検証済みソリューション：金融業界

改訂：2022 年 10 月 12 日

ソリューションの概要

このガイドでは、Cisco SD-Access と Cisco SD-WAN をベースとする大規模な金融業界向けの展開の作成と検証に焦点を当てています。この展開では、Cisco SD-WAN コントローラと Cisco DNA Center を統合せずに個別に管理する独立ドメインモデルを使用します。このガイドは、金融ネットワークの展開に関する参考資料として使用できます。

金融機関は、小規模な ATM から大規模な企業オフィスまで、世界中で何百ものブランチを運営しています。サイトごとに独自の特別な要件がありますが、金融業界では一般に、標準化されたセキュアなネットワーク接続、簡素化されたネットワーク運用とメンテナンス、耐障害性に優れたシステム、組織全体での一貫したポリシー実装が求められます。

Cisco DNA Center の 3 ノードのハイアベイラビリティやディザスタリカバリなど、復元力を高める機能を使用することで、稼働時間の最大化、運用コストの削減、ワークフローの合理化、パフォーマンスの最適化、セキュアなエンドツーエンド接続が実現します。

システムとネットワークの復元力

この金融業界向けソリューションは、低レベルのデバイスやリンクの障害から、コントローラの障害、さらにはデータセンターの停止に至るまで、複数のレイヤにおける障害に対処できます。Cisco DNA Center のハイアベイラビリティやディザスタリカバリの機能により、システムの復元力が提供されます。さらに、Cisco SD-Access と SD-WAN により、デュアル SD-Access ボーダー、デュアル Cisco SD-WAN WAN エッジ、スタックと StackWise Virtual リンク（SVL）を備えたファブリックノード、SSO と N+1 のワイヤレスコントローラのサポートを通じてネットワークの復元力が提供されます。

セキュリティ

このソリューションは、組み込みのセキュリティ機能に加え、Cisco ISE と Cisco DNA Center の統合により、高度にセキュアなセグメント化されたシステムを提供します。

Cisco ISE は、ネットワークへのセキュリティの提供を簡素化し、グループベースポリシー（GBP）のサポートを提供するポリシーエンジンです。Cisco GBP は、スケーラブルグループタグ（SGT）を使用して、エンドポイントを論理グループに動的に編成します。SGT は、IP アドレスよりもリッチなコンテキストを活用したビジネス上の決定に基づいて割り当てられます。SGT により、把握と管理が容易になります。グループベースのルールは、IP アドレスに基づく同等のルールセットよりも数が劇的に少なくなります。Cisco ISE は、ネットワークデバイスおよびエンドクライアントとの AAA 機能も実行します。

Cisco DNA Center は、ネットワークを拡張し、ファブリック内の重要なアプリケーションへのアクセスを制限しながら、ネットワークの状況認識を向上させます。Cisco ISE が Cisco DNA Center と統合された後、Cisco DNA Center は Cisco ISE からグループベースポリシーを取得して、不正なエンドポイントおよびクライアントからアプリケーションを保護します。Cisco ISE は、Cisco DNA アシュアランス 用にネットワーク、ユーザ、およびデバイスからコンテキスト情報をリアルタイムで収集します。この統合により、不正行為を防止して機密データを保護する金融機関の高度なセキュリティニーズが簡単になります。ネットワークアクセスのプロビジョニングの促進、セキュリティ運用の高速化、ネットワーク全体への一貫したポリシーの適用が実現します。

Cisco GBP とアイデンティティベースのアクセス制御機能（IEEE 802.1X/MAC 認証バイパス、サイトレベルの MACsec 暗号化、FQDNベースの証明書）により、金融業界のセキュリティニーズを達成できます。

ネットワークのセグメント化

ネットワーク セグメンテーションは、重要なビジネス資産を保護するために不可欠です。Cisco DNA Center は、仮想ネットワーク（VN）間のデータを保護するために、マクロセグメンテーションと呼ばれる単純化されたアプローチを提供します。さらに、Cisco DNA Center は、VN 内のエンドポイントにグループベースのアクセスコントロールを使用してマイクロセグメンテーションを展開するためのフレームワークも提供します。

