



Cisco DNA Center 1.3.3 SD-Access ワイヤレス設計および 導入ガイド

SD-Access	2
SD-Access ワイヤレス	
SD-Access ワイヤレスアーキテクチャ	5
Cisco DNA Center を使用した SD-Access ワイヤレスのセットアップ	15
SD-Access の設計	
SD-Access のポリシー	
SD-Access オーバーレイのプロビジョニング	
SD-Access ワイヤレス:内部の仕組み	85
SD-Access のワイヤレス統合の設計	89
SD-Access ワイヤレスゲストアクセス設計	
SD-Access ワイヤレスでのマルチキャスト	100
SD-Access ワイヤレスのハイアベイラビリティ	
付録:SD-Access ワイヤレス機能の詳細情報	108

改訂日:2020年3月13日

エグゼクティブサマリー

デジタル化は、あらゆる業界のビジネスを変革しています。その結果、すべての企業が IT 企業への転換を迫られてい ます。調査によると、デジタルを使いこなす企業は収入を増やすだけでなく、平均で 29 % 以上も収益性を高めてい ます(出典:Leading Digital)。この変革はきわめて重要で差し迫った事態です。というのも、企業の 40 % は淘汰さ れる危険にさらされているからです(出典:Digital Vortex)。

Cisco Digital Network Architecture (Cisco DNA Center)は、以下の機能を提供する一連の設計原則に基づいて構築された、オープンなソフトウェア主導型アーキテクチャです。

- ・ビジネス革新の高速化を促進するインサイトとアクション
- ・ビジネスとユーザの期待に応えながら、コストと複雑さを低減する自動化とアシュアランス
- ・組織の継続的な拡大や成長に伴うリスクを低減するセキュリティとコンプライアンス

Cisco[®] Software-Defined Access (SD-Access) は Cisco DNA の重要な構成要素であり、シスコのお客様に、Cisco DNA の原則と利点を提供します。

SD-Access

SD-Access はシスコの次世代エンタープライズ ネットワーキング アクセス ソリューションであり、セキュリティ、セグ メンテーション、および柔軟性の高いサービスロールアウトをファブリックベースのインフラストラクチャで統合でき るように設計されています。優れた GUI エクスペリエンスが特長で、Cisco DNA Center アプリケーションによってネッ トワーク プロビジョニングを自動化します。構成、プロビジョニング、トラブルシューティングなどの日常的なタスク を自動化することで、ネットワークの適応時間を短縮し、問題解決を改善するとともに、セキュリティ侵害の影響を軽 減します。これらの利点によって、ビジネスの CapEx および OpEx を大幅に節約できます。

図1は、SD-Accessの利点をまとめたものです。

図 1. SD-Access の利点



このドキュメントでは、SD-Access のワイヤレス統合に重点を置いています。読者は SD-Access ファブリックの概念 とこのネットワークアーキテクチャの主要コンポーネントに精通していることが想定されています。

SD-Access 機能の詳細については、SD-Access サイト (https://www.cisco.com/c/ja_jp/solutions/enterprisenetworks/software-defined-access/index.html) および『SD-Access 設計ガイド』(シスコ検証済みデザイン(CVD))を 参照してください。

SD-Access ワイヤレス

SD-Access ワイヤレスは、ファブリックおよび Cisco DNA Center による自動化の利点をすべて得ることを目的に、 SD-Access アーキテクチャにワイヤレスアクセスを統合します。

SD-Access ワイヤレスの利点には次のようなものがあります。

- ・集中管理型ワイヤレス コントロール プレーン: Cisco Unified Wireless Network 導入環境で提供されている革新的 な RF 機能が、SD-Access ワイヤレスでも活用されます。IT 導入を簡素化させる無線リソース管理 (RRM)、ク ライアント オンボーディング、クライアントモビリティなどに関して、ワイヤレスの運用は Cisco Unified Wireless Network の場合と同じです。
- ・分散型データプレーンの最適化:データプレーンは、トラフィックの分散に通常伴う処理(VLAN のスパニン グ、サブネット化、大規模なブロードキャストドメインなど)なしに最適なパフォーマンスと拡張性を実現する ために、エッジスイッチに分散されます。
- ・場所を問わないシームレスなレイヤ2ローミング: SD-Access ファブリックにより、クライアントは同じ IP アドレスを保持しながらキャンパス全体でシームレスにローミングできます。
- ・ゲストおよびモビリティのトンネリングの簡素化:アンカー ワイヤレス コントローラ (WLC) が不要になり、 フォーリンコントローラをホッピングせずにゲストトラフィックをネットワークエッジ (DMZ) に直接送信でき ます。
- ・ポリシーの簡素化: SD-Access では、ポリシーとネットワークの構成体 (IP アドレスや VLAN) との間の依存関係が解消されるため、有線クライアントとワイヤレスクライアントのポリシーを定義および実装する方法がシンプルになります。
- ・セグメンテーションの簡略化:セグメンテーションはファブリック内をエンドツーエンドで伝達され、仮想ネットワーク ID (VNI) とスケーラブルグループタグ (SGT) に基づいて階層化されます。有線とワイヤレスの両方のユーザに同じセグメンテーションポリシーが適用されます。

次の事項を維持しながらこれらすべての利点を獲得できます。

- ・将来に備えた Wi-Fi 6 アクセスポイント (AP)、802.11 Wave 1、802.11ac Wave 2 AP、Cisco 3504、5520、8540、C9800-40、C9800-80、C9800-CL、および EWC (Catalyst 9300、9400、9500 で実行されている 9800 ソフトウェア)を含む最高クラスのワイヤレス。
- •既存の AireOS WLC をサポートし、**投資を保護する**。SD-Access ワイヤレスは 802.11ac Wave 2 AP に最適化され ていますが、Wave 1 AP もサポートしています。

図 2. SD-Access ワイヤレスの利点



SD-Access のワイヤレス統合

SD-Access ファブリックに基づく有線ネットワークを使用しているお客様には、ワイヤレスアクセスを統合するための2つのオプションがあります。

- SD-Access ワイヤレス アーキテクチャ
- Cisco Unified Wireless Network ワイヤレスオーバーザトップ (OTT)

SD-Access ワイヤレスオプションは、ワイヤレスユーザとモノのためにファブリックの利点を最大限に活用している ため、最初に検討してみましょう。最初にアーキテクチャと主要なコンポーネントを紹介し、その後、Cisco DNA Center を使用して SD-Access ワイヤレスネットワークを設定する方法を説明します。

OTT は基本的に、ファブリック有線ネットワーク上で従来のワイヤレスを実行します。このオプションについては、 設計上の考慮事項を含め後に本書で説明でされます。

SD-Access ワイヤレスアーキテクチャ

図3は、全体的なSD-Access ワイヤレスアーキテクチャを示しています。

図 3. SD-Access ワイヤレスアーキテクチャ



SD-Access ワイヤレスでは、コントロールプレーンが集中管理されます。つまり、Cisco Unifieid Wireless Network と同 様に、AP と WLC の間で Control and Provisioning of Wireless Access Points (CAPWAP) トンネルが維持されます。主な 違いは、SD-Access ワイヤレスではデータプレーンはファブリック対応 AP から直接 Virtual Extensible LAN (VXLAN)を使用して分散されることです。WLC と AP は、ファブリックに統合されて、AP は、「特別な」クライ アントとしてファブリックオーバーレイ (エンドポイント ID スペース)ネットワークに接続されます。

SD-Access ワイヤレスアーキテクチャのコンポーネント

図 4 は、SD-Access ワイヤレスアーキテクチャの主要なコンポーネントを示しています。これらのコンポーネントの 説明を以下に示します。

図 4. SD-Access ワイヤレスアーキテクチャのコンポーネント



- Network Automation Simple GUI and APIs for intent-based Automation of wired and wireless fabric devices
- Network Assurance Data Collectors analyze Endpoint to Application flows and monitor fabric device status
- Identity Services NAC & ID Services (e.g. ISE) for dynamic Endpoint to Group mapping and Policy definition
- Control-Plane Nodes Map System that manages Endpoint to Device relationships
- Fabric Border Nodes A fabric device (e.g. Core) that connects External L3 network(s) to the SD-Access fabric
- Fabric Edge Nodes A fabric device (e.g. Access or Distribution) that connects Wired Endpoints to the SD-Access fabric
- Fabric Wireless Controller A fabric device (WLC) that connects Fabric APs and Wireless Endpoints to the SD-Access fabric
- ・コントロールプレーン(CP)ノード:エンドポイント ID とデバイス間の関係を管理するホストデータベース。
- ・ファブリックボーダー (FB) ノード:外部レイヤ3ネットワークを SD-Access ファブリックに接続するファブ リックデバイス (コアやディストリビューション スイッチなど)。
- ・ファブリックエッジ (FE) ノード: 有線エンドポイントを SD-Access ファブリックに接続するファブリックデバ イス (アクセススイッチなど)。
- ・ファブリック WLC:ファブリック対応のワイヤレスコントローラ。
- ・ファブリック AP:ファブリック対応のアクセスポイント。
- Cisco DNA Center:エンタープライズネットワークの自動化およびアシュアランスを一元管理できるソリューション。Cisco DNA Centerは、エンタープライズソフトウェア定義型ネットワーキング (SDN) コントローラ、ポリシーエンジン (Cisco Identity Services Engine (ISE))、および分析エンジン (Cisco ネットワーク データ プラットフォーム (NDP))を統合します。
- ・ポリシーエンジン:ユーザまたはデバイスをグループに動的にマッピングし、ポリシーを定義する外部 ID サービス (ISE など)。
- ・アシュアランスエンジン:ユーザまたはデバイスからアプリケーションへのフローを分析し、ファブリックス テータスをモニタするデータコレクタ(NDP)。

次のセクションでは、SD-Access ワイヤレスアーキテクチャの主なコンポーネントの役割と機能について説明します。

コントロール プレーン ノード

ファブリック コントロール プレーン ノードは LISP **マップサーバ/リゾルバに基づいており**、ファブリックエンドポ イント ID データベースを実行してオーバーレイ到達可能性情報を提供します。

図 5. コントロール プレーン ノード



CP はホストデータベースであり、エンドポイント ID (EID) とその他の属性をエッジノードバインドまで追跡します。次の処理を実行します。

- ・複数のタイプの EID ルックアップキー(IPv4/32、IPv6/128*、または MAC アドレス)をサポートします。
- エッジノード、有線ローカルエンドポイントのファブリック WLC とワイヤレスクライアントそれぞれからプレ フィックス登録を受信します。
- ・リモートエッジノードからのルックアップ要求を解決し、エンドポイントを特定します。
- ・ファブリックエッジノード、ワイヤレス クライアント モビリティを設定したボーダーノードおよびルーティン グロケータ(RLOC)情報を更新します。

ファブリックエッジノード

ファブリックエッジは、ファブリックに接続されたユーザとデバイスの接続を行います。

図 6. ファブリックエッジノード



ファブリックエッジは次の処理を実行します。

- ・有線エンドポイントの識別と認証を行います。
- ・コントロールプレーンノードにワイヤレス IPv4 または IPv6 エンドポイント ID 情報を登録します。
- ・接続されたエンドポイントにエニーキャストレイヤ3ゲートウェイを提供します。
- ・ワイヤレスクライアントに仮想ネットワーク (VN) サービスを提供します。

- ・APをファブリックにオンボーディングし、APに VXLANトンネルを構成します。
- ・ゲストボーダーおよびゲスト コントロール プレーン ノードと通信するワイヤレスホストにゲスト機能を提供します。

ファブリックボーダーノード

ファブリックに出入りするすべてのトラフィックは、ファブリックボーダーノードを経由します。



図 7. ファブリックボーダーノード

- ファブリックボーダーノードには、ボーダーノードとデフォルトボーダーノードの2種類があります。どちらの タイプも、ファブリックオーバーレイに出入りするすべてのデータトラフィック、および VN やグループベース のポリシー適用(ファブリック外のトラフィックに対して)に対して、基本的なルーティングエントリポイン トと出口ポイントを提供します。
- ファブリックボーダーを使用して、「既知の」IP またはマスクルートをマップシステムに追加します。既知の ルートとは、ファブリックエッジノード(リモート WLC、共有サービス、データセンター、ブランチ、プライ ベートクラウドなど)にアドバタイズする任意の IP またはマスクのことです。
- ・デフォルトボーダーは、ラストリゾートゲートウェイとして「不明」ルート(インターネットやパブリッククラ ウドなど)に使用されます。
- ・ボーダーは、ファブリックドメインと非ファブリックドメインがエンドポイントの到達可能性とポリシー情報を 交換する場所です。
- ・ボーダーは、ドメイン間でコンテキスト (Virtual Route Forwarding (VRF) および SGT) の変換を行います。

ファブリック対応 WLC

・ファブリック対応 WLC は LISP コントロールプレーンに統合されます。

ワイヤレス機能については、コントロールプレーンは WLC で集中管理されます。

図 8. ファブリック対応 WLC



- ・WLC は、AP イメージまたは設定、RRM、クライアントセッション管理およびローミング、その他すべての無線 コントロールプレーン機能を引き続き提供します。
- ・ファブリック統合について
 - ・ワイヤレスについては、EID としてクライアント MAC アドレスが使用されます。
 - ・SGT および VNI を使用した**クライアント MAC アドレスの登録**のために、コントロールプレーンノードのホ スト トラッキング データベースと通信します。
 - ・VN 情報は、ファブリックエッジ上の VLAN にマッピングされます。
 - ・WLC はホスト トラッキング データベースをワイヤレスクライアントのローミング情報で更新します。
- ・ファブリック対応 WLC は AP と同じサイトに物理的に配置する必要があります(初期リリースでは、WLC から WAN 経由で AP を展開することはサポートされていません)。



ファブリック AP

ファブリック AP では、ワイヤレスエッジに SD-Access データプレーンを拡張します。



図 9. ファブリック AP

・ファブリック AP はローカルモード AP であり、ファブリックエッジスイッチに直接接続する必要があります。
・CAPWAP コントロールプレーンは、トランスポートとしてファブリックを使用して WLC に移動します。

- ・ファブリックは、サービスセット識別子(SSID)ごとに有効になります。
 - ・ファブリック対応 SSID の場合、AP は 802.11 トラフィックを 802.3 に変換し、クライアントの VNI および SGT 情報をエンコードする VXLAN にカプセル化します。
 - APは、WLCによってプログラムされた転送テーブルに基づいてクライアントトラフィックを転送します。
 通常、VXLANトンネルの宛先は最初のホップのスイッチになります。
 - ファブリック SSID 上のワイヤレスユーザの SGT および VRF ベースポリシーは、有線の場合と同様に、 ファブリックエッジで適用されます。
- ・ファブリック対応 SSID の場合、カプセル化として VXLAN を利用し、AP にユーザデータプレーンが分散され ます。
- AP は、SSID ポリシー、Application Visibility and Control (AVC) 、Quality of Service (QoS) などのすべてのワイヤ レス固有の機能を適用します。



主) AP 上の機能サポートについては、WLC リリースノートを参照してください。

AP は、サポートされているファブリック拡張ノードのいずれかにオプションで接続できます。サポートされている スイッチモデルについては、発注ガイド (<u>https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/software-</u> <u>defined-access/guide-c07-739242.html</u>) を参照してください。

SD-Access ワイヤレスプロトコルと通信インターフェイス

図 10 は、SD-Access ワイヤレスで使用されるプロトコルとインターフェイスを示しています。

図 10. 異なるコンポーネント間の通信



- ・WLC と AP 間: コントロールプレーン WLC と AP 間の通信は、既存のモードと同様に CAPWAP を通じて行われ ます。
- AP とスイッチ間:データトラフィックは VXLAN トンネルカプセル化を使用して AP からエッジスイッチにス イッチングされます。UDP ポートは標準の 4789 です。
- ・WLC とコントロールプレーンノード間:WLC は、コントローラの TCP ポート 4342 上で実行されているコント ロールプレーンと通信します。
- Cisco DNA Center と WLC 間:最初のリリースでは、Cisco DNA Center は SSH/Telnet を介してコマンドライン イ ンターフェイス (CLI) を使用し、WLC を設定します。
- Catalyst 9800 プラットフォームでは、Cisco DNA Center は netconf-yang モデルを使用してデバイスの設定をプッシュおよびプロビジョニングします。netconf-yangの有効化については、以降の項で説明します。netconf は TCP ポート 830 を使用します。
- EWC (Catalyst 9300、9400 および 9500 で実行されている 9800 ソフトウェア) では、コントロールプレーンは Catalyst スイッチにあります。9800 ソフトウェアにコントロールプレーンと通信する LISP エージェントが存在し ます。
- ・スイッチとコントロールプレーンノード間:ファブリック対応スイッチは、TCP ポート 4789 のコントロールプ レーンノードと通信します。

SD-Access ワイヤレスプラットフォームのサポート

SD-Access ワイヤレスアーキテクチャは次の WLC および AP でサポートされます。 Cisco 3504、5520、8540 シリーズ ワイヤレスコントローラ Cisco Catalyst 9800 シリーズ ワイヤレスコントローラ (9800-40、9800-80、9800-L、9800-CL) C9300、C9400、C9500 シリーズ スイッチの Cisco Catalyst 9800 組み込み型ワイヤレス Wi-Fi 6 アクセスポイント : Cisco Catalyst 9115AX および Cisco Catalyst 9117AX Wi-Fi 6 アクセスポイント : Cisco Catalyst 9120AX シリーズ Wi-Fi 6 アクセスポイント : Cisco Catalyst 9130AX シリーズ 802.11 Wave 2 アクセスポイント : Cisco Aironet 1800、2800、3800 シリーズ 802.11 Wave 1 アクセスポイント : Cisco Aironet 1700、2700、3700 シリーズ 802.11 Wave 2 屋外アクセスポイント : Cisco Aironet 1540、1560 802.11 Wave 2 アクセスポイント : Cisco Aironet 4800 アクセスポイント

サポートされるデバイスとソフトウェアの最新情報については、SD-Access 互換性マトリックス (<u>https://www.cisco.com/c/en/us/solutions/enterprise-networks/software-defined-access/compatibility-</u> <u>matrix.html</u>) を参照してください。

SD-Access ワイヤレスネットワーク展開

この項では、SD-Access ワイヤレスネットワークに WLC と AP を展開する際の重要な考慮事項について説明します。 次の図を参照してください。

アクセスポイントは次のように展開する必要があります。

- ・ファブリックエッジ(または拡張ノードスイッチ)に直接接続されている
- ファブリックオーバーレイの一部である
- ・グローバル ルーティング テーブルにマップされている INFRA_VN に属す
- ・ローカルモードで WLC に接続する

WLC は次のように展開する必要があります。

- ・ファブリックの外部に接続されている(必要に応じてボーダーに直接接続)
- ・グローバル ルーティング テーブル内に存在する
- ・VRF 間リークは AP が WLC に接続する際に不要である
- ・1 つのコントロールプレーンノード(冗長性のために 2 つ)としか通信しないため、1 つの WLC は 1 つのファブ リックドメイン(FD)にしか属せない

(注) ファブリック コントロール プレーン プロトコルに耐障害性を持たせるには、各ファブリックノードのグロー バル ルーティング テーブルに WLC への特定のルートが存在することが重要です。WLC の IP アドレスへの ルートは、ボーダーでアンダーレイ内部ゲートウェイプロトコル (IGP) に再配布されるか、各ノードで静的 に設定する必要があります。WLC は SD-Access 内の RLOC と見なされるため、LISP RLOC 到達可能性チェッ クの一環として、アンダーレイ上に WLC への特定のルートが必要です。つまり、WLC はデフォルト ルート 経由で到達できません。

図 12. AP と WLC の展開



APとWLC間の通信

ネットワーク展開の観点からは、アクセスポイントはオーバーレイネットワークに接続され、WLC は従来の IP ネッ トワークの SD-Access ファブリックの外にあります。



(注) WLC が物理的にサイトに設置され、WAN を経由しないようにします。ファブリック AP はローカルモードに し、AP と WLC の間の遅延は 20 ミリ秒未満にする必要があります。

WLC サブネットは、アンダーレイにアドバタイズされるので、ネットワーク内のファブリックノード(ファブリッ クエッジおよびコントロールプレーン)はネイティブルーティングを実行して WLC に到達できます。オーバーレイ の AP サブネットは外部ネットワークにアドバタイズされ、WLC はオーバーレイ経由で AP に到達できます。

ここで、CAPWAP トラフィックがファブリック対応 SSID の AP と WLC 間でどのように流れるかを少し詳しく見ていき ましょう。これは、AP 接続操作専用のコントロール プレーン トラフィックと他のすべてのコントロール プレーン トラ フィックです(クライアント データ プレーン トラフィックは AP から VXLAN を使用してスイッチに配信されるため、 WLC には送信されません)。

APからWLCへの南北方向のCAPWAPトラフィックを図13に示します。

図 13. AP から WLC への南北方向の CAPWAP トラフィック



- ・ボーダー(内部または外部)は、アンダーレイ内の WLC ルートを(選択した IGP を使用して)再配布します。
- •FE がグローバル ルーティング テーブルでルートを学習します。
- FE が AP から CAPWAP パケットを受信すると、FE は RIB で一致を検出し、パケットは VXLAN カプセル化なし で転送されます。
- ・APからWLCへのCAPWAPトラフィックがアンダーレイで移動します。

WLC から AP への北南方向の CAPWAP トラフィックを図 14 に示します。

図 14. WLC から AP への北南方向の CAPWAP トラフィック



- AP サブネットは、オーバーレイの一部として、コントロールプレーンに登録されています。
- ・ボーダーは、AP のローカル EID スペースをコントロールプレーンからグローバル ルーティング テーブルにエク スポートし、AP ルートを LISP マップキャッシュエントリにインポートします。
- ・ボーダーは外部ドメインにローカル AP EID スペースをアドバタイズします。
- ・ボーダーは、WLC から CAPWAP パケットを受信すると、LISP ルックアップが行われ、トラフィックは VXLAN カプセル化を使用して FE に送信されます。
- ・WLC から AP への CAPWAP トラフィックがオーバーレイで移動します。



(注) AP から WLC までの CAPWAP トラフィックパスについて説明してきました。AP から発信された他のタイプ のトラフィックにも同じパスが適用され、DHCP、DNS などのグローバル ルーティング テーブルで既知の宛 先に送信されます。

Cisco DNA Center を使用した SD-Access ワイヤレスのセットアップ

この項では、Cisco DNA Center を使用して SD-Access でワイヤレス機能を設定するためのステップバイステップガイド を提供します。Cisco DNA Center では、SD-Access ソリューションの自動化、ポリシー、およびアシュアランスを一元 管理できます。

SD-Access ワイヤレスをセットアップするための前提条件の1つとして、Cisco DNA Center がインストールされてい る必要があります。ワイヤレス LAN コントローラ (WLC) は、Cisco DNA Center でサポートされているイメージと ともにインストールする必要があります。

以降の項のワークフローとスクリーンショットは、Cisco DNA Center 1.3.3 のものです。

Identity Service Engine (ISE) をインストールし、少なくともプライマリ PAN、PSN、MNT のペルソナを準備する必要があります。必要な規模をサポートする分散モデルに対応するには、後述の ISE 導入ガイドを参照してください。 Identity Service Engine (ISE) では、PxGRID および ERS API サービスが実行されている必要があります。

SDA の互換性のあるソフトウェアに関する推奨事項の詳細については、下記の互換性マトリックスガイドを参照して ください。

SD-Access 互換性ガイド

Cisco DNA Center のインストールおよびアップグレードプロセスについては、次のリンクの手順に従ってください。

Cisco DNA Center インストールガイド

Cisco ワイヤレス LAN コントローラ (WLC) をインストールして設定し、初期設定を完了します。Aire-OS または Catalyst 9800 プラットフォームについては、以下の手順を参照してください。

<u>Cisco Aire-OS 8540 導入ガイド</u>

<u>Cisco Aire-OS 5520 導入ガイド</u>

Cisco Catalyst 9800 導入ガイド

Identity Services Engine (ISE) のインストールガイド

9800 組み込みワイヤレス LAN コントローラ (EWC)

Catalyst 9k スイッチに組み込みワイヤレスコントローラをインストールするための前提条件の1つとして、netconf が 有効になっている必要があります。Cisco DNA Center はデバイスで netconf を有効にします。netconf は、Cisco DNA Center がデバイスに設定をプロビジョニングするために使用する方法の1つです。

