# IBM Storage Virtualize: Secured Data Replication with IPsec

Enable and manage encryption of data in flight for remote copy over IP network.



## Table of contents

Glossary	3
Overview	4
Intended audience and scope	4
IBM Storage Virtualize data replication services	5
Introduction to IP security	8
Overview of IPsec for IP replication	9
Pre-requisites to form secured IP partnerships	11
Configure secured IP partnership	12
Switch between unsecured and secured IP partnerships	27
Verify secured status of a partnership	29
Troubleshooting	31
Summary	33
Get more information	33
About the authors	34
Acknowledgments	34

## Glossary

Term	Definition
Storage Virtualize	IBM's modular storage appliance that provides symmetric virtualization. Can also be referred as SVC, IBM Storage FlashSystem or Spectrum Virtualize
SVC	SAN Volume Controller
EDIF	Encryption of Data in Flight
SVPC	IBM Spectrum Virtualize for Public Cloud
СА	Certificate Authority
ICA	Intermediate Certificate Authority
IPsec	Internet Protocol security
IKE	Internet Key Exchange is one of the IPsec protocols used for key exchange
ESP	Encapsulation Security Payload is one of the IPsec protocols
РКІ	Public Key Infrastructure
DH Group	Diffie-Hellman Group
ISC	Internally Signed Certificate
ESC	Externally Signed Certificate
CSR	Certificate Signing Request

## Overview

#### Challenge

IP Replication traffic traverses WAN links over long distances, exposing it to security threats like eavesdropping, sniffing, repudiation, and replay attacks across untrusted networks.

#### Solution

IBM Storage Virtualize implements a solution utilizing the IPsec protocol, an industrystandard for IP communications. This solution offers robust encryption, integrity algorithms, peer authentications, and advanced features including Access Control, Perfect Forward Secrecy, Replay Protections, and more.

This white paper introduces an IBM<sup>®</sup> Storage Virtualize solution that enables creation of a secured IP partnership between two partner systems over native IP links. It details out the planning considerations, certificate-based authentication, configurations steps along with the deployment scenarios.

## Intended audience and

## scope

This document aims to provide configuration information for establishing secure IP partnerships, specifically targeting first-time readers who are IBM Spectrum Virtualize users and administrators. However, it is equally beneficial for developers and testers. To fully benefit from this technical paper, readers should possess a basic understanding of the following prerequisites:

- IBM Storage Virtualize range of products.
- Installation of IBM System Storage<sup>®</sup> SAN Volume Controller (SVC) or IBM Storwize<sup>®</sup> systems with IBM Spectrum Virtualize software that supports IP replication. Additionally, they should have basic knowledge of configuring Ethernet connections, switches, and related components.
- Familiarity with the fundamentals of the IP replication feature is also essential.

## IBM Storage Virtualize data replication services

IBM Storage Virtualize offers Remote Copy services to manage partnerships between systems. These services are commonly used for volume data copying, facilitating migration, disaster recovery, and high availability. In Remote Copy, relationships are established between a master volume and an auxiliary volume, with the master volume typically receiving data from host applications. Updates are then copied to the auxiliary volume, allowing the system to maintain multiple backup copies of the data. Consistency Groups can be utilized to ensure consistent copies when data dependencies exist across hosts or volumes.

The Remote Copy function supports various types of remote copy operations:

### Metro Mirror (MM)

MM creates a synchronous copy of data from a master volume to an auxiliary volume. Both volumes have identical data upon completion, but performance on host applications may be impacted due to the synchronous nature of the copy operation over remote distances.

## Global Mirror (GM)

GM remote copy provides an asynchronous copy process. With asynchronous copy, confirmation of I/O completion is received before the write operation is completed for the copy on the auxiliary volume when host applications write to master volumes.

# Global Mirror with Change Volumes (GMCV)

GMCV also offers asynchronous copy operations between master and auxiliary volumes for disaster recovery. In GMCV, a separate volume is created to track changes, and copy-on-write technology is employed to maintain a consistent image of the primary volume for the background copy process to read. GMCV eliminates the risk of missing updates that can occur when using Global Mirror without change volumes.

### Policy Based Replication (PBR)

PBR is a preferred method for simplified configuration and management of asynchronous replication between two systems. It utilizes volume groups and replication policies to automate the deployment and management of replication. PBR greatly simplifies configuration, management, and monitoring of replication between systems. For detailed information on PBR, refer to <u>Getting started with policy-based replication</u> on ibm.com.

### Need for secured IP replication

Secured IP replication is necessary due to the inherent security threats associated with IP replication traffic traveling over long distances on untrusted WAN links. These threats include eavesdropping, sniffing, repudiation, and replay attacks through untrusted networks. To address these risks and ensure data confidentiality, data integrity, and peer authentications, a robust solution is required. Users can select any of the remote copy operations mentioned earlier according to their requirements and secure all replication traffic from potential threats or vulnerabilities.

### Secure IP replication deployments

IBM Storage Virtualize introduced Encryption of Data in Flight (EDIF) support starting from the 8.5.2.0 (22Q3) release to secure IP replication deployments. Following are the existing use cases where Remote Copy over IPsec is supported:

#### **IP** partnerships

The introduction of EDIF ensures the security of all replication traffic flowing between two Storage Virtualize endpoints.



Secured IP Partnership

Figure 1. Secured IP partnership.

IBM Storage Virtualize, utilizing EDIF, supports the secure establishment of multiple IP partnerships. These secured partnerships enable the formation of connections between one primary site and up to three different auxiliary sites.



3 Multi-IP Secured Partnerships

#### Partnership with Spectrum Virtualize Public Cloud (SVPC)

Starting from the 8.5.2.0 (22Q3) release, IBM Storage Virtualize also provides EDIF support in SVPC. This allows the formation of secured IP partnerships between traditional on-premises Storage Virtualize systems and Spectrum Virtualize for Public Cloud.



