IBM Storage Virtualize: Secured Data Replication with IPsec

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

IBM

Table of contents

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
CA	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
PKI	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 industry-standard 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® 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® SAN Volume Controller (SVC) or IBM Storwize® 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 Getting started with policy-based replication 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.

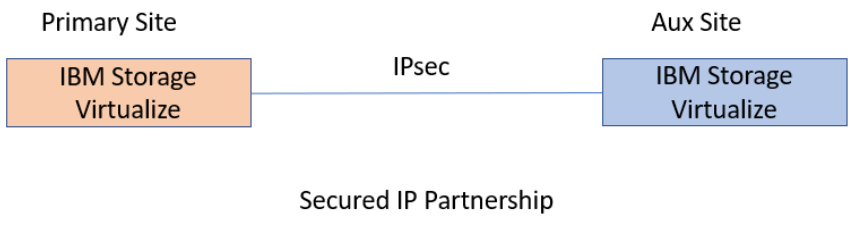

Figure 1. Secured IP partnership.

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.

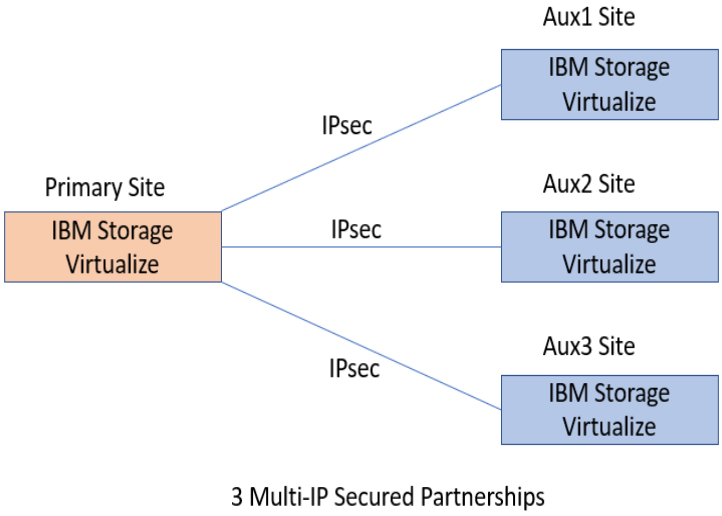

Figure 2. Multi-IP secured partnership.

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.

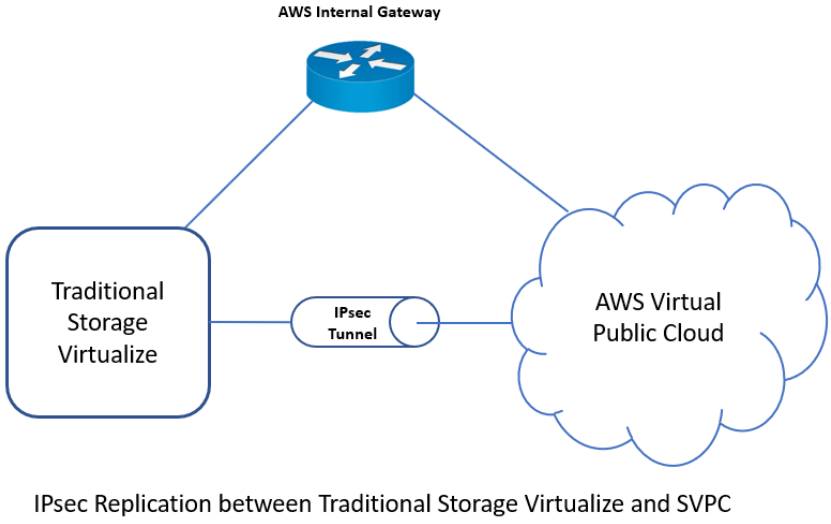

Figure 3. IPsec replication between traditional storage virtualize and SVPC.

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.

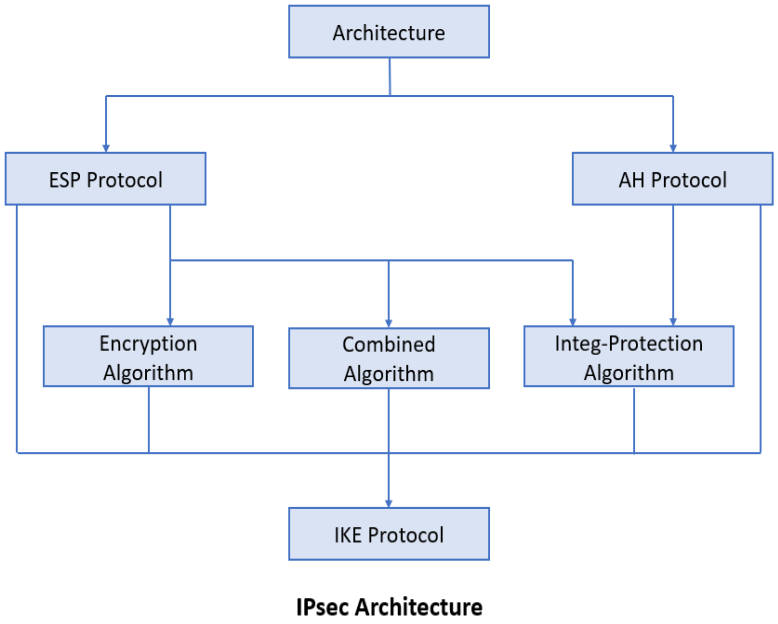

Figure 4. IPsec architecture.

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.

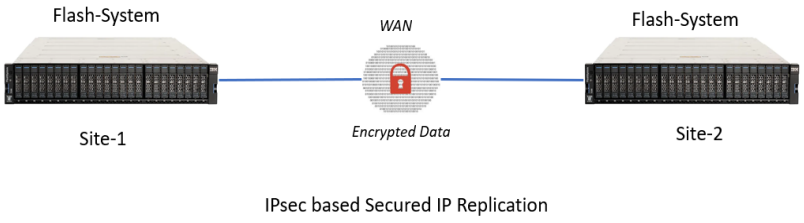

Figure 5. IPsec based secured IP replication.

