検証済みプロファイル：エンタープライズおよび政府/自治体（SD-Access）部門

2005 年 10 月 31 日

ソリューションの概要

Cisco Software-Defined Access（SD-Access）は、従来のキャンパス LAN 設計の進化形であり、組織の目的（インテント）をそのまま反映できます。SD-Access は、Catalyst Center ソフトウェアで動作するアプリケーションパッケージです。インテリジェントキャンパスの有線/ワイヤレスネットワークの設計、プロビジョニング、ポリシー適用、および作成を確実に行うことができます。

SD-Access の不可欠な部分であるファブリックテクノロジーにより、有線/ワイヤレスのキャンパスネットワークとプログラム可能なオーバーレイおよび簡単に導入できるネットワーク仮想化を可能にし、設計の意図を満たすように 1 つ以上の論理ネットワークをホストする物理ネットワークを実現します。

エンタープライズ市場セグメントは、政府または自治体、金融、医療、小売など、さまざまな業種に分類できます。このドキュメントは、政府または自治体の部門を対象としています。

エンタープライズおよび政府/自治体環境では、通常、メインファブリックサイトに多数のデバイスとエンドポイントが含まれます。このソリューションは、ファブリック自動化のあらゆる導入例と大規模環境でのアシュアランスを検証することに焦点を当てています。重要な要素は次のとおりです。

- 最大限のファブリックの規模を持つエンドツーエンドのソリューション展開
- 共通の Cisco Identity Services Engine（Cisco ISE）クラスタを使用する複数の Catalyst Center インスタンス

  政府または自治体の大規模な展開では、複数の Catalyst Center インスタンスが必要になります。マルチ Catalyst Center 機能を使用すると、複数の Catalyst Center を同じ Cisco ISE クラスタと統合できます。すべての仮想ネットワーク、セキュリティグループ、アクセス契約、セキュリティポリシーが作成され、Catalyst Center 間で共有されます。この操作はプライマリノード（作成者ノード）を介して実行され、Cisco ISE およびその他の Catalyst Center にプッシュされます。

- IPv6 への移行

  デバイスは IPv6 上で実行されることが増えていますが、ネットワーク インフラストラクチャは IPv4 上に維持されると考えられます。Catalyst Center は、IPv6 への移行のシームレスなワークフローを提供します。

- ワイヤレスへの移行（ワイヤレス OTT の展開からファブリックワイヤレスへの移行）。

  大企業の展開では、SD-Access ネットワークへの段階的な移行が採用される場合があります。最初に有線ネットワークが移行されます。従来のワイヤレスネットワークは、ファブリック有線ネットワーク上で実行されます。このタイプのネットワークは、ワイヤレス オーバーザトップ オブ ファブリック（ワイヤレス OTT）と呼ばれます。次の段階で、ファブリック ワイヤレス ネットワークに移行して有効化します。

- Cisco Catalyst Assurance

  アシュアランスは、エンドツーエンドのネットワーク全体にわたるユーザとアプリケーションの実際のエクスペリエンスを可視化します。

ハードウェアとソフトウェアの仕様

ソリューションは、次の表に示すハードウェアとソフトウェアで検証されています。

ロール	ハードウェア プラットフォーム	ソフトウェア リリース	
Cisco Catalyst Center コントローラ	DN2-HW-APL-XL	2.3.7.7	2.3.7.9
アイデンティティ管理、RADIUS サーバー	ISE-VM-K9	3.3 パッチ 4	3.3 パッチ 4
Cisco SD-Access ファブリックボーダー	C9500-24Y4C	17.9.5、17.12.4	17.9.6a、17.12.5、17.15.3
Cisco SD-Access ファブリックエッジ	C9500-40X, C9404R, C9300	17.9.5、17.12.4	17.9.6a、17.12.5、17.15.3
Cisco SD-Access 中継ノード	C9500-24Y4C	17.9.5、17.12.4	17.9.6a、17.12.5、17.15.3
シスコ ワイヤレス コントローラ	C9800-80-K9 AIR-CT-8540	17.9.6、17.12.4 8.10.190.0	17.9.6、17.12.5 8.10.190.0
シスコアクセスポイント	C9115AX, C9120AX, C9130AX AIR-AP-3800, AIR-AP-4800	17.9.6、17.12.4 8.10.190.0	17.9.6、17.12.5 8.10.190.0

ソリューションの導入例のシナリオ

この検証済みソリューションは、次の自動化およびアシュアランスの導入例をサポートします。

自動化の導入例

- 政府または自治体の大規模なファブリックサイトの展開
- LAN 自動化を使用したファブリックデバイスのオンボーディング
- 仮想ネットワークおよび IP セグメントの追加
- IP および TCP 伝送
- マルチキャストの有効化
- 同じ Cisco ISE クラスタとのマルチ Catalyst Center 統合
- 仮想ネットワーク、セキュリティグループタグ、アクセス契約、セキュアなポリシーの作成
- Catalyst Center 間でのロール変更（作成者ノードの昇格）
- ポリシーの適用と認可変更（COA）
- ワイヤレス OTT の展開とファブリックワイヤレスへの移行
- IPv4 専用ネットワークからデュアルスタック ネットワークへの移行
- 有線およびワイヤレス ファブリック デバイス イメージのアップグレードの検証
- 有線およびワイヤレスデバイスを含む、サイトレベルのデバイスイメージのアップグレード
- Catalyst Center 3 ノードクラスタのアップグレードの検証
- Catalyst Center の 2.3.5.6 から 2.3.7.7 へのアップグレード
- ネットワークとサービスのフェールオーバー/冗長性の検証
- Catalyst Center の高可用性
- ISE PAN、PSN、pxGrid サービスのフェールオーバー
- クリティカル VLAN で到達不能な ISE
- ボーダー SVL とアクセススイッチスタックのフェールオーバー
- ファブリックデバイスの RMA ワークフローと AP 更新ワークフロー
- ファブリックデバイスと障害のある AP RMA
- Wav2 AP から 11ax AP への AP 全体の交換
- ファブリックの規模とパフォーマンス

