

AD-キャンパス6.2

自動化構成ガイド

2023Copyright©New H3C Technologies Co.,Ltd. All rights reserved.

本書のいかなる部分も、New H3C Technologies Co.,Ltd.の事前の書面による同意なしに、いかなる形式または手段によっても複製または送信することはできません。

New H3C Technologies Co.,Ltd.の商標を除き、本書に記載されているすべての商標は、それぞれの所有者の所有物です。

本書の内容は、予告なしに変更されることがあります。

内容

制限事項およびガイドライン	3
概要	6
デバイスモデルと役割のマトリックス	6
ネットワークアーキテクチャの設計	6
3 層アーキテクチャ	6
2 層アーキテクチャ	7
シングルリーフアーキテクチャ	8
アンダーレイネットワークとコントローラー間の接続モード	9
導入ワークフローの自動化	9
工場出荷時のデフォルト設定の復元とデバイスの再起動	11
自動化パラメーターの構成	12
ネットワークリソースと IP アドレスの計画	12
SeerEngine-個別のネットワークアダプタを使用するキャンパスコントローラーと統合プラットフォーム(推奨)	12
SeerEngine-同じネットワークアダプタを使用するキャンパスコントローラーと統合プラットフォーム	13
ユーザーVLAN の計画	15
3 層または 2 層のアーキテクチャ導入の準備	17
L3 スイッチの設定	17
コントローラーの設定	18
シングルリーフアーキテクチャ導入の準備	30
L3 スイッチの設定	30
リーフデバイス用の IRF スタッキングの設定	30
コントローラーの設定	30
自動オンボーディング	32
単一のスパインデバイスのオンボード	32
工場出荷時のデフォルト設定でのスパインデバイスの起動	32
スパインデバイスの自動設定	32
AC インターフェースの自動設定	33
スパインデバイスでの展開結果の確認	33
コントローラーでのスパインの展開の確認	34
構成の完全なデプロイメント	35
スパイン IRF ファブリックのオンボード	36
Spine IRF 展開の制限事項とガイドライン	36
スパインデバイスとリーフデバイス間の複数のリンク	38
シングルリーフデバイスのオンボード	38
工場出荷時のデフォルト設定でのリーフデバイスの再起動	38
リーフインターフェースの自動設定	39
展開結果の確認	40
複数のリーフデバイスのオンボード	42
リーフ IRF ファブリックのオンボード	42
Leaf IRF 展開の制限事項とガイドライン	42
冗長なスパインリーフリンクを追加する	44
冗長リーフアクセスリンクの追加	44
1 台のアクセスデバイスのオンボード	45
工場出荷時のデフォルト設定でのリーフデバイスの再起動	45
アクセスデバイスの自動設定	46
アクセスデバイスでの展開結果の確認	46
コントローラーでのアクセス展開の確認	47
アクセス IRF ファブリックのオンボード	47
アクセス IRF ファブリックの展開	47

自動リーフアクセスリンク集約.....	49
複数階層のアクセスデバイスの導入	49
工場出荷時のデフォルト設定での下位層アクセスデバイスの再起動	49
展開の確認.....	50
自動化された IPv6 導入	51
ソフトウェアのアップグレード	51
故障したデバイスの交換.....	55
付録.....	56
スパン自動化テンプレート.....	56
リーフ自動化テンプレート.....	60
Access オートメーションテンプレート	64
O&M モニタリング	67

制限事項およびガイドライン

アンダーレイの自動展開を成功させるには、次の情報をよく読み、記載されている制限、要件、およびガイドラインに従ってください。

ライセンスと DHCP サーバーの要件

- 自動化はライセンスベースです。この機能を使用するには、必要なライセンスを Unified Platform およびコントローラーにインストールする必要があります。
- vDHCP サーバーを正しくセットアップします。これは、自動デバイスオンボーディング中に必要です。

ユーザー名とパスワードの要件

- デバイス設定テンプレートとデバイスコントロールプロトコルテンプレートでは、異なるユーザー名を使用できます。ユーザー名が同じ場合、パスワードも同じである必要があります。デバイス設定テンプレートのユーザー名とパスワードは、リーフデバイスへのスパインデバイスアクセスに使用されます。デバイスコントロールプロトコルテンプレートのユーザー名とパスワードは、デバイスにアクセスするためにコントローラーによって使用されます。
- 自動配置の配置自動化テンプレート内のパスワードが十分に強力で、パスワードポリシーに準拠していることを確認します。自動配置では、弱いパスワードはサポートされません。

一般的な展開の制限とガイドライン

- デバイスをオンボードする前に、その設定を工場出荷時のデフォルトに戻します。
- 新しいデバイスまたは交換用デバイスをオンボードする場合は、1 つずつ、層ごとに行います。1 つのデバイスがオンボードされ、正常に動作していることを確認してから、次のデバイスのオンボードを開始します。この方法は、ネットワーク接続の問題やその他の問題が原因で発生する展開の失敗を回避するのに役立ちます。例えば、スパインデバイスをオンボードしてから、それに接続されているリーフデバイスをオンボードし、次に各リーフデバイスをオンボードしてから、それらに接続されているアクセスデバイスをオンボードします。多層アクセスデバイスを展開する場合も、層ごとに行います。
- 冗長性が必要な場合は、IRF ファブリックを導入します。このソリューションは、デュアルデバイス IRF ファブリックの自動導入のみをサポートします。
- スパイン/シングルリーフ IRF ファブリックをオンボードする場合は、次の手順に従います。
 - a. 2 つのデバイスをコントローラーに接続します。
 - b. 2 つのデバイスを相互に接続します。
 - c. ベストプラクティスとして、ブリッジ MAC アドレスの大きいデバイスを最初にオンボードします。
- リーフ/アクセス IRF ファブリックをオンボードする場合は、次の手順を実行します。
 - a. 2 つのデバイスをアップストリームデバイスに接続します。
 - b. 2 つのデバイスを相互に接続します。
 - c. 2 つのデバイスの設定をクリアし、同時に再起動します。
- AP のデュアルアップリンクは、自動集約をサポートしていません。
- 同じファブリック内のデバイスが異なるモード(手動と自動化)でオンボードされている場合は、異なるモードでオンボードされているデバイスが VSI/VLAN 4094 に異なる IP アドレスを使用していること、および手動でオンボードされたデバイスのアンダーレイ IP アドレスとアンダーレイ VLAN が、自動化テンプレートで定義されているアンダーレイ IP アドレス範囲とアンダーレイ VLAN 範囲に含まれていないことを確認します。

スパイン/シングルリーフデバイスの導入

- IRF ファブリックに組み込む場合を除き、2 つのスパインデバイスを直接接続したり、2 つのリーフデバイスを接続したりしないでください。

- スパインデバイスまたはシングルリーフデバイスでは、L3 スイッチに接続するインターフェースは、Attachment Circuit(AC)インターフェースとして自動的に設定されます。このインターフェースは、物理インターフェースまたは集約インターフェースにすることができます。IRF スタッキングをイネーブルにする場合は、次の手順に従ってスパインまたはシングルリーフ IRF ファブリックを展開します。
 - a. スパインまたはシングルリーフテンプレートで、アップリンクインターフェースを集約インターフェースとして指定します。
 - b. スパインデバイスまたはシングルリーフデバイスの 1 つ(より大きいブリッジ MAC アドレスを持つデバイス)を L3 スイッチに接続します。
 - c. L3 スイッチにダウンリンクインターフェース集約を手動で設定します。
 - d. スパイン/シングルリーフ IRF ファブリックをオンボードする。
 - e. IRF ファブリックがオンボードされ、正常に動作したら、ファブリック内のもう一方のスパインまたはシングルリーフデバイスを L3 スイッチに接続し、アップリンクインターフェースを手動で集約します。
- スパイン IRF ファブリックを展開する場合、またはシングルリーフ展開でリーフ IRF ファブリックを展開する場合は、ブリッジ MAC アドレスの大きいデバイスを最初にオンボードします。ブリッジ MAC アドレスの小さいデバイスを最初にオンボードすると、そのメンバーID が変更され、アップリンクインターフェースの名前が変更されます。この場合、スパインテンプレートのアップリンクインターフェース名またはシングルリーフテンプレートのリーフデバイスのアップリンクインターフェース名を、コントローラー上で手動で変更する必要があります。

アクセスデバイスの展開

- アクセスデバイスを自動展開するには、次の要件に従ってアクセスデバイスを設定する必要があります。
 - このソリューションは、最大 3 つのアクセス層をサポートします。アクセス層 1 はリーフ層に直接接続され、アクセス層 2 はアクセス層 1 に接続されます。
 - GE または Smartrate イーサネットポートを使用して、上位および下位のアクセス層を接続します。下位層のアクセスデバイスには、上位層のアクセスデバイスとの 2 つの物理リンクがありません。
 - IRF ファブリックは、アクセス階層 1 でのみ展開できます。アクセス階層 2 および 3 では、IRF ファブリックはサポートされません。
 - アクセス層 1 に IRF ファブリックを配置する場合は、10-GE ポートを使用してメンバーデバイスを接続します。多層アクセスデバイスに IRF 要件がない場合は、自動化テンプレートで IRF 自動化を無効にし、10-GE ポートを使用して接続できます。
 - 40 GE ポートを使用してアクセス層 1 で IRF ファブリックを形成し、10 GE ポートを使用して下位層のアクセスデバイスに接続するには、テクニカルサポートに連絡して、設定を実装するための自動化テンプレートを編集します。
- このソリューションでは、アクセス層での IRF ファブリックに対する BFD MAD の自動設定はサポートされていません。BFD MAD を手動で設定するには、次の手順に従います。
 - a. BFD MAD の物理インターフェースがダウンしていることを確認し、BFD MAD を設定します。
 - b. BFD MAD の物理インターフェースを接続し、BFD MAD が正常に動作することを確認します。

S7500E および S10500 の制限およびガイドライン

LSU1SUPB0 MPU を使用する S7500E スイッチおよび S10500 スイッチは、記憶容量が少なく、導入自動化に必要な記憶容量を満たすことができません。そのため、導入自動化の前にこれらのデバイスのソフトウェアを手動でアップグレードするか、デバイスが統合プラットフォームに組み込まれた後に統合プラットフォームからアップグレードしてください。

IRF ファブリックの拡張

1 デバイスの IRF ファブリックを拡張するには、以下の手順に従ってください。

1. IRF ファブリック内のデバイスが 2 時間以上オンラインであることを確認します。
2. 新しいデバイスの設定をクリアし、デバイスを再起動します。
3. 新しいデバイスをオンラインデバイスに接続します。

展開の検証

デバイスが自動的にオンボードされたら、Automation > Campus Network > Fabric > Auto Deployment > Auto Device Deployment Tasks を選択し、自動化プロセスを一時停止します。次に、デバイスは vcf-fabric underlay pause コマンドを実行して、自動化プロセスを停止します。

概要

ネットワーク自動化には、アンダーレイの自動化とオーバーレイの自動化が含まれます。このドキュメントでは、アンダーレイの自動化に焦点を当てています。次の情報では、アンダーレイの自動化の構成手順、コントローラーの構成手順、および自動デバイス展開プロセスについて説明します。

デバイスモデルと役割のマトリックス

表1に、AD-Campus ソリューションでサポートされているデバイスモデルを、ネットワークデバイスロールごとに示します。

表1 デバイスモデルと役割の互換性マトリックス

デバイスモデル	デフォルトの役割	サポートされるデフォルト以外の役割
S12500G-AF	スパイン	リーフ/アクセス
S10500X	スパイン	リーフ/アクセス
S7500X	リーフ	スパイン/アクセス
S6550XE-HI	リーフ	アクセス
S6525XE-HI	リーフ	アクセス
S 6520 X-HI	リーフ	アクセス
S 5560 X-HI	リーフ	アクセス
S6520X-EI(マイクロセグメンテーション、EPGとも呼ばれ、サポートされていません)	リーフ	アクセス
S5560X-EI(マイクロセグメンテーション、EPGとも呼ばれ、サポートされていません)	リーフ	アクセス
S6520X-SI	アクセス	なし
S5130-EI S 5130-HI S5130S-EI S5130S-HI	アクセス	なし

ネットワークアーキテクチャの設計

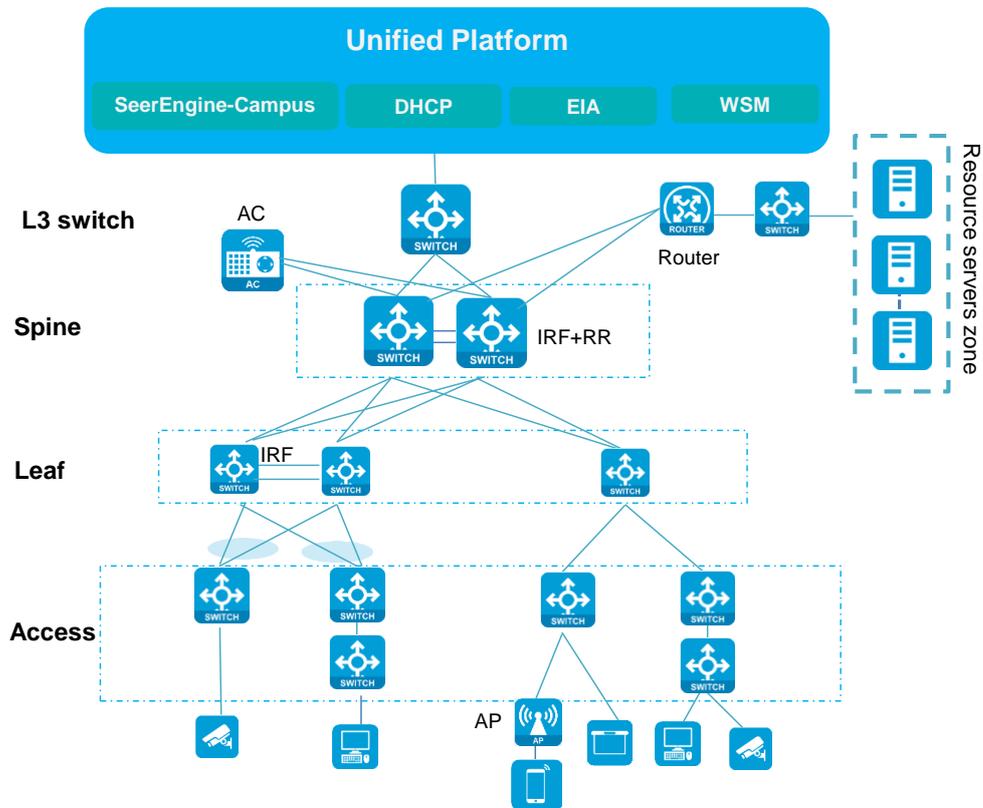
3 層アーキテクチャ

大規模なキャンパスでは、通常、3層のネットワークアーキテクチャを使用します。このアーキテクチャでは、デバイスがスパイン層、リーフ層、アクセス層に配置されます。また、このソリューションでは、最大 3 層のアクセス配置もサポートされます。

冗長性要件に応じて、デュアルデバイス IRF ファブリックをスパイン、リーフ、またはアクセス階層 1 に展開できます。

図 1 3層ネットワークアーキテクチャ

Three-tier network architecture



- Typical three-tier spine-leaf-access network deployment model for campus network
- AP and wired users connected to access devices

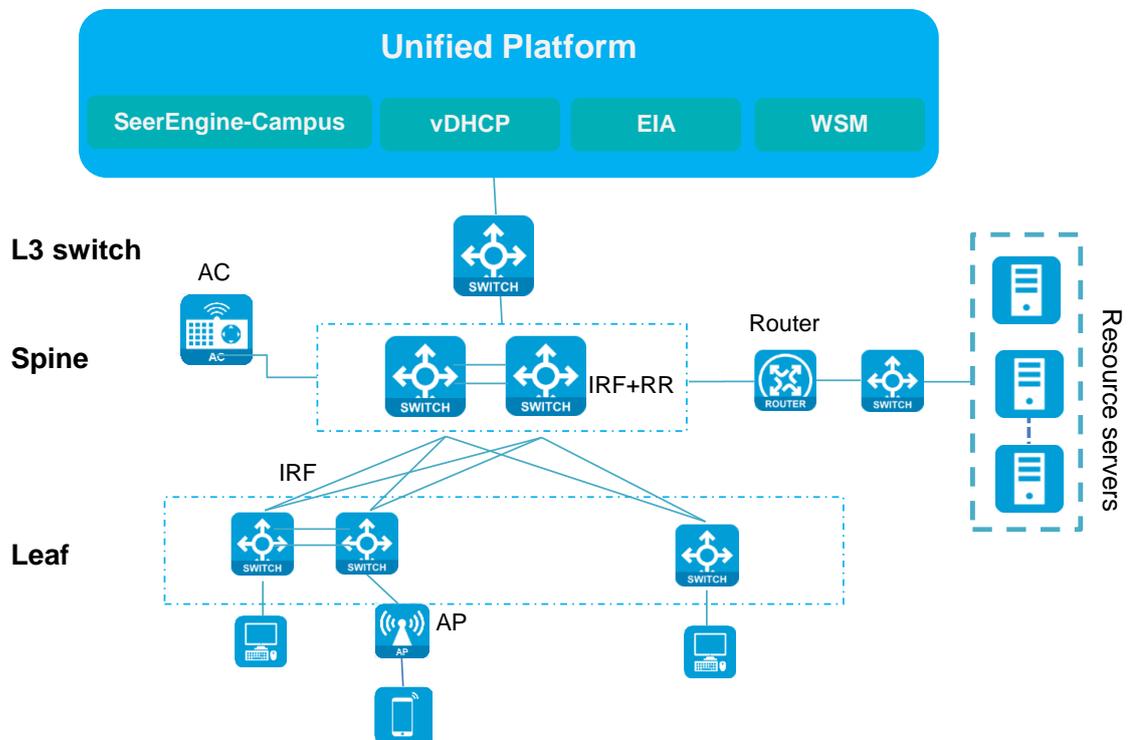
2層アーキテクチャ

小規模または中規模のキャンパスでは、デバイスがスパイン層とリーフ層に配置される2層ネットワークアーキテクチャを使用できます。アクセス層は存在しません。APおよび有線ユーザーはリーフデバイスに接続されます。

冗長性要件に応じて、デュアルデバイス IRF ファブリックをスパイン層とリーフ層に展開できます。

図 2 2層のネットワークアーキテクチャ

Two-tier network architecture



- Spine-leaf two-tier network is a special network model without the access tier.
- AP and wired users are connected to leaf devices.