IPsec Replication between Traditional Storage Virtualize and SVPC

Figure 3. IPsec replication between traditional storage virtualize and SVPC.

Figure 2. Multi-IP secured partnership.

# Introduction to IP security

Internet Protocol Security (IPsec) is a framework that establishes secure communications between two entities. It is used to ensure confidentiality, integrity, and authentication in communications, particularly between trusted private networks across an untrusted network like the internet. IPsec operates at the IP layer, transparent to the transport layer (TCP/UDP) and applications, eliminating the need for software changes in applications to establish secure communications.

The following figure illustrates the structural representation of the IPsec architecture.



Figure 4. IPsec architecture.

The IPsec architecture consists of the following components:

**Authentication Header (AH)** protocol provides data integrity, encryption, and anti-replay but not encryption itself.

**Encapsulating Security Payload (ESP)** protocol offers data integrity, encryption, authentication, and anti-replay. It also authenticates the payload.

**Combined algorithm** identifier supports both AH and ESP protocols, utilizing encryption and integrity protection algorithms together.

**IKE/IPsec protocols** establish an IPsec tunnel between endpoints, security parameters such as allowed IPs, encryption algorithms, crypto key materials, and authentication mechanisms. IKE functions as the control channel, while IPsec operates as the data channel.

**Security Association (SA)** serves as a contract between the communicating hosts, specifying the agreed-upon and shared security attributes. An IKE SA is initially established and is used to negotiate IPsec parameters and create an IPsec SA (Child SA). Both IKE and IPsec SAs are uniquely identified by Security Parameters Index (SPI) identifiers.

# Overview of IPsec for IP replication

This paper focuses on the data replication over IP involving the Storage Virtualize partner systems as the two separated peers (endpoints) seeking a secure network solution in the presence of an untrusted network.



Figure 5. IPsec based secured IP replication.

When replicating data over Ethernet, it traverses long distances hop-by-hop via WAN links, which are inherently insecure. Therefore, the security of IP partnerships becomes crucial to mitigate the risk of data manipulation or interception by hackers in untrusted networks. Secured IP partnerships leverage IPsec protocols to enable enhanced mutual authentication and ensure the confidentiality and integrity of replicated data.

Secured IP partnerships establish mutual authentication between the peers by negotiating security parameters and exchanging encryption keys. IPsec operates in two modes: tunnel mode and transport mode. In the context of Storage Virtualize, secured IP partnerships utilize tunnel mode. In this mode, the entire IP packet is encapsulated within another IP packet, providing an additional layer of security.

## Advantages of secured IP partnerships

Security aspects	Highlights
Mutual authentication	Certificate based authentication, support for different PKI hierarchies.
Secret establishment	Key exchange using IKEv2 for authentication, data encryption.
Data integrity	Strong integrity algorithms.
Data encryption	Strong encryption algorithms.

Table 1. Advantages of secured IP partnerships.

The following sections provide further details on the security aspects.

#### Mutual authentication

Multiple methods of mutual authentication can be used to establish a secure channel between two endpoints, such as Pre-Shared Key, Digital Signature, Certificates, etc. In IBM Storage Virtualize, Remote Copy over IPsec implementation utilizes certificate-based authentication methods to authenticate the two peers involved in a secured partnership.

To enable certificate-based authentication, endpoint certificates and certificate authorities of the partner systems need to be installed based on the system's chosen certificate options.

The following types of certificate-based approaches are supported to establish a secure tunnel:

- 1. **Internally Signed Certificate**: Internally Signed Certificates have their own system's Certificate Authority (CA) to sign the endpoint certificates, ensuring secure connections between the two peers. The root CA can be exported from one system and added to the trust stores of other systems' browsers or devices as an authority for mutual authentication.
- 2. **Externally Signed Certificate**: In the Externally/CA-signed certificate approach, a certificate is signed by a Certificate Authority (CA), which can be a root CA or an intermediate CA (ICA). This requires a complete chain of trust to authenticate the partner certificate received over the network. The end entity certificate (optionally with a chain of trust) is authenticated by a CA or ICA (optionally with its chain of trust).

Note: In the Externally Signed approach, a Certificate Signing Request (CSR) can be signed by any trusted CA authority or its Intermediate CAs to enhance security levels based on customer requirements.

3. **Self-Signed Certificate**: A self-signed certificate does not require any third-party Certificate Authority (CA) for signing. It is generated and installed locally. The exported self-signed certificate is then installed as an authority on partnered systems. Starting from the 8.5.3.0 release, self-signed certificates are no longer created by default. It is recommended to update the system certificate to either an internally signed certificate or an externally signed certificate.

Detailed configuration steps for Internally Signed and Externally Signed certificates are covered in the following sections. For more information on system certificates, refer to the IBM Knowledge Center's <u>Managing certificates for secure communications</u> documentation.

#### Secret Establishment

IBM Storage Virtualize follows the Commercial National Security Algorithm Suite (CNSA) guidelines to establish the Control path security association (IKE SA) and Data path security association (IPsec SA) between two Flash system clusters participating in a secured IP partnership.

- 1. **Control path secret establishment**: In Storage Virtualize, the IKE SA negotiates the aes256-sha384-ecp384 cipher suite. It uses AES encryption algorithm with a 256-bit key length, SHA authentication algorithm with a 256-bit key length, and ECDH key exchange with the NIST P-384 curve.
- 2. **Data path secret establishment**: For IPsec-based replication links, Storage Virtualize uses the aes256gcm16 cipher suite. It is an AEAD (Authenticated Encryption of Associated Data) type of algorithm that provides both data confidentiality and integrity.

