(Optional) Use Fully Qualified Domain Names to Form a Cluster

This chapter is about changing a cluster, that was formed using IP addresses, so that the peers use FQDNs to form the cluster. This is necessary if you want to enforce TLS verification between peers. If you have not yet formed your cluster,see How to Form a Cluster.

If you are creating a cluster of Expressway-Es, they might be in an isolated network such as a DMZ, and you'll need to use a local mapping if you want to enforce TLS verification. If you're forming a cluster of Expressway-Cs, you should not need to use cluster address mapping.

This chapter explains the following:

Cluster Address Mapping for Expressway-E Clusters

For secure deployments like MRA, each Expressway-E peer must have a certificate with a SAN containing its public FQDN. The FQDN is mapped in the public DNS to the Expressway-E's public IP address. This configuration enables external entities, like MRA endpoints, to discover the Expressway-E's public interface and establish a secure connection.

Do You Need Cluster Address Mapping?

- If you simply want to cluster Expressway-E peers and you don't need TLS verification between them, then you can form the cluster using the nodes' private IP addresses. You don't need cluster address mapping.
- If you want the Expressway-E peers in a cluster to verify each other's identities using certificates, you could allow them to use DNS to resolve cluster peer FQDNs to their public IP addresses. This is a perfectly acceptable way to form a cluster if the Expressway-E nodes have only one NIC, are not using static NAT, and have routable IP addresses. You don't need cluster address mapping.

- If your security policy dictates that you enforce TLS verification between the peers, and if the Expressway-Es are using static NAT, or dual NIC, or both, then we do not recommend using the external interfaces or the static NAT addresses to form the cluster.

  Also, do not try to use the public DNS to map the peers' public FQDNs to their private IP addresses, because you will break external connectivity.

  You should use cluster address mapping in these situations.

How Cluster Address Mapping Works

When you use Fully Qualified Domain Names to form the cluster, peers must be able to translate those names into IP addresses. This translation is the main reason for DNS but, if the peers have no access to DNS, or if you need to translate the FQDN into a private IP address, then you can populate the cluster address mapping table to provide a local alternative to the DNS.

Cluster address mappings are FQDN:IP pairs which are shared around the cluster, one pair for each peer. The peers consult the mapping table before they query DNS and, if they find a match, they do not query DNS.

If you choose to enforce TLS, the peers must also read the names from the SAN field of each other's certificates, and check each name against the FQDN side of the mapping. If the SAN matches the FQDN side of the mapping, and if the IP address that presented the certificate matches the IP side of the mapping, then the peer trusts the other peer and they can establish the TLS connection.

Without using DNS, cluster address mapping is the only way to achieve this verification.

Where Does the Suggested Mapping Come From?

If the cluster is already formed, using IP addresses, and the peers already have a **System host name** and a DNS name configured on the **System** > **DNS** page, then you have the option to automatically populate the cluster address mapping table with assumed mappings as follows:

```
Peer1Hostname.Peer1DNSName maps to <Peer1 Private IP address>

….

Peer6Hostname.Peer6DNSName maps to <Peer6 Private IP address>
```

Note **This automatic mapping may be incorrect!** If the peers' certificates do not contain these assumed FQDNs in their SAN fields, then the cluster will not form when **TLS verification mode** is changed to *Enforce*. You must check that the SANs contain the entries that you place in the peer FQDN fields.

Configure Cluster Address Mapping (Expressway-E Clusters)

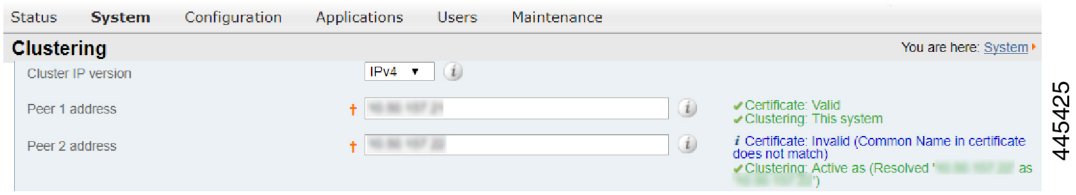
We strongly recommend that you enter the mappings on the primary peer. Address mappings replicate dynamically through the cluster.

The mapping order is unimportant, but if you are using address mappings you must create mappings for every cluster peer, using only **private** IP addresses.

Step 1 Form your cluster using IP addresses (as described in Create a New Cluster of Expressway Peers and Add a Peer to a Cluster) with **TLS verification mode** set to *Permissive*.

Step 2 Verify that the cluster is correctly formed, by checking for green *Clustering* status messages against the peer address fields.

You will also see blue *Certificate: Invalid* ...status messages. This is because your certificates should not correspond with internal/private IP addresses, assuming they are correctly formed to identify peers by FQDN. This is expected behavior and does not prevent you from proceeding.