シングルリーフアーキテクチャ

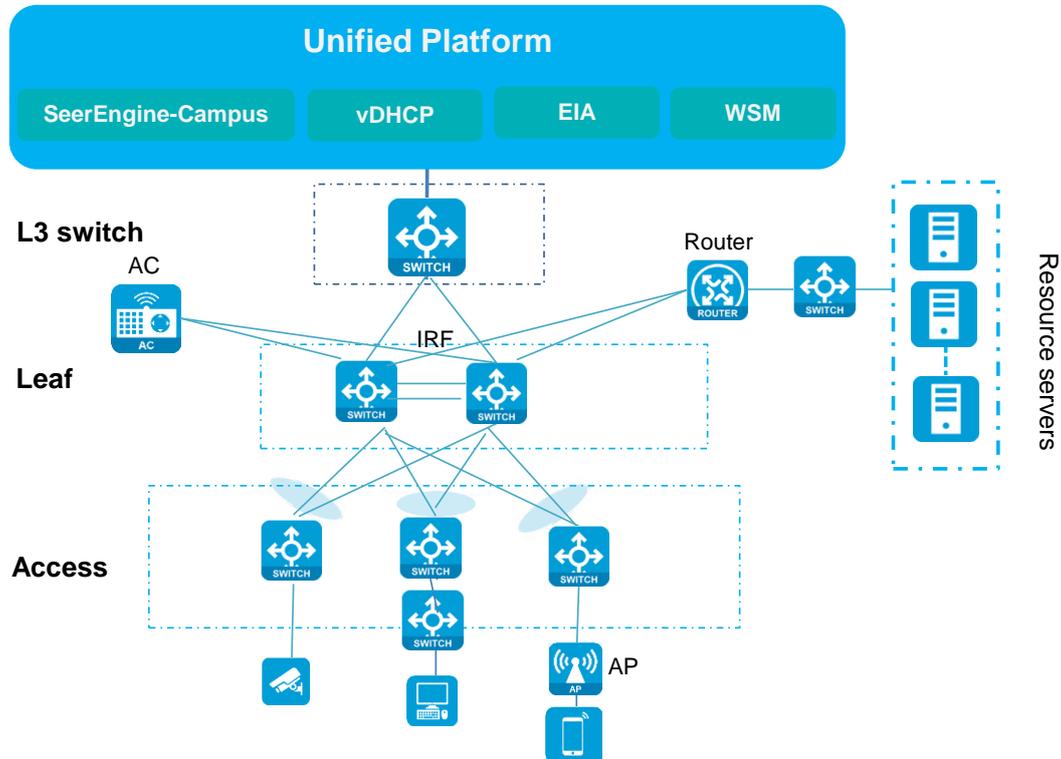
小規模なキャンパスでは、通常、デバイスがリーフ層とアクセス層に配置される2層ネットワークアーキテクチャが使用されます。

冗長性要件に応じて、シングルリーフデバイス、または各アクセスデバイスがデュアルホーム接続されているデュアルリーフ IRF ファブリックを配置できます。

アクセスデバイスの最大3つの階層をカスケードできます。アクセス階層1では、冗長性の必要に応じてデュアルデバイス IRF ファブリックを配置できます。

図 3 シングルリーフネットワークアーキテクチャ

Single-leaf network architecture



- The architecture has only leaf and access tiers and is suitable for small-sized networks.

アンダーレイネットワークとコントローラー間の接続モード

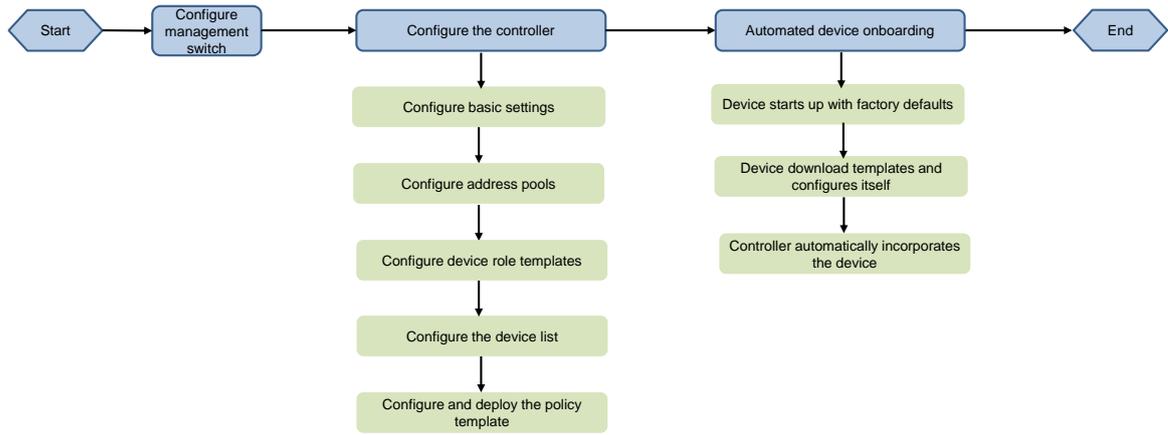
このソリューションでは、スパイン層に SeerEngine キャンパスコントローラーとのレイヤ3 接続が必要です。このソリューションは、SeerEngine キャンパスコントローラーと統合プラットフォームに対して、同じネットワークアダプタまたは 2 つの個別のネットワークアダプタの使用をサポートします。ネットワーク接続の詳細については、「AD-Campus 6.2 Basic Configuration Guide」を参照してください。

導入ワークフローの自動化

図 4 に、デバイスの自動アンダーレイ展開ワークフローを示します。このワークフローには、次の主要フェーズが含まれます。

1. コントローラーでデプロイメント自動化パラメーターを設定します。
2. デバイスは工場出荷時のデフォルトコンフィギュレーションファイルで起動し、ロールコンフィギュレーションテンプレートを自動的に取得してデバイス自体を設定します。
3. コントローラーのプライマリ RR を指定します。コントローラーは自動的に BGP 設定を展開します。EVPN トンネルは、スパインデバイスとリーフデバイス間に設定されます。
4. コントローラーは自動的にデバイスを組み込み、対応するデバイスグループおよびインターフェースグループにデバイスを追加します。

図 4 自動化されたアンダーレイ導入ワークフロー



工場出荷時のデフォルト設定の復元とデバイスの再起動

restore factory-default コマンドを実行して、デバイスを工場出荷時のデフォルト設定に復元します。

```
<Sysname> restore factory-default
```

This command will restore the system to the factory default configuration and clear the operation data. Continue [Y/N]:y

Restoring the factory default configuration. This process might take a few minutes. Please wait.....Done.

Please reboot the system to place the factory default configuration into effect.

自動化パラメーターの構成

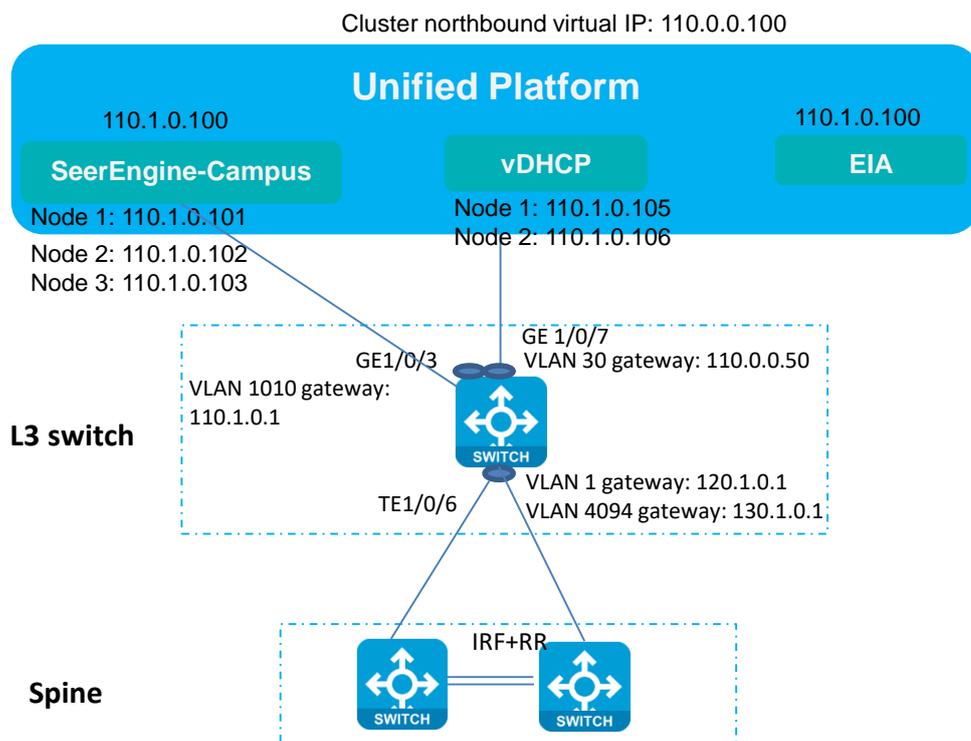
ネットワークリソースとIPアドレスの計画

ネットワークの導入を自動化する前に、ネットワークアーキテクチャとリソースを適切に計画します。SeerEngine キャンパスコントローラーと Unified Platform は、同じネットワークアダプタを共有することも、個別のネットワークアダプタを使用することもできます。

SeerEngine-個別のネットワークアダプタを使用するキャンパスコントローラーと統合プラットフォーム(推奨)

SeerEngine キャンパスコントローラーと統合プラットフォームでは、異なるネットワークアダプタとサブネットが使用されます。この場合、EIA と統合プラットフォームでは同じサブネットが使用され、SeerEngine キャンパスと vDHCP では同じサブネットが使用されます。

図 5 SeerEngine-個別のネットワークアダプタを使用するキャンパスコントローラーと統合プラットフォーム



ネットワークダイアグラムに示すように、SeerEngine キャンパスコントローラーと vDHCP サーバーは、Unified Platform に基づいて配置されます。コントローラーと vDHCP サーバーは同じ物理アダプタを共有します。L3 スイッチと vDHCP サーバーはケーブルで接続されます。

L3 スイッチのサーバー接続ポートを VLAN 1010(または VLAN 1 と VLAN 4094 を除く任意の VLAN)に追加します。これは、コントローラーおよび vDHCP サーバーの管理 VLAN であり、L3 スイッチとの L3 接続を保証します。サブネットは 110.1.0.0/24 です。

L3 スイッチで、スパインデバイスとの通信用に VLAN-interface 1 と VLAN-interface 4094 を設定します。DHCP を有効にします。VLAN-interface 1 で DHCP リレーを有効にします。

表 2 に、SeerEngine キャンパスコントローラーと Unified Platform が別々のネットワークアダプタを使用する場合に使用されるアドレッシング方式を示します。

表 2 アドレス指定方式

項目	アドレス	説明
VLAN 1サブネット(ゲートウェイIP)	120.1.0.0/24(120.1.0.1)	VLAN 1のネットワーク。自動オンボーディングに使用されます。
VLAN 4094サブネット(ゲートウェイIP)	130.1.0.0/24(130.1.0.1)	VLAN 4094のネットワーク。コントローラーとデバイス間の通信に使用されます。
VLAN 4093サブネット(ゲートウェイIP)	30.0.3.0/24(30.0.3.89)	VLAN-interface 4093は、APと通信するためのレイヤ3インターフェースです。
VLAN 30サブネット(ゲートウェイIP)	100.1.0.0/24(100.1.0.1)	PCとUnified Platform間の通信に使用されるUnified Platformのサブネット。
VLAN 1010サブネット(ゲートウェイIP)	110.1.0.0/24(110.1.0.1)	SeerEngineキャンパスのコントローラーとvDHCPのサブネット。コンピュータとコントローラー間の通信に使用されます。
アンダーレイIPサブネット	200.1.1.0/24	スパインデバイスおよびリーフデバイスのループバックインターフェースのサブネット。
Unified PlatformノースバウンドIP	100.1.0.100	Unified Platformへのログインに使用するアドレス。
EIA	100.1.0.100	EIAサーバードレス。
SeerEngine-キャンパスクラスターIP	110.1.0.100	SeerEngineキャンパスコントローラークラスターのアドレス。
SeerEngine-キャンパスノードIP	ノード1:110.1.0.101 ノード2:110.1.0.102 ノード3:110.1.0.103	SeerEngineキャンパスコントローラークラスター内の3つのノードのアドレス。
vDHCPクラスターIP	110.1.0.104	使用されないvDHCPサーバークラスターのアドレス。
vDHCPノードIP	ノード1:110.1.0.105 ノード2:110.1.0.106	vDHCPサーバークラスター内の2つのノードのアドレス。

注:

SeerEngine キャンパスと vDHCP のアドレスは、Unified Platform によって自動的に割り当てられます。

SeerEngine-同じネットワークアダプタを使用するキャンパスコントローラーと統合プラットフォーム

SeerEngine キャンパスコントローラーと Unified Platform は、1 つのネットワークアダプタを共有します。この場合、SeerEngine キャンパスコントローラー、vDHCP、および EIA サーバーは、同じサブネット内の IP アドレスを使用します。

図 6 SeerEngine-キャンパスコントローラーと統合プラットフォームが1つのネットワークアダプタを共有

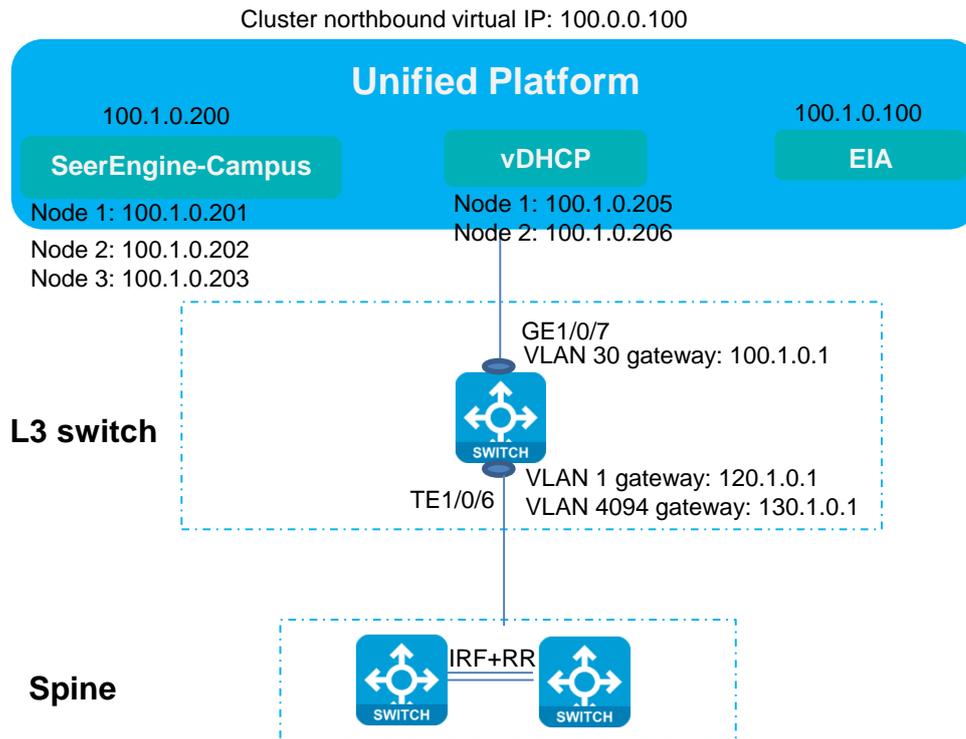


表 3 に、SeerEngine キャンパスコントローラーと Unified Platform が同じネットワークアダプタを使用する場合に使用されるアドレッシング方式を示します。

表 3 アドレス指定方式

項目	アドレス	説明
VLAN 1サブネット(ゲートウェイIP)	120.1.0.0/24(120.1.0.1)	VLAN 1のネットワーク。自動オンボーディングに使用されます。
VLAN 4094サブネット(ゲートウェイIP)	130.1.0.0/24(130.1.0.1)	VLAN 4094のネットワーク。コントローラーとデバイス間の通信に使用されます。
VLAN 30サブネット(ゲートウェイIP)	100.1.0.0/24(100.1.0.1)	Unified Platform、SeerEngineキャンパスコントローラー、およびvDHCPサーバーのサブネット。
VLAN 4093サブネット(ゲートウェイIP)	30.0.3.0/24(30.0.3.89)	VLAN-interface 4093は、APと通信するためのレイヤ3インターフェースです。
アンダーレイIPサブネット	200.1.1.0/24	スパインデバイスおよびリーフデバイスのループバックインターフェースのサブネット。
Unified PlatformノースバウンドIP	100.1.0.100	Unified Platformへのログインに使用するアドレス。
EIA	100.1.0.100	EIAサーバーアドレス。
SeerEngine-キャンパスクラスターIP	100.1.0.200	SeerEngineキャンパスコントローラークラスターのアドレス。
SeerEngine-キャンパスノードIP	ノード1:100.1.0.201	SeerEngineキャンパスコントローラー

項目	アドレス	説明
	ノード2:100.1.0.202 ノード3:100.1.0.203	一クラスター内の3つのノードのアドレス。
vDHCPクラスターIP	100.1.0.204	使用されないvDHCPサーバークラスターのアドレス。
vDHCPノードIP	ノード1:100.1.0.205 ノード2:100.1.0.206	vDHCPサーバークラスター内の2つのノードのアドレス。

ユーザーVLAN の計画

SeerEngine キャンパスには、事前定義された 3 つの VLAN プールがあります。Automation > Campus Network > Network Devices ページに移動します。右上隅の VNID Pools をクリックして、VNID プール設定ページを開きます。VLANs タブには、システム内のすべての VLAN プールが表示されます。

システムデフォルトキャンパスアクセス VLAN プール default_access、セキュリティグループ VLAN プール default_security_group、およびキャンパス認証フリーVLAN プール default_auth_free の名前は編集できません。

△ 注意:

デフォルトでは、SeerEngine キャンパスコントローラーは、自動 IRF ファブリックの BFD に VLAN 100 を使用し、予約済み VLAN として VLAN 4092~VLAN 4094 を使用します。

VLAN プールには、次のタイプがあります。

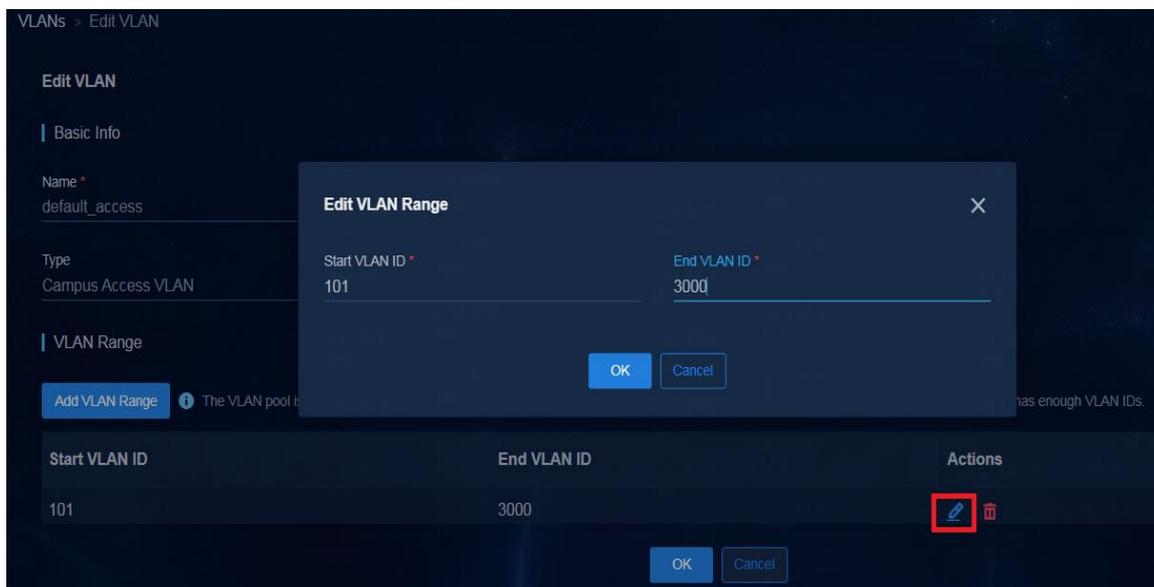
- **キャンパスアクセス VLAN:** このタイプの VLAN プールは、オンボードアクセスデバイスに VLAN 設定を割り当てるために使用されます。デフォルトでは、VLAN 範囲は 101~3000 です。
- **セキュリティグループ VLAN:** このタイプの VLAN プールは、ユーザーアクセスを実装するために、隔離ドメイン内のセキュリティグループに VLAN ID を割り当てるために使用されます。デフォルトでは、VLAN 範囲は 3501~4000 です。
- **Campus Auth-free VLAN:** このタイプの VLAN プールを使用して、隔離ドメイン内の認証フリーバインディングに VLAN ID を割り当て、認証フリー設定でバインドされたアクセスデバイスに VLAN 設定を展開します。デフォルトでは、VLAN 範囲は 4051~4060 です。