ネットワークセグメンテーションは新しい概念ではありませんが、この数年の間に大幅な進化を遂げました。当初ネットワーク セグメンテーションは、仮想 LAN（VLAN）を使用して、1 つの「フラットな」ネットワークまたはブロードキャストドメインを小さなセグメントに分割するプロセスとして定義されていました。場所にかかわらず組織全体でネットワークセグメントを拡張する必要性から、VN または Virtual Routing and Forwarding（VRF; 仮想ルーティングおよびフォワーディング）インスタンスの概念が導入され、ネットワークセグメント間のレイヤ 3 分離が実装されました。

各 VRF が独自のルーティングおよび転送を維持し、仮想ネットワークを作成することで分離されます。1 つの VRF に含まれるルートが別の VRF には含まれておらず、相互の通信が制限されるためです。Cisco GBP では、セグメンテーションは、IP アドレッシングやルーティングを使用した VLAN や VRF に基づいて実現されるものではなくなっています。IP アドレッシングに関わりなく、ロールベースまたはグループベースのメンバーシップを使用してポリシーを作成することで、ネットワークをセグメント化します。

ネットワーク運用の簡素化

Cisco DNA Center は、ネットワークデバイスのプロビジョニング、ソフトウェアイメージの管理（SWIM）、インベントリの管理などのワークフローを自動化するインテントベースのソリューションを提供します。また、Cisco DNA Center は、組織の目的をポリシーとしてすべてのサイトにプッシュします。このソリューションでは、ファブリックボーダーとゲートウェイの間のレイヤ 3 接続にスイッチ仮想インターフェイス（SVI）番号を再利用でき、管理者が各ボーダーで SVI 割り当てを標準化するためのフレームワークを提供します。Cisco DNA Center は、ネットワーク、クライアント、および重大な問題の アシュアランス ダッシュボードなど、アシュアランス を使用してネットワークの正常性に関する実用的な情報も提供します。単一のデバイスまたはクライアントにドリルダウンする機能により、トラブルシューティング プロセスが簡単になります。

堅牢なネットワークと接続性

Cisco SD-WAN は、単一のファブリックを介して複数のサイトを接続するオーバーレイ WAN アーキテクチャです。Cisco SD-WAN アーキテクチャは、個別のオーケストレーション、管理、コントロール、およびデータの各プレーンで構成されています。Cisco vBond コントローラは、SD-WAN オーバーレイへの SD-WAN ルータの自動オンボーディングを提供します。Cisco vManage コントローラは、一元的な設定とモニタリングの役割を担います。Cisco vSmart コントローラは、SD-WAN ネットワークの中央集中型コントロールプレーンの役割を担います。WAN エッジは、他の WAN エッジとのセキュアなデータプレーン接続を確立します。

Cisco SD-WAN エッジは、Cisco SD-Access IP トランジットを使用して Cisco SD-WAN ファブリック全体の SD-Access サイトに接続し、ネットワーク全体で標準のセキュアな接続を維持します。独立ドメイン展開モデルでは、Cisco vManage と Cisco DNA Center は相互に通信しません。Cisco SD-Access VN は、VRF-Lite を使用して Cisco SD-WAN バーチャル プライベート ネットワーク（VPN）に接続されます。これにより、2 つの SD-Access サイトからの VN が Cisco SD-WAN 間で通信できるようになります。VN/VPN 内でのルートの交換用に、SD-WAN WAN エッジと Cisco SD-Access ボーダーの間に外部ボーダー ゲートウェイ プロトコル（eBGP）が設定されます。

