority and retry settings.
- If applicable, on the primary VTL 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 VTL via iSCSI. One iSCSI target is created in VTL for each iSCSI client initiator. The VTL PowerVS instance is running Ethernet under an IBM Cloud private network that belongs to a VLAN subnet; no extra VLAN is set on the VTL server.

Check Type-Model

Confirm the IBM PTF is installed on the client by checking the *Type-Model* that 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.

Opt	Description	Type-Model	Status	Resource Name
	Virtual IOP	298A-001	Operational	CMB01

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 VTL 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 VTL yet. After the SQL command completes, you will use the same target name on VTL when configuring the iSCSI client later.

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 VTL 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 VTL system log, `/var/log/messages`. Take a note of the target name in the log, that you need to use when configuring the iSCSI target in the VTL console. You can a message similar to the following one:
   `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 VTL server.

Add block storage

Follow the steps below if you need to attach additional block storage to a VTL server.

1. Select your power system from *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 VTL management console, select *Rescan physical resources* 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. Select your power system from the *Resource list - Services and software* menu.
2. Click *Virtual Appliances* and select your instance.
3. Click *Edit details* to increase the licensed repository capacity of object storage. You will then receive an email from ibmsales@falconstor.com with a new license keycode for additional required space.
4. From the VTL management console, select the server.
5. Enter the new license keycode.
6. Right-click the server, select *Deduplication - Add/Expand Deduplication Data Repository*.
7. Enter a new capacity in the dialog. You must have enough object storage capacity; the system cannot check whether there is sufficient free space.
8. 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 VTL 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. Select your power system from the *Resource list - Services and software* menu.
2. Click *Virtual Appliances* and select your instance.
3. Stop VTL 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 VTL services for changes to take effect.

Add CPU

Follow the steps below if you need to change the number of CPU cores of a VTL 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.

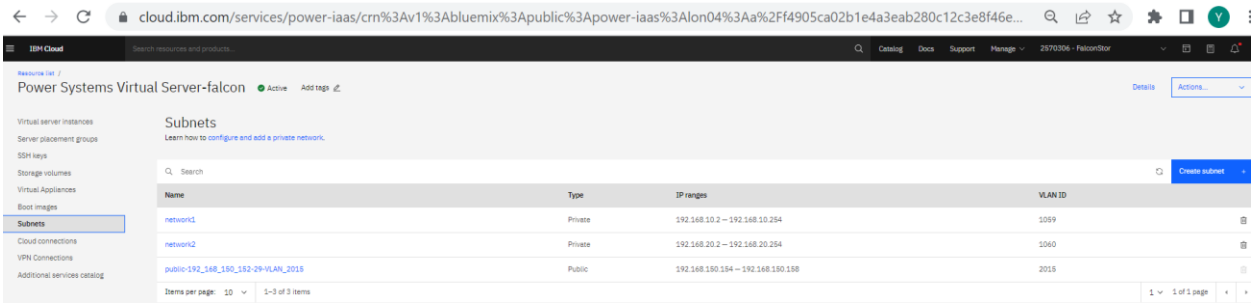
1. Select your power system from the *Resource list - Services and software* menu.
2. Click *Virtual Appliances* and select your instance.
3. Make sure it is in an *Active* or *Stopped* state, and click *Edit details* to enter new values for CPU cores.
   For details, refer to the following IBM document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