図 7 VLAN プール

Name	Type	VLAN Range	Default VLAN Pool
default_wireless_manage	Wireless Management VLAN	Ranges (1)	Yes
default_mlag	M-LAG VLAN Pool	Ranges (1)	Yes
default_wireless	Wireless Service VLAN Pool	Ranges (1)	Yes
default_wired	Wired Service VLAN Pool	Ranges (1)	Yes
default_security_group	Security Group VLAN	Ranges (1)	Yes
default_access	Campus Access VLAN	Ranges (1)	Yes

VLAN プールの VLAN 範囲を変更するには、VLAN プールの Edit アイコンをクリックします。表示されたページで、VLAN 範囲の Edit アイコンをクリックし、必要に応じて編集します。

図 8 VLAN 範囲の編集



3層または2層のアーキテクチャ導入の準備

3層またはスパインリーフ2層アーキテクチャ配置の場合は、このセクションの設定に従います。

L3 スイッチの設定

1. スパイン層デバイスとの通信用に VLAN-interface 1 および VLAN-interface 4094 を設定します。

```
#
vlan1
#
#
vlan 4094
#
#
interface Vlan-interface1
ip address 120.1.0.1 255.255.255.0
dhcp select relay
dhcp relay server-address 110.1.0.105 // vDHCP server IP
dhcp relay server-address 110.1.0.106 // vDHCP server IP
#
#
interface Vlan-interface4094 //管理アドレスはコントローラーによって割り当てられます。ここでは
DHCP リレーは必要ありません。
ip address 130.1.0.1 255.255.255.0
#
```

2. Unified Platform と通信するための VLAN インターフェース 30 を設定します。

```
#
vlan 30
#
#
interface Vlan-in
terface30
ip address 100.1.0.1 255.255.255.0
#
```

3. SeerEngine キャンパスコントローラーおよび vDHCP サーバーと通信するための VLAN インターフェース 1010 を設定します。

```
#
vlan 1010
#
#
interface Vlan-interface1010
ip address 110.1.0.1 255.255.255.0
#
```

4. DHCP を有効にします。


```
#
dhcp enable
#
```
5. STP をイネーブルにします。


```
#
stp global enable
#
```
6. デフォルトルートを追加します。

ユーザーがオンラインになるには、L3 スイッチでスタティックルーティングまたはダイナミックルーティングを設定して、認証のために EIA サーバーと通信できるようにする必要があります。使用可能なルートがない場合、ユーザーはセキュリティグループから IP アドレスを取得した後、EIA サーバーに対して認証できなくなります。

```
#
ip route-static 0.0.0.0 0 130.1.0.2 // スパインデバイス上の VSI 4094 の IP アドレスとして
ネクスト ホップを使用してデフォルト ルートを構成します。
#
```
7. スパインデバイスに接続されるインターフェースを設定します。


```
#
interface Ten-GigabitEthernet1/0/6
port link-mode bridge
description to_spine
port link-type trunk
port trunk permit vlan 1 4094
#
```
8. Unified Platform に接続されたインターフェースを設定します。


```
#
interface GigabitEthernet1/0/7 //統合プラットフォームの管理インターフェイスに接続されてい
ます。
port access vlan30
stp edged-port
#
```
9. コントローラーおよび vDHCP サーバーに接続されたインターフェースを設定します。

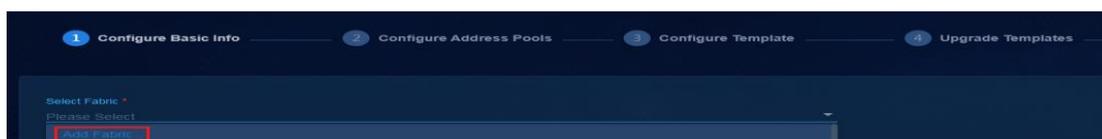

```
#
interface GigabitEthernet1/0/3 // SeerEngine-CampusコントローラーとvDHCP サーバー
の管理インターフェイスに接続されています。
port access vlan 1010
stp edged-port
#
```

コントローラーの設定

基本設定の構成

1. **SeerEngine キャンパスコントローラーにログインします。** Guide > Campus Wizard > Device Onboarding Plan > Configure Basic Info ページに移動します。

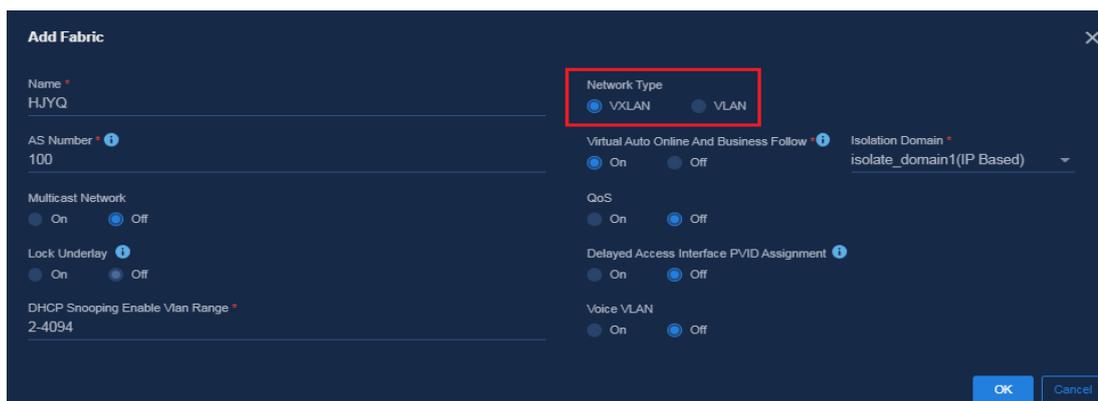
図 9 基本設定



2. **Select Fabric** をクリックしてファブリックを追加し、**OK** をクリックします。

- **Name:** ファブリック名を指定します。最大 255 文字の文字列で、大文字と小文字が区別されます。
- **Network Type:** デフォルトのネットワークタイプ VXLAN を使用します。
- **AS Number:** ファブリックの BGP AS 番号を 1~4294967295 の範囲の整数で入力します。マルチファブリックネットワークでは、各ファブリックで異なる AS 番号を使用する必要があります。
- **Isolation Domain:** ファブリックが属する分離ドメインを選択します。
- **Multicast Network:** オプション **Off** がデフォルトで選択されています。必要に応じて **On** を選択します。
- **QoS:** オプション **Off** がデフォルトで選択されています。必要に応じて **On** を選択します。
- **Lock Underlay:** デフォルトではオプション **Off** が選択されています。ファブリックを追加するときに設定を編集することはできません。この機能は、自動デバイスオンボーディング中はオフにする必要があります。自動化が完了したら、必要に応じて **On** にできます。
- **Delayed Access Interface PVID Assignment:** オプション **Off** がデフォルトで選択されており、デバイスがアクティブになったときにコントローラーによって PVID が自動的に割り当てられます。**On** オプションを選択すると、デバイスがアクティブになったときにコントローラーによって PVID が自動的に割り当てられず、必要に応じて PVID を設定できます。
- **Virtual Auto Online And Business Follow:** デフォルトではオプション **On** が選択されています。組み込まれるデバイスには、デバイスシリーズライセンスが必要な場合、仮想ネットワーク自動オンラインおよびビジネスフォローライセンスも必要です。ライセンスが不十分な場合、デバイスを組み込むことはできません。**Off** オプションを選択すると、組み込まれたデバイスは対応するライセンスを占有しませんが、分離ドメインには追加できません。

図 10 ファブリックの追加



3. **Use Optimized Automated Deployment:** オプション **Yes** がデフォルトで選択されています。構成の詳細は、「AD-Campus 6.2 Optimized Automation Configuration Guide」を参照してください。このドキュメントでは、元の自動デプロイメントプロシージャについて説明しているため、**No** オプションを選択します。

4. **TFTP Service** で **Yes** を選択します。

図 11 基本設定



5. **RR MAC** ボックスに、スパインデバイスのブリッジ MAC アドレスを入力します。ファブリックでシングルリーフアーキテクチャが使用されている場合は、このフィールドを空のままにしておくことができます。

△ **注意:**

スパイン IRF ファブリック、または複数の MPU を持つ単一のスパインデバイスの場合は、ファブリック内の各 MPU のブリッジ MAC アドレスを RR MAC フィールドに入力する必要があります。各ブリッジ MAC はカンマ(,)で区切ります。

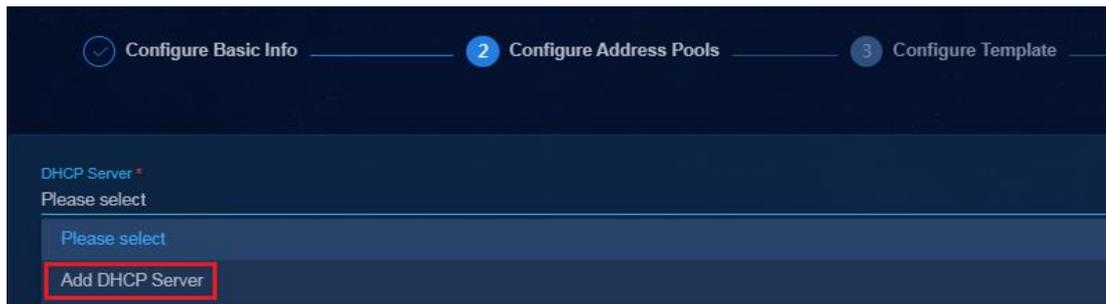
スパインデバイスのブリッジ MAC アドレスを取得するには、次のいずれかの方法を使用します。

- 方法 1: `display device manuinfo` コマンドを使用します。
[h3c]display device manuinfo chassis 1 slot 0 // MPUのスロット番号を指定します。
Chassis 1:
Slot 0 CPU 0:
DEVICE_NAME : LSUM1SUPC0
DEVICE_SERIAL_NUMBER : 210231A4B8H174000229
MAC_ADDRESS : 60DA-8309-E000
MANUFACTURING_DATE : 2017-04-13
VENDOR_NAME : H3C
[H3C]
- 方法 2: `probe` ビューで `debug stack show memberinfo` コマンドを使用します。
[H3C-probe]debug stack show memberinfo chassis 1 slot 0 //MPU のスロット番号を指定します。
=====
Member Information of STACK ModuleMember Information of STACK Module
=====
=====
MemID:1, LocalSlotID:0,
MemID:1, LocalSlotID:0, Priority:0, Mode:90 Priority:0, Mode:90
MaxMemNum:4, MaxPortMemberPort:16, StackCapability:5
MaxMemNum:4, MaxPortMemberPort:16, StackCapability:5
BridgeMac:60:da:83:09:e0:00 BridgeMac:60:da:83:09:e0:00
[H3C-probe]

アドレスプールの設定

1. **DHCP Server** をクリックし、**Add DHCP Server** を選択します。

図 12 アドレスプールの設定



2. H3C vDHCP パラメーターを設定します。

- **Management Mode: Tight** を選択します。vDHCP では、タイトモードのみがサポートされます。
- **High Availability**: クラスター環境でこのオプションを選択します。スタンドアロンモードでは、このオプションを選択する必要はありません。
- **IPv4/IPv6 Dual Stack**: IPv6 自動化が関係している場合、またはユーザーが IPv6 サービスを有効にしている場合は、このオプションを選択します。IPv6 サービス構成の詳細は、「AD-Campus 6.2 IPv6 Service Configuration Guide」を参照してください。
- **First IPv4 Address/Second IPv4 Address**: パブリックネットワークのデプロイ時に割り当てられた IPv4 アドレスを入力します。IPv4 アドレスを取得するには、**System > Deployment > Public Service** を選択し、**Details** アイコン  をクリックして、vDHCP サーバーの IP アドレスを表示します。

Component Details

Cluster IP 110.1.0.104 (System Allocated) VRRP Group Number 20

vdhcps1								
Host Name	Host NIC	Container NIC	Container NIC...	IP Address So...	Node ID	Network Name	Network Type	Subnet
matrix01	ens224	eth1	110.1.0.105	System Alloca...	node1	network	MACVLAN	network
Showing 1 entries.								
vdhcps2								
Host Name	Host NIC	Container NIC	Container NIC...	IP Address So...	Node ID	Network Name	Network Type	Subnet
matrix02	ens224	eth1	110.1.0.106	System Alloca...	node2	network	MACVLAN	network

- **Vendor: H3C** を選択します。

図 13 DHCP サーバーの追加

Add DHCP Server

Name *
vdhcp

Management Mode *
Tight

First IPv4 Address *
110.1.0.105

Second IPv4 Address *
110.1.0.106

Vendor *
H3C

High Available IPv4/IPv6 Dual Stack

OK Cancel

注:

自動デバイスオンボードに使用される DHCP サーバーは、H3C vDHCP サーバーである必要があります。

3. VLAN 1 アドレスプールを作成します。そのネットワークを VLAN 1 用に計画されたネットワークアドレス(120.1.0.0/24)に設定し、ゲートウェイアドレスを L3 スイッチの VLAN-interface 1 に割り当てられた IP アドレスに設定します。

図 14 VLAN 1 の IP アドレスプールの追加

Add IP Address Pool

Name *
vlan1

Type
Campus VLAN1 Network

Address Pool *
120.1.0.0/24

Gateway Address *
120.1.0.1

Using the Enterprise Code *
 Yes No

Add Address Range

Start IP	End IP	State	Actions
No Data			

Showing 0 entries.

OK Cancel

4. VLAN 4094 アドレスプールを追加します。そのネットワークを VLAN 4094(130.1.0.0/24)用に計画されたネットワークアドレスに設定し、ゲートウェイアドレスを L3 スイッチの VLAN インターフェース 4094 に割り当てられた IP アドレスに設定します。

図 15 VLAN 4094 の IP アドレスプールの追加

Start IP	End IP	State	Actions
No Data			

5. コントローラー、vDHCP サーバー、および EIA サーバーのサブネット 110.1.0.0/24 および 100.1.0.0/24 を追加します。サブネットはカンマ(,)で区切ります。

注:

Unified Platform、コントローラー、および EIA が異なるサブネットにある場合は、これらのサブネットをすべて追加します。

図 16 IPv4 管理サブネット

Controller and Other Server Subnets
110.1.0.0/24,100.1.0.0/24

注:

アンダーレイのオートメーションには IPv6 サービスがありません。VLAN4094 IPv6 アドレスプールとその IPv6 ネットワークアドレスを設定する必要はありません。

6. **Next** をクリックして、デバイスロールテンプレートの設定ページを開きます。

デバイスロールテンプレートの設定

1. デバイスロールテンプレート(自動化テンプレート)の設定:
 - **Local Username** および **Local Password**: ローカルユーザー名が **Control Protocol Template** で設定されたログインユーザー名と同じ場合、ローカルパスワードも **Control Protocol Template** で設定されたログインパスワードと同じである必要があります。コントロールプロトコルテンプレート内のユーザー名とパスワードは、コントローラーがデバイスにアクセスするために使用されます。ローカルユーザー名とローカルパスワードは、スパインデバイスがリーフデバイスにアクセスするために使用されます。
 - **NTP Server**: Unified Platform の展開時に NTP サーバーが設定されている場合は、ベストプラクティスとして、ここで NTP サーバーを Unified Platform のクラスターノースバウンドサービス IP として設定します。ユーザーネットワーク上の NTP サーバーのアドレスを入力することもできます。NTP サーバーがネットワーク上で到達可能であることを確認します。
 - **Control Protocol Template**: デフォルトの制御プロトコルテンプレートを選択します。ユーザー名とパスワードは空です。ユーザー名とパスワードを編集するには、**Automation > Campus Network > Fabrics > Auto Deployment > Control Protocol Templates** に移動します。

図 17 デバイスロールテンプレートの作成

2. 3層アーキテクチャの場合は、**Spine Template**、**Leaf Template/Single Leaf Template** および **Access Template** を選択します。**Leaf Template/Single Leaf Template** 領域で、**Leaf Template** を選択します。
3. 次のテンプレートパラメーターを設定します。
 - **Support for Version Upgrade:** デフォルトでは、オプション **No** が選択されており、自動化はソフトウェアバージョンのアップグレードをサポートしません。自動化中にソフトウェアバージョンをアップグレードするには、オプション **Yes** を選択し、アップグレードモードを選択します。
 - **Software Version:** デバイスをアップグレードするソフトウェアバージョンを選択します。アップグレードできるのは、同じモデルのデバイスのみです。

図 18 スパインテンプレート

- **Control Protocol Template:** 初期制御プロトコルテンプレートには、ユーザー名とパスワードが構成されていません。**Edit Template** をクリックして、制御プロトコルテンプレートにログインユーザー名とパスワードを構成します。制御プロトコルテンプレートに構成されたログインユーザー名が、ページの上部に構成されたローカルユーザー名と同じ場合、制御プロトコルテンプレートのログインパスワードもローカルパスワードと同じである必要があります。

図 19 コントロールプロトコルテンプレートの編集

- **Master Spine MAC:** スパインデバイスのブリッジ MAC アドレスを指定します。マスタースパイン MAC のスパインデバイスは、アンダーレイ IP アドレスとアンダーレイ VLAN を割り当てます。ス

スパインデバイスが IRF ファブリック内にある場合は、IRF ファブリック内のマスターのブリッジ MAC アドレスをマスタースパイン MAC として指定します。

