

WHITE PAPER

FortKnox for NetBackup

Security Design

Version 3.0



ABSTRACT

An overview of the security model and attributes for FortKnox for NetBackup.

TABLE OF CONTENTS

Introduction	3	Network / Hardware Requirements	11
Role-based access control (RBAC)	4	Azure, GCP and AWS IP Ranges	12
How FortKnox for NetBackup Communicates with NetBackup	5	Alternate Network Connections	12
FortKnox for NetBackup Security Fundamentals and Architecture	6	Azure ExpressRoute with Microsoft Peering	12
Data Security	7	Microsoft vNet Peering	12
Data In Transit	7	Connecting to FortKnox for NetBackup Storage with ExpressRoute	13
Data-at-rest	7	Ports	14
Immutability/WORM Storage	9	AWS	15
Data Deletion	9	Other helpful FAQs	16
Data Handling	10	Conclusion	17
		Sources	17
		About Cohesity	18

Introduction

Data isolation is a crucial component of a comprehensive backup strategy designed to protect against cybersecurity threats, power outages, human error, and natural disasters. The 3-2-1 rule is a widely accepted industry best practice for data protection and recovery. By having three copies of data on two different media, with one stored off-site, organizations gain a simple yet highly effective strategy to ensure data resilience and availability in the face of cyberattacks, hardware failures, or natural disasters. In the past, data has been isolated using magnetic tape, which was then shipped off-site to create a true “air gap.” However, to meet the more stringent RPO and RTO requirements of the modern cloud era, companies must have a secure data vault, either on-premises or in the cloud, with data managed under third-party custodianship to create a modern air gap.

FortKnox for NetBackup is a cloud-based storage platform for enterprise organizations to centrally manage secondary and tertiary copies of backup data. FortKnox for NetBackup customers can protect their NetBackup compressed and de-duplicated data in a secure Cohesity tenant hosted in multiple Cloud Service Provider’s (CSP). Most CSPs have adopted a “shared responsibility model” which makes it clear that the providers will not take any action to protect customers’ data. The job of protecting the data in the CSP is completely the responsibility of the customer. Customers who adopt FortKnox for NetBackup are seeing the following results: complete backup and recovery of all their application data, fast and flexible data recovery, and secure and flexible provisioning.

Role-based access control (RBAC)

FortKnox for NetBackup is integrated tightly into NetBackup, and NetBackup provides the ability to apply role-based access control (RBAC) in your environment. Use RBAC to provide access for users that do not currently have access to NetBackup. Or, for current NetBackup users with administrator access, you can provide limited access and permissions, based on their role in your organization.

The following are relevant roles included with NetBackup for FortKnox for NetBackup:

1. Administrator

- a. This role has permissions to perform all actions within the NetBackup Web UI.

2. Default Security Administrator

- a. This role has permissions to manage NetBackup security, including RBAC, certificates, hosts, identity providers and domains, global security settings, and other permissions. This role can also view settings and assets in most areas of NetBackup, including workloads, storage, licensing, and other areas.

3. Default Storage Administrator

- a. This role has permissions to configure and manage disk-based storage and cloud storage.

Either the Storage Administrator or the Backup Administrator must perform the modifications to the MSDP storage to add a cloud tier. The Security Administrator may also be involved if a new media server is involved as part of the preparation of the environment to add FortKnox for NetBackup. Security Administrators do not have the required permissions to see or modify storage configurations.

How FortKnox for NetBackup Communicates with NetBackup

NetBackup Primary Server, Media servers, and clients communicate with each other using TLS architecture that conforms to the X.509 Public Key Infrastructure (PKI) standard in the form of certificates, either managed by the Primary server or managed by an External Certificate Authority. This is a common form of endpoint verification on the web, as well. Cloud providers will also have their own certificates for TLS encrypted communication. Communication and data transmission between the NetBackup Deduplication engine and the cloud tier leverages this same trust of the cloud vendor certificates. Our Cloud Provider package reflects the currently supported cloud solutions.

Ensure secure communication with the media server hosting MSDP, according to the procedures in the NetBackup Security & Encryption Guide. Communication to AWS or Azure for FortKnox for NetBackup is handled by the Cloud Provider package, where the certificates are already trusted by NetBackup. The version of the Cloud Provider package is aligned to the version of NetBackup.

