CHAPTER 9

バックアップと復元、リカバリ、および削除

この章の内容は、次のとおりです。

バックアップと復元

バックアップと復元に関する推奨事項

バックアップと復元を適切に機能させるために、以下を推奨しています。

- マルチホスト モードで実行する。これによりアクティブな高可用性（HA）が有効になるので、バックアップやリカバリの時間が短縮されます。
- サイトのプロビジョニングにデバイスを使用する前に、必要に応じて設定を復元できるように、実行中の設定を IWAN_RECOVERY.cfg ファイルとしてブートフラッシュに保存することを推奨します。
- サイトを削除した場合は、IWAN_RECOVERY.cfg ファイルに保存されている設定と共にルータをリロードする。
- 毎日バックアップを実行して、データベースとファイルの現在のバージョンを維持する。
- システムで変更を開始した後に、バックアップと復元を実行する。
- 前に実行した目的（インテント）を取り消すためにバックアップと復元を使用しない。アプリケーションでサポートされているワークフローを使用して、目的を遂行してください。
- Cisco IWAN に追加された（または証明書が更新された）デバイスを追跡する。
- Cisco IWAN から削除された（または証明書が取り消された）デバイスを追跡する。

バックアップと復元のシナリオ

バックアップと復元は以下の状況で*機能*します。

- IWAN アプリの機能的役割に対してコントローラが安定した状態である。
- バックアップから復元までの間に Cisco IWAN アプリケーションの機能的役割が実行されていない。
- サイトのステータスが成功または失敗になっており、サイト リカバリが進行していない。
- 同じ期間中に、アクティブになっているスケジュール済みジョブがない。

バックアップと復元は以下の状況では*機能しません*。

- Cisco IWAN が、内部データベースの操作やデバイス ポリシーの更新など、アプリケーションの機能的役割を遂行している。
- Cisco APIC-EM にはリスクがあります。復元後にコントローラとネットワークが同期しなくなり、その結果、一部またはすべてのサイトがポリシー違反状態になる場合があります（[Site Status] 画面に表示）。セキュリティ関連の問題など、一部のポリシー違反の状況は検出されないことがあります。
- バックアップと復元の操作中に Cisco IWAN アプリケーションで実行されたワークフローが失われ、追跡することも回復することもできない。次の表は、ワークフロー シナリオと可能な回避策を示しています。

表 9-1　バックアップと復元に失敗したワークフロー シナリオと回避策

シナリオ	回避策

バックアップと復元の操作中に IWAN に追加されたサイト（1 つ以上のデバイス）。	1. PKI トラストポイントを削除し、各デバイスのキーをゼロに設定します。次のコマンドを使用して、各デバイスのトラストポイントと証明書をクリアします。
	`no crypto pki trustpoint sdn-network-infra-iwan`
	`crypto key zeroize rsa sdn-network-infra-iwan`
	2. プラグアンドプレイ ワークフローを再開します。これにより、デバイスは要求されていないデバイスとして Cisco IWAN アプリに表示されます。
	3. デバイスがサイトとしてすでに追加されている場合は、スタートアップ コンフィギュレーションを実行コンフィギュレーションにコピーし、影響を受ける各ルータにそのルータをリロードします。PnP コール ホーム ワークフローが後を引き継ぎ、デバイスは要求されていないデバイスとしてワークフローに表示されます。
	4. サイト プロビジョニングを再適用します。
	5. 作成ワーク フローを繰り返します。

表 9-1　バックアップと復元に失敗したワークフロー シナリオと回避策（続き）

シナリオ	回避策

バックアップと復元の操作中に証明書が更新されたデバイス。	1. PKI トラストポイントを削除し、各デバイスのキーをゼロに設定します。
	2. 次のコマンドを使用して、各デバイスのトラストポイントと証明書をクリアします。
	`no crypto pki trustpoint sdn-network-infra-iwan`
	`crypto key zeroize rsa sdn-network-infra-iwan`
	3. デバイスまたは一連のデバイスに対してサイト作成ワーク フローを繰り返します。
	デバイスが Cisco IWAN でプロビジョニングされると、身元を証明する証明書がデバイスに提供されます。この証明書の有効期間は 1 年です。証明書の有効期間の 80 パーセントが経過すると、デバイスは証明書の自動更新を試みます。
	バックアップと復元の間にデバイスが証明書の更新を試みた場合、データベースには証明書が未更新であると表示されます。
	デバイスとその証明書のステータスを追跡することは困難であるため、シスコでは、クライアント ID 証明書が失効したデバイスや間もなく期限切れになるデバイスを特定する API を提供しています。
	デバイスのクライアント ID 証明書が失効した後は、デバイスの再プロビジョニングが唯一の手段になります。