- **Underlay IP Range:** スパインデバイスおよびリーフデバイス上のループバック 0 インターフェースに IP アドレスを割り当てるためのアドレス範囲を指定します。
- **Auto Allocate Underlay IP:** オプション **Yes** が既定で選択されています。
 - **Yes:** コントローラーは、設定されたアンダーレイ IP 範囲の IP アドレスを、スパインデバイスおよびリーフデバイス上の Loopback 0 インターフェースに自動的に割り当てます。
 - **No:** スパインデバイスとリーフデバイスの Loopback 0 インターフェースに IP アドレスを手動で割り当てます。**No** を選択した場合は、スパインテンプレートとリーフテンプレートでホワイトリストをイネーブルにし、指定したデバイスのアンダーレイ IP アドレスをデバイスリストに追加する必要があります。
- **Underlay VLAN Range:** アンダーレイ OSPF ネイバー関係を確立するための VLAN の範囲を指定します。デフォルト設定を使用することをお勧めします。
- **Uplink Interface:** スパインデバイスを L3 スイッチに接続するアップリンクインターフェースのフルネームを指定します。自動アンダーレイ展開中、コントローラーは、デバイスとコントローラー間のサービストラフィック用に、このインターフェース上の VLAN4094-VXLAN4094 の AC 設定を自動的に展開します。スパインデバイスがデュアルアップリンクを使用する IRF ファブリックの場合は、アップリンクインターフェースとして集約インターフェースを指定します。
- **IRF Stacking:** IRF スタッキングを有効にした場合、コントローラーは、デバイスが相互に関連付けられ、デバイスモデルとデバイスロールが同じであることを検出すると、2 つのデバイスを自動的に設定して IRF ファブリックを形成します。
- **Enable Whitelist:** コントローラーがデバイスリストを使用して展開するデバイスを識別するかどうかを指定します。
 - **No** を選択すると、デバイスの展開時に次の処理が実行されます。

デバイスのシリアル番号がデバイスリストにある場合、コントローラーは、デバイスリストで指定された情報に基づいてデバイスを展開し、指定されたタグをデバイスに組み込みます。

デバイスのシリアル番号がデバイスリストにない場合、コントローラーはデバイスのデフォルトロールに基づいてデバイスを展開し、デバイスをロール+VLAN4094_IP 形式のデフォルトタグに組み込みます。
 - **Yes** を選択すると、コントローラーはデバイスを展開するときに次の処理を行います。

デバイスのシリアル番号がデバイスリストにある場合、コントローラーは、デバイスリストで指定された情報に基づいてデバイスを展開し、指定されたタグをデバイスに組み込みます。

デバイスのシリアル番号がデバイスリストにない場合、自動オンボーディングは失敗します。
- **Enable Olt:** このパラメーターはリーフテンプレートで使用可能です。このパラメーターは、EPON ネットワーク用に構成する必要があります。詳細は「AD-Campus 6.2 EPON 構成ガイド」を参照してください。
- **Enable Auto Aggregation:** このパラメーターは、リーフテンプレートで使用できます。オプション **Yes** がデフォルトで選択されています。ネットワークで DRNI が使用されている場合は、**No** を選択する必要があります。
- **Enable Auto Aggregation of Uplinks:** このパラメーターは、アクセステンプレートで使用できます。オプション **Yes** がデフォルトで選択されています。ネットワークで DRNI が使用されている場合は、**No** を選択する必要があります。

注:

スパインデバイスが IRF ファブリック内にある場合は、IRF ファブリック内のマスターのブリッジ MAC アドレスをマスタースパイン MAC として指定します。

アンダーレイの自動展開中にソフトウェアをアップグレードするには、テンプレートでターゲットソフトウェアバージョンを指定します。この方法では、同じモデルのデバイスのみを一括してアップグレードできます。異なるモデルをアップグレードするには、「Upgrading software」を参照してください。

図 20 スパインテンプレート

The screenshot shows the configuration page for a Spine Template. At the top, three template roles are selected: Spine Template, Leaf Template/Single Leaf Template, and Access Template. The Spine Template section is expanded, showing various settings:

- Support for Version Upgrade: Yes, No
- Control Protocol Template: default_protocol_template (with an Edit Template button)
- Auto-Allocate Underlay IP: Yes, No
- Underlay VLAN Range: 3001-3500
- IRF Stacking: Yes, No
- Command Segments: (expandable)
- Software Patch: Please select
- Master Spine MAC: 58:6a:b1:e5:26:00
- Underlay IP Range: 200.1.1.0/24
- Uplink Interface: Ten-GigabitEthernet1/3/0/2
- Enable Whitelist: Yes, No

図 21 リーフテンプレート

The screenshot shows the configuration page for a Leaf Template/Single Leaf Template. The Leaf Template role is selected. The configuration options include:

- Support for Version Upgrade: Yes, No
- Control Protocol Template: default_protocol_template (with an Edit Template button)
- IRF Stacking: Yes, No
- Enable Olt: Yes, No
- Command Segments: (expandable)
- Software Patch: Please select
- Enable Whitelist: Yes, No
- Enable Auto Aggregation: Yes, No (with a note: "You must disable automatic aggregation when M-LAG is enabled.")

図 22 Access テンプレート

The screenshot shows the configuration page for an Access Template. The configuration options include:

- Support for Version Upgrade: Yes, No
- Control Protocol Template: default_protocol_template (with an Edit Template button)
- IRF Stacking: Yes, No
- Enable Auto Aggregation of Uplinks: Yes, No (with a note: "You must disable automatic aggregation when M-LAG is enabled.")
- Command Segments: (expandable)
- Software Patch: Please select
- Enable Whitelist: Yes, No

4. **Next** をクリックします。デバイスリストページが開きます。

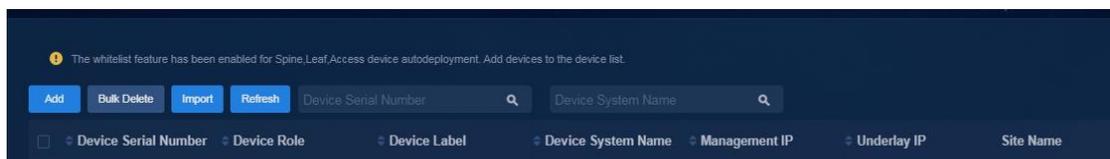
デバイスリストの構成

デバイスリストでは、デバイスシリアル番号によってデバイスが一意に識別されます。デバイスリストの各エントリーには、デバイスのシリアル番号とデバイスロールマッピングが記録されます。デバイスリストを使用すると、ネットワーク内の各デバイスのロールを計画できます。

デバイスリストは、デバイスホワイトリスト機能に使用されます。

- デバイスの自動化に対してホワイトリスト機能が有効になっている場合、コントローラーはデバイスの展開時に次の処理を行います。
 - デバイスのシリアル番号がデバイスリストにある場合、コントローラーは対応するデバイスロールテンプレート(自動化テンプレート)を取得して、デバイスの自動オンボーディングを完了します。
 - デバイスのシリアル番号がデバイスリストにない場合、デバイスの自動オンボーディングは失敗します。
- デバイスの自動化に対してホワイトリスト機能が有効になっていない場合、コントローラーはデバイスの展開時に次の処理を行います。
 - デバイスのシリアル番号がデバイスリストにある場合、コントローラーは、デバイスリストで指定されたデバイスロールに基づいてデバイスをオンボードします。
 - デバイスのシリアル番号がデバイスリストにない場合、コントローラーはデバイスのデフォルトロールに基づいてデバイスをオンボードします。

図 23 デバイスリスト



デバイスリストエントリーを追加するには:

1. デバイスをデバイスリストに手動で追加するには、**Add** をクリックします。複数のデバイスを一括して追加するには、**Import** をクリックしてインポートテンプレートをダウンロードします。次に、例として手動設定を使用します。
2. デバイスを追加するには、次のパラメーターを設定します。
 - **Network Type:** デフォルトでは VXLAN。
 - **WebSocket:** **Yes** を選択すると、コントローラーとデバイスは WebSocket 通信を使用します。最適化された自動構成の場合は、**Yes** を選択する必要があります。このドキュメントでは、元の自動デプロイメントプロシージャについて説明しているため、**No** オプションを選択します。
 - **Serial Number:** デバイスを一意に識別するデバイスの SN を入力します。モジュラデバイスの場合は、シャーシおよび MPU の SN をセミコロンで区切って入力します。デバイスの SN 情報を取得するには、次のコマンドを使用します。
 - S10500X/S10500 スイッチシリーズで、シャーシ情報と MPU 情報を表示します。


```
display device manuinfo chassis * slot *
```
 - S7500E スイッチシリーズで、MPU の情報を表示します。


```
display device manuinfo chassis * slot *
```
 - 固定ポートデバイス(S6550XE/S6525XE/6520X/S5560X シリーズ)で、スロット 1 に関する情報を表示します。


```
display license device-id slot 1
```
 - S7500X シリーズで MPU の情報を表示します。


```
display device manuinfo chassis * slot *
```
 - 固定ポート S51 シリーズで、スロット 1 に関する製造情報を表示します。


```
display device manuinfo slot 1
```

注:

デバイスシリーズがわからない場合は、テクニカルサポートにお問い合わせください。

- **Device Role:** オプションには、**Spine**、**Leaf**、**Access**、および **Aggregation** があります。コントローラーは、デバイスリストでデバイスに指定したロールを使用してデバイスを設定します。
- **Device System Name:** デバイスのシステム名。コントローラーは、デバイスのシステム名を、デバイスオンボーディング時にデバイスリストで指定された名前に変更します。
- **Management IP:** デバイスのオンボード後の VSI インターフェース 4094 または VLAN インターフェース 4094 の管理 IP アドレスを指定します。このパラメーターはオプションです。
 - 管理 IP アドレスが設定されている場合、SeerEngine キャンパスコントローラーは、デバイスのオンボード後に、設定されたアドレスをデバイスに割り当てます。
 - 管理 IP アドレスが設定されていない場合、SeerEngine キャンパスコントローラーは、VLAN4094 アドレスプールから自動的に選択されたアドレスを割り当てます。
- **Underlay IP:** デバイスのオンボード後の Loopback 0 インターフェースの IP アドレスを指定します。このパラメーターはオプションです。
 - アンダーレイ IP アドレスが設定されている場合、SeerEngine キャンパスコントローラーは、デバイスのオンボード後に、設定されたアドレスをデバイスに割り当てます。
 - アンダーレイの IP アドレスが設定されていない場合、SeerEngine キャンパスコントローラーは、アンダーレイの IP 範囲から自動的に選択されたアドレスを割り当てます。
- **Site Name:** デバイスが属するサイトを選択するか、必要に応じて設定します。ダッシュボード機能を使用する場合は、このパラメーターを指定する必要があります。

図 24 デバイスリストエントリーの追加

Add Device List [Close]

Network Type: VXLAN VLAN

WebSocket: Yes No

Device Serial Number: 210235A1YGX20B00000X

Device Role: spine

Device Label: _____

Device System Name: Spine7506

Management IP: _____

Underlay IP: _____

Site Name: _____

[OK] [Cancel]

ポリシーテンプレートの設定

ポリシーテンプレートは、サービスコントロールおよびプロビジョニング用です。自動デバイス展開の一部ではありません。ポリシーテンプレートの設定の詳細については、「AD-Campus 6.2 Basic Configuration Guide」を参照してください。

シングルリーフアーキテクチャ導入の準備

L3 スイッチの設定

「Configuring the L3 switch」を参照してください。

リーフデバイス用の IRF スタッキングの設定

ここでは、リーフファブリックの設定に必要な設定についてのみ説明します。

1. リーフデバイスの 1 つを L3 スイッチに接続します。リーフデバイスを相互に接続します。
2. シングルリーフテンプレートで、アップリンクインターフェースを集約インターフェースとして指定します。
3. L3 スイッチにダウンリンクインターフェース集約を手動で設定します。

```
#
interface Ten-GigabitEthernet0/0/48
port link-mode bridge
port link-type trunk
port trunk permit vlan all
port link-aggregation group 102
#
interface Ten-GigabitEthernet0/0/47
port link-mode bridge
port link-type trunk
port trunk permit vlan all
port link-aggregation group 102
#
interface Bridge-Aggregation102
port link-type trunk
port trunk permit vlan all
link-aggregation mode dynamic
#
```

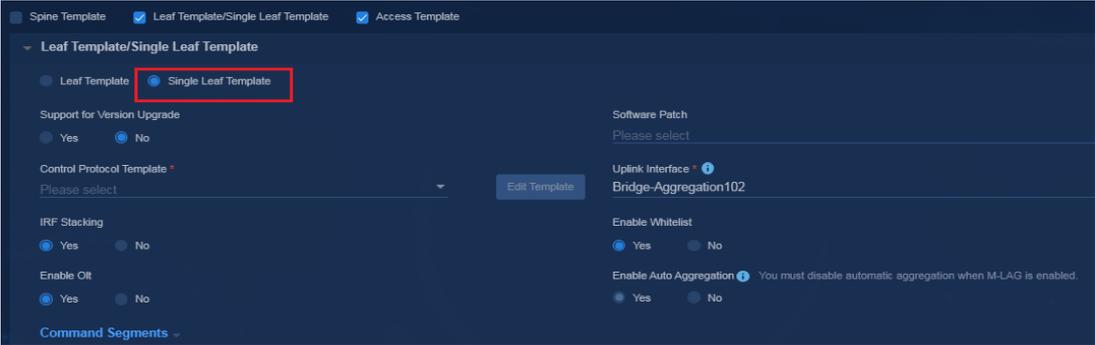
4. リーフデバイスは VLAN 1 を取得し、ファブリックを正常に形成します。
5. ファブリック内の他のリーフデバイスを L3 スイッチに接続し、アップリンクインターフェースを手動で集約します(テンプレートで設定されているのと同じ集約インターフェースを使用します)。

コントローラーの設定

次に、3 層構成と異なるシングルリーフ構成のみを示します。

1. 基本情報ページでは、RR の MAC アドレスは必要ありません。
2. デバイスロールテンプレートの設定ページで、次の手順を実行します。
 - **Spine Template** の選択を解除し、**Leaf Template/Single Leaf Template** および **Access Template** を選択します。
 - **Leaf Template/Single Leaf Template** 領域で、**Single Leaf Template** を選択します。
 - アップリンクインターフェースを、リーフデバイスを L3 スイッチに接続するインターフェースとして設定します。

図 25 シングルリーフテンプレートの設定



Spine Template Leaf Template/Single Leaf Template Access Template

Leaf Template/Single Leaf Template

Leaf Template Single Leaf Template

Support for Version Upgrade

Yes No

Control Protocol Template *

Please select [Edit Template](#)

IRF Stacking

Yes No

Enable OR

Yes No

Software Patch

Please select

Uplink Interface * [?](#)

Bridge-Aggregation102

Enable Whitelist

Yes No

Enable Auto Aggregation [?](#) You must disable automatic aggregation when M-LAG is enabled.

Yes No

Command Segments -

自動オンボーディング

単一のスパインデバイスのオンボード

工場出荷時のデフォルト設定でのスパインデバイスの起動

スパインデバイスは工場出荷時のデフォルト設定で起動し、IP アドレスとスパイン設定テンプレートを自動的に取得します。

```
Automatic configuration attempt: 10.  
Interface used: Vlan-interface1.  
Enable DHCP client on Vlan-interface1.  
Set DHCP client identifier: 70f96dab1fdf-VLAN0001  
Obtained an IP address for Vlan-interface1: 120.1.0.10.  
Obtained configuration file name HJYQ.template and TFTP server name 110.1.0.10 //コント  
ローラー上の TFTP サーバーのアドレス  
Resolved the TFTP server name to 110.1.0.100.  
INFO: Get device tag file device_tag.csv success.  
INFO: Read role spine from tag file.  
  
Successfully downloaded file HJYQ_spine.template //コントローラー上のスパインテンプレートの  
名前  
Executing the configuration file. Please wait...  
INFO: Read location spine123 from tag file.  
Automatic configuration successfully completed.  
Line aux1/0 is available.  
Press ENTER to get started.
```

スパインデバイスの自動設定

スパインデバイスは、ダウンロードされたテンプレートに基づいて自動的に設定されます(この例では、テンプレート名は **HJYQ_spine.template** です)。

このフェーズでは、VSI インターフェース 4094 の IP アドレスはまだ設定されていません。

```
[Spine]display vcf-fabric underlay autoconfigure  
success command:
```

```
#  
system  
clock timezone beijing add 08:00:00  
  
#  
system  
ip vpn instance vpn default  
route distinguisher 1:1  
vpn target 1:1 both  
address family evpn  
vpn target 1:1 import extcommunity  
vpn target 1:1 export extcommunity  
addressfamily ipv6 family ipv6  
vpnvpn--target 1:1 importtarget 1:1 import--extcommunity extcommunity  
vpnvpn--target 1:1 exporttarget 1:1 export--extcommunity extcommunity
```

```

#
system
lldp global enable lldp global enable
#
system
interface Vlaninterface Vlan--interface1 interface1
ip address dhcpip address dhcp--alloc alloc
#
system
ospf 1 ospf 1
nonnon--stopstop--routing routing
area 0.0.0.0 area 0.0.0.0
#
system
interface LoopBack0interface LoopBack0
#
system
netconf soap https enablenetconf soap https enable
netconf ssh server enablenetconf ssh server enable
restful https enablerestful https enable
#
system
telnet server enabletelnet server enable
#
system
infoinfo--center logghost 192.168.1.2center logghost 192.168.1.2
#
system

```

AC インターフェースの自動設定

デバイスは、取得したテンプレートに基づいて、サーバーに接続されている物理インターフェースを AC インターフェースとして自動的に設定した後、VSI インターフェース 4094 の IP アドレスを取得します。

```

#
interface Ten-GigabitEthernet1/1/0/1
port link-mode bridge
port link-type trunk
port trunk permit vlan all
#
service-instance 4094
encapsulation s-vid 4094
xconnect vsi vxlan4094
#

```

スパインデバイスでの展開結果の確認

アンダーレイの自動展開中に、display interface brief コマンドを実行して、スパインデバイスの IP 割り当てステータスを監視できます。

```

[spine123]display int brief | in UP
InLoop0          UP    UP(s)  --
Loop0            UP    UP(s)  200.1.1.254

```

NULL0	UP	UP(s)	--		
REG0	UP	----			
Tun1	UP	UP	--		
Tun2	UP	UP--			
Vlan1	UP	UP	120.1.0.10		
Vlan3498	UP	UP	200.1.1.254		
Vlan3499	UP	UP	200.1.1.254		
Vsi4092	UP	UP	130.1.0.2		SDN_VRF_VSI_Interface_4092
Vsi4094	UP	UP	130.1.0.2		
XGE1/5/0/1	UP	10G(a)	F(a)	T	1
XGE1/5/0/13	UP	10G(a)	F(a)	T	1
XGE1/5/0/15	UP	10G(a)	F(a)	T	1
XGE1/5/0/19	UP	10G(a)	F(a)	T	1

次の出力例では、デバイスはインターフェース Loopback 0、VLAN-interface 1、および VSI-interface 4094 の IP アドレスを取得しています。デバイスは、1 つのダウンリンクポートに対して VLAN 3498 を自動的に作成し、別のダウンリンクポートに対して VLAN 3499 を作成しました。リンクは自動的に ECMP パスとして設定されます。VLAN ID は、自動化テンプレートで設定されたアンダーレイ VLAN 範囲からコントローラーによって割り当てられました。