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 Managing certificates for secure communications 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 IP partnership configuration 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.

Configuration steps	Internally Signed Certificate	Externally Signed Certificate
1. Endpoint Certificate Installation	Endpoint Certificate (ISC)	Endpoint Certificate (ESC)
2. Remote Certificate Authority Installation	Certificate Authority (ISC)	Certificate Authority (ESC)
3. Secured IP partnership creation	Secured IP partnership 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.

- Create secured IP partnership using GUI.
- Create secured IP partnership using CLI.

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.**

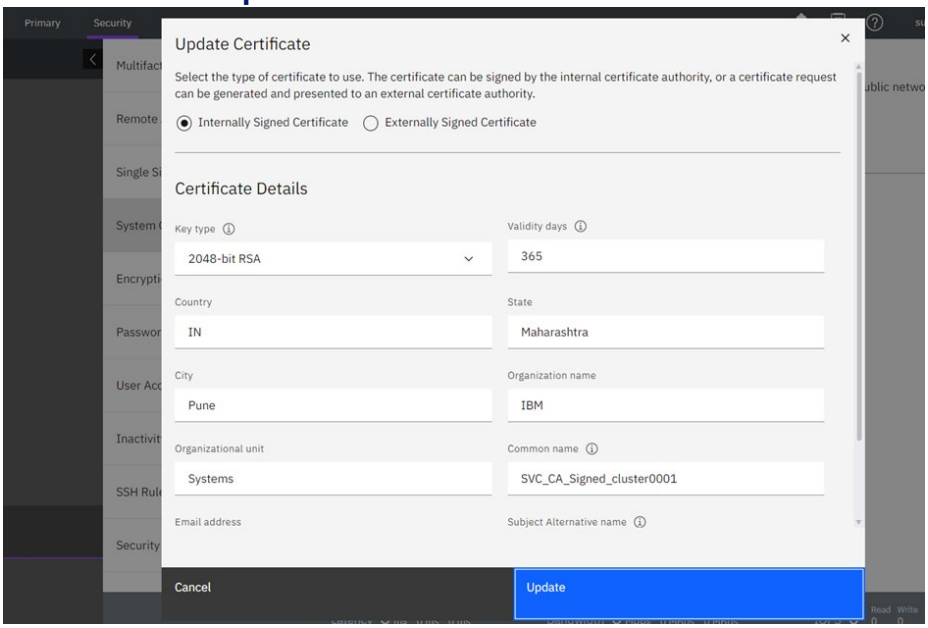

Figure 6. Update internally signed certificate.

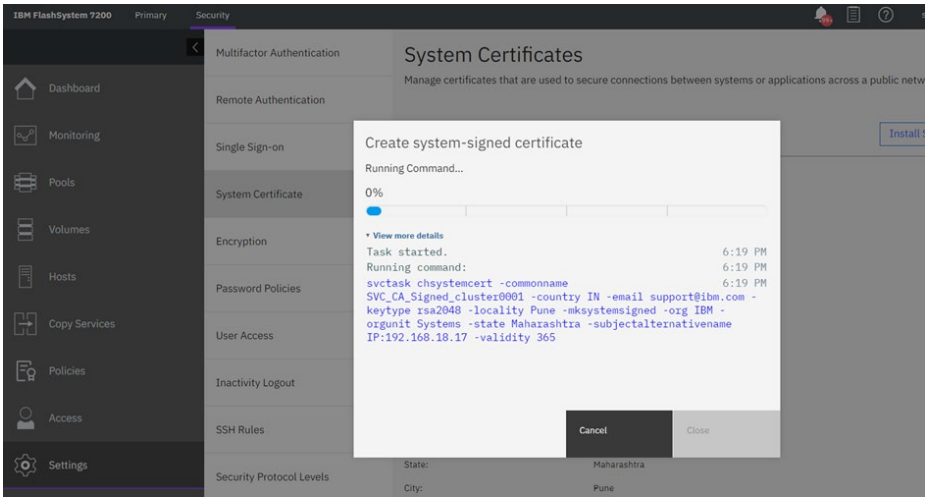

Figure 7. Create system-signed certificate.

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 →Security →System Certificate** to verify the installed certificate.

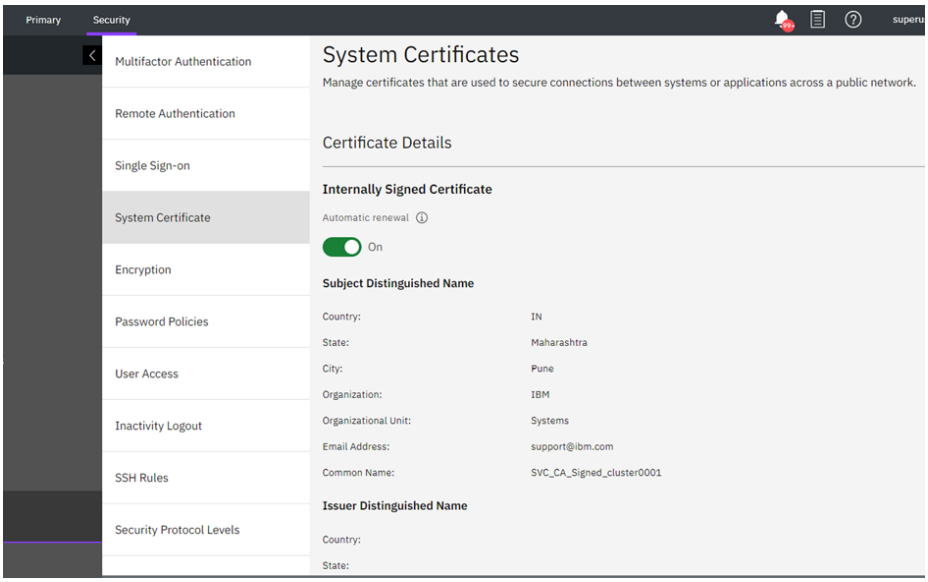

Figure 8. Certificate Details.

