Using Replication for Disaster Recovery of Event Broker Services (Controlled Availability)

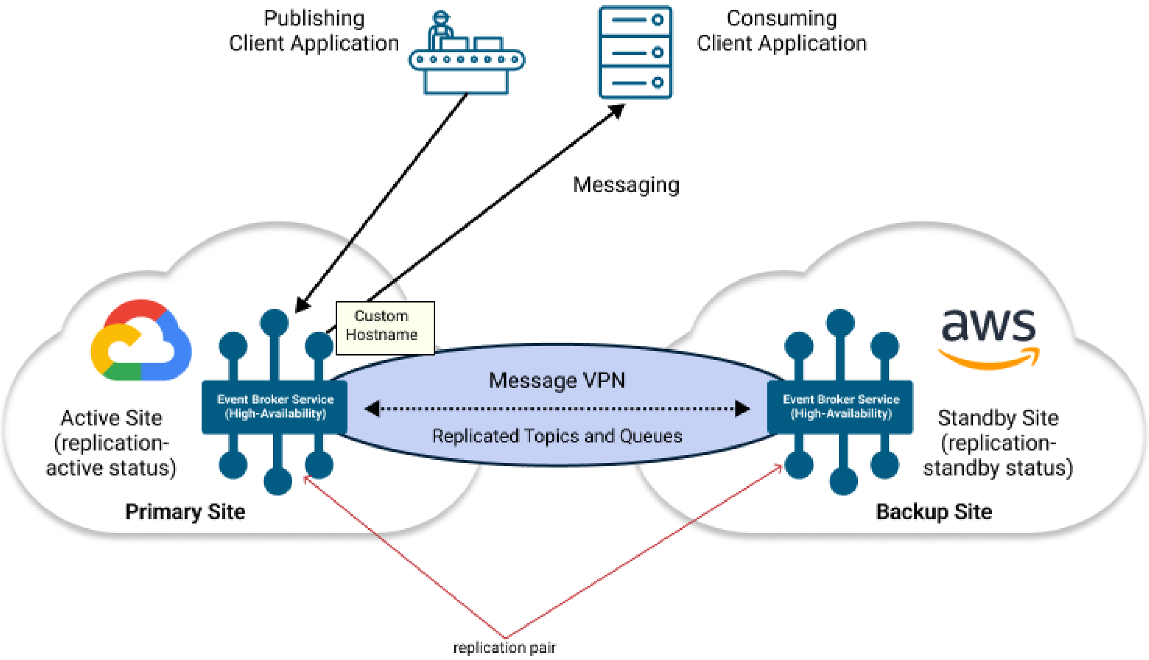
Generated: Friday, December 22, 2023

Contents

Using Replication for Disaster Recovery of Event Broker Services

To mitigate downtime and data loss that results when disasters occur, SAP offers *replication* as the solution for disaster recovery for deployments of event broker services. When you use replication, you create identical event broker service in separate cloud regions or data centers (at least 50-100 miles away from each other). For simplicity, the main location where you use your event broker services is referred to as the *Primary site*; the replicated site used as the alternate location is referred to as the *Backup site*. Each combination of Primary and Backup sites is referred to as a *replication pair*.

You can configure replication with any deployment ownership model (Public Region, Dedicated Region, and Customer-Controlled Region). You can also choose to use a mix of deployment ownership models when you configure your Primary and Backup sites. For example, you can choose to use a Customer-Controlled Region for your Primary site and a Dedicated Region for your Backup site. The site where the Message VPN of the event broker service has a replication status of `active` is referred to as the *Active site*, while the site that is in a `standby` status is referred to as the *Standby site*. Client applications connect to the site using a custom hostname (sometimes referred to as an alternate hostname), which is assigned only to the Active site. The Active site can be the Primary site or Backup site depending on the replication status.



Roles and Responsibilities for Disaster Recovery of Event Broker Services

Disaster recovery for Home Cloud and the Cloud Console is the responsibility of SAP.

You (the customer) are responsible for:

- configuring replication for the event broker services
- performing replication failovers, either for testing purposes or if a disaster condition impacts your event broker services
- monitoring your replication sites

The following table lists the various roles and responsibilities for replication with advanced event mesh. Though you are responsible for configuring, managing, and operating replication for your deployment, you can contact SAP for support. Note that:

- Support tickets are generated to document your conversations and interactions with SAP.
- You own the process of configuring replication and recovering your event broker services.

Activity	You (the Customer)	SAP
Disaster recovery for Home Cloud and Cloud Console	✗	✓
Providing the Global-Admin account for the event broker services (See Getting a Global-Admin Access Account for an Event Broker Service)	✗	✓
Planning and implementation of replication for disaster recovery ofevent broker services	✓	✗
Creating the event broker service (the replication mate) at the Backup site	✓ We recommend that you notify SAP that you plan to configure replication.	✗

Activity	You (the Customer)	SAP
Configuring replication	✓	✕
Configuring the Dynamic Messaging Routing (DMR) links within the DMR cluster (internal DMR links) between other DMR nodes (external DMR links). External DMR links are only required if you creating a mesh using external DMR links.	✓	✕
Testing replication	✓	✕
Performing a failover between replication sites	✓ You are responsible for notifying SAP that you are testing your replication configuration.	✕
Recovering a failed replication site after an uncontrolled failover	✓	✓

Considerations and Best Practices for Using Replication

The following is a list of considerations, limitations, and best practices for using replication of event broker services in advanced event mesh:

Limitations of Using Replication

The following are the limitations of using replication for event broker services.

- Only Enterprise services (broker version 10.0 or later) are supported. Standard 100 services are not supported.

- The Active site must be configured with a custom hostname. SAP recommends that customers use only one hostname.

  Client applications must only connect to the event broker service using the custom hostname configured for the replication pair. Client applications must not use the IP addresses or the default, generated names for the event broker services because during failover, they won’t be able to connect to the correct site.

- During the configuration of replication, you must disable and remove the cluster name from the Backup site. This temporarily causes inconsistencies during the configuration process in advanced event mesh and that status of the event broker service , but are resolved upon completion of the procedures in this guide.

- If your event broker service is part of an event mesh that was created with Mesh Manager, you cannot use Mesh Manager (Beta) to configure the external DMR links for the replication site. As described in this guide, you must manually configure the Dynamic Message Routing (DMR) links between:

  - each DMR node in the DMR cluster using Solace CLI
  - each DMR node that requires an external DMR link using Broker Manager
  - between the replication mates

  For more information, see Configuring Replication in an Event Mesh.

  > Though you can view your event mesh using Mesh Manager there may be validation errors when you perform a Health Check. You won't be able to use Mesh Manager to further manage the event mesh.

- The replication configuration information and statistics for replication are not monitored by SAP for replication. See Monitoring Best Practices for options.

- To set up a replication pair, the Message VPN names must match. You cannot change the name of the Message VPN after service creation in advanced event mesh.

  If you do not set the matching Message VPN name for your replication pair, you must delete the service and recreate it. For more information about how to set the Message VPN name at service creation time, see Setting the Message VPN Name.

- Advanced configuration options performed in the Cloud Console using Cluster Manager must be manually synchronized. In addition, some configuration is not synchronized between the replicated pairs because there are properties that are considered unique to the event broker service in advanced event mesh.

Monitoring Best Practices

It is your responsibility to monitor the replication sites. The replication configuration information and statistics for replication are not monitored by SAP. You have these options:

1. (Recommended) If you have subscribed to Insights, you can monitor the following SYSLOG in Datadog using Insights:
   - `VPN_REPLICATION_SERVICE_DEGRADED`
   - `SYSTEM_CFGSYNC_DOWN`

   With Insights, you can also use the following metrics to monitor replication:
   - `derived_metrics.vpn.replication_status`
   - `derived_metrics.vpn.replication_sync_eligible.reject`
   - `derived_metrics.vpn.replication_sync_eligible.downgrade`
2. Monitoring event broker services using SYSLOG, you must monitor for these broker events:
   - `VPN_REPLICATION_SERVICE_DEGRADED`
   - `SYSTEM_CFGSYNC_DOWN`

Event Broker Service Best Practices

The following are best practices when configuring your event broker services for replication help ensure that you replication functions as you expect:

- SAP recommends that you synchronize all service configuration in the Cloud Console between the event broker services **before** you enable replication. If replication is already enabled, ensure that you synchronize all the configuration configured in the Cloud Console before you make any changes in Broker Manager. The configuration must be manually synchronized between the event broker services using **Cluster Manager > Manage** in the Cloud Console.

  > If you are making multiple configuration changes, you can remove the replication feature, make and manually synchronize the configuration changes between the event broker services, and then re-enabling replication feature.

- Config-Sync synchronizes the configuration between the replication pairs, such as client profiles and client usernames between the Active and Standby sites. However, advanced configuration options performed in the Cloud Console using Cluster Manager must be manually synchronized. In addition, some configuration is not synchronized between the replicated pairs because they are properties that are considered unique to the event broker service.

These configuration options must be manually performed on both the event broker service on the Active and Standby sites for:

- port configuration (connection endpoints)

> We recommend that the same ports and port numbers be configured on both the Active and Standby sites.

- message spool sizes

> Message spool sizes must be the same size on both event broker service in your replication pair (both the Active and Standby site). After you enable replication, you cannot resize the message spool on the Standby site.

- log forwarding
- LDAP authentication

> If replication is enabled, the LDAP profiles must be synchronized prior to using LDAP authentication. If you use an LDAP profile before it is synchronized on the Standby site, this may cause Config-Sync state to go down.

- SEMP request over message bus

Terminology for Replication

The following terms are used throughout the discussions of and instructions for replication of event broker services in advanced event mesh.

Primary Site

For a pair of replication mates, this is the main site and the event broker service that is has the replication-active status.

Backup Site

For a pair of replication mates, this site often acts as the Standby site and the event broker service that is has the replication-standby status.

Failed Site

The site that is currently in a bad status due to a disaster. It might be the Active site at the time the disaster occurred. A Restored site is a failed site whose serviced has been recovered. Prior to recovery of the Failed site, the activity has been switched over to the Backup site.

Replication Pair

Refers to two event broker services that have the same Message VPN name, typically configured in separate regions, and configured with the replication feature. Each are replication mates of each other.

Replication Mate

Refers the other event broker service in a replication pair.

Replication-Active

Indicates the active event broker in the context of the Replication feature. This term is used to avoid confusion with active event broker service in a High-Availability Configuration where there is an active event broker and standby event broker.

Replication-Standby

Indicates the standby event broker in the context of the Replication feature. This term is used to avoid confusion with active event broker service in a High-Availability Configuration where there is an active event broker and standby event broker.

Active Site

The Message VPN for an event broker service in a replication pair that clients connect to for messaging traffic. It has a replication status of `active`. Generally, the Primary site is the Active site. Depending on the replication status, the Active site can be the Primary site or Backup site.

Standby Site

The Message VPN for an event broker service in a replication pair that is not active and replicates the messages. It has the replication status of `standby`. Generally, the Backup site is the Standby site. Depending on the replication status, the Standby site can be the Primary site or Backup site.

Redundancy Group

A redundancy group is an event broker service configured with high-availability (HA), which is required to configure replication in advanced event mesh. The group consists of three software event brokers, which are the *primary event broker*, *backup event broker*, and *monitoring node*. When you are configuring replication, you must use the router name of the primary event broker. For more information, see see High Availability in SAP Integration Suite, Advanced Event Mesh .

The primary event broker provides messaging services to client applications while the backup event broker waits in standby mode. The backup broker only provides service should the primary event broker fail. The monitoring node is a third event broker that acts as a tie-breaker and prevents split-brain scenarios that would otherwise cause both the primary and backup event brokers to be active simultaneously.

Failover

The act of switching activity from one event broker service to its replication mate. The failover is complete when the custom hostname is assigned to newly Active site.

Host List

For client applications, a host list specifies the list of hosts to try. When replication is configured for event broker services, the host list should never use the generated names nor the

IP addresses of the event broker services. Only the custom hostname for the replication pair must be used.

Custom Hostname

In advanced event mesh, you must configure a custom hostname for client applications to use to connect to the replication-Active event broker service. The custom hostname is an alternate hostname to access the event broker service. When you use the replication feature, you cannot use the system-generated hostnames for failover and we recommend that you do not use the initial generated hostnames for client connections.

Uncontrolled Failover

An uncontrolled failover occurs due to a sudden loss of connectivity to an Active site. When this occurs, only synchronous replication mode messages are guaranteed not to be lost. Messages remaining in the replication queue are not available at the disaster recovery site.

Controlled Failover

A controlled failover occurs when activity is transferred from one replication site to its replication mate in a planned manner for operational reasons. When you successfully follow the controlled failover procedure, no messages are lost, regardless of the replication mode of the messages.

Synchronous Message Replication

A message or transaction is not considered persisted until it has been confirmed to be stored on both the active and standby sites. While providing a greater guarantee that the published message or transaction is not lost in an uncontrolled failover, synchronous replication incurs a performance penalty for the publisher, especially blocking publishers. This is because the publisher has to wait for communication between the two replication sites to complete before publishing the next message or transaction. In those use cases, the maximum message rate of a single publisher is limited by the round-trip time and available bandwidth between the active and the standby sites.

Asynchronous Message Replication

A message or transaction is considered persisted once it has been spooled and put into the replication queue (`#MSGVPN_REPLICATION_DATA_QUEUE`) on the Active site. This type of replication gives improved performance, since the event broker service does not have to wait for communication with the Standby site to complete. However, during an uncontrolled failure of the Active site, there is a chance that a message or transaction that the client has been told has completed was not actually delivered to the standby site. In this uncontrolled case, messages or transactions may be lost or duplicated.

Configuring Replication of Event Broker Services

SAP recommends that you synchronize all service configuration in the Cloud Console between the replicated pair **before** you enable the replication feature. For more information, see Considerations and Best Practices for Using Replication.

To configure replication, you use a mix of Solace CLI commands, theBroker Manager, and the Cloud Console.

Prerequisites

To configure replication, you must be familiar with configuring event broker services using the Solace CLI commands, the Cloud Console, and Broker Manager.

- You require a new user account on the event broker service. For more information, see Getting a Global-Admin Access Account for an Event Broker Service.
- You require a user account in advanced event mesh with the Cluster Editor or Administrator role, and access to Broker Manager. For more information, see Roles and Permissions.
- Your client applications must connect to event broker service using its custom hostname as an alternate hostname. Your client applications that use messaging must not use the initial, generated name created for the event broker service. For more information, see Adding a custom hostname.

High-Level Steps

The following are the high-level steps to configure replication for advanced event mesh:

1. In the Cloud Console, add a new event broker service as to be your replication pair.
2. Using the Solace CLI on both event broker services (replication mates) in the replication pair, configure the replication settings.
3. Repeat the process as required for each replication pair.

If you want your event broker service to be part of an event mesh, add the Primary site to your event mesh before you start configuring replication. For more information about configuring an event mesh with replication, see Configuring Replication in an Event Mesh.

For a summary of the configuration settings used in the set-up procedures, see Example Replication Information.

Replication only starts copying messages from the point in time when it is configured (enabled) and the replication topics are set for those queues. Any long-lived messages in the queue before replication is configured or before the replication topics are configured, are not copied over to the replication mate.

Example Replication Information

The following table summarizes the example configuration information that is used in the examples for configuring replication. These examples are for illustrative purposes only. We recommend that you record your settings when you configure replication for your event broker services.

Event Broker Configuration Item	Primary Site	Backup Site	Description Details for the Sites
Name of service	primary-myfirstservice Service-class: Enterprise 250 Region: EKS - US East (Ohio)	backup-myfirstservice Service class: Enterprise 250 Region: EKS - Canada Central (Canada)	Both must be broker version 10.0. Both services must have the CLI

Event Broker Configuration Item	Primary Site	Backup Site	Description Details for the Sites
			port enabled (CLI Host (SSH) port option in the connection endpoint)
Name of Message VPN	myfirstservice	myfirstservice	These must be the same.
Default Hostname	mr-connection-bo3i1bd7ewc.messaging.solace.com	mr-connection-u4ehjwoe9xa.messaging.solace.com	This is the default generated hostname that you use to access the event broker service. These names must not be used by the client applications that connect for

Event Broker Configuration Item	Primary Site	Backup Site	Description Details for the Sites
			messaging.
Name of primary router	nanoproductionazzn9vsqdk5solaceprimary0	nanoproduction89il3uubs0csolaceprimary0	For all examples, we are presuming the primary router in the High-Availability Group is active.
Name of backup router	nanoproductionazzn9vsqdk5solacebackup0	nanoproduction89il3uubs0csolacebackup0	
Name of cluster	my-first-cluster	my-first-cluster	
User with Global access and Admin level	**User**: mycompany-global-admin **Password**: myglobaladminpassword	**User**: mycompany-global-admin **Password**: myglobaladminpassword	
Name of client profile	myfirstprofile	myfirstprofile	
Name for clientusername	myfirstclientusername	myfirstclientusername	

Event Broker Configuration Item	Primary Site	Backup Site	Description Details for the Sites
Password of client username	myfirstclientpassword	myfirstclientpassword	
Custom Hostname	myfirsthostname	N/A	Only configure one hostname between the replication mates in your replication pair.

Configuring the Event Broker Services for as a Replication Pair

You configure two event broker services as *replication mates* for your replication pair. The Primary site is where your VM-based event broker service is located (the source) and the Backup site, is where your copy of the event broker service exists that's in a Kubernetes-based deployment.

> SAP recommends that you synchronize all service configuration in the Cloud Console between the replicated pair **before** you enable the replication feature. For more information, see Considerations and Best Practices for Using Replication.

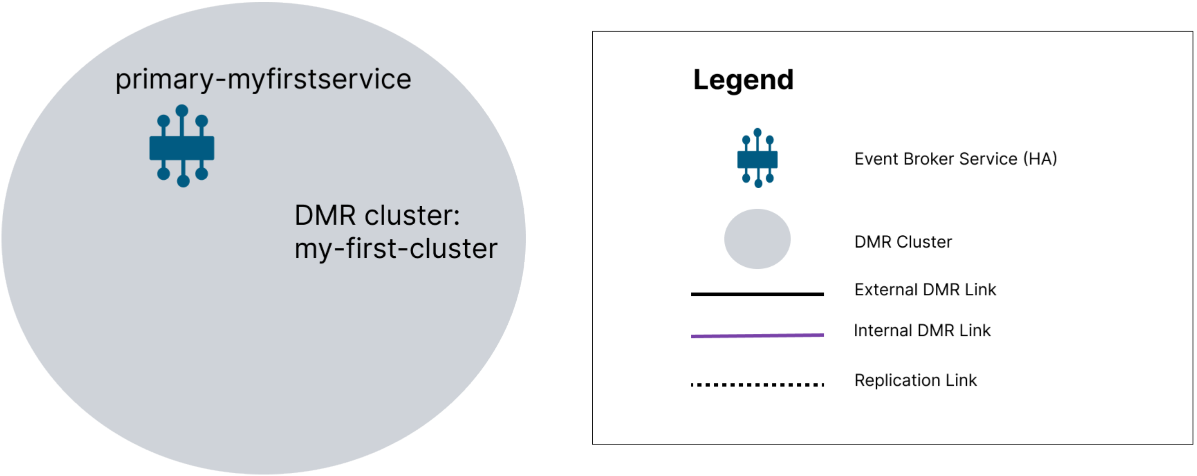
The high-level steps for creating a replication pair are as follows:

1. In the Cloud Console, create event broker services Backup replication site. This presumes you have a Primary site created. See Event Broker Service Best Practices about creating your event broker services.
2. Enable **Secured CLI Host (SSH)** on the event broker services.
3. Create specific client profiles and client usernames for replication on each event broker service.
4. Create a custom hostname on the event broker service that will be the initial active site for the replication pair (generally this is the primary site).