コントローラーでのスパインの展開の確認

スパインデバイスがオンボードになったら、コントローラーの **Automation > Campus Network > Network Devices** ページに移動します。デバイスに VSI インターフェース 4094 の IP アドレスが組み込まれ、スパインデバイスグループにも自動的に追加されていることを確認します。

図 26 スパインデバイス

Device Label	System Name	Fabric	Manage IP	Device ...	Device S...	Manage...	Data Sy...	Actions
spine_130.1.0.6	Spine75062	HJYQ	130.1.0.6	spine	Active	Managed	🟢	🔍 📄 🗑️ 🔄

図 27 スパインデバイスグループ

Edit General Policy Group

Name: Spine Device Group | Description:

Fabric: HJYQ | Group Type: Device Group

Subtype: NONE

Member	Policy			
Device Label	System Name	IP Address	Description	Actions
<input type="checkbox"/> spine_130.1.0.4	Spine7506	130.1.0.4	--	🗑️
<input type="checkbox"/> spine_130.1.0.6	Spine75062	130.1.0.6	--	🗑️

Showing 1 - 2 of 2 entries. Page 1 of 1. | 15 /page

構成の完全なデプロイメント

スパインデバイスが 1 つしかオンボードされていない場合、コントローラーは動的 BGP ピア設定を展開しません。代わりに、コントローラーは、少なくとも 1 つのリーフデバイスがオンボードされた後にだけ BGP ピア設定を展開し、アンダーレイ OSPF ネイバー関係を確立し、Loopback 0 インターフェースのインターフェースを取得します。

スパインテンプレートには、固定の BGP 設定だけが含まれています。

ユーザービューでは、`dir` コマンドを使用して **HJYQ_spine.template** という名前のテンプレートファイルを識別し、**more HJYQ_spine.template** コマンドを使用してテンプレートの設定を表示できます。

展開された設定の詳細については、「スパイン自動化テンプレート」を参照してください。パラメーター値は、実際のネットワークの状態によって異なります。

スパインIRFファブリックのオンボード

Spine IRF 展開の制限事項とガイドライン

デュアルスパイン IRF ファブリックを自動的に展開するには、次の要件が満たされていることを確認します。

- 2つのデバイスが IRF ファブリックを確立できることを確認します。
- 10 GE(またはそれ以上の速度)ポートを介して2つのデバイスを接続します。
- 2つのデバイスの役割は同じです。

スパイン IRF ファブリックを展開する場合は、次の手順に従います。

1. 2つのデバイスを L3 スイッチに接続します。
2. 2つのデバイスを相互に接続します。
3. まず、より大きいブリッジ MAC アドレスを持つデバイスをオンボードします。

注:

アップリンク集約が必要な場合に限り、2番目の IRF メンバーデバイスを L3 スイッチに接続する必要があります。この場合、アップリンクインターフェースを集約インターフェースとして指定し、L3 スイッチ上のスパインデバイスへのリンクを手動で集約する必要があります。

スパイン 1:

```
%Sep 30 10:43:06:700 2017 spine-0.137 VCF/5/VCF_IRF_FOUND: -MDC=1; In phase 2.0.1, device with MAC address 487a-dae0-ce00 found peer 50da-006d-6600 with the same role spine. Availability of IRF configuration is 0.
%Sep 30 10:43:46:745 2017 spine-0.137 VCF/5/VCF_IRF_START: -MDC=1; In phase 2.0.2, device with MAC address 487a-dae0-ce00 started IRF configuration: Current member ID 2, new member ID 2, priority 31, [None] bound to IRF-port 1, ['Ten-GigabitEthernet1/3/0/45'] bound to IRF-port 2.
%Sep 30 10:44:42:992 2017 spine-0.137 VCF/5/VCF_IRF_FINISH: -MDC=1; In phase 2.0.3, device with MAC address 487a-dae0-ce00 finished IRF configuration with peer 50da-006d-6600. The result is 0.
```

スパイン 2:

```
%Sep 30 09:21:32:258 2017 75inA301 VCF/5/VCF_IRF_FOUND: -MDC=1; In phase 2.0.1, device with MAC address 50da-006d-6600 found peer 487a-dae0-ce00 with the same role spine. Availability of IRF configuration is 0.
%Sep 30 10:43:23:942 2017 75inA301 VCF/5/VCF_IRF_START: -MDC=1; In phase 2.0.2, device with MAC address 50da-006d-6600 started IRF configuration: Current member ID 1, new member ID 1, priority 2, ['Ten-GigabitEthernet1/2/0/1'] bound to IRF-port 1, [None] bound to IRF-port 2.
%Sep 30 10:44:23:262 2017 75inA301 VCF/5/VCF_IRF_FINISH: -MDC=1; In phase 2.0.3, device with MAC address 50da-006d-6600 finished IRF configuration with peer 487a-dae0-ce00. The result is 0.
%Sep 30 10:44:30:055 2017 75inA301 VCF/5/VCF_IRF_REBOOT: -MDC=1; In phase 2.0.4, device with MAC address 50da-006d-6600 will reboot.
%Sep 30 10:45:35:113 2017 75inA301 DEV/5/SYSTEM_REBOOT: -MDC=1; System is rebooting now.
```

スタンバイデバイスが再起動して、マスターデバイスと IRF ファブリックを形成します。

```
%Sep 30 11:51:34:904 2017 spine-0.137 VCF/5/VCF_IRF_ALREADY: -MDC=1; In phase 2.0.10, device with MAC address 487a-dae0-ce00 has been irf successfully, standby Mac
```

50da-006d-6600.

<spine-0.137>display irf

MemberID	Slot	Role	Priority	CPU-Mac	Description
1	0	Standby 2		00e0-fc0a-15e0	---
*+2	0	Master	31	00e0-fc0f-8c13	---

* indicates the device is the master.

+ indicates the device through which the user logs in.

The bridge MAC of the IRF is: 487a-dae0-ce00

Auto upgrade : yes

Mac persistent : always

Domain ID : 0

Auto merge : yes

IRF mode : normal

IRF ファブリックが確立されると、IRF ファブリックは自動的に BFD MAD を設定します。

%Feb 28 05:08:12:592 2011 leaf-0.14 LLDP/5/LLDP_PVID_INCONSISTENT: PVID mismatch discovered on Ten-GigabitEthernet1/0/15 (PVID 100), with leaf-0.14 Ten-GigabitEthernet5/0/15 (PVID 1).

%Feb 28 05:08:12:592 2011 leaf-0.14 LLDP/6/LLDP_CREATE_NEIGHBOR: Nearest bridge agent neighbor created on port Ten-GigabitEthernet1/0/15 (IfIndex 15), neighbor's chassis ID is 9428-2eb8-afc4, port ID is Ten-GigabitEthernet5/0/15.

%Feb 28 05:08:12:753 2011 leaf-0.14 IFNET/3/PHY_UPDOWN: Physical state on the interface Vlan-interface100 changed to up.

%Feb 28 05:08:12:754 2011 leaf-0.14 IFNET/5/LINK_UPDOWN: Line protocol state on the interface Vlan-interface100 changed to up.

%Feb 28 05:08:17:143 2011 leaf-0.14 OPTMOD/5/RX_POW_NORMAL: -Slot=5; Ten-GigabitEthernet5/0/15:RX power is normal!

%Feb 28 05:08:18:290 2011 leaf-0.14 BFD/5/BFD_MAD_INTERFACE_CHANGE_STATE: BFD MAD function enabled on Vlan-interface100 changed to the normal state.

複数の IRF リンクがある場合、IRF ファブリックはリンクの 1 つを BFD MAD リンクとして使用し、次の設定で物理インターフェースを設定します。

```
#
interface Ten-GigabitEthernet1/0/15
port link-mode bridge
port access vlan 100
undo stp enable
```

```
#
interface Ten-GigabitEthernet5/0/15
port link-mode bridge
port access vlan 100
undo stp enable
#
```

IRF ファブリックは VLAN-interface 100 を設定し、インターフェース上の各デバイスに MAD IP アドレスを割り当てます。

```
#
interface Vlan-interface100
mad bfd enable
mad ip address 192.168.100.2 255.255.255.0 member 1
mad ip address 192.168.100.1 255.255.255.0 member 2
#
```

デバイスで BFD MAD を手動でイネーブルにします。

```
[spine] mad bfd enable
```

スパインデバイスとリーフデバイス間の複数のリンク

スパインデバイスにリーフデバイスへの複数のリンクがある場合、リンクは自動的に ECMP パスとして設定されます。

```
[spine]display lldp neighbor-information list | in leaf2
XGE1/5/0/13      88df-9e62-ee50  Ten-GigabitEthernet1/0/11  leaf2
XGE1/5/0/19      88df-9e62-ee50  Ten-GigabitEthernet5/0/33  leaf2
[spine]display vcf-fabric underlay autoconfigure
Downlink interface:
  Ten-GigabitEthernet1/5/0/13
  Ten-GigabitEthernet1/5/0/19
LoopBack0 IP allocation:
Device_MAC      Loopback_IP      Management_IP      State
88df-9e62-ee50  200.1.1.253      120.1.0.14        Up
70f9-6dab-1fdf  200.1.1.254      120.1.0.10        Up
0000-fc00-a001  200.1.1.249      120.1.0.13        Up
50da-0054-f400  200.1.1.251      120.1.0.12        Up
IRF allocation:
Self Bridge Mac: 70f9-6dab-1fdf
IRF Status: No
Member List: [1]
VLAN ID Allocation:
VLAN range: 3001-3500
VLAN exist and system reserved:
[1]
Interface      VLAN ID
Ten-GigabitEthernet1/5/0/13  3500
Ten-GigabitEthernet1/5/0/19  3499
```

リンク上の ECMP ルートがルーティングテーブルに生成されていることを確認します。

```
[spine]dis ip routing-table 200.1.1.253
Summary count : 2
Destination/Mask  Proto  Pre Cost      NextHop      Interface
200.1.1.253/32    O_INTRA  10  2      200.1.1.253  Vlan3500
200.1.1.253      Vlan3499
```

シングルリーフデバイスのオンボード

工場出荷時のデフォルト設定でのリーフデバイスの再起動

起動時に、リーフデバイスは IP アドレスとリーフテンプレートを取得します。次に出力例を示します。

```
Automatic configuration attempt: 14.
Interface used: Vlan-interface1.
Enable DHCP client on Vlan-interface1.
Set DHCP client identifier: 0000fc005eae-VLAN0001
Obtained an IP address for Vlan-interface1: 120.1.0.8.
Obtained configuration file name HJYQ.template and TFTP server name 110.1.0.100Set
DHCP client identifier: 0000fc005eae-VLAN0001
Obtained an IP address for Vlan-interface1: 120.1.0.8.
```

Obtained configuration file name HJYQ.template and TFTP server name 110.1.0.100

```
//コントローラー上の TFTP サーバーのアドレス
Resolved the TFTP server name to 110.1.0.100.
INFO: Get device tag file device_tag.csv success.
INFO: Read role leaf from tag file.
Successfully downloaded file HJYQ_leaf.template. //コントローラー上のリーフテンプレート名

Executing the configuration file. Please wait...
INFO: Read location 6520X from tag file.
Automatic configuration successfully completed.
Line aux1/0 is available.
Press ENTER to get started.
```

リーフデバイスは、取得したリーフ設定テンプレートに基づいて、自身を自動的に設定します。ユーザービューでは、dir コマンドを使用して **HJYQ_leaf.template** という名前のテンプレートファイルを識別し、more **HJYQ_leaf.template** コマンドを使用してテンプレートの設定を表示できます。

テンプレートの詳細については、「Leaf automation template」を参照してください。パラメーターの値は、実際のネットワークの状態によって異なります。

リーフインターフェースの自動設定

リーフデバイスは、アップリンクポートとダウンリンクポートを自動的に検出して設定します。

アップリンクポートの設定

この例では、VLAN 3498 に割り当てられているスパインリーフリンクは 1 つだけです。複数のリンクが展開されている場合、各リンクは 1 つの異なる VLAN に割り当てられ、リンクは ECMP パスとして設定されます。

```
#
interface Ten-GigabitEthernet1/1/0/23
port link-mode bridge
port link-type trunk
port trunk permit vlan 1 3498
lldp source-mac vlan 3498
lldp management-address arp-learning vlan 3498
lldp tlv-enable basic-tlv management-address-tlv interface LoopBack0
#
```

ダウンリンクポート設定

ダウンリンクポートはトランクポートとして設定され、各サービスインスタンス 4094 は VLAN 4094 に一致するように設定され、トラフィック転送のために VSI vxlan4094 に関連付けられます。

```
#
interface Ten-GigabitEthernet1/1/0/35
port link-mode bridge
port link-type trunk
port trunk permit vlan 1 101 to 3000 4094
#
service-instance 4094
encapsulation s-vid 4094
xconnect vsi vxlan4094
#
```

展開結果の確認

展開中に、展開の各フェーズを確認できます。

#最初に、リーフデバイスが VLAN-interface 1 とインターフェース Loopback 0 の IP アドレスを取得したことを確認します。リーフとスパインのリンクが VLAN(この例では、自動化テンプレートで定義されたアンダーレイ VLAN 範囲から VLAN 3498)に割り当てられ、Loopback 0 から借用した IP アドレスが割り当てられています。

```
[7503EM]display int brief | in UP
InLoop0          UP   UP(s)  --
Loop0            UP   UP(s)  200.1.1.250
NULL0           UP   UP(s)  --
REG0             UP   ----
Tun1             UP   UP      --
Tun3            UP   UP      --
Vlan1            UP   UP      120.1.0.8
Vlan3498         UP   UP      200.1.1.250
Vsi4092          UP   UP      130.1.0.3SDN_VRF_VSI_Interface_4092
Vsi4094          UP   UP      130.1.0.3
XGE1/1/0/23     UP   10G(a) F(a)   T    1
XGE1/1/0/35     UP   10G(a) F(a)   T    1
```

#リーフデバイスとスパインデバイスが OSPF ネイバー関係を確立していることを確認します。

```
#
interface Vlan-interface 3498
ip address unnumbered interface LoopBack0
ospf network-type p2p
ospf 1 area 0.0.0.0
#
[7503EM]display ospf peer
OSPF Process 1 with Router ID 200.1.1.250
Neighbor Brief Information
Area: 0.0.0.0
Router ID      Address          Pri Dead-Time  State          Interface
200.1.1.254 200.1.1.254      1  40           Full/ -Vlan3498
```

#スパインデバイスとリーフデバイスで BGP ピア関係が確立されていることを確認します。

マスターRR がリーフデバイスを検出した後、ディレクタは、BGP ピア関係を確立するために、BGP 設定(この例では BGP 100)をスパインデバイスとリーフデバイスに発行します。

次に、リーフデバイスに展開された BGP 設定例を示します。

```
bgp 100
non-stop-routing
router-id 200.1.1.250
peer200.1.1.254 as-number 100
peer200.1.1.254 connect-interface LoopBack0
#
address-family l2vpn evpn
peer200.1.1.254 enable
#
ip vpn-instance vpn-default
#
address-family ipv4 unicast
import-route static
#
return
```

#リーフデバイスとスパインデバイス間に BGP EVPN ピア関係を確立します。

```
[7503EM]display bgp peer l2vpn evpn
```

```
BGP local router ID: 200.1.1.250
```

```
Local AS number: 100
```

```
Total number of peers: 1
```

```
Peers in established state: 1
```

```
* -Dynamically created peer
```

```
Peer          AS  MsgRcvd  MsgSent  OutQ  PrefRcv  Up/Down  State
200.1.1.254   100    99      44      0     14 00:28:30  Established
```

スパインデバイスとリーフデバイスが BGP EVPN ピア関係を確立し、両者の間に VXLAN トンネルが確立されると、リーフデバイスは VSI インターフェイス 4094 の IP アドレスを取得します。

#コントローラーで、**Automation > Campus Network > Network Devices** ページに移動します。

#デバイスに VSI インターフェイス 4094 の IP アドレスが組み込まれていることを確認します。

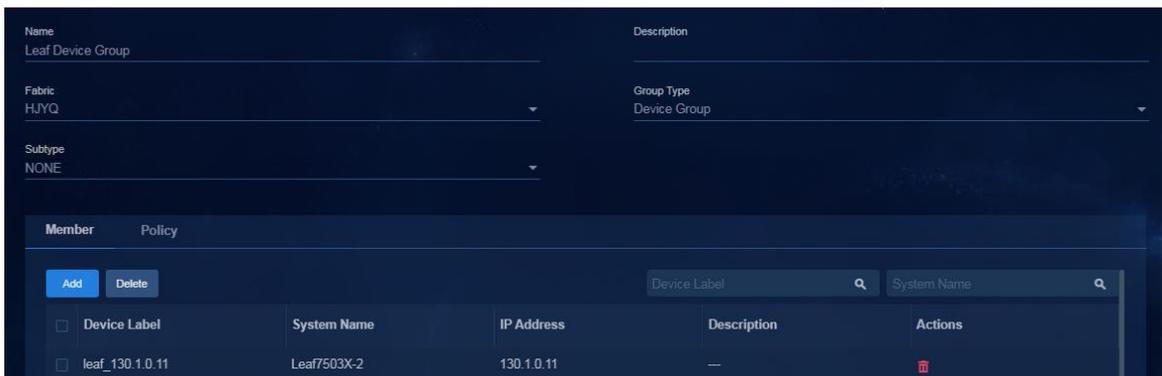
図 28 リーフデバイス



Device Label	System Name	Fabric	Manage IP	Device ...	Device S...	Manage...	Data Sy...	Actions
leaf_130.1.0.11	Leaf7503X-2	HJYQ	130.1.0.11	leaf	Active	Managed	●	  

#デバイスがリーフデバイスグループに自動的に追加されたことを確認します。

図 29 リーフデバイスグループ



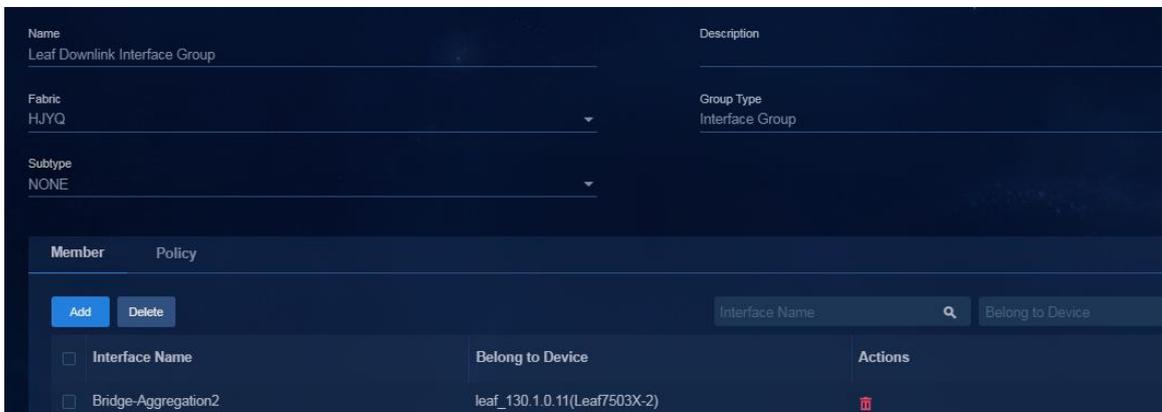
Name	Description
Leaf Device Group	

Fabric: HJYQ, Group Type: Device Group, Subtype: NONE

Member	Policy
<input type="checkbox"/> Device Label	
<input type="checkbox"/> leaf_130.1.0.11	