When setting up the cloud tier for MSDP, after the storage account information has been added, additional security settings are available in the Advanced section. By default, SSL is enabled, and this is also where to toggle immutability using object lock

FortKnox for NetBackup Security Fundamentals and Architecture

FortKnox for NetBackup uses Media Server Deduplication Pool cloud tier (MSDP-C) to directly write deduplicated data to cloud object storage from memory. No additional gateway server is required, as the cloud tiering functionality is built directly into NetBackup.

Unlike self-managed cloud storage that is also supported by NetBackup, the storage used by FortKnox resides in the Cohesity tenant of the chosen CSP. Cohesity manages cloud object storage and each customer has their own storage account as a sub-tenant. Storage buckets are not shared across multiple customers, and all customer data remains completely isolated from other customers. In addition, a customer may choose to set IP restrictions on

their FortKnox access. Communication to the external storage bucket requires port 443 to be opened outbound so the NetBackup API can communicate with the cloud providers storage bucket through HTTPS.

The FortKnox for NetBackup underlying cloud storage is provided by third parties, such as Microsoft Azure, Google Cloud Platform (GCP) and Amazon Web Services (AWS). When provisioning FortKnox for NetBackup, customers select the CSP and physical regions where the backup data is hosted. Cohesity does not make copies or replicate your data. Cohesity also does not have access to customer data in an unencrypted format, as encryption keys are managed separately by the customer.

Data Security

Security of your data is paramount to Cohesity. Customer data is categorized as “Highly Confidential” and encrypted at all times in transit. The service transmits using TLSv1.2 and stores all customers’ encrypted data in FortKnox storage using AES 256 cipher modules.

Any credentials stored within the NetBackup database are hashed and can also be stored using FIPS 140-2 cryptography modules.

Note: FIPS 140-2 is only supported on Windows.

Available in NetBackup 10.3 and later, NetBackup can scan the stored FortKnox for NetBackup backups for malware using the built-in NetBackup Malware Scanner or third-party malware scanner integrations using customer-provided Microsoft Defender or Symantec’s Protection Engine. When a customer wishes to perform a recovery, the NetBackup users can visually see in the backup history if the data being restored was identified as infected with malware prompting several alerts as an effort to prevent reinfection.

Data In Transit

Data Channel in Transit Encryption (DTE) is an option within the NetBackup boundaries to negotiate TLS encrypted paths for the data channel. The data is not modified in this scenario, and there is no impact to deduplication rates. This feature requires NetBackup clients at 9.1 or higher. By default, this feature is off, but can be configured with global options or for specific clients.

- **Preferred Off (default):** Specifies that the data-in-transit encryption is disabled in the NetBackup domain. This setting can be overridden by the NetBackup client setting.

- **Preferred On:** Specifies that the data-in-transit encryption is enabled only for NetBackup 9.1 and later clients. Configuring data-in-transit encryption (DTE) 363 Configure the global data-in-transit encryption setting This setting can be overridden by the NetBackup client setting.
- **Enforced:** Specifies that the data-in-transit encryption is enforced if the NetBackup client setting is either ‘Automatic’ or ‘On’. With this option selected, jobs fail for the NetBackup clients that have the data-in-transit encryption set to ‘Off’ and for the hosts earlier than 9.1

DTE is supported for MSDP storage, and “Use SSL” is a default and recommended option for the blob or bucket.

The data path between the customer’s NetBackup installation of MSDP and the CSP should utilize the endpoints according to the desired transmission route, with considerations to name resolution and firewall ports to allow NetBackup Deduplication traffic. For more information, see the NetBackup Network Ports Reference Guide. Additional security concerns for this segment of communication are outside Cohesity’ span of control.

Data-at-rest

NetBackup data stored in FortKnox for NetBackup is storage-optimized using MSDP deduplication and uses a combination of Data Encryption Keys wrapped with Key Encryption Keys. The Key Encryption Keys can be provisioned within NetBackup’s built-in Key Management System (nbkms), or from an external KMS that supports the KMIP protocol. NetBackup uses AES256-bit encryption and also supports [FIPS140-2 cryptography modules](#) when writing the data to FortKnox for NetBackup Object storage (backed by Azure).