ポリシー管理の一元化

Cisco DNA Center システムのエンドポイントのスケールと Cisco ISE のスケールの間には数の違いがあります。金融業界のような、地理的に離れた複数のブランチやサイトが世界中に分散した大規模な Cisco ISE 展開では、複数の Cisco DNA Center クラスタを単一の Cisco ISE クラスタに統合することでメリットが得られます。シスコでは、Cisco ISE をより有効に活用できるように Cisco ISE 展開ごとに複数の Cisco DNA Center クラスタをサポートし、複数の Cisco DNA Center のポリシーを一元管理する管理プレーンを提供しています。マルチ Cisco DNA Center 展開では、最初の Cisco DNA Center システムがグループベースのアクセスポリシーの作成者ノードとして機能します。作成者ノードでスケーラブルグループ、アクセス契約、ポリシー、および VN を管理します。これらのポリシーやセキュリティの要素の作成、変更、削除は、作成者ノードでのみ可能です。追加のリーダーノードは、ネットワークデバイスの個別のセットを管理する独立したシステムです。リーダーノードでは、ローカルの VN やグループベースのアクセスポリシーを管理しません。リーダーノードでは、読み取り専用で VN とスケーラブルグループの確認のみが可能です。

ネットワーク サービス

トレーディングフロアのアーキテクチャの多くでは、データおよびビデオフィードサービスにマルチキャストプロトコルを使用します。Cisco DNA Center と Cisco SD-WAN により、ハブからブランチへのマルチキャストを可能にするフレームワークが提供されます。

ハードウェアとソフトウェアの仕様

ソリューションは、次の表に示すハードウェアとソフトウェアでテストされています。サポートされているハードウェアの完全なリストについては、「Cisco Software-Defined Access Compatibility Matrix」を参照してください。

ロール	ハードウェア プラットフォーム	ソフトウェア リリース
Cisco DNA Center コントローラ	DN2-HW-APL-L、DN2-HW-APL-XL	2.3.3.3
Cisco Identity Service Management、RADIUS サーバ	物理/仮想アプライアンス	3.0 パッチ 5、3.1 パッチ 3
Cisco SD-WAN NMS コントローラ	vManage	20.6.1
Cisco SD-Access コントロールプレーンノード	ASR1001-X, C9500	17.6.2、17.8.1、17.8.1a
Cisco SD-Access ファブリックボーダーノード	C9500	17.6.2、17.8.1
Cisco SD-Access ファブリックエッジノード	C9200, C9300, C9400	17.6.2、17.8.1
Cisco Wireless LAN Controller（WLC）	AireOS	8.10MR8
	C980040	17.6.2、17.8.1
Cisco SD-WAN WAN エッジ	ASR1002-X, ISR4331	17.6.3
Cisco Stealthwatch コントローラ	物理/仮想アプライアンス	7.1.2

ソリューションの導入例のシナリオ

金融業界のプロファイルについて、トポロジ で定義されたトポロジを使用して次のユースケースを実施しています。

- Cisco DNA Center と Cisco SD-Access を使用してインテントベース ネットワークを実装。
  - 管理者は、ネットワークデバイスのプロビジョニングを自動化および簡素化できます。
  - 管理者は、インベントリを維持および監視し、問題を簡単に解決できます。
  - 管理者は、Cisco DNA Center SWIM を使用して、スイッチ、ルータ、ワイヤレスコントローラなどの複数のデバイスをアップグレードできます。
- 複数の Cisco DNA Center を単一の Cisco ISE に統合。
  - 管理者は、作成者ノードでインテントベースのポリシーを作成、変更、削除し、自動的にリーダーノードと同期できます。
  - 管理者は、Cisco DNA Center リーダーノードから作成者ノードへの昇格を要求できます。
- 地理的に離れた複数のサイトを Cisco SD-WAN を使用して接続。
  - 管理者は、キャンパスとブランチの間を接続するように Cisco SD-WAN を設定できます。
  - 管理者は、IP トランジットを介して SD-Access ファブリックに接続するように Cisco SD-WAN WAN エッジを設定できます。
  - 管理者は、Cisco TrustSec を使用してエンドツーエンドを維持するように Cisco SD-WAN WAN エッジでインライン SGT 伝播を設定できます。
  - 管理者は、Cisco SD-WAN vManage を使用して Cisco SD-WAN WAN エッジのイメージをアップグレードできます。
- システムとネットワークの復元力。
  - 既存のアプリケーション、トラフィック、ユーザへの影響を最小限に抑えて、ネットワークがデバイスやリンクの障害から自動的に回復します。
  - 管理者は、3 ノード HA モードで Cisco DNA Center を設定できます。Cisco DNA Center でサービスやノードの障害が発生した場合、システムはユーザの介入なしで回復します。
  - 管理者は、異なるデータセンターにある Cisco DNA Center でディザスタリカバリを設定できます。複数のノードで障害が発生したり、回復不能なネットワークの問題が発生した場合、シスコのディザスタリカバリによって別のデータセンターにある Cisco DNA Center への自動フェールオーバーがトリガーされます。
  - 管理者は、Cisco DNA Center ディザスタリカバリが設定された状態でアップグレードやメンテナンス作業を実行できます。
  - 管理者は、スタンバイ Cisco DNA Center にフェールオーバーできます。
  - 管理者は、Cisco ISE 分散展開で複数のポリシー管理ノード（PAN）、ポリシーサービスノード（PSN）、および Cisco Platform Exchange Grid（pxGrid）を設定できます。