#リーフポートが、リーフダウンリンクインターフェイスグループに自動的に追加されることを確認します。

図 30 リーフダウンリンクインターフェイスグループ



Name	Description
Leaf Downlink Interface Group	

Fabric: HJYQ, Group Type: Interface Group, Subtype: NONE

Member	Policy
<input type="checkbox"/> Interface Name	
<input type="checkbox"/> Bridge-Aggregation2	leaf_130.1.0.11(Leaf7503X-2)

#リーフデバイスで、VLAN 101~3000 がリーフノードに展開されていることを確認します。

```
[leaf1]display vlan
```

```
Total VLANs: 2913
```

The VLANs include:
1(default), 15, 101-3000, 4094

複数のリーフデバイスのオンボード

リーフの展開は自動化されているため、展開、特に BGP 設定の展開を監視および確認するだけで済みます。

コントローラーで、リーフデバイスが組み込まれていることを確認します。

スパインデバイスで、デバイスがすべてのリーフデバイスと BGP EVPN ピア関係を確立しており、スパインデバイスと各リーフデバイス間の VXLAN トンネルがアップしていることを確認します。

次の出力例では、3 つのリーフデバイスがオンボードされています。

```
[spine123]display bgp peer l2vpn evpn
BGP local router ID:200.1.1.254
Local AS number: 100
Total number of peers: 3                Peers in established state: 3
* -Dynamically created peer
Peer          AS   MsgRcvd  MsgSent OutQ  PrefRcv Up/Down  State
200.1.1.250   2222    48      101    0     6 00:31:56 Established
200.1.1.251   2222   1311    1376   0     5 20:10:17 Established
200.1.1.253   2222    12      21     0     4 00:04:45 Established
```

リーフ IRF ファブリックのオンボード

リーフ IRF 展開の制限事項とガイドライン

デュアルリーフ IRF ファブリックを導入するには、次の要件が満たされていることを確認します。

- 2 つのデバイスが IRF ファブリックを確立できることを確認します。
- 10 GE(またはそれ以上の速度)ポートを介して 2 つのデバイスを接続します。
- 2 つのデバイスの役割は同じです。

スパイン IRF ファブリックを展開する場合は、次の手順に従います。

1. 2 つのデバイス(リーフ 1 とリーフ 2)をスパイン層に接続します。
2. 2 つのデバイスを接続します。
3. 2 つのデバイスの設定をクリアし、同時に再起動します。

リーフ 1 は、リーフ 2 に接続された 10 GE(またはそれ以上の速度)ポートがあることを検出すると、リーフ 2 との IRF ファブリックを自動的に確立します。これらのポートの役割は同じです。

リーフ 1:

```
%Sep 30 14:30:24:708 2017 leaf-0.139 VCF/5/VCF_IRF_FOUND: In phase 2.0.1, device
with MAC address 600b-038a-92d1 found peer 84d9-3190-0282 with the same role leaf.
Availability of IRF configuration is 0.
```

```
%Sep 30 14:31:04:719 2017 leaf-0.139 VCF/5/VCF_IRF_START: In phase 2.0.2, device
with MAC address 600b-038a-92d1 started IRF configuration: Current member ID 5, new
member ID 5, priority 1, [None] bound to IRF-port 1, ['Ten-GigabitEthernet5/1/17'] bound
to IRF-port 2.
```

```
%Sep 30 14:32:03:817 2017 leaf-0.139 VCF/5/VCF_IRF_FINISH: In phase 2.0.3, device
with MAC address 600b-038a-92d1 finished IRF configuration with peer 84d9-3190-0282.
The result is 0.
```

リーフ 2:

```
%Sep 30 14:30:53:272 2017 leaf-0.140 VCF/5/VCF_IRF_FOUND: In phase 2.0.1, device
with MAC address 84d9-3190-0282 found peer 600b-038a-92d1 with the same role leaf.
Availability of IRF configuration is 0.
%Sep 30 14:31:33:286 2017 leaf-0.140 VCF/5/VCF_IRF_START: In phase 2.0.2, device
with MAC address 84d9-3190-0282 started IRF configuration: Current member ID 1, new
member ID 1, priority 2, ['Ten-GigabitEthernet1/3/17'] bound to IRF-port 1, [None] bound
to IRF-port 2.
%Sep 30 14:32:30:523 2017 leaf-0.140 VCF/5/VCF_IRF_FINISH: In phase 2.0.3, device
with MAC address 84d9-3190-0282 finished IRF configuration with peer 600b-038a-92d1.
The result is 0.
```

スタンバイデバイスが再起動して、マスターデバイスと IRF ファブリックを形成します。

```
%Sep 30 14:32:08:402 2017 leaf-0.139 VCF/5/VCF_IRF_REBOOT: In phase 2.0.4,
device with MAC address 600b-038a-92d1 will reboot.
%Sep 30 14:32:12:511 2017 leaf-0.139 DEV/5/SYSTEM_REBOOT: System is rebooting
now.
%Sep 30 14:36:36:263 2017 leaf-0.140 VCF/5/VCF_IRF_ALREADY: In phase 2.0.10,
device with MAC address 84d9-3190-0282 has been irf successfully, standby Mac 600b-
038a-92d1.
<leaf-0.140>display irf
MemberID   Role   Priority CPU-Mac      Description
*+1        Master 2        00e0-fc0f-8c02 ---
5          Standby 1        00e0-fc0f-8c06 ---
-----
* indicates the device is the master.
+ indicates the device through which the user logs in.
The bridge MAC of the IRF is: 84d9-3190-0282
Auto upgrade      : yes
Mac persistent    : always
Domain ID         : 0
```

IRF ファブリックが確立されると、IRF ファブリックは自動的に BFD MAD を設定します。

```
%Feb 28 05:08:12:592 2011 leaf-0.14 LLDP/5/LLDP_PVID_INCONSISTENT: PVID
mismatch discovered on Ten-GigabitEthernet1/0/15 (PVID 100), with leaf-0.14 Ten-
GigabitEthernet5/0/15 (PVID 1).
%Feb 28 05:08:12:592 2011 leaf-0.14 LLDP/6/LLDP_CREATE_NEIGHBOR: Nearest
bridge agent neighbor created on port Ten-GigabitEthernet1/0/15 (IfIndex 15), neighbor's
chassis ID is 9428-2eb8-afc4, port ID is Ten-GigabitEthernet5/0/15.
%Feb 28 05:08:12:753 2011 leaf-0.14 IFNET/3/PHY_UPDOWN: Physical state on the
interface Vlan-interface100 changed to up.
%Feb 28 05:08:12:754 2011 leaf-0.14 IFNET/5/LINK_UPDOWN: Line protocol state on
the interface Vlan-interface100 changed to up.
%Feb 28 05:08:17:143 2011 leaf-0.14 OPTMOD/5/RX_POW_NORMAL: -Slot=5; Ten-
GigabitEthernet5/0/15: RX power is normal!
%Feb 28 05:08:18:290 2011 leaf-0.14
BFD/5/BFD_MAD_INTERFACE_CHANGE_STATE: BFD MAD function enabled on Vlan-
interface100 changed to the normal state.
```

複数の IRF リンクがある場合、IRF ファブリックはリンクの 1 つを BFD MAD リンクとして使用し、次の設定で物理インターフェースを設定します。

```
#
interface Ten-GigabitEthernet1/0/15
port link-mode bridge
port access vlan 100
undo stp enable
```

```
#
interface Ten-GigabitEthernet5/0/15
port link-mode bridge
port access vlan 100
undo stp enable
#
```

IRF ファブリックは VLAN-interface 100 を設定し、インターフェース上の各デバイスに MAD IP アドレスを割り当てます。

```
#
interface Vlan-interface100
mad bfd enable
mad ip address 192.168.100.2 255.255.255.0 member 1
mad ip address 192.168.100.1 255.255.255.0 member 2
#
```

4. IRF ファブリックで BFD MAD を手動でイネーブルにします。
[leaf]mad bfd enable

冗長なスパインリーフリンクを追加する

リーフ IRF ファブリックとスパインデバイス(またはスパイン IRF ファブリック)間の冗長リンクは、それぞれ VLAN に割り当てられ、ECMP パスとして自動的に設定されます。

スパインリーフリンクを表示するには、display lldp neighbor-information コマンドを実行します。

```
[leaf2] display lldp neighbor-information list | in spine
XGE1/0/11      70f9-6dab-1fdf  Ten-GigabitEthernet1/5/0/13 spine
XGE5/0/33      70f9-6dab-1fdf  Ten-GigabitEthernet1/5/0/19 spine
<leaf2>display vlan
```

Total VLANs: 3407

The VLANs include:

1(default), 2,101-3500, 3498-3499, 4094 //一方のアップリンクに VLAN 3498 が作成され、もう一方のアップリンクに VLAN 3499 が作成されました。

```
<leaf2>display vlan brief
```

5	VLAN 3498	BAGG1024	XGE1/0/15	XGE5/0/33	XGE5/0/47
8	VLAN 3499	BAGG1024	XGE1/0/11	XGE1/0/15	XGE5/0/47

冗長リーフアクセスリンクの追加

❗ 重要:

自動アンダーレイ展開では、各集約は 2 つの物理リンクしか持つことができません。

冗長リーフアクセスリンクは、自動的に集約されます。

次に、このプロセス中のサンプルメッセージを示します。

```
%Sep 30 15:05:51:383 2017 access-0.130 LAGG/6/LAGG_ACTIVE: Member port XGE1/0/50
of aggregation group BAGG1024 changed to the active state.
%Sep 30 15:05:51:390 2017 access-0.130 IFNET/5/LINK_UPDOWN: Line protocol state on
the interface Ten-GigabitEthernet1/0/50 changed to up.
%Sep 30 15:05:51:478 2017 access-0.130 IFNET/3/PHY_UPDOWN: Physical state on the
interface Bridge-Aggregation1024 changed to up.
%Sep 30 15:05:51:482 2017 access-0.130 IFNET/5/LINK_UPDOWN: Line protocol state on
the interface Bridge-Aggregation1024 changed to up.
```

%Sep 30 15:05:55:437 2017 access-0.130 VCF/6/VCF_AGGR_CREATE: In phase 2.0.5, device with MAC address 741f-4aea-80d1 created aggregation group 1024. The member port list is Ten-GigabitEthernet1/0/50,Ten-GigabitEthernet1/0/49.

<access-0.130>display link-aggregation verbose

Loadsharing Type: Shar --Loadsharing, NonS --Non-Loadsharing

Port Status: S --Selected, U --Unselected, I --Individual

Port: A --Auto port, M --Management port, R --Reference port

Flags: A --LACP_Activity, B --LACP_Timeout, C --Aggregation,

D --Synchronization, E --Collecting, F --Distributing,

G --Defaulted, H --Expired

Aggregate Interface: Bridge-Aggregation1024

Aggregation Mode: Dynamic

Loadsharing Type: Shar

Management VLANs: None

System ID: 0x8000, 741f-4aea-80d1

Local:

Port	Status	Priority	Index	Oper-Key	Flag
XGE1/0/49	S	32768	2	2	{ACDEF}
XGE1/0/50(R)	S	32768	1	1	{ACDEF}

Remote:

Actor	Priority	Index	Oper-Key	SystemID	Flag
XGE1/0/49	32768	2	2	0x8000, 84d9-3190-0282	{ACDEF}
XGE1/0/50	32768	1	1	0x8000, 84d9-3190-0282	{ACDEF}

集約インターフェースが作成されると、コントローラーは自動的に集約メンバーポートの元の設定を削除し、集約インターフェースのダウンリンク設定を再設定します。

1台のアクセスデバイスのオンボード

アクセスデバイスをオンボードする前に、アップストリームリーフデバイスがオンボードされ、オンラインになっていることを確認します。

アクセスデバイスを手動で組み込む場合は、そのアップストリームリーフデバイスがコントローラーに組み込まれ、オンラインになっていることを確認する必要があります。

デバイスの自動インストールに失敗した場合は、デバイス設定をクリアして、自動展開を再実行します。

工場出荷時のデフォルト設定でのリーフデバイスの再起動

工場出荷時のデフォルト設定に復元した後、アクセスデバイスを再起動します。

起動時に、アクセスデバイスは VLAN インターフェース 1 の IP アドレスとアクセスデバイス設定テンプレートを自動的に取得します。次に、出力例を示します。

Automatic configuration attempt: 2.

Interface used: Vlan-interface1.

Enable DHCP client on Vlan-interface1.

Set DHCP client identifier: 487ada2f7ad2-VLAN0001

Obtained an IP address for Vlan-interface1: 120.1.0.7.

Obtained configuration file name HJYQ.template and TFTP server name 110.1.0.100.

//コントローラー上の TFTP サーバーのアドレス

Resolved the TFTP server name to 110.1.0.100.

INFO: Get device tag file device_tag.csv success.

INFO: Read role access from tag file.

```
Successfully downloaded file HJYQ_access.template //コントローラ上のアクセステンプレートの名前
Executing the configuration file. Please wait...
INFO: Read location access3 from tag file.
Automatic configuration successfully completed.
Line aux4 is available.
Press ENTER to get started.
```

アクセスデバイスの自動設定

アクセスデバイスは、取得したアクセスデバイステンプレート(たとえば、HJYQ_access.template)に基づいて、自身を自動的に設定します。

デバイスの各ダウンリンクポートには、一意の PVID が割り当てられます。アクセスデバイスが PoE 対応の場合、PoE はすべての PoE 対応ポートでイネーブルになります。AP デバイスがポートに接続されている場合、VLAN 4093 が展開され、そのポートの PVID として設定されます。

ユーザービューでは、dir コマンドを使用して **HJYQ_access.template** という名前のテンプレートファイルを識別し、**more HJYQ_access.template** コマンドを使用してテンプレートの設定を表示できます。

テンプレートの詳細については、「Access automation template」を参照してください。パラメーターの値は、実際のネットワークの状態によって異なります。

アクセスデバイスでの展開結果の確認

アクセスデバイスを設定した後、アクセスデバイスが VLAN インターフェース 1 および VLAN インターフェース 4094 の IP アドレスを取得したことを確認します。

```
[access3]displayint brief | in UP
InLoop0          UP   UP(s)  --
NULL0           UP   UP(s)  --
Vlan1            UPUP          120.1.0.7
Vlan4094         UP   UP      130.1.0.35
XGE1/0/25       UP   10G(a)
```

アクセスデバイスのアップリンクポートがトランクポートとして設定され、すべての VLAN の通過が許可されていることを確認します。

```
#
interface Ten-GigabitEthernet1/0/25
port link-type trunk
port trunk permit vlan all
#
```

インターフェースの設定を確認します。次の出力例では、AP が接続されているため、インターフェースは PoE 対応で、PVID 4093 が割り当てられています。

```
#
interface GigabitEthernet5/0/5
port link-type trunk
port trunk permit vlan all
port trunk pvid vlan 4093
poe enable
#
```

コントローラーでのアクセス展開の確認

コントローラー上のデバイスを表示します。アクセスデバイスが管理対象デバイスとして組み込まれていることを確認します。その管理 IP アドレスは、VLAN インターフェース 1 の IP アドレスから VLAN インターフェース 4094 の IP アドレスに変更されました。

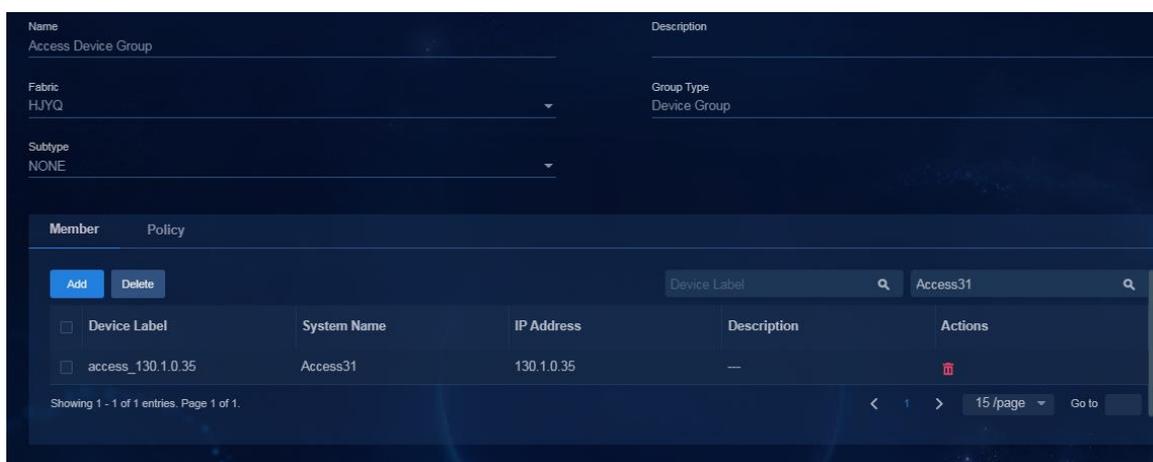
図 31 アクセスデバイス



Device Label	System Name	Fabric	Manage IP	Device ...	Device S...	Manage...	Data Sy...	Actions
<input type="checkbox"/> access_130.1.0.35	Access31	HJYQ	130.1.0.35	access	Active	Managed		

アクセスデバイスがアクセスデバイスグループに割り当てられていることを確認します。

図 32 アクセスデバイスグループ



Name	Description
Access Device Group	
Fabric: HJYQ	Group Type: Device Group
Subtype: NONE	

Member	Policy
<input type="checkbox"/> Device Label	System Name
<input type="checkbox"/> access_130.1.0.35	Access31

Showing 1 - 1 of 1 entries. Page 1 of 1.

アクセスIRFファブリックのオンボード

アクセス IRF ファブリックの展開

- 2つのデバイス(アクセス 1 とアクセス 2)をリーフ層に接続します。
- 2つのデバイスを接続します。
- 2つのデバイスの設定をクリアし、同時に再起動します。

アクセス 1 は、アクセス 2 に接続された 10 GE ポートがあることを検出すると、アクセス 2 との IRF ファブリックを自動的に確立します。これらのポートの役割は同じです。

- IRF ファブリックが確立されていることを確認します。

```
<access3>dis irf
MemberIDRole    Priority CPU-Mac      Description
*+1             Master  2            00e0-fc0f-8c02 ---
5               Standby 1          00e0-fc0f-8c06 ---
```

* indicates the device is the master.

+ indicates the device through which the user logs in.

