Backup, Restore, Recovery, and Delete

This chapter provides information about backup, restore, recovery, and delete mechanisms for IWAN on APIC-EM:

Backup and Restore for IWAN on APIC-EM

Backup and restore will work in the following scenarios:

- The controller is at stasis with respect to IWAN application business intent. Stasis is the state of the system when IWAN application business intent has succeeded or failed.
- IWAN application business intent has not been initiated between backup and restore.
- Site status is in success or failure state, with no site recovery in progress.
- No scheduled jobs are active in the same period.

Backup and restore will not work in the following scenarios:

- IWAN application is handling IWAN application business intent, including internal database operations and device policy updates.
- Workflows performed on IWAN application, when backup and restore session is underway, will be lost and cannot be tracked or retrieved later:
  - Sites (one or more devices) are added to IWAN
  - Devices that had their certificates renewed
  - Sites that are deleted from IWAN or have their certificates revoked
  - Configuration or policy updates

Recommendations

Cisco recommends the following for the proper working of backup and restore:

- Run in multi-host mode as far as possible. This enables active HA thereby reducing the backup and recovery windows.
- Perform a backup everyday to maintain a current version of your database and files.

- Perform a backup and restore after you initiate changes in the system, basically after a stasis period.
- Do not use backup and restore to undo any intent that you performed earlier. Use workflows supported in the application to accomplish intent.
- Track devices that are added to IWAN or have their certificates updated.
- Track devices that are deleted from IWAN or have their certificates revoked.

Caveats and Workarounds

There is a risk in this version of APIC-EM, in which the controller and the network will be out of sync after a restore and consequentially some or all sites may be out of policy (as displayed on the Site Status screen). Some out of policy situations, such as security related issues, may not be detected.

For workflows mentioned above, the following workarounds is recommended:

Sites (one or more devices) are added to IWAN

Remove the PKI trustpoint and zero-out the keys on each device. Use the following commands to clear trustpoints and certificates on each device:

no crypto pki trustpoint sdn-network-infra-iwan

crypto key zeroize rsa sdn-network-infra-iwan

Restart the plug and play (PnP) workflow to allow the device to show as an unclaimed device in the IWAN application. If the device is already added as an IWAN site, copy the startup configuration to the running configuration and reload the router on each affected router. Following, this, the PnP call home workflow takes over and the device shows up as an unclaimed device in the IWAN workflow. The IWAN site provisioning must be reapplied. Repeat the IWAN site creation workflow.

Device that had their certificate renewed

Remove the PKI trustpoint and zero-out the keys on each device . Use the following commands to clear trustpoints and certificates on each device:

no crypto pki trustpoint sdn-network-infra-iwan

crypto key zeroize rsa sdn-network-infra-iwan

Repeat the IWAN site creation workflow for the device or set of devices.

Note When a device is provisioned by IWAN, it is provided with a certificate to prove its identity. This certificate is valid for one year. When eighty percent of the certificate lifetime expires, the device will automatically attempt to renew this certificate. As it is difficult to track devices and their certificate status, Cisco will provide an API, to determine devices with expired client ID certificates or devices with client ID certificates that will expire soon. If devices renew certificates between a backup and a restore, the database certificate displays that the device has not been renewed after completion of the restore session. These API's will provide a method to determine the devices that need to renew certificates or reprovision the expiring or expired client ID certificates respectively. After a device's client ID certificate has expired, the only option is to reprovision it.

Sites that are deleted from IWAN or have their certificates revoked

Revoke the certificate for each device via the controller user interface. If the site is a part of the IWAN network, the **Site Delete** button can be used to revoke the certificate and clear the IWAN application for that site.

Configuration or policy updates

Cisco IWAN Application can detect changes on devices that are in conflict with the controller. If updates made to a site between a backup and a restore, the site is removed from the policy. It is recommended that you reapply the same set of changes that were previously applied. However, the success rate of this approach depends on the nature of the change. If the site is removed from the policy, manual intervention is required. This is because the controller is no longer in charge for removing policy from the sites unless the manual changes are successful.

Note It is recommended that the audit log entries for adding and deleting devices along with the status of their certificates (revoked or created) be tracked automatically via using an automated script. This script can be useful when restoring a nonstatis system. All audit records are useful in when reapplying the changes lost due to system instability. This automated script must run at regular intervals after backup is complete to prepare the system for restore.

