AWS Marketplace を使用した展開

AWS Marketplace を使用した AWSでの Cisco DNA Center の手動展開

AWS の管理に精通している場合は、AWS Marketplace を使用して AWS アカウントで Cisco DNA Center を手動展開するオプションが用意されています。

AWS Marketplace ワークフローを使用した手動展開

このメソッドで AWS に Cisco DNA Center を展開するには、大まかに言って次の手順を実行します。

1. 前提条件を満たします。AWS Marketplace を使用した手動展開の前提条件 （2 ページ）を参照してください。
2. （任意）AWS 上の Cisco ISE と Cisco DNA Center VA を統合します。「AWS での AWS 上の Cisco ISE と Cisco DNA Center の統合に関するガイドライン」を参照してください。
3. AWS Marketplace を使用して AWS に Cisco DNA Center を展開します。AWS Marketplace を使用した AWS での Cisco DNA Center の手動展開 （7 ページ） を参照してください。
4. 環境のセットアップと Cisco DNA Center VA の設定が正しく行われ、想定どおりに動作していることを確認します。展開の検証 （7 ページ）を参照してください。

AWS Marketplace を使用した手動展開の前提条件

AWS での Cisco DNA Center の展開を開始する前に、次のネットワーク、AWS、Cisco DNA Center の要件が満たされていることを確認してください。

ネットワーク環境

ご使用のネットワーク環境に関する次の情報を把握しておく必要があります。

- エンタープライズ DNS サーバーの IP アドレス
- （オプション）HTTPS ネットワークプロキシの詳細

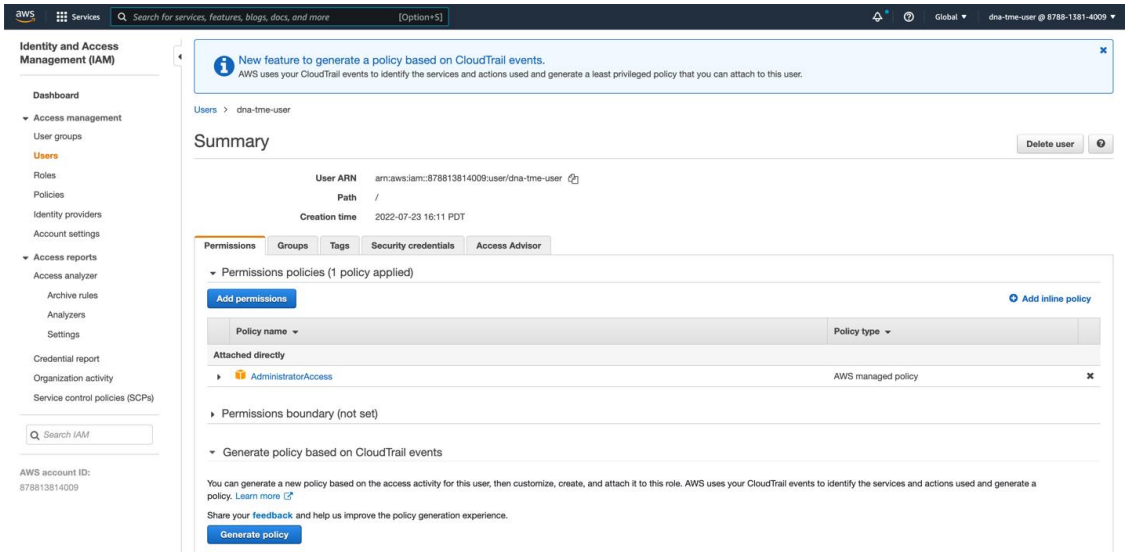
AWS 環境

次の AWS 環境要件を満たす必要があります。

- AWS アカウントにアクセスするための有効なログイン情報を保有していること。

（注） リソースの独立性と分離を維持するために、AWS アカウントをサブアカウント（子アカウント）にすることを推奨します。サブアカウントを使用することで、Cisco DNA Center を展開しても既存のリソースは影響を受けません。

- **重要**：お使いの AWS アカウントが AWS Marketplace の Cisco DNA Center Virtual Appliance - Bring Your Own License (BYOL) に登録されていること。
- AWS アカウントに管理者アクセス権限が割り当てられていること（AWS では、ポリシー名は **AdministratorAccess** と表示されます）。



- 次のリソースとサービスを AWS で設定する必要があります。
  - **VPC**：推奨されている CIDR 範囲は /25 です。IPv4 CIDR 表記では、IP アドレスの最後のオクテット（4番目のオクテット）の値に指定できるのは0または128のみです。（例：x.x.x.0 または x.x.x.128xxx）。
  - [Subnets]：推奨されるサブネット範囲は /28 です。企業のサブネットと重複しないようにする必要があります。
  - [Route Tables]：VPC サブネットが VPN GW または TGW を介してエンタープライズ ネットワークと通信できることを確認します。
  - [Security Groups]：AWS 上の Cisco DNA Center とエンタープライズ ネットワーク内のデバイス間の通信では、AWS 上の Cisco DNA Center に割り当てる AWS セキュリティ グループで次のポートを許可する必要があります。
    - TCP 22、80、443、9991、25103、32626
    - UDP 123、162、514、6007、21730