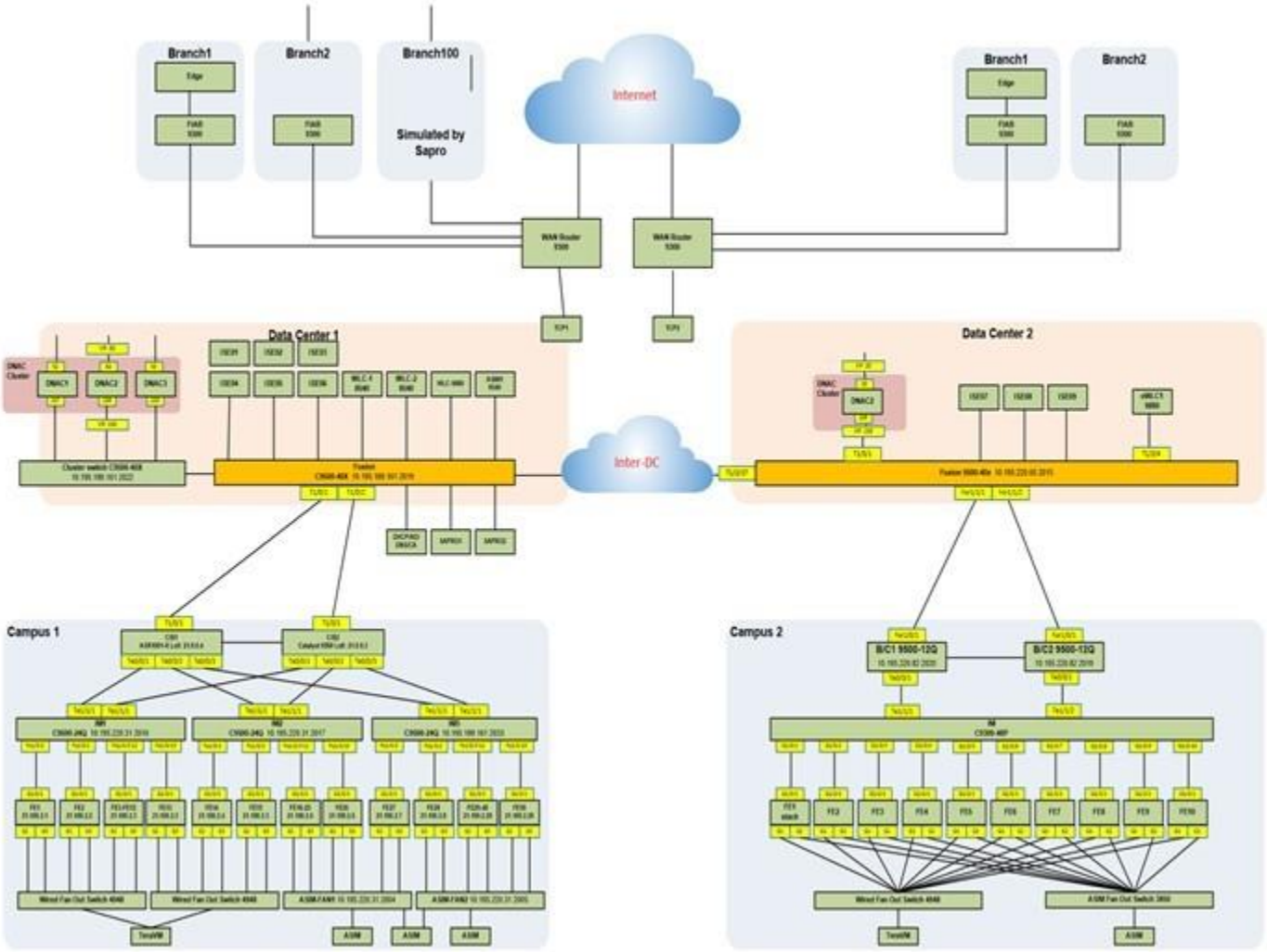
アシュアランスの導入例

- デュアルスタック ファブリック クライアントのオンボーディング
- 有線およびワイヤレス デュアルスタック クライアントのオンボーディング
- クライアントダッシュボードには、オンボーディングされたクライアントデバイスのリストが、適切な正常性スコアおよびその他すべての必要とされる情報とともに表示されます
- ネットワークデバイスのオンボーディング
- ネットワークダッシュボードには、オンボーディングされたネットワークデバイスのリストが、適切な正常性スコアおよびその他すべての必要とされる情報とともに表示されます
- アシュアランスの問題のレポート
- ネットワークデバイスのリンクダウン問題の発生
- AP ダウン問題の発生
- スタックメンバのダウン
- クライアントの正常性の詳細
- アシュアランスチャート、[クライアントの正常性（Client Health）] ページ
- アシュアランスチャート、[Client 360] ページ
- ネットワークの正常性の詳細
- アシュアランスチャート、[ネットワークの正常性（Network Health）] ページ
- アシュアランスチャート、[Device 360] ページ
- ファブリックアシュアランス
- ファブリックの正常性スコアとアシュアランスチャート、[ファブリックの正常性（Fabric Health）] ページ
- アシュアランスと拡張性
- アシュアランスチャート、300,000 の同時エンドポイントと 750,000 の一時エンドポイント
- 耐用期間/ソークテスト