- 管理者は、ユーザやデバイスに影響を与えることなく、Cisco ISE 分散展開でメジャーリリースへのアップグレードや新しいパッチの適用を行うことができます。
- 管理者は、Cisco DNA Center コントローラの設定とデータを随時またはスケジュールに従ってバックアップできます。
- 管理者は、Cisco DNA Center コントローラの設定とデータを復元できます。

- 組織全体の統合ネットワークインテントを設定。
  - 管理者は、一貫したマクロセグメンテーションを実現するために組織全体で VN を作成できます。
  - 管理者は、単一の VN に複数の SGT を適用し、VN 内のマイクロセグメンテーション トラフィック用のグループベースのアクセスポリシーを作成できます。
  - 管理者は、有線クライアントとワイヤレスクライアントの dot1x 認証を設定できます。
  - 管理者は、VN の追加/削除によって新しいユーザグループを追加または削除し、IP プールを VN に関連付けまたは関連付け解除できます。

- 強化されたセキュリティを設定して機密性の高い財務データを保護。
  - 管理者は、不正アクセスを防ぐために、有線およびワイヤレスのデバイスとユーザに対してクローズド認証オンボーディング（dot1x）を有効にできます。
  - 管理者は、MACsec を使用してセキュアなサイトレベルのファブリックトラフィックを設定できます。
  - 管理者は、セキュリティを強化するために、Cisco DNA Center で信頼できる CA の FQDN ベースの証明書を適用できます。
  - 管理者は、脅威の検出、脅威の封じ込め、および ESA 自動化のための SSA 用に Stealthwatch を Cisco DNA Center と統合できます。
  - 管理者は、詳細なロールベースのユーザを作成し、監査ロギングを使用して Cisco DNA Center のアクティビティを監視できます。
  - 管理者は、ポリシーの変更、ポリシーの変更の展開、展開のステータス、および変更を開始したユーザと時期を監査できます。

- アシュアランスと分析を使用してネットワークとクライアントの状態を監視。
  - ネットワーク管理者は、ネットワーク、有線ユーザ、およびワイヤレスユーザの状態を単一の画面で監視できます。
  - ネットワーク管理者は、ネットワークやデバイスに関する重大な問題や進行中の問題を調査し、アシュアランス の推奨措置に従って問題を解決できます。
  - ネットワーク管理者は、ネットワークに接続されている有線およびワイヤレスのユーザとデバイスの状態を監視できます。
  - ネットワーク管理者は、単一のデバイス、有線ユーザ、またはワイヤレスユーザを確認し、詳細情報を取得できます。

- ネットワーク管理者は、アプリケーションデータの詳細な使用状況を確認できます。
- ネットワーク管理者は、センサーを使用してワイヤレスネットワークの状態を監視できます。