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.

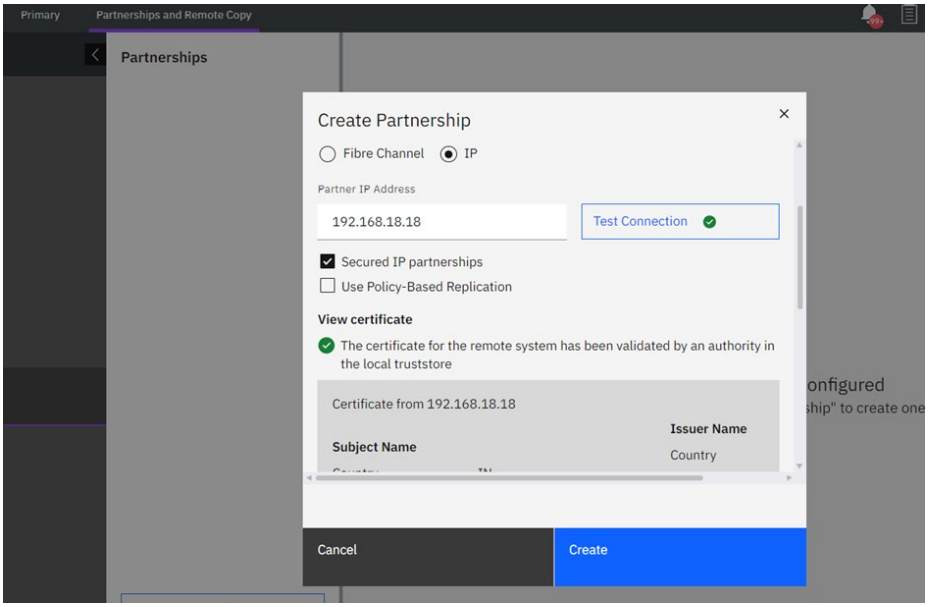

Figure 9. Create secured IP partnership.

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

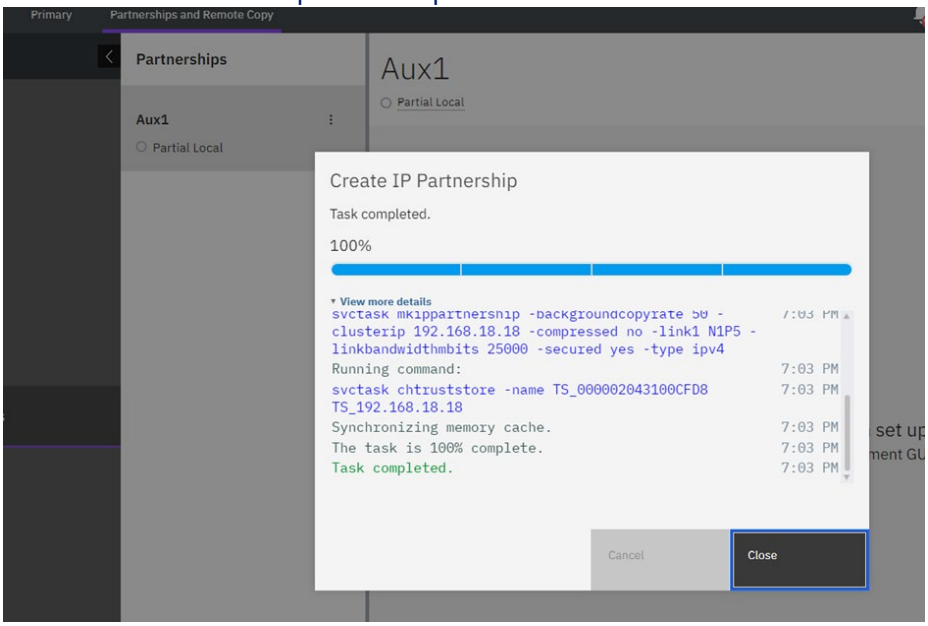

Figure 10. Create IP partnership task completed.

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.

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.

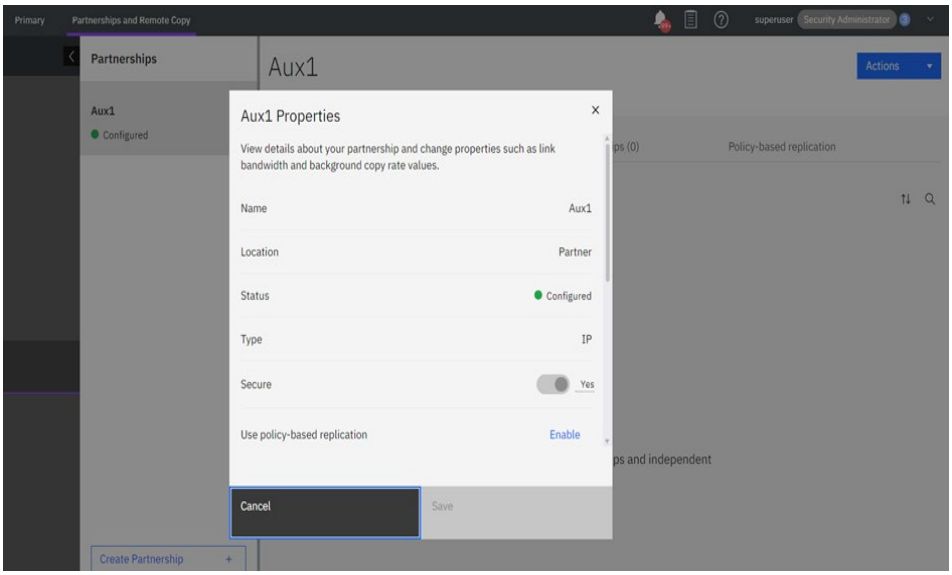

Figure 11. Secured partnership status.