# Pre-requisites to form secured IP partnerships

To form secured IP partnerships, certain prerequisites need to be fulfilled. In addition to the planning and considerations for unsecured partnerships, the following considerations are necessary to ensure mutual authentication between the partner systems:

- Activation of encryption license based on security requirements.
- Configuration of portsets and assignment of IP addresses for data replication (for detailed information refer to <u>IP partnership configuration</u> on ibm.com).
- System time synchronization between the partnered systems.
- Installation of endpoint certificates and related certificate authorities as required, based on certificate choices and security requirements.

# Configure secured IP partnership

To create a secured IP partnership, follow these three high-level steps in the specified order:

- 1. **Install endpoint certificate**: Install the signed endpoint certificate on the systems participating in the partnership.
- 2. **Install remote certificate authority**: Install the remote certificate authority in the truststore of the systems involved in the partnership.
- 3. **Create secured partnership**: After completing the first two steps, create the IP partnership using the "-secured yes" flag on both clusters.

### **Configuration steps summary**

Following table can be utilized as a reference to facilitate the configuration steps:

To proceed with the configuration, follow the links corresponding to your choice of certificate signatures (Internal or External), based on your specific security requirements.

<b>Configuration steps</b>	Internally Signed Certificate	<b>Externally Signed Certificate</b>
1. Endpoint Certificate Installation	Endpoint Certificate (ISC)	Endpoint Certificate (ESC)
2. Remote Certificate Authority Installation	Certificate Authority (ISC)	<u>Certificate Authority (ESC)</u>
3. Secured IP partnership creation	Secured IP partner	ship creation

Table 2. Summary of secured IP partnership configuration steps.

#### Install endpoint certificate (internally signed)

The internal certificate signing approach involves the signing of the endpoint certificate by system's own root CA. This signed certificate is used for authentication at the partner system to create a secure connection.

The installation process of the internally signed endpoint certificate can be carried out using both Graphical User Interface (GUI) and Command Line Interface (CLI) methods.

- Install endpoint certificate using GUI (internally signed).
- Install endpoint certificate using CLI (internally signed).

#### Install remote CA (internally signed)

Starting with version 8.5.3.0, IBM Storage Virtualize uses its own root CA to internally sign system certificates. The root certificate is then exported and provided to partner systems in their truststores for authentication purposes.

The installation process of the internally signed remote CA can be carried out using both Graphical User Interface (GUI) and Command Line Interface (CLI) methods.

- Install remote CA using GUI (internally signed).
- Install remote CA using CLI (internally signed).

#### Install endpoint certificate (externally signed)

The external certificate signing approach involves the signing of the endpoint certificate by a reliable third-party CA, serving as an external provider of certificates. To achieve this, the system generates a new Certificate Signing Request (CSR) that is subsequently signed by the trusted third-party CA. The resulting externally signed endpoint certificate is then installed back onto the system.

The installation process of the externally signed endpoint certificate can be carried out using both Graphical User Interface (GUI) and Command Line Interface (CLI) methods.

- Install endpoint certificate using GUI (externally signed).
- Install endpoint certificate using CLI (externally signed).

#### Install remote CA (externally signed)

The external certificate signing approach involves using the root Cas as trusted third-party Cas to issue al CSRs. Then the root CA is added to the truststore of partner systems across three sites for authentication purposes.

The installation process of the externally signed remote CA can be carried out using both Graphical User Interface (GUI) and Command Line Interface (CLI) methods.

- Install remote CA using GUI (externally signed).
- Install remote CA using CLI (externally signed).

#### Create secured IP partnership

To create a Secured IP partnership, ensure that all required certificates are installed on all clusters participating in the formation of the secured partnership. Depending on the requirement, you can choose either an internally or externally signed certificate approach.

The secured IP partnership can be created using both Graphical User Interface (GUI) and Command Line Interface (CLI) methods.

- <u>Create secured IP partnership using GUI.</u>
- <u>Create secured IP partnership using CLI.</u>

#### Install endpoint certificate using GUI (internally signed)

This section illustrates the endpoint certificate installation steps between master and remote clusters.

For master cluster:

- 1. Open IBM FlashSystem GUI dashboard.
- 2. Navigate to **Settings** → **Security** → **System Certificate**.
- 3. Select **Internally Signed Certificate** under Update Certificate. Enter all the required details and click **Update**.

Security			_ (?) s
K Multifact	Update Certificate	· · · · · · · · · · · · · · · · · · ·	` _
Muthaci	Select the type of certificate to use. The certificate can be s	igned by the internal certificate authority, or a certificate request	ublic netw
Remote.	Internally Signed Certificate     C Externally Signed Certificate	ertificate	
Single Si	Certificate Details		
System (	Key type 🚯	Validity days (	
	2048-bit RSA 🗸	365	
Encrypti	Country	State	
Passwor	IN	Maharashtra	
User Acc	City	Organization name	
	Pune	IBM	
Inactivit	Organizational unit	Common name ①	
SSH Rule	Systems	SVC_CA_Signed_cluster0001	
	Email address	Subject Alternative name	
Security			
	Cancel	Update	
			Read Write

Figure 6. Update internally signed certificate.

IBM FlashSystem 7200		
	Multifactor Authentication	System Certificates
Dashboard	Remote Authentication	Manage certificates that are used to secure connections between systems or applications across a public net
میک Monitoring	Single Sign-on	Create system-signed certificate
Pools	System Certificate	Running Command 0%
Volumes	Encryption	• View more details Task started. 6:19 PM
Hosts	Password Policies	Running command: 6:19 PM svctask chsystemcert -commonname 6:19 PM SVC_ASigned_cluster0001 -country IN -email support@ibm.com -
Copy Services	User Access	keytype rsa2048 -locality Pune -mksystemsigned -org IBM - orgunit Systems -state Maharashtra -subjectalternativename IP:192.168.18.17 -validity 365
Policies	Inactivity Logout	
Access	SSH Rules	Cancel Close
Settings	Security Protocol Levels	State: Maharashtra City: Pune

Figure 7. Create system-signed certificate.