Note: FIPS 140-2 is currently only supported on Windows.

Using KMS with MSDP is set at the time of storage server creation and adding KMS to an existing storage server is not supported.

NetBackup Encryption keys can be rotated as needed, while external KMS vendor solutions offer their own controls to rotate keys. NetBackup KMS can be operated in the FIPS mode, wherein the encryption keys that you create are always FIPS 140-2 approved.

Enabling encryption using the `pd.conf` file is not recommended. Use the `contentrouter.cfg` for these configuration changes.

Enable encryption on the storage server at the time of creation, or else configure this option in the configuration file:

```
[storage location]/etc/puredisk/  
contentrouter.cfg
```

Edit with the following:

```
ServerOptions=verify_so_references,fast,  
encrypt
```

Authentication with external KMS server uses security certificates. During each operation, NetBackup presents the certificate to the external KMS. eKMS validates the certificate and performs that operation if the user has the required permissions.

Data stored at rest in Azure is encrypted using Azure's Storage Service Encryption with Microsoft-managed keys. In AWS, data at rest is encrypted with Amazon S3-managed keys (SSE-S3). On GCP, data is stored at rest using GCP-managed keys.

Immutability/WORM Storage

Immutability/WORM (Write Once Read Many) storage is utilized and required in FortKnox for NetBackup. In addition, immutability needs to be enabled on the media server that will be the MSDP-C storage server. FortKnox does not allow data to be stored in a non-immutable format, and once data is written to FortKnox it cannot be deleted until its retention period has passed.

Note: For more information on immutability refer to the NetBackup Deduplication Guide: [Introducing the NetBackup media server deduplication option | NetBackup™ Deduplication Guide](#) | Please Note: users must create retention policies carefully because once data is stored in FortKnox, it cannot be deleted prior to the expiration data that is set at the time that the data is written.

Data Deletion

Data is retained until the service is cancelled, terminated or suspended for non-payment.

Unless otherwise prohibited by law or court order, decommissioned FortKnox for NetBackup Customer Data will be deleted in accordance with Cohesity' standard deletion practices.

Customer data is stored in Azure, GCP or AWS. The customer manages their own data retention via NetBackup policies. When data is deleted, the CSP performs erasure and disposal according to their standards:

Azure: "Data deletion" is discussed on page 21 in the Data Protection in Azure document:
<https://go.microsoft.com/fwlink/p/?LinkId=2114156&clcid=0x409&culture=en-us&country=US>

GCP: Data Deletion on Google Cloud: <https://docs.cloud.google.com/docs/security/deletion>

AWS: Discusses the various methods to delete data located in AWS S3 buckets.
<https://aws.amazon.com/premiumsupport/knowledge-center/s3-delete-objects-and-buckets/>

Data Handling

Cohesity has a policy that details how information is classified with appropriate controls. The Cohesity Information Classification and Handling Method specifies the requirements for classifying, labelling, and protecting data. Information is classified by its value, legal requirements, sensitivity, criticality to the organization and information handling protocol for the different types of information classification. Cohesity data is classified as Public, Confidential or Highly Confidential based on the above factors.

Customer data is treated as Cohesity Highly Confidential and restricted to a subset of Employees and contractors handling customer data following the least privilege rule. The least privilege rule means all access is denied except which is specifically granted by management. Access is granted to individual user accounts performing roles which have limited responsibilities to perform their jobs

All parties who contractually provide services on behalf of Cohesity are required to meet security policy standards of Cohesity.

Network / Hardware Requirements

NetBackup writes to FortKnox for NetBackup using a NetBackup MSDP-C server. Hardware requirements for the MSDP role on the media server are:

- **Hardware requirements for block storage only MSDP pool** - No change from NetBackup MSDP guidance. Max capacity is 960 TB for the NetBackup Appliance, and 400 TB for BYO MSDP.
- **Hardware requirements for object storage only pool** - Max capacity of 1 PB and 196 GB of memory. The default is 1 TB of available local storage per cloud Logical Storage Unit (LSU), and the overall file system utilization should not exceed 90% full.