以下の項では、Cisco DNA Center を使用して netconf を有効にしない場合に、Catalyst 9k スイッチで netconf を手動で 有効にするために必要な手順について説明します。Cisco DNA Center でデバイスに netconf をプロビジョニングするに は、ディスカバリプロセス中にログイン情報の 1 つとして netconf が選択されていることを確認します。ワイヤレス パッケージをインストールするには、Catalyst スイッチをインストールモードで実行する必要があります。ワイヤレ スパッケージのバージョンは、スイッチング プラットフォームで実行されている Cisco IOS-XE のバージョンと同じ である必要があります。

Catalyst 9k スイッチが 16.11.1c で実行されている場合、9800-SW パッケージは同じバージョン(16.11.1)である必要 があります。ワイヤレスパッケージを適切にインストールするには、スイッチで DNA-Advantage ライセンスがアク ティブになっている必要があります。これは show version コマンドで確認できます。アクティブでない場合は、通常 のライセンスコマンドを使用して評価版をアクティブ化できます。

Catalyst 9k ファミリのワイヤレスパッケージのソフトウェアは、Cisco.comのスイッチング製品ファミリにあります。

イメージは特別リリースとしても掲載されており、SDA 互換性マトリックスを介して特別リリースの参照でイメージ を取得できます。

Software Download Download Store / Switches / Campus LAN Switches - Access / Establisht \$300 Series Switches / Catalyst \$300-245-A Switch Select a Software Type	Cisco Catalyst 9800 Embedded Wireless on C9300, C9400, C9500 Series Switch	IOS XE 16.12.2t , IOS XE 16.12.1s, IOS XE 16.11.1c	IOS XE 17.1.1s IOS XE 16.12.2t, IOS XE 16.12.1s, IOS XE 16.11.1c
I IOS X E Software I IOSXXE Krimska Controller Software Peckaget NBAR2 Protocol Pecks			

EWC は現在、SD-Access 展開でのみサポートされています。Cisco DNA Center は、Catalyst 9k スイッチでのワイヤレ スパッケージのプロビジョニングとインストールに使用されます。

ステップ1 DNA-Advantage ライセンスが有効になっていることを確認します。

Switch#show version b Technology					
Technology Package License Information:					
Technology-package Technology-package					
Current	Туре	Next reboot			
network-advantage Permanent network-advantage					
dna-advantage	Subscription	dna-advantage			

ステップ2 Catalyst スイッチで netconf を手動で有効にします。

Switch# netconf-yang - > NETCONF/YANG をグローバルに有効にします。初期化に最大 90 秒かかることがあります。 Switch# aaa new-model Switch# authorization exec default local - > NETCONF-SSH 接続と edit-config 操作に必要
Switch#show netconf-yang status netconf-yang: enabled -> netconf ステータス netconf-yang ssh port: 830-> Cisco DNA Center がデバイスに接続するためのポート netconf-yang candidate-datastore: disabled

ステップ3 デバイスが検出されてファブリックに追加されたら、Catalyst 9k スイッチで 9800-SW を有効にする必要 があります。ワイヤレスコントローラ機能を有効にするには、デバイスをクリックしてデバイスの詳細ページを開き ます。詳細ページで、管理者はデバイスでサポートされている機能を確認できます。サポートされている機能の1つ に [Embedded Wireless] があります。スライドバーを移動してオプションを有効にします。

Devices V Fabric Services Fabric-Enabled Sites	S ^D All Fabrics > colarado COIRADO	9300-BR.sand.com (9.201.201.13)
EQ. Find Hierarchy ✓ ② colrado ▲ colarado	C Fabric Infrastructure 2 device(s) in this site are not com	Refres Details Fabric Port Channel Configuration Interfaces Remove From Fabric Fabric Image: Bigge Node Image: Bigge Node Image: Bigge Node Image: Bigge Node Image: Configure Image: Control Plane
	Saturd States Satues Sa	Capability Image: Capability

ステップ4 組み込みワイヤレス機能を追加したら、次のプロセスでは、Cisco DNA Center の SWIM モジュールを使用してデバイスに 9800-SW イメージをインポートします。[OK] をクリックして SWIM プロセスを実行します。

9300-BR.sand.com (9.201.201.13) ☺ ⊘ Reachable Uptime: 35 minutes		
🖳 Run Comman	ds 🛛 🖻 View 360 🔹 Last updated: 2:34 PM	🕄 Refre
Details Fabric Port Channel Configuration Interfaces	Stack	
Remove Fabric		
Bendaryour Daint	Displied (1)	
		Cancel Add

9300-BR.sand.com				>
Select an image from computer Choose File C9800-SW-los2.01.SPA.bin	2 Manage Scope	3 Advanced	4 Summary	
OR Enter image URL				
Activate image after import				
Cancel			Back	
9300-BR.sand.com				
Download Image Image imported successfully	2 Manage Scope	3 Advanced	4 Summary	
C9800 Image activated successfully			<i>v</i>	
Cancel			Back	

ステップ 5 イメージの場所を指定します。アクティブ化オプションを有効にして [Import] をクリックします。

ステップ6 イメージがデバイスにインポートされてアクティブになったら、デバイスによって管理されるサイトを 選択します。

9300-BR.sand.com	×
Download Image Download Image Cope 3 Advanced 4 Summary	
ΞQ Find Hierarchy	
✓ ෯ ☐ Global (2)	
 ✓ IBGL11 (3) Image: Second seco	
	_
Cancel Back Nex	ĸt



9300-BR.sand.	com				\times
	Download Image	Manage Scope	Advanced	4 Summary	
SYSTEM DETAILS					
Device Name:		9300-BR.sand.con	1		
Platform Id:		C9300-48UXM, CS	9300-24UX		
Device IP:		9.201.201.13			
Device Location:		BGL11			
SSID(S)					
Name:		sand-site2-1x (sa	and-denver-profile)		
Туре:		Enterprise			
Security:		wpa2_enterprise			
Admin status:		Enabled			
Broadcast: _		Enabled			
Cancel				Back	Save

ステップ8 組み込みワイヤレスを追加したら、ファブリック設定を保存します。

Modify Fabric Domain	
When Now Later	Cancel Apply

ファブリック対応 AP とファブリックエッジとしての Catalyst 4500E

SD-Access ファブリックがファブリックエッジ (FE) としての Catalyst 4500E で構成され、AP が直接接続されている 場合は、特別な考慮が必要です。ファブリック対応ワイヤレス (FEW) を使用すると、シスコのアクセスポイントは それぞれのファブリックエッジへの VxLAN トンネルを作成します。Catalyst 4500E で VxLAN トンネルをサポートす るには、スイッチをインストールモードで起動する必要があります。スイッチ上のドーターカードは、アクセストン ネルからの VxLAN ヘッダーのカプセル化を解除します。

Catalyst 4500E でサポートされている推奨リリース、スーパーバイザモジュール、およびラインカードについては、 SDA 互換性ガイドを参照してください。

もう1つの重要な考慮事項は、アクセスポイント(AP)をサポートされているラインカードに直接接続できる一方で、アップストリームを残りのファブリックに接続するためにスーパーバイザモジュールのポートを使用する必要があることです。

ドーターカードがプラットフォームで有効になっているかどうかを確認するには、show module CLI を使用してください。

	Jard Type		Model	Serial No.
1 12 5 2 12 1 3 48 1	Sup 8-E 10GE (SFP 10GE SFP+ 100/1000/2500/500	+), 1000BaseX (SFP) 0/10GBaseT UPOE E S	WS-X45-SUP8-E WS-X4712-SFP+E Ser WS-X4748-12X48U+E	CAT1947L0LU CAT1849L2F2 CAT1925L9E3
M MAC add:	resses	Hw Fw	Sw	Status
1 a89d.21d 2 74a0.2fa 3 78ba.f9a Mod Submoo	17.70c0 to a89d.2 a2.eec8 to 74a0.2 a0.9270 to 78ba.f dule	1d7.70cb 1.3 15.1(1 fa2.eed3 2.0 9a0.929f 1.0 0.0 Model	r)SG17 03.11.00.E Serial No. Hw St	Ok Ok Ok
+	ter Card	WS-UA-SUP8E	CAT1948LG9Z 1.1 0	 C
1 Daught				
1 Daugh: Mod Lineca	rdMode			

SD-Access WLC アンダーレイディスカバリ

Cisco DNA Center にログインする前に、ご使用のブラウザを最新バージョンにアップグレードしてください。

手順

ステップ1 インストール時に割り当てた管理 IP アドレスとログイン情報を使用して、Cisco DNA Center にロ グインします。



ステップ2 ログイン後、Cisco DNA Center ランディングページが表示されます。

Cisco DNA Center DESIGN	POLICY PROVISION	ASSURANCE PLATFORM			∠⊗ ۹ Ⅲ	◊ ◊ ≣
Welcome, admin				Get Started	d Take a Tour	🕑 Learn More
		In a few simple steps, discover your device Get S	s to begin your Cisco DNA Center journ tarted	ey!		
Assurance Summary						
Health 0 Healthy as of Jan 28, 2020 11:35 AM			Critical Issues Last 24 Hours			
Network Devices	Wireless Clients	% Wired Clients	O		D	
		View Details				View Details
Network Snapshot						
		Network Devices As of Jan 28, 2020 11:46 AM		Application Policies As of Jan 28, 2020 11:46 AM		
		0	Unclaimed: 0	0	Successf	ul Deploys: 0

Cisco DNA Center への ISE の追加

SGT のダウンロードおよび新しいポリシーの作成には、Cisco DNA Center が安全に ISE と通信できる必要があります。 ISE サーバと Cisco DNA Center は pxGrid と REST API サービスを使用して情報を交換します。 Cisco DNA Center に ISE を追加するのは非常に簡単です。Cisco DNA Center で、ホームページの右上隅にある「歯 車」シンボルをクリックして [System Settings] に移動します。



[System Settings] ページで、[Authentication and Policy Servers] をクリックし、[Add] をクリックして新しいサーバを追加します。

Cisco DNA Center DESIGN	POLICY PROVISION ASSURANCE	PLATFORM			∠9 Q III <	> • =
System 360 Software Updates	Settings Data Platform Users	Backup & Restore				
≡Q, Search	Authentication and Policy	Servers				
Account Lockout Anonymize Data	Use this page to specify the servers that authen	ticate Cisco DNA Center users. ISE servers can also su	upply policy and user information.			
Authentication and Policy Servers				Last updated: 1:53 PM	C Refresh 🖞 Export	🕂 Add
Certificate						
Cisco Credentials						
CMX Servers	IP	Address	Protocol	Туре	Status	
Debugging Logs			No matching records found			
Device Controllability						
Device EULA Acceptance						
Email Configuration						
Events and Subscription						
High Availability						
Integration Settings						
Integrity Verification						
IP Address Manager						

ISE 情報を入力します(忘れずに [Cisco ISE server] スイッチを切り替えます)。

Add AAA/ISE server	×
Server IP Address* 10.195.180.131	
Shared Secret*	S)
Cisco ISE server	
admin Password*	₹¢
FQDN* prabhjit-ise.cisco.com	
Subscriber Name* • dnac-133	
SSH Key	
Virtual IP Address(es)	
♥ View Advanced Settings	
Cancel Apply	

共有秘密は、ネットワークデバイス(スイッチおよび WLC)で使用されるパスフレーズを定義するもので、ネット ワーク アクセス デバイス (NAD)の作成時に ISE で設定されます。Cisco DNA Center により、ネットワークデバイ ス上の RADIUS サーバ設定と ISE サーバ上の NAD 設定が自動化されます。ユーザ名とパスワードは、ISE クラスタ の管理者ログイン情報です。ISE の FQDN(ホスト名 + ドメイン名)を入力します。

(注) 管理者ログイン情報が Web GUI と SSH アクセスで同じであることを確認します。

今日の時点では、Cisco DNA Center は DNS を使って FQDN を検証しませんが、この名前は ISE サーバの実名と一致す る必要があります。サブスクライバの名前を追加することを忘れないでください。これは、pxGrid ログイン情報を確 立するために重要です(この名前は、ISE 上の既存のユーザ名と一致する必要はありません)。

	ulu Idootitu	Convision Er	ogina							_	
¢	sco identity	Services El	ngine	Home	Contex	t Visibility	 Operations 	s 🕨 Poli	cy 🗸 Ad	ministration	 Work Centers
	- System	Identity Mana	agement	Network Re	esources	▶ Device	Portal Manage	ment px0	Frid Service:	s 🔹 🕨 Feed S	ervice 🕨 Threat C
	Deployment	Licensing	▶ Certificat	tes 🕨 Logg	jing 🕨	Maintenance	e Upgrade	▶ Backup	& Restore	Admin Ac	cess 🕨 Settings
	1										
	Deploymer	nt			Deploy	ment Nodes	s List > ise-sar	nd			
	(= • E	•		\. ∰.	Edit	Node					
	🕨 🐝 Depla	oyment			Ge	neral Setting	s Profiling	Configuratio	n		
	🔆 PAN	Failover									
					H	ostname		is	e-sand		
					FC	DN .		is	e-sand.cise	co.com	
					IP	Address		9	.1.0.20		
					N	ode Type		ld	lentity Servi	ices Engine (IS	SE)
					R	de standa		Make Pr	imary		
					\checkmark	Adminis	tration				
					\checkmark	👻 Monitorir	g				

ISE クラスタの FQDN 名を取得するには、プ ライマリ PAN の Web GUI にログインし、次 のリンクに移動します。

[Administration] > [System] > [Deployment] > クラスタのホスト名

ISE に移動し、[Administration]、[pxGrid Services] の順に移動して、サブスクライバ名 dnac-133 を承認することで Cisco DNAC の pxGrid 接続を承認します。

-thule Identity Services Engine Home Context Visibility Operations Policy Admin	istration				0	License Warning 🔺	۹ 6	0	•
System Identity Management Network Resources Device Portal Management pxGrid Services	Feed Service Threat Centric	NAC			Click here to do wireless	etup and visibility set	up Do not show	w this agai	in. ×
All Clients Web Clients Capabilities Live Log Settings Certificates Permissions									
✓ Enable Ø Disable Ø Approve	¥				1 selected item 1 - 8	of 8 Show 25 🗸	, per page	Page 1	\$
Client Name Client Description Capabilities	Status	Client Group(s)	Auth Method	Log					
ise-admin-prabhjit-ise Capabilities(5 Pub, 2 Sub)	Online (XMPP)	Internal	Certificate	View					
ise-pubsub-prabhjit-ise Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate	View					
□ ▶ ise-pubsub-ise-vm-1 Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate	View					
□ ▶ ise-fanout-ise-vm-1 Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate	View					
Ise-bridge-prabhjit-ise Capabilities(0 Pub, 4 Sub)	Online (XMPP)	Internal	Certificate	View					
□ ► ise-fanout-prabhjit-ise Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate	View					
□ ► ise-mnt-prabhjit-ise Capabilities(2 Pub, 1 Sub)	Online (XMPP)	Internal	Certificate	View					
✓ Independent Andread Capabilities(0 Pub, 0 Sub)	Pending		Certificate	View					

Cisco DNAC で ISE のステータスを確認します。

Cisco DNA Center DESIGN	POLICY PROVISION ASSURANCE PLATFORM			⊴¶ Q ⊞ Ф © ≣
System 360 Software Updates	Settings Data Platform Users Backup & Restore	e		
EQ. Search	Authentication and Policy Servers			
Account Lockout Anonymize Data	Use this page to specify the servers that authenticate Cisco DNA C	Senter users. ISE servers can also supply policy and user informat	ion.	
Authentication and Policy Servers			L	ast updated: 4:37 PM 🤤 Refresh 🔟 Export 🛛 🕂 Add
Certificate				
Cisco Credentials CMX Servers	IP Address	Protocol	Туре	Status
Debugging Logs	0 10.195.180.131	RADIUS	ISE	ACTIVE
Device Controllability				
Device EULA Acceptance				
Email Configuration				
Events and Subscription				

SD-Access WLC ディスカバリ

Cisco DNA Center のディスカバリツールは、Cisco Discovery Protocol または IP アドレス範囲で既存のアンダーレイデ バイスを検索する場合に使用します。ここでの前提条件は、有線ネットワークがすでに検出されていることです。 **ステップ1** Cisco DNAC のホームページで、[Tools] > [Discovery] まで下にスクロールするか、右上にある [Discovery] を選択してデバイスを検出し、Cisco DNA Center のプロセスを開始します。

Cisco DNA Center DESIGN POLICY PROV CONTENTION OF A Content of the network, devices product problems faster and ensure that policy and configuration business instent and the user experience you want. Assurance Health Assurance Issues	ASSURANCE PLATFORM A applications to changes achieve the Use DNA Center Platform, to programmaticall integrate with your preferred IT systems to cre multi-vendor devices. • View the API Catalog • Configure DNA Center - to - Third Party Int • Schedule and Download - Data and Report	y access your network through Intent APIs, ate end-to-end solutions and add support for egrations	COULS Discovery Topology Command Runner License Manager Template Editor Security Advisories
Tools Discovery Automate addition of devices to controller inventory	Topology Visualize how devices are interconnected and how they communicate	Command Runner.	Network Telemetry Data and Reports
Template Editor An interactive editor to author CLI templates	Security Advisories Identify security vulnerabilities in the network	Network Telemetry Network Telemetry Design and Provision	Data and Reports Access Data Sets, Schedule Data Extracts for Download in multiple formats like PDF Reports, CSV, Tableau etc.

検出されたデバイスの概要を確認できる [Discovery Dashboard] が表示されます。[Add Discovery] をクリックして新しい検出を開始します。

Cisco DNA Center	Discovery	∠® Q ⊞ ¢ ⊙ ≡
Discovery Dashboard		
Add Discovery View All Discoveries	Inventory Overview As of Jan 28, 2020 2:04 PM Discover devices to view data.	Latest Discovery As of Jan 28, 2020 2:04 PM Discover devices to view data.
Device Controllability is Enabled.		
Discovery Type As of Jan 28, 2020 2:04 PM O IP Address/Range : 0 LLDP : 0	Discovery Status As of Jan 28, 2020 2:04 PM Queued : 0 In Progress : 0 Completed : 0 Aborted : 0 Scheduled : 0	Recent 10 Discoveries As of Jan 28, 2020 2:04 PM Discover devices to view data.

手順

ステップ2 検出名を入力し、検出タイプとして [Range] を選択し、ネットワークの WLC の管理 IP アドレスを範囲の開始および終了として入力します。

Cisco DNA Center		Discovery	∠● ♀ Ⅲ ♥ ◎ Ⅲ
Search by Discovered Device IP O No Discoveries Added. Fill out the 'NEW DISCOVERY' form and start your first scan.	New Discovery Discovery Name* WLC		← Back to Dashboard
	 ✓ IP Address/Range * Discovery Type ● CDP ● IP Address/Range ○ LLDP From* ● 192.168.1.10 Preferred Management IP Address ● ● None ○ Use Loopback 	- To* 0 +	
	Credentials At least one CLI credential and one SNM Netconf is mandatory for enabling Wirele GLOBAL Task-specific CLI	credential are required. is Services on Wireless capable devices such as C9800-Switches/Controllers. SNMPv2c Read	G Add Credentials
	No credentials to display SNMPv2c Write No credentials to display	No credentials to display SNMPv3 No credentials to display	
Device Controllability is Enabled. discovery/inventory or when devic	Config changes will be made on network device e is associated to a site. Learn More Disable	during	Reset Discover

ステップ3 [Add Credentials] をクリックして、WLC にアクセスするためのログイン情報を追加します。デバイス の Simple Network Management Protocol (SNMP) ログイン情報(読み取りおよび書き込み)を次のよ うに入力します。

Exp statuto to Decource is In Discovery Name* WC In Discovery Name* WC In P Address/Range* Discovery Type 0 In Discovery Type 0	Cisco DNA Center	Discovery	∠● ♀ Ⅲ ㅎ ◎ Ⅲ
No credentials to display No credentials to display	Cisco DNA Center EQ → Search by Discoveres 2 More P No Discoveres Added Fill out the NEW DISCOVEY' from and start your first scan.	Discovery Image: State of the second state of the secon	Add Credentials CLI SNAPV2C SNAPY PROPERTIES HTTP(S) NETCONF Netrone admin wc demande Enable Passeord Enable Passeord C Save as global setting: Settings will be used for this task and saved for later Reset Save

Add Credentials ×	Add Credentials × cli SNMPv2c SNMPv3 PROPERTIES HTTP(S) NETCONF
Read Write Name/Description* pbagga pbagga Read Community* Image: Save as global settings Save as global settings Settings will be used for this specific Discovery only Reset Save	Read Write Name/Description* pbagga Write Community* Save as global settings Settings will be used for this task and saved for later Reset Save

検出中にログイン情報に対して指定されたすべてのオプションを有効にすると、検出された WLC で Cisco DNA Center によってその設定が行われます。Cisco DNA Center は Telnet/SSH 経由でデバイスにログインし、デバイスで SNMP と netconf を有効にします。SNMP の読み取りおよび書き込みはアシュアランスに使用され、netconf はワイヤ レス LAN コントローラ (WLC) に設定をプロビジョニングする方法の1つとして使用されます。プラットフォーム で SSH を有効にする方法については、ワイヤレス LAN コントローラのコンフィギュレーション ガイドを参照してく ださい。

Cisco DNA Center	Discovery	<⊘ Q Ⅲ Φ ⊙ Ⅲ
EQ ~ Search by Discovered Device IP No Discoveries Added. Fill out the 'NEW DISCOVERY' form and start	New Discovery Discovery Name*	Add Credentials × cli shimpyze shimpy shimpys https://wetconf
your first scan.	WLC • Netconf is mandatory for enabling Wireless Services on Wireless capable devices such as C9800-Switches/Controllers. • GLOBAL • Task-specific CLI SNMPV2C Read • admin admin-wic • pbagga	Port B30 Settings will be used for this specific Discovery only Reset Save
	SNMPv2c Write SNMPv3 No credentials to display	
	HTTP(S) Read HTTP(S) Write No credentials to display No credentials to display NETCONF	

ステップ4 [Credentials] セクションを折りたたんで、[Advanced] セクションを展開します。クリックして [Telnet] や [SSH] を選択します。SSH は、AIRE-OS ベースのワイヤレス LAN コントローラ (WLC) ではデ フォルトで有効になっています。Catalyst 9800 ワイヤレス LAN コントローラ (WLC) で SSH を有効 にするには、コンフィギュレーション ガイドを参照してください。

	✓ Advanced Protocol Order ●		
	SSH Teinet		
Device Controllability is Enabled. Con discovery/inventory or when device i	tfig changes will be made on network devices during associated to a site. Learn More Disable	Reset	Discover

右下隅にある [Discover] をクリックします。ディスカバリが開始すると、ページにディスカバリ設定と 詳細が表示されます。

Cisco DNA Center				Discovery					29	Q 11	¢	0	
i Discovered devices will be added to	Inventory automatic	ally after successful completion of each disc	covery. View Invent	ory									×
WLC 1 Reachable Devices Range 192.168.1.10-192.168.1.10		Ľ	DEVICE STATUS	~			∀ Filter					Histo	ry 🗸
							IP Address	Device Name	Status ICMP -	SNMP	CLI	NETCONF	I
		1 Devices)	 Success(1) Unreachable(Discarded(0) 	0)		192.168.1.10	WLC-3504				•	
	Discovery D	etails											
	CDP Level	None			LLDP Level	None							
	Protocol Order	ssh telnet			Retry Count	3							
	Timeout	5 second(s)			IP Address/Range	192.168.1.10-192.168.1.10	Show 25		Showing 1 to 1 of	Pa	ge 1	¢ of 1	
	IP Filter List	None			Preferred Management IP Address	None		SUCCESS	UNREACHABLE	S FAILURE	NOT TRIEC		
	CLI Credentials	admin			SNMPv2c READ	pbagga							
	SNMPv2c WRITE	pbagga			SNMPv3	None							
	HTTP(S) READ	None			HTTP(S) WRITE	None							
	NETCONF	None											

同様に、ファブリックに含める他のデバイスをネットワーク内で検出します。有線デバイスが検出され、その名前が画面の右側に順次表示されます。

 (注) ここでも、他のファブリックの有線デバイス(ボーダーノードとエッジノード)がすでに検 出されていることが前提とされています。スイッチには Cisco Discovery Protocol ディスカバ リを使用することをお勧めします。

