



Compass®

Compass Quick Start Guide for IBM i Data Protection

June 2026

Table of Contents

<i>Overview of Compass Tape Gateway for IBM i Protection.....</i>	<i>1</i>
<i>Pre-Requisites for Compass Tape Gateway VTL.....</i>	<i>1</i>
<i>Step 1: Choosing a Compass Vault Model.....</i>	<i>2</i>
Dedicated Vaults.....	2
Shared Vaults.....	2
<i>Step 2: Provisioning a Dedicated Compass Vault.....</i>	<i>3</i>
<i>Step 3: Provisioning Secure Automated Backup with Compass.....</i>	<i>3</i>
<i>Step 4: Configuring Network Connectivity to Compass Vaults</i>	<i>5</i>
Dedicated Vaults.....	5
Shared Vaults.....	5
Performance Considerations	5
Performance guidance	6
Other General Guidance.....	6
<i>Step 5: Configuring a Compass VTL</i>	<i>7</i>
<i>Step 6: Configuring CHAP authentication for Compass VTL.....</i>	<i>8</i>
<i>Step 7: Configuring Your IBM i for Compass VTL Access.....</i>	<i>8</i>
General Guidance	9
<i>Step 8: Configuring Your IBM i for BRMS or SAV Backups & Restores</i>	<i>9</i>
<i>Step 9: Performing DR Operations from Secondary Compass VTL.....</i>	<i>10</i>
<i>Step 10: Migrating Data to Compass from Legacy Tapes.....</i>	<i>10</i>
<i>Troubleshooting</i>	<i>10</i>
<i>How to Get Support.....</i>	<i>10</i>
<i>Common Customer Questions.....</i>	<i>10</i>



Overview of Compass Tape Gateway for IBM i Protection

Compass Tape Gateway (CTG) integrates virtual tape library (VTL) capabilities directly into the Compass data protection platform. CTG allows the creation of VTLs in Compass Vaults. This provides comprehensive virtual tape library capabilities including support for iSCSI tape library, drive, and volume commands. As a result, in addition to all of its other supported platforms, IBM® i backup data can now be ingested into Compass Vaults via tape operations (for example, IBM i BRMS or SAV operations). Compass can protect IBM i workloads running either on-premises or in the IBM PowerVS Cloud.

There are two major Compass Vault deployment options for IBM i data:

1. IBM i data can be protected in **Dedicated Compass Vaults** deployed either on-premises or in the customer's IBM Cloud account. This deployment scenario requires a customized sizing and proposal that includes Compass SaaS pricing as well as compute and storage. Compute and storage can be delivered as pre-configured hardware appliances (for on-premises deployments) or using IBM Cloud resources.
2. IBM i data can be protected into **Shared Compass Vaults** in the IBM Cloud using a simple \$/stored GB/month pricing. This is the **Secure Automated Backup with Compass** offering in the IBM Cloud Catalog.

This Compass IBM i Quick Start Guide describes the general steps required for Compass protection of IBM i workloads.

Pre-Requisites for Compass Tape Gateway VTL

There are several pre-requisites for using the Compass VTL.

1. You need access to a Compass Vault capable of operating the Compass VTL for your workloads. You can choose either a Dedicated or Shared Compass Vault as described in the next section.
2. The following IBM i PTFs (specific to each release) should be applied to your IBM i system for VTL and Compass usage.
 - a. IBM i v7r3:
 - i. Must have technical refresh 13 installed (MF99213)
 - ii. SF99724 level 71 contains PTFs needed to run iSCSI
 - iii. SI79923, MJ07938, MJ08365, MJ08438
 - b. IBM i v7r4:
 - i. Must have technical refresh 12 installed (MF99312)
 - ii. SF99664 level 49 contains PTFs needed to run iSCSI
 - iii. MJ07930, MJ08366, MJ08439
 - c. IBM i v7r5:
 - i. SF99954 level 19 contains PTFs needed to run iSCSI
 - ii. MJ03921, MJ07928, MJ08367, MJ08440
 - d. IBM i v7r6:
 - i. SF99964 level 3 contains PTFs needed to run iSCSI



ii. MJ07924, MJ08368, MJ08441

Please note that there may be additional PTFs required for proper IPsec, VPN, and VTL functioning on specific IBM i releases. Please refer to the following links for current and more complete documentation on IBM i PTF requirements:

- e. <https://www.ibm.com/support/pages/system/files/inline-files/IBM%20i%20Support%20for%20iSCSI%20VTL%201.8%200.pdf>
 - f. <https://www.ibm.com/support/pages/ibm-i-removable-media-ptfs>
 - g. <https://www.ibm.com/support/pages/node/6413715>
3. Proper network connectivity must be established between your IBM i instances and the Compass Vaults. Guidance for this is provided in Step 4 below.

