Backup and Restore, Recovery, and Delete

This chapter contains the following sections:

Backup and Restore

Backup and Restore Recommendations

We recommend the following for the proper working of backup and restore:

- Run in multihost mode. This enables active high availability (HA) thereby reducing the backup and recovery windows.
- Before you use the devices to provision the site, we recommend that you save the running configuration in bootflash in the IWAN_RECOVERY.cfg file so that the configuration can be restored if needed.
- If a site is deleted, the routers are reloaded with the configuration that is saved in the IWAN_RECOVERY.cfg file.
- Perform a backup every day to maintain a current version of your database and files.
- Perform a backup and restore after you initiate changes in the system.
- 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 Cisco IWAN or have their certificates updated.
- Track devices that are deleted from Cisco IWAN or have their certificates revoked.

Backup and Restore Scenarios

Backup and restore *works* in the following scenarios:

- The controller is in a stable state with respect to IWAN app business intent.
- Cisco 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 *does not work* in the following scenarios:

- Cisco IWAN is handling application business intent, which includes internal database operations and device policy updates.
- There is a risk in Cisco APIC-EM where the controller and the network is out of sync after a restore and consequentially some or all sites might be out of policy (as displayed on the Site Status screen). Some out of policy situations, such as security related issues might not be detected.
- Workflows performed on the Cisco IWAN application during the backup and restore operation, will be lost and cannot be tracked or retrieved. The following table shows workflow scenarios with possible workarounds:

Table 9-1 Workflow Scenarios Where Backup and Restore Fails With Workaround

Scenario	Workaround

Sites (one or more devices) added to IWAN during the backup and restore operation.	1. 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`
	2. Restart the Plug-n-Play workflow. This displays the device as an unclaimed device in the Cisco IWAN app.
	3. If the device is already added as a site, copy the startup configuration to the running configuration and reload the router on each affected router. The PnP call home workflow takes over and the device appears as an unclaimed device in the workflow.
	4. Reapply site provisioning.
	5. Repeat the site creation workflow.

Devices that had their certificates renewed during the backup and restore operation.	1. Remove the PKI trustpoint and zero out the keys on each device.
	2. 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`
	3. Repeat the site creation workflow for the device or set of devices.
	When a device is provisioned by the Cisco IWAN application, 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 automatically attempts to renew the certificate.
	If the devices try to renew their certificates between a backup and a restore, the database displays that the certificate has not been renewed.
	Because it is difficult to track devices and their certificate status, Cisco provides an API to determine the devices whose client ID certificates have expired; and devices whose client ID certificates are going to expire soon.
	After a device's client ID certificate expires, the only option is to re-provision it.

Table 9-1 Workflow Scenarios Where Backup and Restore Fails With Workaround

Scenario	Workaround
Sites that are deleted from Cisco IWAN or have their certificates revoked during the backup and restore operation.	Do one of the following: • Revoke the certificate for each device using the controller's user interface. • If the site is part of a network, from the **Actions** column in the Site Status page, click the **X** icon to revoke the certificate and clear the application for that site.
Configuration or policy updates during the backup and restore operation.	The Cisco IWAN application can detect changes on devices that are in conflict with the controller. If updates are made to a site between a backup and a restore, the site is removed from the policy. We recommend 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 the policy from the sites unless the manual changes are successful. **Note** We recommend that use an automated script, which automatically tracks the audit log entries for adding and deleting devices along with the status of their certificates (revoked or created). This script is useful when restoring an unstable system. The audit records are also useful when reapplying the changes lost due to system instability. Run the automated script at regular intervals after backup is complete to prepare the system for restore.

Recovery

Recovering a Cisco IWAN Site

Use this procedure to recover a site when site provisioning fails.

Step 1 From the Cisco IWAN home page, click **Manage Branch Sites**. The Sites page opens.

Step 2 Click the **Site(s)** tab. From the **Action** column in the Site Status page, click the **Recovery** icon.

After attempting to recover a site, if the site recovery is a success, the site moves to the Success state, otherwise the **Recovery** icon appears again allowing you to retry recovering the site.

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

Post Provisioning Recovery for Hub and Branch Sites

The post provisioning recovery feature allows you to reapply the last change to the hub and spoke devices after the sites have been provisioned.

Recovery can be attempted multiple times. To recover a hub or a branch site, click the **Recovery** icon in the **Action** column in the Site Status page.

If recovery fails after multiple attempts, you can choose to delete the site permanently by clicking the delete **X** icon in the **Action** column in the Site Status page.

Delete

Deleting a Hub Site

You can delete a primary hub if the primary hub is in a failed state and no branch sites have been provisioned.

If both the primary hub and transit hub are in failed state, you must delete the transit hub first in order to delete the primary hub. If the delete operation succeeds, both the primary hub and transit hub are reset to the brownfield validation state.

When a hub is deleted after hub provisioning fails, the Cisco IWAN application does the following:

- Revokes the PKI certificate and trustpoint.
- Releases the IP addresses to the IP address pool.
- Deletes the hub from the inventory.

If the delete operation succeeds, the hub is removed from **Sites** page.