4. Wait for the installation process to complete. It takes a minute to install. After endpoint certificate is installed on your primary cluster, connection will be lost, login and verify installed certificate.

5. Navigate to **Settings**  $\rightarrow$  **Security**  $\rightarrow$  **System Certificate** to verify the installed certificate.



Figure 8. Certificate Details.

This marks the successful installation of endpoint certificate. Perform similar steps on remote cluster to install endpoint certificate.

- Link back to install endpoint certificate (internally signed).
- Link back to configuration steps summary.

#### Install endpoint certificate using CLI (internally signed)

This section illustrates the endpoint certificate installation steps between master and remote clusters.

Follow these steps in sequential order to install internally signed certificates:

For master cluster

Run 'mksystemsigned' command to install endpoint certificate locally on Master Cluster.

```
chsystemcert -mksystemsigned -country IN -state Maharashtra -locality
Pune -org IBM -orgunit Systems -commonname
Internally_Signed_MasterCluster -email support@ibm.com
```

Wait for the installation process to complete. It takes a minute to complete. This marks the successful installation of the local endpoint certificate for master cluster.

Perform similar steps on remote cluster to install endpoint certificate.

- Link back to install endpoint certificate (internally signed).
- Link back to configuration steps summary.

#### Install Root CA using GUI (internally signed)

For master cluster

- 1. Open IBM FlashSystem GUI Dashboard.
- 2. Navigate to Copy Services → Partnerships and Remote Copy → Create Partnership.
- 3. Enter the Partner IP Address and select Secured IP partnerships.
- 4. Click **Test Connection**, the green check mark is displayed on Test Connection, indicating successful connection and remote authority certificates are extracted with details.

Primary	Partnerships and Remote Copy			👆 🗐
	< Partnerships			
		Create Partnership		×
		◯ Fibre Channel		1
		Partner IP Address		
		192.168.18.18	Test Connection	
		Secured IP partnerships Use Policy-Based Replication View certificate		
		The certificate for the remote system ha the local truststore	is been validated by an authority in	
		Certificate from 192.168.18.18	Torres Manag	onfigured ship" to create one
		Subject Name	Country	*
		Cancel	Create	

Figure 9. Create secured IP partnership.

5. Click **Create** to create partnership.

Aux1	AUX1	
O Partial Local	Create IP Partnership	
	lask completed.	
	100%	
	svctask mklppartnersnip -backgroundcopyrate 50 - clusterip 192.168.18.18 -compressed no -linkl N1P5 - linkbandwidthmbits 25000 -secured yes -type ipv4 Running command: svctask chtruststore -name TS_000002043100CFD8	7:03 PM . 7:03 PM 7:03 PM
	TS_192.168.18.18	7.02.04
	The task is 100% complete.	7:03 PM S
	Task completed.	7:03 PM
	Cancel	lose

Figure 10. Create IP partnership task completed.

On the Master Cluster, you have successfully created a secured IP partnership by installing the root certificate of the remote system (Aux Cluster) as an authority.

Primary	Partnerships and Remote Copy			🍓 🗐 (	) superuser Security Ac	ministrator 3	: <b>x</b>
	Partnerships	Aux1				Actions	
	Aux1 Configured	Aux1 Properties View details about your partnership an bandwidth and background copy rate v	d change properties such as link alues.	× ps (0)	Policy-based replication		
		Name	Aux1	5		11	Q
		Location	Partner				
		Status	Configured				
		Туре	IP				
		Secure	Yes				
		Use policy-based replication	Enable	+ ps and independent			
		Cancel	Save				

On the Aux Cluster, follow the same steps to create a secured IP partnership by installing the root certificate of the remote system (Master Cluster) as an authority.

Figure 11. Secured partnership status.

Fully configured secured IP partnership is established now from GUI with internally signed certificate approach.

- Link back to install Root CA (internally signed).
- Link back to configuration steps summary.

#### Install Root CA using CLI (internally signed)

This section illustrates the root CA installation steps between master and Aux cluster.

For master cluster

1. Run 'exportrootcertificate' command to generate the root certificate.
 # satask exportrootcertificate

'root\_certificate.pem' file is generated in /dumps directory /dumps/root\_certificate.pem.

- 2. Copy the Master Cluster's root certificate to remote Aux Cluster. Copy /dumps/root\_certificate.pem from Master Cluster as /dumps/root\_certificate\_Master.pem onto Aux Cluster
- 3. Run 'mktruststore' command to install authority.
   # svctask mktruststore -file /dumps/ root\_certificate\_Aux.pem -ipsec on
   -restapi on

Perform the similar steps on remote Aux cluster to install root CA.

- Link back to install Root CA (internally signed).
- Link back to configuration steps summary.

#### Install endpoint certificate using GUI (externally signed)

This section illustrates the endpoint certificate installation steps between master and remote clusters.

For master cluster

- 1. Open IBM FlashSystem GUI dashboard.
- 2. Navigate to Settings  $\rightarrow$  Security  $\rightarrow$  System Certificate.
- 3. Select **Externally Signed Certificate** under Update Certificate. Enter all the required details and click **Update**.
- 4. Click **Generate Request** to generate and download 'certificate.csr' file onto the downloads folder.

IBM FlashSystem 7200	ecurity			Ć
	Multifact	Update Certificate	Â	I
Dashboard	Remote	Select the type of certificate to use. The certificate can be si can be generated and presented to an external certificate au	igned by the internal certificate authority, or a certificate request uthority.	ut
	Single Si	U Internativ Signed Certificate	- uncate	
Pools	System (	Generate signing request for external certif	Country	
Volumes	Encrypti	2048-bit RSA ~	IN	
	Passwor	State Maharashtra	City Pune	
	User Acc	Organization name	Organizational unit	
Fo Policies	Inactivit	Common name (i)	Email address	
Access	SSH Rule	GUI_Master	support@ibm.com	
	Security	Subject Alternative name (		
		Cancel	Generate Request	-

Figure 12. Update externally signed certificate.

