概要

Cisco ACI ファブリックをパブリック クラウドに拡張する

Cisco Application Centric Infrastructure プライベート クラウドを所有している（ACI）顧客は、パブリック クラウドでワークロードの一部を実行することがあります。ただし、ワークロードをパブリック クラウドに移行するには、別のインターフェイスで作業し、接続を設定してセキュリティ ポリシーを定義するさまざまな方法を学習する必要があります。これらの課題に対処すると、運用コストが増加し、一貫性が失われる可能性があります。

Cisco ACI は、Cisco Cloud Network Controller を使用して、マルチサイト ファブリックを Amazon Web Services（AWS）、Microsoft Azure、および Google Cloud パブリック クラウドに拡張できます。

Cisco Cloud Network Controller とは

Cisco Cloud Network Controller は、クラウドベース仮想マシン（VM）で展開可能な Cisco APIC のソフトウェア デプロイメントです。Cisco Cloud Network Controller は、次の機能を提供します。

- Amazon AWS、Microsoft Azure、または Google Cloud パブリック クラウドと対話するための既存の Cisco APIC インターフェイスと同様のインターフェイスを提供します。
- クラウド導入の導入と設定を自動化します。
- クラウド ルータ コントロール プレーンを設定します。

- オンプレミス Cisco ACI ファブリックとクラウドサイト間のデータ パスを設定します。
- Cisco ACI ポリシーをクラウド ネイティブ ポリシーに変換します。
- エンドポイントを検出します。

Cisco ACI Extension からパブリック クラウドへのメリットを享受するには

Cisco Cloud Network Controller は、パブリック クラウドへの Cisco ACI 拡張の重要な部分です。Cisco Cloud APICは、オンプレミスのデータセンターまたはパブリック クラウドの両方またはいずれかに展開されたワークロードに対して一貫したポリシー、セキュリティ、および分析を提供します。

パブリック クラウドへの Cisco ACI 拡張は、オンプレミスのデータセンターとパブリック クラウド間の自動接続を提供し、プロビジョニングとモニタリングを容易にします。また、オンプレミスのデータセンターとパブリック クラウド間、またはクラウド サイト間でポリシーを管理、監視、およびトラブルシューティングするための単一のポイントを提供します。

AWS GovCloud のサポート

Cisco Cloud Network Controller は、us-gov-west および us-gov-east リージョンで AWS GovCloud をサポートしています。Cisco CCR は、us-gov-east リージョンにも展開できます。

AWS GovCloud に Cisco Cloud Network Controller を展開する場合、これらの領域には固有の設定があることに注意してください。

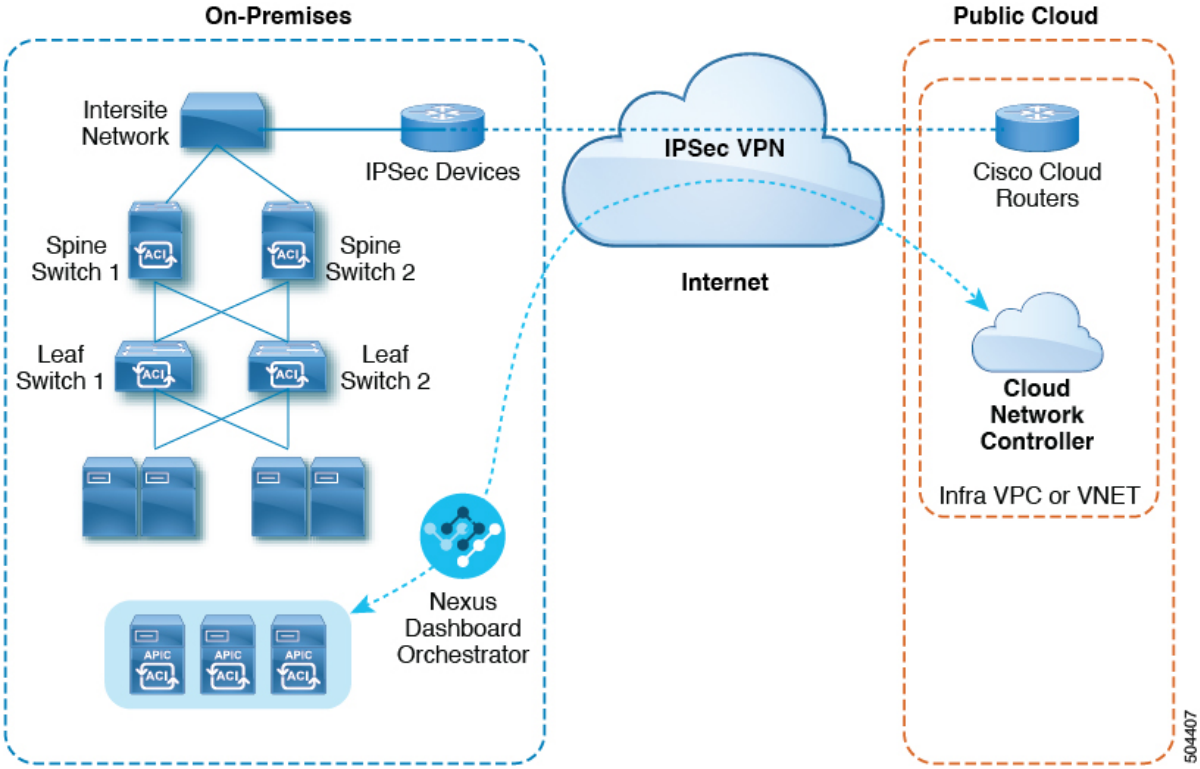
- 商用アカウントで CCR に登録します。
- 商用アカウントで Cisco Cloud Network Controller に登録します。
- 商用アカウントからクラウド形成テンプレートを起動し、ログインのために AWS GovCloud にリクエストをリダイレクトします。