For a summary of the configuration settings used in the steps below, see Example Replication Information.

Create Event Broker Service in Different Regions in the Cloud Console

The steps below presume you have created an event broker service (for example, the `primary-myfirstservice` has a Message VPN name of `myfirstservice` and a cluster name of `my-first-cluster` that will be the Primary replication site. For example the starting topology or steps is a single event broker service. In advanced event mesh, event broker services are enabled with DMR and reside in their own cluster.



The Backup event broker services (Backup site) that you create to be the replication mate must be the same :

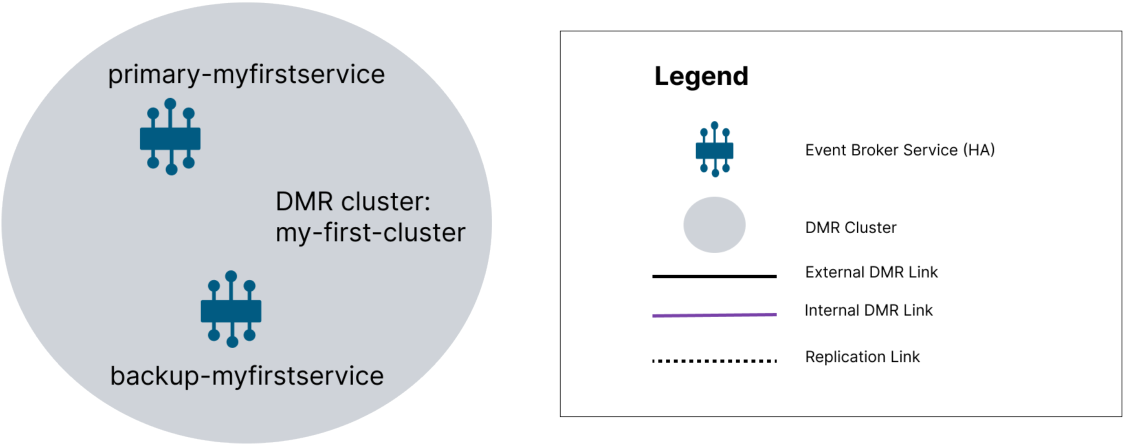
- have high-availability (HA) configured
- be the same Enterprise service class
- have the same Message VPN name

- we recommend that you create the backup in a different regions
- the same cluster name
- have the same ports configured

For more information about what to ensure you synchronize after creation, see Event Broker Service Best Practices

To create the event broker service, in the Cloud Console in Cluster Manager, do the following:

1. In the region you want to use as the Backup site, create an event broker service using the same service class. Ensure that you set the Message VPN name **and** the cluster name to be the same as the event broker service of your Primary site. For example, create a service named `backup-myfirstservice`, with a Message VPN name of `myfirstservice` and a cluster name of `my-first-cluster`. After you create the `backup-myfirstservice` in the same cluster as the `primary-myfirstservice` topology:



For information about creating event broker service, see Creating Event Broker Services.

> If you did not create matching Message VPN names for your pair of replication mates, you must delete them and recreate them. Message VPN names can only be configured when you create the event broker service and cannot be modified in advanced event mesh after service creation. For more information, see Setting the Message VPN Name.

Enable the Secure CLI Host (SSH) Port on the Event Broker Services

We recommend that you enable the Secure CLI Host port only for private endpoints in Dedicated Regions or Customer-Controlled Regions because those are accessible via private IP addresses instead of the public Internet.

For Public Regions, we recommend that you only enable the CLI port when you to need to configure replication or when a failover is required, otherwise disable the port.

You can enable the Secure CLI Host (SSH) port in the Cloud Console. Remember to apply the same changes for both the primary and backupevent broker services in your replication pair. For more information, see Changing the Port Configuration for an Event Broker Service .

Create a Client Profile and Client Username for Replication

You must create a client profile specifically for replication. A replication-specific client profile is required because:

- If there is a difference of message delivery priority between replication and messaging activities, it ensure a higher priority is given to site replication.
- WAN tuning is required for replication. You must set **Priority Queues - G-1 Minimum Burst** to `66000`. The default value the setting is `256`.

> We recommend you use the same client profile and client username for both replication mates.

For example:

1. On the primary event broker service, create a replication-specific client profile (for example, **myfirstclientprofile** on **Primary-myfirstservice**) and configure the following settings:
   - Toggle **Add Shared Subscriptions** so that it is enabled.
   - Set **Priority Queues - G-1 Minimum Burst** to 66000.
2. Confirm the following additional settings in the client profile:
   - Send guaranteed messages (Enabled)
   - Use transacted sessions (Enabled)
   - Use compression (Enabled)

- Receive guaranteed messages (Enabled)
- Allow client to create endpoints (Enabled)
- Connect as a bridge (Enabled)

3. Ensure that the **Connect When Replication Standby** setting is disabled. It is not used for replication in advanced event mesh.
4. Create a client username and set the **Client Profile** field to the client profile you created in the previous step.

   For example, create a client username called `myfirstclientusername` on `Primary-myfirstservice`
5. Enable the client username and set the password (for example, `myfirstclientpassword`). Make a note of the password for configuring the rest of replication.
6. Repeat steps 1 to 5 for the other event broker service in your replication pair. For example, create a client profile named **myfirstclientprofile** on the event broker service called **Backup-myfirstservice**.

Create a Custom Hostname for the Replication Pair

Clients must use a custom hostname to connect to one of the replication mates when you use replication in advanced event mesh. Client applications must not use the IP address or the initial, system-generated hostnames for event broker services configured as replication pairs in advanced event mesh.

1. Choose the event broker service in your replication pair.
2. Add a custom hostname to that event broker service, such as `myfirsthostname`.
   For information about creating a custom hostname , see Adding a Custom Hostname.

> Do not create a hostname for the event broker service at the Standby site.
>
> As part of the procedure for failing over to the other replication site, the custom hostname is reassigned the newly Active site.

Configuring the Replication Mates

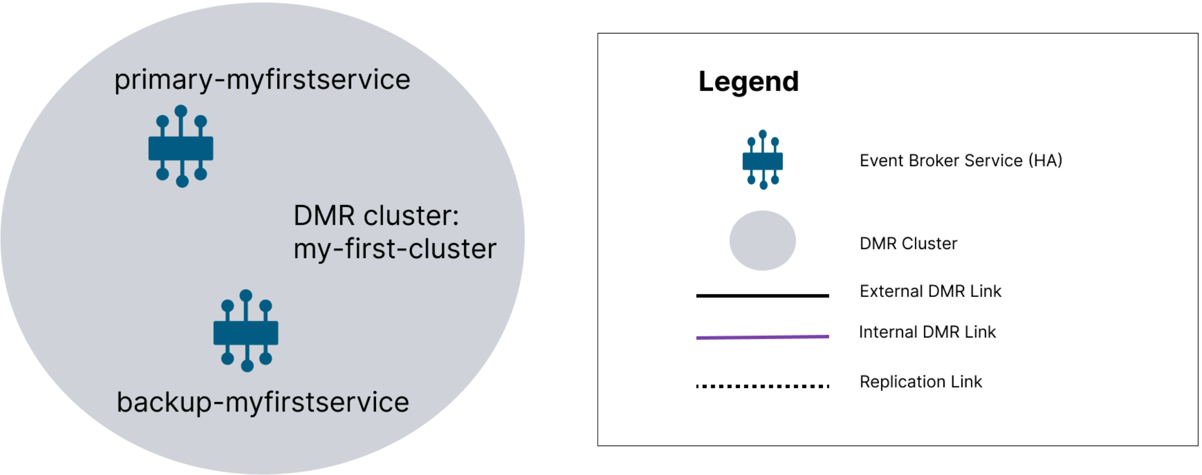
You use a combination of Solace CLI commands, the Cloud Console, and Broker Manager to complete the configuration of the replication feature on your event broker services.

> The Solace CLI is used to configure and monitor event brokers. The commands are organized in a tree-like structure. When you the Solace CLI to configure a feature on an event broker, generally you start with system-level configuration, proceed to Message VPN level configuration, and then more specific parameter changes to tune feature behavior. For more information, see Using the Solace CLI on the Solace website.

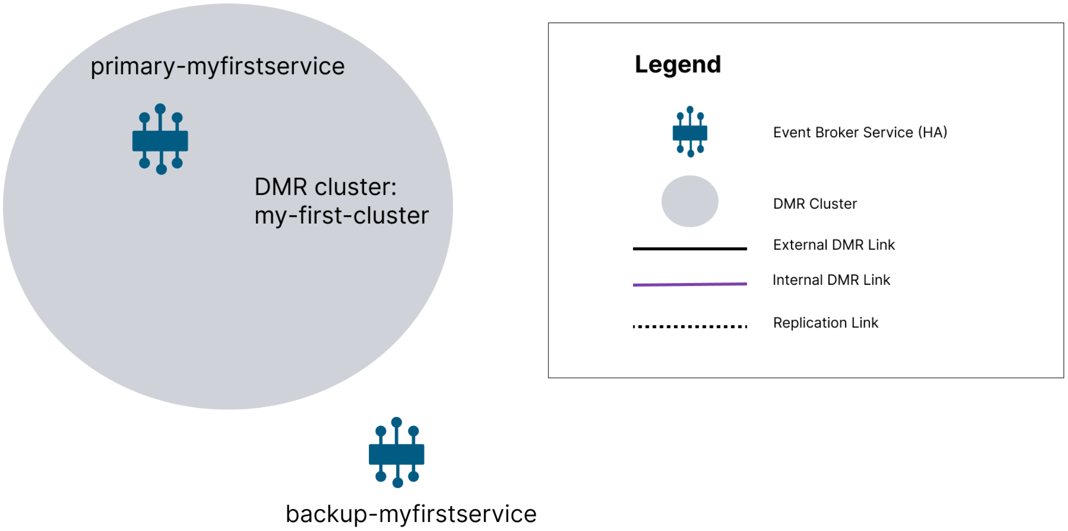
After you have created the two event broker services for the Primary and Backup sites, you use the following steps to configure the settings for replication. These steps presume that you have created the two event broker services as follows:

- the Message VPN name is the same on both
- the cluster name is the same on both
- you have the ports on both event broker services enabled and the CLI port is enabled
- you have a Global-Admin account. For more information, see Getting a Global-Admin Access Account for an Event Broker Service.

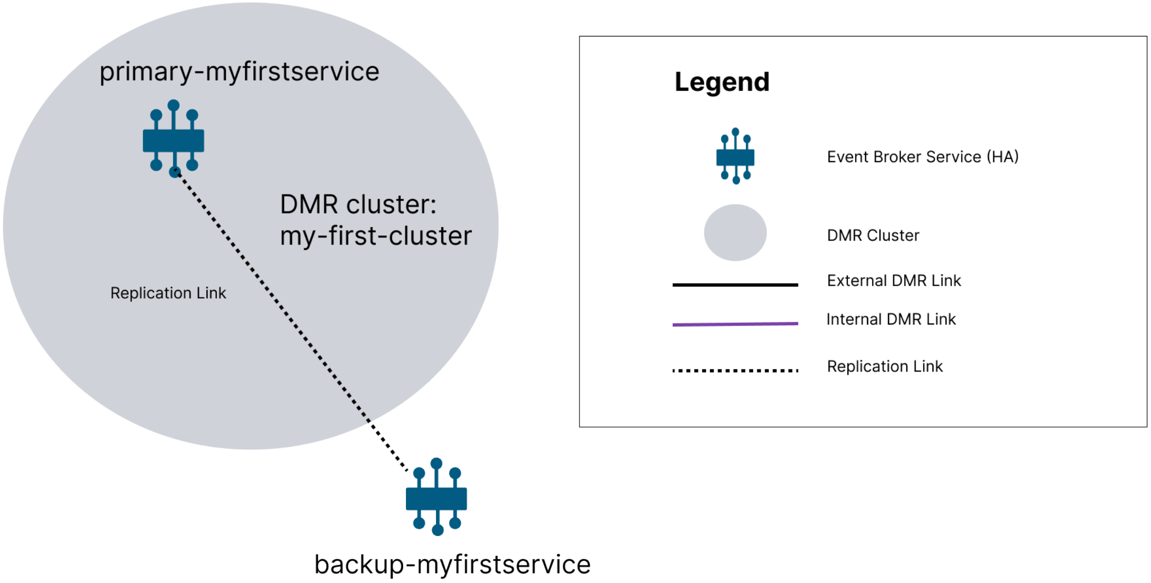
The topology before you begin these steps is two services in the same cluster:



1. Disable Dynamic Message Routing on the Backup Site. After this step, the topology shows the backup-myfirstservice without a DMR cluster.

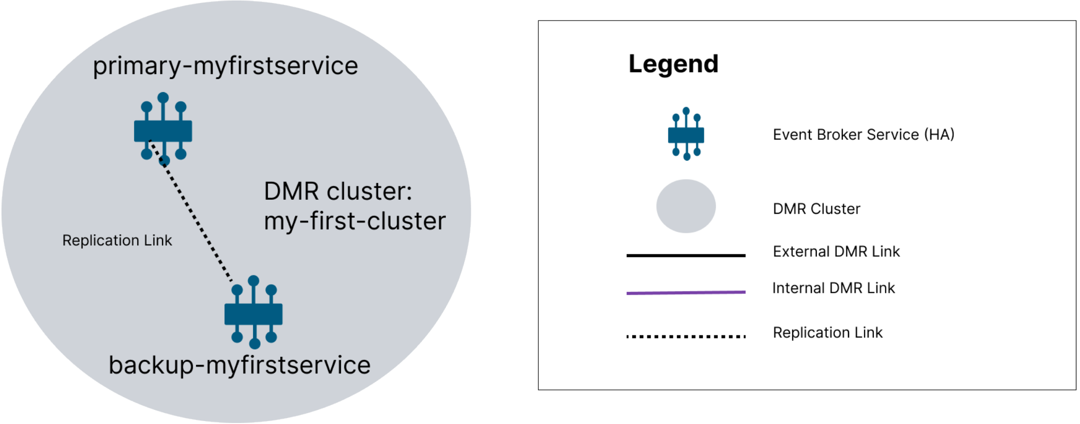


2. Configure the Replication Mate Settings.
3. Configure the System-Level Replication Settings.
4. Configure the VPN-Level Replication Settings.
5. Set the Replication State of the Message VPN as follows:
   - For the event broker service that has the custom hostname assigned, set it as the `active` state
   - For the other event broker service, set it as `standby` state
6. Enable Replication. After this step, you have configured replication and the topology is a replication link between the primary-myfirstservice and backup-myfirstservice.

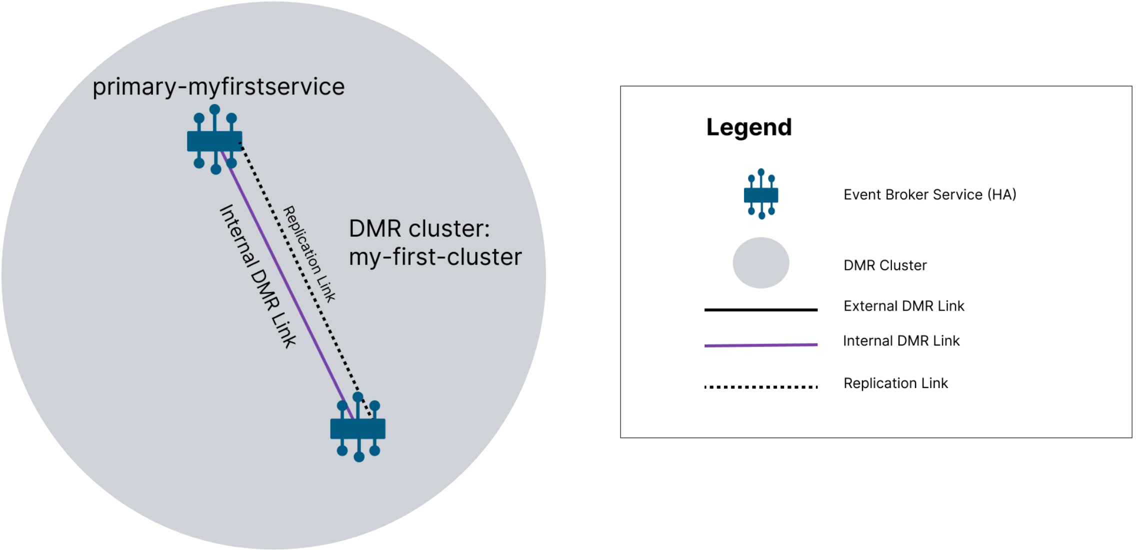


7. Validate the Replication Configuration.

8. Add the Backup Site to the DMR Cluster of the Primary Site. After this step, the `primary-myfirstservice` and `backup-myfirstservice` belong to the same DMR cluster.



9. Add the DMR Internal Link Between the Primary Site and Backup Site. After this step, the `primary-myfirstservice` and `backup-myfirstservice` have an internal DMR link between them.



10. Specify the Queues and Topics for Replication.

For all examples and procedures, we assume that the primary event broker is Active in the High-Availability Group.

Replication only starts copying messages from the point in time when it is correctly configured (enabled) and the replication topics are set for those queues. Any long-lived messages in the queue before replication is configured and the replication topics are configured, are not copied over to the replication mate.

For example, `ssh to mr-connection-bo3i1bd7ewc.messaging.solace.com` and `ssh mr-connection-u4ehjwoe9xa.messaging.solace.com`, respectively.

Disable Dynamic Message Routing on the Backup Site

By default, event broker services are enabled with the Dynamic Message Routing (DMR) feature and hence are assigned a cluster name at creation time. This cluster name is stored in advanced event mesh for SAP Integration Suite, but must be deleted prior to configuring the replication to disable DMR on the Backup site.

After you disable DMR and remove the cluster name, the cluster name still appears in the **Status** tab for the event broker service in Cluster Manager. This is expected and you will be re-adding it back later.

1. If you haven't done so yet, use SSH to login to the event broker service using its generated hostname and your Global-Admin account. For information, see Getting a Global-Admin Access Account for an Event Broker Service.
2. Run the `show cluster *` command to see the name of your cluster. For example:

```
nano-production-azzn9vsqdk5-solace-primary-0> show cluster *
Cluster Name          : my-first-cluster
Node Name             : nanoproductionazzn9vsqdk5csolaceprimary0
Enabled               : Yes
Operational           : Yes
Fail Reason         :
Uptime              : 5d 1h 0m 56s
Links Up            : 1 of 1
Channels Up         : 1 of 1
Topology Issues     : 0
```

3. Using the Solace CLI, delete the cluster name and disable the DMR feature Solace CLI on the Backup site. For example, run the following commands:

```
SolaceCLI > enable
SolaceCLI # configure
SolaceCLI (configure)# routing dynamic-message-routing cluster <name-of-cluster>
SolaceCLI (...uting/dynamic-message-routing/cluster)# shutdown
SolaceCLI (...uting/dynamic-message-routing/cluster)# exit
```

For example, on the Backup site:

```
nano-production-azzn9vsqdk5-solace-primary-0> enable
nano-production-azzn9vsqdk5-solace-primary-0# configure
nano-production-azzn9vsqdk5-solace-primary-0(configure)# routing dynamic-message-routing cluster my-first-cluster
nano-production-azzn9vsqdk5-solace-primary-0(...uting/dynamic-message-routing/cluster)# shutdown
nano-production-azzn9vsqdk5-solace-primary-0(...uting/dynamic-message-routing/cluster)# exit
nano-production-azzn9vsqdk5-solace-primary-0(...igure/routing/dynamic-message-routing)# no cluster my-first-cluster
```

4. If you run the `show cluster *` command in the Solace CLI, no cluster is listed.

You are now ready to configure being configuring replication.