Cisco DNA Center			Discovery					_10	Q	i ¢	0	:
EQ - Search by Discovered Device IP	Devices @	Completed 5 Reachable Devices	00h:00m:07s				+	Back to	o Dashb	oard	O Take a	Tour
Devices 5 Reachable Devices Range 3.3.3.1-3.3.3.100			DEVICE STATUS	~	∀ Filter						Histor	ry 🗸
WICL Beachable Devices					IP Address	Device Name	Status		SNMP	CLI	NETCONF	1
Range 192.168.1.10-192.168.1.10			-		3.3.3.9	FE1-9300- 03.cisco.com					•	
		5	Unreachable(0)		3.3.3.13	FE2-9300- 04.cisco.com					•	
		Devices	Discarded(0)		3.3.3.21	CONTROL- PLANE.cisco.co m					•	
					3.3.3.5	INT- BOR.cisco.com					•	
	Discovery D	Details			3.3.3.1	pb-fusion- router					•	
	CDP Level	None	LLDP Level	None								
	Protocol Order	ssh	Retry Count	3								
	Timeout	5 second(s)	IP Address/Range	3.3.3.1-3.3.3.100	Show 25		Showing	1 to 5 of 5	P	age 1	¢ of 1	
	IP Filter List	None	Preferred Management IP Address	None		Success	O UNREAU	CHABLE (FAILURE BLE	NO TRI	T IED	
	CLI Credentials	lab	SNMPv2c READ	pbagga								
	SNMPv2c WRITE	pbagga	SNMPv3	None								
	HTTP(S) READ	None	HTTP(S) WRITE	None								
Device Controllability is Enabled. C discovery/inventory or when device	onfig changes will is associated to a	be made on network devices during site. Learn More Disable					De	elete	Copy & I	Edit	Re-discov	ver

(注) デバイスディスカバリが完了すると、検出されたデバイスがすべて Cisco DNA Center のデ バイスインベントリに表示されます。

インベントリ アプリケーション

手順

ステップ1: デバイスのディスカバリ後、デバイス インベントリ アプリケーションを開いてそのデバイスを表示する には、上部で [Provision] > [Inventory] の順にクリックします。

ステップ2: [Provision] の [Inventory] ページで、すべてのデバイスの [Reachability Status] が [Reachable] に、[Last Inventory Collection Status] が [Managed] になっている必要があります。

(注) 前述のディスカバリ手順を省略した場合は、デバイスが [Managed] と表示されていることを確認しま す。そうなっていない場合は、次に進む前に修正する必要があります。

Cisco DNA Center DESIGN	N POLICY PROVISION ASSURA	NCE PLATFOR	RM						⊿10 Q	⊞ ¢ ⊘	1
Devices V Fabric Service	es										
EQ Find Hierarchy	DEVICES (6) FOCUS: Inventory ~				💡 Glob	bal				Take a Tour	••
💩 Global	DEVICE TYPE All Routers Sv	vitches APs	WLCs	REACHABILITY	All	Reachable Unr	eachable				
	Filter Add Device Tag Device	e Actions v ()							La	st updated: 4:23 PM	0
	Device Name 🔺	IP Address	Support Type	Device Family	Site	Reachability	Last Sync Status	Last Updated	Serial Number	Device Series	I
	CONTROL-PLANE.cisco.com	3.3.3.21	Supported	Switches and Hubs	Assign	Reachable	Managed	4 hours ago	FCW2243E0UD	Cisco Catalyst 9300	0 Series 5
	☐ FE1-9300-03.cisco.com ⊡*	3.3.3.9	Supported	Switches and Hubs	Assign	Reachable	Managed	4 hours ago	FCW2248AHLW	Cisco Catalyst 9300	0 Series 5
	FE2-9300-04.cisco.com	3.3.3.13	Supported	Switches and Hubs	Assign	Reachable	Managed	an hour ago	FCW2248DHHS	Cisco Catalyst 9300	0 Series 5
	□ INT-BOR.cisco.com ◻	3.3.3.5	Supported	Switches and Hubs	Assign	Reachable	Managed	4 hours ago	FCW1934C1D8	Cisco Catalyst 3850	0 Series E
	D pb-fusion-router	3.3.3.1	Supported	Switches and Hubs	Assign	Reachable	Managed	3 hours ago	FDO1735Q0FR	Cisco Catalyst 3650	0 Series 5
	□ □ WLC-3504 0 [*]	192.168.1.10	Supported	Wireless Controller	Assign	Reachable	Managed	4 hours ago	FCW2221M0JT	Cisco 3500 Series	Wireless I

SD-Access の設計

Cisco DNA Center Design の使用開始

Cisco DNA Center には強力な設計アプリケーションが備わっており、あらゆる規模のお客様が、物理サイトおよび共通リソースを簡単に定義できます。これは、直感的に使用できる階層形式で実装されており、デバイスのプロビジョニング時に複数の場所で同じリソースを再定義する必要がありません。

手順

ステップ1 次の例のような [Design] ページを使用して、ネットワークのサイトとサイト階層を作成します。





ネットワーク設定 (Network settings)

Cisco DNA Center では、[Design] の [Network Settings] アプリケーションに共通のリソースと設定を保存できます。これにより、企業に属する情報が保管できるため、Cisco DNA Center 全体で再利用できます。DHCP、DNS サーバおよびデバイスログイン情報はここで定義されている必要があります。

IP プールの作成

AP とクライアントサブネット両方の IP プールを、DHCP サーバのネットワーク アドレッシング スキームに従って手動 で設定します。また、DHCP オプション 43 を AP IP プールの DHCP サーバに定義し、AP を WLC に登録します。このガ イドでは、IP アドレスマネージャ (Infoblox) の統合を活用しないため、Cisco DNA Center ではこの手順は自動化されま せん。

手順

メニューを使用し、[Design] > [Network Settings] の順に移動し、[IP Address Pools] を選択します。[Add] をク リックして、ダイアログボックスを開き新しい IP プールを作成します。



完了したら、Cisco DNA Center のクライアントおよび AP 用の [IP Address Pools] タブは次のページのようになります。

Cisco DNA Center DESIG	N POLICY PROVISION ASSURANCE	PLATFORM			_10		
Network Hierarchy Network S	Settings 🗸 Image Repository Network	Profiles Authentication Ten	nplate				
EQ. Find Hierarchy	Network Device Credentials IP Addre	ess Pools QoS Wireless					
✓ ♣ Global							
> 💩 San Jose	IP Address Pools (4)				Last updated: 4:42 PM 🛛 📿 Refresh		
	√ Filter ● Add Actions ∨ su	BNET TYPE All IPv4	IPv6				
	Name 🔺	Туре	IPv4 Subnet	IPv6 Subnet	Actions		
	AP-Pool	Generic	192.168.18.0/24 0% IPs available	-	Edit Delete		
	BorderHandoff	Generic	20.20.20.0/24 0% IPs available	-	Edit Delete		
	Campus	Generic	192.16.11.0/24 0% IPs available		Edit Delete		
	ют	Generic	192.168.12.0/24 0% IPs available		Edit Delete		

ワイヤレス SSID の作成

手順

ステップ1 [Network Settings] の [Wireless] タブをクリックします。



SSID の作成は2段階のプロセスです。ネットワークのタイプを選択し、セキュリティタイプを割り 当て、まずワイヤレスネットワークを作成し、次にワイヤレスプロファイルを作成または割り当て ます。新しいプロファイルを作成する場合は、この SSID をブロードキャストするサイトを追加しま す。ワークフローを実行するには、次の手順を参照してください。

ステップ2 エンタープライズワイヤレス SSID (この例では「Internal03」) で [Add] をクリックし、[Level of Security] として [WPA2 Personal] とセキュアなパスフレーズを選択します。Fast Transition (802.11r) は、SSID の作成のフェーズで設定できます。
Enterorise Wireless Network 2 Wireless Profiles				
Wireless Network Name(SSID)*	Type Of Enterprise Network *			
pbagga-internal	Voice and Data			
Fast Lane	○ Data only			
SSID STATE				
Admin Status:				
Broadcast SSID:				
Wireless Option				
Dual band operation (2.4GHz and 5GHz)				
O Dual band operation with band select				
○ 5GHz only				
○ 2.4GHz only				
Level Of Security*				
○ WPA2 Enterprise				
ore secure				
password (Pre-Shared Key PSK with WPA2 encryption) is needed to access the wireless network				
ass Phrase*				
<i>\$</i>				
		Cancel	Previous	Next

- (注) このガイドのすべての例では、SSID、プロファイル、プールなどの名前は参考用です。ユー ザは自分自身で任意の名前を指定できます。
- ステップ3 [Next] をクリックします。まだ設定されていない場合、Cisco DNA Center ではワイヤレスプロファイ ルを作成して SSID に関連付けるように求められます。この場合のワイヤレスプロファイルの名前は 「employee」です。すでにプロファイルがある場合は、既存のプロファイルのいずれかを選択できま す。ネットワークプロファイルは、SSID、ファブリックまたは非ファブリックのタイプ、およびブ ロードキャストされるサイトを定義します。[Finish] をクリックしてワイヤレスプロファイルを作成 します。

[Wireless Profile] で、プロファイルが SD-Access ファブリック用かどうかを指定し、このプロファイ ルの SSID がブロードキャストされる場所を追加します。下記の例では、SSID pbagga-internal がサイ ト Sanjose にマップされています。子サイト (Floor-1) は設定を継承します。サイトの最初の文字を 入力し、表示されるかを確認します。

Cisco DNA Center DESIG	N POLICY PROVISION ASSURANCE PLATFORM		∠@ ♀ ▦ ё ◦ ≡
Network Hierarchy Network S	Settings Image Repository Network Profiles Authentication Template	Sites	×
EQ Find Hierarchy	Network Device Credentials IP Address Pools QoS Wireless		
V & Global	Create an Enterprise Wireless Network		
> 🗄 San Jose	Enterprise Wireless Network Wireless Profiles	 ∞ ee _ Gooal (1) ∞ @ Z San Jose (1) ∞ ee Z Building 22 (1) 	
	Wireless Prote Name * employee	Sec Z Floor3	
	Fabric		
	⊙ Yes ◯ No		
	😤 Sites 3 sites		
	Attach Template(s)		
	Device Type Device Tag ()		
		Back OK	

ステップ4 プロファイルを設定したら、[Save] をクリックし、SSID のメインページに戻ります。

Cisco DNA Center DESIGN	POLICY PROVISION ASSURANCE PLATFORM			10 Q	Ш	¢	0	
Network Hierarchy Network Se	ettings - Image Repository Network Profiles Authentication Template							
EQ Find Hierarchy	Network Device Credentials IP Address Pools QoS Wireless							
A Global								
> 💩 San Jose	Enterprise Wireless					• A	dd	
	√ Filter Zelit. I Delete							
	Network Name (SSID) 🔺	Security	Wireless Profiles					
	pbagga-internal	wpa2_personal	employee					
		Showing 1 of 1						

ステップ5 これで、ゲスト SSID を作成できます。[Guest Wireless] にある [Add] アイコンをクリックし、ゲスト SSID を追加します。

Cisco DNA Center DESI	GN POLICY PROVISION ASSURANCE PLATFORM		۹ 🐠		> 0	
Network Hierarchy Network	Settings v Image Repository Network Profiles Authentication Template					
EQ Find Hierarchy	Network Device Credentials IP Address Pools QoS Wireless					
v 💩 Global	Create a Guest Wireless Network					
⇒ 💩 San Jose	Guest Wireless Network 2 Wireless Profiles 3 Portal Customization					
	Wireless Network Name(SSD) * Guest-WiFi					
	SSID STATE					
	Admin Status:					
	Broadcast SSID:					
	Level Of Security *					
	Web Policy Open					
	Most secure :					
	Guest users are redirected to a Web Portal for authentication					
	Authentication Server					
	⊙ ISE Authentication ○ Web Authentication ○ Web Passthrough					
	What kind of portal are you creating today ? Where will your guests redirect after successful authentication ? Self Registered V Original URL V					
	Show Advanced Settings					
	01	ancel	Previo	JS	N	ext

ステップ6 非ゲスト SSID の場合と同様に、SSID をネットワークプロファイルに追加します。

				∠10 ⊂	
Settings - Image Repository Netwo	rk Profiles Authentication Template		Edit Wireless Profil	е	×
Network Device Credentials IP Ad	dress Pools QoS Wireless		Wireless Profile Name *		
Create a Guest Wireless Network			employee		
Guest Wireless Network	Wireless Profiles 3 Portal Customic	ization	Fabric • Yes O No		
Profiles			Sites 3 sites.		
			O Sites without configured ISE will be O Sites without configured ISE will be	e unselected automatically	
Filter 1 Selected			Attach Template(s)		
Profile Name	Version	Created By			Add
employee	1	admin	Device Type Tag (Template	
		Showing 1 of 1		No data to display	
			Ca	ncel Save	
	Network Device Credential IP Adi Create a Guest Wireless Network Image: Create a Guest Wireless Network Image: Create a Guest Wireless Network Image: Create a Guest Wireless Network Image: Create a Guest Wireless Network Image: Create a Guest Wireless Network Image: Create a Guest Wireless Network Image: Create a Guest Wireless Network Image: Create a Guest Wireless Network Image: Create a Guest Wireless Network Image: Create a Guest Wireless Network Image: Create a Guest Wireless Network Image: Create a Guest Wireless Network Image: Create a Guest Wireless Network Image: Create a Guest Wireless Network Image: Create a Guest Wireless Network Image: Create a Guest Wireless Network Image: Create a Guest Wireless Network Image: Create a Guest Wireless Network Image: Create a Guest Wireless Network Image: Create a Guest Wireless Network Image: Create a Guest Wireless Network Image: Create a Guest Wireless Network Image: Create a Guest Wireless Network Image: Create a Guest Wireless Network Image: Create a Guest Wireless Network Image: Create a Guest Wireless Network Image: Create a Guest Wireless Network Image: Create a Guest Wireless Network Image: Create a Guest Wireless Network Image: Create a Guest Wireless Network Image: Create a Guest Wireless Network Image: Create a Guest Wireless Network Image: Create a Guest Wireless Network Image: Create a	Network Device Circederdiality IP Address Paola Gold Wartees	Interest Device Condentiality Paddress Prodies Ood Werless Image: Condentiality Image: Condentiality	Interest Evented Lederetistik Create a Guest Wireless Network	Intervent Total calcularity Create al Guest Wireless Network Croifies Toffies Total Name Create al Guest Total Name Create al Guest Total Name Create al Guest Stowing 1 of 1

ステップ7 Cisco DNA Center は、ポータルおよびプロファイル設定用に ISE とのバックエンド統合を提供します。以下のスクリーンショットには、ポータルのカスタマイズに使用できるオプションがあります。ISE を使用した中央 Web 認証 (CWA) がサポートされています。



ステップ8 [Finish]をクリックして、ゲスト SSID 設計フェーズを完了します。

Network	Device Credentials IP Address Pools QoS Wi	reless		
Create a Gue	est Wireless Network Wireless Network	Portal Customization		
Portals				🕂 Add
	Portal Name	Туре	Action	
۲	GuesPortal	Self registered	Edit Delete	
		Showing 1 of 1		
			Cancel	Finish

ステップ9 必要に応じて、カスタマイズされた RF プロファイルを設定できます。設計フェーズのプロファイル
 は、プロビジョニングフェーズで適用されます(このガイドで後述)。ワイヤレスページを下にスクロールし、使用可能なワイヤレス無線周波数プロファイルを表示します。

CISCO CENTER	DESIGN	POLICY PROVISION					111	\$	ii (
EQ. Find Hierarchy	*								
v Global									
 Milpitas 		Wireless Rad	o Frequency	Profile				•	Add
San Jose									
SantaClara		∀ Filter							
		Profile Name	Туре	5Ghz Data Rates	2.4Ghz Data Rates	Channel Width			
		HIGH	2.4 GHz ,5 GHz	12,18,24,36,48,54	9,12,18,24,36,48,54	20 MHz		View	
		LOW	2.4 GHz ,5 GHz	6,9,11,12,18,24,36,48,54	1,2,5.5,6,9,11,12,18,24,36,48,54	20 MHz		View	
		TYPICAL	2.4 GHz ,5 GHz	6,9,12,18,24,36,48,54	9,12,18,24,36,48,54	20 MHz		View	

新しいプロファイルを作成するには、[Add New]をクリックします。次のページが表示されます。

Create Wireless Radio Frequency Profile	
PROFILE NAME*	
demo	
PROFILE TYPE	
∧ 2.4 GHz	(m
Parent Profile	
e High ○ Medium (Typical) ○ Low ○ Custom	
∧ 5 GHz	Co
Parent Profile	
⊖ High ⊖ Medium (Typical) ⊖ Low	
	Cancel

2.4 または 5 GHz バンドの親プロファイルに対して、カスタマイズパラメータ(動的帯域幅選択、DCA チャネルの柔軟性と HD RF 設定)を選択します。

Channel Width Best	v												
20 MHz													
40 MHz			🔄 UNII-2 5	2-144				UNII-3	149-165				
00.104			52	56	60	64		149	153	157	161		
80 MHZ			2 100	2 104	2 108	112	C] 165					
160 MHz			116	2 120	2 124	128							
Best			132	2 136	2 140	144							
Note Posts													
Data Rate	12	18	24	_	36	45	54						
Data Rate	52	18	24	_	36	, 48	54					RX SOP	
TX Power Configuration Power Level	ΰ	18 0	24		36	48	54 30				5	RX SOP Auto	~
Data Rate 9 FIX Power Configuration Power Level	12	18 O dbr	24		36	48	54 30 dilm					RX SOP Auto High	~
Data Rate	12	ið Ó	ž		36	48	S4					RX SOP Auto High	
Data Rate	12	10 10 to dbr	24		36 36	48	54 30 68m					RX SOP Auto High Medium	v

SD-Access のポリシー

SD-Access では、ネットワークポリシーは、Cisco TrustSec[®] に基づくグループベースポリシーです。仮想ネットワーク (VN) (VRF に相当)とスケーラブルグループタグ (SGTS)は、階層的なネットワークポリシーとセグメンテー ションを提供するために使用されます。マクロレベルでは、VN を使用して、コントロールプレーンとデータプレー ンの観点からユーザグループを完全に分離できます。これはステートフル セグメンテーションで、通常 VRF 間のト ラフィックを許可するためにファイアウォールを通過します。VN では、SGT を使用して、セキュリティ グループ ア クセス コントロール リスト (SGACL) に基づいて、ユーザ間でステートレスポリシーを定義し、マイクロセグメン テーションを実装できます。SD-Access の利点は、これが有線とワイヤレスの両方のユーザに当てはまるということ です。

以降では、ファブリック内の 2 つのグループ間にポリシーを作成し、コントラクトを割り当てます。2 つのユーザグ ループ「employees」と「pci_servers」の間で HTTP アクセスを許可するコントラクト「demo_access」が作成され ます。

SGT をユーザに割り当てるには、Identity Services Engine (ISE) ガイドでセグメンテーションについて参照してください。

ISE セグメンテーションガイド

ステップ1 [Policy] > [Virtual Network] ページで、[+] アイコンをクリックして新しい VN を作成します。名前を選 択して VN にスケーラブルグループを割り当てます。この手順は任意です。

Cisco DNA Center DESIGN	POLICY PRO	VISION	ASSURANCE	PLATFO	RM						∠10 ⊂ 🏢 🌣	⊘ :≣
Group-Based Access Control 🗸 IF	P Based Access	Control 🗸	- Applic	ation 🗸	Traffic Co	opy ∽ Vir	ual Netwo	ork				
EQ Find Virtual Network	Create or M	odify Virtua	I Network by	selecting A	vailable Sca	lable Groups.					Reset	Save
New Virtual Network	Virtual Network	Name*										
DEFAULT_VN (18)	loT							vManage VPN		\sim	Guest Virtual Network 🚯	
INFRA_VN (0)												
	Available Sca	alable Group	S					Groups in th	e Virtual Netv	vork		
	EQ Find Scala	able Group			Show	Unselected	~	EQ Find Sca	lable Group			
	AU	BY	со	DE	DS	EM		PO	PC	UN		
	Auditors	BYOD	Contract ors	Develop ers	Develop ment_S	Employe es		Point_of _Sale_S	PCI_Ser vers	Unknow n		
	EX	GU	IN	NS	PS	PU						
	Extranet	Guests	Intranet	Network _Servic	Producti on_Serv	Producti on_User						
	QS	TS	TS									
	Quaranti ned_Sy	Test_Se rvers	TrustSe c_Devic									

- (注) この時点で VN にグループ (SGT) を追加する理由は、オンボーディングセクションで明確になります。SSID またはポートに SGT を静的に割り当てる場合は、プールの関連付けを使用して行い、この時点で VN に含まれている SGT から選択できる SGT を選択します。
- **ステップ2** [Save] をクリックして VN を作成します。 正常に作成されると、画面の右下隅にメッセージがポップアップ表示されます。
- ステップ3 次に、[Policy] > [Group-Based Access Control] > [Access Contracts] の順にクリックして、コントラクトを 追加します。コントラクトとは、スケーラブルグループ間で許可されるトラフィックを定義する場所 です。



ウィンドウの右上隅にある [Add Contract] アイコンをクリックして、次のようにコントラクトエディタを開 きます。この例では、特定のポートまたはプロトコル(この場合は HTTP)の許可アクションを使って 「demo_access」を作成しました。暗黙の拒否アクションに注意してください。これをデフォルトの許可アク ションに変更できます。[Save] をクリックして、コントラクトを作成します。

Cisco DNA Center DESIGN	POLICY PROVISION ASSURANCE PLATFORM		200	Q Ⅲ Φ © Ⅲ
Migration is complete. Cisco DNA Cent the administration mode in GBAC Confi	er will be the policy administration point, and screens of Scalable Groups, Access Contracts gurations	and Policies in Cisco ISE will be read-only. You o	can review the policy mi	gration log, and/or change $~~ imes~$
Group-Based Access Control V	P Based Access Control ~ Application ~ Traffic Copy ~ Virtua	I Network		
Access Contracts (8)		Last updated: 5	5:03 PM 📿 Refresh	Create Access Contract
∑ Filter Actions ∨ Deploy				
Name •	Description	Rules Count	Deployed	Policies
AllowDHCPDNS	Sample contract to allow DHCP and DNS	2	No	0
AllowWeb	Sample contract to allow access to Web	2	No	1
Deny IP	Deny IP SGACL		No	3
Deny_IP_Log	Deny IP with logging		No	0
DenyRemoteServices	Sample contract to block Remote Access and telnet services	4	No	0
CONTRACT CONTENT (1) # Action • Application	Transport Protocol Source / Destination Port	Logging Action		
1 Permit V http	CP Destination 80	— + ×		
Default Action Permit ~	Logging			
		Cancel Save		

新しいコントラクトが作成されますが、まだ展開されていません。展開するには、新しいコントラクトのチェック ボックスをクリックし、[Deploy] をクリックします。

isco DNA Center Design Poli	CY PROVISION ASSURANCE PLATFORM		∠10	Q Ⅲ � ◎ Ⅲ	
Migration is complete. Cisco DNA Center wi the administration mode in GBAC Configura	II be the policy administration point, and screens of Scalable Groups, Access Contractions	ts and Policies in Cisco ISE will be read-only	. You can review the policy migra	ation log, and/or change $~~ imes~$	
iroup-Based Access Control V IP Ba	used Access Control V Application V Traffic Copy V Virtu	ual Network			
ccess Contracts (9)		Last upo	lated: 5:07 PM C Refresh	Create Access Contract	
Filter Actions V Deploy					
Name •	Description	Rules Count	Deployed	Policies	
AllowDHCPDNS	Sample contract to allow DHCP and DNS	2	No	0	
Sync not started	Sample contract to allow access to Web	2	No	1	
demo_access		1	No	0	
Migration is complete. Cisco DN the administration mode in GBA	A Center will be the policy administration point, and screens of Sca C Configurations	alable Groups, Access Contracts an	d Policies in Cisco ISE		
Group-Based Access Control ~ Access Contracts (9)	IP Based Access Control \checkmark Application \checkmark	Traffic Copy ~ Virtual N	etwork		
∇ Filter Actions \vee Deploy	1 Selected				
Name 🔺	Description		Rule		
AllowDHCPDNS	Sample contract to allow DHCP and DNS		2		
AllowWeb	Sample contract to allow access to Web		2		
demo_access			1		
Cisco DNA Center DESIGN	POLICY PROVISION ASSURANCE PLATFORM			∠10 Q	III � ⊘
Wigration is complete. Cisco DNA Ce the administration mode in GBAC Co	inter will be the policy administration point, and screens of Scalable Group: nfigurations	s, Access Contracts and Policies in Cis	co ISE will be read-only. You	can review the policy migratio	n log, and/or change
Group-Based Access Control ~	IP Based Access Control V Application V Traffic Co	opy 🗸 Virtual Network			
Access Contracts (9)			Last updated	5:07 PM C Refresh	Create Access Co
∑ Filter Actions ∑ Deploy					
Name 🔺	Description		Rules Count	Deployed	Policies
AllowDHCPDNS	Sample contract to allow DHCP and DNS		2	Yes	0
AllowWeb	Sample contract to allow access to Web		2	Yes	1