Note The hub site is deleted on a best-effort basis. If the devices are unreachable, they are not restored to the original configuration. In this case, you must manually clean up the configuration on the devices. See Manually Cleaning Up Devices, page 9-6.

You can re-provision the hub from the Configure Hub Site page as part of the hub provisioning (see Wizard Step 5—Configuring the IWAN Aggregation Site, page 4-12.

Deleting a Transit Hub

You can delete a transit hub irrespective of the state of the transit hub—whether it is provisioned or failed.

When a transit hub is deleted, IWAN performs the following:

- Revokes the PKI certificate and trustpoint from all devices in the transit hub.
- Releases the IP addresses to the IP address pool.
- Deletes the transit hub from inventory.
- Cleans the Network and Wireless Services (NWS) state.

If the delete operation succeeds, the transit hub is removed from the **Sites** page.

Note The transit-hub site is deleted on a best-effort basis. If the devices are unreachable, they are not restored to the original configuration. In this case, you must manually clean up the configuration on the devices. See Manually Cleaning Up Devices, page 9-6.

Deleting Branch Sites

You can delete branch sites from IWAN irrespective of the branch state—in progress, provisioned, or failed.

Procedure

Step 1 From the Cisco IWAN home page, click **Manage Branch Sites**. The Sites page opens.

Step 2 Click the **Site(s)** tab. From the **Action** column in the Site Status page, click the **X** icon to delete the site.

Note Branch sites are deleted on a best-effort basis. If the devices are unreachable, they are not restored to the bootstrap configuration. In this case, you must manually clean up the configuration on the devices. See Manually Cleaning Up Devices, page 9-6.

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

- Revokes the PKI certificates and trust points.
- Releases the IP addresses from IP address pools.
- Cleans the site information from the database.
- Does the following to try to revert the routers of the deleted site to the bootstrap configuration file: IWAN_RECOVERY.cfg. Does the following:
  - Copies the IWAN_RECOVERY.cfg to the startup configuration.
  - Reloads the device.

See Backup and Restore, page 9-1.

After the site is deleted, the branch devices are removed from the **Devices** tab and are displayed in the unclaimed device list, thereby, allowing you to re-provision the branch site.

Manually Cleaning Up Devices

After a hub site, transit-hub site, or branch site delete operation, the devices in the site are deleted on the best-effort basis. If the devices are unreachable, they are not restored to the original configuration. In this case, you must manually clean up the configuration on the devices.

Use this procedure to manually clean up the configuration on the devices.

Procedure

Step 1 Remove the IWAN PKI trust point. Use the following command:

no crypto pki trustpoint sdn-network-infra-iwan

Step 2 Remove the IWAN RSA key from NVRAM. Use the following commands:

crypto key zeroize rsa sdn-network-infra-iwan

write erase

Step 3 Restore the original configuration. Use the following commands:

config replace bootflash:<original-config-file> force

write

Example:

```
RPRE-GA-1-HUB-INET# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
PRE-GA-1-HUB-INET(config)# no crypto pki trustpoint sdn-network-infra-iwan
% Removing an enrolled trustpoint will destroy all certificates
 received from the related Certificate Authority.

Are you sure you want to do this? [yes/no]: yes
% Be sure to ask the CA administrator to revoke your certificates.

PRE-GA-1-HUB-INET(config)# crypto key zeroize rsa sdn-network-infra-iwan
Do you really want to remove these keys? [yes/no]: yes
PRE-GA-1-HUB-INET(config)# end
PRE-GA-1-HUB-INET# write erase
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
PRE-GA-1-HUB-INET# config replace bootflash:clean-config force
%EIGRP: Deleting base topology is not allowed.
% Interface GigabitEthernet0/0/4 IPv4 disabled and address(es) removed due to enabling VRF
IWAN-TRANSPORT-2% Profile is applied to Tunnel11-head-0 (head) and possibly other crypto
maps
% No such key-chain% Profile is applied to Tunnel11-head-0 (head) and possibly other
crypto maps% Profile is applied to Tunnel11-head-0 (head) and possibly other crypto maps%
Profile is applied to Tunnel11-head-0 (head) and possibly other crypto maps% Profile is
applied to Tunnel11-head-0 (head) and possibly other crypto maps
The rollback configlet from the last pass is listed below:
********
!List of Rollback Commands:
no crypto ikev2 profile FVRF-IKEv2-IWAN-TRANSPORT-2
end
********


Rollback aborted after 5 passes
PRE-GA-1-HUB-INET# write
```

Adding or Deleting Site Prefixes

You can add or delete site prefixes after hub provisioning.

Note This option is only available for L3 brownfield sites.

Procedure

Step 1 From the Cisco IWAN home page, click **Manage Branch Sites**. The Sites page opens.

Step 2 Click the **Site(s)** tab. From the **Action** column in the Site Status page, click the **Update Site Prefix** (pen) icon. The LAN Site Prefix dialog box opens.

Step 3 To add a site prefix, click the **+** icon.

Step 4 To delete a site prefix, select the check box next to the prefix that you want to delete, and then click the **X** icon.

Note You cannot delete all prefixes. You must have at least one prefix per site.

Step 5 Click **Apply Changes**.