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 → Security → 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.

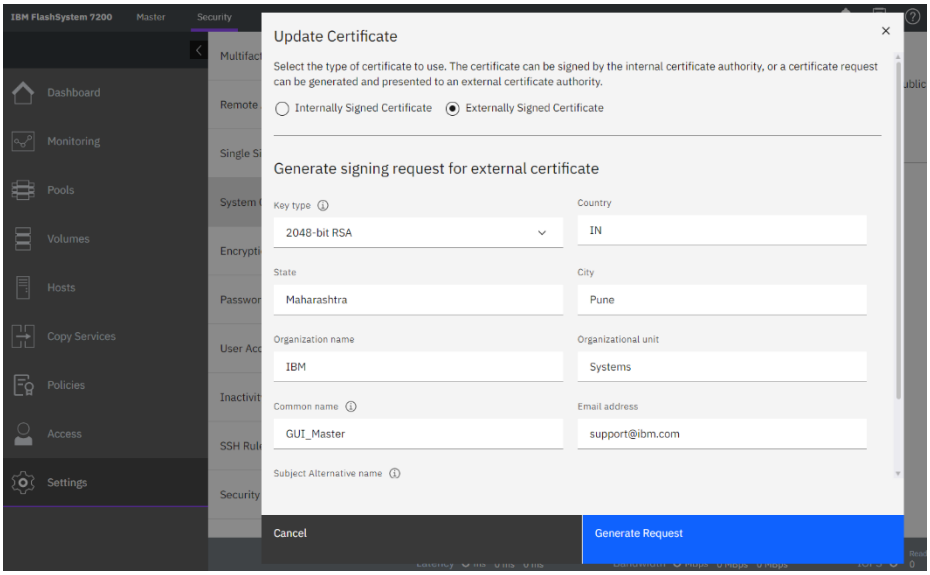

Figure 12. Update externally signed certificate.

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.

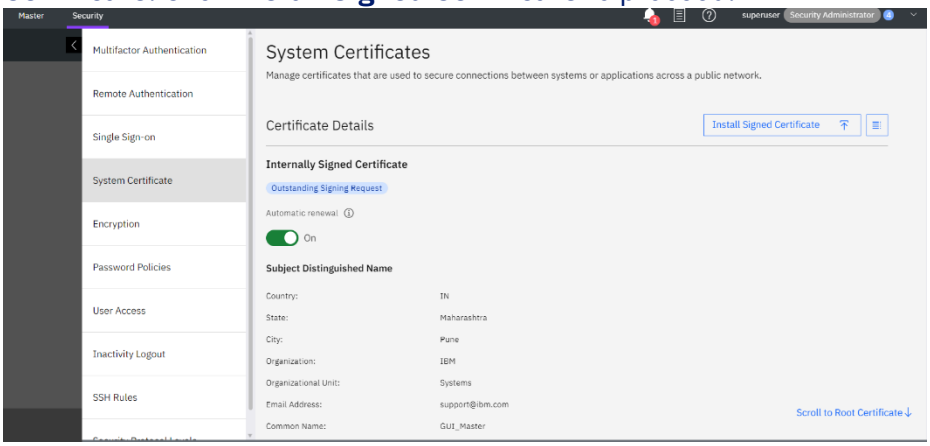

Figure 13. Outstanding Signing request.

9. Click **Add file** to upload signed endpoint certificate ‘GUI_Master.pem’, and then click **Install**.

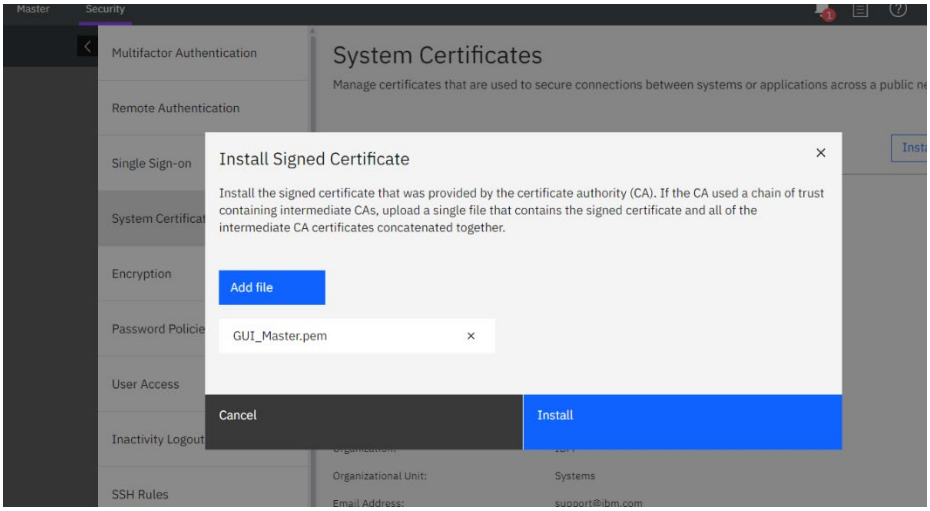

Figure 14. Install signed certificate.

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 →Security →System Certificate** to verify the installed certificate.