- **Hardware requirements for mixed object and block storage** - Similar hardware requirements as local storage only pool. Total max capacity is 1.2 PB.
- **Operating system** - Cloud LSUs can be configured on the storage servers running on Red Hat Linux Enterprise or CentOS platforms. No platform limitations for clients and load-balancing servers.

The FortKnox for NetBackup network capacity will depend greatly on the amount of data that is being sent offsite and the speed at which it needs to arrive at the cloud provider. FortKnox for NetBackup does require port 443 to be opened outbound so it can communicate through HTTPS to the cloud provider.

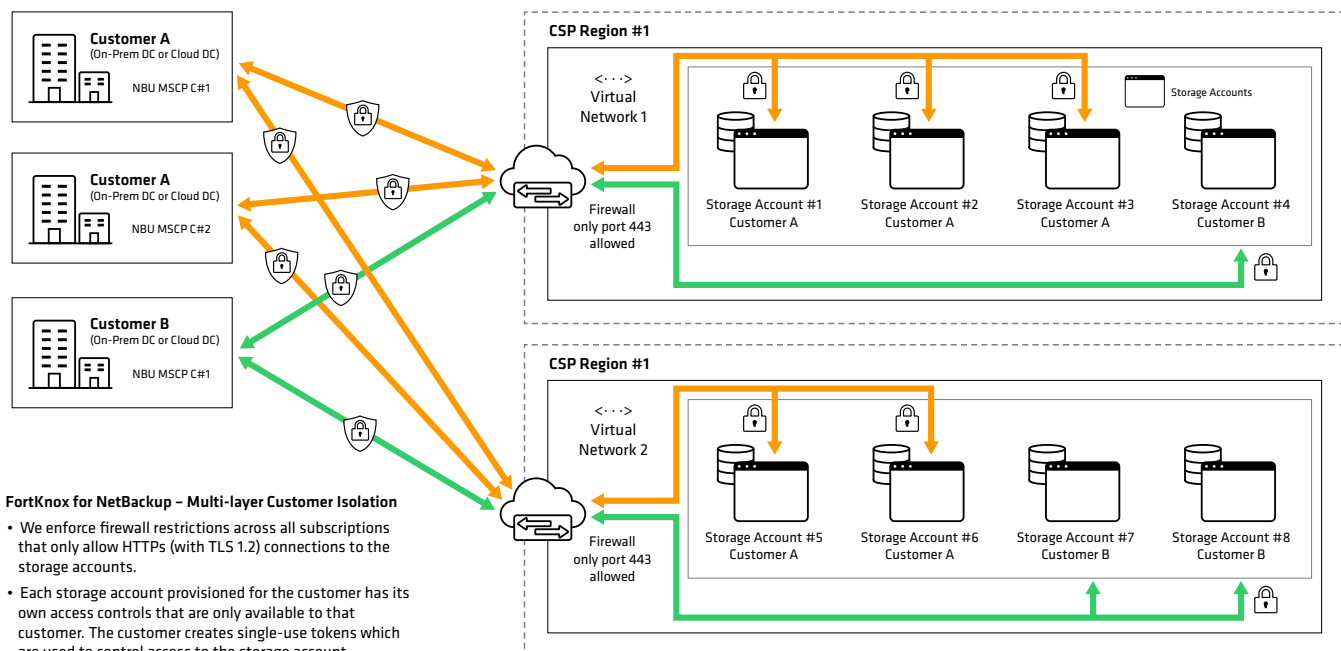


Figure 1. FortKnox for NetBackup – Storage Isolation and Security Design

Azure, GCP and AWS IP Ranges

For customers that want to whitelist the AWS and/or Azure IP ranges to connect to Microsoft and/or Amazon, please refer to the following sites:

Azure: <https://www.microsoft.com/en-us/download/confirmation.aspx?id=56519>

AWS: <https://docs.aws.amazon.com/general/latest/gr/aws-ip-ranges.html>

GCP: [Subnets](#) | [Virtual Private Cloud](#) | [Google Cloud Documentation](#)

Alternate Network Connections

Cohesity is aware that standard internet-routed connectivity methods may not meet every individual customers' requirements. Cohesity supports the following alternative connection methods other than HTTPS with outbound port 443.