(注)

スクリーン ショットは参考用です。コントラクトに自由に名前を付け、任意の許可アクションを割り当てできます。

ステップ4 最後に、コントラクト(ステップ3で作成)を使用してグループベース アクセス ポリシーを作成し、ス ケーラブルグループをひも付けます。[Policy] > [Group-Based Access Control] > [Policies] に移動します。

Cisco DNA Ce	nter	DESIGN	POLICY	PROVISION	ASSURANCE	PLATFO	RM
Migration is c the administr	complete. ation mod	Cisco DNA (de in <mark>GBAC</mark> C	Center will be t	he policy administ	tration point, and s	creens of Sc	calable Grou
Group-Based Ac	cess Co	ontrol 🗸	IP Based	Access Contro	ol 🗸 Applica	ation 🗸	Traffic
, Scalable Groups	(9) s						
Policies	~	Deploy					

ステップ5 [Policy] に、送信元と宛先のスケーラブルグループを含むマトリックスが表示されます。スケーラブル グループの任意の組み合わせ([Employees] > [PCI_Servers] など)をクリックします。

Cisco DNA Center design policy provision assurance platfor	Create Policy ×
Migration is complete. Cisco DNA Center will be the policy administration point, and screens of Scr	Employees -> POL Servers Default Prior State France State
Group-Based Access Control V IP Based Access Control V Application V	Enabled
Policies (5) 💒 Enter full screen	Contract: Change Contract
∀ Filter Deploy ○ Refresh	
Permit Deny Custom Default	
Sures 8 12/1/11/11/11/11/11/11/11	
Auditors	
BYOD	
Contractors	
Developers	
Development_S	
Employees	
Guesta	
Network_Servic	
PCI_Servers	
Point_of_Sale	
Printers	
Production_Ser	
	Cancel Save

右側のペインで [Change Contract] をクリックし、前の手順で作成した「demo_access」コントラクトを選択します。これは、Employee と PCI_Servers 間のポリシーです。

< Edit Policy Change Contract Create Con						
∇	Filter					
	Name	Description 🔺	Policies Referencing			
۲	demo_access		0			
0	Deny IP	Deny IP SGACL	3			
0	Deny_IP_Log	Deny IP with logging	0			
0	dfsfsd	dfsndfsdnf	0			
0	Permit IP	Permit IP SGACL	1			
0	Permit_IP_Log	Permit IP with logging	0			
0	AllowWeb	Sample contract to allow access to Web	1			
0	AllowDHCPDNS	Sample contract to allow DHCP and DNS	0			
0	DenyRemoteServices	Sample contract to block Remote Access and telnet services	0			
Show	10 entries	Showing 1 - 9 of 9	Previous 1 Next			
			Cancel Change			

[Change] と [Save] をクリックして、このポリシーが適用されることを確認します。

ポリシーのマトリックスページで、スケーラブル グループ アクセス リスト ポリシーが作成されたことを確認し ます。



(注) 上のスクリーンショットは説明のみを目的としたものです。選択したスケーラブルグループに応じてポリ シーを作成してください。

SD-Access オーバーレイのプロビジョニング

[Provision] セクションでは、ネットワークの設定を実際にデバイスにプッシュします。

デバイス (WLC) のプロビジョニング

手順

ステップ1 トップメニューから [Provision] タブを選択します。

WLCを選択し、設計フェーズで作成済みのサイトに関連付けて、プロビジョニングプロセスを開始します。

ステップ2 1回クリックして WLC を選択します。WLC を選択したら、[Actions] メニューをプルダウンして [Assign Device to Site] を選択し、WLC が物理的に設置されている場所に割り当てます。この手順は、物理的に配置されているサイトに対応する規制ドメインに WLC を割り当てる上で重要です。このサイトは、建物またはフロア、つまり座標を持つサイトである必要があります。

(注) 上のスクリーンショットは説明のみを目的としたものです。ご自身の WLC を選択してください。

Vertices v Fabric Sortices e Fact Heardry e Global	Sisco DNA Center DESIG	N POLICY PROVISION ASSURANCE PLATFORM					29	0, Ⅲ Φ Θ	
Outsigned Devices (1) > 20 indexto de vices (1) > Nacionality A indexto de vices Nacionality A indexto de vices Nacionality A indexto de vices Nacionality Nacionality A indexto de vices Nacionality	Jevices Fabric Servic 2 Find Hierarchy	DEMOES (6) FOCUS: Inventory V		Q Global				Take a Tour	\$
Inventory Stre Reschability And Address Perice Rele Hunge Version Uptime I Contract-FAME diseaccom FEI-9300-93.diseaccom TEI-9300-93.diseaccom 3.3.3 Supported Assign Device To Site Provision Device TEI-9300-93.diseaccom 3.3.3 Supported LAN Automation Configure VILC FIA Supported <li< td=""><td> Unassigned Devices (1) > San Jose </td><td>DEWCE TYPE All Routers Switches APs WLCs</td><td>Selected</td><td>Reachable Unreachable</td><td></td><td></td><td></td><td>Last updated: 5:11 PM</td><td>0</td></li<>	 Unassigned Devices (1) > San Jose 	DEWCE TYPE All Routers Switches APs WLCs	Selected	Reachable Unreachable				Last updated: 5:11 PM	0
Image: Contract-RANE disease of fei-size 3.3.13 Supported Statign Device to Site 22/Floor3 Reschable 64:ad:13:0a:700 POISTRBUTION 16.11.1c 14 days 20 hrs 18 mins N Image: Contract-RANE disease of fei-size 23.3.13 Supported Poisson Device Poi		Device Name • IF Software Image >	Device Family Site	Reachability	MAC Address	Device Role	Image Version	Uptime	I S
Provision Device 2//Floor 3 Others Provision Device 2//Floor 3 Provision Device Provision D		CONTROL-PLANE.cisco.com B [*] 3 Provision > Device Replacement>	Assign Device to Site	22/Floor3	d4:ad:71:30:a7:00	ODISTRIBUTION	16.11.1c	14 days 20 hrs 18 mins	N
FE2-9300-04.cks.co.com 07 3.3.3.3 Supported LAN Automation Status 2//Foor3 © Reschable 0.028:22751:00 Ø ACCESS 16.11.1c 18 days 16 hrs 00 mins N Image:		□ □ FE1-9300-03.cisco.com D' 3 Others >	Provision Device	22/Floor3 🖉 Reachable	00:29:c2:be:0e:00	Ø ACCESS	16.11.1c	18 days 16 hrs 13 mins	N
Image: Definition review of the supported in the supported in the support of the		FE2-9300-04.cisco.com D [*] 3.3.3.13 Supported	LAN Automation Status	22/Floor3 🕜 Reachable	00:29:c2:27:51:00	ACCESS	16.11.1c	18 days 16 hrs 08 mins	N
Compute vice r d' 3.3.3.1 Supported 22/Floor.3 @ Reschable cols72atredat80 @ ACCESS 16.11.20190312.035643 107 days 20 hrs 6 mins M WLC-3504 G' 192.168.1.10 Supported Wineless Controller Assign @ Reschable 0.05x56/168.1300 # ACCESS 16.11.20190312.035643 107 days 20 hrs 6 mins M		C INT-BOR.cisco.com D 3.3.3.5 Supported	Learn Device Config	22/Floor3 ⊘ Reachable	38:ed:18:67:a6:00	O DISTRIBUTION	16.11.1c	43 days 20 hrs 48 mins	N
WLC-3504 Cl 192.168.1.10 Supported Wireless Controller Assign Or Reachable 005bc:601d:81:00 # ACCESS 8.8.100.0 209 days 1 hrs 55 mins M		Definition-router D 3.3.3.1 Supported	Configure WLC HA	22/Floor3 📀 Reachable	c0:67:af:ed:af:80	ACCESS	16.11.20190312:035643	107 days 20 hrs 06 mins	N
		WLC-3504 0° 192.168.1.10 Supported	Wireless Controller Assign	🖉 Reachable	00:bc:60:fd:81:00	Ø ACCESS	8.8.100.0	209 days 1 hrs 55 mins	N

Choose a site	
EQ Find Hierarchy	
◇ 畿 Global (1)	
◇ 続 San Jose (1)	
√ i i i i i i i i i i i i i i i i i i	
SFloor3	

(注) ステートフル スイッチオーバー ハイ アベイラビリティ (SSO HA)を設定する場合、2番目の WLC は、この時点で同じサイトに追加する必要があります。次に、同じ [Device Inventory] ページから、プラ イマリとして設定する WLC をクリックし、[High Availability] タブに移動します。ここでは、プライマ リとセカンダリの両方のコントローラの管理および冗長性管理情報を入力し、[OK] をクリックしま す。コントローラが再起動され、しばらくした後に、インベントリ内の WLC が1つのみ表示されるよ うになります。今後、単一の WLC であるかのようにプロビジョニングを続行することができます。

	ble Uptime: 209 days 1 hours 55 r	ninutes	
		E	Run Commands 🛛 🖄 View 360 🔹 Last updated: 5:13 PM 📿 Refresh
Details Interfaces	s Wireless Info Mobility		
Device Name	WLC-3504	Location	Global/San Jose/Building 22/Floor3
Device Type	Wireless Controller	Reachability	Reachable
P Address	192.168.1.10	Uptime	209 days 1 hours 55 minutes
Last Sync Status	Managed	Role	ACCESS
MAC Address	00:bc:60:fd:81:00		
INVENTORY			
Serial Number	FCW2221M0JT	Resync Interval	6 hours
Last synced	3 hours ago	Series	Cisco 3500 Series Wireless LAN Controller
Platform	AIR-CT3504-K9		
SOFTWARE II	MAGES		
Software Image	Cisco Controller	Software Version	8.8.100.0
Image Series	-	Update Status	This image needs to be golden
PROVISION			
Provision Status	Not Provisioned	Last Provisioned	-

ステップ3 WLCをサイトに追加したら、その WLCを選択して [Provision] をクリックします。

isco DNA Center DESI	GN POLICY PROVISION ASSU	RANCE PLATFORM						(9) C		
evices V Fabric Servi	ces									
Find Hierarchy	DEVICES (6) FOCUS: Inventory ~			💡 Glo	obal				Take a Tour 📃	24
& Global	DEVICE TYPE All Routers	Switches APs WLCs	REACHABILITY AI	Reachable U	Inreachable					
 Unassigned Devices 	√ Filter	rice Actions v 🕕 👔	Selected						Last updated: 5:13 PM	0
	Device Name	Inventory > Software Image >	Device Family Site	R	teachability	MAC Address	Device Role	Image Version	Uptime	I s s
	CONTROL-PLANE.cisco.com	Provision >	Assign Device to Site	22/Floor3	Reachable	d4:ad:71:30:a7:00	O DISTRIBUTION	16.11.1c	14 days 20 hrs 18 mins	N
	FE1-9300-03.cisco.com 0	3. Others >	Provision Device	22/Floor3	Reachable	00:29:c2:be:0e:00	Ø ACCESS	16.11.1c	18 days 16 hrs 13 mins	N
	FE2-9300-04.cisco.com @	3.3.3.13 Supported	LAN Automation Status	22/Floor3	Reachable	00:29:c2:27:51:00	Ø ACCESS	16.11.1c	18 days 16 hrs 08 mins	N
	<	3.3.3.5 Supported	Learn Device Config	22/Floor3	Reachable	38:ed:18:67:a6:00		16.11.1c	43 days 20 hrs 48 mins	N
	D pb-fusion-router C	3.3.3.1 Supported		22/Floor3	Reachable	c0:67:af:ed:af:80	Ø ACCESS	16.11.20190312:035643	107 days 20 hrs 06 mins	N
	WLC-3504 0	192.168.1.10 Supported	Wireless Controller/Buildin	ng 22/Floor3	Reachable	00:bc:60:fd:81:00	Ø ACCESS	8.8.100.0	209 days 1 hrs 55 mins	N

ステップ4 WLC を配置する場所を選択します。Syslog/SNMP や NTP などのネットワークプロファイルで定義された設定が WLC にプッシュされます。

Cisco DNA Center DESIGN	POLICY PROVISION ASSURANCE PLATFORM	
Provision Devices		
1 Assign Site 2 Configuration	3 Advanced Configuration 4 Summary	
Serial Number	Devices	
FCW2221M0JT	WLC-3504	ក្រឹត្រ Global/San Jose/Building 22/Floor3 $ imes$

ステップ5 この WLC で管理される AP ロケーションを選択します。存在する場合、AP が導入されるフロアを選択することが重要です。[Next] をクリックします。

Cisco DNA Center DE	ESIGN POLICY PRO	DVISION ASSURANCE	PLATFORM	
Provision Devices				
1 Assign Site 2 Cont	figuration 3 Advance	ed Configuration (4) s	Summary	
♥ WLC-3504	Serial Number	Devices	WLC Role	
	FCW2221M0JT	WLC-3504	● Active Main WLC ①	A Managing 1 Primary location(s)
			⊖ Guest Anchor	Relect Secondary Managed AP Locations
	Mobility Group			
	Name RF C	Configure Reset		
	1			

ステップ6 Cisco DNA Center から WLC プロビジョニングの一環としてプッシュされる設定(システム詳細や、認証、許可、およびアカウンティング(AAA)、DHCP、DNS サーバ、SSID および管理サイトのグローバル設定)を確認します。[Deploy] をクリックします。

Cisco D	NA Center design policy provision assurance p	LATFORM (@ Q II 0 0 II
Provision	Devices	
1 Assi	in Site 2 Configuration 3 Advanced Configuration 4 Summa	87
WLC-	✓ Device Details	
3504	Device Name:	WLC-3504
	Platform Id:	AIR+CT3504-K9
	Device IP:	192.168.1.10
	Device Location:	Giobal/San Jose/Building 22/Floor3
	Device Role:	Active Main WLC
	 Vetwork Setting 	
	AAA Client Server:	AAA clerifiendooist settlons are configured based on the settlons added for each Managed AP location.
		WARNING: Do not use "admin" as the username for your drive CUI credentials. If you are using DE as your AAA server. If you do, this can result in you not being able to login to your drives.
	DHCP Server:	10.5.130.12
	DNS Domain Name:	elece.com
	DNS Primary Server:	171.70.166.183
	(anyologia)	
	SSID (employee)	
	Name:	pbsgga-internal
	Type:	Enterprise
	Security.	wpaz_personal Adapting
	rasi nalisituti. Traffic Turos	Maguive Value + Data
	Eabric Enabled	
	East Lana anablart	No
	Mac Elitering Enabled:	No.
	Flex Connect enabled:	No
	Broadcast Enabled:	Yes
	Arlenin Chabura	Eastland
		Cancel Deploy

(注) WLC の国コードは、アクセスポイントがマッピングされている地域に基づいて選択されます。たとえば、WLC がインドと米国の地域にマッピングされたアクセスポイントを管理している場合、DNAC によってプッシュされる国 コードは「US、IN」です。国コードは建物にマッピングされ、その下のフロアは国コードを建物から継承します。 Cisco DNA Center によって WLC にプッシュされる国コードについては、次のスクリーンショットを参照してくだ さい。

Provision	Devices	
1 Assign	Site 2 Configuration 3 Advanced Configuration 4 Summary	
	MFP Client Protection	Optional 🚺
	✓ Managed Sites	
	Primary WLC:	Global/colarado/denver/BGL11/F1
		Global/colarado/denver/bangalore/F1 (India)
		Global/colarado/denver/Japan (Japan)
		Global/colarado/denver/Japan/f1 (Japan)
	Y Rolling AP Upgrade	
	Rolling AP Upgrade	Disabled
	AP Reboot Percentage	25

ステップ6 Cisco DNA Center を使用してプッシュされる設定(RADIUS サーバが認証やアカウンティングで使用 する設定など)は、WLC で表示できます。2 つのWLANが作成されていて、ID は 17 より大きく、ス テータスは無効に設定されていて、各サイトに 1 つ WLAN が関連付けられています。ホストオンボー ディングを設定して SSID にプールを割り当てるまで、WLAN は無効状態になります。

սիսիս			Sa <u>v</u> e	Configuration Ping	Logout <u>R</u> efresh
CISCO	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS	HELP FEEDBACK			n <u>H</u> ome
Security	RADIUS Authentication Servers			Apply	New
AAA General KADIUS Authentication Accounting Fallback DNS Downloade AVP TACACS+ LDAP Local Net Users	Auth Called Station ID Type AP MAC Address:SSID Use AES Key Wrap (Designed for FIPS customers and requires a key wrap compliant RADIUS MAC Delimiter Hyphen Framed MTU 1300 Network Tunnel Server	S server)			
MAC Filtering	User Management Proxy Index Server Address(Ipv4/Ipv6)	Port	IPSec	Admin Status	
User Login Policies AP Policies Password Policies	✓ ✓ <u>1</u> * 10.195.180.131	1812	Disabled	Enabled	
Local EAP					
Advanced EAP					
Priority Order					
Certificate					
Access Control Lists					
Wireless Protection Policies					
Web Auth					
TrustSec					
Local Policies					
Umbrella					
Advanced					

cisco	MONITOR V	<u>V</u> LANs	CONTROLLER	WIRELESS	<u>s</u> ecurity	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK		Save Configuration	Ping Logout <u>R</u> efresh
WLANs	WLANs											Entries 1 - 2 of 2
VLANs	Current Filter	Non	e [Ch	ange Filter] [C	lear Filter]				Create New	Go		
Advanced	WLAN ID	Туре	Profile	Name		WLAN SSID			Admin Status	Security Policies		
	<u> </u>	WLAN	Internal	03_F_2866e		Internal03			Disabled	[WPA2][Auth(802.1X)]		
	<u>18</u>	WLAN	Guest03	_F_450ae		Guest03			Disabled	MAC Filtering		

Cisco Catalyst 9800 WLC のスクリーンショット:

	-7800-1#sh wian summary			
Numb	er of WLANs: 3			
ID	Profile Name	SSID	Status	Security
17	sand-site2_Sanjos_F_c2d2d249	sand-site2-1x	DOWN	[WPA2][802.1x][AES]
18	sand-mac-s_Global_F_183f26d4	sand-mac-site2	DOMN	[open]
19	sand-nonfa_Sanjos_NF_584c9d37	sand-nonfabric	DOMN	[WPA2][802.1x][AES]

(注) 上のスクリーンショットは説明のみを目的としたものです。ご自身のネットワークに関連する設定(IP アドレスと名前)が WLC で表示されるのを確認できます。

これで、Cisco DNA Center はサイト内のどこにデバイスがあるのかを認識するので、ファブリック プロビ ジョニングを開始できます。

ファブリックの作成

手順

- **ステップ1** メニューから [Fabric] を選択します。SD-Access ファブリックを作成、管理するための新しいページが 表示されます。
- **ステップ2**新しいファブリックを作成するか、[Default LAN Fabric] をクリックします。次の例では、San Jose という新しいファブリックを作成しました。

Cisco DNA Center DESIGN PO	LICY PROVISION A	SSURANCE	PLATFORM
Devices V Fabric Services			
SD-Access Fabrics Choose a Fabric or Transit/Peer Network below to Fabrics	and Transit	/Peer clicking 'Add Fa	Networks bric or Transit/Peer Network!
Default LAN Fabric	San Jose		
0 Site , 0 Fabric Device 0 Control Plane , 0 Border LAN	1 Site , 4 Fabric D 1 Control Plane , 1 B	evice order LAN	

San Jose ファブリックで、[Floor 3] をクリックします。

All Fabrics 2 San Jose Eq. Find Herarchy	
EQ. Find Herarchy v @ San Jose v @ San Jose	
✓ Q San Jose ✓ (A: San Jose	
✓ db Building 22	
Floor3 ¢ Floor3	
CONTROL-PLANE INT-BOR.clico.com	

ステップ3 [Select Devices] をクリックし、ノードをファブリックに追加します。デバイスをファブリックに追加するには、WLC-3504 をクリックし、[Wireless] オプションボタンを選択して WLC をファブリックに追加します。[Add] をクリックします。

Cisco DNA Center DESIGN	POLICY PROVISION ASSURANCE PLATFORM		_● Q Ⅲ ☎ ◎ Ⅲ
Devices ~ Fabric Services			
Fabric-Enabled Sites	All Fabrics > Floor3	≡q I	Find by device IP, type, role, family & MAC 🍙 🛛 🔳 🕏
50 Find Herrerby	Sali Jose O Fabric Infrastructure O Host Onboarding		Show Task Status
 ∠ Pind Herarchy ∠ Ø San Jose 	Authentication on Extended Node and Critical VI AN features are not use enabled. Do you	want to enable three features? Enable Authentication on Extended Note and Critical VI AN	
 分 San Jose 、 会 Building 22	Aurencedori ori cuenteri noce ani unica vuni realues are ini yet enaueu, to you	nan wienaue situe reautes: Chane Autrenication on Exemety note and Visica VENI.	Collapse All Custom View Mar 12, 2020 5:33 PM
€● Floor3 🔶		**)	
	WLC-3504	pb-fusion-router () () () () () () () () () ()	
			Cancel Save
WLC-3504 (192.168.1.10)	minutes Image: Commands cf Wer 350 Last updated: 5:34 PM C Refresh Inde Mobility Last updated: 5:34 PM C	✓ WLC-3504 (192.168.1.10) ③ @ Reachable Uptime: 209 days 5 hours 7 minutes ■ Run Commands If Vew 2 Details Fabric Port Channel Interfaces Wireless Info Mobility	X C Refresh
Fabric		Fabric	
Wreless		Witers	
	Cancel Add		Cancel Add
[Save] と [Apply] をク	リックして設定を WLC にプッシュし	、WLC をファブリックに含めます。	
** **		Modify Fabric Domain	×
pb-fusion-router		When	
0	6	Now Later	
INT-BOR.cisco.com	CONTRE.elseo.com	Cancel	ly
	0		
LC-3504 FE2-94.cisco.com	P FE1-9		
	٥		
	Cancel Save		

ステップ4 次の例のようにデバイスがファブリックに追加されると、色がグレーから青に変化します。



(注) 上のスクリーンショットは説明のみを目的としたものです。ファブリックには複数のノードを設定で きます。

AP およびホストオンボーディング

このガイドでは、ファブリック有線ネットワークがすでにプロビジョニングされていることが前提となっているため、WLC を追加した後は、AP とワイヤレスクライアントをオンボーディングする必要があります。そのため、IP アドレス プールを追加し、ファブリック内での通信に AP とワイヤレス ホストを有効にする必要があります。SD-Access に IP プールを設定すると、Cisco DNA Center はすぐに各エッジノードに接続し、ホストが通信できるように適切なスイッチ仮想インターフェイス(SVI)を作成します。

また、エニーキャストゲートウェイがすべてのエッジノードに適用されます。ホストが追加のプロビジョニングを行わずに、どのエッジノードにもローミングが簡単にできるため、これは SD-Access の不可欠な要素です。

手順

ステップ1 この画面の上部の [Host Onboarding] をクリックして、AP およびクライアントデバイスの IP プールの 有効化を開始します。

Cisco DNA Center DESI	N POLICY PROVISION ASSURANCE PLATFORM
Devices ~ Fabric Servi	nes l
Fabric-Enabled Sites	All Fabrics > Floor3 San Jose
EQ. Find Hierarchy	⊘ Fabric Infrastructure ⊘ Host Onboarding
 ✓ Ø San Jose ✓ Ø San Jose 	> Authentication Template
Floor3	Virtual Networks
	> Wireless SSID's
	> Port Assignment