- 5. Rename 'certificate.csr' file to 'GUI\_Master.csr'.
- 6. Copy the .csr file from the cluster and sign it using a PKI host or any certificate-signing authority as per your requirement.

```
For example:
# openssl x509 -CA CAOneICA3.pem -CAkey CAOnePrivateKey3.pem -
CAcreateserial -in GUI_Master.csr -req -days 365 -out GUI_Master.pem
```

Here, the GUI\_Master.csr file is signed with the intermediate CA3 of Root CAone, and a signed endpoint certificate 'GUI\_Master.pem' is generated.

Note: Certificate signing authority can be an intermediate CA or a root CA depending on security requirements and planning.

7. Copy the certificate 'GUI\_Master.pem' to window's folder to upload and install.

8. Notice that a 'Outstanding Signing Request' appears under **Internally Signed Certificate**. Click **Install Signed Certificate** to proceed.

Master	Security		👍 🗉	⑦ superuser Se	curity Administr	ator 🥝 🖂
	K Multifactor Authentication	System Certificates	seuro segnostions batuleon sustema es apolications assess a o	ublic natural		
	Remote Authentication	manage certificates that are used to se	scure connections between systems of applications across a p	JUIC HEIWOIK.		
	Single Sign-on	Certificate Details		Install Signed Certif	ficate 🏹	
	System Certificate	Internally Signed Certificate Outstanding Signing Request				
	Encryption	Automatic renewal (j)				
	Password Policies	Subject Distinguished Name				
		Country:	IN			
	User Access	State:	Maharashtra			
	Remote Authentication         Single Sign on         System Certificate         Encryption         Password Policies         User Access         Inactivity Logout         SSH Rules	City:	Pune			
	Inactivity Logout	Organization:	IBM	Image: Construction of a public network.         Scool to Root Certificate		
		Organizational Unit:	Systems			
	Multifactor Authentication Remote Authentication Single Sign-on System Certificate Encryption Password Policies User Access Inactivity Logout SSH Rules	Email Address:	support@ibm.com		Scroll to Root (	Certificate J
		Common Name:	GUI_Master			

Figure 13. Outstanding Signing request.

9. Click **Add file** to upload signed endpoint certificate 'GUI\_Master.pem', and then click **Install**.

		curity				-0		(?
Multifacto	Multifactor Authe	ntication	System Certif	icates				
		Remote Authentication		Manage certificates that ar	e used to secure connections between systems or a	pplications ad	cross a (	publ
		Single Sign-on	Install Signe	d Certificate		×		
		System Certificat	Install the signed containing interm intermediate CA c	certificate that was provided ediate CAs, upload a single file ertificates concatenated toge	by the certificate authority (CA). If the CA used a cha e that contains the signed certificate and all of the ther.	ain of trust		
		Encryption	Add file					
		Password Policie	GUI_Master.pe	m ×				
		User Access						
		Inactivity Logout	Cancel		Install			
		SSH Rules		Organizational Unit:	Systems			

Figure 14. Install signed certificate.

- 10. Wait for the installation process to complete. It takes a minute to install. After endpoint certificate is installed on your master cluster, connection will be lost, login and verify installed certificate.
- 11. Navigate to **Settings**  $\rightarrow$  **Security**  $\rightarrow$  **System Certificate** to verify the installed certificate.

IBM FlashSystem 7200	Master Se	curity		
	<	Multifactor Authentication	Certificate Details	
Dashboard		Remote Authentication	Externally Signed Certificate	
ഹ്ര <sup>മ</sup> Monitoring		Single Sign-on	Subject Distinguished Name	IN
Pools		System Certificate	State: City:	Maharashtra Pune
Volumes		Encryption	Organization: Organizational Unit:	IBM Systems
Hosts		Password Policies	Email Address: Common Name:	support@ibm.com GUI_Master
Copy Services		User Access	Issuer Distinguished Name	
Policies		Inactivity Logout	State:	IN
Access		SSH Rules	Organization:	ІВМ
∑́ó) Settings		Security Protocol Levels	Email Address:	
			Common Name:	CA1_intermediate3

Figure 15. Externally signed certificate details.

Externally signed endpoint certificate is installed successfully on Master Cluster.

Perform similar steps on remote cluster to install certificate. Signing authority can be same as used in master cluster or different depending upon the requirements.

- Link back to install endpoint certificate (externally signed).
- Link back to configuration steps summary.

#### Install endpoint certificate using CLI (externally signed)

This section illustrates the endpoint certificate installation steps between master and remote clusters.

Follow these steps in sequential order to install externally signed certificates:

For master cluster

1. Generate the 'certificate.csr' file by running the 'mkrequest' command.

```
# svctask chsystemcert -mkrequest -country IN -state Maharashtra -
locality Pune -org IBM -orgunit Systems -commonname
CA_Signed_MasterCluster -email support@ibm.com
```

Running this command will generate the 'certificate.csr' file in the /dumps directory. Copy the 'certificate.csr' file to a PKI host or any certificate signing authority for signing and generating the signed endpoint certificate.

2. Sign the certificate with the root CAOne and generate the endpoint certificate using the 'openssl' command.

```
# openssl x509 -CA CAOneICA3.pem -CAkey CAOnePrivateKey3.pem -
CAcreateserial -in certificate.csr -req -days 365 -out
SignedMasterEndpoint.pem
```

Running this command will generate the signed endpoint certificate 'SignedMasterEndpoint.pem ' file signed with intermediate CA3 of root CAOne.

Copy this generated file back to master Cluster in /dumps/ directory.

Externally signed endpoint certificate is installed successfully on master cluster.

Perform similar steps on remote cluster to install certificate. Signing authority can be same as used in master cluster or different depending upon the requirements.