Step 1: Choosing a Compass Vault Model

Compass provides several options for deploying Vaults as targets for IBM i backup data.

DEDICATED VAULTS

IBM i Customers with one or more of the following needs should consider a dedicated Compass Vault deployment:

- a. Wanting to deploy on-premises Compass Vaults for protecting their IBM i data
- b. Desiring private Compass infrastructure in the IBM Cloud
- c. Having large amounts of IBM i data
- d. Having stringent backup performance requirements
- e. Having strict data governance regulations

New Compass customers must purchase a Dedicated Compass CTG Vault (either hardware based for on-premises or cloud based for IBM Cloud deployments) based on a customized sizing. Existing Compass customers can either purchase a new Compass CTG Vault or work with the Cobalt Iron Deal Desk team to ascertain if an existing Compass Vault has sufficient resources to host the VTL service. Outside of the additional stored capacity usage (for IBM i backup data), there is no additional feature charge for Compass VTL.

To request a Dedicated Compass Vault sizing and proposal, please provide your sizing information at the following link:

<https://www.cobaltiron.com/compass-ibm-sizing/>

In the “Additional Details” section, be certain to request a Dedicated Vault sizing and specify whether you want a physical on-premises Dedicated Vault, a Dedicated Vault in the IBM Cloud, or (for existing Compass customers) if you want to determine if an existing Vault can be used for VTL. The Cobalt Iron Deal Desk team will work with you or your partner on providing a proposal for a Dedicated Compass deployment. If you have questions or require any assistance, contact us at info@cobaltiron.com.

SHARED VAULTS

For rapid and immediate deployment, Shared Compass Vaults are already deployed in IBM Cloud data centers worldwide and are ready to service IBM i workloads. This SaaS offering, Secure Automated Backup with Compass, is available from the IBM Cloud Catalog. The Shared Vault option is priced



www.cobaltiron.com



based on \$/GB/month of stored data after deduplication and compression of your IBM i data. There is no additional charge for the Compass VTL feature.

The Shared Compass Vaults are perfect for those wishing to deploy immediately and especially for smaller workloads and workloads in the IBM PowerVS Cloud. Note that for on-premises IBM i systems backing up to Shared Compass Vaults in the IBM Cloud, you must ensure proper network connectivity.

Optionally, Shared Compass Vaults in the IBM Cloud can be the replication targets for 2nd copies of backup data replicated from primary, Dedicated Compass Vaults.

To request an estimated Secure Automated Backup with Compass sizing, please provide your sizing information at the following link:

<https://www.cobaltiron.com/compass-ibm-sizing/>

Step 2: Provisioning a Dedicated Compass Vault

Dedicated Compass Vaults can be deployed either on-premises as physical appliances or in the cloud. If you going to use a Dedicated Compass Vault for your IBM i backups, the Cobalt Iron Customer Enablement and Systems teams will be working with you on the deployment of your Vault.

Step 3: Provisioning Secure Automated Backup with Compass

If you will be using Shared Compass Vaults in IBM Cloud (either for primary backup copies or for DR copies), you need to create the Secure Automated Backup with Compass service from your IBM Cloud account. You create the Compass service from your IBM Cloud account through the IBM Cloud Catalog at the following link:

https://cloud.ibm.com/catalog/services/secure-automated-backup-with-compass?catalog_query=aHR0cHM6Ly9jbG91ZC5pYm0uY29tL2NhdGFsb2c%2Fc2VhcmNoPWNvbXBhc3Mjc2VhcmNoX3Jlc3VsdHM%3D

The entire Compass backend infrastructure is already provisioned in IBM Cloud data center locations and ready to service your IBM i backups. When you provision Compass from the IBM Cloud tile, further Compass automation does the following (in about 15 minutes):

1. Creates a Compass VPC and connects it to your Local Transit Gateway (TGW)
 - a. If a Local Transit Gateway does not exist, Compass will create one for use.
 - b. If more than one Local TGW already exists, Compass automation will cycle through all of them and select the one most recently updated. If this is not the desired TGW for Compass use, please reconfigure to connect the Compass VPC to the desired TGW.
2. Creates VPEs and CSEs for secure, high-performance connectivity from your PowerVS workspace to the Compass Vaults using your private IP address range that you give as

input. The actual IP addresses needed to access the Compass Vaults are provided at the end of the provisioning.