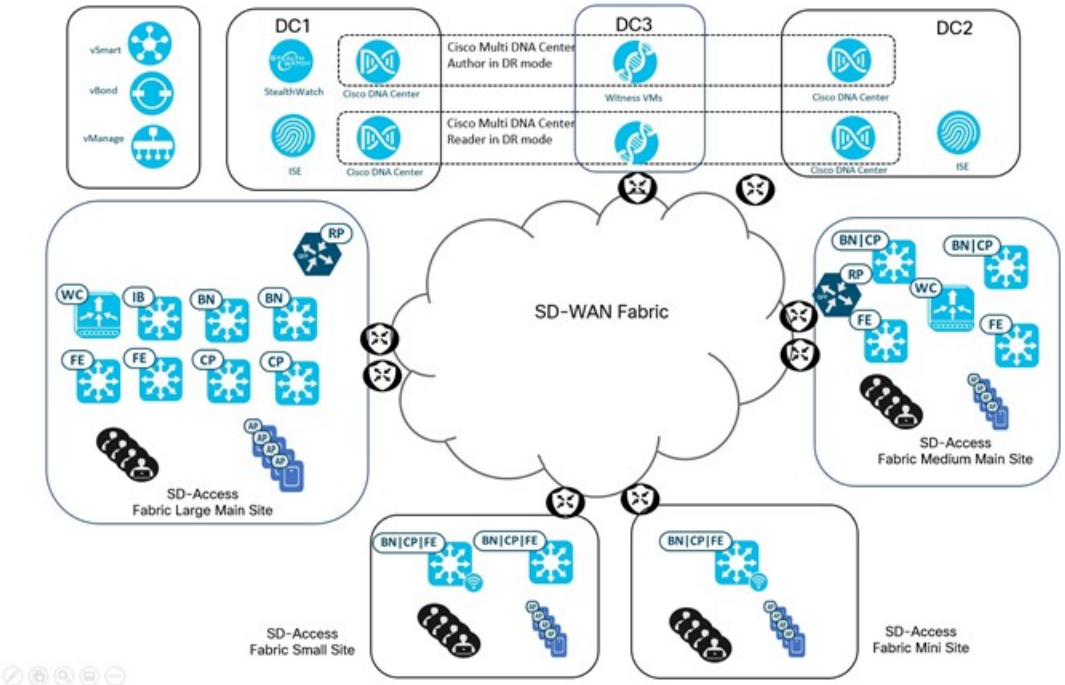
トポロジ

金融業界向けのテストトポロジには4つのCisco DNA Centerがあります。これらは複数のデータセンターに展開され、Cisco DNA Centerディザスタリカバリが設定されています。データセンター1にはメインCisco DNA Centerクラスタがあります。データセンター2にはCisco DNA Centerディザスタリカバリ用のリカバリCisco DNA Centerクラスタがあります。データセンター3にはウィットネスが収容されています。各データセンターに2つのCisco DNA Center展開があります。1つはマルチCisco DNA Centerの作成者で、もう1つはリーダーです。Cisco ISEのポリシー管理ノード（PAN）とポリシーサービスノード（PSN）は、データセンター1とデータセンター2に分散して展開されています。Cisco SD-WANコントローラはデータセンター1にあります。SD-WANファブリックでCisco SD-WAN WANエッジを介して複数のファブリックサイトが接続されています。サイトの説明は次のとおりです。

- 大規模メインサイトには、デュアルボーダー、デュアル非コロケーションCP、およびワイヤレスLANコントローラがあります。中規模メインサイトには、デュアルボーダー、コロケーションCP、およびワイヤレスLANコントローラがあります。
- 小規模サイトには、ワイヤレスLANコントローラが組み込まれたデュアル一体型ファブリックがあります。
- ミニサイトには、ワイヤレスLANコントローラが組み込まれた一体型ファブリックがあります。
- すべてのファブリックサイトに、ASMオーバーレイ、SSMアンダーレイ、およびネイティブマルチキャストを使用したSD-Accessマルチキャストがあります。外部RPはメインサイトにあります。メインサイト間でのサイト固有のマルチキャスト送信元の伝達にはMSDPピアリングが使用されます。