- Link back to install endpoint certificate (externally signed).
- Link back to configuration steps summary.

#### Install Root CA using GUI (externally signed)

For master cluster

Since the endpoint certificate was signed using Intermediate CA3 of root CAOne, it is necessary to create a concatenated chain of trust that includes CAOne up to Intermediate CA3. This concatenated chain of trust should be combined into a single PEM file, which can then be installed as an authority on the remote cluster.

cat CAOneICA3.pem > auth\_chain\_Master.pem

- cat CAOneICA3.pem >> auth\_chain\_Master.pem
- cat CAOneICA3.pem>> auth\_chain\_Master.pem
- cat CAOnePubKey.pem >> auth\_chain\_Master.pem

Here, 'auth\_chain\_Master.pem' is chain of trust which is installed as an authority on remote cluster (Aux Cluster).

Remote authority can be installed via **Create Partnership** option through GUI.



Figure 16. Create secured IP partnership.

- 1. Open IBM FlashSystem GUI Dashboard.
- 2. Navigate to Copy Services → Partnerships and Remote Copy → Create Partnership.
- 3. Enter the **Partner IP Address** and select **Secured IP partnerships**. If the green check mark is displayed on Test Connection, then **Validate certificate** option is enabled.

Click **Upload File** to upload remote CA of Aux cluster (auth\_chain\_Aux.pem) and click **Create** to create partnership.

Master Pa	artnerships and Remote Copy			
<	Partnerships	Aux1		
	Aux1 Configured	Aux1 Properties View details about your partnership and change properties such as bandwidth and background copy rate values.	× link	ips (0)
		Name	Aux1	
		Location	Partner	
		Status	Configured	
		Туре	IP	
		Secure	Yes	
		Use policy-based replication	Enable	ps and
		Cancel Save		
	Create Partnership	+		

Figure 17. Secured IP partnership configured.

For Aux cluster

Perform the previous steps on Aux cluster to install the externally signed certificate. On remote cluster, an endpoint certificate 'GUI\_Aux.pem' signed from intermediate CA3 of root CATwo was installed.

cat CATwoICA3.pem > auth\_chain\_Aux.pem
cat CATwoICA3.pem >> auth\_chain\_Aux.pem
cat CATwoICA3.pem>> auth\_chain\_Aux.pem
cat CATwoPubKey.pem >> auth\_chain\_Aux.pem

Here, 'auth\_chain\_Aux.pem' is the chain of trust which will be installed as an authority on remote cluster (master cluster).

IBM F	ashSystem 7200 Aux1	Security		
	R	Multifactor Authentication	Certificate Details	
	Dashboard	Remote Authentication	Externally Signed Certificate	
~~^P	Monitoring	Single Sign-on	Country:	IN
₿	Pools	System Certificate	State: City:	Maharshtra Pune
	Volumes	Encryption	Organization: Organizational Unit:	IBM Systems
	Hosts	Password Policies	Email Address: Common Name:	support@ibm.com GUI_Aux1
G	Copy Services	User Access	Issuer Distinguished Name	IN
- ଜି	Policies	Inactivity Logout	State: City:	
	Access	SSH Rules	Organization: Organizational Unit:	IBM
হ্ট্য	Settings	Security Protocol Levels	Email Address: Common Name:	CA2_intermediate3
			Serial Number:	17065446100944968590

Figure 18. Externally signed certificate details.

Aux1 Par	tnerships and Remote Copy		
<	Partnerships	Master	
	Master Configured	Master Properties View details about your partnership and change properties bandwidth and background copy rate values.	such as link
		Name	Master
		Location	Partner
		Status	Configured
		Туре	IP
		Secure	Yes
		Use policy-based replication	Enable 🖕 ps a
		Cancel Save	
	Create Partnership +		

Figure 19. Fully configured secured IP partnership.

Fully configured secured IP partnership is established now from GUI with externally signed certificate approach.

- Link back to install Root CA (externally signed).
- Link back to configuration steps summary.

#### Install Root CA using CLI (externally signed)

This section illustrates the root CA installation steps between master and Aux cluster. For master cluster

- 1. Install remote certificate as an authority by running the 'mktrustore' command.
   # svctask mktruststore -file /dumps/auth\_chain\_Aux.pem -ipsec on restapi on
- 2. create partnership with Aux cluster with '-secured yes' as an additional parameter. For example:

```
# mkippartnership -type ipv4 -clusterip <clusterAux-ip> -
linkbandwidthmbits 2500 -backgroundcopyrate 50 -link1 1 -link2 2 -
secured yes
```

3. Run 'lspartnership' command and verify detailed output to check 'secured yes' status.

#### For Aux cluster

- 1. Install remote certificate as an authority by running the 'mktrustore' command.
   # svctask mktruststore -file /dumps/ auth\_chain\_Master.pem -ipsec on
- 2. create partnership with Master cluster with '-secured yes' as an additional parameter. For example:

# mkippartnership -type ipv4 -clusterip <clusterMaster-ip> linkbandwidthmbits 2500 -backgroundcopyrate 50 -link1 1 -link2 2 secured yes

3. Run 'lspartnership' command and verify detailed output to check 'secured yes' status.

Note: The example shows two different certificate authorities (CAs) being used. However, it is also possible to use the same CA for both partner systems.

For more information on externally signed certificates, refer to <u>Managing certificates for secure</u> <u>communications</u> on ibm.com.

- Link back to install Root CA (externally signed).
- Link back to configuration steps summary.

#### Create secured IP partnership using GUI

To create a Secured IP Partnership using the GUI, follow these steps:

- 1. Enable the **Secured IP partnership** checkbox in the **Create Partnership** section and perform a test connection.
- 2. If a green check mark is displayed during the test connection, the **Validate certificate** option will appear.
- 3. In the **Validate certificate** section, upload the remote authority to successfully create the secured partnership.