Azure ExpressRoute with Microsoft Peering

Connectivity to FortKnox for NetBackup in Azure over ExpressRoute depends on the endpoint type used:

- 1) If the service is exposed via **Azure Private Endpoint**, customers should use **ExpressRoute Private Peering**.
- 2) If access relies on public service endpoints, connectivity may require **ExpressRoute Microsoft Peering** with appropriate route filters. This approach is not supported by Microsoft for all customers, and requires a special request and approval by Microsoft.

Private Endpoint-based connectivity is the preferred model as it keeps traffic on private networks and avoids public exposure.

The differences are described on Microsoft's site: <https://docs.microsoft.com/en-us/azure/expressroute/expressroute-circuit-peering>

Microsoft vNet Peering

Cohesity does not support using Microsoft vNet Peering for FortKnox for NetBackup.

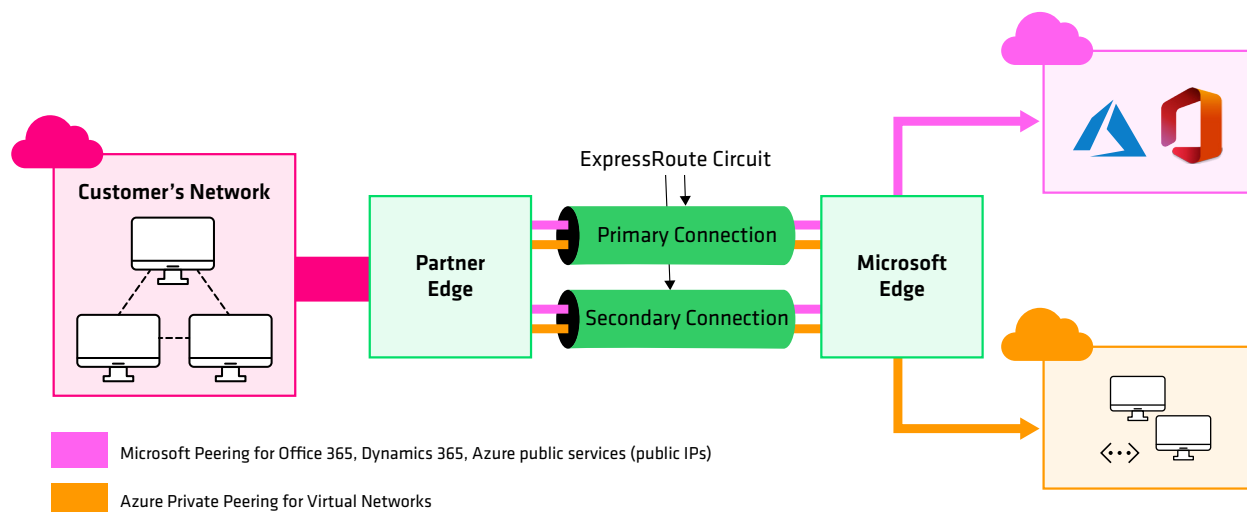


Figure 2. Microsoft ExpressRoute configuration compatible with FortKnox for NetBackup.

Connecting to FortKnox for NetBackup Storage with ExpressRoute

The following is an abbreviated list of steps that are needed to connect to FortKnox storage.

Note: Once configured, Azure ExpressRoute is transparent to FortKnox and NetBackup.

When requesting storage from Cohesity, your FortKnox for NetBackup storage buckets, created by Cohesity, will have immutability enabled. All NetBackup Cloud Storage Units must be created with Governance mode immutability enabled to ensure data is written in an immutable format.

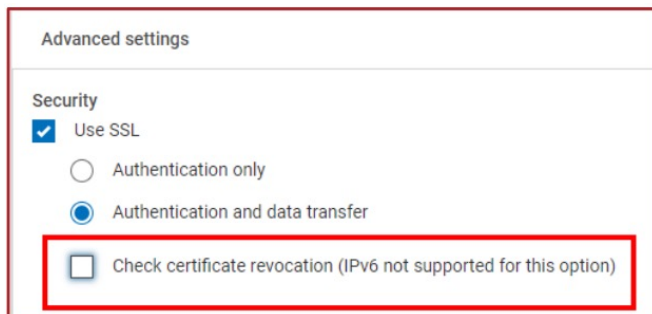
Immutability gives you the ability to write once, and read many (WORM), to your FortKnox storage and select how long you would like the images to be retained. In the event of a threat actor/malware compromise, immutability prevents the threat actor from expiring your backup images in FortKnox or manipulating the data in any way.