The bridge MAC of the IRF is: 50da-00ea-d9f8

Auto upgrade : yes

Mac persistent : always

Domain ID : 0

注:

このソリューションは、アクセス層での IRF ファブリックの BFD MAD の自動設定をサポートしていません。

5. BFD MAD を手動で設定します。

#BFD MAD の物理インターフェースがダウンしていることを確認してから、BFD MAD を設定します。

#

vlan 100 //この VLAN は BFD MAD だけに使用されます。

#

```
interface GigabitEthernet1/0/20
```

```
port link-type trunk
```

```
undo port trunk permit vlan 1
```

```
port trunk permit vlan 100
```

```
undo stp enable
```

```
stp edged-port //このコマンドが含まれていない場合、監査の相違はコントローラーで検出されます。
```

```
undo lldp enable
```

```
#
```

```
#
```

```
interface GigabitEthernet5/0/20
```

```
port link-type trunk
```

```
undo port trunk permit vlan 1
```

```
port trunk permit vlan 100
```

```
undo stp enable
```

```
stp edged-port //このコマンドが含まれていない場合、監査の相違はコントローラーで検出されます。
```

```
undo lldp enable
```

```
#
```

```
#
```

```
interface Vlan-interface100
```

```
mad bfd enable
```

```
mad ip address 192.168.100.1 255.255.255.0 member 1
```

```
mad ip address 192.168.100.5 255.255.255.0 member 5
```

```
#
```

#BFD MAD の物理インターフェースを接続し、BFD MAD が正常に動作することを確認します。

```
[5130s-hi-down]disp mad verbose
```

```
Multi-active recovery state: No
```

```
Excluded ports (user-configured):
```

```
Excluded ports (system-configured):
```

```
  IRF physical interfaces:
```

```
    Ten-GigabitEthernet1/0/25
```

```
    Ten-GigabitEthernet5/0/25
```

```
  BFD MAD interfaces:
```

```
    Bridge-Aggregation1022
```

```
    Bridge-Aggregation1024
```

```
    GigabitEthernet1/0/2
```

```
    GigabitEthernet1/0/20
```

```
    GigabitEthernet5/0/1
```

```
    GigabitEthernet5/0/20
```

```
    Ten-GigabitEthernet1/0/26
```

```
    Ten-GigabitEthernet5/0/26
```

```
    Vlan-interface100
```

```
MAD ARP disabled.
```

```

MAD ND disabled.
MAD LACP disabled.
MAD BFD enabled interface: Vlan-interface99
MAD status                : Normal
Member ID  MAD IP address  Neighbor  MAD status
1           192.168.100.1/24  5         Normal
5           192.168.100.5/24  1         Normal

```

自動リーフアクセスリンク集約

❗ 重要:

自動アンダーレイ展開では、各集約は 2 つの物理リンクしか持つことができません。

```

<access3> display lldp neighbor-information list | inc leaf
GE1/0/15      9428-2eb8-8742  Ten-GigabitEthernet1/0/17  leaf1
GE5/0/15      9428-2eb8-8742  Ten-GigabitEthernet1/0/25  leaf1
<access3>display vlan brief
Brief information about all VLANs:
Supported Minimum VLAN ID: 1
Supported Maximum VLAN ID: 4094
Default VLAN ID: 1
VLAN ID  Name                    Port
1         VLAN 0001                   BAGG1024  GE1/0/15  GE5/0/15
101      VLAN 0101                   BAGG1024  GE1/0/1   GE1/0/15

```

複数階層のアクセスデバイスの導入

複数階層のアクセスデバイスを配置する場合は、GE ポートを使用してカスケード接続します。

このソリューションは、最大 3 つのアクセス層をサポートします。アクセス層 1 はリーフ層に直接接続され、アクセス層 2 はアクセス層 1 に接続されます。

注:

Tier 1 デバイスが配置されると、そのダウンリンクポートには 101 から 3000 の範囲の PVID が割り当てられます。デバイス上のダウンリンクポートが起動すると、ポートが H3C スイッチに接続する場合、その PVID は 1 に変更されます。この変更により、下位層のアクセスデバイスの自動配置が保証されます。Tier 1 デバイスが H3C デバイスでない場合、ダウンリンクポートの PVID を手動で 1 に変更する必要があります。

自動展開を使用すると、下位層のアクセスデバイスは、上位層のアクセスデバイスに接続するために集約された最大 2 つの物理リンクを持つことができます。

工場出荷時のデフォルト設定での下位層アクセスデバイスの再起動

起動時に、アクセスデバイス(Tier 2 アクセスデバイスなど)は自動的に自身を設定します。次の出力例は、自動化されたオンボーディングプロセスを示しています。

```

Automatic configuration attempt: 2.
Interface used: Vlan-interface1.           Enable DHCP client on Vlan-interface1.

```

Set DHCP client identifier: 487ada92a6cb-VLAN0001
 Obtained an IP address for Vlan-interface1: 120.1.0.102.
 Obtained configuration file name HJYQ.template and TFTP server name 110.1.0.100

//コントローラー上の TFTP サーバーのアドレス
 Resolved the TFTP server name to 110.1.0.100.
 INFO: Get device tag file device_tag.csv success.
 INFO: Read role access from tag file.

Successfully downloaded file HJYQ_access.template. //コントローラー上のアクセステンプレートの名前

Executing the configuration file. Please wait...
 INFO: Read location access22 from tag file.
 Automatic configuration successfully completed.
 Line aux4 is available.
 Press ENTER to get started.

展開の確認

VLAN-interface 1 および VLAN-interface 4094 がそれぞれ IP アドレスを取得したことを確認します。

[access22]dis int brief

Brief information on interfaces in route mode:

Link: ADM -administratively down; Stby -standby

Protocol: (s) -spoofing

Interface	Link	Protocol	Primary IP	Description
InLoop0	UP	UP(s)	--	
NULL0	UP	UP(s)	--	
Vlan1	UP	UP	120.1.0.102	
Vlan4094	UP	UP	130.1.0.32	

コントローラーで、Tier 2 アクセスデバイスが組み込まれていることを確認します。

図 33 アクセスデバイス

Device Label	System Name	Fabric	Manage IP	Device ...	Device S...	Manage...	Data Sy...	Actions
access_130.1.0.32	Access333-to2	HJYQ	130.1.0.32	access	Active	Managed		

Tier 2 アクセスデバイスは、アクセスデバイスグループに自動的に追加できます。

図 34 アクセスデバイスグループ

Name	Description
Access Device Group	

Fabric	Group Type
HJYQ	Device Group

Subtype
NONE

Member	Policy										
<table border="1"> <thead> <tr> <th>Device Label</th> <th>System Name</th> <th>IP Address</th> <th>Description</th> <th>Actions</th> </tr> </thead> <tbody> <tr> <td>access_130.1.0.32</td> <td>Access333-to2</td> <td>130.1.0.32</td> <td>--</td> <td></td> </tr> </tbody> </table>	Device Label	System Name	IP Address	Description	Actions	access_130.1.0.32	Access333-to2	130.1.0.32	--		
Device Label	System Name	IP Address	Description	Actions							
access_130.1.0.32	Access333-to2	130.1.0.32	--								

自動化された IPv6 導入

IPv6 導入を自動化するには、自動化テンプレートで VLAN4094 IPv6 アドレス プールを構成します。次に、ネットワーク デバイスはテンプレートから IPv6 構成を取得します。IPv6 構成の詳細については、「AD-Campus 6.2 IPv6 サービス構成ガイド」を参照してください。

ソフトウェアのアップグレード

自動化テンプレートでターゲット ソフトウェア バージョンを指定することにより、同じモデルのデバイスを一括でアップグレードできます（「デバイス ロール テンプレートの設定」を参照）。**Automation > Configuration Center > Software Library** ページでデバイスをアップグレードすることもできます。

NOTE:

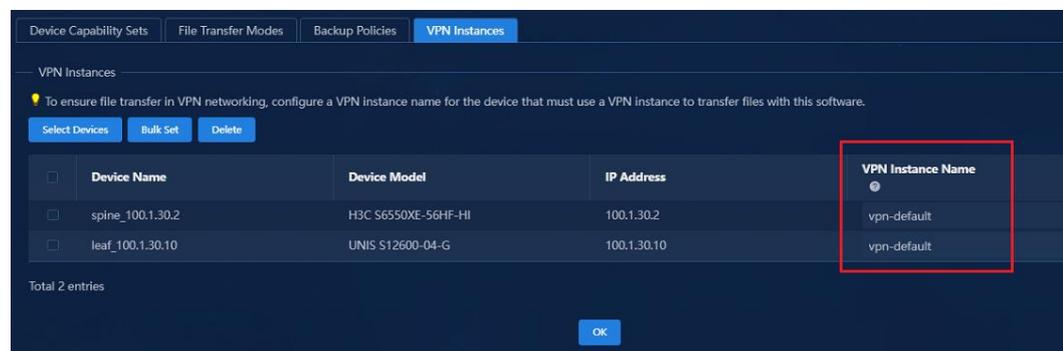
自動展開中にソフトウェアを正常にアップグレードするには、デバイス側の残りのスペースがアップロードされたバージョンのサイズの 2 倍である必要があります。LSU1SUPB0 MPU を使用する S7500E スイッチおよび S10500 スイッチは、ストレージ容量が小さいため、要件を満たすことができません。

これらのデバイスの場合は、自動展開の前にソフトウェアを手動でアップグレードするか、デバイスが統合プラットフォームに組み込まれた後に統合プラットフォームからソフトウェアをアップグレードします。

ソフトウェアをアップグレードするには:

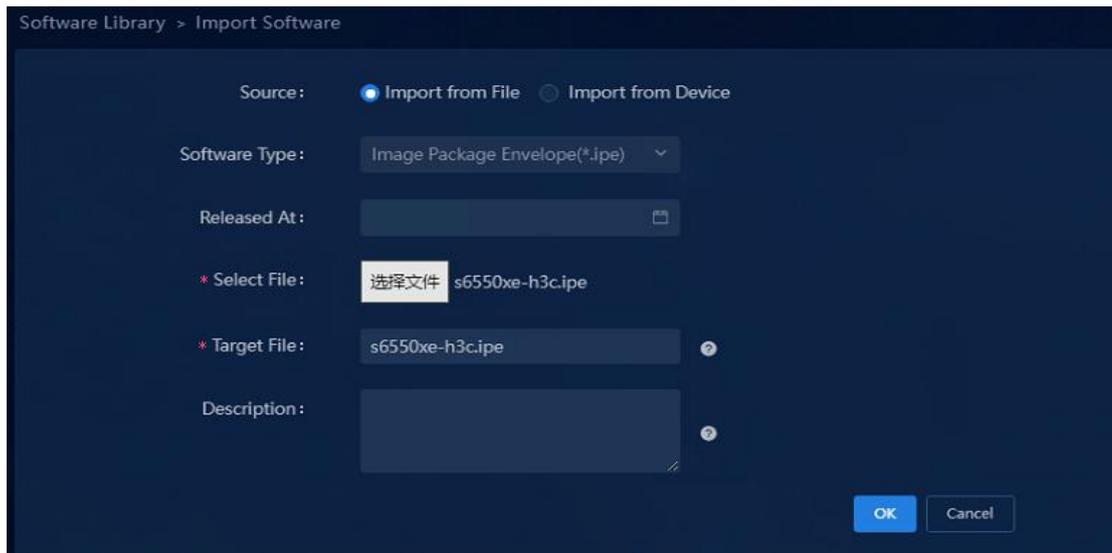
1. **Automation > Configuration Center > Deploy Parameters > VPN Instances** を選択し、管理 VPN インスタンスを追加します。インスタンス名は **vpn-default** です。

図 35 管理 VPN インスタンスの追加



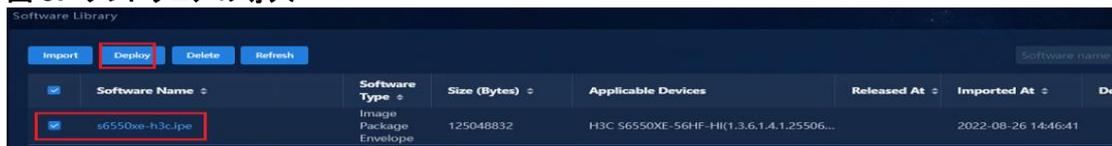
2. **Automation > Configuration Center > Software Library** を選択します。Import をクリックし、アップグレードに必要なソフトウェア バージョン ファイルをアップロードします。

図 36 ソフトウェアのインポート



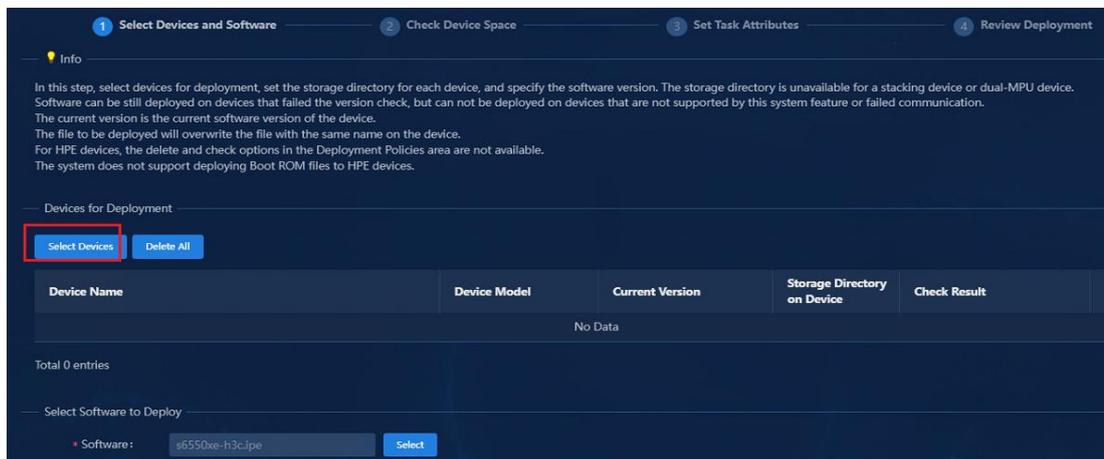
3. Deploy をクリック。

図 37 ソフトウェアの導入



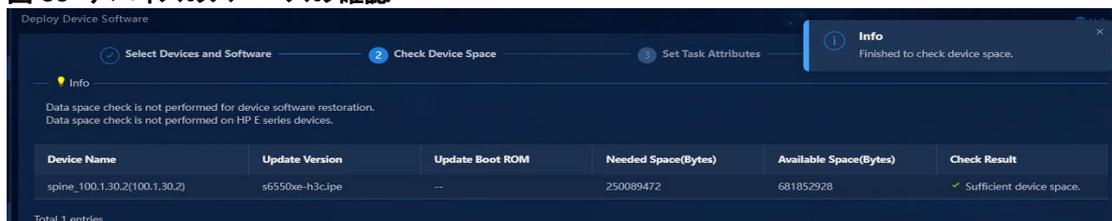
4. アップグレードするデバイスを選択し、展開するソフトウェアを選択します。

図 38 デバイスとソフトウェアの選択



5. デバイスのスペースを確認する。

図 39 デバイスのスペースの確認



6. **Set Task Attributes** を選択し、必要に応じてスケジュール時間を選択します。

図 40 タスク属性の設定

The screenshot shows a dark-themed configuration window with three steps: 'Select Devices and Software', 'Check Device Space', and 'Set Task Attributes' (the active step, indicated by a blue circle with the number 3). The 'Set Task Attributes' section contains the following fields:

- * Task Name:** Task 2022-08-26 14:48:33
- Task Type:** Deploy Device Software
- Schedule Type:** Once
- * Schedule Time:** Scheduled (dropdown), 2022-08-26 15:48:33 (calendar icon)
- Schedule Sequence:** Immediately (dropdown), **Scheduled** (dropdown), Sort (button)
- Error Handling:** Stop Deployment on the Curren... (dropdown)
- Task Description:** Software: s6550xe-h3c.ipe

At the bottom right, there are three buttons: 'Previous', 'Next', and 'Cancel'.

7. 導入設定を確認し、**Finish** をクリックします。

図 41 設定の確認

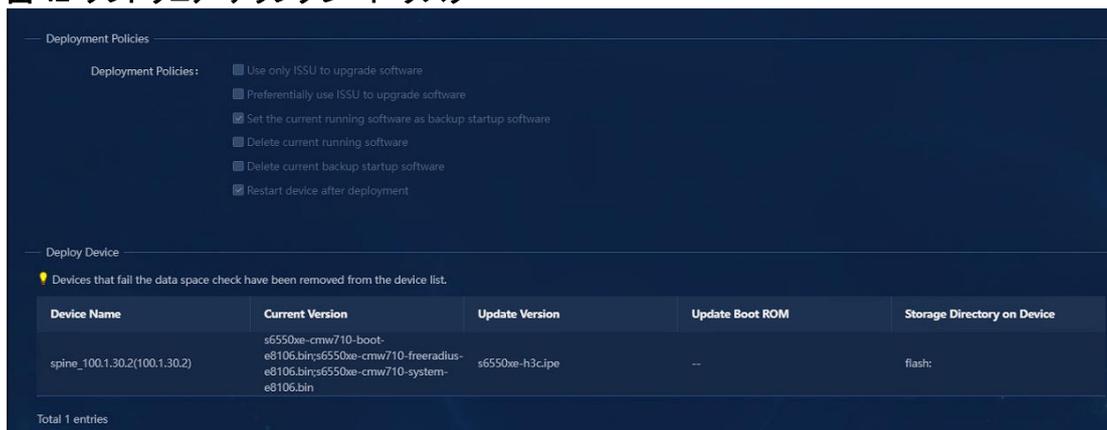
The screenshot shows a dark-themed confirmation window titled 'Task Attributes'. It displays the same configuration as Figure 40:

- Task Name:** Task 2022-08-26 14:48:33
- Task Type:** Deploy Device Software
- Schedule Type:** Once
- Schedule Time:** Scheduled, 2022-08-26 15:48:33
- Schedule Sequence:** Concurrent
- Error Handling:** Stop Deployment on the Curren...
- Task Description:** Software: s6550xe-h3c.ipe

Below the 'Task Attributes' section is a 'Deployment Policies' section with a list of checkboxes:

- Use only ISSU to upgrade software
- Preferentially use ISSU to upgrade software
- Set the current running software as backup startup software
- Delete current running software
- Delete current backup startup software
- Restart device after deployment

図 42 ソフトウェア アップグレード タスク



8. 特定のステップに関する詳細情報を表示するには、**Operation Result** をクリックし、**Details** を選択します。

図 43 演算結果

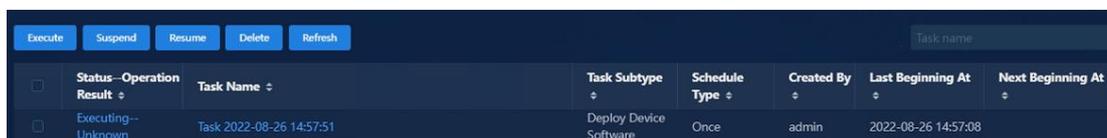


図 44 詳細を表示

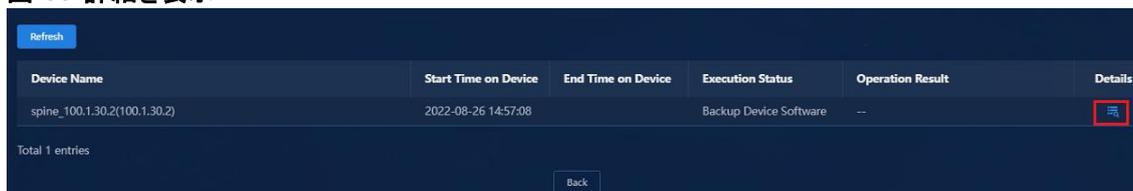


図 45 ステップの詳細

Index	Description	Result	Suggestion
1	Initialize task parameters.	Succeeded.	
2	Back up device's running software to system.	Succeeded.	
3	Delete device's current backup startup software.	Succeeded.	
4	Upload software to device from system.	Succeeded.	
5	Set device's running software as device's backup startup software.	Succeeded.	
6	Set software as device's next startup software.	Succeeded.	
7	Reboot device.	Succeeded.	
8	End to execute task.	Succeeded.	