3. Creates your specified organization name in the Compass Commander interface and provides single sign-on access to Commander through your IBM Cloud credentials.

Usage of the above IBM Cloud resources is included in the single Compass SaaS pricing – there are no additional charges for these cloud resources nor for use of Compass VTL. Instructions for creating the Secure Automated Backup with Compass service in the IBM Cloud is provided in the following video:

<https://www.youtube.com/watch?v=qdQ7y2dXwmU>

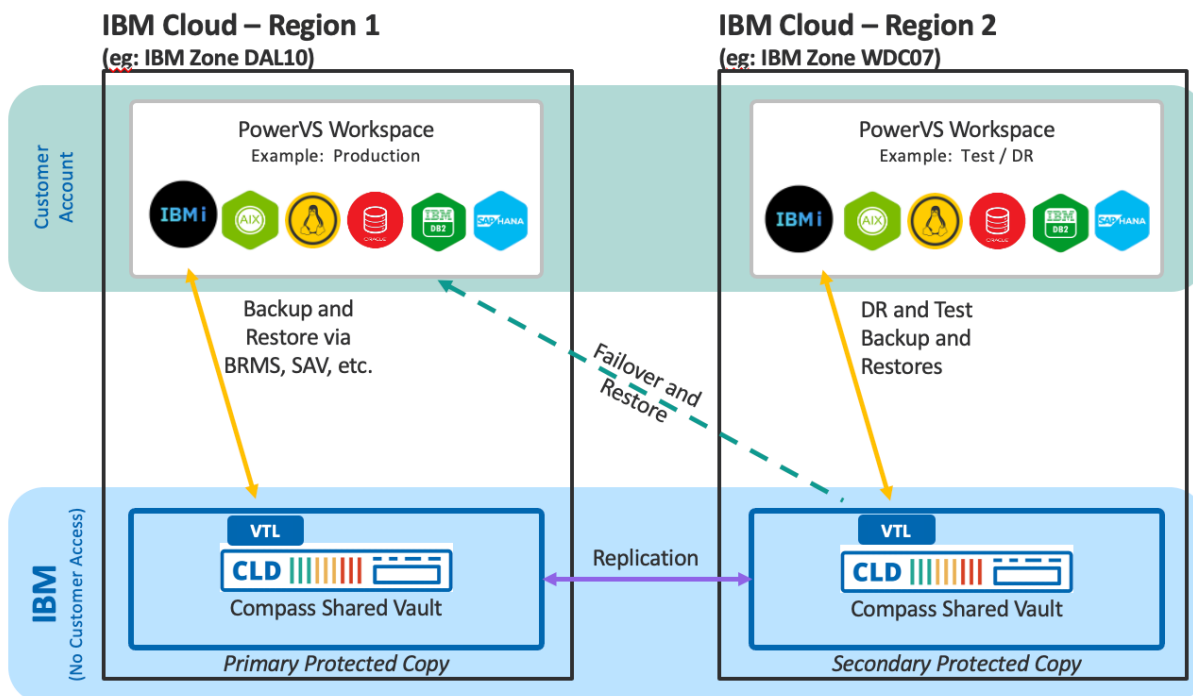
Prior to attempting to create the Secure Automated Backup service, validate the following:

1. The person provisioning Compass must have the proper IBM Cloud permissions (for example, writer or editor) for the IBM Cloud account that Compass is being provisioned from in order for Compass automation to create or edit the cloud resources mentioned above (ie, VPC, VPEs, CSEs).
2. A valid IBM Cloud API key is needed for Compass automation to invoke the IBM Cloud API. If a new Cloud API key is needed, review the following documentation:

https://cloud.ibm.com/docs/account?topic=account-userapikey&interface=ui#create_user_key

IBM i on PowerVS Data Protection Via Compass VTL

Shared Reference Architecture





Step 4: Configuring Network Connectivity to Compass Vaults

DEDICATED VAULTS

Dedicated Vaults in the IBM Cloud are deployed on in-account VPC resources. If you are running a Dedicated VPC Vault in the IBM Cloud, your PowerVS Workspace will connect to the Compass Vault via a local Transit Gateway.