Configure the Replication Mate Settings

You must set up the replication mates to start configuring replication. This step configures the replication mate information for your replication pair. The router names of the Message VPN for each of the event broker services and the generated hostnames are used.

The following are the steps to configure the replication mates:

1. If you haven't done so yet, use SSH to login to the event broker service using its generated hostname and your Global-Admin account. For information, see Getting a Global-Admin Access Account for an Event Broker Service.

   For example, `ssh to mr-connection-bo3i1bd7ewc.messaging.solace.com` and `ssh mr-connection-u4ehjwoe9xa.messaging.solace.com`, respectively.

2. Determine the router names of the Message VPN for each of the replication mates on both the Primary and Backup sites. The router name of the primary event broker (not the backup event broker) in a high-availability event broker service must be used for configuring replication.

You can use the `show redundancy group` USER command to determine the router name of the primary broker. For example, if you were on the backup broker on the Primary site, the router name of the primary broker is `nanoproductionazzn9vsqdk5solaceprimary0`) :

```
nano-production-azzn9vsqdk5-solace-backup-0(configure/redundancy)#
show redundancy group
Node Router-Name   Node Type       Address           Status
-----------------  --------------  ----------------  ---------
nanoproductionazz  Message-Router  nano-production-  Online
n9vsqdk5solacebac                    azzn9vsqdk5-so
up0                                  lace-backup-0.
*                                    .nano-productio
                                     n-azzn9vsqdk5-
                                     -solace-discove
                                     ry.solace-clou
                                     d.svc
nanoproductionazz  Monitor         nano-production-  Online
n9vsqdk5csolacemon                   azzn9vsqdk5-so
itoring                              lace-monitor-0
                                     .nano-producti
                                     on-azzn9vsqdk5
                                     -solace-discov
                                     ery.solace-clo
                                     ud.svc
nanoproductionazz  Message-Router  nano-production-  Online
n9vsqdk5csolacepri                   azzn9vsqdk5-so
mary0                                lace-primary-0
                                     .nano-producti
                                     on-azzn9vsqdk5
                                     -solace-discov
                                     ery.solace-clo
                                     ud.svc


* - indicates the current node
```

3. Configure the replication mate for each event broker service using the **primary router name** and default generated hostnames:

```
SolaceCLI > enable
SolaceCLI # configure
SolaceCLI (configure)# replication
SolaceCLI (configure/replication)# mate virtual-router-name
```

```
v:<primary-router-name-of-replication-mate>
SolaceCLI (configure/replication)# mate connect-via <hostname-of-
replication-mate>:55443 ssl
```

Where :

- `<primary-router-name-of-replication-mate>` is the router name that you determined from step 2. Ensure you use the replication mate (the other event broker service) and the event broker service's own router name.
- `<hostname-of-replication-mate>` is the generated hostname of the event broker service. Ensure you don't use your custom hostname. We recommend that you use the Secured SMF Host port. The default is 55443, but this may depend on your [port configuration for the service](#) .

The steps presume that you are using the primary node in a High-Availabilty configuration. If you are preforming the

For example, on the Primary site (`nano-production-azzn9vsqdk5-solace-primary-0`), run the mate command using the virtual router name and generated hostname of the Backup site:

```
nano-production-azzn9vsqdk5-solace-primary-0> enable
nano-production-azzn9vsqdk5-solace-primary-0# configure
nano-production-azzn9vsqdk5-solace-primary-0(configure)# replication
nano-production-azzn9vsqdk5-solace-primary-0(configure/replication)#
mate virtual-router-name v:nanoproduction89il3uubs0csolaceprimary0
nano-production-azzn9vsqdk5-solace-primary-0(configure/replication)#
mate connect-via mr-connection-
u4ehjwoe9xa.messaging.solace.cloud:55443 ssl
nano-production-azzn9vsqdk5-solace-primary-0(configure/replication)#
```

On Backup site (`nano-production-89il3uubs0c-solace-primary-0`), run the mate command using the virtual router name and generated hostname of the Primary site:

```
nano-production-89il3uubs0c-solace-primary-0> enable
nano-production-89il3uubs0c-solace-primary-0# configure
nano-production-89il3uubs0c-solace-primary-0(configure)# replication
nano-production-89il3uubs0c-solace-primary-0(configure/replication)#
mate virtual-router-name v:nanoproductionazzn9vsqdk5solaceprimary0
nano-production-89il3uubs0c-solace-primary-0(configure/replication)#
mate connect-via mr-connection-
bo3i1bd7ewc.messaging.solace.cloud:55443 ssl
nano-production-89il3uubs0c-solace-primary-0(configure/replication)#
```

Configure the System-Level Replication Settings

After you have formatted the virtual-router name and connect-address, configure the authentication schemes and validation name settings as system-level settings - namely the replication Config-Sync Bridge settings. We recommend that you at use at least basic authentication, SSL, Server Certificate Validation, enable SSL, and then configure the replication bridge to use the client username specific for replication you created on your event broker services.

The following are the steps to configure the replication Config-Sync:

1. If you haven't already use SSH to login to the event broker service using its generated hostname and your Global-Admin account. For information, see Accessing the CLI for Event Broker Services.

   For example, `ssh to mr-connection-bo3i1bd7ewc.messaging.solace.com` and `ssh mr-connection-u4ehjwoe9xa.messaging.solace.com`, respectively.

2. Configure replication Config-Sync Bridge and run the following command to:

   - shutdown the bridge
   - enable SSL for TLS/SSL encryption
   - configure the authentication scheme (in our example, we use basic)
   - SSL Server Certificate Validation
   - restart the bridge

   ```
   SolaceCLI > enable
   SolaceCLI # configure
   SolaceCLI (configure)# replication
   SolaceCLI (configure/replication)# config-sync bridge
   SolaceCLI (configure/replication/config-sync/bridge)# shutdown
   SolaceCLI (configure/replication/config-sync/bridge)# ssl
   SolaceCLI (configure/replication/config-sync/bridge)# authentication auth-scheme basic
   SolaceCLI (configure/replication/config-sync/bridge)# ssl-server-certificate-validation
   SolaceCLI (...dge/ssl-server-certificate-validation)# validate-server-name
   SolaceCLI (...dge/ssl-server-certificate-validation)# exit
   SolaceCLI (configure/replication/config-sync/bridge)# no shutdown
   ```

   For example, configure the Primary site (`nano-production-azzn9vsqdk5-solace-primary-0`):

```
nano-production-azzn9vsqdk5-solace-primary-0> enable
nano-production-azzn9vsqdk5-solace-primary-0# configure
nano-production-azzn9vsqdk5-solace-primary-0(configure)# replication
nano-production-azzn9vsqdk5-solace-primary-0(configure/replication)#
config-sync bridge
nano-production-azzn9vsqdk5-solace-primary-0
(configure/replication/config-sync/bridge)# shutdown
nano-production-azzn9vsqdk5-solace-primary-0
(configure/replication/config-sync/bridge)# ssl
nano-production-azzn9vsqdk5-solace-primary-0
(configure/replication/config-sync/bridge)# authentication auth-scheme
basic
nano-production-azzn9vsqdk5-solace-primary-0
(configure/replication/config-sync/bridge)# ssl-server-certificate-
validation
nano-production-azzn9vsqdk5-solace-primary-0(...dge/ssl-server-
certificate-validation)# validate-server-name
nano-production-azzn9vsqdk5-solace-primary-0(...dge/ssl-server-
certificate-validation)# exit
nano-production-azzn9vsqdk5-solace-primary-0
(configure/replication/config-sync/bridge)# no shutdown
nano-production-azzn9vsqdk5-solace-primary-0
(configure/replication/config-sync/bridge)#
```

Then configure the Backup site (`nano-production-89il3uubs0c-solace-primary-0`):

```
nano-production-89il3uubs0c-solace-primary-0> enable
nano-production-89il3uubs0c-solace-primary-0# configure
nano-production-89il3uubs0c-solace-primary-0(configure)# replication
nano-production-89il3uubs0c-solace-primary-0(configure/replication)#
config-sync bridge
nano-production-89il3uubs0c-solace-primary-0
(configure/replication/config-sync/bridge)# shutdown
nano-production-89il3uubs0c-solace-primary-0
(configure/replication/config-sync/bridge)# ssl
nano-production-89il3uubs0c-solace-primary-0
(configure/replication/config-sync/bridge)# authentication auth-scheme
basic
nano-production-89il3uubs0c-solace-primary-0
(configure/replication/config-sync/bridge)# ssl-server-certificate-
validation
nano-production-89il3uubs0c-solace-primary-0(...dge/ssl-server-
certificate-validation)# validate-server-name
nano-production-azzn9vsqdk5-solace-primary-0(...dge/ssl-server-
certificate-validation)# exit
nano-production-89il3uubs0c-solace-primary-0
(configure/replication/config-sync/bridge)# no shutdown
nano-production-89il3uubs0c-solace-primary-0
(configure/replication/config-sync/bridge)#
```

You can run the USER command `show replication` following command to validate that replication configuration is correct. For Config-Sync, the SSL and Validate Server Name are set to Yes on both event broker services (both the Primary and Backup site).

For example:

```
(configure)# show replication
------------------
nano-production-azzn9vsqdk5-solace-primary-0> show replication

Replication Interface:
Replication Mate:
v:nanoproduction89il3uubs0csolaceprimary0
    Plain Text:

    Compressed:

    SSL:                           mr-connection-
u4ehjwoe9xa.messaging.solace.cloud:5
5443

SSL:
  Default Cipher Suite List:       Yes
  Cipher Suites:                   ECDHE-RSA-AES256-GCM-SHA384
                                   ECDHE-RSA-AES256-SHA384
                                   ECDHE-RSA-AES256-SHA
                                   AES256-GCM-SHA384
                                   AES256-SHA256
                                   AES256-SHA
                                   ECDHE-RSA-AES128-GCM-SHA256
                                   ECDHE-RSA-AES128-SHA256
                                   ECDHE-RSA-AES128-SHA
                                   AES128-GCM-SHA256
                                   AES128-SHA256
                                   AES128-SHA
  Trusted Common Names:

ConfigSync:
  Bridge:
    Admin State:                   Enabled
    State:                         n/a
    Authentication:
      Scheme:                      Basic
    Compressed:                    No
    SSL:                           Yes
    Message Spool:
      Window Size:                 65535
    Retry Delay:                   3
    SSL Server Certificate Validation:
      Enforce Trusted Common Name: No
      Maximum Chain Depth:         3
      Validate Certificate Dates:  Yes
      Validate Server Name:        Yes

nano-production-azzn9vsqdk5-solace-primary-0>
```

Configure the VPN-Level Replication Settings

You must configure a client username for the Message VPN. There is only one Message VPN for an event broker service. We recommend that you enable Server Certificate Validation.

You must also configure the VPN to use the client username and password you created for use for replication when you created the event broker service.

The following are the steps to configure Message VPN for replication:

1. If you haven't already, use SSH to login to the event broker service using its generated hostname and your Global-Admin account. For information, see Getting a Global-Admin Access Account for an Event Broker Service.

   For example, `ssh to mr-connection-bo3i1bd7ewc.messaging.solace.com` and `ssh mr-connection-u4ehjwoe9xa.messaging.solace.com`, respectively.

2. Use the Solace CLI to configure the Message VPN replication settings to use Server Certificate Validation.

```
SolaceCLI > enable
SolaceCLI # configure
SolaceCLI (configure)# message-vpn <Message VPN name>
SolaceCLI (configure/message-vpn)# bridging ssl server-certificate-validation
SolaceCLI (...ing/ssl/server-certificate-validation)# validate-server-name
```

where:

- `<Message VPN name>` is the Message VPN that is the same between your replication pair.

For example, on the Primary site (`nano-production-azzn9vsqdk5-solace-primary-0`):

```
nano-production-azzn9vsqdk5-solace-primary-0> enable
nano-production-azzn9vsqdk5-solace-primary-0# configure
nano-production-azzn9vsqdk5-solace-primary-0(configure)# message-vpn myfirstservice
nano-production-azzn9vsqdk5-solace-primary-0(configure/message-vpn)# bridging ssl server-certificate-validation
nano-production-azzn9vsqdk5-solace-primary-0(...ing/ssl/server-certificate-validation)# validate-server-name
```

Then on the Backup site (`nano-production-89il3uubs0c-solace-primary-0`):

```
nano-production-89il3uubs0c-solace-primary-0> enable
nano-production-89il3uubs0c-solace-primary-0# configure
nano-production-89il3uubs0c-solace-primary-0(configure)# message-vpn myfirstservice
nano-production-89il3uubs0c-solace-primary-0(configure/message-vpn)# bridging ssl server-certificate-validation
nano-production-89il3uubs0c-solace-primary-0(...ing/ssl/server-certificate-validation)# validate-server-name
```

3. Use Solace CLI configure the Message VPN bridge authentication with the client username you created for replication.

```
SolaceCLI > enable
SolaceCLI # configure
SolaceCLI (configure)# message-vpn <Message VPN name>
SolaceCLI (configure/message-vpn)# replication
SolaceCLI (configure/message-vpn/replication)# bridge ssl
SolaceCLI (configure/message-vpn/replication)# bridge authentication basic
SolaceCLI (...plication/bridge/authentication/basic)# client-username
<dr-client-username> password <dr-clientname-password>
```

Where :

- `<Message VPN name>` is the Message VPN that is the same between your replication pair.
- `<dr-client-username>` is the client username that was created on the event broker service. This client username must use the a client profile with specific settings. For more information, see Create a Client Profile and Client Username for Replication
- `<dr-clientname-password>` the password for the client username.

For example, on the Primary site (`nano-production-azzn9vsqdk5-solace-primary-0`):

```
nano-production-azzn9vsqdk5-solace-primary-0> enable
nano-production-azzn9vsqdk5-solace-primary-0# configure
nano-production-azzn9vsqdk5-solace-primary-0(configure)# message-vpn
myfirstservice
nano-production-azzn9vsqdk5-solace-primary-0(configure/message-vpn)#
replication
nano-production-azzn9vsqdk5-solace-primary-0(configure/message-
vpn/replication)# bridge ssl
nano-production-azzn9vsqdk5-solace-primary-0(configure/message-
vpn/replication)# bridge authentication basic
nano-production-azzn9vsqdk5-solace-primary-0
(...plication/bridge/authentication/basic)# client-username
myfirstclientusername password Test12345
nano-production-azzn9vsqdk5-solace-primary-0
(...plication/bridge/authentication/basic
```

and then on Backup site (`nano-production-azzn9vsqdk5-solace-primary-0`):

```
nano-production-89il3uubs0c-solace-primary-0> enable
nano-production-89il3uubs0c-solace-primary-0# configure
nano-production-89il3uubs0c-solace-primary-0(configure)# message-vpn
myfirstservice
nano-production-89il3uubs0c-solace-primary-0(configure/message-vpn)#
replication
nano-production-azzn9vsqdk5-solace-primary-0(configure/message-
vpn/replication)# bridge ssl
nano-production-89il3uubs0c-solace-primary-0(configure/message-
vpn/replication)# bridge authentication basic
nano-production-89il3uubs0c-solace-primary-0
(...plication/bridge/authentication/basic)# client-username
myfirstclientusername password Test12345
```

```
nano-production-89il3uubs0c-solace-primary-0
(...plication/bridge/authentication/basic
```

Set the Replication State of the Message VPN

You must set the state of the Message VPN for each of the event broker services in your replication pair, which is referred to as the *replication state*. You must set the replication state to `active` for the event broker service Primary site (where you assigned a custom hostname) and `standby` to its replication mate using the following Solace CLI command:

```
SolaceCLI (configure/message-vpn/replication)# state <status>
```

Where :

- `<status>` is a value of `active` or `standby` for the state of the event broker service.

1. If you haven't already, use SSH to log in to the event broker service using its generated hostname and your Global-Admin account. For information, see Getting a Global-Admin Access Account for an Event Broker Service.

   For example, `ssh` to `mr-connection-bo3i1bd7ewc.messaging.solace.com` and `ssh mr-connection-u4ehjwoe9xa.messaging.solace.com`, respectively.

2. Use Solace CLI on the event broker service (the Primary site) that has the hostname assigned to it and set the replication state to `active` using the following command:

   ```
   SolaceCLI > enable
   SolaceCLI # configure
   SolaceCLI (configure)# message-vpn myfirstservice
   SolaceCLI (configure/message-vpn)# replication
   SolaceCLI (configure/message-vpn/replication)# state active
   ```

   Where :

   - `<Message VPN name>` is the Message VPN that is the same between your replication pair.

   For example, on the Primary site for `nano-production-azzn9vsqdk5-solace-primary-0`:

   ```
   nano-production-azzn9vsqdk5-solace-primary-0> enable
   nano-production-azzn9vsqdk5-solace-primary-0# configure
   nano-production-azzn9vsqdk5-solace-primary-0(configure)# message-vpn
   myfirstservice
   nano-production-azzn9vsqdk5-solace-primary-0(configure/message-vpn)#
   replication
   ```

```
nano-production-azzn9vsqdk5-solace-primary-0(configure/message-
vpn/replication)# state active
```

3. Use Solace CLI to set the replication mate (the event broker service) that does not have the custom hostname assigned to it as `standby` using the following command:

   ```
   SolaceCLI (configure/message-vpn/replication)# state standby
   ```

   For example, on the Backup site (`nano-production-89il3uubs0c-solace-primary-0`):

   ```
   nano-production-89il3uubs0c-solace-primary-0> enable
   nano-production-89il3uubs0c-solace-primary-0# configure
   nano-production-azzn9vsqdk5-solace-primary-0(configure)# message-vpn
   myfirstservice
   nano-production-azzn9vsqdk5-solace-primary-0(configure/message-vpn)#
   replication
   nano-production-azzn9vsqdk5-solace-primary-0(configure/message-
   vpn/replication)# state standby
   ```

Enable Replication

Replication is not enabled by default on the Message VPN, so you must start replication on both event broker services (or replication mates) in the replication pair.

1. If you haven't already use SSH to login to the event broker service using its generated hostname and your Global-Admin account. For information, see Accessing the CLI for Event Broker Services.

   For example, `ssh to mr-connection-bo3i1bd7ewc.messaging.solace.com` and `ssh mr-connection-u4ehjwoe9xa.messaging.solace.com`, respectively.

2. Use the Solace CLI to restart the Message VPN using the following commands on the event broker service:

   ```
   SolaceCLI > enable
   SolaceCLI # configure
   SolaceCLI (configure)# message-vpn <Message VPN name>
   SolaceCLI (configure/message-vpn) # replication
   SolaceCLI (configure/message-vpn/replication)# no shutdown
   ```

   Where :

   - `<Message VPN name>` is the Message VPN that is the same between your replication pair.