 ステップ2 [Virtual Networks] で [INFRA VN] をクリックすると、アドレスプールが設定済みのウィンドウが開きます。AP のアドレス プールを選択します。この VN に対して AP プロビジョニングとレイヤ 2 拡張機能がすでにオンになっていることに注意してください。どちらも AP をオンボードするために必要です。 [Save] をクリックします。

Cisco DNA Center	DESIGN	POLICY PROVISION ASS	URANCE	PLATFORM				∠9 Q Ⅲ	¢ 0	
Devices ~ Fabric	Services		Edit V	/irtual Network: INF	RA_VN					×
Fabric-Enabled Sites	e	All Fabrics > Floor3 San Jose								
EQ Find Hierarchy		⊘ Fabric Infrastructure	Advar	nced View	G Reset 🍈 E	xport	🕂 Add			
 San Jose San Jose 		> Authentication Temp	n D	elete	EQ Fin	d				
				IP Address Pool 🔺	Pool Type	Authentication Policy	Layer-2 Extension	Layer-2 Floodin	9	
Floor3	¢	 Virtual Networks 		SJC-AP	AP	SJC-AP	Enabled	Disabled		
		Select a virtual Network : Critical Pool: Not Select Campus > Wireless SSID's > Port Assignment				Showing 1 of 1				
								Cancel	Sav	re

レイヤ2拡張機能の設定により、レイヤ2LISP を有効にし、レイヤ2VNID をこのプールに関連付けることで、イー サネットフレームをファブリック上にエンドツーエンドで伝送できます。これにより、レイヤ2ストレッチ済みサブ ネットサービスのシミュレートが可能になります。 [AP Provision Pool] を選択すると、すべてのエッジノードスイッチに設定マクロが自動的にプッシュされます。そのため、AP が直接接続されている場合、スイッチは Cisco Discovery Protocol を介して AP であることを認識し、そのポートにマクロが自動的に適用され、プールに関連付けられた適切な VLAN に物理ポートが割り当てられます。

ポートに対して [No Authentication] テンプレートを選択した**場合にのみ**、AP オンボーディングの FE で CDP マクロが プッシュされます。

Cisco DNA Center 1.2.x では、ファブリックエッジ(FE)に接続されたデバイスを AP として識別するためにマクロが 使用されていました。マクロがデバイスをシスコのアクセスポイントとして検出すると、関連する設定がそのポート にプロビジョニングされます。

Cisco DNA Center 1.3.x では、デバイスをシスコのアクセスポイントとして識別するために Autoconf が使用されるため、ポートに適切な設定がプロビジョニングされます。次の例は、[No Authentication] モードに設定されたポートを示しています。アクセスポイントは、クローズド認証ポートに接続できます。クローズド認証モードでアクセスポイントをオンボードする方法の詳細については、次の項で説明します。Autoconf は、デバイス分類子を使用して、ポートに接続されているエンドデバイスを識別します。

Cisco DNA Center	DESIGN	POLICY PROVISION	ASSURANCE PLATFORM				∠9 Q Ⅲ	0 C	
Devices V Fabric	Services								
Fabric-Enabled Sites	•	All Fabrics > Floor3 San Jose							
EQ. Find Hierarchy		⊘ Fabric Infrastructure	e 🔗 Host Onboarding					Show Task	Status
 ✓ ③ San Jose ✓ ④ San Jose ✓ ④ Building 22 		 Authentication Te Select Authenti 	emplate ication Template ①						
€ Floor3	٥	Settings will be ap	oplied to all Fabric Edge host ports, unle	ss overridden by a static port as	signment.				
		0	Open Authentication 🛈		Edit				
		0	Closed Authentication ①		Edit				
		0	Low Impact ①		Edit				
		۲	No Authentication ①						
						Set as Default			

[Port Assignment] セクションで、AP に接続されているポートを選択し、[Connected Device Type] として [Access Point (AP)] を選択します。

Port Assignment	×
Selected Interfaces (1) GigabilEthemet1/0/4	
Connected Device Type Access Point(AP)	
Eq. Search Dropdown	
User Devices (ip-phone,computer,laptop)	
Access Point(AP)	
Server	
Description	

この時点では、AP は適切な VLAN またはサブネットに割り当てられ、指定されたプールから IP アドレスを 取得し、標準のメカニズム(プラグアンドプレイ、DHCP オプション 43、DNS など)のいずれかを使用して WLC を検出します。その後、AP が WLC に接続されます。

クローズド認証による AP オンボーディング

この項では、ユーザがクローズド認証モードを理解していることを前提としています。DNAC 1.3.3 の SD-Access ファ ブリックは、dot1x の優先順位が最も高く、次にマシン認証バイパス(MAB)が続く、クローズド認証モードをサ ポートします。すぐに使用できるアクセスポイントでは、dot1x サプリカントが有効になっておらず、ファブリック エッジで認証するためのログイン情報がプロビジョニングされていません。クローズド認証で AP をオンボードする ために使用される主な機能の1つに、Identity Services Engine (ISE)のプロファイリング機能があります。

このプロファイリング機能により、ISE はエンドポイントの ID を識別し、プロファイリング後に適切な認証プロファ イルを割り当てることができます。

プロファイリングの詳細については、コミュニティページのガイドを参照してください。 <u>ISE Profiling Design Guide</u>

Cisco DNA Center により、ファブリックデバイスのプロファイリング設定が自動化されます。ファブリックデバイス にプッシュされるプロファイリング設定の例を次に示します。 device-sensor filter-list cdp list iseCDP tlv name device-name tlv name capabilities-type tlv name version-type tlv name platform-type 1 device-sensor filter-list dhcp list iseDHCP option name host-name option name parameter-request-list option name class-identifier device-sensor filter-list lldp list iseLLDP tlv name system-name tlv name system-description tlv name system-capabilities device-sensor filter-spec dhcp include list iseDHCP device-sensor filter-spec lldp include list iseLLDP device-sensor filter-spec cdp include list iseCDP device-sensor notify all-changes

Cisco DNA Center により、ファブリックエッジ上のテンプレートが自動化されます。このテンプレートは、Identity Services Engine でアクセスポイントがプロファイリングされた後、属性として返される必要があります。

template ApAutzTemplate switchport access vlan 2045 switchport mode access access-session interface-template sticky timer 10

クローズド認証の AP オンボーディングフローについて説明します。

ステップ 1: AP がクローズド認証用に設定されたファブリックエッジのポートに接続します。AP は dot1x メッセー ジに応答できず、ファブリックエッジは MAB にフォールバックします。

MAB を使用したアクセスポイントの初期認証:

dentity Services I	Engine Home	 Context Vis 	sibility > Operations -	Policy Administration	Work Centers			
Bets Profiling	Posture Client Provis	ioning Po	licy Elements		Click here	to do wireless setup and visibility setup Do n	ot show th	is again. ×
					Results			
Status Rule	e Name	Condit	ions		Profiles	Security Groups	Hits	Actions
ch								
						Auto create security group		
Wire	BAM_ be	£:	Normalised Radius-RadiusFI	lowType EQUALS WiredMAB	× PermitAccess	Select from list	2	¢
	Sentity Services Bets Profiling Status Rul ch	sentity Services Engine Home Sets Profiling Posture Client Provis Status Rule Name ch	entity Services Engline Home Context Vis Sets Profiling Posture Client Provisioning Po Status Rule Name Condit ch	sentity Services Engine Home Context Visibility Operations sets Profiling Posture Client Provisioning Policy Elements Status Rule Name Conditions ch Conditions	Jentify Services Engine Home Context Visibility Operations Policy Administration Status Rule Name Conditions Conditions	eentry' <u>Services Engline</u> Home <u>Contreted Visibility</u> <u>Operations</u> <u>Policy</u> <u>Administration</u> <u>Work Centers</u> eese Profiling Posture Client Provisioning <u>Policy Elements</u> Click there to the there are a the	serutify Services Engine Home Conted Visibility Operations Policy Elements Click here to do wireless setup and visibility setup. Do n Results Profiles Seturity Groups ch Variation Auto create security group Status Rule Name Normalised Radius FlowType EQUALS WiredMAB	Jentify Services Engline Home

May 03, 2020 12:37:21.973 PM	0	0	0	ap1234	78:72:5D:ED:CC:1A	Cisco-AP-Aironet-4800	Default >> Dot1X	Default >> Cisco_AP_Profiling	Ap_template_return_1
May 03, 2020 12:37:21.957 PM	V	0		ap1234	78:72:5D:ED:CC:1A	Cisco-AP-Aironet-4800	Default >> Dot1X	Default >> Cisco_AP_Profiling	Ap_template_return_1
May 03, 2020 12:37:21.908 PM	~	0		ap1234	78:72:5D:ED:CC:1A	Cisco-AP-Aironet-4800	Default >> Dot1X	Default >> Cisco_AP_Profiling	
May 03, 2020 12:35:28.569 PM	~	Q		78:72:5D:ED:CC:1A	78:72:5D:ED:CC:1A	Cisco-AP-Aironet-4800	Default >> MAB	Default >> Cisco_AP_Profiling	Ap_template_return_1
May 03, 2020 12:35:00.498 PM	~	0		78:72:5D:ED:CC:1A	78:72:5D:ED:CC:1A	Cisco-AP-Aironet-4800	Default >> MAB	Default >> Cisco_AP_Profiling	Ap_template_return_1
May 03, 2020 12:34:29.267 PM	~	0			78:72:5D:ED:CC:1A				
May 03, 2020 12:34:19.444 PM	~	0		78:72:5D:ED:CC:1A	78:72:5D:ED:CC:1A	Cisco-AP-Aironet-4800	Default >> MAB	Default >> Cisco_AP_Profiling	Ap_template_return_1
May 03, 2020 12:34:19.419 PM		9			78:72:5D:ED:CC:1A				
May 03, 2020 12:34:19.052 PM		à		78:72:5D:ED:CC:1A	78:72:5D:ED:CC:1A		Default >> MAB	Default >> wired _MAB	PermitAccess

ステップ2: MAB を使用してポートが承認されたら、Identity Services Engine はエンドポイントをプロファイリング し、アクセスポイントとして分類します。

ISE はファブリックエッジへの COA を開始します。ファブリックエッジが認証プロセスを再開します。

これらの手順は、以下の ISE ポリシーログで強調表示されています。ファブリックエッジは、RADIUS アカウンティングパケットを使用してプロファイリング情報を Identity Services Engine に送信します。

ISE のポリシーセット:

cisco.	Ider	ntity Service	es Engine Home	e → Co	intext Visibility	 Operations 	▼Policy	► Administration	Work Cent	enters										
Poli	cy Set	s Profiling	g Posture Client Pr	rovisioning	Policy Ele	ements									Click	< here	to do wireless setup and visibility s	setup <mark>Do na</mark>	it show th	is again. ×
														Results						
		Status R	Rule Name		Conditions									Profiles			Security Groups		Hits	Actions
Se	earch																			
		@	Cisco_AP_Profiling		ំ៖ EndPo	oints-LogicalProfile E	QUALS Cisc	to AP						× Ap_template_retum_1		+	Auto create security group	- +	87	¢
																	Ocicer non nor			

ISE のプロファイリング情報:

diadia cisco	Identity Services Engine	Home	Visibility F Operations	▶ Policy ► Admir	nistration 🗸 Work	Centers	
▶ Ne	twork Access 🔹 🕨 Guest Access	▶ TrustSec ▶ BYO	D ▼Profiler 	• • Device Administratio	on F assiveID		
Overv	iew Ext Id Sources Network De	vices Endpoint Class	ification Node Config Fe	eds 🔸 Manual Scans	Policy Elements	Profiling Policies Pol	icy Sets 🔸 Troubleshoot Repo
	ENDPOINTS [®]		🗗 🖸 END	POINT CATEGOR	RIES®	0	NETWORK DEVICES
	Type Profile		001	OS Types Identity Group	þ		Location Type Device Nam
0 Se	mise: [80%]		16: [50%]	apple, inc.: [50%]_		, inc: [50%]	locartion % [100%]
0	🕂 🗹 💼 ANC –	Change Authorization	 Clear Threats & Vulne 	rabilities Export -	Import - MDM Ac	ctions – Release R	ejected Revoke Certificate
	MAC Address	Anomalous B	IP Address	Username	Hostname	Location	Endpoint Profile
×	MAC Address	Anomalous Beha	IP Address	Username	Hostname	Location	Endpoint Profile
] 78:72:5D:ED:CC:1A		9.11.50.202	ар		Location + All Lo	Cisco-AP-Aironet-4800

ファブリックエッジによって Identity Services Engine (ISE) に送信されるプロファイリングデータ:

iliali cisco	Identity Servio	ces Eng	ine	Home	► Context	√isibility	▶ Operat	ons	▶ Policy	► Admi	nistration	₩Vo	rk Centers
► N	etwork Access	▶ Guest	Access	▶ Trust8	Sec 🕨 BYOI	⊃ ▼ Pr	ofiler 🕨 Po	sture	Device Ad	ministrati	on ⊧Pa	ssiveID	
Ove	rview Ext Id Sour	rces Ne	etwork De	vices Er	ndpoint Class	fication	Node Config	Feeds	▶ Manua	l Scans	Policy El	ements	Profiling Po
en	dpoints > 78:72:	:5D:ED:C	C:1A										
7	78:72:5D:ED:CC:1A ① 区 図												
(-A MA Us En Cu Lor	C Addres ername: dpoint Pr irrent IP A cation: Lo	ss: 78:72: ap ofile: Cisc address: 9 ocation →	5D:ED:CC: co-AP-Airc).11.50.202 ▶ All Locat	1A onet-4800 2 ions								
	Application	is 📘	Attribute	s i	Authentication	٦	Threats	Vulnera	abilities				
G	ieneral Attributes												
	escription)												
5	itatic Assignment		false										
E	indpoint Policy		Cisco-A	P-Aironet-	4800								
9	tatic Group Assign	nment	false										
l	dentity Group Assi	gnment	Profiled										
C	ther Attributes												
C	UI			Cisc	o Systems, In	•							
с	dpCachePlatform			cisco	AIR-AP4800-	A-K9							
с	dpCacheVersion			Cisc 14-2	o AP Software 015 by Cisco	, ap3g3-k Systems,	(9w8 Version: Inc.	16.12.2.1	32 Technic	al Suppor	t: http://www	w.cisco.co	om/techsuppi
I	dpSystemDescrip	tion		Cisc 86-2	o AP Software 019 by Cisco	, ap3g3-k Bystems,	9w8 Version: Inc. Compile	16.12.2.1 d Sun De	32 Technic c 15 03:23:0	al Suppor 03 PST 20	t: http://www)19 by viper	w.cisco.co ndya	om/techsuppi

アクセスポイントの認証プロファイル:

Authorization Profiles > Ap_	_template_return_	1				
AUTIONZAUON PROMe						
* Name	Ap_template_ret	urn_1				
Description						
* Access Type	ACCESS_ACCEPT	*				
Network Device Profile	號 Cisco 🔻 🕀					
Service Template						
Track Movement						
Passive Identity Tracking	ty Tracking 🔲 👔					
Common Tasks MACSec Policy						
NEAT						
✓ Interface Template ApAutzTemplate						
Interface Template		ApAutzTemplate				
Interface Template Web Authentication (Local Web Auth)	ApAutzTemplate				
Interface Template Web Authentication (Local Web Auth)	ApAutzTemplate				
Web Authentication (Local Web Auth)	ApAutzTemplate				
Interface Template Web Authentication (Local Web Auth)	ApAutzTemplate				
Interface Template Web Authentication (Advanced Attribute	Local Web Auth) es Settings	ApAutzTemplate				
Interface Template Web Authentication (Advanced Attribute Select an Item	Local Web Auth) es Settings © = [ApAutzTemplate				
Interface Template Web Authentication (Advanced Attribute Select an item	Local Web Auth) es Settings	ApAutzTemplate				
Interface Template Web Authentication (Advanced Attribute Select an item Attributes Details	Local Web Auth) es Settings	ApAutzTemplate				
Interface Template Web Authentication (Advanced Attribute Select an item Select an item Attributes Details Access Type = ACCESS_cisco-av-pair = interface-	Local Web Auth) es Settings = ACCEPT template-name=Ap	ApAutzTemplate				

ISE COA および後続の再認証:

May 03, 2020 12:37:21.973 PM	0	0	0	ap1234	78:72:5D:ED:CC:1A	Cisco-AP-Aironet-4800	Default >> Dot1X	Default >> Cisco_AP_Profiling	Ap_template_return_1
May 03, 2020 12:37:21.957 PM	~	0		ap1234	78:72:5D:ED:CC:1A	Cisco-AP-Aironet-4800	Default >> Dot1X	Default >> Cisco_AP_Profiling	Ap_template_return_1
May 03, 2020 12:37:21.908 PM	~	0		ap1234	78:72:5D:ED:CC:1A	Cisco-AP-Aironet-4800	Default >> Dot1X	Default >> Cisco_AP_Profiling	
May 03, 2020 12:35:28.569 PM		Q		78:72:5D:ED:CC:1A	78:72:5D:ED:CC:1A	Cisco-AP-Aironet-4800	Default >> MAB	Default >> Cisco_AP_Profiling	Ap_template_return_1
May 03, 2020 12:35:00.498 PM	~	Q		78:72:5D:ED:CC:1A	78:72:5D:ED:CC:1A	Cisco-AP-Aironet-4800	Default >> MAB	Default >> Cisco_AP_Profiling	Ap_template_return_1
May 03, 2020 12:34:29.267 PM	~	Q			78:72:5D:ED:CC:1A				
May 03, 2020 12:34:19.444 PM	×	ò		78:72:5D:ED:CC:1A	78:72:5D:ED:CC:1A	Cisco-AP-Aironet-4800	Default >> MAB	Default >> Cisco_AP_Profiling	Ap_template_return_1
May 03, 2020 12:34:19.419 PM		ò			78:72:5D:ED:CC:1A				
May 03, 2020 12:34:19.052 PM		ò		78:72:5D:ED:CC:1A	78:72:5D:ED:CC:1A		Default >> MAB	Default >> wired _MAB	PermitAccess

ステップ 3: MAB を使用して再認証した AP が、オプション 43 を使用して Cisco Wireless LAN Controller (WLC) に 接続します。WLC には、アクセスポイントで dot1x サプリカントを有効にするための関連設定があります。アクセス ポイントで dot1x 設定を有効にする方法の詳細については、次の URL を参照してください。WLC の設定を有効にす るには、WLC にログインするか、Cisco DNA Center のテンプレートを使用します。

AIRE-OS ベースのワイヤレス LAN コントローラにおける dot1x の有効化: https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-7/b_802_1x_eap_supplicant_on_cos_ap.html

Catalyst 9800 ワイヤレス LAN コントローラにおける dot1x の有効化: https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/b_wl_16_10_cg/802-1x-support.html Catalyst 9800 ワイヤレス LAN コントローラのサンプルテンプレートのスクリーンショットを次に示します。このテン プレートは説明を目的としたものです。必要に応じてテンプレートを書き換え、変更してください。

Cisco DNA Center		Ter	mplate Ed
≣Q, Find template	•	9800-sap ×	
∧ Onboarding Configuration			
✓ 9800-template		Actions v Edit v 9800-eap	
9800-eap	¢	Template	
∧ switch-preauthacl		l en profile default-an-profile	
∧ Cloud DayN Templates		2 description "default ap profile" 3 dotlx eap-type eap-peap	
		4 dotlx username ap1234 password 0 ap1234	

ステップ4:アクセスポイントがリセットされ、dot1x サプリカントが有効になり、ISE で認証されます。承認の一環 として、ISE はファブリックエッジのテンプレート「ApAutzTemplate」を返し、適切なテンプレートをポートに割り 当てます。

dot1x サプリカントが有効になった AP のリセットと ISE での認証:

May 03, 2020 12:37:21.973 PM	0	0	0	ap1234	78:72:5D:ED:CC:1A	Cisco-AP-Alronet-4800	Default >> Dot1X	Default >> Cisco_AP_Profiling	Ap_template_return_1
May 03, 2020 12:37:21.957 PM	~	0		ap1234	78:72:5D:ED:CC:1A	Cisco-AP-Aironet-4800	Default >> Dot1X	Default >> Cisco_AP_Profiling	Ap_template_return_1
May 03, 2020 12:37:21.908 PM		ò		ap1234	78:72:5D:ED:CC:1A	Cisco-AP-Aironet-4800	Default >> Dot1X	Default >> Cisco_AP_Profiling	
May 03, 2020 12:35:28.569 PM	~	0		78:72:5D:ED:CC:1A	78:72:5D:ED:CC:1A	Cisco-AP-Aironet-4800	Default >> MAB	Default >> Cisco_AP_Profiling	Ap_template_return_1
May 03, 2020 12:35:00.498 PM	~	0		78:72:5D:ED:CC:1A	78:72:5D:ED:CC:1A	Cisco-AP-Aironet-4800	Default >> MAB	Default >> Cisco_AP_Profiling	Ap_template_return_1
May 03, 2020 12:34:29.267 PM		0			78:72:5D:ED:CC:1A				
May 03, 2020 12:34:19.444 PM		0		78:72:5D:ED:CC:1A	78:72:5D:ED:CC:1A	Cisco-AP-Aironet-4800	Default >> MAB	Default >> Cisco_AP_Profiling	Ap_template_return_1
May 03, 2020 12:34:19.419 PM	~	0			78:72:5D:ED:CC:1A				
May 03, 2020 12:34:19.052 PM	<u>~</u>	Q		78:72:5D:ED:CC:1A	78:72:5D:ED:CC:1A		Default >> MAB	Default >> wired _MAB	PermitAccess

(注) プロファイリングを必要な精度で行うには、Identity Services Engine でプロファイラフィードを最新に更新する 必要があります。EAP-FAST または PEAP の場合、アクセスポイントで使用するログイン情報を Identity Services Engine (ISE) で設定する必要があります。EAP-TLS の場合、AP に証明書をプッシュする必要があります。アクセス ポイントに証明書をプッシュする方法については、ステップ 3 の URL を参照してください。

AP のプロビジョニング

これで AP は IP アドレスを取得し、WLC の管理 IP アドレスを学習したため、AP は、WLC に接続されます。もちろん、これは AP と WLC の間に IP 接続があることを前提としています(これは本書の対象から外れ、WLC が接続されている場所に依存し、通常はファブリックの外にあります)。AP は、WLC に登録されると、Cisco DNA Center の [Inventory] ページに表示されます。 **ステップ1** [Provision] > [Devices] > [Inventory] に戻ると、ファブリック対応のワイヤレスコントローラに参加して いる AP が表示されます。

cisco	DNA Center				Design	Policy	Provision
Devic	es Fabric						
Dev	vice Inventory						
Inve	ntory (5) Unassigned D	evices					
Select	Devices						
7	Tilter						
	Device Name	Device Type	IP Address	Site	Seria	I Number	
	AP1850-Edge1	Unified AP	9.6.51.53	SJC-14	KWC1	93904BH	
	AP3800-Edge1	Unified	9.6.51.54	SJC-14	FCW2	034NWUX	
	Border_Node.demo.com	Switches and Hubs	9.6.48.1	SJC-14	FCW2	024F05A	
	Edge1.demo.com	Switches and Hubs	9.6.48.4	SJC-14	FCW2	025C049	
	Fab-WLC1	Wireless Controller	9.6.40.4	SJC-14	FCH1	925V05W	

- (注) 上のスクリーンショットは説明のみを目的としたものです。ご使用の設定では、別の 802.11ac Wave 2 アクセスポイントモデルの場合があります。
- ステップ2 次の例のように、[Device] 一覧から1つ以上の AP を選択し、[Assign Device to Site] を選択します。



AP が配置されるフロアを選択し、[Assign] をクリックします。AP が登録されている WLC が、そのフ ロアを管理するためにプロビジョニングされていることを確認します。フロアが後に追加された場合 は、戻って、WLC をもう一度プロビジョニングし、特定のフロアを追加できます。

CISCO CENTER	DESIGN POLICY	PROVISION ASSURANCE				Q III	٥	1
Devices Fabric								
Assign Devic	Assign Device to Site							
						Close		Assign
Serial Number FDW2130B3L2	Devices AP4001.7A70.6004	Choose a floor /Diegem/Floor-1/Diegem Choose a floor						
FDW2130B3KR	AP500F.8086.7866	loor-1/Diegem × 🗸						

ステップ3 次の例のように、[Device] 一覧から 1 つ以上の AP を選択してプロビジョニングします。今回は、[Actions] メニューから [Provision] を選択します。