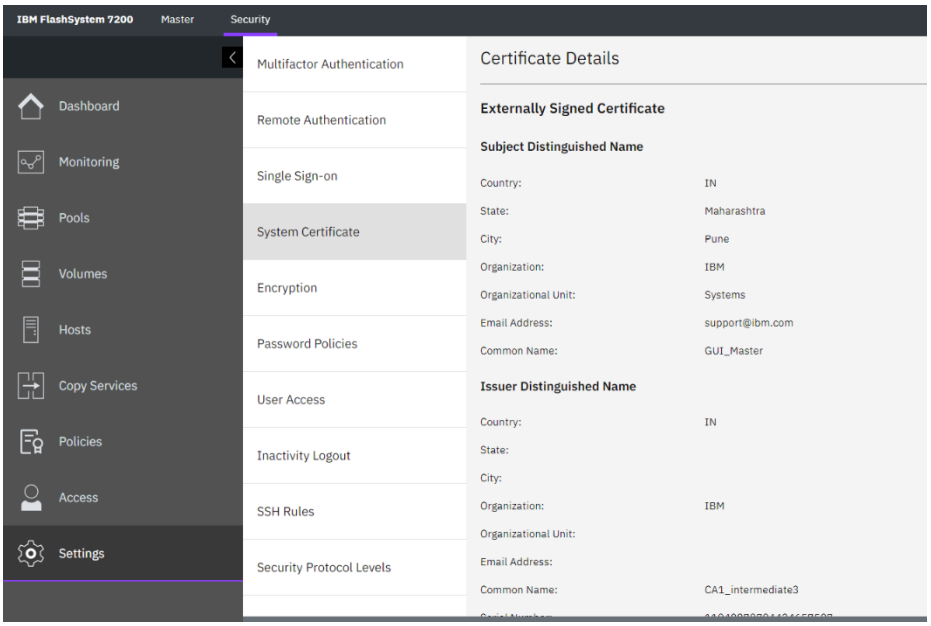

Figure 15. Externally signed certificate details.

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.

3. Install the endpoint certificate by running the ‘chsystemcert’ command

```
# chsystemcert -install -file /dumps/ SignedMasterEndpoint.pem
```

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.

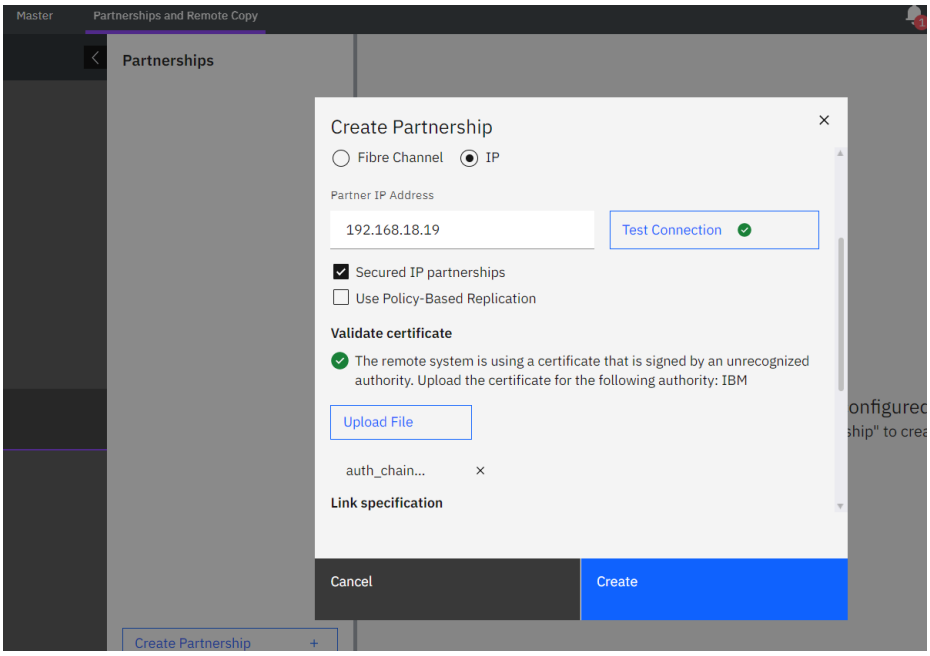

Figure 16. Create secured IP partnership.

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.

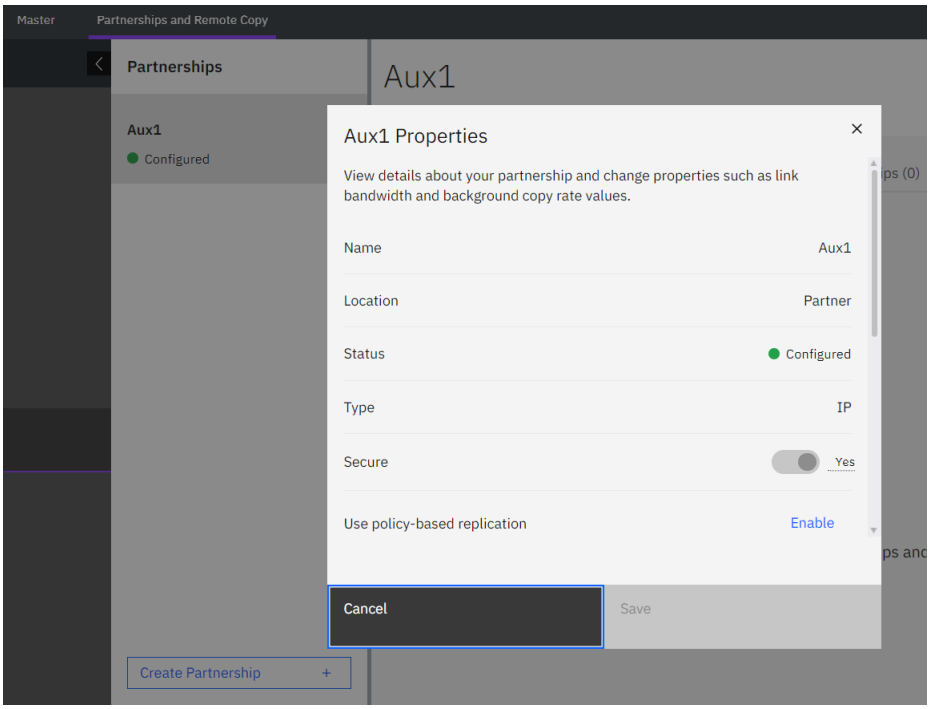

Figure 17. Secured IP partnership configured.