次の図は、ソリューションのテストベッドの論理トポロジを示しています。

図 *1*: ソリューションのテストトポロジ



スケール

ソリューションのテストでは、次の表に示すスケールについて確認しました。ハードウェアキャパシティについては、Cisco DNA Center のデータシートを参照してください。

表 *1*: ソリューションのテストスケール

カテゴリ	値
デバイスインベントリ	2000
ファブリックサイトあたりのデバイスの数	1 ー 500
サイトあたりの VN の数	3 ー 64
サイトあたりの WLC の数	HA あたり 2
ファブリックサイトの数	450
サイトあたりの AP の数	最大 1000
エンドポイントの数	100,000（ワイヤレス 60,000、ゲスト 20,000、有線 20,000）
SSID の数	4

カテゴリ	値
SGT の数	500
トラフィックプロファイル	ユニキャストおよびマルチキャスト

ソリューションの重要事項

ここでは、ソリューションの展開に役立つテクニカルノートについて説明します。

マルチ Cisco DNA Center

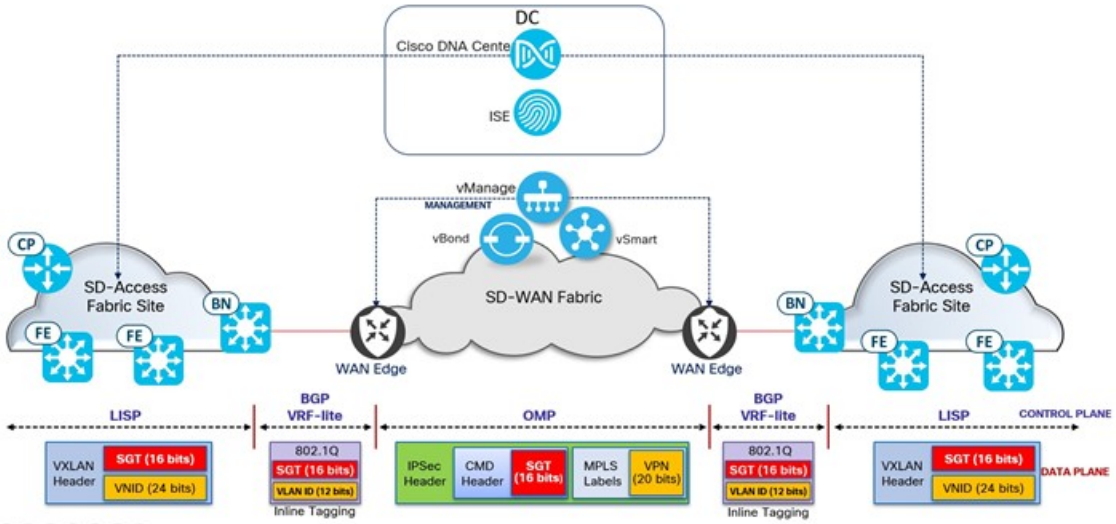
金融業界のような大規模な Cisco ISE 展開では、複数の Cisco DNA Center クラスタを 1 つの Cisco ISE クラスタに統合することでメリットが得られます。Cisco DNA Center では、Cisco ISE をより有効に活用できるように Cisco ISE 展開ごとに複数の Cisco DNA Center クラスタをサポートし、複数の Cisco DNA Center のポリシーを一元管理する管理プレーンを提供しています。詳細については、「Support for Multiple Cisco DNA Center Clusters with a Single Cisco ISE System」を参照してください。