Devices I	Fabric	
Device Ir	nventory	
Inventory (7)	Unclaimed Devices (1	1)
∑ Filter	Actions ~	
✓ Filter✓ Device	Actions Assign Device to Site	/ice Type
Filter Image: Constraint of the second sec	Actions Assign Device to Site Provision	vice Type

フロアを選択するか、または、すでに選択されている場合、[Next] をクリックします。

(注) サイトをすべてのデバイスにマッピングするには、[Apply to All]を選択します。

ステップ4 APのRFプロファイルとして [High]、[Typical]、[Low] のいずれかを選択するか、または以前に定義されたカスタマイズされたものを選択します。下記の例では、[Typical] を選択して [Next] をクリックしています。

Devices Fabric			
Provision De	evices		
1 Assign Site	2 Configuration	3 Summary	
Serial Number	Device Name	RF Profile	
FDW2130B3L2	AP4001.7A70.6004	TYPICAL	~
		Apply to All	
FDW2130B3KR	AP500F.8086.7866	TYPICAL	~

ステップ5 [Deploy] をクリックすると、AP プロビジョニングの一環として、設定は次のように AP にプッシュされます。AP は再起動し、WLC に再度参加します。

Devices Fabric			
10010			
Provision Devices			
1 Assign Site 2 Configuration	3 Summan		
Assign site	Summary		
AP4001.7A70.6004			
	 Device Details 		
AP500F.8086.7866	Device Name:	AP4001.7A70.6004	
	Serial Number:	FDW2130B3L2	
	Mac Address	70:70:8b:20:29:00	
	Device Location:	Floor-1	
	RF Profile:	TYPICAL	
	Radio Type:	2.4GHz/5GHz	
	Channel Width:	20 MHz	
	2.4GHz/5GHz Data Rates	9,12,18,24,36,48,54/6,9,12,18,24,36,48,54	
			Cancel Deploy

ポップアップ表示されるウィンドウで [Run Now] をクリックします。

Provision Device			×
Run Now	O Schedule Later		
	Cancel	Apply	

AP が再起動されることを警告するメッセージが表示されます。OK をクリックします。



ステップ6 AP の [Provision Status] が [Success] と表示されます。

Device Name -	Device Type	IP Address	Site	Serial Number	Uptime	OS Version	OS Image	Sync Status	Last Provision	Provision Status
AP4001.7A70.6004	Unified AP	172.16.3.131	loor-1/Diegem	FDW2130B3L2	2days 20:44:26.110	8.5.110.0	Not Available	Managed	Jan 15 2018 14:03:20	Success
AP500F.8086.7866	Unified AP	172.16.3.130	loor-1/Diegem	FDW2130B3KR	2days 20:44:26.110	8.5.110.0	Not Available	Managed	Jan 15 2018 14:03:20	Success

- (注) 上のスクリーンショットは説明のみを目的としたものです。AP 導入の詳細については、ご使 用の設定では異なる場合があります。
- **ステップ**7 AP プロビジョニングの一環として、一部の設定は WLC にプッシュされます。

AP グループは、マッピング先のサイト(前述の手順3)の名前を付けて作成されます。

ululu cisco	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP FEEDB	ACK	Sa <u>v</u> e Configuration	<u>P</u> in	g Logout <u>R</u> efresh <mark>i H</mark> ome
WLANs	WLANs											Entries 1 - 5 of 5
 ▼ WLANs WLANs ▼ Advanced 	Current Filter	r: Nor	ne <u>(Chan</u>	<u>ge Filter] [Clea</u>	ar Filter]			Create New	Go			
AP Groups	WLAN ID	Туре	Profile Na	me		WLAN SSID		Admin Status	Security Polic	ies		
	<u>1</u>	WLAN	ssid-1			ssid-1		Disabled	[WPA2][Auth(8	02.1X)]		
	<u>17</u>	WLAN	Guest-WiFi	_Global_F_c4d	14f67	Guest-WiFi		Disabled	MAC Filtering		-	
	<u>18</u>	WLAN	pbagga-int	_Global_F_16a	cea8c	pbagga-internal		Disabled	[WPA2][Auth(P	5K)]		
	<u>23</u>	WLAN	pbagga-em	p_Global_F_3:	lddd44d	pbagga-employee-c	pen	Disabled	None		-	
	<u>24</u>	WLAN	pbagga123	4_Global_F_c8	cc58b2	pbagga1234		Disabled	[WPA2][Auth(P	5K)]	-	

下記の例では、APと	WLAN はこの AP グルー	-プに含まれています。
------------	-----------------	-------------

արտիս									Sa <u>v</u> e Conf	iguration	<u>P</u> ing	Logout <u>R</u> efresh
CISCO	MONITOR	<u>W</u> LANs	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK				n <u>H</u> ome
WLANs	AP Group	05								Entries 1 -	2 of 2	Add Group
WLANs	AP Group !	Name	A	P Group Desc	ription							
 Advanced AP Groups 	Floor3 TVPI default-grou	CAL 08d44										

Catalyst 9800 WLC の場合は、アクセスポイントに3つのタグが割り当てられます。

サイトタグ:サイトタグには、CAPWAP タイマー、AP ユーザ名、パスワードなどの AP 接続プロファイルの特性が 含まれています。

RF タグ: RF タグには、割り当てられた RF プロファイルの特性が含まれています。

ポリシータグ:ポリシータグには、WLAN およびポリシープロファイルのマッピングが含まれています。

タグの使用方法の詳細については、Catalyst 9800の設定モデルを説明する次の URL を参照してください。

Understand Catalyst 9800 Wireless Controllers Configuration Model

アクセスポイントに割り当てられたタグ:

Cisco Cat	alyst 9800-CL Wireless Controller		Welcome sand	% 🖹 🕻
Q Search Menu Items	Configuration * > Wireless * > Access Points	Edit AP		
		Location*	Global/colarado/den	Predowr
Dashboard	All Access Points	Base Radio MAC	7872.5dee.53c0	Predowr
Monitoring >	Number of AP(s): 1	Ethernet MAC	7872.5ded.cc1a	Next Ret
🔾 Configuration 🔹 🗸	AP Admin ✓ IP ✓ Base Radio ✓ AP AP Name ✓ Model Slots ✓ Status Address MAC Model	Admin Status		Boot Ver
(တြဲ) Administration 🧄 🤊	sand-4800- AIR-AP4800- 3 🥑 9.11.50.202 7872.5dee.53c0 Local	AP Mode	Local v	IOS Vers
Y Troubleshooting	ii	Operation Status	Registered	Mini IOS
ому		Fabric Status	Enabled	IP Conf
	> 5 GHz Radios	LED State	ENABLED	CAPWA
	> 2.4 GHz Radios	LED Brightness Level	8 🗸	DHCP IP
	> Dual-Band Radios	CleanAir <u>NSI Key</u>		Static IP
		RLOC IP	9.201.201.14	Time St
	Country	Control Plane Name	default-control- plane	Up Time
	LSC Provision	Tags	Controlle	
		Policy	PT_denve_BGL11_F V	
		Site	default-site-tag 🔻	
		RF	TYPICAL	

ポリシータグの詳細:

Q Search Menu Items	Configuration > Tags & Profiles > Tags		Edit Policy Tag		
Dashboard	Policy Site RF AP		🛦 Changes may	y result in loss of connectivity fo	or some clients that are associated to APs with th
Monitoring >	+ Add X Delete		Name*	PT_denve_BGL11_F	
	Policy Tag Name	× 1	Description	PolicyTagName PT_(
🔞 Administration	default-policy-tag	c	V WLAN-POLIC	Y Maps: 3	
°У́°	PT_denve_BGL11_F1_45efe				
X I roubleshooting	H 4 1 🕨 H 10 🗸 items per page		+ Add × Delet		
			WLAN Profile		V Policy Profile
			sand-mac-s_Glob	oal_F_4256d671	sand-mac-s_Global_F_4256d671
			sand-site2_Sanjo:	s_F_7a13809e	sand-site2_Sanjos_F_7a13809e
			sand-nonfa_Sanjc	os_NF_5aec7152	sand-nonfa_Sanjos_NF_5aec7152
				10 🔻 items per page	

RF タグの詳細:



サイトタグの詳細:

O Search Menu Items	Configuration > Tags & Profiles > Tags	Edit Site Tag					
	Policy Site RF AP	Name* default-site-tag					
	+ Add × Delete	AP Join Profile default-ap-profile v					
🔾 Configuration 🕠	Site Tag Name	Control Plane Name					
() Administration	default-site-tag	Enable Local Site					
💥 Troubleshooting							

オンボーディング クライアント

次に、クライアントがワイヤレスネットワークに参加できるように、ワイヤレスクライアントと SSID に IP プールを 割り当てる必要があります。

手順

ステップ1 Cisco DNA Center のホームページから、[Provision] > [Fabric] の順に移動します。

この例では、「California」という名前でファブリックを編集します。ファブリックにはすでにコント ロールプレーンとボーダーが設定されていると想定します。この項では、ワイヤレス LAN コントロー ラをファブリックに追加し、ワイヤレスクライアントでホストのオンボーディングを有効にする方法 について説明します。

Cisco DNA Center DESIGN	POLICY PROVISION	ASSURANC	Cisco DNA Center	DESIGN	POLICY	PROVISION	ASSURANCE	PLATFORM
Devices V Fabric Services			Devices 🗸 🛛 Fabric	Services				
SD-Access Fabri Choose a Fabric or Transit/Peer Network being	cs and Trans	sit/Pee	Fabric-Enabled Sites	•	All Fabrics Califori	> california Nia		
			EQ, Find Hierarchy					
Fabrics ()			 ✓ ② california ✓ ♀ ♀ Sanjose 				ф В11	
		1	▲ <u>n</u> B11	¢		C	B	
Default LAN Fabric	california				sa	and-cp.sand.com	sand-b	r-2 om
0 Site , 0 Fabric Device 0 Control Plane , 0 Border LAN	1 Site , 5 Fab 1 Control Plane	ric Device . 1 Border LAN			_			

ステップ2 Cisco DNAC 1.3.3 では、新しい VN を作成した場合、ファブリックに手動で追加する必要があります。1.3.3 に移行する場合、以前のバージョンに存在していたすべての VN がホストのオンボーディングページで使用可能になります。ホストのオンボーディングページで VN を使用できない場合は、サイトの横にある「歯車」アイコンをクリックして、ファブリックに VN を追加します。または、ホストのオンボーディングページから VN を追加します。追加する新しい VN にファブリックボーダーから設定されたハンドオフがあることを確認します。
Cisco DNA (Center	DESIGN	POLICY	PROVISION	ASSI	JRANCE			£ 24
Devices 🗸	Fabric	Services					Add	Virtual Network	
Fabric-Enabled Sites		•	All Fabrics COIrado	> colarado			Selected	virtual network(s) will be used	in the Fabric.
≣Q, Find Hierarchy			⊘ Fab	oric Infrastruc	ture	⊘ Host On			
🗸 🕗 colrado									
^ 🖑 colarad	lo	¢	> Au	thentication	Templa	te		Virtual Network 🔺	
				N's to a fabirc s	site			CAMPUS	
	Add VN T	o Site 🕕 🍼	 Virtual Networks Select a Virtual Network to associate one c 						
	Configure	Multicast①				issociate one c			
			c	Sritical Pool: No	t Selected			guest	
	Delete Si	te							
				INFRA_VN					

⊘ Fabric Infrastructure ⊘ Host Onboarding	Show Task Sta
✓ Virtual Networks	
Select a Virtual Network to associate one or more IP Pool(s) with the selecte	ed VN.
Critical Pool: Not Selected	Add Virtual Network
INFRA_VN corp	
	Add Virtual Network
Fabrics > colarado	Add Virtual Network
Fabrics > colarado Dirado	Add Virtual Network
Fabrics > colarado DIrado ⊘ Fabric Infrastructure	Add Virtual Network
Fabrics > colarado DIrado ⊘ Fabric Infrastructure	Add Virtual Network Selected virtual network(s) will be used in the Fabric Ultrual Network
Fabrics > colarado DIrado © Fabric Infrastructure	Add Virtual Network Selected virtual network(s) will be used in the Fabric Ultruel Network Comparis
Fabrics > colarado DIrado © Fabric Infrastructure	Add Virtual Network Selected virtual network(s) will be used in the Fabric Virtual Network CAMPUS
Fabrice 3 colarado Olfado © Fabric Infrastructure Virtual Networks Select a Virtual Network to associate one or more IP Pool(s) with the selected VN. Critical Pool: Not Selected	Add Virtual Network Selected virtual network(a) will be used in the Fabric Ulritual Network CAMPUS DEFAULT_VN

ステップ3 仮想ネットワークをサイトに追加したら、ファブリック内のクライアントが使用する VN に IP プール を関連付ける必要があります。VN(次の例では corp)をクリックし、使用可能なアドレスプールから ワイヤレスクライアントのアドレスプールを選択します。

重要:ワイヤレスクライアントがプールを使用する必要がある場合は、オプション [Wireless Pool] を有効にします。





[Add] をクリックして、プールを VN に関連付けます。トラ フィックタイプのオプション ([Data] または [Voice + Data]) は、有線クライアントにのみ関連します。ワイヤレスクライ アントに対する対応設定は、SSID レベルで実行されます。

Cisco DNA Center 1.3 以降のデフォルトでは、管理者はプール をワイヤレス LAN コントローラ (WLC) にプッシュするため に [Wireless Pool] オプションを有効にする必要があります。 これは、Cisco WLC にプロビジョニングされたレイヤ 2 VNID を最適化するための措置です。[Wireless Pool] オプションが有 効になっていないプールは、それぞれのレイヤ 2 VNID で WLC にプロビジョニングされません。

(注) クライアント認可の一環として VNID オーバーライドを
 使用する場合は、オーバーライドプールで [Wireless Pool] オ
 プションが有効になっていることを確認してください。

ステップ4 以前に設定したプールに、SSIDを関連付けます(必要に応じて、この SSID に参加するすべてのクラ イアントに割り当てられるように SGT を関連付けることもできます)。

Wir	eless SSID's & □ Enable Wireless	Multicast					Reset	Save
	SSID	Tupo	Cocurity	Traffic	Address Dool	Scalable Group	EQ Find	
	Name	туре	security	Туре	Address POOI	scalable Group		
	sand-site1- 1x	Enterprise	WPA2 Enterprise	Voice + Data	Choose Pool 9_10_60_0-corp 🛛 🔀 🗸	Assign SGT		<u> </u>

オンボーディング ゲスト クライアント

ゲスト SSID において、2つの実装方法を選択できます(後に、ゲスト設計の項でさまざまな使用可能な設計の詳細について説明します)。

- ゲストトラフィックに同じエンタープライズゲスト CP ノードを使用します。ゲスト SSID はファブリックの専用 ゲスト VN に関連付けられ、ファブリック セグメンテーション (VNI、SGT) を利用してゲストトラフィックを隔 離します。
- 2. ゲストトラフィック専用のゲストコントロールプレーンとボーダーを使用します。

両方のケースにおいて、SSID を設定する前に、VN をゲストが有効であるとマークする必要があります。これに より、これが適切に設定される必要がある「特別な」VNであることを Cisco DNA Center に通知することになり ます。

[Policy] > [Virtual Networks] の順に移動し、新しい VN を作成します。以下に示すように、[Guest Virtual Network] チェックボックスをオンにし、この仮想ネットワークに属するスケーラブルグループを追加します。

Cisco DNA Center DESIGN	POLICY PROVISION ASSURANCE PLATFORM	<u>∠</u> ⊜ Q III
Group-Based Access Control 🗸	IP Based Access Control V Application V Traffic Copy Virtual Network	
EQ Find Virtual Network	Create or Modify Virtual Network by selecting Available Scalable Groups. Virtual Network Name* guest Available Scalable Groups EQ Find Scalable Group EQ Find S	Reset
guest (1)	AU BY CA CO DE DS EM Auditors BYOD Cisco_A Contract Develop mant S Employe TS UN FW WC WI WC WP TrustSe Unknow flex, wir wired_c wireless wireless wireless	

VNをサイトに追加するには、クライアントオンボーディングの項のステップ2を参照してください。

これで、オンボーディングセッションで SSID を設定できます。一般的なコントロールプレーンノードについては、 手順は、他の SSID の設定と同様です。ゲストクライアントに使用している VN をクリックし、使用可能なアドレス プールからワイヤレスクライアントのアドレスプールを選択します。[Update] をクリックします。次の例を参照して ください。

California					
⊘ Fabric Infrastructure	⊘ Host Onboarding				Show Task S
> Authentication Temp	late				
✓ Virtual Networks					
Select a Virtual Network to	associate one or more IP Pool(s) with the s	selected VN.			
Critical Pool: Not Select	ed				Add Virtual Network
DEFAULT_VN	INFRA_VN	corp	gu	est X	

Edit Virtual Network: guest	Edit Virtual Network: guest					
< Back	Basic View	Add				
guest_pool (9.10.61.0/24)	Actions \sim	EQ Find				
Authentication <u>9</u> 0ifØ_61_0-gL Scalable Group	IP Addr Pool	ress Authentication Policy Traffic Scalable Group				
Traffic						
Critical Pool	guest 1	_poo 9_10guest Data -				
		Showing 1 of 1				

DNAC 1.3 以降では、[Wireless SSID's] サブセクションでこの IP プールをワイヤレス SSID に関連付けるには、 [Wireless Pool] チェックボックスをクリックする必要があります。

次に、通常のエンタープライズ SSID に対してステップ 4 で行ったように、ゲスト SSID をプールに関連付けて [Save] をクリックします。

V Wir	eless SSID'	3						
	Enable Wireles	Reset	Save					
	SSID Name	Туре	Security	Traffic Type	Address Pool	Scalable Group		
	sand-guest- 1	Guest	Web Auth	Data	Chaose Paol	Assign SGT		<u> </u>
	sand-site1- 1×	Enterprise	WPA2 Enterprise	Voice + Data	9_10_61_0-guest	Assign SGT		~

ゲストトラフィック専用のボーダーとコントロールプレーンを使用する場合は、ゲストコントロールプレーンとボー ダーをファブリックに追加する必要があります。デバイスアイコンをクリックしてデバイスの詳細ページを開き ます。

下記のウィンドウがポップアップ表示され、ボーダーとコントロールプレーンの両方の機能を選択できます。また、 ゲストが有効であるとマークした VN がここに表示されます。内部的に Cisco DNA Center はファブリック設定を処理 してゲスト SSID をプールに関連付け、そのプールをゲストコントロールプレーンおよびボーダーにマッピングし ます。

注目すべき重要なポイントは、ゲストボーダーおよびコントロールプレーンを同じデバイスに配置することが推奨される点です。ゲストボーダーからのハンドオフは手動プロセスで、管理者は外部ドメインへのハンドオーバーを行う ための任意のプロトコルを設定できます。

All Fathjos > colarado COLTACO	sand-csr-2.sand.com (9.1.0.249) ❀ ⊘Reachable Uptime: 30 days 5 hours 42 minutes					
Fabric Infrastructure	🛃 Run Commands 🛛 🕾 View 36					
() 2 device(s) in this site are not comp	Details Fabric Port Channel Configuration Interfaces					
Click on the node	Remove From Fabrio Fabric Edge Node Border Node Control Plane Guest Border / Control Plane 					

Enable Guest		×
Select the role(s) you intent to assign		
Set as default border		
Routing Protocol		
BGP ✓		
● ASPLAIN ○ ASDOT ○ ASDOT+		
Routing AS number/process 65003		
Select one quest virtual network		
guest		
	Cancel	Enable

ステップ5 ステップ4で SSID をプールに関連付けした場合は、WLC で、SSID の [Admin Status] が [Enabled] に なっていることが確認できます。

Cisco Cataly	st 9800-CL Wireless Controller	🖀 🌾 🖺 🌣 🖗 🕢 🎜 Search APs and C
Q Search Menu Items	Configuration > Tags & Profiles > WLANs	
Dashboard	+ Add × Delete Enable WLAN Disable WLAN Number of WLANs selected : 0	
Configuration >	Status v Name v ID v S	SSID v Security
~	sand-guest_Sanjos_F_927bb184 17 e	sand-guest-1 [open],MAC Filtering
(O) Administration >	sand-site1_Sanjos_F_6e15a102 18	sand-site 1-1x [WPA2][802.1x][AES]
~~	H 4 1 - H 10 - items per page	

- **(注)** 上の WLC のスクリーンショットは説明のみを目的としたものです。WLAN 名とセキュリティ は、ご使用の設定では異なる場合があります。
- **ステップ6** これで、クライアントはファブリック対応のワイヤレス SSID に接続可能です。WLC に移動し、接続されたクライアントの詳細を確認できます。

[Monitoring] > [Wireless] > [Clients] に移動します。

Cisco Cat	Catalyst 9800-CL Wireless Controller Welcome sand											
Q Search Menu Items	Monitoring >> Wireless >> Clients											
📷 Dashboard	Clients Steeping Clients Excluded Clients											
Monitoring >	× Delete	× Delete										
Configuration >	Total Client(s) in the Network: 2 Number of Client(s) selected: 0											
(O) Administration >	Client MAC Address	 IPv4 Address 	AP Name	SSID	V WLAN ID	State v	Protocol	√ UserNa	ime v			
💥 Troubleshooting	1c36.bb00.1704	9.10.60.204	sand-3800-site1	sand-site1-1x	18	Run	11ac	sand				
	1c36.bbee.09b4	9.10.61.200	sand-3800-site1	sand-guest-1	20	Run	11ac					
	14 4 1 > 10 y items pe	r page										

クライアント ファブリック ステータスと SGT タグが、認証ルールに基づいて ISE から WLC にプッシュされていることを確認できます。

Monitorin	g > Wireless > Clients						Client				
							360 View	General	QOS Statistic	s ATF Statistics	Mobility I
Clients	Sleeping Clients Exc	luded	Clients				Client Prop	erties	AP Properties	Security Information	Client St
							VLAN			uerauit	
X De							Multicast VL	AN		0	
							Server IP			9.1.0.20	
Total C	lient(s) in the Network: ∠						11v DMS Ca	pable		No	
Number	of Client(s) selected: U						QoS Map Ca	apable		No	
	Client MAC Address	v	IPv4 Address∨	IPv6 Address	AP Name v	SSID	FlexConnect	FlexConnect Data Switching			
	1c36.bb00.1704	ж	9.10.60.204	fe80::6d87:cd22:da30:4472	sand-3800-site1	sand-site 'N	HexConnect	Authenticat	N/A		
	1c36.bbee.09b4	Ж	9.10.61.200	N/A	sand-3800-site1	sand-guest	FlexConnect	Central As	ociation	N/A	
	1 b 10 itema na						Control plane name			default-control-plane	
		n page	3				antenna O			9 s ago	36 dBm
							antenna 1			9 s ago	36 dBm
Click	on the client						EoGRE			No/Simple client	
mac	to open the						Туре			55 17	
	details						Data			11	
							Fabric				
							Enbrin Statue			Evolution	
							Papric Status			Enabled	
							REUC			9.254.254.70	
							COL			8210	
							L SGI	mina Maiah	box List	٥١	
							Assisted R08	anang weigh	DUT LISE		

マルチキャストの設定

ワイヤレスでマルチキャストを有効にするには、最初に有線ネットワークでマルチキャストを設定する必要がありま す。次の手順で説明されているように、Cisco DNA Center により、両方の設定が非常に簡単になります。



) ワイヤレスマルチキャストは慎重に検討する必要があります。

マルチキャスト IP トラフィックが AP に到達すると、これらのパケットはブロードキャストレイヤ2フレームとして 無線で送信されます。これは、基本的にトラフィックが最高の必須データレート(接続されたすべてのクライアント に到達できるように)で送信されることを意味し、伝送フレームが認識されないため、電波でコリジョンが発生し、 フレームが損失します。これは、電波を介したマルチキャストトラフィックの達成可能なスループットに影響を与え ます。Wi-Fi 経由でマルチキャストトラフィックのパフォーマンスと信頼性を向上させるために、シスコは AP でマル チキャストフレームをユニキャストフレームに変換する VideoStream 機能を開発し、前述の問題を解決しました。 VideoStream (マルチキャスト ツー ユニキャスト機能とも呼ばれる)は、Cisco DNA Center 1.3 以降のテンプレートを 使用してサポートされます。 ステップ1 [Fabric] > [San Jose] > [Floor 3] でサイトの歯車メニューをクリックし、[Configure Multicast] をクリック します。これをクリックすると、ファブリックでマルチキャストを有効にする手順のウォークスルー が表示されます。

EQ Fin
I VLAN.