If you are running a Dedicated physical Vault on-premises, you need to ensure IP connectivity from your IBM i systems to the Compass Vault.

For more complex network requirements, CI will work with your network team and cloud providers to architect the optimal network configuration.

SHARED VAULTS

If you are backing up IBM i workloads running in a IBM PowerVS workspace, your required IBM Cloud networking connectivity should be set up automatically by Compass when you provision Secure Automated Backup (previous step). In particular, Virtual Private Endpoints (VPEs) and Cloud Service Endpoints (CSEs) are created for secure, high-performance connectivity from your PowerVS workspace to the Compass Vaults using your private IP address range that you specified. Compass VTLs on IBM Cloud Shared Vaults are accessed through these VPE connections.

A specific IP address is assigned for each Compass Vault. These IP addresses are taken from the IP address range you specified when provisioning Secure Automated Backup. You will need the Compass Vault IP address when you configure IBM i for the Compass VTL (step 7 below). You can find the specific IP address assigned for your Compass Vault in your IBM Cloud Data Center by following these steps.

1. Go to the Cloud Resource List in your IBM Cloud account and go to the Storage category
2. Double click the Secure Automated Backup Compass cloud service
3. Click “Get Started”
4. Click “Step 2 – Setup Compass Name Resolution”

PERFORMANCE CONSIDERATIONS

The overall throughput performance for a CTG VTL will depend on many factors, primarily including:

1. Network bandwidth, latency, and congestion/utilization
2. Number of VTL drives driven in parallel
3. Ability of the VTL iSCSI initiator client/source system (eg, the IBM i system) to push the data to the VTL
4. Compass Vault workload and resources



To optimize VTL backup and restore throughput performance, it is important to fully understand all of the elements that constitute each of the above factors. The network topology and configurations can be complex and impact performance.

PERFORMANCE GUIDANCE

Cobalt Iron recommends the following for optimizing VTL performance:

1. The following frame settings are recommended for IBM i:
 - a. The maximum frame size for the line description should be set to 8996.
 - b. The MTU on the associated interface should be set to “*LIND”
2. The following guidance on iSCSI latency is provided for proper Compass CTG VTL processing.
 - a. Optimal iSCSI latency: 5ms or less
 - b. Acceptable: 5ms to 20ms
 - c. Problematic: 20ms and above
 - d. For larger data volumes, lower latencies are needed/required.

OTHER GENERAL GUIDANCE

Typical IBM i VTL workloads are deployed as one of two categories:

1. Dedicated Vaults
 - a. CTG VTL targets deployed on dedicated, in-account IBM Cloud Vaults
 - b. CTG VTL targets deployed on dedicated, on-premises Vault appliances
 - c. Accessed directly via customer on-premises or in-account IP connections and networking
2. Shared Vaults
 - a. CTG VTL targets on multi-tenant IBM Cloud shared Vaults
 - b. Accessed through a VPE connection

For IBM Cloud deployments, acceptable performance requires the source system and the VTL target Vaults to be in the same IBM Cloud data center. Where the source system can push a steady stream of data to the VTL target and in ideal conditions (see performance considerations), the configuration guidance would be as follows:

1. Dedicated Vaults
 - a. With a 20 Gbps or faster network interface to the VTL
 - b. Expect up to 200 MB/s throughput per drive
 - c. Utilize up to 6-8 drives in parallel for backup and restore activities.
2. Shared Vaults
 - a. With a 10 Gbps VPE network interface to the VTL
 - b. Expect approximately 100 MB/s throughput per drive
 - c. Utilize up to 4 drives in parallel for backup and restore activities

Additional drives may be used but overall throughput performance is less linear after 6-8 drives.



This guidance will be updated as Cobalt Iron continues to optimize VTL ingest performance and IBM Cloud networking configurations.