Add network

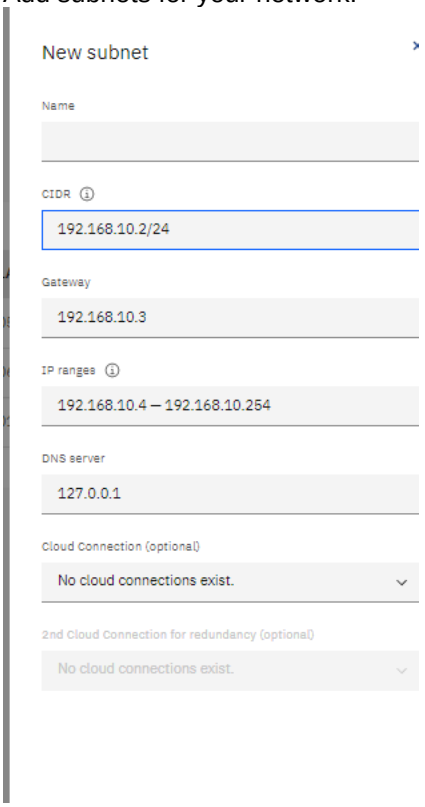
Private network

Follow the steps below if you need to add a private network interface to a VTL instance.

1. Select your power system from the *Resource list - Services and software* menu.
2. Select *Subnets* and click *Create subnet*.