ソリューション環境

トポロジ

次のトポロジは、大企業および政府または自治体における展開環境を示しています。



コントローラによる統合：

- データセンター 1：3 ノード x 1、112 コア Catalyst Center クラスタ、ISE PAN/MNT x 2、PSN ノード x 3。
- データセンター 2：単一ノード x 1、112 コア Catalyst Center、ISE PSN ノード x 3。
- 共有サービスには、DNS、DHCP、AD、NTP、HTTP、TFTP、およびバックアップサーバが含まれます。WLC は共有サービスにも存在します。

2 つの大規模なファブリック キャンパス サイト：

- キャンパス 1：デュアルファブリック ボーダー/CP、1000 ファブリックエッジ、1000 IP セグメント。
- キャンパス 2：SVL をサポートするボーダー、1000 ファブリックエッジ、600 IP セグメント。
- ブランチ：中継 CP ノード（キャンパスごとに 1 つ）を介してキャンパスと通信するブランチの FIAB。

- 両方のキャンパスには、多数のシミュレーション ファブリック ノード、AP、およびシミュレーション有線/ワイヤレス エンドポイントが含まれます。

スケール

ソリューションのテストでは、次の表に示すスケールの数値について確認しました。ハードウェアのキャパシティについては、『Cisco Catalyst Center Data Sheet』を参照してください。

属性	値	注
Catalyst Center クラスタ	4	3 ノードクラスタ x 1 と単一ノード x 1、112 コアアプライアンス
Cisco ISE クラスタ	8	PAN/MNT x 2、PSN x 6（pxGrid x 2 を含む）
インベントリのデバイス数	10,000	ルータ、スイッチ、ワイヤレスコントローラ
ファブリックあたりのデバイス数	1054	ボーダー/コントロールプレーン x 2 + スイッチ x 50 + シミュレートスイッチ x 950 ファブリックボーダー/コントロールプレーン x 2 + ファブリックエッジノード x 50 + シミュレートスイッチ x 1,000 + ワイヤレスコントローラ x 2
スタティックホストポート	700,000	物理インターフェイス x 700,000
ネットワーク階層内のサイト要素数	10,000	エリア、ビルディング、およびフロア
ファブリック内の VN	256	—
ファブリックサイト内の IP プール	1000	IP セグメント x 1000
ファブリックサイトのワイヤレスコントローラ	2	C9800-80 x 1 AIR-CT-8540 x 1
SSID	10	—
インベントリの AP	25,000	—
ファブリックサイトの AP	6000	—
エンドポイント	300,000	200,000 有線 100,000 ワイヤレス
マルチ Catalyst Center 環境の Catalyst Center	2	—
SGT	400	—
ACA ポリシー	25,000	—

動作	パフォーマンスの測定結果（分単位）
IP セグメントの追加	35
IP セグメントの削除	26
ファブリックエッジノードの追加	28
ファブリックエッジノードの削除	15
外部ボーダー/コントロールプレーンの追加	48
外部ボーダー/コントロールプレーンの削除	37
VN でのマルチキャストの有効化	50
VN でのマルチキャストの無効化	40
1 つの IPv4 セグメントでの IPv6 の有効化	35
100 AP のプロビジョニング	4
SWIM を介した 50 スイッチへのイメージの配信	21
SWIM を介した 50 スイッチでのイメージのアクティブ化	40
マルチ Catalyst Center ロールの変更（同期時間を含む）	33（4000 SGT）
Catalyst Center のバックアップ	Fusion データ：22（46 GB）

ベストプラクティスと推奨事項

ここでは、ソリューションの展開に役立つテクニカルノートについて説明します。

ワイヤレス OTT の移行

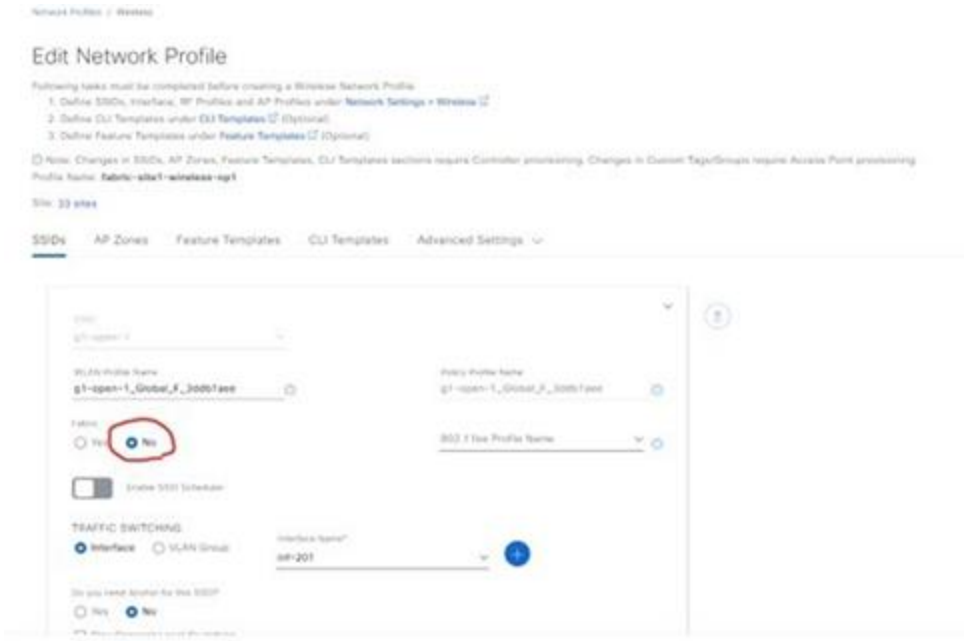
ワイヤレス OTT は、SD-Access ファブリック上で実行される従来のワイヤレスです。このモードは、有線ネットワーク上で SD-Access を最初に実装し、次にワイヤレス統合を計画しているお客様向けの移行手順として重要です。OTT 展開を SD-Access ワイヤレスネットワークに移行する場合は、ワイヤレスネットワークの SSID 名を同じに保つために、以下の手順を実行してください。