Step 5: Configuring a Compass VTL

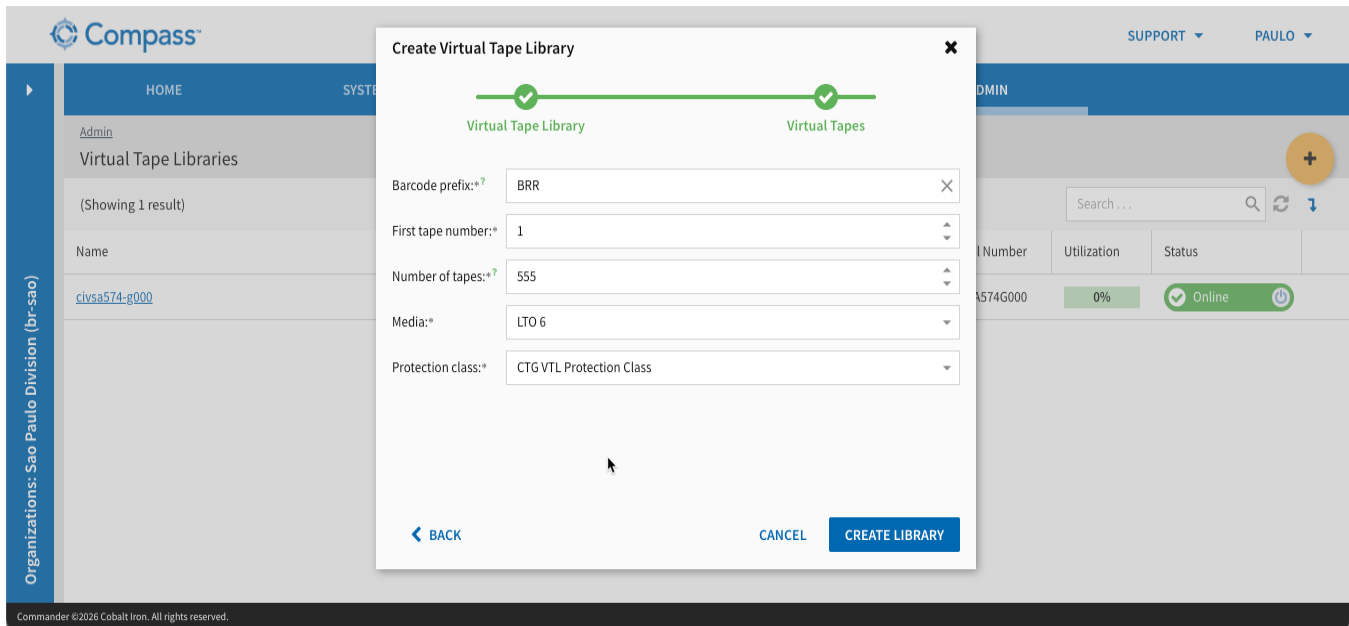
Commander is the web-based user interface for Compass where customers define their Compass VTL (either in Dedicated or Shared Vaults). You configure a Compass VTL using the Compass VTL Wizard in Commander.

To configure a VTL through Commander, navigate to the Virtual Tape Libraries tile in the Admin tab and click Add to open the Create Virtual Tape Library wizard. Alternatively, you can click Add in the Virtual Tape Libraries panel on the Accelerator Details page.

Enter the appropriate details in the Virtual Tape Library and Virtual Tapes sections of the wizard. Select “Compass 03584L32 (for IBM i)” for the Library Type and “Compass ULT3580-TD6” for the Drive Type from the selection menus. Then click Create Library. The Virtual Tape Libraries Details page is displayed to review your entries and enter any other required data. Please refer to the Cobalt Iron Compass Tape Gateway User’s Guide for more details on configuring a Compass VTL in Commander.

Note that customers using Shared Compass Vaults as part of Secure Automated Backup with Compass will have templates to choose from for defining the number of drives and the virtual tape volume size. Currently the template options are:

1. 1 Drive, 400GB Tapes
2. 2 Drives, 400GB Tapes
3. 4 Drives, 400GB Tapes
4. 1 Drive, 800GB Tapes
5. 2 Drives, 800GB Tapes.