- マルチ Cisco DNA Center パッケージはリリースのソフトウェアイメージにはバンドルされていないため、個別にダウンロードする必要があります。
- Cisco ISE に最初に統合した Cisco DNA Center が作成者ノードになります。作成者ノードは、すべての SD-Access ポリシー情報の情報源です。作成者ノードを変更することは推奨されません。いずれの Cisco DNA Center を作成者ノードにするかを最初に決定してください。
- 以降に Cisco ISE に統合した Cisco DNA Center（最大 3 つ）はリーダーノードになります。新しく展開した Cisco DNA Center をリーダーノードとして追加することをお勧めします。既存のポリシーデータがある場合、そのノードは Cisco ISE と統合しないでください。
- マルチ Cisco DNA Center 展開では、すべての Cisco DNA Center で同じバージョンのソフトウェアを実行する必要があります。

Cisco SD WAN

Cisco SD-WAN は、ファブリックサイトやブランチが世界中に分散する環境において、Cisco SD-Access サイトのアンダーレイとオーバーレイの間の接続に堅牢なトランスポートを提供します。インライン SGT タギングを使用すると、SGT がエンドツーエンドで維持され、ドメイン全体およびファブリックエッジで一貫したポリシーの適用が可能になります。次の図は、インライン SGT タギングを使用した SD-Access SD-WAN 統合を示しています。

図 *2 : SD-Access SD-WAN* 統合（インライン *SGT* 対応）

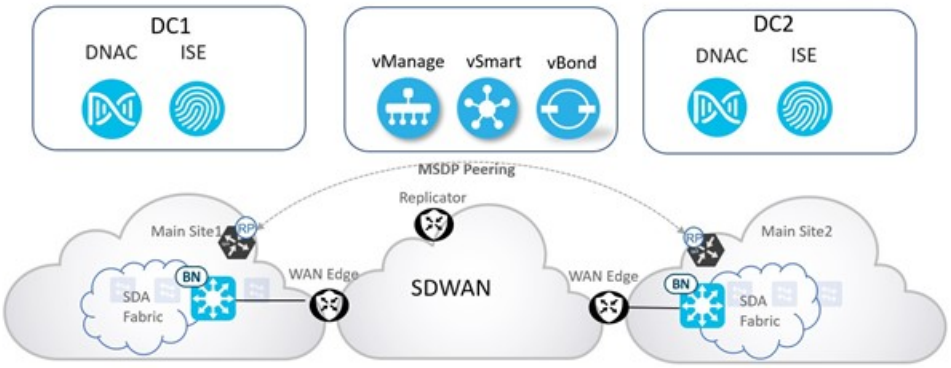


- Cisco SD-WAN コントローラが起動し、WAN エッジが Cisco SD-WAN コントローラによってオンボーディングされて管理されると、Cisco SD-Access ネットワークとの統合が VRF Lite および eBGP を使用したファブリックボーダーでの IP トランジット L3 ハンドオフによって実現されます。
- ファブリックボーダーと WAN エッジの間のレイヤ 3 MTU の整合性が確認され、エンドツーエンドの大規模なパケット転送が一貫して保証されます。
- **cts manual** で TrustSec を有効にすると、一時的にインターフェイスでフラッピングが発生します。
- SD-Access ボーダーが Cisco Catalyst スイッチの場合、SD-Access ボーダーのスイッチポートで **cts manual** の後に **policy static sgt <sgt number> trusted** を設定すると、トランクリンクのすべての VLAN で CTS が有効になります。SD-WAN エッジでは、親の物理インターフェイスで **cts manual** を設定し、サブインターフェイスで **cts manual** と **policy static sgt <sgt number> trusted** を設定します。<*sgt number*> は、タグが付いていないか信頼されていない着信トラフィックに適用する SGT 値です。

ハブからブランチへのレイヤ 3 マルチキャスト

トレーディングフロアのアーキテクチャでは、データおよびビデオフィードサービスにマルチキャストプロトコルを使用します。Cisco DNA Center と Cisco SD-WAN により、ハブからブランチへのマルチキャストを可能にするフレームワークが提供されます。次の図は、レイヤ 3 マルチキャストトポロジを示しています。