バックアップと復元の操作中に Cisco IWAN から削除されたサイト、または証明書が取り消されたサイト。	次のいずれかを実行します。 • コントローラのユーザ インターフェイスを介して各デバイスの証明書を取り消します。 • サイトがネットワークの一部の場合は、[Site Status] ページの [Actions] 列で [X] アイコンをクリックし、サイトの証明書を取り消してアプリケーションをクリアします。
バックアップと復元の操作中に設定またはポリシーを更新。	Cisco IWAN アプリケーションは、コントローラと競合するデバイスでの変更を検出できます。バックアップと復元の間にサイトに更新が加えられた場合、そのサイトはポリシーから削除されます。以前に適用されたものと同じ変更セットを再適用することを推奨します。ただし、このアプローチが成功する割合は変更の性質に応じて異なります。サイトをポリシーから削除する場合は、手動による操作が必要です。手動による変更が成功しない限り、コントローラはサイトからのポリシーの削除を管理しないからです。 （注）　自動化スクリプトを使用することをお勧めします。このスクリプトは、証明書のステータス（取り消しまたは作成）とともに、デバイスの追加と削除に関する監査ログ エントリを自動的に追跡します。このスクリプトは、不安定なシステムを回復させる場合に役立ちます。監査レコードは、システムの不安定さにより失われた変更を再適用する場合にも役立ちます。システムを復元する準備として、バックアップの完了後にこの自動スクリプトを定期的に実行してください。

回復

Cisco IWAN サイトのリカバリ

サイトのプロビジョニングに失敗した場合は、次の手順でサイトをリカバリします。

手順 1　Cisco IWAN のホームページで、[Manage Branch Sites] をクリックします。[Sites] ページが開きます。

手順 2　[Site(s)] タブをクリックします。[Site Status] ページの [Action] 列で、[Recovery] アイコンをクリックします。

サイトのリカバリを試みて成功した場合は、サイトのステータスが [Success] に変わります。成功しなかった場合は [Recovery] アイコンが再び表示され、サイトのリカバリを再度試みることができます。

サイトのリカバリは何度も試行できます。ただし、サイトをリカバリできない場合は、サイトを削除することが唯一の選択肢となります。

ハブ サイトおよびブランチ サイトのポストプロビジョニング リカバリ

ポストプロビジョニング リカバリ機能を使用すると、サイトのプロビジョニング後にハブとスポーク デバイスに最後の変更を再適用できます。

リカバリは何度も試行できます。ハブまたはブランチ サイトをリカバリするには、[Site Status] ページの [Action] 列で [Recovery] アイコンをクリックします。

リカバリを複数回試みて失敗した場合は、削除 [X] アイコン（[Site Status] ページの [Action] 列）をクリックすることにより、サイトを完全に削除することもできます。

サイトとデバイスの削除

ハブ サイトの削除

プライマリ ハブが障害状態にあり、どのブランチ サイトもプロビジョニングされていない場合は、プライマリ ハブを削除できます。

プライマリ ハブと中継ハブの両方が障害状態の場合に、プライマリ ハブを削除するには、最初に中継ハブを削除する必要があります。削除操作が成功すると、プライマリ ハブと中継ハブの両方がブラウンフィールド検証状態にリセットされます。

ハブのプロビジョニングに失敗した後にハブを削除した場合は、Cisco IWAN アプリケーションにより以下が実行されます。

- PKI 証明書とトラストポイントが取り消される。
- IP アドレスが IP アドレス プールにリリースされる。
- インベントリからハブが削除される。

削除操作が成功すると、ハブは [Sites] ページから削除されます。

(注)　ハブ サイトはベスト エフォート方式で削除されます。デバイスが正常にプロビジョニングされた場合やデバイスが到達不能の場合、元の設定に復元されません。その場合は、デバイスの設定を手動でクリーンアップする必要があります。手動によるデバイスのクリーンアップ（9-6 ページ）を参照してください。

ハブのプロビジョニングの一環として、[Configure Hub Site] ページからハブを再プロビジョニングできます（IWAN 集約サイトの設定（4-16 ページ）を参照）。