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).

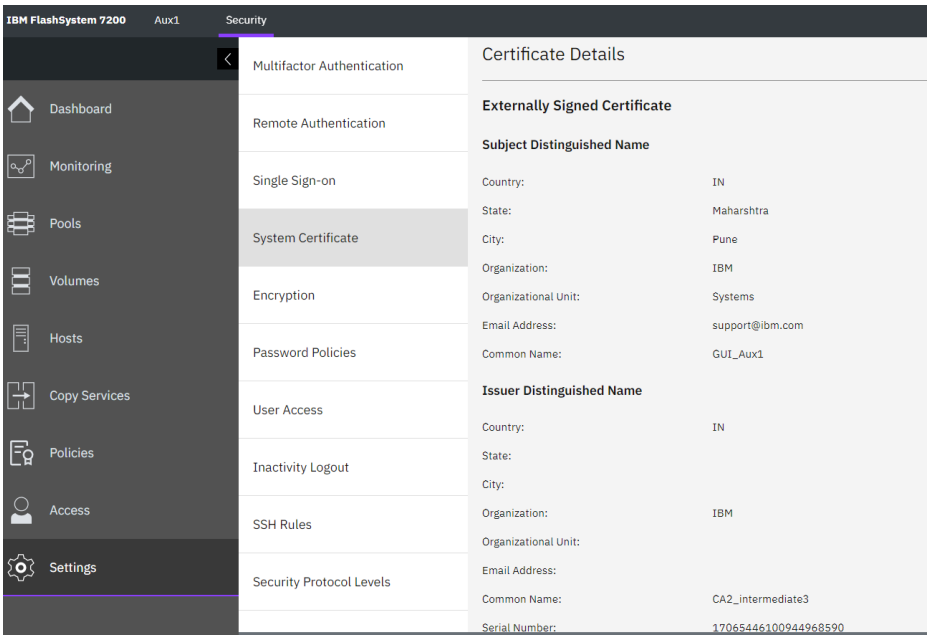

Figure 18. Externally signed certificate details.

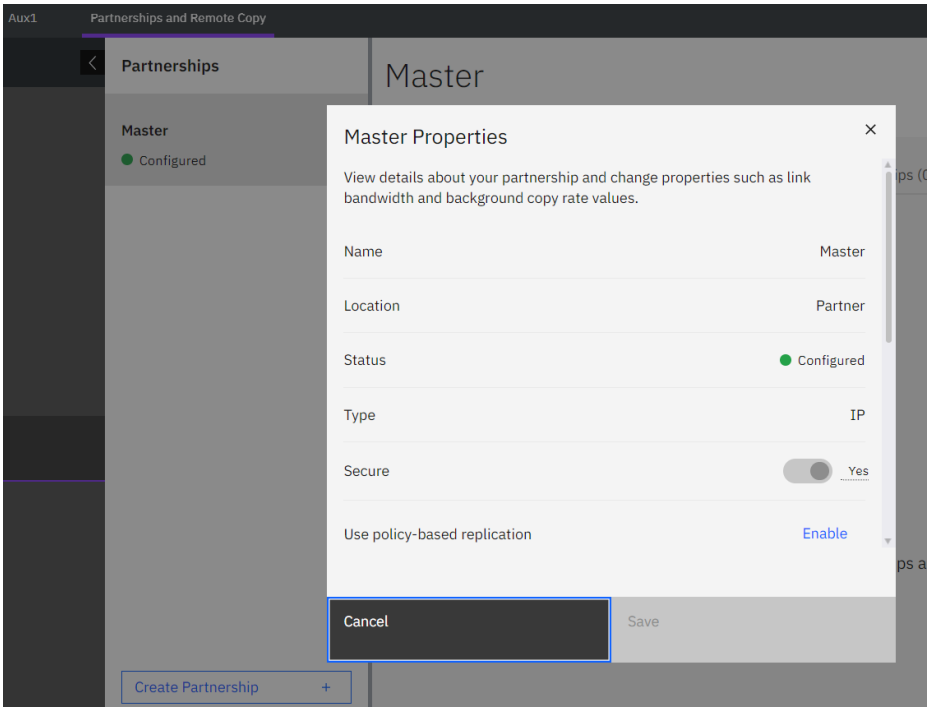

Figure 19. Fully configured secured IP partnership.

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 Managing certificates for secure communications 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.