   For example, on the Primary site (`nano-production-azzn9vsqdk5-solace-primary-0`):

```
nano-production-azzn9vsqdk5-solace-primary-0> enable
nano-production-azzn9vsqdk5-solace-primary-0# configure
nano-production-azzn9vsqdk5-solace-primary-0(configure)# message-vpn
myfirstservice
nano-production-azzn9vsqdk5-solace-primary-0(configure/message-vpn)#
replication
nano-production-azzn9vsqdk5-solace-primary-0(configure/message-
vpn/replication)# no shutdown
```

Then on the Backup site (`nano-production-89il3uubs0c-solace-primary-0`):

```
nano-production-89il3uubs0c-solace-primary-0> enable
nano-production-89il3uubs0c-solace-primary-0# configure
nano-production-azzn9vsqdk5-solace-primary-0(configure)# message-vpn
myfirstservice
nano-production-azzn9vsqdk5-solace-primary-0(configure/message-vpn)#
replication
nano-production-azzn9vsqdk5-solace-primary-0(configure/message-
vpn/replication)# no shutdown
```

Validate the Replication Configuration

To verify if replication is working, you check if the Replication Queue is bound.

You can run commands to see the validate that the configuration is correct using the following command:

```
SolaceCLI > show message-vpn <Message VPN name> replication
```

Where :

- `<Message VPN name>` is the name of the Message VPN for the replication pair.

If the Replication Queue is bound, these are the values you should also see. If you don't see these values, this may help you to determine what is incorrect in your Replication configuration.

- A (Admin State)—(U)p on both the Active and Standby site
- C (Config State)—(A)ctive on currently Active site and (S)tandby on Standby site
- B (Bridge State)—(U)p on the Standby site

- Q (Queue state) - (U)p on Active site. This value indicates whether the replication bridge is bound.
- R (Remote Bridge State)—(U)p on the Active site
- S/M/T—These flags show more configuration and operational state information, but are not important for controlled failover.

For example, if you run the commands on the Primary site for the Message VPN name of `myfirstservice`:

```
nano-production-azzn9vsqdk5-solace-primary-0> show message-vpn
myfirstservice replication

Flags Legend:
A - Admin State (U=Up, D=Down, -=N/A)
C - Config State (A=Active, S=Standby, -=N/A)
B - Local Bridge State (U=Up, Q=Queue Unbound, D=Down, -=N/A)
R - Remote Bridge State (U=Up, D=Down, -=N/A)
Q - Queue State (U=Up, D=Down, -=N/A)
S - Sync Replication Eligible (Y=Yes, N=No, -=N/A)
M - Reject Msg When Sync Ineligible (Y=Yes, N=No, -=N/A)
T - Transaction Replication Mode (A=Async, S=Sync, -=N/A)

Message VPN                      A C B R Q S M T
-------------------------------- - - - - - - - -
myfirstservice                   U A - U U Y N A
```

And then on the Backup site() for the Message VPN name of `myfirstservice`:

```
nano-production-89il3uubs0c-solace-primary-0(configure/message-
vpn/replication)# show message-vpn myfirstservice replication

Flags Legend:
A - Admin State (U=Up, D=Down, -=N/A)
C - Config State (A=Active, S=Standby, -=N/A)
B - Local Bridge State (U=Up, Q=Queue Unbound, D=Down, -=N/A)
R - Remote Bridge State (U=Up, D=Down, -=N/A)
Q - Queue State (U=Up, D=Down, -=N/A)
S - Sync Replication Eligible (Y=Yes, N=No, -=N/A)
M - Reject Msg When Sync Ineligible (Y=Yes, N=No, -=N/A)
T - Transaction Replication Mode (A=Async, S=Sync, -=N/A)
```

```
Message VPN                      A C B R Q S M T
-------------------------------- - - - - - - - -
myfirstservice                   U S U - - - N A

```

Here's another example of the Primary site for the Message VPN name of `myfirstservice`, if you use the `details` parameter, you can see the Queue state is bound:

```
nano-production-azzn9vsqdk5-solace-primary-0> show message-vpn
myfirstservice replication detail

Message VPN:                       myfirstservice
Admin Status:                      enabled
Config Status:                     active
Local Bridge:
  State:                           n/a
  Name:                            n/a
  Queue State:                     n/a
  Authentication:
    Scheme:                        Basic
    Basic:
      Client Username:             myfirstclientusername
      Password Configured:         Yes
    Client Certificate:
      Certificate File:
      Using Server Certificate:    Yes
  Compressed:                      No
  SSL:                             No
  Message Spool:
    Window Size:                   255
  Unidirectional:
    Client Profile:                #client-profile
  Retry Delay:                     3
Remote Bridge:
  State:                           up
  Name:
#bridge/v:nanoproduction89il3uubs0csolaceprimary0/
myfirstservice/1
Queue:
  State:                           bound
  Quota (MB):                      60000
  Reject Msg to Sender on Discard: Yes
Ack Propagation:
  Interval in Messages:            20
Sync Replication:
  Eligible:                        yes
    Duration:                      0d 0h 2m 43s
  Mate Flow Congested:             no
    Duration:                      0d 0h 0m 0s
  Reject Msg When Sync Ineligible: No
Transaction Replication Mode:      async
```

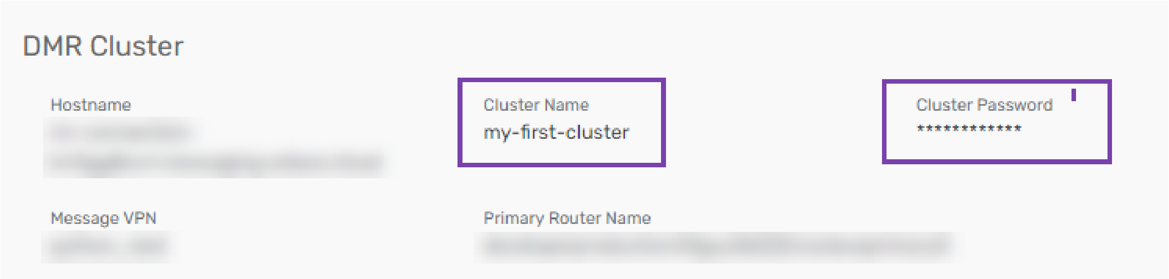
In Broker Manager, you can go to **Message VPN > Replication > Details** to see the status. If the Queue is Bound, you have correctly configured replication.

Add the Backup Site to the DMR Cluster of the Primary Site

You must re-add and enable the DMR cluster because the DMR is enabled on the Primary and they must belong to the same cluster. The DMR feature was disabled when you removed the cluster name from the Backup site as part of preparing your Backup site to configure replication and you will also need to note the cluster password.

To set the cluster name, perform the following steps in the Solace CLI:

1. Log in to the Cloud Console if you have not done so yet. The URL to access the Cloud Console differs based on your authentication scheme. For more information, see Logging into the Cloud Console.
2. Select **Cluster Manager** from the navigation bar.
3. On the **Services** page, click the card of the event broker service of the Primary site. For example, the name of the **Cluster Name** is `my-first-cluster` and make note of the cluster password.



DMR Cluster

Hostname

Cluster Name
my-first-cluster

Cluster Password
****

Message VPN

Primary Router Name

4. If you haven't done so yet, use SSH to login to the event broker service of the Backup site using its generated hostname and your Global-Admin account. For information, see Getting a Global-Admin Access Account for an Event Broker Service.
5. Run the following commands to add the event broker service (Backup site) to the same DMR cluster of the Primary site and set the cluster password after you've added using the cluster password for the Backup site. To determine the cluster password, see the **Status** tab in Cluster Manager

```
SolaceCLI > enable
SolaceCLI # configure
SolaceCLI (configure)# routing dynamic-message-routing
SolaceCLI (...igure/routing/dynamic-message-routing)# create cluster <cluster-name>
SolaceCLI (...igure/routing/dynamic-message-routing)# cluster <cluster-name>
SolaceCLI (...uting/dynamic-message-routing/cluster)# authentication basic password <cluster-password-from-console>
SolaceCLI (...uting/dynamic-message-routing/cluster)# no shutdown
```

For example, on the Backup site:

```
nano-production-89il3uubs0c-solace-primary-0> enable
nano-production-89il3uubs0c-solace-primary-0# configure
nano-production-89il3uubs0c-solace-primary-0(configure)# routing dynamic-message-routing
nano-production-89il3uubs0c-solace-primary-0(...igure/routing/dynamic-message-routing)# create cluster my-first-cluster
nano-production-89il3uubs0c-solace-primary-0(...igure/routing/dynamic-message-routing)# cluster first-cluster
nano-production-89il3uubs0c-solace-primary-0(...igure/routing/dynamic-message-routing)# authentication basic password <cluster-password-from-console>
nano-production-89il3uubs0c-solace-primary-0(...uting/dynamic-message-routing/cluster)# no shutdown
```

The Backup site and Primary site are now in the same DMR cluster but now requires an internal DMR link to be configured.

Add the DMR Internal Link Between the Primary Site and Backup Site

After you've configured the Primary and Backup sites be in the same DMR cluster, you must configure an internal DMR link between the Primary and Backup sites.

To configure each link between a node within the DMR cluster, at minimum in advanced event mesh , configure these link attributes:

- span to be internal
- authentication settings
- `connect-via` must not be set
- TLS must be enabled
- the link must be enabled

To create an internal DMR link, you use the Solace CLI and your global-admin account.

> If you have other services in your DMR cluster, you must also request the global-admin password to those event broker services.

The following steps show you how to configure the internal link using the Solace CLI:

1. If you haven't done so yet, use SSH to log in to the event broker service using its generated hostname and your Global-Admin account. For information, see Getting a Global-Admin Access Account for an Event Broker Service.
2. In the Cloud Console, get the primary router name and the cluster password for both the **Primary** and **Backup** site (see the **Status** tab in Cluster Manager) and get the cluster name of the services, the cluster name for each service, and the primary router name. For example, these are the names we'll use in our example:
   - Cluster name: my-first-cluster
   - Primary site:
     - Primary router name: nanoproductionazzn9vsqdk5solaceprimary0
     - Cluster Password: myprimarysiteclusterpassword
   - Backup site:
     - Primary router name: nanoproduction89il3uubs0csolaceprimary0
     - Cluster Password: mybackupsiteclusterpassword
3. Use the Solace CLI to create an internal DMR link between the Backup site and Primary site. In this example, this is a two-step process for a single link that requires you to:

- Access the Primary site to:
    - create an internal DMR link between the Primary and Backup site using the primary router name of the Backup site
    - enable SSL on the link
    - configure authentication (in our example, we use basic authentication using the cluster password for the Backup site)
    - enable the link
- Access the Backup site to:
    - create an internal DMR link between the Backup and Primary site using the primary router name of the Primary site
    - enable SSL on the link
    - configure authentication (in our example, we use basic authentication using the cluster password for the Primary site)

You must complete these steps on each event broker service

```
SolaceCLI > enable
SolaceCLI # configure
SolaceCLI (configure)# routing dynamic-message-routing
SolaceCLI (...igure/routing/dynamic-message-routing)# cluster
<cluster-name>
SolaceCLI (...uting/dynamic-message-routing/cluster)# create link
<other-site-primary-router-name>
SolaceCLI (.../dynamic-message-routing/cluster/link)# span internal
SolaceCLI (.../dynamic-message-routing/cluster/link)# transport ssl
SolaceCLI (.../dynamic-message-routing/cluster/link)# authentication
basic password <other-site-cluster-pw>
```

For example, on the Primary site:

```
nano-production-azzn9vsqdk5-solace-primary-0> enable
nano-production-azzn9vsqdk5-solace-primary-0# configure
nano-production-azzn9vsqdk5-solace-primary-0(configure)# routing
dynamic-message-routing
nano-production-azzn9vsqdk5-solace-primary-0(...igure/routing/dynamic-
message-routing)# cluster  my-first-cluster
nano-production-azzn9vsqdk5-solace-primary-0(...uting/dynamic-message-
routing/cluster)# create link nanoproduction89il3uubs0csolaceprimary0
nano-production-azzn9vsqdk5-solace-primary-0(.../dynamic-message-
routing/cluster/link)# span internal
nano-production-azzn9vsqdk5-solace-primary-0(.../dynamic-message-
routing/cluster/link)# transport ssl
nano-production-azzn9vsqdk5-solace-primary-0(.../dynamic-message-
routing/cluster/link)# authentication basic password
```

```
mybackupsiteclusterpassword
nano-production-azzn9vsqdk5-solace-primary-0(.../dynamic-message-
routing/cluster/link)# no shutdown
```

For example, on the Backup site:

```
nano-production-89il3uubs0c-solace-primary-0> enable
nano-production-89il3uubs0c-solace-primary-0# configure
nano-production-89il3uubs0c-solace-primary-0(configure)# routing
dynamic-message-routing
nano-production-89il3uubs0c-solace-primary-0(...igure/routing/dynamic-
message-routing)# cluster  my-first-cluster
nano-production-89il3uubs0c-solace-primary-0(...uting/dynamic-message-
routing/cluster)# create link nanoproductionazzn9vsqdk5solaceprimary0
nano-production-89il3uubs0c-solace-primary-0(.../dynamic-message-
routing/cluster/link)# span internal
nano-production-89il3uubs0c-solace-primary-0(.../dynamic-message-
routing/cluster/link)# transport ssl
nano-production-89il3uubs0c-solace-primary-0(.../dynamic-message-
routing/cluster/link)# authentication basic password
myprimarysiteclusterpassword
nano-production-89il3uubs0c-solace-primary-0(.../dynamic-message-
routing/cluster/link)# no shutdown
```

> Typically, it takes under five minutes as the internal DMR link between the Primary and Backup site synchronize, but this may vary depending on network factors such as latency.

4. Run the `show cluster * link *` command to verify the internal DMR link you created is up (the name of the link is what you specified when you ran the `create link` command.

```
show cluster * link *
```

For example, on the Primary site:

```
SolaceCLI > show cluster * link *
Cluster Name          : my-first-cluster
Node Name             : nanoproductionazzn9vsqdk5solaceprimary0
Link                                  Admin Oper  Fail Reason /
Uptime
-------------------------------------- ----- ----- -----------------
-----------
```

```
#ACTIVE                                  Up    Up    43d 3h 45m 13s
nanoproduction89il3uubs0csolaceprimary0  Up    Up    0d 9h 41m 55s
```

To see the status of the individual link, run the following command:

```
show cluster <cluster-name> link <link-name>
```

For example, on the Primary site:

```
show cluster  my-first-cluster link * detail
...
...
Remote Node Name        : nanoproduction89il3uubs0csolaceprimary0
Enabled               : Yes
Span                  : internal
Initiator             : lexical
Connect-Via           :
Message Spool
Window Size         : 255
Transport
Compressed          : No
SSL                 : Yes
Authentication
Auth-Scheme         : Basic
Basic
Password?         : Yes
Attributes
nodeName            : nanoproductionazzn9vsqdk5solaceprimary0
span                : internal
Operational           : Yes
Fail Reason         :
Uptime              : 0d 9h 50m 14s
Channels Up         : 1 of 1
Remote Cluster Name : my-first-cluster
```

Specify the Queues and Topics for Replication

After replication is configured, you can specify the topics and queues to be replicated. By default, nothing is replicated.

To add topics or queues to replicate, you specify a topic pattern that uses a similar syntax as topic subscriptions. This topic pattern can be a topic subscription or a queue name subscription (a subscription for a queue is `#P2P/QUE/<queueName>`). In addition, you can specify exceptions using leading `!` character to the topic subscription.

For each topic or queue add, you must also specify the replication mode of transactions is determined by the Message VPN setting. See Configuring the Replication Mates for more information:

- Sync Messages are acknowledged when replicated (spooled remotely).
- Async Messages are acknowledged when pending replication (spooled locally).

The following are the steps to configure the topics from advanced event mesh for SAP Integration Suite:

1. Log in to the Cloud Console if you have not done so yet. The URL to access the Cloud Console differs based on your authentication scheme. For more information, see Login URLs for SAP Integration Suite, advanced event mesh Console.
2. Select **Cluster Manager** from the navigation bar.
3. On the **Services** page, select the event broker service that has replication configured.
4. Select the **Manage** tab and click **Message VPN**.
5. In Broker Manager, on the **Message VPN** page, click **Replication**.
6. On the **Replication** tab, click **Replicated Topics**.
7. Click the **+Replicated Topic** button.
8. In the **Create Replicated Topic** dialog box, you can add topics and queues. For each topic or queue want to replicate to the event broker service replication mate:
   - enter the topic or queue in the box
   - select the replication mode to use **Sync** or **Async** to specify whether to synchronously or asynchronously replicate the topic, from the list on right of the box
   - click the **Add New** link.
   - (optional) click the X on the box of the topic or queue you've added .
9. Repeat the previous step and when you have the topics you want to replicate. click **Create**.
10. Click **Create** when you're ready to add the list of the topics.

The list of topics appears on the **Replication Topics** page.

Getting a Global-Admin Access Account for an Event Broker Service

All event broker services are configured with a default management account that you can use for CLI access. This account is separate from the accounts that you use to access the Cloud Console. This management account is specific to each event broker service and has limited access to perform management actions and read-write privileges on only the Message VPN, which is referred to as Message VPN-scoped account. The elevated privilege would be admin.

To enable other features that require elevated scope and access levels, you require an account with elevated privileges on each event broker service. For example, to configure replication you require an account for the event broker service that has global scope and admin access-level, referred to as a *global-admin account*. You require a scope of global to configure components other than the Message VPN. You require this global-admin account for each event broker service on both the Primary and Backup sites.

To request a global-admin account, contact SAP.

> You must exercise caution when you use the Solace CLI commands with an account with global scope and admin access-level. With this global-admin account, you can run commands that cause service-disruptions. If you cause a service-disruptions, it voids your service level agreements (SLAs) for advanced event mesh.

Configuring Replication in an Event Mesh

In advanced event mesh, if your Primary site is part of an event mesh and you want to configure replication, it requires that you have a more in-depth understanding of Dynamic Messaging Routing (DMR), which is the underlying technology for an event mesh. For more information about DMR, see Dynamic Message Routing.

During the procedure, it is expected that the state of the DMR cluster will be reported as `Down` and topology errors will be raised while links are being established between nodes. In spite of these errors, traffic will continue to flow through the network and no message loss is expected. The examples in this section are based on the examples from the rest of this guide.

At this time, you cannot use Mesh Manager to configure or manage an event broker service that has replication configured. Instead, you must manually configure the links using a combination of Solace CLI and Broker Manager.

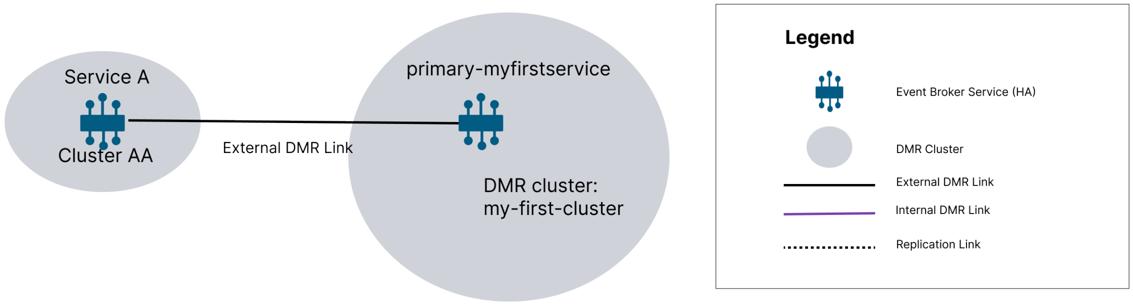
If you want to configure replication on an event broker service that also needs to be part of an event mesh, perform the steps in the following order:

1. Use Mesh Manager to add the Primary site into an existing event mesh or create a new event mesh using the Primary site as one of the services.