Step 6: Configuring CHAP authentication for Compass VTL

Challenge-Handshake Authentication Protocol (CHAP) is an authentication protocol that is negotiated between an iSCSI initiator and target. In this case, your IBM i system is the iSCSI initiator and the Compass VTL on the Vault serves as the iSCSI target. IBM i supports one-way CHAP where the iSCSI target provides the inbound credentials to authenticate the initiator. CTG also supports mutual/bidirectional CHAP where (additionally) the initiator is configured with outbound credentials to authenticate the target.

When creating the Compass VTL in the Commander interface, the Target Configuration panel provides the target IP address, port information, and CHAP secret required for establishing iSCSI protocol authentication from the IBM i system. Upon VTL creation through Commander, these Target Configuration fields are populated by default. New iSCSI listeners can be added by clicking (+) in the Target Configuration panel header while in Edit mode.

Step 7: Configuring Your IBM i for Compass VTL Access

Once you have configured the Compass VTL on your target Compass Vault, you must attach the Compass VTL to your IBM i system as an iSCSI target device. Fibre Channel connectivity to the Compass VTL is not currently supported.



IBM Navigator for i is the preferred method for configuring iSCSI targets to IBM i. Detailed instructions for attaching a VTL to IBM i can be found at the following links:

- <https://www.ibm.com/support/pages/system/files/inline-files/IBM%20i%20Support%20for%20iSCSI%20VTL%201.8%200.pdf>
- <https://www.ibm.com/docs/en/i/7.6.0?topic=iscsi-creating-targets>
- <https://www.ibm.com/docs/en/i/7.6.0?topic=services-add-iscsi-target-procedure>

GENERAL GUIDANCE

Use the following Compass-provided fields as ADD_ISCSI_TARGET parameters:

- VTL Vault IP Address as the 'target-host-name' parameter.
 - o For Dedicated Vaults, this IP address is available in Commander by drilling into the Virtual Tape Library details, selecting the Primary tab, viewing the Target Configuration section, and selecting the VTL IP address from the Address field.
 - o For Shared Vaults, please use the IP address or hostname provided for the Compass Vault in your Cloud Data Center. This is obtained as described in step 4 above by going to the Storage category in the Cloud Resource List in your IBM Cloud account, drilling into the Compass service resource, then selecting "Get Started" and then "Step 2 – Setup Compass Name Resolution". Using this IP address will leverage the Compass provisioned VPE for the Compass Vault, resulting in better performance.
- VTL Port from Commander as the 'target-port' parameter
- CHAP secret from Commander as the 'initiator-chap-secret' parameter

Note: Fibre Channel-attached devices are immediately available to vary on and use after an IBM i system reboot. However, iSCSI-attached devices require TCP services which may take a few minutes to initialize after a reboot. If you perform an IBM i system reboot or startup, please delay a few minutes before attempting to vary on the Compass VTL or drives. This is to ensure TCP services on your IBM i system are fully up before attempting to vary on the Compass VTL which uses those services.

Step 8: Configuring Your IBM i for BRMS or SAV Backups & Restores

Once the Compass VTL is configured to your IBM i system, you are ready to perform BRMS, SAV, or other tape-based operations with Compass. The Compass VTL can be used like any other physical or virtual tape library.

Detailed instructions on use of IBM i Backup, Recovery, and Media Services (BRMS) are available at the following link:

https://www.ibm.com/docs/en/ssw_ibm_i_74/rzai8/sc415345.pdf

Detailed instructions on use of the IBM i Save (SAV) command are available at the following link:

<https://www.ibm.com/docs/en/i/7.4.0?topic=systems-using-save-sav-command>



Detailed instructions on using TCP/IP in Restricted State are available at the following link:
<https://fortradocs.atlassian.net/wiki/spaces/IWT/pages/165642515/Using+TCP+IP+in+Restricted+State>

Step 9: Performing DR Operations from Secondary Compass VTL

IBM i systems perform backups via BRMS or SAV operations to a primary Compass VTL residing on a Compass Vault. When replication is enabled, Compass automatically copies the VTL data to a secondary Compass VTL residing on a Compass Vault at a geographically separate DR site. In a disaster, IBM i at the DR site connects to this secondary VTL over iSCSI and performs full recovery operations

Step 10: Migrating Data to Compass from Legacy Tapes

Organizations may have Long Term Retention (LTR) data on volumes in legacy tape libraries that you want migrated into Compass. If this LTR data was written by BRMS, you can leverage the BRMS DUPMEDBRM command to duplicate data from a legacy tape volume to a new Compass tape volume. As part of volume duplication operations it is important to save media information for data governance tracking.