Recovery for IWAN Devices

Use the **Recovery** icon to recover a site after when site provisioning fails. After a attempting to recover a site, if site recovery is a success, the site moves to the Success state, else the **Recovery** icon reappears allowing you to retry recovering the site. An attempt will be made to push the last change that was made.

You can attempt to recover a site multiple times. If site is cannot be recovered the only option is to delete the site.

Recovery Mechanism for Hub and Branch Sites

Step 1 Navigate to the Site Status page and click the **Recovery** icon .

The **Recovery** icon is displayed in the Recovery column.

Step 2 If recovery succeeds, you can start provisioning the hub and the **Recover** icon is grayed out until next failure.

Post Provisioning Recovery Mechanisms for Hub and Branch Sites

Post provisioning recovery of the hub and branch sites after the sites have been provisioned allows for the last change set to be reapplied. means retrying the last change set for the hub and spoke devices.

- In case of hub device, recovery can be attempted several times. The **Recovery** button appears on the Main Landing page.
- In case of site device, recovery can be attempted multiple times. The **Recovery** button appears on the Sites Landing page. If recovery fails after multiple attempts, you can choose to delete the site by clicking on the **Delete** icon against the **Site Delete** column to remove site permanently.

Deleting Sites

In addition to recovering hub and branch sites, you can also delete sites in IWAN via the **Delete Site** icon in the Sites Listing page.

Deleting a Hub Site

You can delete a primary hub if the primary hub is in failed state and no branch sites have been provisioned. A primary hub cannot be deleted after branch sites have been provisioned. The **Delete Site** icon is disabled thereby disallowing you to delete the hub. When you delete the primary hub, the transit POP are also deleted. The configuration on the primary hub is reset to brownfield validation state.

When a hub is deleted after hub provisioning fails, IWAN performs the following:

- PKI certificate and trustpoint is revoked
- IP addresses are released to the IP address pool
- Hub is deleted from inventory

If the delete operation succeeds, the primary hub is removed from Site Listings page. You can reprovision the primary hub via the main page as part of the hub provisioning. If the delete operation fails, the following message is displayed and you can reprovision hub again.

```
Unable to revert configuration on devices. Please restore site manually before
re-provisioning.
```

Deleting Transit POPs (Datacenters)

You can delete a transit POP (datacenter) irrespective of the datacenter state—provisioned or failed.

When a POP site is deleted, IWAN performs the following:

- Revoke PKI certificate and trustpoint from all devices in pops.
- Release IP addresses to IP address pool.
- Delete POPs from inventory.
- Clean the Network and Wireless Services (NWS) state.

If the delete operation succeeds, the transit pop is removed from IWAN and the devices are cleaned. If the delete operation fails, which might happen when a device is cannot be reached on a network, the following message appears and the states of the pops is deleted. You must reprovision the transit pops.

```
Unable to revert configuration on devices. Please restore site manually before
re-provisioning.
```

Deleting Branch Sites

You can delete branch sites from IWAN irrespective of the branch state—provisioned or failed—via the **Delete Site** icon in the Sites Listing page. As a part of the Multilink feature, you can delete branch sites either from the “IWAN Aggregation Site” tab or from the “Select Topology” tab.

Note Deleting branch sites must be performed on a best effort basis when devices cannot be reverted to greenfield validation. After deleting a branch site, the device must be cleaned manually.

When a branch site is deleted, IWAN performs the following:

- The initial configuration is saved to the **bootflash:IWAN_RECOVERY.cfg** file on device.
- The site is recovered to bootstrap configuration by performing the following:
  - Copying the **boothflash:recovery.cfg** file information to startup configuration
  - Reloading the device
- PKI certificate and trustpoint is revoked.
- IP addresses are released to the IP address pool.
- The site information is cleaned in the database.

When the delete operation succeeds, the branch site is removed from the Sites Listing page and is displayed in the unclaimed device list thereby allowing you to reprovision the branch site. If delete fails, the branch site is not added to the unclaimed device list and displays the following message

```
Unable to revert configuration on devices. Please restore site manually before
re-provisioning.
```