   For more information about adding the Active site (event broker service) to an event mesh, see Creating an Event Mesh or Adding an Event Broker Service to an Existing Event Mesh.

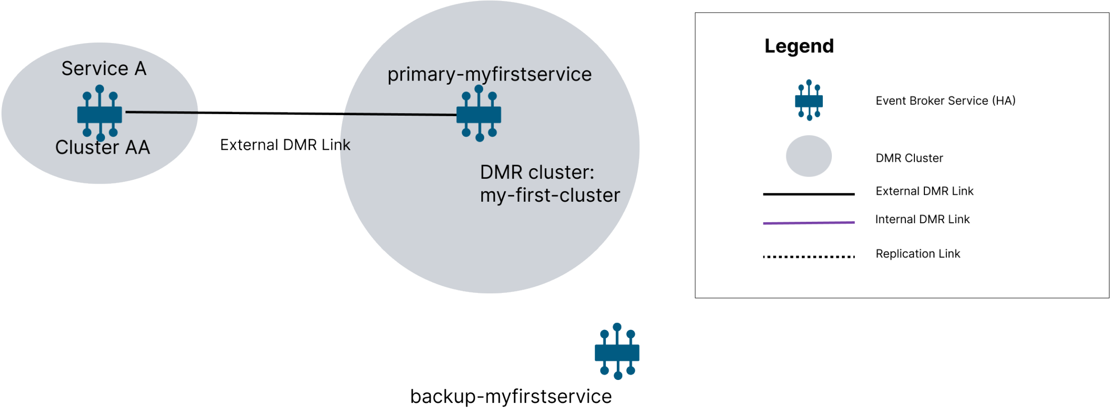
   > You can only use Mesh Manager if there are no event broker services that have replication configured; otherwise you must manually configure the DMR links between the services in the event mesh.

   For example, your event mesh might be simply two event broker services that are connected via an external DMR link. We use this example as a basis for the steps that precede.

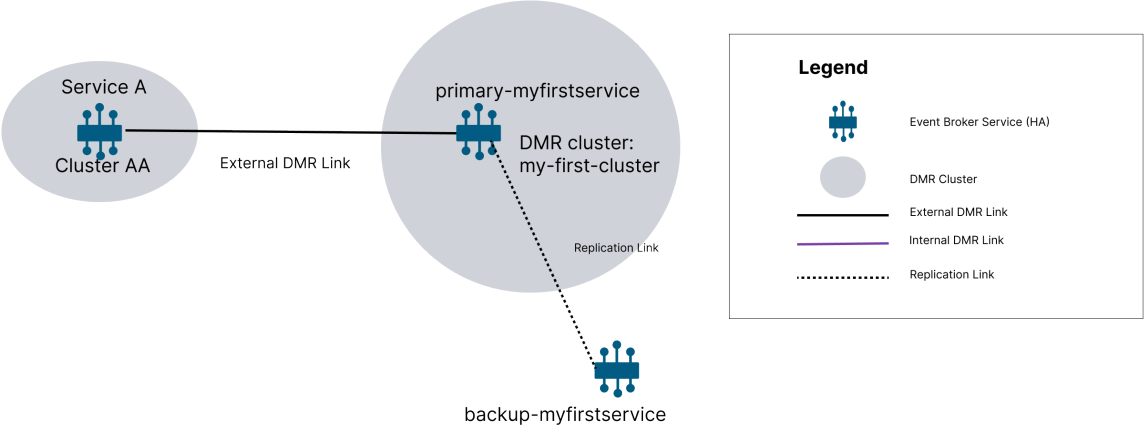


2. Create the event broker service for the Backup site. The Primary site is presumed have a Custom Hostname configured. For more information, see Create a Custom Hostname for the Replication Pair.

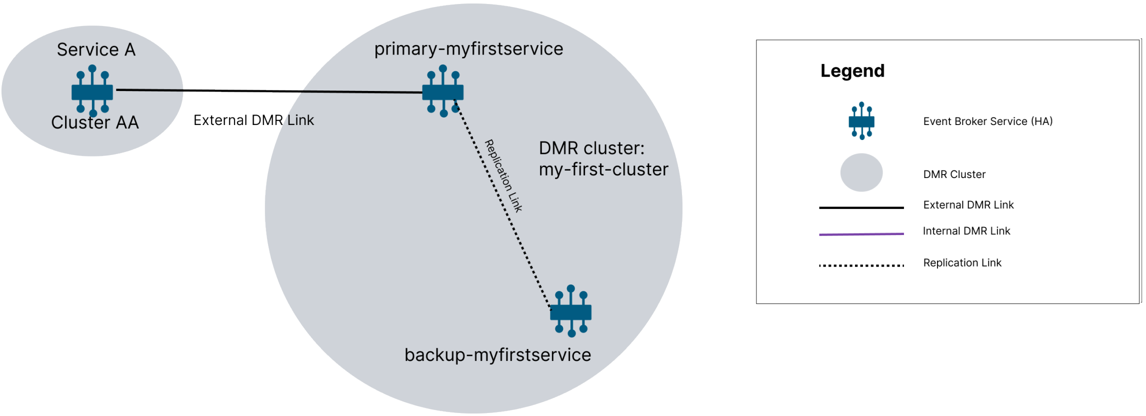
   After you create the Backup site and disable Dynamic Message Routing (DMR) (removed it from the DMR cluster) on only the Backup site, your topology looks like the following diagram where `backup-myfirstservice` (the Backup site) is separate from the Cluster `my-first-cluster`. For more information about removing the Backup site (event broker service) from the DMR cluster and disabling DMR, see Disable Dynamic Message Routing on the Backup Site.



   After you have configured replication, your service topology shows the replication mates (services `primary-myfirstservice` and `backup-myfirstservice`) connected via a replication link.



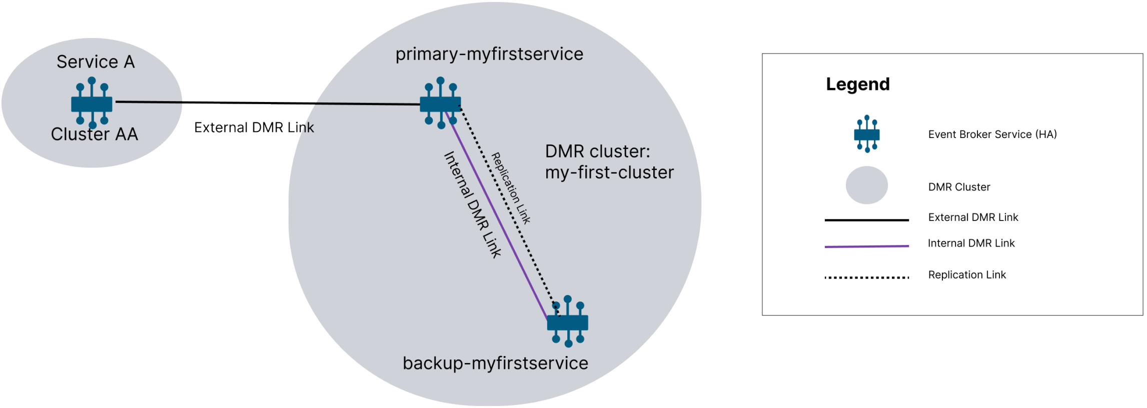
3. Add the event broker service for the Backup site to the same cluster as the Primary site. For more information, see Add the Backup Site to the DMR Cluster of the Primary Site. After this step, your service topology shows services `primary-myfirstservice` and `backup-myfirstservice` in cluster `my-first-cluster` (the cluster name of service `primary-myfirstservice`):



4. In the Solace CLI, configure the internal DMR links. For more information, see Create the DMR Internal Links Within the DMR Cluster. You must add internal DMR links:
   - between the Backup site and Primary site
   - between the Backup site and other event broker services in your DMR cluster (if they exist)

   > Internal DMR links between your Primary site and other services in the same DMR cluster may have been configured for you previously by SAP. If not, those links must be configured as well.

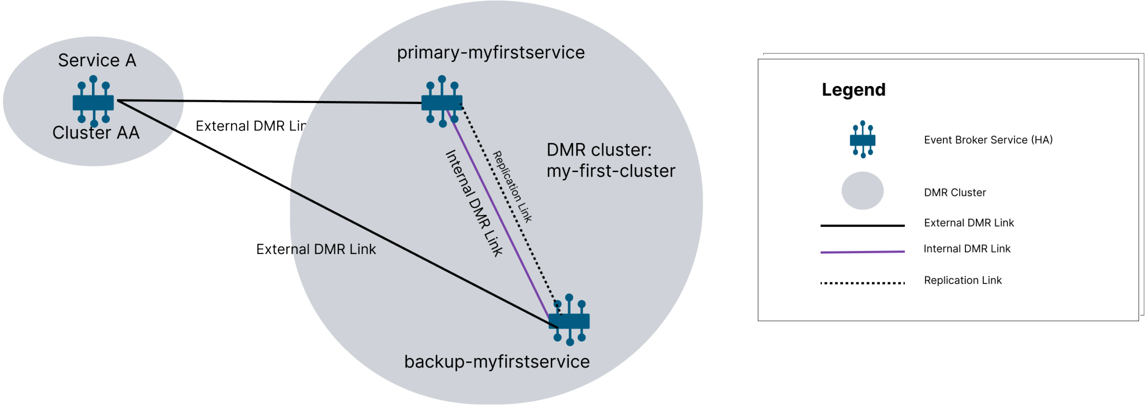
   After configuring the internal DMR link, the following topology shows an internal DMR link between `primary-myfirstservice` and `backup-myfirstservice` in addition to the pre-existing replication link.



5. If in the DMR cluster the Primary site is the DMR gateway node (or the only service in the DMR cluster prior to configuring the replication mate), you must add the external DMR links between your Backup site and other event broker services in that cluster.

   To add the external DMR links you must use Broker Manager. For more information, see Create DMR External Links in the Event Mesh. After you completed the configuration for the external DMR link, both `primary-myfirstservice` and `backup-myfirstservice` now have an external

DMR link to Service A and the full-mesh topology is complete with replication configured on one of the nodes:



Considerations When Using Replication and DMR for an Event Mesh

These are the considerations when you want to configure replication when your event broker service (Primary site) is part of an event mesh. Event meshes in advanced event mesh use the Dynamic Message Routing feature.

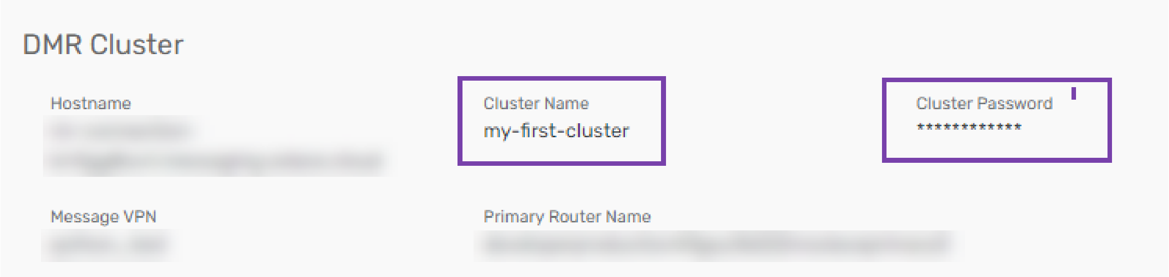
- We recommend that you configure your event mesh using Mesh Manager **before** you configure replication.
- If an event mesh has at least one event broker service configured with replication, you can no longer use Mesh Manager to manage or configure the event mesh. In addition, Health Checks will report errors in Mesh Manager. Lastly, you must use Broker Manager to add or remove external DMR links between the DMR nodes in your event mesh.
- Though the event mesh is a full-mesh, the same configuration rules apply which you must manually manage using Broker Manager. These rules are as follows:
  - If you have more than one event broker service in a DMR cluster, internal DMR links must connect all event broker services in the DMR cluster.
  - If you have multiple services (DMR nodes) in the DMR cluster (not including the one configured as the replication mate), either:
    - only one of the event broker services can function as a DMR gateway and must have external DMR links to other event broker services in the event mesh
    - if there are multiple services and the event broker service (Primary site) is the DMR gateway, you must configure external DMR links from both the DMR Primary site and the Backup site to other services in your event mesh

Add the Backup Site to the DMR Cluster of the Primary Site

You must re-add and enable the DMR cluster because the DMR is enabled on the Primary and they must belong to the same cluster. The DMR feature was disabled when you removed the cluster name from the Backup site as part of preparing your Backup site to configure replication and you will also need to note the cluster password.

To set the cluster name, perform the following steps in the Solace CLI:

1. Log in to the Cloud Console if you have not done so yet. The URL to access the Cloud Console differs based on your authentication scheme. For more information, see Logging into the Cloud Console.
2. Select **Cluster Manager** from the navigation bar.
3. On the **Services** page, click the card of the event broker service of the Primary site. For example, the name of the **Cluster Name** is `my-first-cluster` and make note of the cluster password.



DMR Cluster

Hostname
[redacted]

Cluster Name
my-first-cluster

Cluster Password
****

Message VPN
[redacted]

Primary Router Name
[redacted]

4. If you haven't done so yet, use SSH to login to the event broker service of the Backup site using its generated hostname and your Global-Admin account. For information, see Getting a Global-Admin Access Account for an Event Broker Service.
5. Run the following commands to add the event broker service (Backup site) to the same DMR cluster of the Primary site and set the cluster password after you've added using the cluster password for the Backup site. To determine the cluster password, see the **Status** tab in Cluster Manager

```
SolaceCLI > enable
SolaceCLI # configure
SolaceCLI (configure)# routing dynamic-message-routing
SolaceCLI (...igure/routing/dynamic-message-routing)# create cluster
<cluster-name>
SolaceCLI (...igure/routing/dynamic-message-routing)# cluster
<cluster-name>
SolaceCLI (...uting/dynamic-message-routing/cluster)# authentication
basic password <cluster-password-from-console>
SolaceCLI (...uting/dynamic-message-routing/cluster)# no shutdown
```

For example, on the Backup site:

```
nano-production-89il3uubs0c-solace-primary-0> enable
nano-production-89il3uubs0c-solace-primary-0# configure
nano-production-89il3uubs0c-solace-primary-0(configure)# routing
dynamic-message-routing
nano-production-89il3uubs0c-solace-primary-0(...igure/routing/dynamic-
message-routing)# create cluster my-first-cluster
nano-production-89il3uubs0c-solace-primary-0(...igure/routing/dynamic-
message-routing)# cluster first-cluster
nano-production-89il3uubs0c-solace-primary-0(...igure/routing/dynamic-
message-routing)# authentication basic password <cluster-password-
from-console>
nano-production-89il3uubs0c-solace-primary-0(...uting/dynamic-message-
routing/cluster)# no shutdown
```

The Backup site and Primary site are now in the same DMR cluster but now requires an internal DMR link to be configured.

Create the DMR Internal Links Within the DMR Cluster

After you've configured the Primary and Backup sites be in the same DMR cluster, you must configure an internal DMR link between the Primary and Backup sites.

To configure each link between a node within the DMR cluster, at minimum in advanced event mesh , configure these link attributes:

- span to be internal
- authentication settings
- `connect-via` must not be set
- TLS must be enabled
- the link must be enabled

To create an internal DMR link, you use the Solace CLI and your global-admin account.

> If you have other services in your DMR cluster, you must also request the global-admin password to those event broker services.

The following steps show you how to configure the internal link using the Solace CLI:

1. If you haven't done so yet, use SSH to log in to the event broker service using its generated hostname and your Global-Admin account. For information, see Getting a Global-Admin Access Account for an Event Broker Service.
2. In the Cloud Console, get the primary router name and the cluster password for both the **Primary** and **Backup** site (see the **Status** tab in Cluster Manager) and get the cluster name of the services, the cluster name for each service, and the primary router name. For example, these are the names we'll use in our example:
   - Cluster name: my-first-cluster
   - Primary site:
     - Primary router name: nanoproductionazzn9vsqdk5solaceprimary0
     - Cluster Password: myprimarysiteclusterpassword
   - Backup site:
     - Primary router name: nanoproduction89il3uubs0csolaceprimary0
     - Cluster Password: mybackupsiteclusterpassword
3. Use the Solace CLI to create an internal DMR link between the Backup site and Primary site. In this example, this is a two-step process for a single link that requires you to:

   - Access the Primary site to:
     - create an internal DMR link between the Primary and Backup site using the primary router name of the Backup site
     - enable SSL on the link
     - configure authentication (in our example, we use basic authentication using the cluster password for the Backup site)
     - enable the link
   - Access the Backup site to:
     - create an internal DMR link between the Backup and Primary site using the primary router name of the Primary site
     - enable SSL on the link
     - configure authentication (in our example, we use basic authentication using the cluster password for the Primary site)

   You must complete these steps on each event broker service

   ```
   SolaceCLI > enable
   SolaceCLI # configure
   SolaceCLI (configure)# routing dynamic-message-routing
   SolaceCLI (...igure/routing/dynamic-message-routing)# cluster
   <cluster-name>
   SolaceCLI (...uting/dynamic-message-routing/cluster)# create link
   <other-site-primary-router-name>
   SolaceCLI (.../dynamic-message-routing/cluster/link)# span internal
   SolaceCLI (.../dynamic-message-routing/cluster/link)# transport ssl
   ```

```
SolaceCLI (.../dynamic-message-routing/cluster/link)# authentication
basic password <other-site-cluster-pw>
```

For example, on the Primary site:

```
nano-production-azzn9vsqdk5-solace-primary-0> enable
nano-production-azzn9vsqdk5-solace-primary-0# configure
nano-production-azzn9vsqdk5-solace-primary-0(configure)# routing
dynamic-message-routing
nano-production-azzn9vsqdk5-solace-primary-0(...igure/routing/dynamic-
message-routing)# cluster  my-first-cluster
nano-production-azzn9vsqdk5-solace-primary-0(...uting/dynamic-message-
routing/cluster)# create link nanoproduction89il3uubs0csolaceprimary0
nano-production-azzn9vsqdk5-solace-primary-0(.../dynamic-message-
routing/cluster/link)# span internal
nano-production-azzn9vsqdk5-solace-primary-0(.../dynamic-message-
routing/cluster/link)# transport ssl
nano-production-azzn9vsqdk5-solace-primary-0(.../dynamic-message-
routing/cluster/link)# authentication basic password
mybackupsiteclusterpassword
nano-production-azzn9vsqdk5-solace-primary-0(.../dynamic-message-
routing/cluster/link)# no shutdown
```

For example, on the Backup site:

```
nano-production-89il3uubs0c-solace-primary-0> enable
nano-production-89il3uubs0c-solace-primary-0# configure
nano-production-89il3uubs0c-solace-primary-0(configure)# routing
dynamic-message-routing
nano-production-89il3uubs0c-solace-primary-0(...igure/routing/dynamic-
message-routing)# cluster  my-first-cluster
nano-production-89il3uubs0c-solace-primary-0(...uting/dynamic-message-
routing/cluster)# create link nanoproductionazzn9vsqdk5solaceprimary0
nano-production-89il3uubs0c-solace-primary-0(.../dynamic-message-
routing/cluster/link)# span internal
nano-production-89il3uubs0c-solace-primary-0(.../dynamic-message-
routing/cluster/link)# transport ssl
nano-production-89il3uubs0c-solace-primary-0(.../dynamic-message-
routing/cluster/link)# authentication basic password
myprimarysiteclusterpassword
nano-production-89il3uubs0c-solace-primary-0(.../dynamic-message-
routing/cluster/link)# no shutdown
```

> Typically, it takes under five minutes as the internal DMR link between the Primary and Backup site synchronize, but this may vary depending on network factors such as latency.