故障したデバイスの交換

障害が発生したデバイスの交換については、「AD-Campus デバイス交換構成ガイド」を参照してください。

付録

スパイン自動化テンプレート

```
## Please note:The following variable names are used by the internal system,please do not use
## _underlayIntfUp _underlayIntfDown _all_leaf _master_spine
## _master_spine_mac _underlayIPRange
##
##NEW_VERSION
#USERDEF
##Template version
template_version = 5.0
##BACKUP_SERVER
##Local user: Username
_username = admin
##Local user: Password
_password = *****
## User roles
_rbacUserRole = network-admin
##ntp_server_begin_var
##IP address of the NTP server
_ntp_server_0 = 100.1.0.100
##ntp_server_end_var
##MAC address of the master spine device
_master_spine_mac = 586a-b1e5-2600
##MAC address of the master spine device and address range of loopback interfaces
##Format: 1122-3344-5566:10.100.0.0/16, AABB-CCDD-EEFF:10.101.0.0/16
_underlayIPRange = 586a-b1e5-2600:200.1.1.0/24
##MAC address and VLAN ID range of the spine device
##Format: 1122-3344-5566:2-100 ,AABB-CCDD-EEFF:101-200
_underlayVLANRange = 586a-b1e5-2600:3001-3500
##IP address of the log host
_loghost_ip = 110.1.0.100
##is_ipv6_begin_var
##Device is automatically online by ipv6
_is_ipv6 = false
##is_ipv6_end_var
##Out of band
_OOB = False
##SSH enabled
_SSH = True
##Disable automatic IRF setup
_irf_disable = false
##Enabling whitelist filtering (False by default)
white_list_check = true
##Disabling automatic allocation of an underlay IP (False by default)
_ip_disable = false
##Enabling automatic IRF mode switching
_irf_mode_auto_convert = True
##MAD BFD
_mad_vlan = 100
_mad_ip = 192.168.100.1, 192.168.100.2
##BGP AS number
bgp_as_campus = 100
```

```
## OSPF router ID is the IP address of loopback 0
_ad_loopback0_routerid = True
```

```
[H3CS5560X]
driver = 5560X
_switch_mode = 1
```

```
[H3CS6520X]
driver = 6520X
_switch_mode = 1
```

```
[H3CS125??G-AF]
driver = 125GAF
_tcam_resource = arp
_vxlan_resource = l3gw
_routing_mode_resource = ipv6-128
```

```
##
#STATICCFG
#
clock timezone beijing add 08:00:00
#
ip vpn-instance vpn-default
route-distinguisher 1:1
vpn-target 1:1 both
##address_family_evpn_begin
address-family evpn
vpn-target 1:1 import-extcommunity
vpn-target 1:1 export-extcommunity
##address_family_evpn_end
##address_family_ipv6_begin
address-family ipv6
vpn-target 1:1 import-extcommunity
vpn-target 1:1 export-extcommunity
##address_family_ipv6_end
#
lldp global enable
#
interface Vlan-interface1
ip address dhcp-alloc
#
ospf 1
non-stop-routing
fast-reroute lfa
area 0.0.0.0
#
##loopback0_begin_all
interface LoopBack0
##loopback0_end_all
#
interface $$_underlayIntfDown
ip address unnumbered interface LoopBack0
ospf 1 area 0.0.0.0
ospf network-type p2p

#
```

```

netconf soap https enable
netconf ssh server enable
restful https enable
#
ssh server enable
#
info-center loghost $$_loghost_ip
#
stp mode pvst
stp vlan 1 enable
undo stp vlan 2 to 4094 enable
stp global enable
stp vlan 1 priority 0
#
local-user $$_username
password simple $$_password
service-type http https ssh
authorization-attribute user-role $$_rbacUserRole
#
line vty 0 63
authentication-mode scheme
user-role $$_rbacUserRole
#
bgp $$bgp_as_campus
non-stop-routing
address-family l2vpn evpn
ip vpn-instance vpn-default
##address_family_ipv4_unicast_begin
address-family ipv4 unicast
import-route static
##address_family_ipv4_unicast_end
##address_family_ipv6_unicast_begin
address-family ipv6 unicast
import-route static
##address_family_ipv6_unicast_end
#
l2vpn enable
#
vlan 4094
#
interface Vsi-interface4094
ip binding vpn-instance vpn-default
local-proxy-arp enable
##local-proxy-nd_enable_begin
local-proxy-nd enable
##local-proxy-nd_enable_end
arp proxy-send enable
arp send-gratuitous-arp interval 30000
#
interface Vsi-interface4092
ip binding vpn-instance vpn-default
ip address unnumbered interface Vsi-interface4094
##ipv6_address_auto_link_local_begin
ipv6 address auto link-local
##ipv6_address_auto_link_local_end
l3-vni 4092
description SDN_VRF_VSI_Interface_4092

```

```

#
vsi vxlan4094
gateway vsi-interface 4094
vxlan 4094
evpn encapsulation vxlan
mac-advertising disable
nd mac-learning disable
arp mac-learning disable
route-distinguisher auto
vpn-target auto export-extcommunity
vpn-target auto import-extcommunity
##ipv6_dhcp_snooping_trust_tunnel_begin
ipv6 dhcp snooping trust tunnel
##ipv6_dhcp_snooping_trust_tunnel_end
loopback-detection action block
loopback-detection enable vlan 4094
#
vxlan tunnel mac-learning disable
vxlan tunnel arp-learning disable
vxlan tunnel nd-learning disable
#
vcf-fabric topology enable
#
vxlan default-decapsulation source interface LoopBack 0
#
snmp-agent
snmp-agent community read *****
snmp-agent community write *****
snmp-agent sys-info version all
snmp-agent packet max-size 4096
#
telnet server enable
#
netconf soap https enable
netconf soap http enable
local-user admin
password simple *****
service-type telnet ssh http https
authorization-attribute user-role network-admin
#
##l3_static_route_begin_all
ip route-static 110.1.0.0 24 120.1.0.1
ip route-static vpn vpn-default 110.1.0.0 24 130.1.0.1
ip route-static 100.1.0.0 24 120.1.0.1
ip route-static vpn vpn-default 100.1.0.0 24 130.1.0.1
ip route-static 101.0.143.0 24 120.1.0.1
ip route-static vpn vpn-default 101.0.143.0 24 130.1.0.1
ip route-static 192.168.2.0 24 120.1.0.1
ip route-static vpn vpn-default 192.168.2.0 24 130.1.0.1
#
##l3_static_route_end_all
##ipv6_static_route_begin_all
ipv6 route-static vpn vpn-default 2020:130A:0:0:0:0:0:0 64 2020:1:0:0:0:0:1
ipv6 route-static vpn vpn-default 190:0:0:0:0:0:0:0 64 2020:1:0:0:0:0:1
#
##ipv6_static_route_end_all
#

```

```

##ntp_server_begin_cmd
ntp-service enable
ntp-service unicast-server $$_ntp_server_0 vpn-instance vpn-default

#
##ntp_server_end_cmd

```

リーフ自動化テンプレート

```

##
## Please note:The following variable names are used by the internal system,please do not use
## _underlayIntfUp _underlayIntfDown _all_leaf _master_spine _backup_spine
## _master_spine_mac
##
##NEW_VERSION
#USERDEF
##Template version
template_version = 5.0
##Local user: Username
_username = admin
##Local user: Password
_password = *****
## User roles
_rbacUserRole = network-admin
##ntp_server_begin_var
##IP address of the NTP server
_ntp_server_0 = 100.1.0.100
##ntp_server_end_var
##master_leaf_mac_begin_var
##MAC address of the master leaf device
_master_leaf_mac=${master_leaf_mac}
##master_leaf_mac_end_var
##IP address of the log host
_loghost_ip = 110.1.0.100
##is_ipv6_begin_var
##Device is automatically online by ipv6
_is_ipv6 = false
##is_ipv6_end_var
##Out of band
_OOB = False
##Supporting aggregation (True by default)
_lagg_enable = True
##Enforcing aggregation
_lagg_force = True
##Do not delete aggregation group
_lagg_fake_delete = True
##SSH enabled
_SSH = True
##Disable automatic IRF setup
_irf_disable = false
##Enabling whitelist filtering (False by default)

_white_list_check = true
##Enabling automatic IRF mode switching
## Enable OLT interface

```

```

_olt = true
## OSPF router ID is the IP address of loopback 0
_ad_loopback0_routerid = True
## auto IRF mode convert
_irf_mode_auto_convert = True
##MAD BFD
_mad_vlan = 100
_mad_ip = 192.168.100.1, 192.168.100.2
##BGP AS number
bgp_as_campus = 100
##Disable lldp function when MAD BFD
_mad_undo_lldp=True
[H3CS5560X]
driver = 5560X
_switch_mode = 1
[H3CS6520X]
driver = 6520X
_switch_mode = 1
[H3CS125??G-AF]
driver = 125GAF
_tcam_resource = mix
_vxlan_resource = l3gw
_routing_mode_resource = ipv6-128
[UNISS5600X]
driver = 5560X
_switch_mode = 1
[UNISS6600X]
driver = 6520X
_switch_mode = 1
##
#STATICCFG
#
clock timezone beijing add 08:00:00
#
ip vpn-instance vpn-default
route-distinguisher 1:1
vpn-target 1:1 both
##address_family_evpn_begin
address-family evpn
vpn-target 1:1 import-extcommunity
vpn-target 1:1 export-extcommunity
##address_family_evpn_end
##address_family_ipv6_begin
address-family ipv6
vpn-target 1:1 import-extcommunity
vpn-target 1:1 export-extcommunity
##address_family_ipv6_end
#
lldp global enable
#
dhcpsnooping enable vlan 2 to 4094
#
interface Vlan-interface1
ip address dhcp-alloc
#
ospf 1
non-stop-routing

```

```

fast-reroute lfa
area 0.0.0.0
#
##loopback0_begin_all
interface LoopBack0
##loopback0_end_all
#
stp mode pvst
stp vlan 1 enable
undo stp vlan2 to 4094 enable
stp global enable
stp vlan 1 priority 8192
#
netconf soap https enable
netconf ssh server enable
restful https enable
#
ssh server enable
#
info-center loghost $$_loghost_ip
#
local-user $$_username
password simple $$_password
service-type http https ssh
authorization-attribute user-role $$_rbacUserRole
#
line vty 0 63
authentication-mode scheme
user-role $$_rbacUserRole
#
bgp $$bgp_as_campus
non-stop-routing
address-family l2vpn evpn
ip vpn-instance vpn-default
##address_family_ipv4_unicast_begin
address-family ipv4 unicast
##address_family_ipv4_unicast_end
##address_family_ipv6_unicast_begin
address-family ipv6 unicast
##address_family_ipv6_unicast_end
#
interface $$_underlayIntfUp
ip address unnumbered interface LoopBack0
ospf 1 area 0.0.0.0
ospf network-type p2p
#
interface $$_underlayIntfDown
port link-type trunk
port trunk permit vlan 1 4094
##_underlayIntfDown_undo_port_trunk_permit_vlan_mad_position
undo port trunk permit vlan $$_mad_vlan
stp tc-restriction
service-instance 4094
encapsulation s-vid 4094
xconnect vsi vxlan4094
#
interface $$_underlayIntfGe

```

```

poe enable
#
interface $$_underlayIntfONU
port link-type trunk
port trunk permit vlan all
undo port trunk permit vlan $$_mad_vlan
#
interface $$_underlayIntfRONU
port link-type trunk
port trunk permit vlan all
undo port trunk permit vlan $$_mad_vlan
#
l2vpn enable
#
vlan 4094
#
interface Vsi-interface4094
ip binding vpn-instance vpn-default
local-proxy-arp enable
##local-proxy-nd_enable_begin
local-proxy-nd enable
##local-proxy-nd_enable_end
arp proxy-send enable
#
interface Vsi-interface4092
ip binding vpn-instance vpn-default
ip address unnumbered interface Vsi-interface4094
##ipv6_address_auto_link_local_begin
ipv6 address auto link-local
##ipv6_address_auto_link_local_end
l3-vni 4092
description SDN_VRF_VSI_Interface_4092
#
vsi vxlan4094
gateway vsi-interface 4094
vxlan 4094
evpn encapsulation vxlan
mac-advertising disable
nd mac-learning disable
arp mac-learning disable
route-distinguisher auto
vpn-target auto export-extcommunity
vpn-target auto import-extcommunity
##ipv6_dhcp_snooping_trust_tunnel_begin
ipv6 dhcp snooping trust tunnel
##ipv6_dhcp_snooping_trust_tunnel_end
dhcp snooping trust tunnel
loopback-detection action block
loopback-detection enable vlan 4094
#
ip verify source exclude vlan 1
ip verify source exclude vlan 4094
#
vxlan tunnel mac-learning disable
vxlan tunnel arp-learning disable
vxlan tunnel nd-learning disable
#

```

```

vcf-fabric topology enable
#
vxlan default-decapsulation source interface LoopBack 0
#
#
snmp-agent
snmp-agent community read *****
snmp-agent community write *****
snmp-agent sys-info version all
snmp-agent packet max-size 4096
#
telnet server enable
#
netconf soap https enable
netconf soap http enable
local-user admin
password simple *****
service-type telnet ssh http https
authorization-attribute user-role network-admin
#
###3_static_route_begin_all
ip route-static 110.1.0.0 24 120.1.0.1
ip route-static vpn vpn-default 110.1.0.0 24 130.1.0.1
ip route-static 100.1.0.0 24 120.1.0.1
ip route-static vpn vpn-default 100.1.0.0 24 130.1.0.1
ip route-static 101.0.143.0 24 120.1.0.1
ip route-static vpn vpn-default 101.0.143.0 24 130.1.0.1
ip route-static 192.168.2.0 24 120.1.0.1
ip route-static vpn vpn-default 192.168.2.0 24 130.1.0.1
#
###3_static_route_end_all
###ipv6_static_route_begin_all
ipv6 route-static vpn vpn-default 2020:130A:0:0:0:0:0:0 64 2020:1:0:0:0:0:0:1
ipv6 route-static vpn vpn-default 190:0:0:0:0:0:0:0 64 2020:1:0:0:0:0:0:1
#
###ipv6_static_route_end_all
#
###ipv6_dhcp_snooping_enable_begin
ipv6 dhcp snooping enable vlan 2 to 4094
#
###ipv6_dhcp_snooping_enable_end
###ntp_server_begin_cmd
ntp-service enable
ntp-service unicast-server $$ntp_server_0 vpn-instance vpn-default
#

```

Accessオートメーションテンプレート

```

##
## Please note:The following variable names are used by the internal system,please do not use
## _underlayIntfUp _underlayIntfDown _all_leaf_master_spine_backup_spine
## _master_spine_mac
##
#USERDEF
##Template version
template_version = 5.0

```

```

## User roles
_rbacUserRole = network-admin
##ntp_server_begin_var
##IP address of the NTP server
_ntp_server_0 = 100.1.0.100
##ntp_server_end_var
##IP address of the log host
_loghost_ip = 110.1.0.100
##is_ipv6_begin_var
##Device is automatically online by ipv6
_is_ipv6 = false
##is_ipv6_end_var
##Out of band
_OOB = False
##Supporting aggregation (True by default)
_lagg_enable = True
##Enforcing aggregation
_lagg_force = True
##Do not delete aggregation group
_lagg_fake_delete = True
##lagg role limits
_lagg_role_limits = leaf,access
##SSH enabled
_SSH = True
##Disable automatic IRF setup
_irf_disable = false
##Enabling whitelist matching (False by default)
_white_list_check = true
##Disable lldp function when MAD BFD
_mad_undo_lldp=True
#STATICCFG
#
clock timezone beijing add 08:00:00
#
lldp global enable
#
stp global enable
#
netconf soap https enable
netconf ssh server enable
restful https enable
#
interface Vlan-interface1
ip address dhcp-alloc
#
ssh server enable
#
info-center loghost $$_loghost_ip
#
line vty 0 63
authentication-mode scheme
user-role $$_rbacUserRole
#
interface $$_underlayIntfUp
port link-type trunk
port trunk permit vlan all
#

```

```

interface $$_underlayIntfDown
port link-type trunk
undo port trunk permit vlan 1
port trunk pvid vlan 4093
port trunk permit vlan 2 to 4093
#
interface $$_underlayIntfGe
poe enable
#
vlan 4093
#
vlan4094
#
interface Vlan-interface4094
#
#
vcf-fabric topology enable
#
#
snmp-agent
snmp-agent community read *****
snmp-agent community write *****
snmp-agent sys-info version all
snmp-agent packet max-size 4096
#
telnet server enable
#
netconfsoap https enable
netconf soap http enable
local-user admin
password simple *****
service-type telnet ssh http https
authorization-attribute user-role network-admin
#
###l3_static_route_begin_all
ip route-static 110.1.0.0 24 130.1.0.1 preference 50
ip route-static 110.1.0.0 24 120.1.0.1
ip route-static 100.1.0.0 24 130.1.0.1 preference 50
ip route-static 100.1.0.0 24 120.1.0.1
ip route-static 101.0.143.0 24 130.1.0.1 preference 50
ip route-static 101.0.143.0 24 120.1.0.1
ip route-static 192.168.2.0 24 130.1.0.1 preference 50
ip route-static 192.168.2.0 24 120.1.0.1
#
###l3_static_route_end_all
###ipv6_static_route_begin_all
ipv6 route-static 2020:130A:0:0:0:0:0 64 2020:1:0:0:0:0:0:1
ipv6 route-static 190:0:0:0:0:0:0 64 2020:1:0:0:0:0:0:1
#
###ipv6_static_route_end_all
#
###ntp_server_begin_cmd
ntp-service enable
ntp-service unicast-server $$_ntp_server_0
#
###ntp_server_end_cmd

```

O&M モニタリング

O&M モニタリングの詳細については、「AD-Campus Operations Monitoring Deployment Guide」を参照してください。