中継ハブ サイトの削除

中継ハブの状態（プロビジョニング済みまたは失敗）に関係なく、中継ハブを削除できます。

中継ハブを削除すると、IWAN により以下が実行されます。

- 中継ハブのすべてのデバイスの PKI 証明書とトラストポイントが取り消される。
- IP アドレスが IP アドレス プールにリリースされる。
- インベントリから中継ハブが削除される。
- Network and Wireless Services（NWS）状態が解消される

削除操作が成功すると、中継ハブは [Sites] ページから削除されます。

(注)　中継ハブ サイトはベスト エフォート方式で削除されます。デバイスに到達できない場合、デバイスは元の設定に復元されません。その場合は、デバイスの設定を手動でクリーンアップする必要があります。手動によるデバイスのクリーンアップ（9-6 ページ）を参照してください。

ブランチ サイトの削除

ブランチの状態（進行中、プロビジョニング済み、または失敗）に関係なく、IWAN からブランチ サイトを削除できます。

手順

手順 1　Cisco IWAN のホームページで、[Manage Branch Sites] をクリックします。[Sites] ページが開きます。

手順 2　[Site(s)] タブをクリックします。[Site Status] ページの [Action] 列で、[X] アイコンをクリックしてサイトを削除します。

(注)　ブランチ サイトはベスト エフォート方式で削除されます。デバイスに到達できない場合、デバイスはブートストラップ コンフィギュレーションに復元されません。その場合は、デバイスの設定を手動でクリーンアップする必要があります。手動によるデバイスのクリーンアップ（9-6 ページ）を参照してください。

ブランチ サイトを削除すると、Cisco IWAN アプリケーションにより以下が実行されます。

- PKI 証明書とトラストポイントが取り消される。
- IP アドレスが IP アドレス プールからリリースされる。
- データベースからサイト情報が消去される。
- 削除したサイトのルータをブートストラップ コンフィギュレーション ファイル（IWAN_RECOVERY.cfg）に戻すには、以下を実行します。
  - IWAN_RECOVERY.cfg をスタートアップ コンフィギュレーションにコピーします。
  - デバイスがリロードされます。

バックアップと復元（9-1 ページ）を参照してください。

サイトを削除すると、ブランチ デバイスが [Devices] タブから削除され、要求されていないデバイスのリストに表示されるので、ブランチ サイトを再プロビジョニングできます。

ハブ デバイスの削除

1 つの POP に 3 つ以上のハブ デバイスがある場合、デバイスが 2 つになるまで、プライマリ POP または中継 POP 内の個々のハブ デバイスを削除できます。ハブ デバイスには WAN リンクのみと接続しているブランチがあってはなりません。

以前に正常にプロビジョニングされたハブ デバイスが削除される場合、元の設定に復元されません。この場合、デバイス上で設定を手動でクリーンアップして（手動によるデバイスのクリーンアップ（9-6 ページ）を参照）、元の設定を復元する必要があります。

手動によるデバイスのクリーンアップ

ハブ サイト、中継ハブ サイト、またはブランチ サイトを削除すると、そのサイトのデバイスがベスト エフォート方式で削除されます。デバイスに到達できない場合、デバイスは元の設定に復元されません。その場合は、デバイスの設定を手動でクリーンアップする必要があります。

デバイスの設定を手動でクリーンアップするには、次の手順を実行します。

手順

手順 1　IWAN PKI トラストポイントを削除します。次のコマンドを使用します。

no crypto pki trustpoint sdn-network-infra-iwan

手順 2　NVRAM から IWAN RSA キーを削除します。次のコマンドを使用します。

crypto key zeroize rsa sdn-network-infra-iwan

write erase

手順 3　元の設定を復元します。次のコマンドを使用します。

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

write

例：

```
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
```

サイト プレフィックスの追加または削除

ハブのプロビジョニング後に、サイト プレフィックスを追加または削除できます。

(注)　このオプションは、L3 ブラウンフィールド サイトでのみ使用できます。

手順

手順 1　Cisco IWAN のホームページで、[Manage Branch Sites] をクリックします。[Sites] ページが開きます。

手順 2　[Site(s)] タブをクリックします。[Site Status] ページの [Action] 列で、[Update Site Prefix]（ペン）アイコンをクリックします。[LAN Site Prefix] ダイアログボックスが開きます。

手順 3　サイト プレフィックスを追加するには、[+] アイコンをクリックします。

手順 4　サイト プレフィックスを削除するには、削除するプレフィックスの横にあるチェックボックスをオンにして、[X] アイコンをクリックします。

（注）　すべてのプレフィックスを削除することはできません。サイトごとに少なくとも 1 つのプレフィックスが必要です。

手順 5　[Apply Changes] をクリックします。