4. Run the `show cluster * link *` command to verify the internal DMR link you created is up (the name of the link is what you specified when you ran the `create link` command.

   ```
   show cluster * link *
   ```

   For example, on the Primary site:

   ```
   SolaceCLI > show cluster * link *
   Cluster Name          : my-first-cluster
   Node Name             : nanoproductionazzn9vsqdk5solaceprimary0
   Link                                     Admin Oper  Fail Reason /
   Uptime
   --------------------------------------- ----- ----- -----------------
   -----------
   #ACTIVE                                  Up    Up    43d 3h 45m 13s
   nanoproduction89il3uubs0csolaceprimary0  Up    Up    0d 9h 41m 55s
   ```

   To see the status of the individual link, run the following command:

   ```
   show cluster <cluster-name> link <link-name>
   ```

   For example, on the Primary site:

   ```
   show cluster  my-first-cluster link * detail
   ...
   ...
   Remote Node Name        : nanoproduction89il3uubs0csolaceprimary0
   Enabled               : Yes
   Span                  : internal
   Initiator             : lexical
   Connect-Via           :
   Message Spool
   Window Size         : 255
   Transport
   Compressed          : No
   SSL                 : Yes
   Authentication
   Auth-Scheme         : Basic
   Basic
   ```

```
Password?         : Yes
Attributes
nodeName            : nanoproductionazzn9vsqdk5solaceprimary0
span                : internal
Operational           : Yes
Fail Reason         :
Uptime              : 0d 9h 50m 14s
Channels Up         : 1 of 1
Remote Cluster Name : my-first-cluster
```

> If there are other existing event broker services (nodes) in the cluster, you must also configure internal DMR links from the Backup site to those nodes. Repeat steps 3-4 to create internal links between the Backup site and the other nodes in the DMR cluster that your Primary site is connected to in the DMR cluster.

Create DMR External Links in the Event Mesh

Event broker services in an event mesh are connected using external DMR links. Each event broker service must be connected to all other event broker services in the event mesh to create a full mesh.

If you had used Mesh Manager, external DMR links are created between the Primary site and all the other services in your event mesh. To complete the configuration, you must create external DMR links between the Backup site and the same services that the Primary site has connections to. You do not create an external DMR link between your Primary site and Backup site.

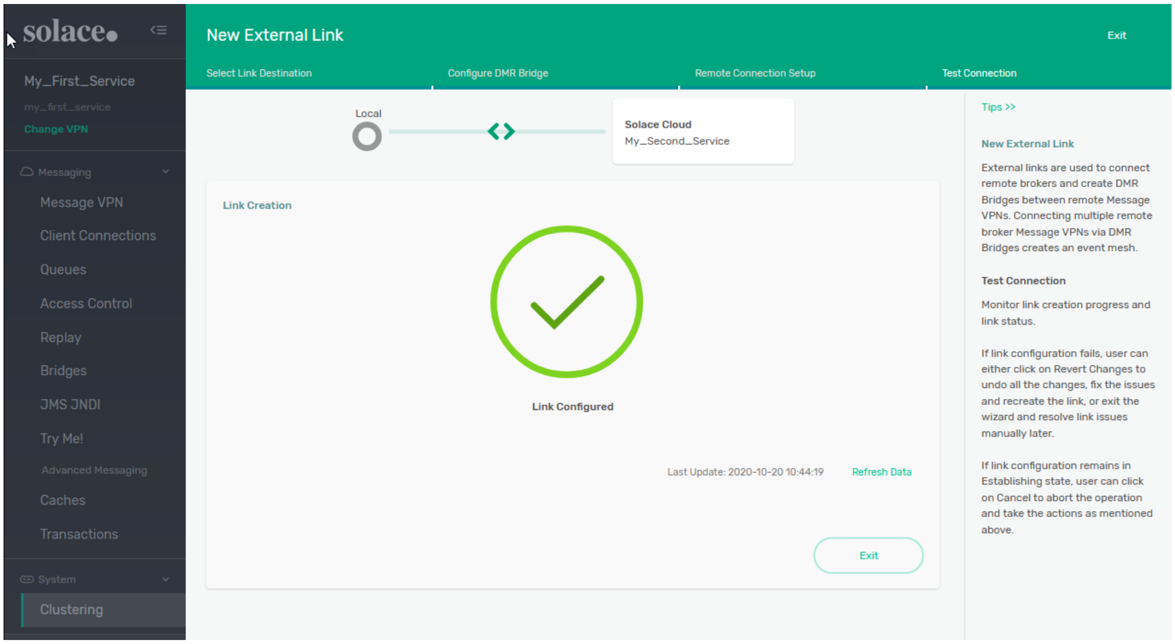
> You only need to create an external DMR links from the Backup site to other nodes in the event mesh if your Primary site is a gateway node for your DMR cluster.

> Prior to creating the external DMR links between services, we recommend that create an API token in Cloud Console. For more information, see Creating an API Token for Click-to-Connect.

To create external links in Broker Manager on the Backup site (or any other event broker service), perform the following steps:

1. Log in to the Cloud Console if you have not done so yet. The URL to access the Cloud Console differs based on your authentication scheme. For more information, see Logging into the Cloud Console.
2. On the navigation bar, select Cluster Manager🌐.
3. On the **Services** page, click on the card for the event broker service and then click **Open Broker Manager**.
4. In Broker Manager, select Message VPN. For example, select **myfirstservice**.
5. In Broker Manager, select **Clustering** on the navigation bar.
6. On the **Clustering** page for your service, select the **External Links** tab, and then click **Click to Connect**.
7. On the **New External Link** page, in the **Select Link Destination** step, beneath **Where to connect to**, select **Cloud**.
8. In the **Cloud Credentials** section, enter the account credentials for advanced event mesh in one of following ways:
   - (Recommended) Select **Token** and paste the API token in the **Token** field. For information about creating an API token, see Managing API Tokens.
   - Select **Username & Password** and then your Cloud Console credentials in the **Username** and **Password** fields.
9. Click **Configure DMR Bridge** at the bottom. Depending on the broker version and if this is the first DMR external link you're creating, the button might be **Select Workspace** and then for subsequent links it is **Configure DMR Bridge**.
10. In the **Configure DMR Bridge** step, select the name of your Message VPN for the service from the **Local Message VPN** drop-down list. For example, **myfirstservice**.
11. In the **Remote Message Service** drop-down list, multiple service names are available (including the service name your connected to).

    Choose the name of one of the services in your event mesh.
12. In the **Remote Message Service Connection** pane, select **Local**, set the **Authentication Scheme** to **Basic**. The other **Remote** and **Local** Cluster fields are pre-filled for you with the cluster passwords.
13. In the **Transport** section, enable the **TLS enabled** toggle.
14. Click **Apply** or **Create Link and Test Connection**.
15. After the link is configured (this normally takes a few minutes), you'll see the result. Click **Exit**



New External Link

Solace Cloud
My_Second_Service

Link Creation

Link Configured

Last Update: 2020-10-20 10:44:19

New External Link

External links are used to connect remote brokers and create DMR Bridges between remote Message VPNs. Connecting multiple remote broker Message VPNs via DMR Bridges creates an event mesh.

Test Connection

Monitor link creation progress and link status.

If link configuration fails, user can either click on Revert Changes to undo all the changes, fix the issues and recreate the link, or exit the wizard and resolve link issues manually later.

If link configuration remains in Establishing state, user can click on Cancel to abort the operation and take the actions as mentioned above.

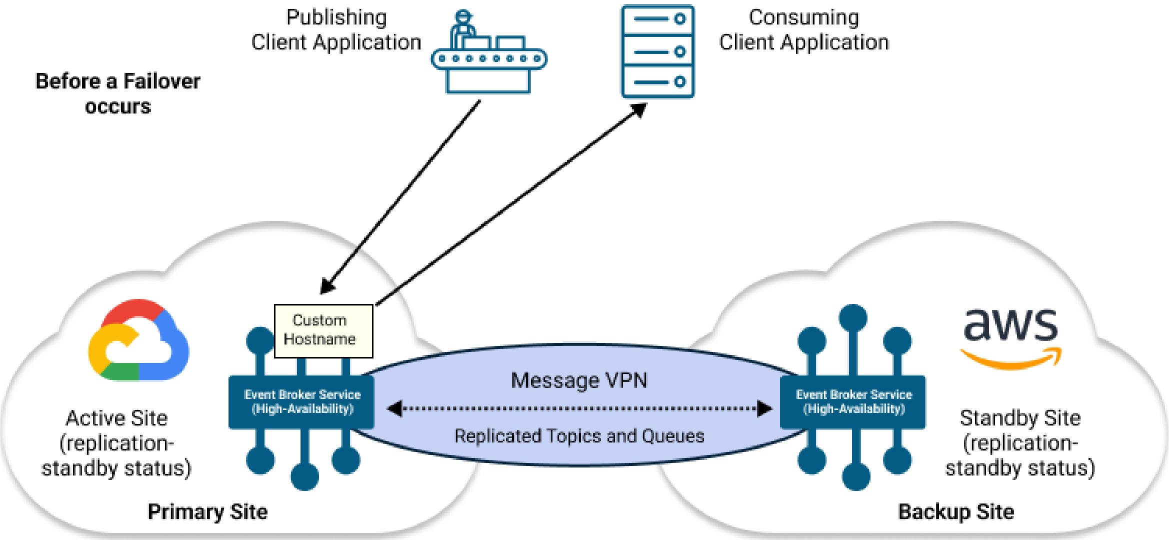
16. Repeat steps 5-15 in this section to configure more external DMR links between any other event broker services and the Backup site. You must have the same external links from the Backup site as the Primary site.

Performing Replication Failovers of Event Broker Services

If you have replication configured, you can perform a failover if you need to:

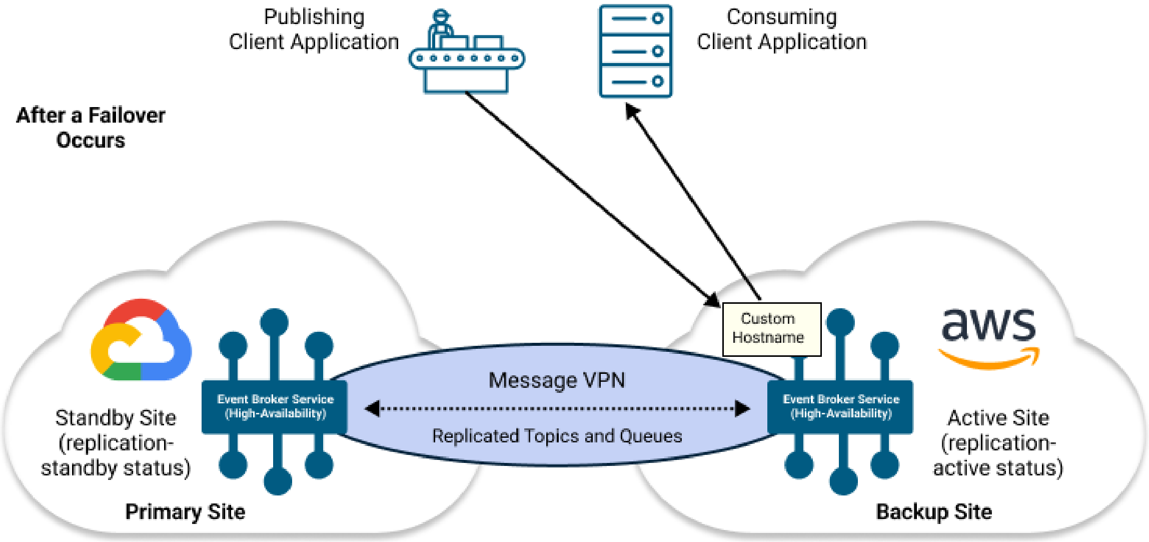
- practice and verify your failover process
- recover messaging service in the rare case where your event broker services experience a severe outage (for example, due to a networking error or power outage that affects a cloud region or datacenter)

A failover consists of transferring (or switching) the replication-active state of the Message VPN on the failed event broker service to its replication mate on the Standby site and also switching the custom hostname. Service is restored when the client applications connect to the newly Active site.


Before a Failover occurs
Publishing Client Application
Consuming Client Application
Custom Hostname
Event Broker Service (High-Availability)
Message VPN
Replicated Topics and Queues
Event Broker Service (High-Availability)
aws
Active Site (replication-standby status)
Primary Site
Standby Site (replication-standby status)
Backup Site

Prior to failover, client applications connect to the Primary site using the custom hostname as shown in the following diagram:

After a failover, client applications connect to the Backup site after replication-state and custom hostname has changed to the event broker service.


Publishing Client Application
Consuming Client Application
After a Failover Occurs
Custom Hostname
aws
Message VPN
Event Broker Service (High-Availability)
Event Broker Service (High-Availability)
Replicated Topics and Queues
Standby Site (replication-standby status)
Active Site (replication-active status)
Primary Site
Backup Site

Transferring activity from one replication site to another can occur through either a controlled or uncontrolled failover. The differences are as follows:

- A *controlled failover* occurs when activity is transferred from one replication site to its mate replication site in a planned manner for operational reasons. When you successfully follow the controlled failover procedure, no messages are lost, regardless of the replication mode of the messages.
- An *uncontrolled failover* occurs due to a sudden loss of connectivity to a replication site with Message VPNs with a replication-active status. When this occurs, only synchronous replication mode messages are guaranteed not to be lost. Messages remaining in the replication queue are not available at the Failed site.

For the detailed procedures for performing failovers, see the following:

- Performing a Controlled Failover of Event Broker Services
- Performing an Uncontrolled Failover of Event Broker Services

Performing a Controlled Failover of Event Broker Services

A controlled failover permits you to gracefully release activity from the Message VPN on the event broker service on your Active site, and to switch the activity to the Standby site (referred to as the newly Active site) so there is no message loss. A controlled failover is often a planned activity. Performing controlled failovers can be useful during upgrade or maintenance activities, such as updating network components that may temporarily disrupt service at one site. Switching activity and having client applications connect to the replication mate allows maintenance to proceed without causing message loss.

To perform a controlled failover in advanced event mesh for SAP Integration Suite, you switch the replication state of the Message VPN on the event broker service to `active` and reassign the custom hostname from the previously Active site to the newly Active site.

Before you begin this procedure, ensure you have fulfilled the Prerequisites.

> SAP recommends that you verify that the configuration on the Standby site is the same as the Active site prior to performing a failover. Any configuration changes that are made in the advanced event mesh to your event broker service on the Active site must be manually duplicated on the Standby site. For more information, see Considerations and Best Practices for Using Replication.

To perform a controlled failover, do the following (you must repeat this procedure for each replication pair):

1. Verify That the Replication Bridge is Bound to the Replication Queue.
2. Switch Activity of the Active Site to a Standby State.
3. Drain the Replication Queue in the Formerly Active Site.
4. Heuristically Commit or Roll Back Any In-Progress Transactions.
5. Change the State of the Message VPN to Active on the Formerly Standby Site .
6. Move the Custom Hostname to the Newly Active Site.

   > At this point, client applications should be able to re-connect to the Message VPN on the event broker service.

7. Delete the Heuristically Completed Transactions.

For the examples provided for this procedure, we use the following values:

Example Item	Value	Description
Name of	`myfirstservice`	The event broker services are in different regions

Example Item	Value	Description
the Message VPN		and name of the Message VPN on both are configured to be the same name.
Primary Site	primary-myfirstservice or `nano-production-azzn9vsqdk5-solace-primary-0`	The Active site at the start of the procedure that becomes the Standby site.
Backup Site	backup-myfirstservice or `nano-production-89il3uubs0c-solace-primary-0`	Upon successful completion of this procedure, the Standby site becomes the newly Active site and client applications connect to it for messaging connectivity.
Name of Queue	`myFirstQueue`	The name of the queue for guaranteed messages.

Prerequisites

To perform a controlled failover in advanced event mesh, you require the following:

- SSH access to both event broker services in the replication pair. SSH access is required to execute Solace CLI commands
  - You may need to enable the connection ports for SSH access depending on your configuration (see Changing the Port Configuration for an Event Broker Service)
- a global-admin account to run the necessary Solace CLI commands for each event broker services (both sites)
- an account in advanced event mesh with either the **Cluster Editor** or **Administrator** role

Verify That the Replication Bridge is Bound to the Replication Queue

Verify that the replication bridge on the event broker service with the replication state of `standby` is bound to the replication queue of the event broker service with the replication state of `active`.

If the replication status is not bound, you must determine the reason before proceeding. In the Solace CLI, enter the following command:

To verify that the replication bridge is bound to the replication queue and check that `Queue`> `State` is a value of `bound` from running the following CONFIG command:

```
SolaceCLI (configure) # show message-vpn <Message
VPN name> replication [detail]
```

Where:

- `<Message VPN name>` is the Message VPN that is the same between your replication pair.
- `[detail]` is an optional parameter to get more details about the replication status.

For example, the Active event broker service is currently `nano-production-azzn9vsqdk5-solace-primary-0` and the Standby event broker service is currently `nano-production-89il3uubs0c-solace-primary-0`. For it to show as bounded, you would expect to see the results from running the following commands:

- Q (Queue state) - (U)p on Active site. This value indicates whether the replication bridge is bound.

If the Replication Queue is bound, these are the values you should also see. If you don't see these values, this may help you to determine what is incorrect in your Replication configuration.