手順 1。 移行中にワイヤレスネットワークの SSID 名を同じに保つには、次の手順を実行します。

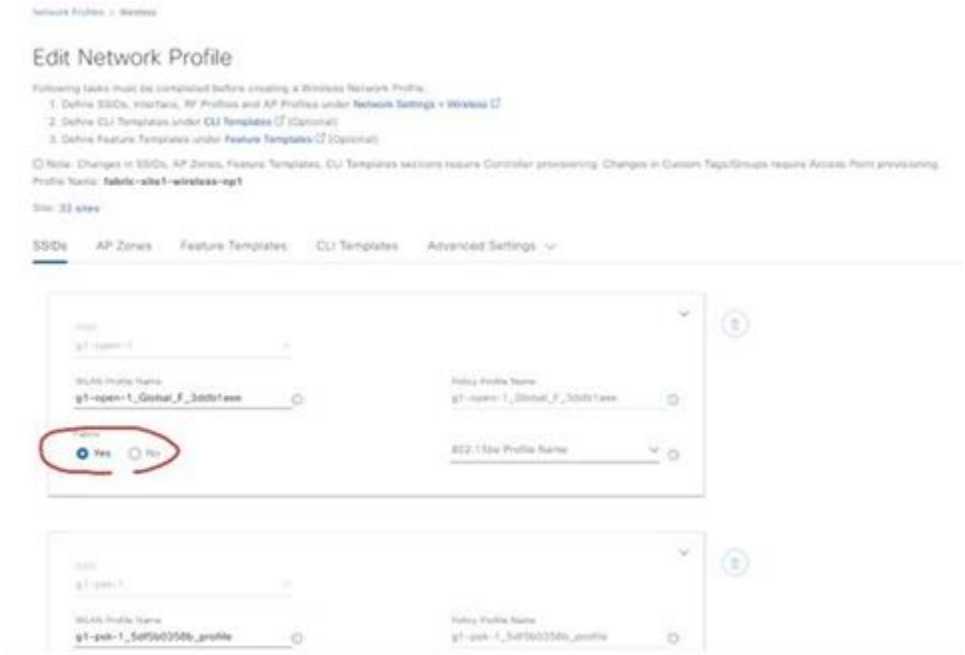
ステップ 1. [Fabric] ページで、ワイヤレスコントローラをファブリックサイトに追加します。

ステップ 2. OTT と同じ SSID をファブリックネットワークで維持します。新しいネットワークプロファイルを作成し、このプロファイルでファブリックを有効にして同じ SSID を追加してください。

OTT ネットワークの元のネットワークプロファイル：



ファブリックワイヤレスの新しいネットワークプロファイル（同じ SSID でファブリックが有効）：



ステップ 3. フロアを新しいネットワークプロファイルに割り当てます。

ステップ 4. 新しいネットワークプロファイルを使用してワイヤレスコントローラを再プロビジョニングします。これにより、古い非ファブリック SSID が削除され、新しいファブリック SSID が生成されます。

ステップ 5. [ホストのオンボーディング（Host Onboarding）] > [ワイヤレス SSID（Wireless SSID）] ページで、ファブリックの SSID にワイヤレスプールを割り当てます。これにより、ワイヤレスコントローラのファブリック SSID が有効になります。

ステップ 6. 割り当てたフロアの AP を再プロビジョニングします。AP が再起動し、ファブリック SSID のブロードキャストを開始します。ファブリックエッジノードのファブリック AP ごとにアクセストンネルが作成されます。