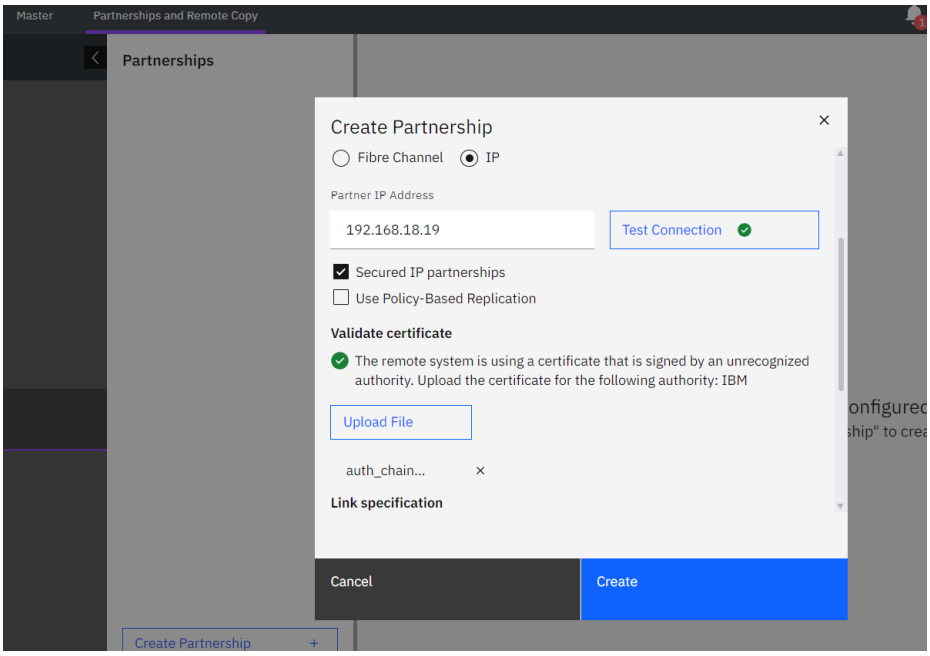

Figure 20. Create secured IP partnership.

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

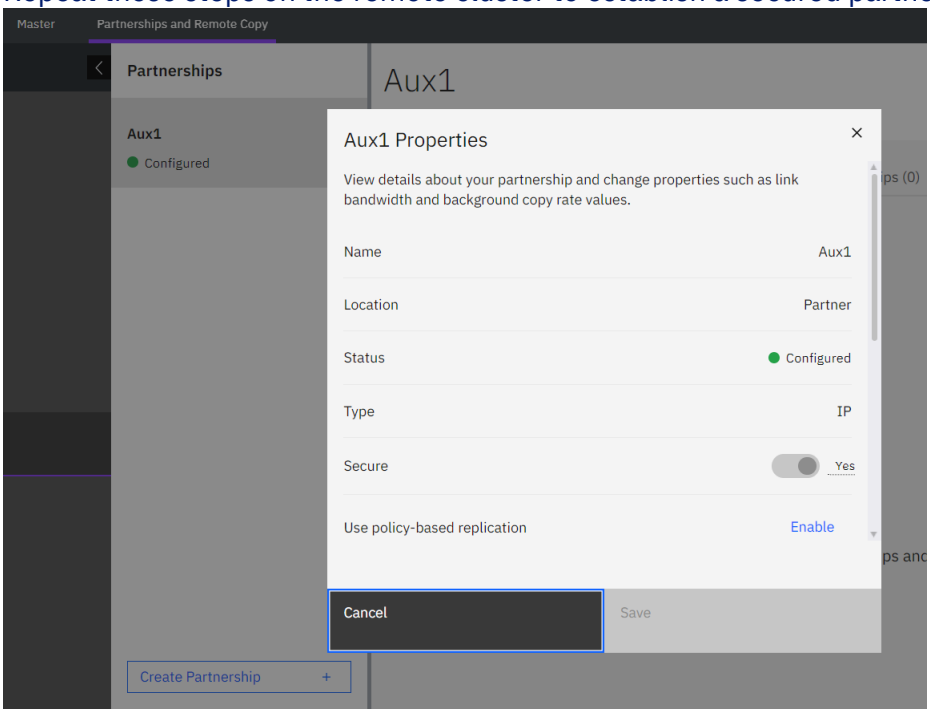

Figure 21. Fully configured secured IP partnership.

- 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.

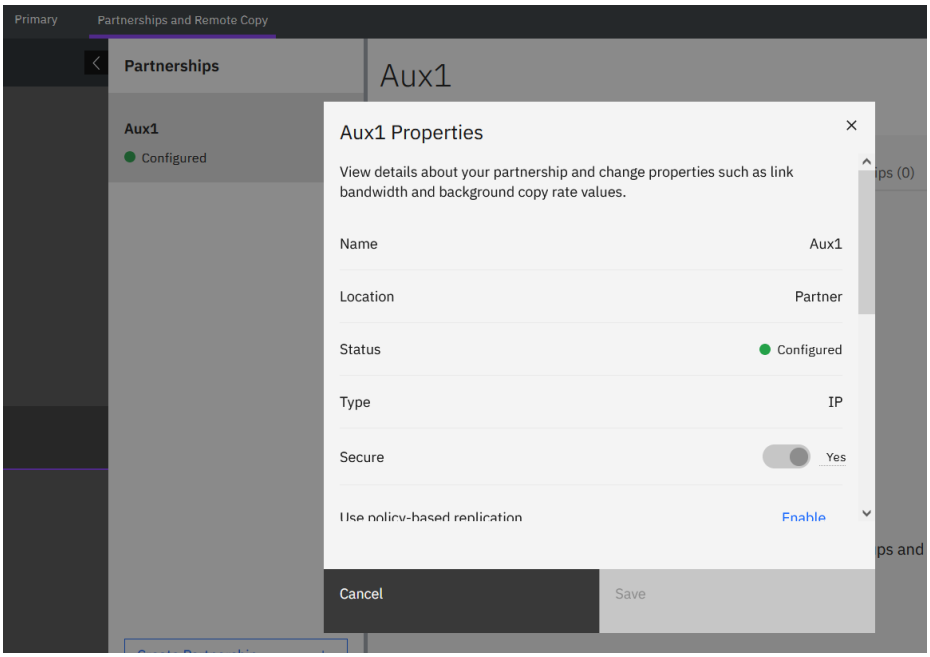

Figure 22. Fully configured secured IP partnership.

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>
```

3. Run the following command on both the clusters to start the partnership.
```
# svctask chpartnership -start <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.