- A (Admin State)—(U)p on both the Active and Standby site
- C (Config State)—(A)ctive on currently Active site and (S)tandby on Standby site
- B (Bridge State)—(U)p on the Standby site
- Q (Queue state) - (U)p on Active site. This value indicates whether the replication bridge is bound.
- R (Remote Bridge State)—(U)p on the Active site
- S/M/T—These flags show more configuration and operational state information, but are not important for controlled failover.

```
nano-production-azzn9vsqdk5-solace-primary-0> show message-vpn
myfirstservice replication

Flags Legend:
A - Admin State (U=Up, D=Down)
C - Config State (A=Active, S=Standby)
B - Local Bridge State (U=Up, Q=Queue Unbound, D=Down, -=N/A)
R - Remote Bridge State (U=Up, D=Down, -=N/A)
```

```
Q - Queue State (U=Up, D=Down, -=N/A)
S - Sync Replication Eligible (Y=Yes, N=No, -=N/A)
M - Reject Msg When Sync Ineligible (Y=Yes, N=No)
T - Transaction Replication Mode (A=Async, S=Sync, -=N/A)

Message VPN                       A C B R Q S M T
-------------------------------- - - - - - - - - -
myfirstservice                    U A - U U Y N A
```

For the Standby site:

```
nano-production-89il3uubs0c-solace-primary-0> show message-vpn
myfirstservice replication

Flags Legend:
A - Admin State (U=Up, D=Down)
C - Config State (A=Active, S=Standby)
B - Local Bridge State (U=Up, Q=Queue Unbound, D=Down, -=N/A)
R - Remote Bridge State (U=Up, D=Down, -=N/A)
Q - Queue State (U=Up, D=Down, -=N/A)
S - Sync Replication Eligible (Y=Yes, N=No, -=N/A)
M - Reject Msg When Sync Ineligible (Y=Yes, N=No)
T - Transaction Replication Mode (A=Async, S=Sync, -=N/A)

Message VPN                       A C B R Q S M T
-------------------------------- - - - - - - - -
myfirstservice                    U S U - - - N A
```

To further troubleshooting, you can see the details for the event broker service on the currently Active site using the `details` option if something wasn't correct. In this example, the configuration is correct and you can `Queue:` > `State:` is `bound`, which indicates that the Replication Queue is correctly bound.

```
nano-production-azzn9vsqdk5-solace-primary-0> show message-vpn
myfirstservice replication detail

Message VPN:                       myfirstservice
Admin Status:                      enabled
Config Status:                     active
Local Bridge:
  State:                           n/a
  Name:                            n/a
  Queue State:                     n/a
  Authentication:
    Scheme:                        Basic
    Basic:
      Client Username:             myfirstclientusername
      Password Configured:         Yes
    Client Certificate:
      Certificate File:
      Using Server Certificate:    Yes
  Compressed:                      No
  SSL:                             No
  Message Spool:
    Window Size:                   255
  Unidirectional:
    Client Profile:                #client-profile
  Retry Delay:                     3
Remote Bridge:
  State:                           up
  Name:
#bridge/v:nanoproduction89il3uubs0csolaceprimary0/myfirst
  service/1
Queue:
  State:                           bound
  Quota (MB):                      60000
  Reject Msg to Sender on Discard: Yes
Ack Propagation:
  Interval in Messages:            20
Sync Replication:
  Eligible:                        yes
    Duration:                      2d 1h 51m 57s
  Mate Flow Congested:             no
    Duration:                      0d 0h 0m 0s
  Reject Msg When Sync Ineligible: No
Transaction Replication Mode:      async
```

Switch Activity of the Active Site to a `Standby` State

When you switch activity, you are switching the replication state of the Message VPN on one event broker service (the Active site) from `active` to `standby`.

In the Solace CLI, use the following command to change replication state on the Message VPN at the currently Active site:

```
SolaceCLI (configure) # message-vpn <Message VPN name>
SolaceCLI (configure/message-vpn)# replication state <newstate>
```

Where :

- `<Message VPN name>` is the Message VPN that is the same between your replication pair.
- `<newstate>` is the state to move the Messge VPN to, which can be `active` or `standby`

For example, the following are the commands to use to switch activity:

```
nano-production-azzn9vsqdk5-solace-primary-0> enable
nano-production-azzn9vsqdk5-solace-primary-0# configure
nano-production-azzn9vsqdk5-solace-primary-0(configure)# message-vpn
myfirstservice
nano-production-azzn9vsqdk5-solace-primary-0(configure/message-vpn)#
replication state standby
nano-production-azzn9vsqdk5-solace-primary-0(configure/message-vpn)#
show message-vpn myfirstservice replication

Flags Legend:
A - Admin State (U=Up, D=Down, -=N/A)
C - Config State (A=Active, S=Standby, -=N/A)
B - Local Bridge State (U=Up, Q=Queue Unbound, D=Down, -=N/A)
R - Remote Bridge State (U=Up, D=Down, -=N/A)
Q - Queue State (U=Up, D=Down, -=N/A)
S - Sync Replication Eligible (Y=Yes, N=No, -=N/A)
M - Reject Msg When Sync Ineligible (Y=Yes, N=No, -=N/A)
T - Transaction Replication Mode (A=Async, S=Sync, -=N/A)

Message VPN                       A C B R Q S M T
-------------------------------- - - - - - - - -
myfirstservice                    U S D U - - N A
```

```
nano-production-azzn9vsqdk5-solace-primary-0(configure/message-vpn)#
```

Drain the Replication Queue in the Formerly Active Site

You must allow any messages or transactions in the Message VPN from the formerly Active site to propagate to the corresponding Message VPN on its replication mate (the newly Active site). We recommend that you allow the propagation of all messages and transactions to prevent the loss of asynchronous replication messages and transactions.

To determine whether the replication queue has drained for the Message VPN on the replication-standby event broker service, enter the following command in the Solace CLI:

```
SolaceCLI > show queue #MSGVPN_REPLICATION_DATA_QUEUE message-vpn
<Message VPN name>
```

Where :

- `#MSGVPN_REPLICATION_DATA_QUEUE` is the name of the replication queue on the Message VPN of your event broker service.
- `<Message VPN name>` is the name of the Message VPN

If the output displays a value of 0 for the `Current Messages Spooled` value, the queue has been drained. If not, wait a few seconds and run the command the again.

> Do not change the replication state for the Message VPN on the formerly Activeevent broker service until `Current Messages Spooled` is 0 for the replication queue.

For example, check that the replication queue has drained on `nano-production-azzn9vsqdk5-solace-primary-0` (the formerly Active site):

```
nano-production-azzn9vsqdk5-solace-primary-0> enable
nano-production-azzn9vsqdk5-solace-primary-0# configure
nano-production-azzn9vsqdk5-solace-primary-0(configure)# show queue
#MSGVPN_REPLICATION_DATA_QUEUE message-vpn myfirstservice
```

```
Name                                 : #MSGVPN_REPLICATION_DATA_QUEUE
Message VPN                          : myfirstservice
Durability                           : Durable
...
...
Bind Time Forwarding Mode            : Store-And-Forward
Current Messages Spooled             : 4
Current Spool Usage (MB)             : 0.0060
High Water Mark (MB)                 : 0.0100
Total Delivered Unacked Msgs         : 0
Max Delivered Unacked Msgs Per Flow  : 250000
...
...
Last Msg Id Delivered            : 150462

nano-production-azzn9vsqdk5-solace-primary-0(configure)#
```

After a period of time, run the command again:

```
nano-production-azzn9vsqdk5-solace-primary-0(configure)# show queue
#MSGVPN_REPLICATION_DATA_QUEUE message-vpn myfirstservice

Name                                 : #MSGVPN_REPLICATION_DATA_QUEUE
Message VPN                          : myfirstservice
Durability                           : Durable
...
...
Bind Time Forwarding Mode            : Store-And-Forward
Current Messages Spooled             : 0
Current Spool Usage (MB)             : 0.0000
High Water Mark (MB)                 : 0.0000
Total Delivered Unacked Msgs         : 0
Max Delivered Unacked Msgs Per Flow  : 250000
...
...
Last Msg Id Delivered            : 150462

nano-production-azzn9vsqdk5-solace-primary-0(configure)#
```

Heuristically Commit or Roll Back Any In-Progress Transactions

If you have applications that use XA transactions, there may be some prepared transactions on the formerly Active site that need to be heuristically committed or rolled back. If not, the steps in this section do not need to be done.

Only prepared transactions (in the PREPARED state) must be addressed. Transactions in other states can be ignored. If you do not deal with the prepared transactions:

- transaction resources are wasted and it reduces the transaction handling capacity of both the Active and Standby sites
- in the event of a failover (or failback) to the originally Active site, duplicate message delivery or message loss may occur

> It is important that you only perform the heuristic commit or heuristic rollback operations on the Message VPN of the formerly Active site.

Whether you decide to commit or rollback the transaction depend on various factors. When you look at XA transactions, the end goal is to make sure that the transactions are treated consistently on all branches of the distributed transaction across both replication sites. Here are some guidelines you can use to make this decision:

- For prepared XA transactions that are controlled by a transaction manager in an application server, you should check the logs or state of the transaction manager for the XID of the prepared transaction to examine the other branches of the distributed transaction:
    - If all the other branches have been committed, you should heuristically commit the transaction
    - If any of the other branches have rolledback, you should heuristically roll back the transaction
- For XA prepared transactions that are not controlled by a transaction manager, manually coordinate the distributed transaction so that all the branches of the distributed transaction are either committed or rolled back.

To show replicated transactions, enter the following command to find all transactions with the state of PREPARED.

```
SolaceCLI > show transaction message-vpn <Message VPN name> state
PREPARED replicated [detail]
```

Where:

- `<Message VPN name>` is the Message VPN that is the same between your replication pair.
- `[detail]` is an optional parameter

For example, to show the replicated transaction for `PREPARED` for the Message VPN of `myfirstservice`, enter the following command:

```
nano-production-azzn9vsqdk5-solace-primary-0> show transaction
message-vpn myfirstservice state PREPARED replicated
Flags Legend
T - Transaction Type (X=XA L=Local)
S - Transaction State (A=Active S=Suspended I=Idle P=Prepared
C=Complete)
R - Replicated (Y=Yes N=No)
XID
Messages
Message VPN                                   T S R Last State Change
 Spooled
--------------------------------------------- - - - -----------------
--------
myfirstservice                                X P Y                1s
       0
```

If you don't see a value, then there are no transactions in the PREPARED state:

For example, to show the details of `PREPARED` transactions for the Message VPN named `myfirstservice`:

```
nano-production-azzn9vsqdk5-solace-primary-0> show transaction
message-vpn myfirstservice state PREPARED replicated detail
XID:                       0021B028-00-01
Message VPN:               myfirstservice
Client:                    username/15848/#000c0001
Client Username:           myfirst-clientusername
Session:                   N/A
Idle Timeout:              0
Type:                      XA
State:                     PREPARED
Replicated:                Yes
Last State Change:         0d 0h 0m 0s
Messages:                  10
Messages Published:        0
Messages Consumed:         150
Publisher Messages:
Message Id           Topic
-------------------- ------------------------------------------------
-----------
Consumer Messages:
Message Id           Type  Endpoint Name
-------------------- ----- ------------------------------------------
-----------
3118727406           queue test
3118727407           queue test
3118727408           queue test
3118727409           queue test
3118727410           queue test
3118727411           queue test
3118727412           queue test
3118727413           queue test
3118727414           queue test
3118727415           queue test
```

To show the details of a particular transaction, enter the following command:

```
nano-production-azzn9vsqdk5-solace-primary-0> show transaction xid
<xidvalue> detail
```

Where:

`xidsvalue` specifies the XID of the transaction to be displayed.

Change the State of the Message VPN to Active on the Formerly Standby Site

When you are ready to switch the activity to the Standby site, you can set the replication status of the Message VPN to the `active` state using the following CONFIG commands:

```
SolaceCLI (configure)# message-vpn <Message VPN name>
SolaceCLI(configure/message-vpn)# replication state <newstate>
```

Where:

- `<Message VPN name>` is the Message VPN that is the same between your replication pair.
- `<newstate>` is the state to move the Messge VPN to, which can be `active` or `standby`. In this case, use `active`.

The following example shows the status before setting the replication state of the Message VPN on the Standby site to the newly Active site:

```
nano-production-89il3uubs0c-solace-primary-0> enable
nano-production-89il3uubs0c-solace-primary-0# configure
nano-production-89il3uubs0c-solace-primary-0(configure)# message-vpn
myfirstservice
nano-production-89il3uubs0c-solace-primary-0(configure/message-vpn)#
show message-vpn myfirstservice replication

Flags Legend:
A - Admin State (U=Up, D=Down, -=N/A)
C - Config State (A=Active, S=Standby, -=N/A)
B - Local Bridge State (U=Up, Q=Queue Unbound, D=Down, -=N/A)
R - Remote Bridge State (U=Up, D=Down, -=N/A)
Q - Queue State (U=Up, D=Down, -=N/A)
S - Sync Replication Eligible (Y=Yes, N=No, -=N/A)
M - Reject Msg When Sync Ineligible (Y=Yes, N=No, -=N/A)
T - Transaction Replication Mode (A=Async, S=Sync, -=N/A)

Message VPN                      A C B R Q S M T
-------------------------------- - - - - - - - -
myfirstservice                   U S U - - - N A

nano-production-89il3uubs0c-solace-primary-0(configure/message-vpn)#
replication state active
nano-production-89il3uubs0c-solace-primary-0(configure/message-vpn)#
show message-vpn myfirstservice replication

Flags Legend:
A - Admin State (U=Up, D=Down, -=N/A)
C - Config State (A=Active, S=Standby, -=N/A)
B - Local Bridge State (U=Up, Q=Queue Unbound, D=Down, -=N/A)
R - Remote Bridge State (U=Up, D=Down, -=N/A)
Q - Queue State (U=Up, D=Down, -=N/A)
S - Sync Replication Eligible (Y=Yes, N=No, -=N/A)
M - Reject Msg When Sync Ineligible (Y=Yes, N=No, -=N/A)
```

```
T - Transaction Replication Mode (A=Async, S=Sync, -=N/A)

Message VPN                      A C B R Q S M T
-------------------------------- - - - - - - - -
myfirstservice                   U A - D D N N A

nano-production-89il3uubs0c-solace-primary-0(configure/message-vpn)#
```

Move the Custom Hostname to the Newly Active Site

In the Cloud Console, you must move the hostname on the event broker service of the formerly Active site to the event broker service on the newly Active site.

1. In **Cluster Manager**, on the **Services** page, click the event broker service that was formerly in the Active state.

   This event broker service should have the custom hostname set.
2. Select the **Manage** tab and then click **Advanced Options**.
3. On the **Hostnames** tile beside the custom hostname, click **Actions** •••, and then in the drop-down list, select **Move**.
4. In the **Move Hostname** dialog, in **Select the service you wish to move it to**, choose the event broker service to which you want to move the hostname.
5. In **Select the endpoint to assign to hostname**, select the name of the endpoint to assign. The type of endpoint available is based what endpoints are configured for the event broker service.

   > For Public Regions, only public endpoints are available.
6. Click **Move Hostname**.

The process to move the hostname may take a few minutes. After the operation completes:

- verify that the hostname was moved to the event broker service on the newly Active site (formerly the Standby site)
- verify that client applications are able to re-connect to the Message VPN on the event broker service on the newly Active site

At this point, full messaging operations resume for your client applications.

Delete the Heuristically Completed Transactions

If there are transactions that you previously heuristically completed (you have applications that use XA Transactions), SAP recommends that you delete them to free up resources. If you do not use XA Transactions, the steps in this section are not required.

You must always delete the completed transactions on the formerly Active site. In addition, you may have to delete completed transactions on the newly Active site (formerly Standby site), depending on the replication mode and the XA transaction manager.

The XA transaction manager may automatically delete the heuristically completed transactions on the Message VPN on your event broker service after it connects to the newly Active site as it reconciles the XA transaction states. We recommend that you allow this process to complete before deleting the completed transactions.

To delete a completed transaction, enter the following ADMIN command on the formerly Active site:

```
SolaceCLI (admin/message-spool )> delete-transaction xid <xid>
```

Where:

- `xid` specifies the XID of the transaction to be deleted.

We recommend that you check both Message VPNs on the Active and Standby sites for completed transactions.

Performing an Uncontrolled Failover of Event Broker Services

There is no automated, uncontrolled failover. You (the customer) are responsible for performing the failover if a disaster condition impacts your event broker services.

In the event of a failure of an active data center or a network isolation, there may not be an opportunity to gracefully release activity from the Message VPNs from the Active site and transition activity to the Standby site.

There are three types of uncontrolled failovers:

- **Short -Term Outage**
  The Active site is out-of-service or isolated for a short duration (for example, minutes or hours). The replication queue has enough capacity to store all replicated messages and transactions during the outage.
- **Long-Term Outage**
  The Active site is out-of-service or isolated for a long duration (for example, days or weeks). The replication queue does not have enough capacity to store all replicated messages and transactions during the outage.
- **Complete Failure**
  The Active site goes out of service and cannot be recovered. A critical component (the event broker, region connectivity, etc.) has been lost, or data on the external disk has been lost.

There are potential consequences of an uncontrolled failover that include:

- The build-up of messages on the replication queue for the duration of the outage at the Active site.
- The replication queue becoming full.
- The loss of one or more event brokers at the failed site prior to restoring operation at the failed site.
- The possibility of lost messages and transactions being replicated asynchronously.
- An increased probability and volume of duplicate message delivery.

No matter which type of uncontrolled failover you experience, the procedure to handle an uncontrolled failover is the same. We recommend that you contact SAP for help to resolve any issues that may be present in the circumstance of a specific uncontrolled failover in the Failed site.

> The procedure to perform an uncontrolled failover in advanced event mesh for SAP Integration Suite is similar to the other SAP software event brokers and appliances. One additional step is the requirement to switch the custom hostname for the event broker service.

Before you begin this procedure, ensure you have fulfilled the Prerequisites.

> SAP recommends that you verify that the configuration on the Standby site is the same as the Active site prior to performing a failover. Any configuration changes that are made in the Cloud Console to your event broker service on the Active site must be manually

> configured duplicated on the Standby site. For more information, see Considerations and Best Practices for Using Replication.

To perform an uncontrolled failover, do the following (you must repeat this procedure for each replication pair):

1. Change the Status of the Message VPN to Active on the Formerly Replication Standby Site.
2. Move the Custom Hostname to the Newly Active Site.
3. Suspend Replication If Necessary.
4. Recover the Failed Site and Set As the Replication Standby. For this recovery, there are a number of steps to complete.

For the examples provided on this page, we use the following values:

Example Item	Value	Description
Name of the Message VPN	`myfirstservice`	The event broker services are in different regions and name of the Message VPN on both are configured to be the same name.
Primary Site	primary-myfirstservice or `nano-production-azzn9vsqdk5-solace-primary-0`	The Active site (or Formerly Active site) at the start of the procedure that becomes the Standby site (for Failed site in this case). This site is in a faulty state.
Backup Site	backup-myfirstservice or `nano-production-89il3uubs0c-solace-primary-0`	The Standby site that becomes the Active site after this procedure. This is the Backup site to which to switch activity.

Prerequisites

To perform a controlled failover in advanced event mesh, you require the following:

- SSH access to both event broker services in the replication pair. SSH access is required to execute Solace CLI commands
    - You may need to enable the connection ports for SSH access depending on your configuration (see Changing the Port Configuration for an Event Broker Service)
- a global-admin account to run the necessary Solace CLI commands for each event broker services (both sites)
- an account in advanced event mesh with either the **Cluster Editor** or **Administrator** role

Set the Administration State for Replication to Down

Change the Status of the Message VPN to Active on the Formerly Replication Standby Site

Follow this procedure after you have determined that an uncontrolled failure has occurred - that is, no messaging activity is possible to your event broker service at the currently Active site.

To restore service, you access the event broker service and then change the replication state of the Message VPN to `active`.

Switch the state of the Message VPN to `active` using the following CONFIG commands:

```
SolaceCLI (configure)# message-vpn <Message VPN name>
SolaceCLI (configure/message-vpn)# replication state <newstate>
```

where:

- `<Message VPN name>` is the Message VPN that is the same between your replication pair.
- `<newstate>` is the state to move the Message VPN to, which can be `active` or `standby`. In this case, use `active`.

The following example shows the status before setting the replication state of the Message VPN on the formerly Standby site to the `active` status:

```
nano-production-89il3uubs0c-solace-primary-0> enable
nano-production-89il3uubs0c-solace-primary-0# configure
nano-production-89il3uubs0c-solace-primary-0(configure)# message-vpn
myfirstservice
nano-production-89il3uubs0c-solace-primary-0(configure/message-vpn)#
```

```
replication state active
```

Since a Standby site is not available (your previously Active site is the Failed site), asynchronous messages and transactions are stored in the replication queue. By default, synchronous replication switches to asynchronous, causing those messages and transactions to also be stored in replication queue. If r`eject-msg-when-sync` ineligible is set on the Message VPN, synchronous replication is blocked until the Message VPN is available (when the Failed site is restored).