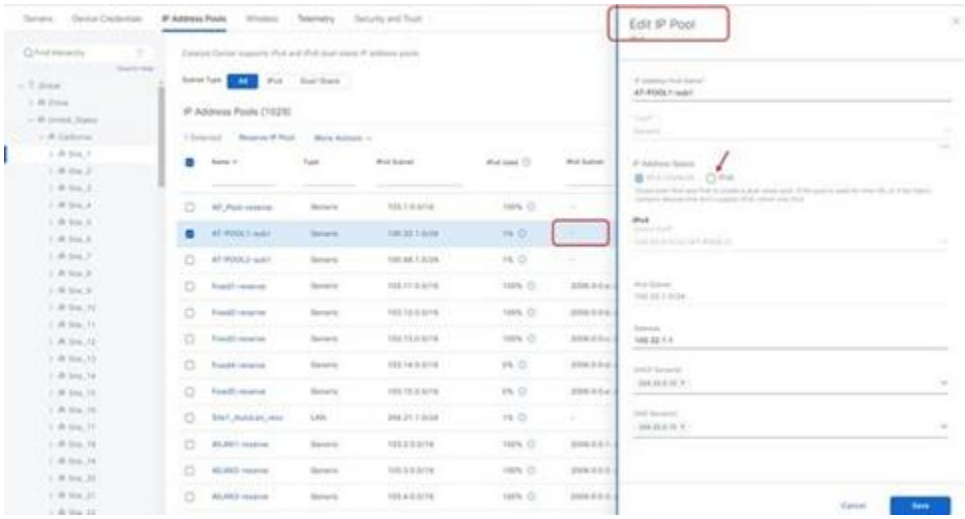
IPv6 への移行（デュアルスタック対応）

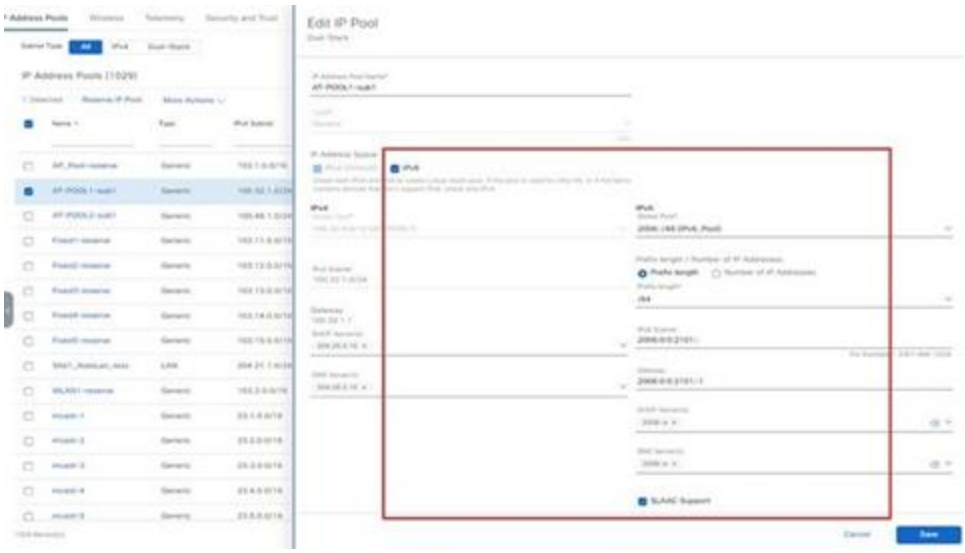
多くの展開では、IPv4 専用セグメントがあります。この手順は IPv6 に推奨されます。

手順 1。 IPv6 をサポートするデュアルスタック環境に移行するには、次の手順を実行します。

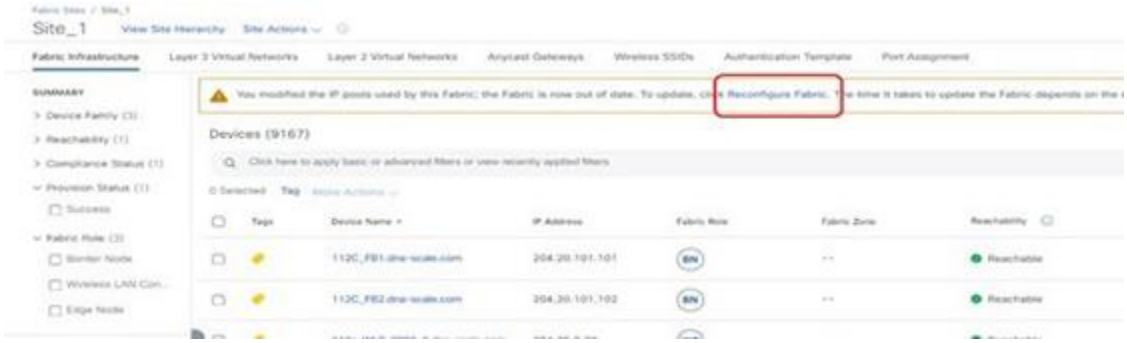
ステップ 1. IPv6 グローバルプールを作成します。

ステップ 2. IPv4 プールを選択し、IPv6 プールを使用して編集します。



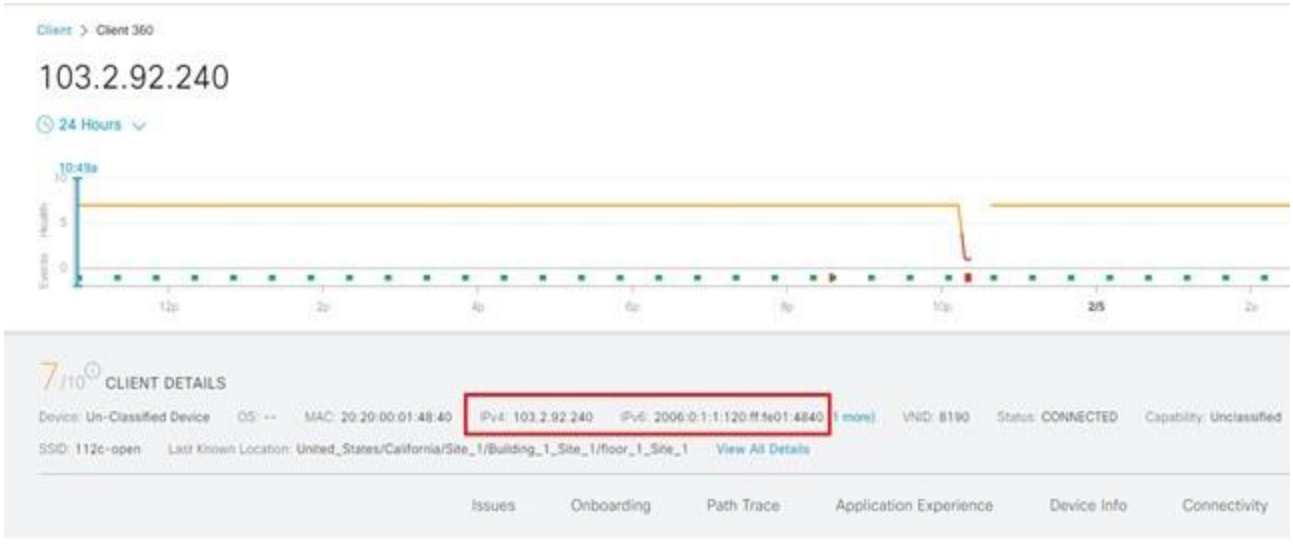


ステップ 3. プール情報が保存されると、Catalyst Center がアラートを [ファブリック（Fabric）] ページに追加します。プロンプトで、ファブリックを再設定します。