Additional instructions for using the DUPMEDBRM command can be found at the following link:
<https://www.ibm.com/support/pages/using-brms-duplicate-media>

Troubleshooting

How to Get Support

If you have more questions, you can contact IBM PowerVS Support (for IBM Cloud, IBM i, cloud permissions, or cloud connectivity issues) or Cobalt Iron Support (for Compass or VTL related issues), depending on your question.

If you are having an issue, here are items to gather that will be needed by support:

- SYSSNAP

You can reach IBM PowerVS Support at
[Contacting IBM PowerVS Support](#)

You can reach Cobalt Iron Support at
<https://support.cobaltiron.com>.

Note: User login required.

Common Customer Questions

1. What if I already have a Local Transit Gateway created on my IBM Cloud account?



- a. If no Local TGW exists, Compass will create one.
 - b. If a Local TGW already exists, Compass automation will connect to it.
 - c. If more than one Local TGW exists, Compass will connect to the one most recently updated. If this is not the correct TGW for backup, please connect the Compass VPC to the proper Local TGW.
2. What versions of IBM i does CTG support?
 - a. CTG supports IBM i 7.2 and later.
3. Are any PTFs needed for Compass VTL?
 - a. Yes, please see the “Pre-Requisites for Compass Tape Gateway VTL” section in this document.
4. Does my networking team need to be involved to provide IP Addresses?
 - a. IP addresses for connectivity to Compass Vaults are selected from the private IP address range provided when provisioning the Secure Automated Backup service.
 - b. Your networking team may need to be involved to help you select the IP address range to use when provisioning. The network may also be needed if there are issues on your network connecting to the Compass Vaults.
5. How are IP addresses arrived at?
 - a. You will need to provide a private IP address range when provisioning Secure Automated Backup for Compass to use. This IP address range should not be in use for any other purposes.
 - b. Compass will use specific IP addresses from this range to assign to Shared Compass Vaults.
 - c. How to obtain the specific IP addresses Compass assigns is described in the “Step 4: Configuring Network Connectivity to Compass Vaults” section in this document.
6. Can I have multiple VTLs?
 - a. Yes, you can have multiple Compass VTLs on a Compass Vault for various purposes. The Compass Vault in use must have sufficient resources to support multiple VTLs.
7. Can I migrate data from my existing tapes into the Compass Vault?
 - a. If your existing tapes were written by BRMS, you can leverage DUPMEDBRM to make copies of tapes into Compass.
 - b. See the “Migrating Data to Compass from Legacy Tapes” section in this document for more details.
8. Can it do bare metal recovery ?
 - a. Yes, Compass VTL supports IPL-able d-mode
9. How many tape drives should I define in my Compass VTL? And what size virtual tape volumes should I define?



- a. Customers using a Shared Compass Vault through the Secure Automated Backup with Compass will have preset tape and virtual volume configuration templates to choose from. Currently the templates you can choose from are:
 - i. 1 Drive, 400GB Tapes
 - ii. 2 Drives, 400GB Tapes
 - iii. 4 Drives, 400GB Tapes
 - iv. 1 Drive, 800GB Tapes
 - v. 2 Drives, 800GB Tapes
 - b. Customers using a Dedicated Compass Vault can work with the Cobalt Iron Customer Enablement team to determine best number of drives and tape volume size. Typically, the number of drives and tape volume size would be based on what you currently are using.
10. Are there limits on the number of drives, volumes, or slots I define?
- a.
11. Are different COS instances maintained for production and DR sites?
- a. Yes, each Compass Vault uses its own COS bucket to provide separate, isolated, security zones for backup data.
12. How to architect to restore from different zones?
- a. Compass supports a variety of recovery scenarios. You can reach out to the Cobalt Iron Customer Enablement team to discuss options.
13. Can data be replicated to another location for DR?
- a. Yes, Compass can replicate copies of all backup data to a 2nd replication target Compass Vault at another location. Replication typically runs on a daily basis after normal backup window.
14. Is replication based on IP communication? How big is the pipe?
- a. Yes, Compass replication operations are based on secure IP communications. The size of the replication pipe varies based on the data center locations. Compass leverages the IBM Cloud network backbone for high speed and low latency operations.