Cisco ACI ファブリックをパブリック クラウドに拡張するためのコンポーネント

マルチサイト ファブリックをパブリック クラウドに拡張するには、それぞれに固有の役割を持つ複数のコンポーネントが必要です。

次の図は Cisco Cloud Network Controller のアーキテクチャの内容を示しています。

図 *1 : Cisco Cloud Network Controller* のアーキテクチャ



オンプレミスデータセンターコンポーネント

Cisco ACI ファブリックおよび Cisco APIC

Cisco ACI では、アプリケーション要件でネットワークを定義できます。このアーキテクチャにより、アプリケーションの導入ライフサイクル全体がシンプルになって最適化され、短時間で完了します。Cisco Application Policy Infrastructure Controller（APIC）の主要コンポーネントです。Cisco ACIこれにより、アプリケーションは、ネットワーク、コンピューティング、およびストレージ機能を含むセキュアで共有された高性能リソース プールに直接接続できます。

マルチサイトおよびマルチサイト オーケストレータ/Cisco Nexus Dashboard Orchestrator

マルチサイトは、プログラムを利用してアプリケーションがネットワーク要件を定義することを可能にするアーキテクチャです。このアーキテクチャにより、アプリケーションの展開が簡素化・最適化され、そして促進されます。Cisco Cloud Network Controller を使用してファブリックをパブリッククラウドに拡張するには、Multi-Siteをインストールする必要があります。

詳細については、Cisco.com の Nexus Dashboard のマニュアルおよびこのガイドのセクション マルチサイトを介した Cisco Cloud Network Controller の管理 を参照してください。

Cisco Nexus Dashboard Orchestrator （NDO）は、複数のファブリック（サイト）で複数の Cisco Application Policy Infrastructure Controller（APIC）のインスタンスを管理します。

Cisco ACI ファブリックをパブリック クラウドに拡張すると、Cisco Nexus Dashboard Orchestrator はオンプレミスのデータセンターとパブリック クラウド間の接続を作成します。マルチサイト

を使用して、オンプレミスのデータセンターとパブリッククラウド全体にテナントを作成します。

（注） オンプレミスファブリックを設定する必要があります。ファブリック外部接続ポリシーを作成し、マルチサイトに必要なオーバーレイTEPおよびその他の情報を定義します。Cisco ACIまた、マルチサイトアーキテクチャにオンプレミスファブリックを追加する必要があります。Cisco ACICisco.com の *Nexus Dashboard Configuration Guide* を参照してください。

詳細については、Cisco.com の Nexus Dashboard のマニュアルおよびこのガイドのセクション マルチサイトを介した Cisco Cloud Network Controller の管理 を参照してください。

IP セキュリティ（IPSec）ルータ

オンプレミス サイトとパブリック クラウド サイト間の IPsec 接続を確立するには、インターネット プロトコル セキュリティ（IPsec）対応のルータが必要です。