Move the Custom Hostname to the Newly Active Site

In the Cloud Console, move the hostname of the event broker service on the Failed site to the event broker service on the Active site (the replication mate that you changed to the `active` state in the previous step).

In the Cloud Console, you must move the hostname on the event broker service of the formerly Active site to the event broker service on the newly Active site.

1. In **Cluster Manager**, on the **Services** page, click the event broker service that was formerly in the Active state.

   This event broker service should have the custom hostname set.
2. Select the **Manage** tab and then click **Advanced Options**.
3. On the **Hostnames** tile beside the custom hostname, click **Actions** ••• , and then in the drop-down list, select **Move**.
4. In the **Move Hostname** dialog, in **Select the service you wish to move it to**, choose the event broker service to which you want to move the hostname.
5. In **Select the endpoint to assign to hostname**, select the name of the endpoint to assign. The type of endpoint available is based what endpoints are configured for the event broker service.

   > For Public Regions, only public endpoints are available.
6. Click **Move Hostname**.

The process to move the hostname may take a few minutes. After the operation completes:

- verify that the hostname was moved to the event broker service on the newly Active site (formerly the Standby site)
- verify that client applications are able to re-connect to the Message VPN on the event broker service on the newly Active site

At this point, client connectivity resumes.

Suspend Replication If Necessary

If it is a prolonged outage, suspend replication to prevent the replication queue from becoming full on your newly active event broker service.

If the replication queue becomes full, messages published to replicated topics (in or out of transactions are rejected), since no replication service can be provided. If you know the outage is prolonged or the replication queue is close to becoming full (high event log has been triggered on the replication queue), it may be necessary to suspend the replication service to continue to provide non-replicated service to the replicated topics.

To suspend replication, disable the `reject-msg-to-send` behavior on the replication queue using the following CONFIG command:

```
SolaceCLI (configure/message-vpn/<Message VPN name>)# replication
queue
SolaceCLI (configure/message-vpn/<Message
VPN name>/replication/queue)# no reject-msg-to-sender-on-discard
```

For example, on newly Active site, perform the following commands to suspend replication:

```
nano-production-89il3uubs0c-solace-primary-0> enable
nano-production-89il3uubs0c-solace-primary-0# configure
nano-production-89il3uubs0c-solace-primary-0(configure)# message-vpn
myfirstservice
nano-production-89il3uubs0c-solace-primary-0(configure/message-vpn)#
replication queue
nano-production-89il3uubs0c-solace-primary-0(configure/message-
vpn/replication/queue)# no reject-msg-to-sender-on-discard
```

After you suspend replication with this setting, the replicated service continues until the replication queue gets full. After the replication queue is full, only local, non-replicated service is provided.

Recover the Failed Site and Set As the Replication Standby

After the Failed site has been recovered, it must have management access available. Client connectivity is also required, but client applications won't be able to connect because connections are made via the custom hostname for the replicated pair. Here the steps for preparing the recovered failed event broker service to be the Standby site:

1. Change the Message VPN on the event broker service at the Failed site to Standby.
2. On the restored site, verify the Message Spool can provide service.
3. On the restored site, heuristically Complete Transactions. This is required only if you have client applications that use XA Transactions.
4. Re-able Replication if necessary.
5. On the restored site, retrieve the replication queue spooled messages from the restored Failed site.

Change the Message VPN to a Standby Status and Enable Replication

Set the replication state on the Message VPN of the event broker service at the Restored site (recovered Failed site) to `standby` using the following CONFIG commands:

```
SolaceCLI (configure)# message-vpn <Message VPN name>
SolaceCLI (configure/message-vpn/<Message VPN name>)# replication
status standby
```

For example, on the event broker service of the failed service, set the Message VPN of `myfirstservice` to the `standby` status:

```
nano-production-azzn9vsqdk5-solace-primary-0> enable
nano-production-azzn9vsqdk5-solace-primary-0# configure
nano-production-azzn9vsqdk5-solace-primary-0(configure)# message-vpn
myfirstservice
```

```
nano-production-azzn9vsqdk5-solace-primary-0(configure/message-vpn)#
replication state standby
```

Verify the Message Spool

We recommend that you verify that the Message Spool for the event broker service at the Failed site is capable of providing service. Enter the following USER command to verify if the event broker service is capable of providing service:

```
SolaceCLI> show redundancy
```

- If the `Activity Status` is `Local Active` and `Message Spool Status` is `AD-Active`, it is capable to provide service
- Otherwise, if the `Activity Status` is `Local Inactive` and the `Message Spool Status` is `AD-Not Ready`, the Message Spool it uses is not yet active. You must resolve the issue to prevent the Message Spool from becoming active. If you cannot, contact SAP.

In this situation, you must prevent the failed event broker service from becoming active to resolve the issue. If you cannot resolve the issue, contact SAP.

Heuristically Complete Transactions

If you have client applications that use XA Transactions, you must heuristically commit or heuristically rollback any prepared transactions on the failed site (previously Active site). If you do not have applications that use XA Transactions, you do not need to perform this step.

Once transactions are heuristically completed (committed or rolled back), delete them to free up the resources.

To commit, rollback or delete a transaction, enter the appropriate ADMIN commands on the Failed site:

```
SolaceCLI (admin/message-spool) commit-transaction xid <xid>
```

and/or

```
SolaceCLI (admin/message-spool) rollback-transaction xid <xid>
```

and then

```
SolaceCLI (admin/message-spool) delete-transaction xid <xid>
```

Where:

`xid` specifies the XID of the transaction to be committed, rolled back, or deleted.

Wait for Synchronous Replication to be Eligible

After connectivity is restored between the previously Failed site and your now Active site, the replication bridge will connect from the Standby site to the Active site and drain the replication queue to synchronize the sites. Depending on how much message and transaction data is in the replication queue and the available bandwidth between the sites, this process may take a long time. When this process is complete, replication is no longer considered to be degraded and the Message VPN on the event broker services are eligible for synchronous replication.

To verify the replication status, run the following USER command:

```
SolaceCLI > show message-vpn <Message VPN name> replication
```

In the following example, the information displayed is for the Active site (`nano-production-89il3uubs0c-solace-primary-0`).

```
nano-production-89il3uubs0c-solace-primary-0> show message-vpn
myfirstservice replication
Flags Legend:
A - Admin State (U=Up, D=Down)
C - Config State (A=Active, S=Standby)
B - Local Bridge State (U=Up, Q=Queue Unbound, D=Down, -=N/A)
R - Remote Bridge State (U=Up, D=Down, -=N/A)
Q - Queue State (U=Up, D=Down, -=N/A)
S - Sync Replication Eligible (Y=Yes, N=No, -=N/A)
M - Reject Msg When Sync Ineligible (Y=Yes, N=No)
T - Transaction Replication Mode (A=Async, S=Sync, -=N/A)
Message VPN                      A C B R Q S M T
-------------------------------- - - - - - - - -
myfirstservice                   U A - - U N N A
```

A `Y` under the `S` (Sync Replication Eligible) column indicates that synchronous replication is eligible for the Message VPN on the event broker service at your .

```
nano-production-89il3uubs0c-solace-primary-0> show message-vpn
myfirstservice replication
Flags Legend:
A - Admin State (U=Up, D=Down)
C - Config State (A=Active, S=Standby)
B - Local Bridge State (U=Up, Q=Queue Unbound, D=Down, -=N/A)
R - Remote Bridge State (U=Up, D=Down, -=N/A)
Q - Queue State (U=Up, D=Down, -=N/A)
```

```
S - Sync Replication Eligible (Y=Yes, N=No, -=N/A)
M - Reject Msg When Sync Ineligible (Y=Yes, N=No)
T - Transaction Replication Mode (A=Async, S=Sync, -=N/A)
Message VPN                      A C B R Q S M T
-------------------------------- - - - - - - - -
myfirstservice                   U A U - U Y N A
```

Re-enable Replication When Necessary

If you previously had to suspend replication because the replication queue was full, you can re-enable it.
Enter the following CONFIG command:

```
SolaceCLI (configure/message-vpn/replication/queue)# reject-msg-to-sender-on-discard
```

For example, enter the following commands on the newly Active site:

```
nano-production-89il3uubs0c-solace-primary-0> enable
nano-production-89il3uubs0c-solace-primary-0# configure
nano-production-89il3uubs0c-solace-primary-0(configure)# message-vpn myfirstservice
nano-production-89il3uubs0c-solace-primary-0(configure/message-vpn)# replication queue
nano-production-89il3uubs0c-solace-primary-0(configure/message-vpn/replication/queue)# reject-msg-to-sender-on-discard
```

Retrieve Replication Queue Spooled Messages From the Restored Failed Site

Asynchronously spooled messages on the restored Failed site (formerly Active site) can only be consumed when the activity is failed back to it. You can fail back to the restore site to recover those messages and to remove any unnecessary duplicated messages (referred to as deduplication). For more information, see Failing Back to a Restored Site After an Uncontrolled Failover.

To retrieve these messages, we recommend that you perform a controlled failover during your next scheduled maintenance window. For more information, see Performing a Controlled Failover of Event Broker Services.

Failing Back to a Restored Site After an Uncontrolled Failover

You may want to fail back (switch the replication state back) to your restored site after an uncontrolled failover. After the message VPN replication has become synchronous eligible on your event broker service, you can fail back to the restored site. SAP recommends that you **do not** the switch back to the your restored site immediately, and that you wait a period of time until all the messages that were replicated before the uncontrolled failover have been consumed. On the restored site, if haven't had to chance to change the status of the Message VPN to `standby`, SAP recommends you do this immediately. To set the formerly Active site to a `standby` status, see Change the Message VPN to a Standby Status and Enable Replication.

The procedure to failback to the restored site is the same as a controlled failover. However, the following considerations apply, especially if you are considering switching back the original Active site after an uncontrolled failover:

- Transactions that were in progress when the uncontrolled failover occurred are at risk of loss or duplication.
- If the Message Spool of the restored site could not be recovered, messages replicated before the failure that have not been consumed on the Active site are lost.

If the Message Spool on the Failed site (the formerly Active site) can be recovered and the replication queue on the now Active site has not been filled, then the messages that were replicated before the failover are available and full replication behavior is restored.

In a long- term failure where the replication queue fills, then the messages and transactions that only made it into the replication queue are available on a fail-back. If there was hardware failure or loss of data on the external disk, then the Message Spool on the failed site cannot be recovered and is empty.

If there is a hardware failure or loss of data on the external disk, then the pre-failure message spool cannot be recovered and is empty.

Transactions that were in progress at the time of the uncontrolled failover are not automatically synchronized after restoring the Failed site. The risks of loss and duplication for synchronous transactions can be eliminated, assuming replication was never disabled if you repeat the following procedure for every endpoint before switching activity back to the restored Failed site.

1. Verify if the Endpoint is Configured to Propagate Consumer Acknowledgments to the Replication Standby Site
2. Display the Internal IDs of Messages on the Formerly Active Site

3. Display the Internal IDs of Messages on the Active Site
4. Delete Messages on the Formerly Active Site

Verify if the Endpoint is Configured to Propagate Consumer Acknowledgments to the Replication Standby Site

On the newly Active site, check if the endpoint is configured to propagate consumer acknowledgments. To perform this, run the following USER command:

```
SolaceCLI > show queue <queue-name> message-vpn <Message VPN
name> detail
```

where:

- `<Message VPN name>` is the Message VPN that is the same between your replication pair.
- `<queue-name>` the name of the endpoint to check.

For example, on the newly Active site (`nano-production-89il3uubs0c-solace-primary-0`), for a queue named `myFirstQueue` and for the Message VPN `myfirstservice`:

```
nano-production-89il3uubs0c-solace-primary-0> show queue myFirstQueue
message-vpn myfirstservice detail

Name                                 : myFirstQueue
Message VPN                          : myfirstservice
Durability                           : Durable
Id                                   : 7
Type                                 : Primary
Admin Ingress                        : Up
Admin Egress                         : Up
...
...
Consumer Ack Propagation             : Yes
Reject Low-Priority-Msg              : No
Reject Low-Priority-Msg Limit        : 0
Low-Priority-Msg Congestion State    : Disabled
...
...
Event Threshold                           Set Value      Clear Value
---------------------------------- ---------------- ----------------
Bind count                                 80%(800)         60%(600)
```

```
Spool usage (MB)                          25%(1250)          18%(900)
Reject Low-Priority-Msg Limit               80%(0)             60%(0)

Egress Flows

nano-production-azzn9vsqdk5-solace-primary-0#
```

Move on to the next endpoint if `Consumer Ack Propagation` is not enabled (`Yes`). Deduplication is required only for endpoints when `Consumer Ack Propagation` is enabled.

Display the Internal IDs of Messages on the Formerly Active Site

On the Restored site (previously the Failed site), enter the following command to find the message identifiers of all messages that were unsent.

For example, to see the details of the Message VPN:

```
nano-production-azzn9vsqdk5-solace-primary-0> show queue myFirstQueue
message-vpn myfirstservice messages detail

Message Id: 2852
  Priority:                         n/a
  Date spooled:                     Nov  2 2022 21:00:28 UTC
  Publisher Id:                     1150
  Replication Group Message Id: rmid1:1b093-ce1bbc2b385-00000000-
00010550
  Sequence Number:                  n/a
  Expiry Time:                      never
  Delivery Eligible Time:           now
  Dead Message Queue Eligible:      no
  Content:                          0.0000 MB
  Attachment:                       0.0000 MB
  Replicated:                       yes
  Replicated Mate Message Id:       n/a
  Sent:                             no
  Redeliveries:                     0

Message Id: 2853
  Priority:                         n/a
  Date spooled:                     Nov  2 2022 21:03:22 UTC
  Publisher Id:                 1150
  Replication Group Message Id: rmid1:1b093-ce1bbc2b385-00000000-
000105de
  Sequence Number:              n/a
  Expiry Time:                  never
  Delivery Eligible Time:       now
  Dead Message Queue Eligible:  no
  Content:                      0.0000 MB
  Attachment:                   0.0000 MB
  Replicated:                   yes
  Replicated Mate Message Id:   n/a
  Sent:                         no
  Redeliveries:                 0

Message Id: 2901
  Priority:                     n/a
  Date spooled:                 Nov  2 2022 21:03:25 UTC
  Publisher Id:                 1150
  Replication Group Message Id: rmid1:1b093-ce1bbc2b385-00000000-
000105df
  Sequence Number:              n/a
  Expiry Time:                  never
  Delivery Eligible Time:       now
  Dead Message Queue Eligible:  no
  Content:                      0.0000 MB
  Attachment:                   0.0000 MB
  Replicated:                   yes
  Replicated Mate Message Id:   n/a
  Sent:                         no
  Redeliveries:                 0

Message Id: 2903
  Priority:                     n/a
  Date spooled:                 Nov  2 2022 21:03:30 UTC
  Publisher Id:                 1150
  Replication Group Message Id: rmid1:1b093-ce1bbc2b385-00000000-
000105e8
  Sequence Number:              n/a
  Expiry Time:                  never
  Delivery Eligible Time:       now
  Dead Message Queue Eligible:  no
  Content:                      0.0000 MB
  Attachment:                   0.0000 MB
  Replicated:                   yes
  Replicated Mate Message Id:   n/a
  Sent:                         no
  Redeliveries:                 0

Message Id: 2944
  Priority:                     n/a
  Date spooled:                 Nov  2 2022 21:09:46 UTC
  Publisher Id:                 1150
  Replication Group Message Id: rmid1:1b093-ce1bbc2b385-00000000-
00010718
  Sequence Number:              n/a
  Expiry Time:                  never
  Delivery Eligible Time:       now
  Dead Message Queue Eligible:  no
  Content:                      0.0000 MB
  Attachment:                   0.0000 MB
  Replicated:                   yes
  Replicated Mate Message Id:   2919
  Sent:                         no
  Redeliveries:                 0

Message Id: 2945
  Priority:                     n/a
  Date spooled:                 Nov  2 2022 21:11:48 UTC
  Publisher Id:                 1150
  Replication Group Message Id: rmid1:1b093-ce1bbc2b385-00000000-
0001077d
  Sequence Number:              n/a
  Expiry Time:                  never
  Delivery Eligible Time:       now
  Dead Message Queue Eligible:  no
  Content:                      0.0000 MB
  Attachment:                   0.0000 MB
  Replicated:                   yes
  Replicated Mate Message Id:   2921
  Sent:                         no
  Redeliveries:                 0


nano-production-azzn9vsqdk5-solace-primary-0
```

Display the Internal IDs of Messages on the Active Site

To see which messages have been replicated, you must run the following command on the newly Active site.

```
SolaceCLI # show queue <queue-name> message-vpn <Message VPN name>
messages oldest
```

where:

- `<Message VPN name>` is the Message VPN that is the same between your replication pair.
- `<queue-name>` the name of the endpoint to check.

For example, to see the oldest message in the queue:

```
nano-production-89il3uubs0c-solace-primary-0> show queue myFirstQueue
message-vpn myfirstservice messages oldest

Name: myFirstQueue


Message VPN: myfirstservice

Message Id                          Replicated Mate Message Id
  Sent
2840                                2852
   yes
2841                                2853
   yes
2919                                n/a
    no
2921                                n/a
    no
```

Delete Messages on the Formerly Active Site

Delete messages on the formerly Active site that match ALL of the following conditions:

- The message must have a Replicated flag set to `yes`.
- The message must have a Replicated Mate Message Id of `n/a`.
- The Message must not match any Replicated Mate Message Id on the newly Active site (`nano-production-89il3uubs0c-solace-primary-0` in the example in the previous section).

In the example, for the messages from the formerly Active site listed in that example:

- Messages 2901 and 2903 can be deleted.
- Messages 2852 and 2853 cannot be deleted because their Message Ids exist in the `Replicated Mate Message Id` field of the newly Active site (`nano-production-89il3uubs0c-solace-primary-0`).
- Messages 2944 and 2945 cannot be deleted because the Replicated Mate Message Id field is not `n/a`.

Enter the following ADMIN command by navigating to the message-spool for the Message VPN where you want to delete the messages:

```
SolaceCLI (admin/message-spool)# delete-messages queue <queue-name>
message <msg-id>
```

Where:

- `<queue-name>` the name of the endpoint to check.
- `<msg-id>` is the identifier on the restore site (formerly Active site).

For example, to delete message 2901 from the queue named `myFirstQueue` in the example above using the ADMIN command on the message spool for the Message VPN called `myfirstservice`:

```
nano-production-azzn9vsqdk5-solace-primary-0> enable
nano-production-azzn9vsqdk5-solace-primary-0# admin
nano-production-azzn9vsqdk5-solace-primary-0(admin)# message-spool
message-vpn myfirstservice
nano-production-azzn9vsqdk5-solace-primary-0(admin/message-spool)#
delete-messages queue myFirstQueue message 2901
This will delete spooled message 2901 in myFirstQueue
Do you want to continue (y/n)? y
```

```
nano-production-azzn9vsqdk5-solace-primary-0(admin/message-spool)#
```

End of Document

This page has been intentionally left empty.