Note: This document is based on NetBackup 10.2 or later.

Ports

Communication to the external storage bucket requires port 443 to be open outbound so the NetBackup API can communicate with the storage bucket through HTTPS. If outbound port 443 cannot be opened for security concerns, a proxy server can be added.

Note: It is a best practice that both DNS and NTP can resolve correctly. Cohesity checks for certificate revocation to ensure the certificates are valid, which means that port 80 needs to be opened outbound on the MSDP-C/storage server unless you do not wish to check for certificate revocation. To remove this certificate validation (not recommended), simply uncheck certificate revocation when creating the disk pool.



Advanced settings

Security

☒ Use SSL

☐ Authentication only

☒ Authentication and data transfer

☐ Check certificate revocation (IPv6 not supported for this option)

Communication to the external storage bucket requires port 443 to be open outbound so the NetBackup API can communicate with the storage bucket through HTTPS. If outbound port 443 cannot be opened for security concerns, a proxy server can be added.

Note: It is a best practice that both DNS and NTP can resolve correctly.

Cohesity checks for certificate revocation to ensure the certificates are valid, which means that port 80 needs to be opened outbound on the MSDP-C/storage server unless you do not wish to check for certificate revocation. To remove this certificate validation (not recommended), simply uncheck certificate revocation when creating the disk pool.

AWS

AWS Direct Connect links your internal network to an AWS Direct Connect location over a standard Ethernet fiber-optic cable. One end of the cable is connected to your router, the other to an AWS Direct Connect router. With this connection, you can create virtual interfaces directly to public AWS services (for example, to Amazon S3) or to Amazon VPC, bypassing internet service providers in your network path. An AWS Direct Connect location provides access to AWS in the Region with which it is associated.

You can use a single connection in a public Region or AWS GovCloud (US) to access public AWS services in all other public Regions.

Please review the AWS guide on setting up a route filter for prefixes: <https://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html>

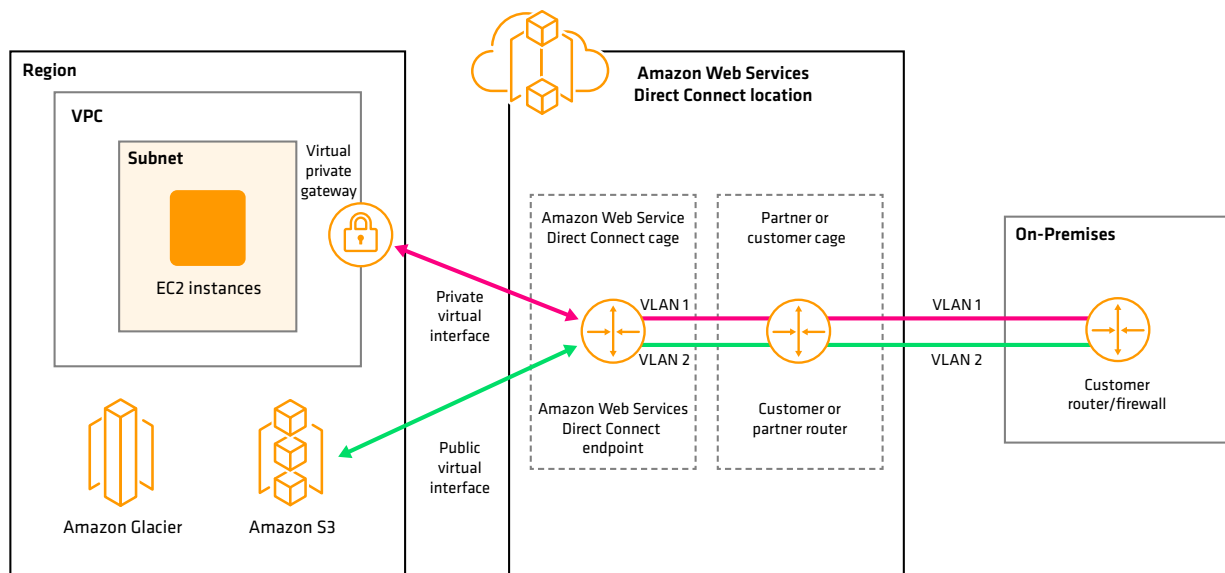


Figure 3. AWS Direct Connect compatible with FortKnox for NetBackup.