Cluster IP version: IPv4

Peer 1 address: [redacted]
✓Certificate: Valid
✓Clustering: This system

Peer 2 address: [redacted]
i Certificate: Invalid (Common Name in certificate does not match)
✓Clustering: Active as (Resolved '[redacted]' as '[redacted]')

Step 3 Go to **System** > **Clustering** on the primary peer, and change the **Cluster address mapping enabled** drop-down to *On* (default is *Off*).

The **Cluster address mapping** fields display.

Step 4 [Optional, see note above] Click **Suggest mappings based on system information** to autofill the mapping fields for each cluster peer. This uses the **System host name** and **DNS name** configured on the System > DNS pages of each peer, and maps them to the IP addresses of the inward facing NICs.

Step 5 [If you used the autofill option] Check that the suggested mappings correspond to the names in the peers' certificates, and the IP addresses of the NICs that you want to cluster. (The data is built up from information which may not match the certificate or DNS.)

Step 6 Edit the mappings so that the public FQDNs of the Expressway-E peers correspond to the IP addresses of their internal facing NICs.

(You can check the public FQDNs in the certificate SAN fields, or by querying DNS).

Step 7 Click **Save**.

The mappings are saved and copied to the other cluster peers.

Note The cluster is still formed using IP addresses and is still using the *Permissive* mode of TLS verification. The cluster will start using these mappings when you change the **Peer N address** fields to the public FQDNs and change the **TLS verification mode** to *Enforce*.

Change Cluster to Use FQDNs

This topic describes how to systematically change the peer address, replacing the IP addresses with FQDN. You can change one peer address at a time, across the whole cluster, before moving on to the next address.

To change an Expressway-E cluster to use FQDNs, you use the addresses that are entered in the mapping table (see Cluster Address Mapping for Expressway-E Clusters, on page 1).

Note While you are changing a peer address, communications between peers are temporarily impacted and you will see alarms that persist until the changes are complete and the cluster agrees on the new addresses.

Step 1 Sign in to all the cluster peers and navigate to **System** > **Clustering** on each.

Step 2 Choose which peer address you are going to change first. We recommend starting at **Peer 1 address**, because you need to repeat the following process, one by one, for all peer addresses in the list.

Step 3 On every peer in the cluster:

- Change the chosen peer address field from the IP address to the corresponding FQDN (if you did mappings, they should be replicated in all peers at this stage).
- Click **Save**.

Caution Make sure you only change one peer address on each box.

Step 4 Switch to the peer that is identified by the peer address you are currently changing and restart this peer (go to **Maintenance** > **Restart options**, then click **Restart** and confirm **OK**.

Note A single restart is needed when changing a peer address across all peers.

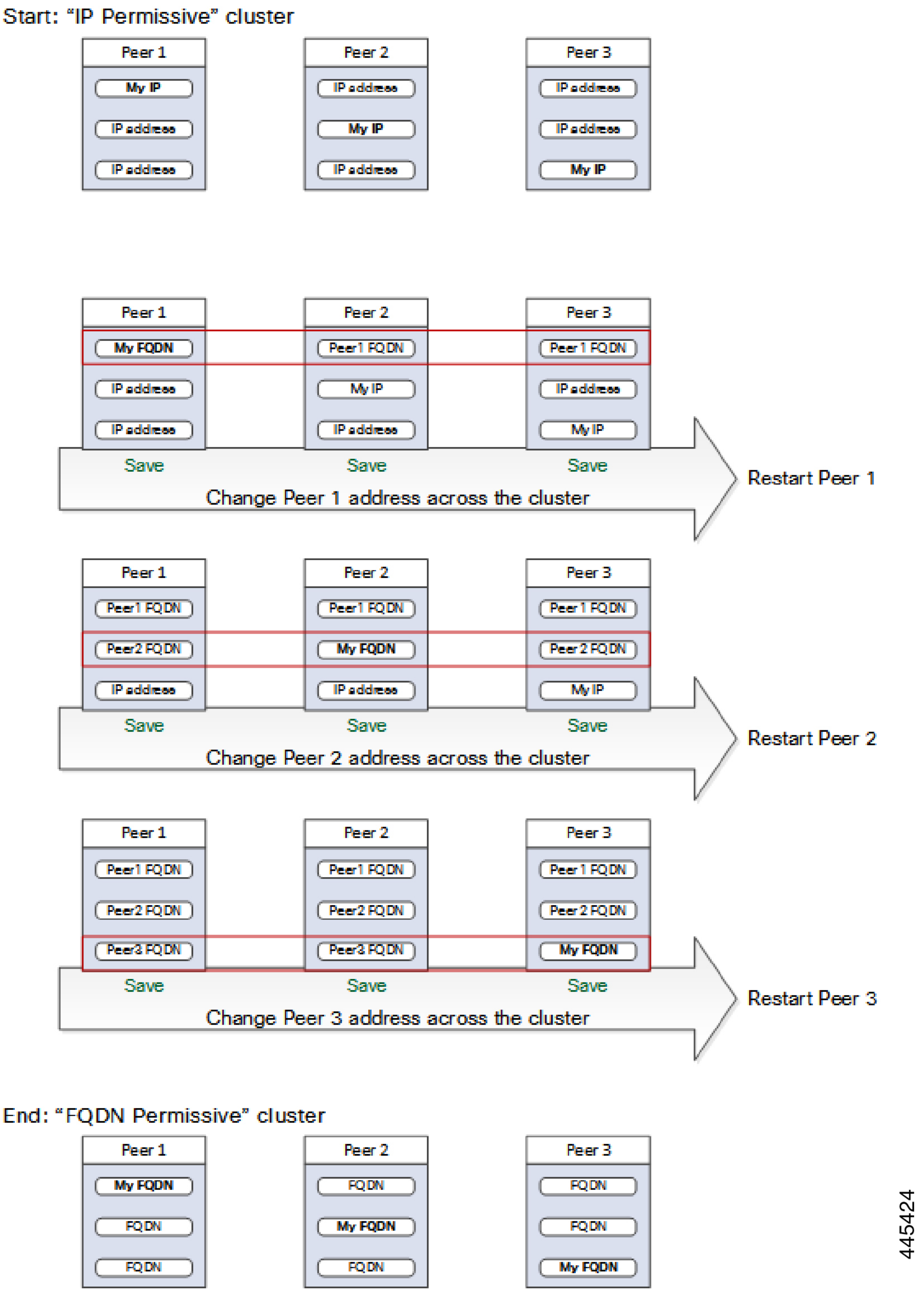
Step 5 Wait for any transient clustering alarms to resolve.