Master Partnerships and Remote Copy		-
Partnerships	Create Partnership O Fibre Channel  IP	×
	Partner IP Address	
	192.168.18.19 Test Connection 📀	
	<ul> <li>Secured IP partnerships         <ul> <li>Use Policy-Based Replication</li> </ul> </li> <li>Validate certificate         <ul> <li>The remote system is using a certificate that is signed by an unrecognized authority. Upload the certificate for the following authority: IBM</li> <li>Upload File</li> <li>auth_chain ×</li> </ul> </li> </ul>	onfigurec ship" to crea
	Link specification	v
	Cancel Create	
Create Partnership	+	

Figure 20. Create secured IP partnership.

#### Repeat these steps on the remote cluster to establish a secured partnership.

Master					
	< Partnerships		Aux1		
	Aux1 Configured	Au Vie bar	X1 Properties w details about your partnership and change properties such a dwidth and background copy rate values.	× s link	<sup>≜</sup> ips (0)
		Nar	ne	Aux1	
		Loc	ation	Partner	
		Sta	tus	Configured	
		Тур	e	IP	
		Sec	ure	Yes	
		Use	policy-based replication	Enable	≠ ps anc
		Car	Save		
	Create Partnership	+			

Figure 21. Fully configured secured IP partnership.

- Link back to create secured IP partnership.
- Link back to configuration steps summary.

#### Create secured IP partnership using CLI

To create a secured IP partnership using CLI perform the following steps.

Add the additional secured parameter to the 'mkippartnership' CLI command to verify whether the partnership is secured or unsecured.

```
# mkippartnership -type ipv4 -clusterip <clusterB-ip> -
linkbandwidthmbits 2500 -backgroundcopyrate 50 -link1 1 -link2 2 -
secured yes
```

Run 'lspartnership' command and verify detailed output to check 'secured yes' status.

Repeat similar steps on remote cluster to establish a secured IP partnership.

- Link back to create secured IP partnership.
- Link back to configuration steps summary.

# Switch between unsecured and secured IP partnerships

Switching from an unsecured to a secured IP partnership involves implementing security measures, such as IPsec, to protect data transmission and establish trust between systems, ensuring confidentiality, integrity, and authentication.

The IP partnership can be converted using both Graphical User Interface (GUI) and Command Line Interface (CLI) methods.

- Convert unsecured to secured IP partnership using GUI
- Convert unsecured to secured IP partnership using CLI

To initiate the conversion of unsecured to secured IP partnerships using the GUI, the following prerequisites must be met:

- Create an unsecured IP partnership, refer to the IP partnership configuration documentation on ibm.com for detailed instructions.
- Install certificates on all clusters that will participate in forming the partnerships. Depending on the requirements, choose either an internally or externally signed certificate approach.

Link back to configuration steps summary.

#### Convert unsecured to secured IP partnership using GUI

To convert unsecured IP partnership to secured IP partnership, perform the following steps:

- 1. Stop partnership on both sites.
- 2. Enable (Yes) **Secure** option on both sites.
- 3. Start partnership from both sites.

Once both sites successfully start the partnership, the Secure flag in the GUI will be enabled to 'Yes', indicating that the conversion from an unsecured to a secured partnership has been accomplished.

Primary P	artnerships and Remote Copy			
	Partnerships	Aux1		
	Aux1 Configured	Aux1 Properties View details about your partnership and bandwidth and background copy rate val	change properties such as link ues.	×
		Name	Aux1	
		Location	Partner	
		Status	Configured	
		Туре	IP	
		Secure	Yes	5
		Use policy-based replication	Enable	∽ ps and
		Cancel	Save	

Figure 22. Fully configured secured IP partnership.

Similarly, it is also possible to convert a secured partnership back to an unsecured one.

• Link back to switch between unsecured and secured IP partnership.

#### Convert unsecured to secured IP partnership using CLI

To convert unsecured IP partnership to secured IP partnership, perform the following steps:

1. Run the following command on both the clusters to stop the partnership.
 # svctask chpartnership -stop <remote\_cluster\_id/ remote\_cluster\_name>

Before converting unsecured to secured IP partnership, install certificates on all the clusters involved in partnership. Choose internal or external certificate approach based on requirement.

2. Run the following command on both the clusters to enable the secured option.

- # svctask chpartnership -secured yes <remote\_cluster\_id/
  remote\_cluster\_name>

Similarly, you can convert a secured partnership to unsecured partnership by using the '- secured no' option.

# svctask chpartnership -secured no <remote\_cluster\_id/
remote\_cluster\_name>

• Link back to switch between unsecured and secured IP partnership.

# Verify secured status of a partnership

Secured status of a partnership can be verified using both Graphical User Interface (GUI) and Command Line Interface (CLI) methods.

#### Verify secured status using GUI

- 1. Open IBM FlashSystem GUI Dashboard.
- 2. Navigate to Copy Services →Partnerships and Remote Copy.
- 3. In the Partnerships tab, select the partnership to be verified.
- 4. Observe the status of **Secure** option, if Secure option is enabled (Yes) then status is secured.

SV2_M	Partnerships and Remote Copy			
<	Partnerships	SV2_A		
	SV2_A Configured	SV2_A Properties View details about your partnership and bandwidth and background copy rate val	change properties such as link ues.	<
		Name	SV2_A	
		Location	Partner	
		Status	<ul> <li>Configured</li> </ul>	
		Туре	IP	
		Secure	Yes	
	Use	Use policy-based replication	Enable	, ps and
		Cancel	Save	

Figure23 . Secure status of a partnership.