Other helpful FAQs

Q – *If a user needs to free up space in FortKnox for NetBackup, is it possible to shorten the retention of older backups to reduce storage consumption?*

A - Once data is written, the retention period is set and cannot be shortened. This is an important security feature of FortKnox, and requires that great care be taken when setting up the retention period as part of a backup policy.

Q - *In the FortKnox for NetBackup technote 'FortKnox for NetBackup (Cohesity.com) there is a caution to not leave I/O streams unlimited, is there any guidance on what limit to set? https://www.Cohesity.com/support/en_US/article.100051821*

A - If “Limit I/O streams” is left cleared, the default value is Unlimited and may cause performance issues. Start low and work your way up. Start with 2, and see what performance looks like, and adjust. Once you are saturating your connection, there is no gain to adding more streams.

Q - *Does FortKnox for NetBackup provide network bandwidth for throttling for replication of data to FortKnox for NetBackup?*

A – Yes. NetBackup utilizes MSDP-C to write to FortKnox for NetBackup. The user would have all the same network options as they would any other MSDP-C target, including throttling.

Q - *Can FortKnox for NetBackup be integrated into the existing environment without major changes?*

A – Yes. You should be able to tier data to FortKnox for NetBackup without disrupting the current environment. MSDP-C doesn't require a lot of local disk, and in most cases no dedicated servers need to be added.

Q - *Do we use a Push model from NBU to FortKnox for NetBackup or is it a pull model over port 443?*

A - All data movement is driven by native NetBackup operations. FortKnox for NetBackup is standard object storage target from the perspective of NBU.

Conclusion

Cohesity FortKnox for NetBackup offers a single, flexible, and secure offsite repository for all your data sources. Through its seamless integration with NetBackup, FortKnox for NetBackup simplifies cloud storage as a service, delivering limitless scale without compromising security or compliance.

Sources

[NetBackup Security and Encryption Guide](#)

[NetBackup Backup Planning and Performance Tuning Guide](#)

[Azure Locations](#)

[ExpressRoute Circuits and Peering](#)

[Download Azure IP Ranges and Service Tags](#)

[Virtual Network Pricing](#)

[ExpressRoute or Virtual Network VPN – What's right for me?](#)

[AWS Locations](#)

[AWS IP Address Ranges](#)

[What is AWS Direct Connect](#)

[Cohesity FortKnox for NetBackup Deployment Guide](#)

[Announcing Default Encryption for Azure Blobs, Files, Table and Queue Storage](#)

About Cohesity

[Cohesity](#) is a leader in AI-powered data security and management. Aided by an extensive ecosystem of partners, Cohesity makes it easier to protect, manage, and get value from data – across the data center, edge, and cloud. Cohesity helps organizations defend against cybersecurity threats with comprehensive data security and management capabilities, including immutable backup snapshots, AI-based threat detection, monitoring for malicious behavior,

and rapid recovery at scale. Cohesity solutions are delivered as a service, self-managed, or provided by a Cohesity-powered partner. Cohesity is headquartered in San Jose, CA, and is trusted by the world's largest enterprises, including six of the Fortune 10 and 42 of the Fortune 100.

Visit our [website](#) and [blog](#), follow us on [Twitter](#) and [LinkedIn](#) and like us on [Facebook](#).

© 2026 Cohesity, Inc. All rights reserved.

Cohesity, the Cohesity Logo, and other Cohesity Marks are trademarks of Cohesity, Inc. or its affiliates in the US and/or internationally. Other names may be trademarks of their respective owners. This material (a) is intended to provide you information about Cohesity and our business and products; (b) was believed to be true and accurate at the time it was written, but is subject to change without notice; and (c) is provided on an "AS IS" basis. Cohesity disclaims all express or implied conditions, representations, warranties of any kind.

COHESITY

[cohesity.com](#)

1-855-926-4374

2625 Augustine Drive, Santa Clara, CA 95054

2000106-001-EN 9-2026