図 *3*: ソリューションのテスト マルチキャスト トポロジ



金融業界では、メインサイト、小規模サイト、およびミニサイトでネイティブマルチキャストが有効になっています。SD-Access ネイティブマルチキャストは、アンダーレイの Source Specific Multicast（SSM; 送信元特定マルチキャスト）に依存します。したがって、SSM 設定はファブリック ノード、中間ノード、および SD-WAN WAN エッジで設定されます。マルチキャスト ランデブー ポイント（RP）は、SD-Access ファブリックの外部にあります。サイト固有のマルチキャスト送信元をリモートマルチキャスト RP に伝達するために MSDP ピアリングが有効になります。レプリケータは SD-WAN WAN エッジで設定されます。

マルチキャストが SD-WAN WAN エッジのサービス VPN サブインターフェイスで有効になり、ファブリックボーダーのアンダーレイネットワークに接続されます。このトポロジにより、ファブリックノードおよび SD-WAN WAN エッジ全体で完全なエンドツーエンドのネイティブマルチキャスト設定が確立されます。

テレメトリ

Cisco DNA Center は、テレメトリを使用してデバイスとクライアントのデータを収集し、アシュアランスのネットワーク正常性情報を提供します。

- テレメトリ接続を有効にするには、デバイスを NETCONF で検出します。
- すでに NETCONF なしで検出されているデバイスについては、NETCONF で再検出し、[Update the Telemetry Settings with Force] オプションを使用します。
- Cisco DNA Center で FQDN 証明書を使用してデバイスのテレメトリを収集する場合、デバイスで Cisco IOS 17.5.1 が実行されている必要があります。

ロールベース アクセス コントロールと監査ログ

金融機関には、ロールに基づくきめ細かいアクセス制御が必要です。Cisco DNA Center は、特定の機能へのユーザアクセスを許可または制限するカスタムロールを定義するためのロールベース アクセス コントロール（RBAC）をサポートしています。詳細については、「Cisco DNA Center User Role Permissions」を参照してください。Cisco DNA Center は、ユーザアクティビティのモニタリングに使用できるイベントベースの監査ログを生成します。

- SUPER-ADMIN-ROLE ユーザのみがカスタムロールを定義できます。Cisco DNA Center では、これらの権限をすでに持つ admin ロールがデフォルトで用意されています。
- 監査ログは日時でフィルタ処理されます。
- 監査ログは、さらなる処理と保存のために外部ログサーバで公開されます。

Cisco DNA Center ディザスタ リカバリ

金融業界ではネットワークの復元力が重要です。Cisco DNA Centerディザスタリカバリは、データセンターの障害保護を提供します。詳細については、「Implement Disaster Recovery」を参照してください。

- メインサイトとリカバリサイトの両方に同じセキュリティ証明書がインストールされています。
- FQDNベースの証明書の場合、システム名がメインサイトとリカバリサイトの両方で同じである必要があります。
- Cisco DNA Center ディザスタリカバリの GUI で、すべてのイベント履歴が保持されます。電子メール、ログサーバ、および Web サーバによる通知が有効になっています。
- 『Cisco DNA Center Security Best Practices Guide』で、ディザスタリカバリの設定に関するベストプラクティスについて説明しています。メインサイトとリカバリサイトがファイアウォールを越える場合にブロックを解除する必要がある TCP ポートと UDP ポートも示してあります。
- Cisco DNA Center ディザスタリカバリのラウンドトリップ時間（RTT）の遅延は 350 ミリ秒です。
- アシュアランス データはクラスタ間で複製されません。フェールオーバーが完了した後に、デバイスから新しいアクティブな Cisco DNA Center クラスタへの アシュアランス データの送信が開始されます。

参照

- Cisco SD-Access Solution Design Guide (Cisco Validated Design)
- Cisco DNA Center のユーザロール権限
- ディザスタリカバリの実装
- Support for Multiple Cisco DNA Center Clusters with a Single Cisco ISE System
- Cisco DNA Center リリースノート

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

この資料の記載内容は2008年10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
〒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
お問い合わせ先：シスコ コンタクトセンター
0120-092-255（フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

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