ステップ2 [Enable Multicast] ワークフローで、[Let's do it] をクリックしてマルチキャストを設定します。



ステップ3 [Native Multicast] または [Headend Multicast] を選択し、[Next] をクリックします。

Cisco DNA Center design policy provision assurance platform	۵	q	Ш	¢	0	ï
Enabling Multicast						
Multicast can be used to streamline packet distribution without over-loading the network with the same packets. It is especially beneficial if your network users conduct realtime streaming or conferencing. Choose the method first.						
How would you like to implement multicast is your network? Native multicast Read-end registration						
← Exit					Next	

ステップ4 Floor3のマルチキャスト設定で使用する仮想ネットワークを選択し、[Next]をクリックします。

Cisco DNA	Cente	CT DESIGN POLICY PROVISION ASSURANCE PLATFORM			Q	ш	¢	0	
	Virtu	ual Networks							
	Select	your virtual networks to use in your multicast setup for Floor3							
	2 S	Selected	EQ Find	i					
		Name 🔺							
		Campus							
		DEFAULT_VN							
		Guest							
		тот							
		Showing 4 of 4							
🗧 Exit		Rev	iew (В	ack			Next	

ステップ 5 [Multicast Pool mapping] ページで、マルチキャストトラフィックの送信に使用する IP プールを選択し ます。マルチキャストを有効にするには、すべてのファブリックノードで VN ごとに IP アドレスが必 要になります。[Next] をクリックして次のセクションに進みます。

Cisco DNA Center design policy provision assurance platform	۷	Q	ш	¢	0	
Multicast Pool mapping						
Every Fabric node requires an IP Address per VN to enable multicast.						
Campus						
IP Pools* Campus-Multicast-SJC (1.1.1.0)						
Guest						
IP Pools*						
EQ Search Dropdown						
Campus-Multicast-SJC (1.1.1.0)						
Guest-Multicast-SJC (2.2.2.0)						
Exit All changes saved Review		Back				

ステップ6 [SSM] または [ASM] を選択します。

Cisco DNA Center design policy provision assurance platform	٢	Q	ш	¢	0	
Select SSM or ASM						
The Source Specific Multicast (SSM) feature is an extension of IP multicast where traffic is forwarded to receivers from only those multicast sources to which the receivers have explicitly joined. For multicast groups configured for SSM, only source-specific multicast distribution trees (no shared trees) are created.						
Multicast can be used to streamline packet distribution without over-loading the network with the same packets. It is especially beneficial if your network users conduct realtime streaming or conferencing. Choose the method first.						
© SSM						
⊖ ASM						
C Exit Review		Back			Next	

ステップ7 SSM の場合はマルチキャスト IP 範囲を選択します。仮想ネットワークごとに IP グループの範囲を追加して、SSM リストを設定します。

Cisco DNA Center Design Poli	CY PROVISION ASSURANCE PLATFO	RM		٢	Q	 ¢	Ø	1
SSM								
Configure your SSM list by add	ding an IP group range for each virtual netwo	rk.						
Campus								
Group Range 232.0.0.0	Wildcard Mask 0.255.255.255	+						
Guest								
Group Range 232.0.0.0	Wildcard Mask 0.255.255.255	+						
Exit All changes saved			Review		Back		Next	

ステップ 8 すべてのマルチキャスト設定を確認し、[Finish] をクリックしてマルチキャストを展開します。

Cisco DNA Center design policy provision assurance platform	29 (ર ⊞	¢	0	
Summary Review your multicast settings and make any changes. Delete Multicast Config					
 Enabling Multicast Edit Implementation Head-end replication 					
Virtual Networks Edit Selected VNs Campus Guest					
 Multicast Pool mapping Edit Campus Campus-Multicast-SJC (1.1.1.0) Guest Guest-Multicast-SJC (2.2.0) 					
V Select SSM or ASM Edit Multicast Type SSM					
SSM Edit Campus 232.0.0.0 0.255.255.255 Guest 232.0.0.0 0.255.255.255					
Exit All changes saved				Finish	

これで、マルチキャスト設定ワークフローが完了します。

CISCO DNA Center design policy provision assurance platform	
Done! Multicast is initiated successfully! Multicast is complete!	
Go to fabric site	

ステップ9 有線ファブリック インフラストラクチャにマルチキャストを展開した後、マルチキャストを SD-Access ワイヤレス インフラストラクチャで有効にする必要があります。ワイヤレスでマルチキャスト を有効にするオプションは、ホストのオンボーディングページの SSID 設定にあります。

Cisco DNA Center のホームページから次のように移動します。

[Provision] > [Fabric] > ファブリックサイト > [Host Onboarding] > [Wireless SSID's]

Cisco DNA Center	DESIGN	POLICY	PROVISION	ASSURANCE	PLATFORM				<u>~</u> 23	Q		۵	٥
Devices V Fabric	Services												
Fabric-Enabled Sites	•	All Fabrics > California	в11 Э										
EQ Find Hierarchy		⊘ Fabri	c Infrastructu	ure 🕑 Ho	st Onboarding						s	how Ta	ask St;
 ✓		> Auth	nentication 1	Femplate									
	Ŷ	> Virtu	ial Networks	S									
		√ Wire	eless SSID's Z Enable Wirele	ess Multicast					Reset			Save	
			SSID Name	Туре	Security	Traffic Type	Address Pool	Scalable Group	=	< Fina			
			sand-site1- 1x	Enterprise	WPA2 Enterprise	Voice + Data	Choose Pool 9_10_60_0-corp	Assign SGT			~	_	

SD-Access ワイヤレス:内部の仕組み

この項では、SD-Access ワイヤレスの基本的な動作について説明し、Cisco DNA Center の「舞台裏」で何が起こって いるのかを明確に理解できるようにします。このフローでは、設計フェーズを完了し、実装およびプロビジョニング フェーズのみに焦点を当てていることを前提としています。

ファブリックに WLC を追加

図 15. ファブリックに WLC を追加



Cisco DNA Center では、最初にファブリックドメインに WLC をプロビジョニングしてから追加します。

- ファブリック設定が WLC にプッシュされます。WLC はファブリックを認識します。最も重要なことは、 ファブリック コントロール プレーンへのセキュアな接続を確立するために、WLC でログイン情報を設定す ることです。
- 2. WLC は SD-Access ワイヤレスへの参加が可能になります。



- 管理者ユーザは、Cisco DNA Center 内のプールを INFRA_VN 内の AP 専用(これはプール定義内の [AP Provisioning] ボックスをチェックすることを意味します)に設定します。Cisco DNA Center は、AP VLAN と関連 テンプレートをファブリックエッジに事前プロビジョニングします。Cisco DNA Center 1.3 以降では Autoconf を使 用し、リリース 1.2 ではマクロを使用します。
- 2. AP は電源に接続されオンになります。FE のデバイス分類子は Cisco Discovery Protocol を介して AP であることを 検出し、テンプレート設定を適用してスイッチポートを正しい VLAN に割り当てます。
- 3. AP は DHCP 経由で IP アドレスを取得します。AP は、ファブリックに有線接続された「特別な」ホストです。

<u>》</u> (注)

Cisco DNA Center 1.3 の時点では、デバイスをアクセスポイントとして識別するために Autoconf が使用されま す。Autoconf は、ポートが [No Authentication] モードに設定されている場合にのみ機能します。スイッチポー トテンプレートはホストオンボーディングの設定時に選択します。次のスクリーンショットを参照してくだ さい。

Devices	Fabric			
Diegem)>			
Select Devic	es Host Or	nboarding		
Select	Authenticatio	on template		
O Closed	d Authentication	O Easy Connect	No Authentication	O Open Authentication

その他の認証テンプレートを選択すると、管理者ユーザは、右の IP プールを AP のスイッチポートに静的にマッピン グする必要があります。AP はクローズド認証ポートでもサポートされます。ワークフローと手順は AP オンボーディ ングの項で定義されています。

図 17. AP オンボーディング



- 1. ファブリックエッジでは、コントロールプレーンノードで AP の IP アドレスが登録されます。これで、AP ロケー ションはファブリックで認識されるようになりました。
- 2. AP は従来の方法(DHCP オプション 43、DNS、プラグアンドプレイ)を使用して WLC について学習し、WLC に接続します。ファブリック AP はローカルモード AP として参加します。
- 3. WLC は AP がファブリック対応 (つまり、Wave 2 または Wave 1 AP) かどうかを確認します。
- 4. AP モデルがサポートされている場合、WLC は CP に AP がファブリックに接続されているかどうかを問い合わせ ます。

図 18. RLOC および EID 情報の交換



- 5. CP は RLOC 情報で WLC に応答します。つまり、AP はファブリックに接続されており、WLC の AP 詳細情報が ファブリック対応として表示されるようになります。
- WLC は、ホスト トラッキング データベースに AP のレイヤ 2 LISP 登録を行います(これにより、AP は「特別な」セキュアクライアントとして登録されます)。これは WLC から FE への重要なメタデータ情報の転送に使用されます。
- 図 19. AP の VXLAN トンネルの作成



- 7. WLC によるこのプロキシ登録に応答して、CP はファブリックエッジに通知して、WLC から受信したメタデータ を渡します(AP であることを示し、AP の IP アドレスを提供するフラグ)。
- ファブリックエッジは情報を処理し、このクライアントが AP であることを認識して、指定された IP アドレスへの VXLAN トンネルインターフェイスを作成します(最適化:スイッチ側はクライアント接続を待機している状態)。

クライアント オンボーディング フロー

図 20. 認証およびポリシーの取得

- クライアントはファブリック対応 WLAN に対して認証されます。WLC は ISE からクライアント SGT を取得し (WLAN が 802.1X 認証用に設定されていることを前提とします)、AP をクライアントのレイヤ 2 VNID および SGT で更新します。WLC は、(AP への接続プロセス中に保存された)自身の内部レコードから AP の RLOC を認 識しています。
- 2. WLC プロキシはクライアントのレイヤ 2 情報を CP に登録します。これは LISP 変更メッセージであり、クライア ント SGT などの追加情報を渡します。
- 3. CP は FE に通知し、FE はクライアントの MAC アドレスをレイヤ 2 転送テーブルに追加し、SGT に基づいて ISE からポリシーを取得します。
- 図 21. DHCP フロー



- 4. クライアントが DHCP 要求を開始します。
- 5. AP はレイヤ 2 VNI 情報を使用して、その要求を VXLAN にカプセル化します。
- 6. ファブリックエッジはレイヤ 2 VNID を VLAN と VLAN インターフェイスにマッピングし、エニーキャスト IP を DHCP リレーとして使用して、オーバーレイの DHCP を転送します(有線ファブリッククライアントの場合と同様)。
- 図 22. オンボーディングプロセスの完了



- 7. クライアントは DHCP から IP アドレスを受信します。
- DHCP スヌーピング(スタティックの場合 ARP またはこの両方)は、ファブリックエッジによるホスト トラッキング データベースへのクライアント登録をトリガーします。これで、クライアント オンボーディング プロセスは完了します。

クライアント ローミング フロー

図 23. クライアント情報の更新



1. クライアントは FE2 の AP2 にローミングします(スイッチ間ローミング)。AP2 は WLC に通知します。

2. WLC は、クライアント情報 (SGT、RLOC IP アドレス)を使用して AP 上の転送テーブルを更新します。

3. WLC は、FE2 の新しい RLOC を使用して CP でレイヤ 2 MAC エントリを更新します。

図 24. コントロールプレーン通知



4. CP は次のように通知します。

- ファブリックエッジ FE2 (「ローミング先」のスイッチ)に、VXLAN トンネルを参照する転送テーブルにク ライアント MAC を追加するように通知します。
- ファブリックエッジ FE1 (「ローミング元」のスイッチ)に、ワイヤレスクライアントのクリーンアップを実行するように通知します。
- ファブリックボーダーに、このクライアントの内部 RLOC を更新するように通知します。
- 5. FE はトラフィックの受信時に、CP でレイヤ 3 エントリ(IP アドレス)を更新します。

FE2 に同じ VLAN インターフェイス (エニーキャストゲートウェイ) があるため、ローミングはレイヤ2です。

SD-Access のワイヤレス統合の設計

前述のとおり、SD-Accessファブリックでワイヤレスを展開するには、次の2つの方法があります。

- Cisco Unified Wireless Network ワイヤレス OTT: SD-Access ファブリックは IP トランスポートネットワークであり、ワイヤレスはピュアなオーバーレイです。
- SD-Access ワイヤレス:ワイヤレスが SD-Access に統合され、ファブリックのすべての利点を活用できます。

Cisco Unified Wireless Network ワイヤレス OTT

この場合は、従来のワイヤレスが SD-Access ファブリック上で実行されます。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。

図 25. Cisco Unified Wireless Network ワイヤレス OTT



- ・CAPWAP を使用する従来型の Cisco Unified Wireless Network アーキテクチャがコントロールプレーンとデータプレーンで使用され、WLC で終端します(中央モード)。
- ・SD-Access ファブリックは AP と WLC 間の有線インフラストラクチャ内の伝送路にすぎません。
- ・CUWN ワイヤレス OTT は完全な SD-Access へ移行するためのステップです。

2 種類の展開のさまざまな設計上の考慮事項を検討する前に、WLC のどのインターフェイスが使用されるのか、また 異なる展開でどのように使用されるのかを明確にしましょう。

WLC インターフェイス

どちらの SD-Access 統合モードでも、SD-Access ワイヤレスと OTT に適用される WLC インターフェイスについて考慮します。

図 26. WLC インターフェイス



- ・WLC は、ファブリックネットワーク外のアンダーレイネットワーク(グローバル ルーティング テーブル)に接続されます。
- ファブリックネットワークに接続されている AP は、オーバーレイネットワークにあるとみなされます。つまり、ファブリックエッジのポートはすべてファブリック対応ということになります。オーバーレイにポートを接続し、アンダーレイに他のポートを接続することはできません。
- ・管理インタフェースは、WLC と AP との CAPWAP コントロールチャネルと、AAA、Cisco DNA Center などの共 有サービスとの通信に通常使用されています。
- SD-Access ワイヤレスを使用して展開した場合、管理インターフェイスはコントロールプレーンノードとの統合 にも使用されます。
- ・冗長ポート (RP) はアクティブおよびスタンバイ HA ペア間の高可用性 (HA) 通信に使用され、ボックス障害 またはネットワーク障害時にシームレスでステートフルなスイッチオーバーを提供します。
- ・ダイナミック インターフェイスは、ワイヤレスがオーバーザトップで導入されている、つまりファブリック イン フラストラクチャが、集中型処理のために WLC に返送される CAPWAP コントロールおよびデータチャネルの伝 送路にすぎない場合のみ使用されます。
- サービスポートは、通常どおり、アウトオブバンド管理に使用されます。

Cisco Unified Wireless Network ワイヤレス OTT ネットワーク設計

まず最初に、Cisco Unified Wireless Network ワイヤレス OTT とは何でしょうか。このモードでは、AP と WLC 間の従来 の CAPWAP トンネルがファブリックネットワークへのオーバーレイとして実行されます。つまり、ファブリックは CAPWAP のトランスポートとなります。Cisco Unified Wireless Network ワイヤレス OTT を導入する理由は主に 2 つあり ます。

- OTT ソリューションは移行のステップとなる場合があります。お客様はまず有線インフラストラクチャを SD-Access ファブリックに移行し、ワイヤレスネットワークを「そのまま」の状態で維持する必要があります。つま り、現在ワイヤレスが動作する方法は変えません。これは、有線およびワイヤレス インフラストラクチャを管理 するさまざまな IT オペレーションチーム、有線ネットワークのアップグレードを最初に決定するさまざまな購入 サイクルが原因となっている可能性があります。または単に IT チームがワイヤレス部分を統合する前にまず有線 側のファブリックを熟知したいと思っていることが原因である可能性もあります。
- また、ワイヤレス OTT を導入するための別の理由として、お客様はワイヤレスのファブリックに移行したくない、またはできない可能性があります。これは、所有している大半の AP が SD-Access でサポートされていない古い AP (802.11n 以前)であるか、SD-Access ワイヤレス (8.5 以上)を実行するために必要な新しい WLC ソフトウェアの証明書を必要としている可能性があります。または、単にお客様がワイヤレスの「そのまま」の状態を維持し、変更を加えたくない可能性もあります。

各コンポーネントの最も重要な設計考慮事項を考えてみましょう。

WLC

図 27. WLC 接続



図 27 に示すように、ファブリックの外部に WLC(または冗長性のために複数の WLC)を接続することを推奨しま す。WLC は、Cisco SD-Access ソリューションのボーダーノードに接続することもできます。そのための設定は、 ボーダーノードで手動で行う必要があります。通常、WLC はネットワークの中央(データセンターまたは共有サー ビス)に接続されているため、WLC はアクセススイッチであることの多いファブリックエッジノードには接続され ていないのが現実的です。

WLC はファブリックの外側に位置するため、ボーダーノードは管理インターフェイスサブネット(この例では 192.168.1.0/24)と AP の IP プール(この例では 10.1.0.0/16)間の到達可能性を提供し、CAPWAP トンネルが形成さ れ、AP は WLC に登録できます。Cisco DNA Center 1.3 では、AP は、グローバル ルーティング テーブルにマップされ ている INFRA_VRF にあるため、ルートリークは必要ありません。



シスコは、SDA ファブリックネットワークでは Cisco Unified Wireless Network Centralized モードと SD-Access ワイヤレスのみをサポートしています。Cisco FlexConnect® モードは、将来のリリースでサポートされます。

アクセスポイント

図 28. AP VLAN



アクセスポイントは単にファブリック インフラストラクチャの有線ホストであるため、ファブリックエッジスイッチ のオーバーレイスペースに接続され、EID スペース内の特定のプールが割り当てられます。ファブリックの利点の1 つは、すべての AP を1つの大きなサブネットに割り当てることができることです。これは、キャンパス全体で同じ で、サブネットの設計を単純化し、オンボーディングの操作を簡素化します。

AP は有線クライアントのようなものなので、接続されているファブリックエッジスイッチによってファブリック コ ントロール プレーン ノードに登録されるため、ファブリック内でその位置がわかり、AP に到達します。この時点 で、CAPWAP トンネルは、ファブリックを介して AP から WLC に形成されます(図 29 を参照)。

図 29. AP から WLC への CAPWAP トンネル



ワイヤレス LAN

図 30. ワイヤレス LAN 接続



先ほど説明した、ワイヤレスが「そのまま」の状態で動作するというのは、WLC のワイヤレス SSID がダイナミック インターフェイスの形式で WLC の VLAN またはサブネットにマッピングされ、ワイヤレストラフィックが WLC の 有線ネットワークに入り、そこでルーティングされるということです。 ボーダーノードは、ワイヤレス クライアント サブネットをファブリックにアドバタイズするため、ファブリックホ ストとワイヤレスクライアント間に接続を確立できるようになります。

クライアント トラフィック フロー

ワイヤレス クライアントがトラフィックを送信すると、CAPWAP トンネルが AP から WLC に構築されます。 CAPWAP トラフィックは、AP からファブリックエッジスイッチに到達し、VXLAN にカプセル化して、ボーダーに 転送します。外側の VXLAN ヘッダーは削除され、基礎となる CAPWAP パケットは WLC に転送されます。



Cisco Unified Wireless Network と同様に、クライアントは WLC によって認証およびオンボーディングされ、ワイヤレ ス クライアント トラフィックはファブリックの外部に送信されます。図 32 は、ワイヤレスクライアントとローカル のファブリック有線ホスト間の通信トラフィックフローを示しています。

図 32. ワイヤレスクライアントとローカルのファブリック有線ホスト間のトラフィックフロー



ワイヤレストラフィックは、WLC に至るまで送信され、WLC ダイナミック インターフェイス VLAN でブリッジされ、 ボーダー経由でファブリッククライアントにルーティングされます。今日、この方法で通常の有線ネットワークは機能 し、ワイヤレスでも同様です。ファブリックの場合は、ファブリックホストがファブリック外部の既知の宛先に通信し ます。

オーバーレイとしてのワイヤレス (OTT) : 設計考慮事項

OTT モードの重要な設計上の考慮事項のいくつかを要約します。

- ・すべての AP と WLC モードがサポートされます。ワイヤレスはファブリックに統合されていないため、ハード ウェアおよびソフトウェアモデルに関する要件はありません。
- ・WLC はファブリックの外部に接続され、任意のコードバージョンをサポートしています。

- ・二重(VXLAN で CAPWAP)カプセル化によるパケットのフラグメント化を防ぐために、パスに沿った最大伝送 ユニット(MTU)を増やすことをお勧めします。これは、パス内のすべてのスイッチがシスコ製品であり、ジャ ンボ フレームをサポートする場合は、自動的に行われます。
- •FCS では、OTT としてサポートされる唯一のモードは一元化されています。

・FCS では Cisco Prime を使用し、OTT ワイヤレス ネットワークを管理します。

図 33. OTT モードの設計上の考慮事項



SD-Access ワイヤレスネットワーク設計

SD-Access ファブリックのすべての利点を得るためには、統合された設計、したがって SD-Access ワイヤレスソリュー ションを選択する必要があります。アーキテクチャの見解から、統合は、次の 3 つの主な利点をもたらします。

- シンプルな管理およびコントロールプレーン: Cisco DNA Center は、ファブリックを起動し、数回クリックするだけでワイヤレス統合を設定するのに必要な自動化を提供します。集中管理型ワイヤレス コントロール プレーン (CAPWAP ベース)は、今日の Cisco Unified Wireless Network コントローラと同じ機能を提供します。
- 最適化されたデータプレーン:データプレーンは、通常生じる問題なしで分散されます。ファブリックのおかげで、複数のアクセススイッチにまたがる VLAN がなくなり、サブネット化が簡単になります。
- 統合されたポリシーとエンドツーエンドのセグメンテーション:ポリシーは補足的なものではなく、アーキテク チャ全体で一元的に統合されています。VXLAN ヘッダーは、VRF (VNID) と SGT の両方の情報を伝送し、エン ドツーエンドの階層的なセグメンテーションを提供します。

図 34 は、統合設計の利点をまとめたものです。

図 34. 統合設計の利点

- ・集中管理型ワイヤレス コントロール プレーン: Cisco Unified Wireless Network 導入環境で提供されている革新的 な RF 機能が、SD-Access ワイヤレスでも活用されます。IT 導入を簡素化させる無線リソース管理(RRM)、ク ライアント オンボーディング、クライアントモビリティなどに関して、ワイヤレスの運用は Cisco Unified Wireless Network の場合と同じです。
- ・分散型データプレーンの最適化:データプレーンは、トラフィックの分散に通常伴う処理(VLAN のスパニング、サブネット化、大規模なブロードキャストドメインなど)なしに最適なパフォーマンスと拡張性を実現するために、エッジスイッチに分散されます。
- ・場所を問わないシームレスなレイヤ2ローミング: SD-Access ファブリックにより、クライアントは同じ IP アドレスを保持しながらキャンパス全体でシームレスにローミングできます。
- ・ゲストおよびモビリティのトンネリングの簡素化:アンカー ワイヤレス コントローラ (WLC) が不要になり、 フォーリンコントローラをホッピングせずにゲストトラフィックをネットワークエッジ (DMZ) に直接送信でき ます。
- ・ポリシーの簡素化: SD-Access では、ポリシーとネットワークの構成体 (IP アドレスや VLAN) との間の依存関係が解消されるため、有線クライアントとワイヤレスクライアントのポリシーを定義および実装する方法がシンプルになります。
- ・セグメンテーションの簡略化:セグメンテーションはファブリック内をエンドツーエンドで伝達され、仮想ネットワーク ID (VNI) とスケーラブルグループタグ (SGT) に基づいて階層化されます。有線とワイヤレスの両方のユーザに同じセグメンテーションポリシーが適用されます。

ワイヤレス統合ソリューションの設計要素を簡単に分析します。

コントローラ

図 35. ファブリックに外部接続する WLC



図 35 に示すように、外部からファブリックに WLC(または冗長性のために複数の WLC)を接続することを推奨し ます。

通常、WLC はネットワークの中央(データセンターまたは共有サービス)に接続されているため、WLC はアクセス スイッチであることの多いファブリックエッジノードには接続されていないのが現実的です。