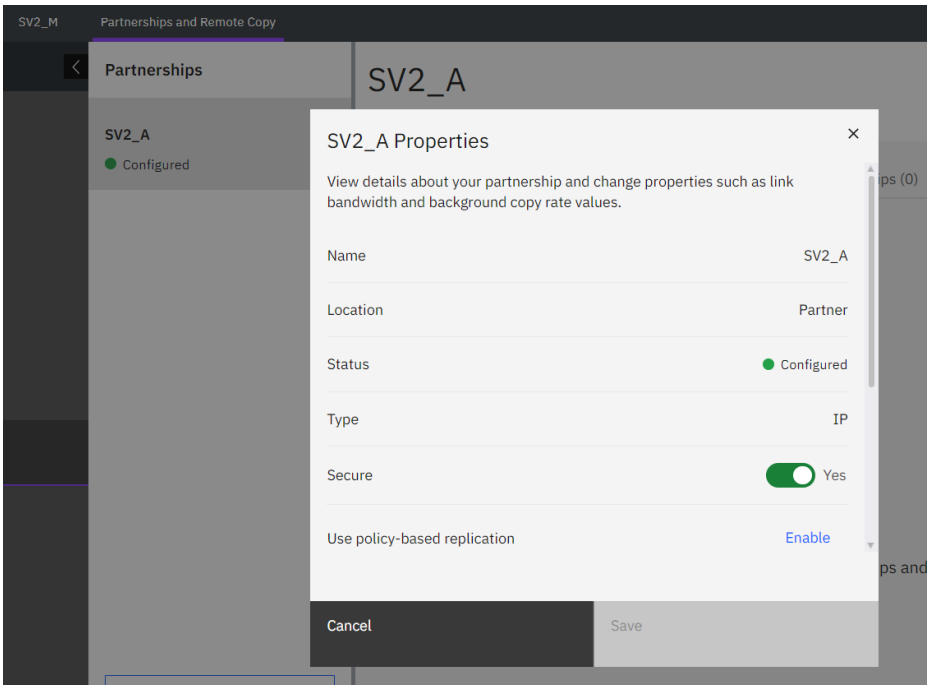

Figure23 . Secure status of a partnership.

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 0000020327E18C06
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 → 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 → Events** section on Cluster A. This is the EDIF error code for authentication failure. Following figure provides the error details:

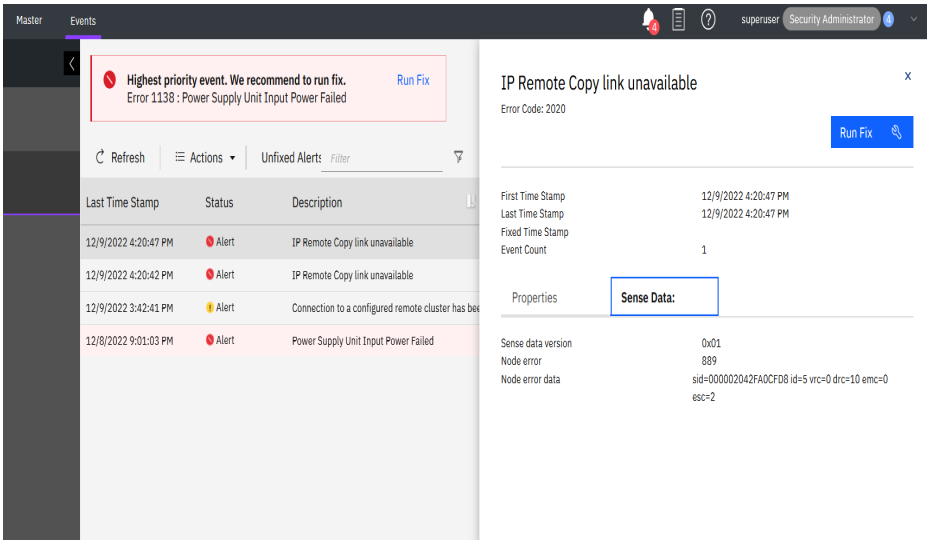

Figure 24. Event sense data for IPsec error code.

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.

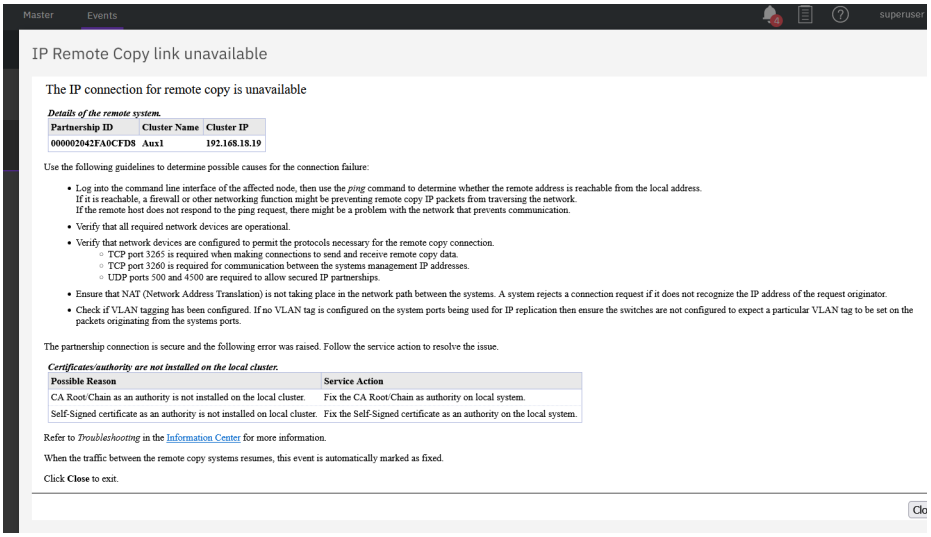

Figure 25. Run fix for IPsec error code.

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.
- RFC4303: IP Encapsulating Security Payload (ESP).
- IPsec and IKE Document Roadmap (RFC).
- Managing Certificates for secure communications.

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: demahaj1@in.ibm.com

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

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: ashjosh1@in.ibm.com

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**

IBM Corporation New Orchard Road Armonk, NY 10504

Produced in the
United States of America
July 2023