ステップ 4. プロビジョニングの完了後、ホストとエンドポイントをオンボーディングします。オンボーディングしたホストには、IPv4 アドレスと IPv6 アドレスの両方が設定されます。

ステップ 5. [アシュアランス（Assurance）] ページで、デュアルアドレスを確認します。

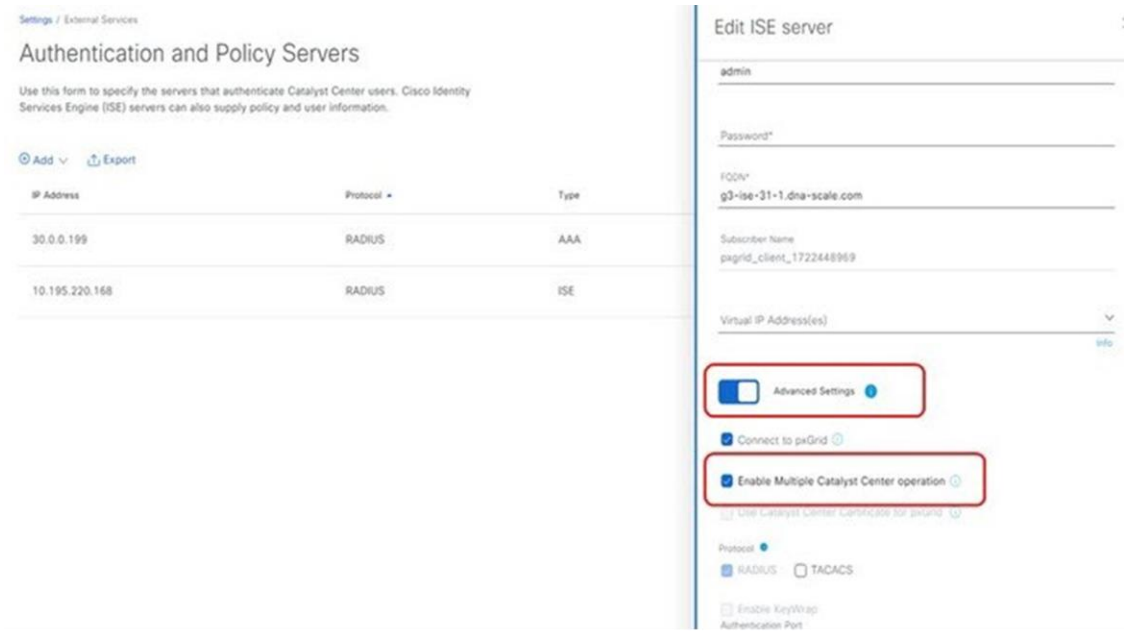


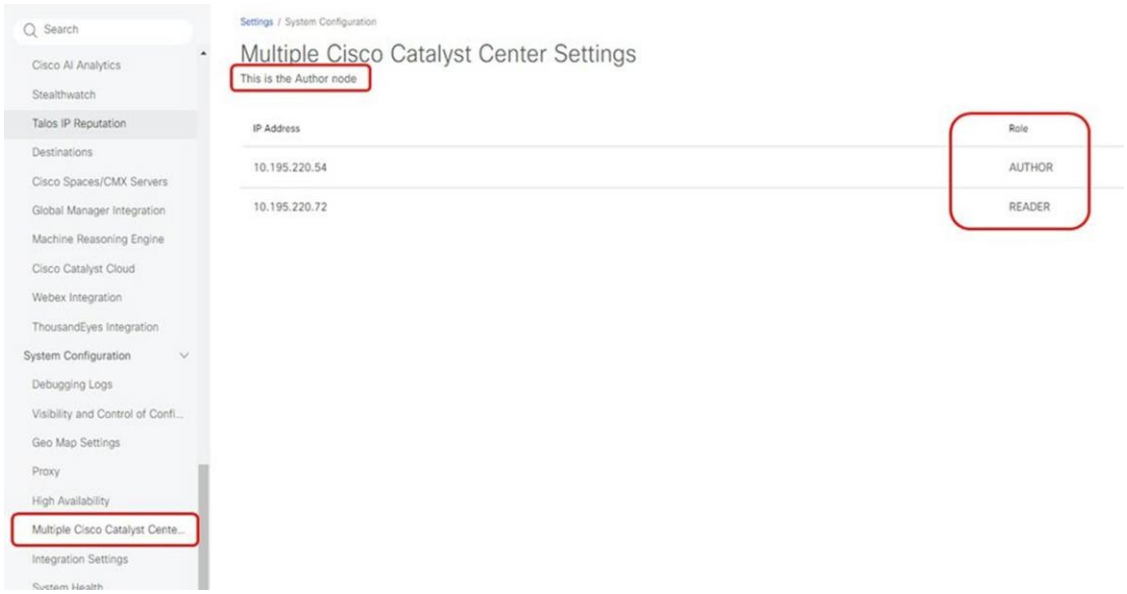
マルチ Catalyst Center 展開

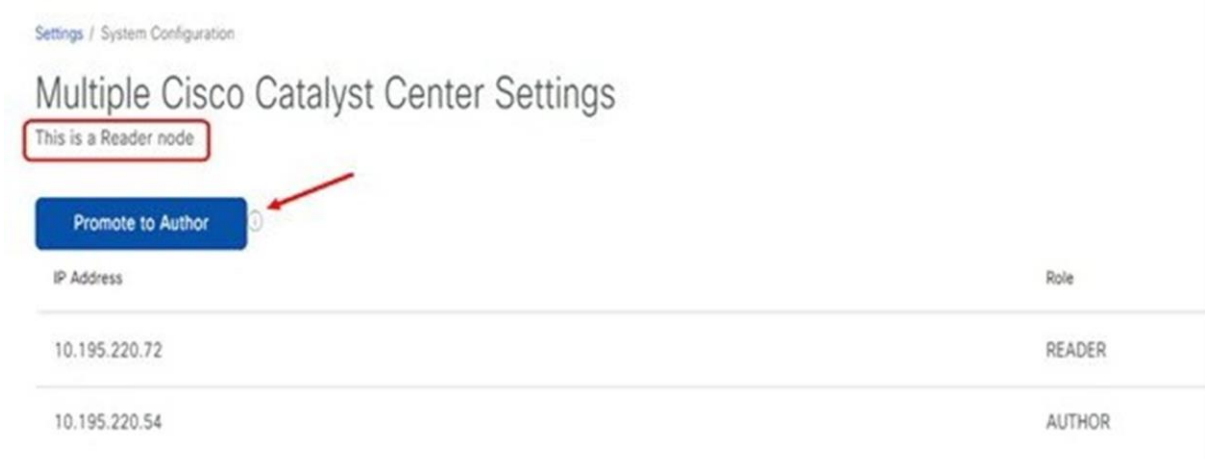
Catalyst Center システムは、25,000 ～ 100,000 エンドポイント（44 コアアプライアンスの場合は 25,000、56 コアアプライアンスの場合は 40,000、112 コアアプライアンスの場合は 100,000）を超えて拡張することはできません。Cisco ISE は 2,000,000 エンドポイントにまで拡張できます。リリース 1.3.3.x 以前では、1 つの Catalyst Center システムは 1 つの Cisco ISE システムとしか統合できませんでした。現在では、大規模な Cisco ISE 展開では、複数の Catalyst Center クラスタを 1 つの Cisco ISE に統合することでメリットが得られます。この機能を Catalyst Center のアクセス制御アプリケーションとともに使用すると、1 つの Cisco ISE システムに最大 4 つの Catalyst Center クラスタを統合できます。

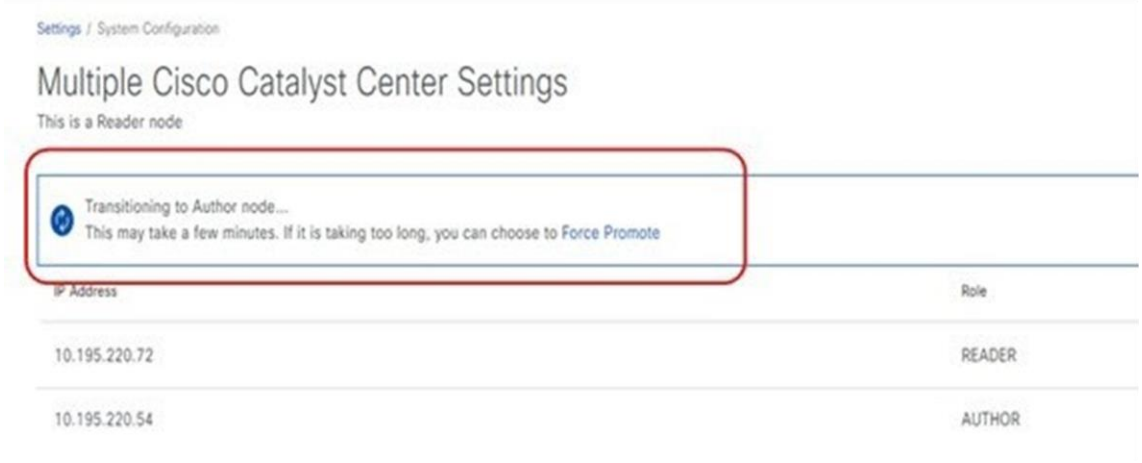
マルチ Catalyst Center 展開に関して理解する必要がある情報：

- この機能は、Catalyst Center 2.3.7.x 以降に組み込まれており、Cisco ISE 3.2 以降と統合されます。[設定（Settings）] ページで機能を有効にする必要があります。それ以外の場合、機能を有効にするには、multi-dnac-enablement アプリケーションパッケージをインストールする必要があります。