AWS パブリック クラウド コンポーネント

Cisco Cloud Network Controller

Cisco Cloud Network Controller は次のアクションを実行します。

- パブリック クラウド上のサイトを定義し、クラウド インフラ仮想プライベート クラウド（VPC）または仮想ネットワーク（VNET）をプロビジョニングし、すべてのリージョンで Cisco クラウド ルータ（CCR）を管理します。
- パブリッククラウドでポリシーモデルをレンダリングし、クラウドの健全性を管理します。Cisco ACI

詳細については、*Cisco Cloud Network Controller* リリース ノート を参照してください。このガイドの AWS での Cisco Cloud Network Controller の展開 および セットアップ ウィザードを使用した Cisco Cloud Network Controller の構成 も参照してください。

Cisco Cloud ルータ

シスコ クラウド ルータ（CCR）は、仮想およびクラウド環境で包括的な WAN ゲートウェイとネットワークサービスを提供します。CCR により、企業はWANをプロバイダーがホストするクラウドに拡張できます。Cisco Cloud Network Controller ソリューションには 2 つの CCR が必要です。

リリース 25.0(3) 以降、Cisco Cloud Network Controller では **Cisco Catalyst 8000V** をクラウド サービス ルータとして使用します。この CCR の詳細については、『CSR 8000v のマニュアル』 を参照してください。

AWS パブリック クラウド

AWSは、コンピューティング、ストレージ、ネットワーク、データベースなどのオンデマンドサービスを提供するクラウドベースのプラットフォームです。AWS のサブスクライバは、インターネット経由でワークロードを実行できる仮想コンピュータにアクセスできます。

詳細については、AWS の Web サイトのマニュアルを参照してください。

オンプレミスデータセンターとパブリッククラウド間の接続

IPsec VPN

パブリックにルーティング可能な IP アドレスを含み、AWS または Microsoft Azure の接続に十分な帯域幅を持つ、IPsec ルータからの VPN とのインターネット接続が必要です。

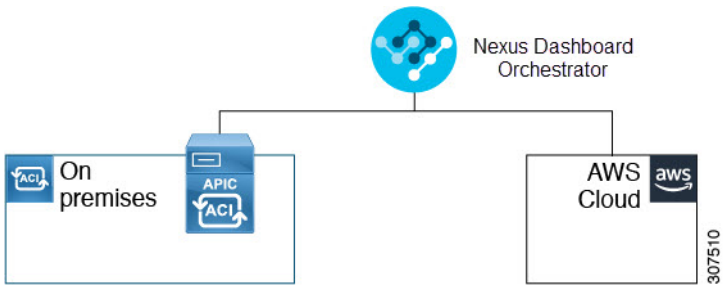
管理接続

オンプレミスのデータ センターの Nexus Dashboard Orchestrator とパブリック クラウドの Cisco Cloud Network Controller の間に管理接続が必要です。

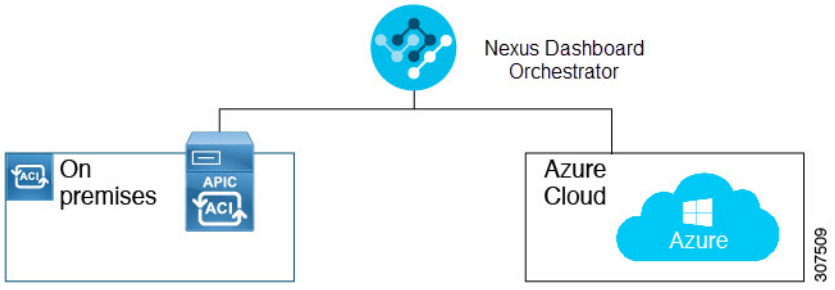
サポートされているクラウドコンピューティング プラットフォームと接続オプション

Cisco Cloud Network Controller は、次のクラウド コンピューティング プラットフォームをサポートしています。

- リリース 4.1(1) の Cisco Cloud Network Controller の初期リリースの一部として、オンプレミスからクラウドへの接続、またハイブリッド-クラウドに対するサポートが提供されており、シス コ Cisco Nexus Dashboard Orchestrator を使用してオンプレミス Cisco ACI サイトを拡張することができます。