WLC はファブリックの外側に位置するため、ボーダーノードは管理インターフェイスサブネット(この例では 192.168.1.0/24)と AP の IP プール(この例では 10.1.0.0/16)間の到達可能性を提供し、CAPWAP トンネルが形成さ れ、AP は WLC に登録できます。AP は、グローバル ルーティング テーブルにマップされている INFRA_VRF にある ため、ルートリークは必要ありません。 また、WLC はアクセスポイントと同じ場所に配置する必要があります。この要件は Cisco Unified Wireless Network の ローカルモード AP の場合と同じです。AP と WLC の間の最大遅延は 20 ミリ秒未満にする必要があり、これは通常、 WLC を AP から WAN を介して配置できないことを意味します。

アクセスポイント

図 36. SD-Access ワイヤレスにおけるアクセスポイント



SD-Access ワイヤレスでは、APをファブリックエッジノードに直接接続する必要があります。アクセスポイントは ファブリック インフラストラクチャの「特別な」有線ホストであるため、ファブリックエッジスイッチのオーバーレ イスペースに接続され、EID スペース内の特定のプールが割り当てられます。ファブリックの利点の1つは、すべて の APを1つの大きなサブネットに割り当てることができることです。これは、キャンパス全体で同じで、サブネッ トの設計を単純化し、オンボーディングの操作を簡素化します。

AP は有線クライアントのようなものなので、接続されているファブリックエッジスイッチによってファブリック コ ントロール プレーン ノードに登録されるため、ファブリック内でその位置がわかり、AP に到達します。AP は、OTT 設計について説明した際と同じ方法で、コントロールプレーンの機能のために WLC への CAPWAP トンネルを形成し ます。

ワイヤレス LAN



図 37. SD-Access ワイヤレスにおけるワイヤレス LAN

ファブリック機能は WLAN 単位で有効になります。ファブリック対応の WLAN の場合、クライアントトラフィック は分散され、中央コントローラには送られませんが、AP の VXLAN にカプセル化されて最初のホップのスイッチに 送信されます。 一元化された CAPWAP WLAN は、共通のファブリック対応 WLC を使用して、同一または異なる AP 上のファブリッ ク対応の WLAN と共存できます。これは「混合モード」と呼ばれ、Cisco DNA Center 1.1 で、既存のファブリックまた は Cisco Unified Wireless Network ワイヤレス構成を持たない WLC 展開をサポートしているため、新しい展開の場合に のみ使用できます。

クライアントフロー

ファブリック対応 SSID の場合、ワイヤレス クライアント トラフィックはスイッチで分散されるため、中央コントローラ へのヘアピニングはありません。有線クライアントへの通信は、ファブリックを通じて直接行われ、最適化されます。



図 38. SD-Access ワイヤレスにおけるクライアントフロー

クライアントサブネットはファブリックエッジスイッチに分散され、WLC で動的インターフェイスとクライアント サブネットを定義する必要はありません。クライアントサブネットは、すべてのファブリックエッジスイッチでエ ニーキャストゲートウェイを使用して定義され、VLAN にマッピングされます。これは、ワイヤレスクライアントが どこに接続しても、サブネットのために同じゲートウェイと話すことができることを意味します。つまり、クライア ントはどこにでも元の IP アドレスを保持できます。言い方を換えれば、ファブリックのすべてのワイヤレスローミン グはレイヤ 2 のローミングということもできます。

図 39. SD-Access ワイヤレスにおけるクライアントサブネット



SD-Access ワイヤレスゲストアクセス設計

ゲスト設計を検討する場合、ファブリックとの統合により3つの異なるソリューションが提供されます。

- ゲストアンカーコントローラを活用する OTT ソリューション
- 専用のゲスト仮想ネットワーク
- 専用のゲストファブリックドメイン

Cisco Unified Wireless Network ゲストアンカーを活用する OTT ソリューション

図 40. ゲストアンカーコントローラを活用する OTT ソリューション



ゲスト無線ネットワークを OTT として展開することにより、ゲストアンカーコントローラへの投資を引き続き活用で きます。ゲスト用の WLAN は、DMZ のゲストアンカーコントローラに固定されるように設定され、トラフィックは ファブリックへのオーバーレイになります。この実績のある Cisco Unified Wireless Network ソリューションはお客様の 投資を保護し、特にブラウンフィールド(既存環境)への導入に最適です。もちろん、このソリューションには、 Cisco Unified Wireless Network ソリューションから継承された制限があります。

・ゲストトンネル数は 71 に制限されています。

・有線ゲストに対応する別のソリューションがあり、アンカー WLC とは異なる方法で管理されます。



この設計では、ゲストネットワークは SD-Access ファブリック内のもう 1 つの VN であるため、ゲストデータプレーン を別のエンタープライズ トラフィックから分離するために、エンドツーエンドのファブリック セグメンテーション (VNI と SGT を必要に応じて異なるゲストロールに使用)を活用します。ゲスト VN を作成し、IP プールを定義し、 SSID をゲスト用の 1 つ以上のプールに関連付けることによって、Cisco DNA Center によって設定されます。このアプ ローチが前述のソリューションと比べて優れている主な点の 1 つは、これが有線と無線のゲストユーザにとって一貫し たソリューションとポリシーであることです。

個別のファブリックドメインとしてのゲスト

データプレーントラフィックだけでなく、コントロールプレーンのためにゲストネットワークを完全に隔離する必要 がある場合、Cisco DNA Center では専用のゲストコントロールプレーンとボーダー(基本的に専用のファブリックド メインである)を設定して、ゲストユーザを管理できます。

このソリューションでは、トラフィックは VXLAN の AP でファブリックエッジスイッチにカプセル化されています が、FE は別のボーダーノードを使用するように設定されています。このボーダーノードは DMZ に存在でき、ゲスト アンカー ソリューションと同様の完全なトラフィック分離を提供します。ゲストユーザは専用 CP(ボーダーと同じ場 所に配置される場合もされない場合もある)に登録され、DMZ 内でユーザに IP アドレスが割り当てられます。

図 42. ゲストコントロールプレーンおよびボーダー



前述の VN ソリューションと同様に、この設計は有線と無線のゲストに対してポリシーの一貫性を提供します。ゲス トコントロールプレーンとボーダーの選択は、ソリューションの拡張性によって異なります。

ゲストボーダーからのハンドオフは手動プロセスで、管理者は DMZ 内の外部ノードへのハンドオーバーを行うため のスタティックルートを含む適切なプロトコルを選択できます。

SD-Access ワイヤレスでのマルチキャスト

SD-Access ワイヤレスでのマルチキャストについて知っておくべき重要な点を次にいくつか示します。

- ・マルチキャストトラフィックは、有線クライアントとワイヤレスクライアントの両方に対して、オーバーレイの EID スペースに転送されます。
- ・ワイヤレスでマルチキャストを有効にするには、WLC でグローバル マルチキャスト モードと Internet Group Management Protocol (IGMP) スヌーピングをグローバルに有効にする必要があります。

Cisco DNA Center 1.3 では、ファブリック内のマルチキャストトラフィック転送で、ヘッドエンドレプリケーションとネイティブ転送の2つの方法が使用されます。これらの方法では、アンダーレイでのマルチキャストトラフィックの転送方法が異なります。ヘッドエンドレプリケーションでは、アンダーレイネットワークをマルチキャスト対応にする必要はありません。ファブリックへ送信されるマルチキャストトラフィックが複数のユニキャスト VXLAN トンネル(一部のマルチキャストレシーバが接続されているファブリックエッジノードごとに1つ)に複製されるため、この方法は最適ではありません。ネイティブマルチキャストの場合、アンダーレイをマルチキャスト対応にする必要があります。オーバーレイのマルチキャストトラフィックはアンダーレイマルチキャストで転送されるため、この方法は効率的です。パケットの複製は、関係するレシーバの場所に基づいてネットワークによって実行されます。

ここでは、マルチキャストのしくみについて説明します。

- ・マルチキャストクライアント(レシーバ)はオーバーレイにあります。マルチキャスト送信元はファブリックの 外側にもオーバーレイ内にもあります(図 43 では送信元はファブリックの外側に表示されています)。
- ・オーバーレイで PIM スパースモード (PIM-SM) または PIM 送信元特定マルチキャスト (PIM-SSM) を実行する 必要があります (VRF ごとに有効にする必要があります)。
- ・クライアントは特定のマルチキャストグループに対して IGMP Join を送信します。
- AP はそれを VXLAN にカプセル化し、アップストリームスイッチに送信します。
- ・ファブリックエッジノードはそれを受信し、ファブリック ランデブー ポイント (RP) に対して PIM Join を実行 します (PIM-SM が使用されていると仮定します)。
- RP はエンドポイント IP スペースの一部としてオーバーレイに存在する必要があります。
- 図 43 に、上記の手順を示します。

図 43. SD-Access ワイヤレスでのマルチキャスト



•この例では、マルチキャスト送信元は、ファブリックの外にあるため、そのセグメントの代表ルータであるファ ブリックボーダーに向けてインターフェイス上でマルチキャストトラフィックを送信します。

・FB はトラフィックを受信し、RP に対して PIM Join を実行します (PIM-SM が使用されていると仮定します)。

・これで、RPには、そのマルチキャストグループの送信元と受信側情報が入るようになりました。

図 44. SD-Access ワイヤレスでのマルチキャスト (北から南)



- ・これで、RPには、特定のマルチキャストグループの送信元と受信側情報が入るようになりました。
- FB は VXLAN トンネルを介してマルチキャスト送信元のトラフィックを RP に送信し、RP はそのトラフィック を別の VXLAN トンネルを介して FE に転送します。
- ・FEは VXLAN パケットを受信し、カプセル化解除してポリシーを適用し、VXLAN トンネルを介して再び AP に 転送します。
- APは、VXLAN ヘッダーを削除し、電波に元の IP マルチキャストパケットを送信します。

図 45. SD-Access ワイヤレスでのマルチキャスト



- ・最初のマルチキャストパケットが FE に配信されると、最短パスフェールオーバー(SPT)が発生し、トラフィックは FB と FE 間で直接転送されます。
- •FE は、受信した最初のマルチキャストパケットに基づいて FB がマルチキャスト送信元を所有していることを認 識し、そのマルチキャストグループの FB に直接 PIM Join を送信します。
- ・これで FB は特定のマルチキャストグループを要求したクライアントを持つ FE を認識するようになりました。
- ヘッドエンドレプリケーションまたはネイティブマルチキャストを実行し、VXLAN はマルチキャストトラフィックをカプセル化し、それを関係する FE に転送します。
- マルチキャストトラフィックがオーバーレイに送信されます。
- ・FEは VXLAN パケットを受信し、カプセル化解除してポリシーを適用し、再び AP に転送します。
- ・APは、VXLANヘッダーを削除し、電波に元のIPマルチキャストパケットを送信します。

SD-Access ワイヤレスのハイアベイラビリティ

SD-Access ワイヤレスソリューションの最も重要なコンポーネントは、WLC およびコントロールプレーンノードです。 有線ファブリッククライアントと比較して、コントロールプレーンはワイヤレスでさらに重要な役割を果たします。ク ライアントロケーション情報を更新する役割を果たすため、クライアントローミングにおいて重要です。

WLC と CP はどちらもハイアベイラビリティをサポートします。

コントローラの冗長性

コントローラのハイアベイラビリティでは、ファブリック対応コントローラに対する N+1 と SSO の両方の使用がサ ポートされています。

SSO を使用したステートフル冗長性

図 46. ステートフル スイッチオーバー



- ・WLC SSO ペアをファブリックは1つのノードと見なします。
- ・アクティブ WLC のみが CP ノードと通信します。
- ・ファブリック設定と CP 状態はアクティブ WLC とスタンバイ WLC の間で同期されます。
- ・障害時は、新しいアクティブ WLC がファブリッククライアントをホスト トラッキング データベース ノードにー 括更新します (LISP 更新)。
- •APとクライアントは接続を維持します。

設計の項で説明したように、FCS では WLC がファブリックの外部に接続されているため、SSO ペアの接続に関する 通常の考慮事項が適用されます。つまり、2 つのコントローラ間の帯域幅および遅延要件は Cisco Unified Wireless Network アーキテクチャと同様です。

N+1を使用したステートレス冗長性

図 47. N+1 冗長



ステートフル HA を必要としない場合は、N+1 の冗長性がサポートされます。N+1 の冗長性は Cisco DNA Center 1.3 まで自動化されていません。この機能のサポートについては、Cisco DNA Center のロードマップを参照してください。重要な考慮事項は次のとおりです。

- AP はプライマリとセカンダリを使用して設定されます。
- ・APと接続しているクライアントはプライマリに登録されます。
- ・プライマリの障害時、AP は接続を解除し、セカンダリに参加します。
- ・クライアントも接続を解除し、セカンダリに参加します。
- ・セカンダリはホスト トラッキング データベースに新規のクライアント登録を行います。



N+1 の冗長性は Cisco DNA Center 1.3 まで自動化されていません。この機能のサポートについては、Cisco DNA Center のロードマップを参照してください。

コントロール プレーンの冗長性

図 48. コントロール プレーンの冗長性



- ・コントロールプレーンノードの冗長性は、アクティブ/アクティブ設定でサポートされています。WLC(および ファブリックエッジ)は2つの CP ノードで設定され、両方に情報を同期させます。
- •1 つの CP ノードで障害が発生した場合、すべてのクライアント情報はもう 1 つの CP ノードで使用できます。 WLC の設定(Aire-OS の参考用スクリーンショット)を次に示します。

uluulu cisco		<u>W</u> I ANs		WIRFLESS	grainny	маластигит
Gontroller	Fabric C	ontrol Pl	ane Configur	ation		
General Trons Inventory Interlaces	Fabric	Enable	a 💿			
Interface Groups	Enterpri	se				
Multicast Network Routes	Z Prime	any IP Addre	cs. [102.158.	16.252		
 Fabric Configuration Control Plane Interface 	Corn	ecton 3tatu	s		0	
Templatas	Seco	ndary 19 Ad	dress 192.168.	10.252		
Redundancy	Pro S	hared Key				1
Mobility Management	000 m	ection Statu	ĸ			

Catalyst 9800 WLC の参考用スクリーンショット:

Cisco Cata	alyst 9800-CL Wireless Controller	Welcome sand
Q Search Menu Items	Configuration > Wireless > Fabric	Edit Control Plane
		Control Plane Name* default-control-plan
📻 Dashboard	General Control Plane Profiles	Control Plane Description
Monitoring >		+ Add × Delete
Configuration >	Control Plane Name	Control F IP Address v
(Ô) Administration →	default-control-plane	9.254.254.65
X Troubleshooting	I4 4 1 ► ► 10 • items per page	9.254.254.69
		1 - 2 of 2 items

付録:SD-Access ワイヤレス機能の詳細情報

次の表に、SD-Access ワイヤレスアーキテクチャでサポートされている主要な機能の一部を示します。

表1:SD-Access ワイヤレスアーキテクチャでサポートされている主要な機能

オープン/スタティック Wired Equivalent Privacy (WEP)	サポート対象
事前共有キーによるワイヤレス保護アクセス(WPA-	サポート対象
PSK)	
802.1X (WPA/WPA2)	サポート対象
MAC フィルタリング	サポート対象
ローカル拡張可能認証プロトコル (EAP)	サポート対象
AAA Override	サポート対象
内部/外部 Web 認証	サポート対象
事前認証アクセスコントロールリスト (ACL)	サポート対象
クライアントの IPv4 ACL	サポート対象(SGT を優先し、推奨)
Application Visibility and Control (AVC)	サポート対象*
ローカルプロファイリング	サポート対象
RADIUS プロファイル	サポート対象
QoS プロファイル	サポート対象
ユーザ単位の帯域幅コントラクト	サポート対象
ワイヤレス侵入防御システム (wIPS)	サポート対象
Cisco Connected Mobile Experiences (CMX) 統合	サポート対象
NetFlow エクスポート	サポート対象
HA SSO	サポート対象

*Wave 2 AP のみ
ここで、ファブリックネットワークでの動作を理解するために、いくつかの機能について説明します。

AAA Override

ISE は SD-Access ワイヤレス SSID のファブリック インターフェイス名、ACL、QoS、SGT などのパラメータをオー バーライドできます。

ファブリック インターフェイス名のオーバーライド

クライアントの認証と役割に基づいて、同じ SSID を異なるプールまたはサブネットにマッピングする場合はどうす ればよいでしょうか。Cisco Unified Wireless Network では、このために VLAN オーバーライドを使用して、VLAN ID (名前または番号) を AAA サーバから WLC に戻します。

ファブリックでは、VLAN にはローカルスイッチだけがあり、IP プールにマップされるのはレイヤ 2 VNID です。こ れは、サブネットまたはプールに関連付けられているネットワーク識別子で、ワイヤレスでは SSID に関連付けられ ています。レイヤ 2 VNID は、AP から VXLAN ヘッダーのスイッチに転送されます。レイヤ 2 VNID は最終的に、 ファブリックエッジスイッチで VLAN に、それから SVI(エニーキャストゲートウェイ)に、その後、レイヤ 3 VNID (VRF) にローカルマッピングされます。

SD-Access ワイヤレスでは、さまざまなプールを区別するためにレイヤ 2 VNID を渡す必要があります。ISE または他の AAA は VNID を直接使用しないため、Cisco Audio-Video Protocol (AVP)の Aire-Interface-Name または Interface-Name を 使用して、クライアント認証時に特定の名前を返します。クライアントのレイヤ 2 認証は常にコントローラで行われる ため、ISE と通信してそのインターフェイス名の値を取得し、レイヤ 2 VNID にマッピングするのは WLC です。



図 49. AAA Override

ISE では、特定のグループ認証プロファイルを設定して、次のスクリーンショットに示すように特定のインターフェ イス名を返す必要があるため、ユーザが認証すると ISE は RADIUS ACCEPT_ACCEPT メッセージの特定の属性を返 します。

 Advanced Attributes Settings 	
Airespace:Airespace-Interface-Nar 💟 = eid_9_6_53_0	<u> </u>
Attributes Details	

ファブリック インターフェイス名は、次のようなマッピングを使用してレイヤ2 インスタンス ID にマッピングされ ます。重要: Cisco DNA Center を設定すると、このマッピングと設定はすべて自動的に行われます。

cisco	<u>M</u> ONITOR <u>W</u> LANS		WIRELESS	<u>S</u> ECURITY	MANAGEMENT		
Controller	Fabric Interface >	New					
General Icons Inventory Interfaces Interface Groups Multicast Network Routes Fabric Configuration Control Plane	Fabric Interface > New Fabric Interface Name L2 Instance ID Network IP Subnet Mask L3 Instance ID		eid_9_6, 200	eid_9_6_53_0			

レイヤ2インスタンス ID は AP に送信され、VXLAN ヘッダーに埋め込まれます。

ACL および QoS プロファイルの AAA オーバーライド

WLC のファブリック ACL は AP に適用されます。ローカル WLC ACL とファブリック ACL の主な違いは、ファブリック ACL は方向を関連付けられていないことです。ファブリック SSID では、Flex ACL が SSID に設定されます。同じ ACL がイングレスとイーグレス両方に適用されます。

ACL の AAA オーバーライドの場合:

- ・オーバーライド ACL 名は AP のファブリック ACL (Flex ACL) である必要があります。
- ・ACL テンプレートは ACL の AP へのプッシュに使用できます。

cisco	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT
Controller	Fabric ACL Templ	ate > Edit	i.		
General Icons	Fabric ACL Template Name	ACL Template			
Inventory	Status	Modified			
Interfaces					
Interface Groups Multicast	ACL	•	Add		
Network Routes					
 Fabric Configuration 	Fabric ACL				
Control Plane	ca-redirect-acl				
Templates	cwa-redirect-acl				
Redundancy	test				
Mobility Management					

WLANs	General WLANS A	PS 802.110	Location	Ports/Module		
AP Groups					Apply	
	AP Group Name	default-group				
	AP Group Description					
	NAS-ID	none				
	Enable Client Traffic QinQ					
	Enable DHCPv4 QinQ 🔮					
	QinQ Service Vlan Id 10	0				
	Fabric Flex ACL	ACL Template 👻				
	**********	*********	4			
~						

QoS プロファイル名のオーバーライドの場合:

- •QoS プロファイル名は ISE からプッシュされます。
- ・アップストリームおよびダウンストリーム QoS が AP で適用されます。
- ・VXLAN トンネル QoS は内部ヘッダーから取得されます。

SGT を使用したグループベースのポリシー

WLC は、クライアントが接続した際に、ワイヤレスクライアントに使用する SGT を AP に送信します。AP は、ワイ ヤレスクライアントからアクセススイッチに VXLAN トンネル経由でデータパケットを転送するときに、VXLAN ヘッダーにこの SGT を追加します。この SGT はファブリックを介してエンドツーエンドに伝送されます。



図 50. VXLAN ヘッダーには SGT および VNI が含まれます

イーグレスアクセススイッチでは、SGT と DGT のペアで適用する SGACL を判断します。SGT はパケットに含まれ ており、DGT は宛先ホストの IP バインドに基づいて導かれます。

ワイヤレスクライアントのためにアクセススイッチに SGACL を適用する場合(アクセススイッチ(VXLAN トンネル 送信元)のワイヤレスクライアントに向かうトラフィックに対する適用)、タグ(SGT と DGT)はスイッチで取得さ れる必要があります。

次の手順は、グループベースポリシーのフローです。

- ・クライアントのレイヤ2認証がWLCで発生します。
- ・WLC はクライアント接続時に SGT を AP に送信します。
- ・WLC はクライアント登録時に CP を SGT で更新します。
- ・CP は FE を隠されたデータの SGT を使用して更新します。受信した SGT に基づいて、スイッチは ISE からポリ シーをダウンロードします。
- ・AP はこの SGT を VXLAN ヘッダーに追加します。
- ・SGT は LISP ヘッダーのファブリックを介してエンドツーエンドで伝送されます。
- ・イーグレススイッチでは、SGT と DGT のペアによってパケットヘッダーの SGT に基づいて SGACL が判断され ます。

図 51. グループベースポリシーの SGT



CWA と BYOD の ISE

この項では、中央 Web 認証 (CWA)の基本的なフローについて説明します。これは、Cisco DNA Centerの自動化でサポートされている唯一の種類の Web 認証です。



- 1. レイヤ 2 認証が ISE サーバで発生します。MAC フィルタリングは、WLC で設定する必要があります。
- 2. クライアント認証フェーズ中に、URL リダイレクト ACL (Flex ACL タイプ) とリダイレクト URL が AP にプッシュされます。
- クライアントトラフィックは、VXLAN トンネルでのデバイス登録とネイティブ サプリカント プロビジョニング のために ISE ポータルにリダイレクトされます。
- 4. 完了すると、ISE は認可変更(CoA)を WLC に送信し、WLC は CoA を AP にプッシュします。
- 5. 次に、クライアントは EAP-TLS を使用して再認証します。デバイスは ISE サーバにとって既知となったため、認 証が成功し、以降のデータトラフィックは AP から VXLAN さらにファブリックエッジにスイッチされます。

フローは次のとおりです。

- 1. レイヤ 2 認証が WLC で発生し、クライアントは WEBAUTH_REQD 状態に移行します。
- 2. HTTP リダイレクトが WLC で発生します。
- 3. Web 認証が内部(WLC でホストされる Web ページ)または外部(外部サーバでホストされる Web ページ)で発生します。
- 4. トラフィックは外部ローカル Web 認証の事前認証 ACL と一致すると、VXLAN トンネルでスイッチされます。内部 Web 認証の場合、トラフィックは CAPWAP を介して WLC に送信されます。
- 5. レイヤ3認証が完了すると、クライアントは RUN 状態になり、事前認証 ACL は削除されます。
- 6. ゲストデータトラフィックは FE から DMZ 内のゲストボーダーノードにスイッチされます。内部 Web 認証の場合、 トラフィックは CAPWAP を介して WLC に送信されます。



©2020 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, および Cisco Systems ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。 本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。 「パートナー」または「partner」という用語の使用は Cisco と他社との間のパートナーシップ関係を意味するものではありません。(1502R) この資料の記載内容は 2020 年 8 月現在のものです。 この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ合同会社

お問い合せ先

〒107‐6227 東京都港区赤坂 9-7-1 ミッドタウン・タワー http://www.cisco.com/jp