- マルチ Catalyst Center 展開で、同じ Cisco ISE クラスタと統合するには、すべての Catalyst Center クラスタが同じリリースである必要があります。Catalyst Center の異なるリリースをマルチ Catalyst Center 展開で混在させることはできません。
- multi-dnac-enablement パッケージと依存関係にあるパッケージは、アクセス制御アプリケーション（ACA）パッケージです。multi-dnac-enablement パッケージをインストールする前に、ACAパッケージをインストールする必要があります。
- 1 つの Cisco ISE システムと複数の Catalyst Center クラスタを含む展開では、作成者ノードでのみ SDA ポリシーオブジェクトを管理できます。Cisco ISE と統合する最初の Catalyst Center クラスタが作成者ノードロールを担うことになります。作成者ノードは、仮想ネットワーク、スケーラブルグループ、アクセス契約、ポリシー、およびスケーラブルグループと仮想ネットワークの関連付けに対する単一の管理ポイントです。リーダーノードには、仮想ネットワーク、スケーラブルグループ、およびスケーラブルグループ間の仮想ネットワークの関連付けに対する読み取り専用ビューがあります。リーダーノードでは、アクセス契約またはポリシーは表示できません。リーダーノードには、作成者ノードへの相互起動リンクがあります。
- Cisco ISE システムとの統合が完了したら、[システム（System）] > [設定（Settings）] > [複数 Cisco DNA Center 設定（Multiple Cisco DNA Center Settings）] ページで、作成者ノードおよびリーダーノードのロールステータスを確認できます。
- リーダーノードを作成者ノードに昇格させて、現在の作成者ノードを置き換えることができます。昇格後、新しい作成者ノードでは、ポリシーデータについて Cisco ISE データベースの再同期を実行する必要があります。クラスタに多数の SGT がある場合、再同期時間が長くなります。再同期の完了後、新しい作成者ノードを使用して、展開全体のすべてのアクセス コントロール ポリシーを管理できます。