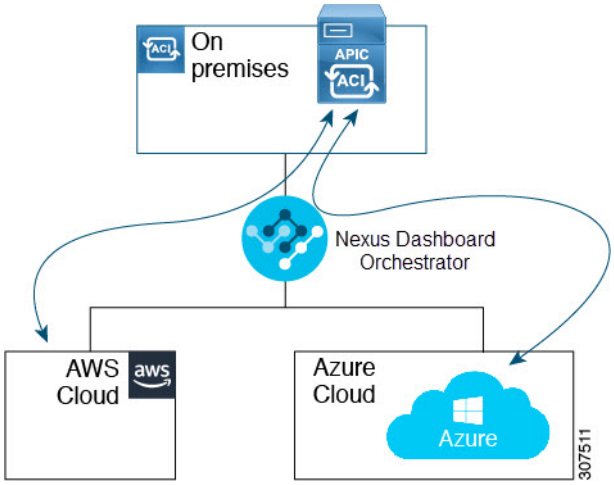
- リリース 4.2(1) 以降、Cisco Cisco Nexus Dashboard Orchestrator を使用してオンプレミス Cisco ACI サイトを Microsoft Azure パブリック クラウドに拡張できるようになりました。



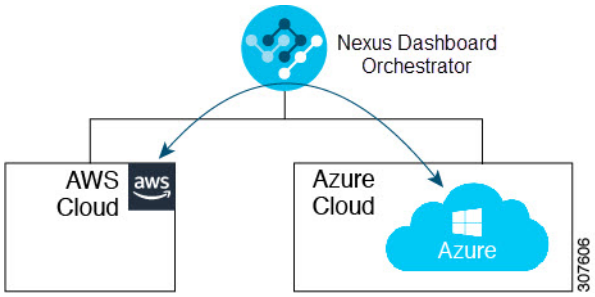
- Cisco Cisco Nexus Dashboard Orchestrator を使用してオンプレミス Cisco ACI サイトを Google Cloud パブリック クラウドに拡張するためのサポートを利用できます。

Cisco Nexus Dashboard Orchestrator を使用して、次のコンポーネント間の接続を確立することもできます。

- オンプレミスからクラウドへの接続：
  - 次のパブリッククラウドサイトの接続：
    - オンプレミス Cisco ACI および Amazon AWS パブリック クラウド サイト
    - オンプレミスおよびMicrosoft Azureパブリッククラウドサイト Cisco ACI
    - オンプレミス Cisco ACI と Google Cloud パブリック クラウド サイト
  - オンプレミスからシングルクラウドサイトへの接続（ハイブリッドクラウド）
  - オンプレミスから複数のクラウドサイトへの接続（ハイブリッドマルチクラウド）



- クラウドサイト間接続（マルチクラウド）：
  - Amazon AWSパブリッククラウドサイト間（Amazon AWSパブリッククラウドサイトからAmazon AWSパブリッククラウドサイト）
  - Microsoft Azureパブリッククラウドサイト間（Microsoft Azureパブリッククラウドサイトから Microsoft Azureパブリッククラウドサイト）
  - Google Cloud パブリック クラウド サイト間（Google Cloud パブリック クラウド サイトから Google Cloud パブリック クラウド サイトへ）
  - Amazon AWS 、Microsoft Azure、および Google Cloud パブリック クラウド サイト間



さらに、シングルクラウド設定（Cloud First）もサポートされます。

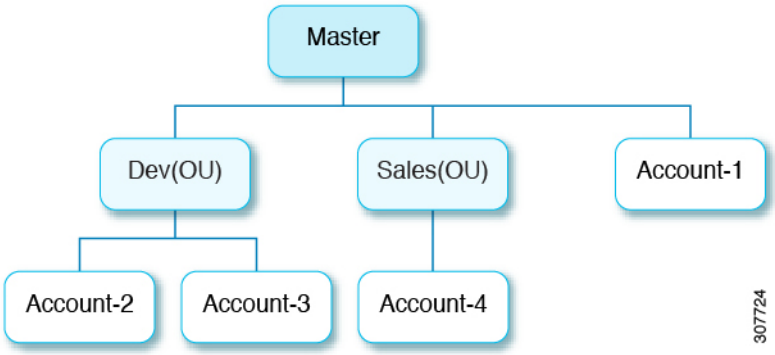
AWS Organizations と組織のユーザ テナントのサポート

組織内の複数のアカウントを使用すると、さまざまなアカウントのアクセスポリシーとアクセス許可を個別に制御するのは簡単ではありませんが、組織内の組織レベルまたは組織内のサブ組織レベルで簡単に行うことができます。