#### Verify secure status using CLI

Verify the partnership details using the following commands:

1. Run the `svcinfo lspartnership` command to obtain the cluster\_id/cluster\_name information.

```
For example:
# svcinfo lspartnership
id name location partnership type cluster_ip
event_log_sequence link1 link2 link1_ip_id link2_ip_id
0000020330E18BFE cluster-1 local
0000020327E18C06 cluster-1 remote fully_configured ipv4 10.10.11.12
portset1 0
```

2. Utilize the cluster\_id/cluster\_name obtained from the previous command output to view the details of the secured partnership status and validate the secured field. It should be set to "yes" as shown.

```
# svcinfo lspartnership cluster-1
id 000020327E18C06
name cluster-1
location remote
partnership fully_configured
code_level 8.5.0.0 (build 157.11.0000000000000)
console_IP 10.10.11.12:443
gm_link_tolerance 300
gm_inter_cluster_delay_simulation 0
gm_intra_cluster_delay_simulation 0
relationship_bandwidth_limit 25
gm_max_host_delay 5
type ipv4
cluster ip 10.10.11.12
```

```
chap_secret
event_log_sequence
link_bandwidth_mbits 100
background_copy_rate 50
max_replication_delay 0
compressed no
link1 portset1
link2
link1_ip_id 0
link2_ip_id
secured yes
```

## Troubleshooting

Directed maintenance procedures (DMPs) can be used to repair problems by selecting the 'Run fix procedure' action on a selected event from the **Monitoring**  $\rightarrow$  **Events** page on the GUI. In EDIF, secured tunnel establishment may fail in various scenarios, such as authentication errors, certificate errors, network errors, timeouts, and so on. As part of the DMPs run fix procedure, proper user actions are proposed to resolve all IPsec related DMP 2020 error codes.

A sample authentication failure DMP scenario with its run fix procedure provided on the GUI is as follows:

#### **Scenario: Authentication Failure**

- 1. Signed Endpoint Certificates are installed on both Cluster A and B.
- 2. The Root CA Authority is erroneously not installed on Cluster A, but it is installed on Cluster B.

As the authority is not installed on Cluster A, an IPsec DMP error code is generated indicating an authentication failure.

#### On Cluster A's GUI:

DMP error code 2020 is generated on the GUI in the **Monitoring**  $\rightarrow$  **Events** section on Cluster A. This is the EDIF error code for authentication failure. Following figure provides the error details:

Master	Events					👍 🗉	? superu	ser Security Administrator	4 1
	K Highest priorit Error 1138 : Po C Refresh ≡ /	<b>y event. We recom</b> wer Supply Unit Inp Actions • Unf	mend to run fix. Run Fix out Power Failed	¥	IP Remote Copy l Error Code: 2020	ink unavailable		Run Fix	×
	Last Time Stamp	Status	Description	IJ	First Time Stamp Last Time Stamp		12/9/2022 4:20:4 12/9/2022 4:20:4	47 PM 47 PM	
	12/9/2022 4:20:47 PM	🔇 Alert	IP Remote Copy link unavailable		Fixed Time Stamp Event Count		1		
	12/9/2022 4:20:42 PM	🔇 Alert	IP Remote Copy link unavailable				-		
	12/9/2022 3:42:41 PM	() Alert	Connection to a configured remote clust	er has bee	Properties	Sense Data:			
	12/8/2022 9:01:03 PM	Alert	Power Supply Unit Input Power Failed		Sense data version Node error Node error data	sic es	0x01 889 1=000002042FA0 c=2	CCFD8 id=5 vrc=0 drc=10 emc=	:0

Figure 24. Event sense data for IPsec error code.

When the **Run Fix** option in the top right corner, highlighted in blue, is selected, user guidelines (with probable reasons) are provided to resolve this DMP error code. Following figure provides the details.



Figure 25. Run fix for IPsec error code.

It is also necessary to check the DMP error codes on the remote cluster (Cluster B).

In general, it is advisable to check the DMP error codes on both partner systems.

## Summary

This white paper offers a fundamental overview of IP security and provides valuable insights into IPsec for IP replication. It presents detailed steps for configuring secured IP partnerships, including various types of certificate-based authentication to ensure data encryption and integrity. Additionally, the paper discusses the conversion of an existing unsecured IP replication link to a secured one between two partner systems. Furthermore, directed maintenance procedures (DMPs) are explored, providing possible reasons and suggested service actions for establishing secured IP partnerships.

## Get more information

- IBM Storage Virtualize IP replication requirements.
- IBM Storage Virtualize Configuring IP replication.
- <u>RFC4303: IP Encapsulating Security Payload (ESP)</u>.
- IPsec and IKE Document Roadmap (RFC).
- <u>Managing Certificates for secure communications.</u>

## About the authors

**Devendra Mahajan** is part of IBM Storage Virtualize team and is responsible for IBM Flash-System Security (EDIF) delivery. You can reach Devendra at: <u>demahaj1@in.ibm.com</u>

**Harishkumar Bhokare** is part of IBM Storage Virtualize team and is responsible for IBM Flash-System Security (EDIF) delivery. You can reach Harish at: <u>harishkumar.bhokare1@ibm.com</u>

**Ashwin Joshi** is a technical leader for IBM Storage Virtualize product. Apart from data security domain, he has design & development contributions in the areas of IO throttling, Fibre Channel protocol development, FC adapter error recoveries, NVMeoFC, Encryption key management, Offloaded data transfers etc. You can reach Ashwin at: <u>ashjosh1@in.ibm.com</u>

## Acknowledgments

The completion of this paper was possible due to the valuable suggestions and inputs provided by the team. The following members of the team deserve recognition for their contributions:

- Bill Scales
- Pankaj Deshpande
- Digambar Ingale
- Abhijit Indulkar
- Pradip Waykos

© Copyright IBM Corporation 2023

IBM Corporation New Orchard Road Armonk, NY 10504

Produced in the United States of America July 2023

IBM and the IBM logo are trademarks of International Business

Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademark is available on the Web at "Copyright and trademark information" at ibm.com/trademark.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY

OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