You've successfully changed this peer's clustering address, from an IP address to an FQDN, across the whole cluster.

Step 6 Choose which peer address you are going to change next, and then repeat steps 3-5. Repeat this loop until you have changed all peer addresses and restarted all of the peers.

The whole cluster should now be operating on FQDNs, and the cluster is still in *Permissive* mode.

If the cluster is an Expressway-E cluster, and you are aiming to enforce TLS verification between the peers, then the peer address fields should match the identities presented in the certificates. Check that both *Clustering and Certificate* status messages are green.


Start: "IP Permissive" cluster
Peer 1
My IP
IP address
IP address
Peer 2
IP address
My IP
IP address
Peer 3
IP address
IP address
My IP
Peer 1
My FQDN
IP address
IP address
Peer 2
Peer1 FQDN
My IP
IP address
Peer 3
Peer 1 FQDN
IP address
My IP
Save
Save
Save
Change Peer 1 address across the cluster
Restart Peer 1
Peer 1
Peer1 FQDN
Peer2 FQDN
IP address
Peer 2
Peer1 FQDN
My FQDN
IP address
Peer 3
Peer 1 FQDN
Peer 2 FQDN
My IP
Save
Save
Save
Change Peer 2 address across the cluster
Restart Peer 2
Peer 1
Peer1 FQDN
Peer2 FQDN
Peer3 FQDN
Peer 2
Peer1 FQDN
Peer2 FQDN
Peer3 FQDN
Peer 3
Peer 1 FQDN
Peer 2 FQDN
My FQDN
Save
Save
Save
Change Peer 3 address across the cluster
Restart Peer 3
End: "FQDN Permissive" cluster
Peer 1
My FQDN
FQDN
FQDN
Peer 2
FQDN
My FQDN
FQDN
Peer 3
FQDN
FQDN
My FQDN
445424

Enforce TLS Verification

Before You Begin

⚠

Caution Verify that your certificate SANs contain the FQDNs that are in the Peer N address fields. You should see green status messages for clustering and certificate next to each address field before you proceed.

Process to Enforce TLS Verification

Step 1 On the primary peer, set **TLS verification mode** to *Enforce*.

Caution A warning will display if any certificates are invalid and will prevent the cluster working properly in enforced TLS verification mode.

The new TLS verification mode replicates throughout the cluster.

Step 2 Verify that **TLS verification mode** is now Enforce on each other peer.

Step 3 Click **Save** and restart the primary peer.

Step 4 Sign in to each other peer and then restart the peer.

Step 5 Wait for the cluster to stabilize, and check that Clustering and Certificate status is green for all peers.

Usage Note for Expressway-E Traversal Zones

This point is about operational usage rather than initial setup, but is provided here for convenience. Be aware that the FQDN of the Expressway-C cluster will need to be configured in the TLS verify subject name field of the Expressway-E traversal zone. Expressway uses the SAN attribute (Subject Alternate Name) to validate the received certificate, not the CN (Common Name).