企業では、AWS Organizations を使用して、次に説明するように、組織内で複数の AWS アカウントを管理することができます。

https://aws.amazon.com/organizations/

組織内のアカウント(またはサブアカウント)のアクセスポリシーの管理は、組織内のアカウント階層のルートにある組織のマスターアカウントによって行われます。次の図は、組織におけるアカウントの設定例を示しています。



AWS アカウントが AWS Organizations の一部になる方法は 2 つあります。

- **作成**: マスターアカウント内の既存の組織内では、AWS GUI または AWS API を使用して、AWS Organizations に自動的に含まれる AWS アカウントを作成できます。
- **招待**: 組織の外部で作成されたが、組織に参加する必要があるアカウントの場合は、マスターアカウントからアカウント所有者に招待を送信する必要があります。招待状に同意すると、招待されたアカウントは組織内のサブアカウントになります。

AWS Organizations を使用して AWS アカウントを統合および管理する場合は、通常のように、AWS Organizations を使用して組織を設定し、作成されたまたは招待されたアカウントを追加します。詳細については、「組織の作成」を参照してください。

作成済みまたは招待されたアカウントを AWS を介して組織に追加したら、Cisco Cloud Network Controller が AWS を通じて行った AWS Organizations の構成を Cisco Cloud Network Controller が認識するように、必要な構成を行います。Cisco Cloud Network Controller は、AWS Organizations テナントのポリシーを管理するために、`OrganizationAccountAccessRole` IAM ロールを使用します。

- マスター アカウント内の既存の組織内で AWS アカウントを**作成**した場合は、その作成した AWS アカウントに組織の `OrganizationAccountAccessRole` IAM ロールが自動的に割り当てられます。この場合、AWS の`OrganizationAccountAccessRole` の IAM ロールを手動で設定する必要はありません。
- マスター アカウントが組織に参加するために既存の AWS アカウントを**招待**した場合は、AWS で`OrganizationAccountAccessRole` IAM ロールを手動で設定する必要があります。組織テナントの AWS で `OrganizationAccountAccessRole` IAM ロールを設定し、Cisco Cloud Network Controller に関連する権限があることを確認します。

  `OrganizationAccountAccessRole` IAM ロールは、組織またはアカウントに使用される SCP（サービス制御ポリシー）とともに、組織またはアカウントに対して、組織またはアカウントに使用する SCP（サービス制御ポリシー）とともに、組織のポリシーを管理するために Cisco Cloud Network Controller に必要な最小限の権限が付与されている必要があります。アクセス ポリシーの要件は、信頼できるテナントまたは信頼できないテナントの要件と同じです。

  詳細については、次の URL にある Cisco Cloud Network Controller for AWS ユーザー ガイドの「テナント AWS プロバイダの設定」の項を参照してください。

その後、共有テナントの設定で説明されている手順を使用して、Cisco Cloud Network Controller GUI を介してテナントに組織タグを割り当てることができます。

ポリシーの用語

Cisco Cloud Network Controller の主要な機能は、 Cisco Application Centric Infrastructure（ACI）ポリシーのパブリック クラウドのネイティブ コンストラクトへの変換です。

次の表に、Amazon Web Services（AWS）のポリシー用語と同等の用語を示します。Cisco ACI

Cisco ACI	**AWS**
テナント	ユーザー アカウント
AAA ユーザ、セキュリティ ドメイン	Identity and Access Management（IAM）
Virtual Routing and Forwarding（VRF）	VPC
BD サブネット	Virtual Private Cloud（VPC）のサブネット CIDR

Cisco ACI	AWS
ACI インフラ（または ACI インフラ テナント）	VPC（Cisco Cloud Network Controller ではインフラ VPC と呼ばれる）
契約、フィルタ	セキュリティ グループ ルールの作成
タブー	ネットワーク アクセス リスト
EPG	セキュリティ グループ
EP から EPG へのマッピング	タグ、ラベル
エンドポイント	EC2 インスタンスのネットワーク アダプタ

Cisco Cloud Network Controller のライセンシング

ここでは、Cisco Cloud Network Controller を使用するためのライセンシング要件を示します。

Cisco Catalyst 8000V

Cisco Cloud Network Controller 上の Cisco Catalyst 8000V は次のライセンス モデルをサポートしています。

1. **所有ライセンス持ち込み（BYOL）**ライセンス モデル
2. **ペイアズユーゴー（PAYG）**ライセンス モデル

BYOL ライセンス モデル

Cisco Catalyst 8000V の BYOL ライセンス モデルでは、Cisco から Catalyst 8000V Cisco DNA ライセンスを購入し、クラウドに展開する必要があります。