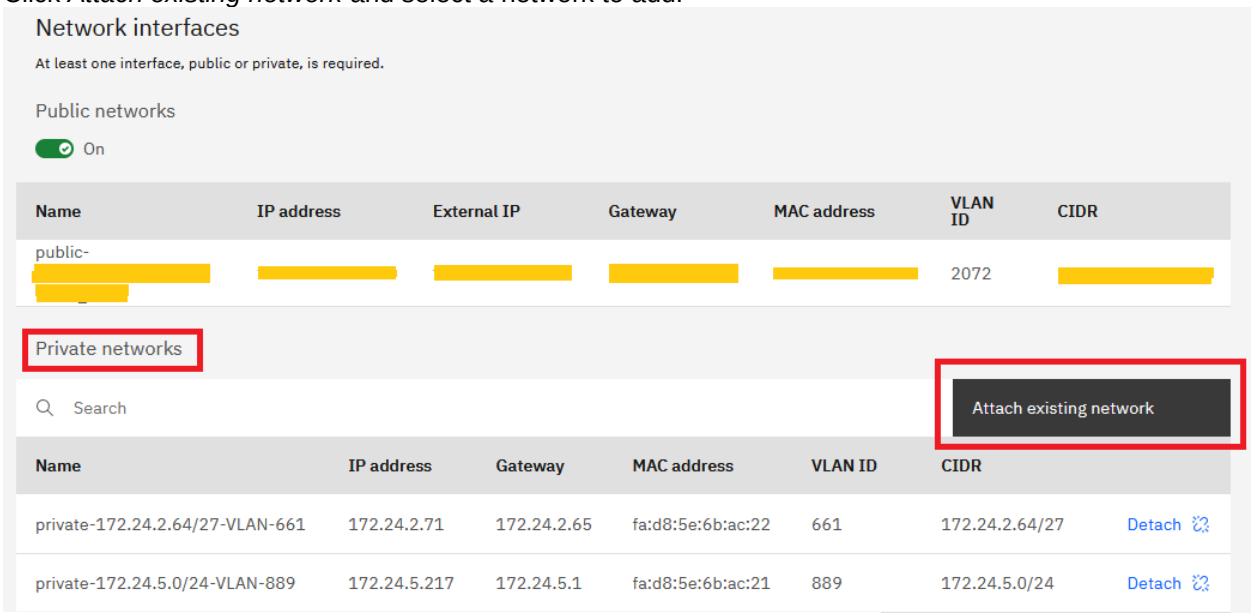


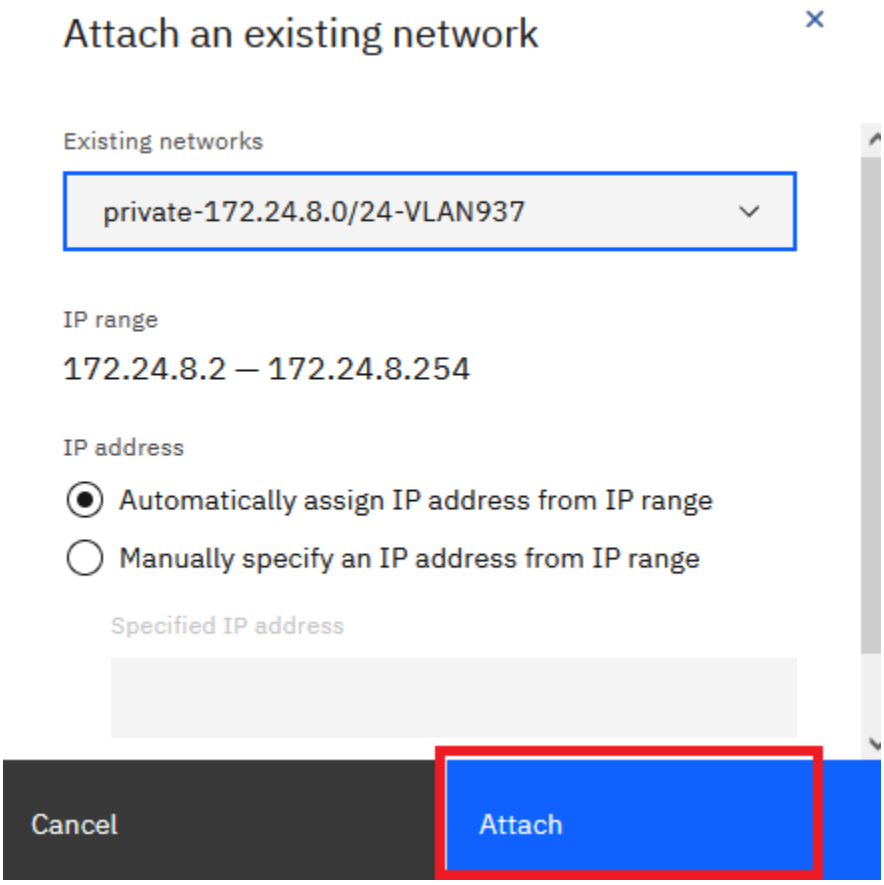
3. Add subnets for your network.



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

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





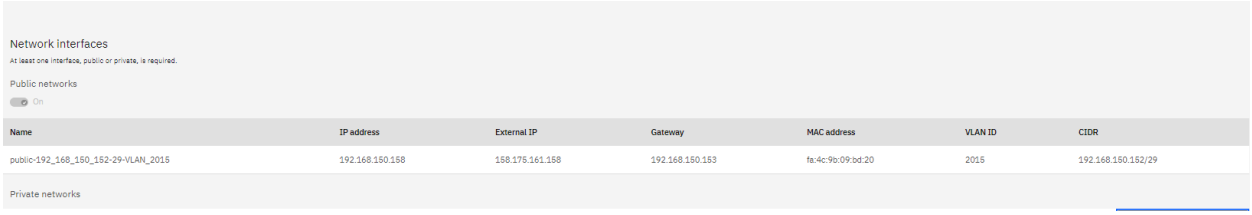
7. Make sure network routers are configured properly in your network infrastructure for the traffic.

8. Open a Linux shell on the VTL server and type the following commands to complete the network device configuration:
    a. # `systemctl restart NetworkManager` (to restart network)
    b. # `ls /sys/class/net` (to see new interface device `ethn`, for example eth3)
    c. # `cat /sys/class/net/eth3/address` (to get 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 ones)
        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 VTL instance.

1. 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 VTL server. After disabling the public IP address, you must restart VTL services.
If deduplication is already enabled while the public interface is in effect, contact FalconStor Tech Support to help.
2. If you need to remove any network interfaces on the VTL server, contact FalconStor Tech Support to help.

Measures for Security Threats

This section describes the security policy implemented for the underlying operating system (OS) and FalconStor VTL 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 allows 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 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 VTL servers.
- A shared secret mechanism based on the Diffie-Hellman algorithm is used for authentication between:
  - Source and replica servers
  - Management console 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.

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 console and host clients use a secured RPC link to communicate with FalconStor servers.

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.
- At least 5 different characters between the old and new password.

The system provides either 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 over. 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.

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.

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 Console 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.