保証

Catalyst Center ホームページの [アシュアランスの概要（Assurance Summary）] ダッシュボードには、ネットワークの全体的な正常性ステータスが表示されます。

手順 1。 Catalyst Center ホームページで [アシュアランスの概要（Assurance Summary）] を表示するには、次の手順を実行します。

- このダッシュボードから、[アシュアランスの全体（Assurance Overall）] ページまたは [アシュアランスの問題（Assurance Issues）] ページにドリルダウンします。

手順 2。 [アシュアランスの全体（Assurance Overall）] ページを使用するには、次の手順を実行します。

ステップ 1. メインメニューから、[アシュアランス（Assurance）] > [正常性（Health）] を選択すると、ネットワークデバイスとクライアントの集約された正常性情報が表示されます。

デフォルトビューには、過去 7 日間のデータが表示されます。

ステップ 2. 過去 3 時間または 24 時間に表示を調整します。

手順 3。 [ネットワークの正常性（Network Health）] ページを表示するには、次の手順を実行します。

- メインメニューから、[アシュアランス（Assurance）] > [正常性（Health）] を選択します。[ネットワーク（Network）] をクリックします。

  [ネットワークの正常性（Network Health）] ページには、次のセクションがあります。

  - [ネットワークデバイスの到達可能性（Network Device Reachability）]
  - [高干渉の上位 N の AP（Top N APs by High Interference）]
  - [AP のアップ/ダウン合計（Total APs Up/Down）]
  - [クライアントカウント別の上位 N の AP（Top N APs by Client Count）]
  - [PoE 動作状態の分布（PoE Operational State Distribution）]
  - [PoE 受電デバイスの分布（PoE Powered Device Distribution）]
  - [PoE インサイト（PoE Insights）]

手順 4。 [クライアントの正常性（Client Health）] ページを表示するには、次の手順を実行します。

- メインメニューから、[アシュアランス（Assurance）] > [正常性（Health）] を選択します。[Client] タブをクリックします。

  [Client Health] ページには、[Wireless Clients] および [Wired Clients] のセクションがあります。

  [ネットワークの正常性（Network Health）] ページには、次のパネルがあります。

  - [クライアントのオンボーディング時間（Client Onboarding Times）]
  - [RSSIの接続（Connectivity RSSI）]
  - [SNR の接続（Connectivity SNR）]
  - [クライアントのローミング時間（Client Roaming Times）]
  - [SSID ごとのクライアント数（Client Count per SSID）]
  - [接続性物理リンク（Connectivity Physical Link）]

手順 5。 [Device 360] ページを表示するには、次の手順を実行します。

- メインメニューから、[プロビジョニング（Provision）] > [インベントリ（Inventory）] を選択します。デバイスをクリックし、[View 360] をクリックします。

手順 6。 [Client 360] ページを表示するには、次の手順を実行します。

- メインメニューから、[アシュアランス（Assurance）] > [正常性（Health）] を選択します。[Client] タブをクリックします。

  [Client 360] ページに、クライアントデバイスの 360 度ビューが表示されます。

手順 7。 ファブリックオーバーレイに提供される分析情報を理解します。

ファブリックオーバーレイのすべてのチャートは、[Device 360] ページと [Client 360] ページで使用できます。

- ファブリック到達可能性：すべてのファブリックノード間の接続チェック
- ファブリックデバイス：ファブリックノードのマッピングエントリ、プロトコル、パフォーマンス
- ファブリッククライアント：クライアント オンボーディングと共有サービス（DHCP、DNS、AAA、RADIUS）

アシュアランスのトラブルシューティング

- 複数のアシュアランスダッシュボードにデータが表示されない場合は、**`magctl appstack status`** コマンドを使用して、すべてのアシュアランスサービスが実行されていることを確認します。Flink ツールを使用して、すべてのアシュアランスパイプラインが実行されていることを確認します。
- [Network Health] ページで断続的にデータが表示されなくなる場合は、Network-health プロセッサまたは Grafana の Graph-Writer LAG を確認します。
- 有線クライアントで正しい詳細が表示されない場合は、Grafana の Wired Pipeline LAG を確認します。

Catalyst Center エアギャップのアップグレード

一部の政府機関では、クラウド環境での管理ソリューションの展開を制限する厳密なセキュリティ要件があります。Catalyst Center はオフラインでのソフトウェアアップデートをサポートしており、Cisco Connected Cloud にアクセスすることなく、セキュアなエアギャップネットワークに展開されている Catalyst Center アプライアンスを最新の Catalyst Center ソフトウェアおよびアプリケーションバージョンに更新できます。エアギャップ環境で Catalyst Center アプライアンスをアップグレードするには、『*Cisco Catalyst Center Standard Air Gap Deployment Guide*』の「2.3.5.x or 2.3.6.x to 2.3.7.x」の章を参照してください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。