- ティアベースの Cisco Catalyst 8000V ライセンスの 1 つにサブスクライブする手順については、Cisco Catalyst 8000V Edge ソフトウェアを参照してください。
- 階層に基づくさまざまなスループットの詳細については、Cisco Cloud Network Controller ユーザー ガイドの、「Cisco Catalyst 8000V について」の「スループット」セクションを参照してください。

PAYGライセンス モデル

25.0(4) リリース以降、Cisco Cloud Network Controller は Cisco Catalyst 8000V でのペイアズユーゴー（PAYG）ライセンス モデルをサポートしています。これにより、ユーザーは VM サイズに基づいてクラウドに Catalyst 8000V インスタンスを展開し、時間単位で使用料を支払うことができます。

スループットを得るために VM サイズに完全に依存しているため、PAYG ライセンス モデルを有効にするには、まず現在の Cisco Catalyst 8000V の展開を解除してから、新しい VM サイ

ズでの初回セットアップを使用して再度展開します。詳細については、セットアップ ウィザードを使用した Cisco Cloud Network Controller の構成を参照してください。

（注） 使用可能な2つのライセンス タイプを切り替える場合も、ライセンスを切り替える手順を使用できます。

（注） AWS マーケットプレイスでライセンスを使用するには、**Catalyst 8000V Cisco DNA Essentials** と **Catalyst 8000V Cisco DNA Advantage** の 2 つの PAYG オプションがあります。Cisco Cloud Network Controller は、**Catalyst 8000V Cisco DNA Advantage** を利用します。「Cisco DNA Advantage」サブスクリプションでサポートされる機能については、『Cisco DNA Software SD-WAN およびルーティング マトリックス』を参照してください。

Cisco Cloud Network Controller およびオンプレミス ACI ライセンスの概要

- オンプレミス Cisco ACI サイトのすべてのリーフスイッチのライセンス要件：
  - Cisco ACI オンプレミス サイトが単一サイトの場合、オンプレミス リーフスイッチには Essentials ライセンス階層（またはそれ以上）を使用します。
  - Cisco ACI オンプレミス サイトがマルチサイトの場合、オンプレミス リーフスイッチには Advantage ライセンス階層（またはそれ以上）を使用します。
- Cisco Cloud Network Controller インスタンスによって管理されるすべての VM インスタンスのライセンス要件：
  - クラウド上の Cisco ACI に Cisco Cloud Network Controller が 1 つしかない場合は、Cisco Cloud Network Controller に Essentials クラウド ライセンス階層（またはそれ以上）を使用します。
  - クラウド上の Cisco ACI に Cisco Cloud Network Controller が 1 つ以上ある場合は、Cisco Cloud Network Controller に Advantage クラウド ライセンス階層（またはそれ以上）を使用します。

Amazon Web Services（AWS）

ライセンスのタイプに基づき、AWS Marketplace を介して 登録する必要があります。

- **BYOL ライセンス モデル**の場合は、**[Cisco Catalyst 8000V エッジ ソフトウェア - BYOL（Cisco Catalyst 8000V Edge Software- BYOL）]** に登録します。
- **PAYG ライセンス モデル**の場合は、**Cisco Catalyst 8000V Edge Software - PAYG** に登録します。

Cisco Cloud Network Controller の関連ドキュメント

Cisco Cloud Network Controller、 Nexus Dashboard、および Amazon Web Services（AWS）に関する情報は、さまざまなリソースから入手できます。

シスコのドキュメント

Cisco.com でシスコ製品のマニュアルを参照してください。

- Cisco Cloud Network Controller の関連ドキュメント

  ビデオ、リリース ノート、基礎、インストール、設定、およびユーザ ガイドが含まれています。

- Nexus Dashboard の関連ドキュメント

  ビデオ、リリース ノート、インストール、設定、およびユーザ ガイドが含まれています。

- Cisco Cloud Router の関連ドキュメント

  リリース ノート、コマンド リファレンス、データ シート、インストール、アップグレード、および設定ガイドが含まれています。

AWS ドキュメント

AWS Web サイトで、ユーザ ガイド、FAQ、ケース スタディ、ホワイト ペーパーなどのドキュメントを検索できます。

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。