    Cisco DNA Center が使用するポート、それらのポート上で通信するサービス、ポート使用におけるアプライアンスの目的、および推奨アクションを次の表に示します。

ポート	サービス名	目的	推奨処置
—	ICMP	デバイスは ICMP メッセージを使用してネットワーク接続の問題を通知します。	ICMP を有効にします。

ポート	サービス名	目的	推奨処置
TCP 22、80、443	HTTPS、SFTP、HTTP	Cisco DNA Centerからのソフトウェアイメージのダウンロードに HTTPS 443、SFTP 22、HTTP 80 を使用します。 Cisco DNA Center からの証明書のダウンロードにHTTPS 443、HTTP 80（Cisco 9800 ワイヤレスコントローラ、PnP）、センサー/テレメトリを使用します。 （注） ポート 80 については、プラグアンドプレイ（PnP）、ソフトウェアイメージ管理（SWIM）、組み込みイベント管理（EEM）、デバイス登録、Cisco 9800 ワイヤレスコントローラを使用しない場合はブロックしてください。	これらのポートでCisco DNA Centerにアクセスできるホストまたはネットワークデバイスの送信元 IP がファイアウォールルールで制限されていることを確認してください。 （注） HTTP 80 の使用は推奨されません。可能な限り HTTPS 443 を使用してください。
UDP 123	NTP	デバイスは時刻の同期にNTPを使用します。	デバイスが時刻を同期できるようにポートを開いておく必要があります。
UDP 162	SNMP	Cisco DNA Center はデバイスから SNMP ネットワークテレメトリを受信します。	SNMP に基づくデータ分析用にポートを開いておく必要があります。
UDP 514	Syslog	Cisco DNA Center はデバイスから syslog メッセージを受信します。	syslogに基づくデータ分析用にポートを開いておく必要があります。
UDP 6007	NetFlow	Cisco DNA Center はデバイスから NetFlow ネットワークテレメトリを受信します。	NetFlow に基づくデータ分析用にポートを開いておく必要があります。
TCP 9991	Wide Area Bonjour サービス	Cisco DNA Center は、Bonjour 制御プロトコルを使用して、サービス検出ゲートウェイ（SDG）エージェントからマルチキャストドメイン ネーム システム（mDNS）トラフィックを受信します。	Bonjourアプリケーションがインストールされている場合、Cisco DNA Center でポートを開いておく必要があります。

ポート	サービス名	目的	推奨処置
UDP 21730	アプリケーション可視性サービス	アプリケーション可視性サービスの CBAR デバイス通信。	ネットワークデバイスで CBAR が有効になっている場合、ポートを開いておく必要があります。
TCP 25103	ストリーミングテレメトリが有効になっている Cisco 9800 ワイヤレスコントローラおよび Cisco Catalyst 9000 スイッチ	テレメトリに使用されます。	Cisco DNA Center と Catalyst 9000 デバイス間のテレメトリ接続用にポートが開いている必要があります。
TCP 32626	インテリジェントキャプチャ（gRPC）コレクタ	Cisco DNA アシュアランス インテリジェントキャプチャ（gRPC）機能で使用されるトラフィック統計情報とパケットキャプチャデータの受信に使用されます。	Cisco DNA アシュアランス インテリジェントキャプチャ（gRPC）機能を使用する場合、ポートを開いておく必要があります。

- [VPN Gateway (VPN GW)] または [Transit Gateway (TGW)]：エンタープライズ ネットワークへの既存の接続が必要です。これはカスタマーゲートウェイ（CGW）を指します。

  CGW から AWS への既存の接続については、ファイアウォール設定またはプロキシゲートウェイのどちらでポートを開くかを問わず、Cisco DNA Center VA との間で送受信されるトラフィックフローに対して適切なポートが開いていることを確認する必要があります。アプライアンスで使用される既知のネットワークサービスポートの詳細については、『Cisco DNA Center First-Generation Appliance Installation Guide, Release 2.3.5』の「Plan the Deployment」の章に記載されている「Required Network Ports」[英語] を参照してください。

- [Site-to-Site VPN Connection]：TGW アタッチメントと TGW ルートテーブルを使用できます。

- AWS 環境は、次のいずれかのリージョンで設定する必要があります。
  - ap-northeast-1（東京）
  - ap-northeast-2（ソウル）
  - ap-south-1（ムンバイ）
  - ap-southeast-1（シンガポール）
  - ap-southeast-2（シドニー）
  - ca-central-1（カナダ）
  - eu-central-1（フランクフルト）
  - eu-south-1（ミラノ）

- eu-west-1（アイルランド）
- eu-west-2（ロンドン）
- eu-west-3（パリ）
- us-east-1（バージニア）
- us-east-2（オハイオ）
- us-west-1（北カリフォルニア）
- us-west-2（オレゴン）

- 複数の IAM ユーザーが同じ環境設定を使用して Cisco DNA Center を設定できるようにするには、次のポリシーを持つグループを作成し、該当するユーザーをそのグループに追加する必要があります。
  - IAMReadOnlyAccess
  - AmazonEC2FullAccess
  - AWSCloudFormationFullAccess

- Cisco DNA Center インスタンスのサイズは、次の最小リソース要件を満たす必要があります。
  - r5a.8xlarge

重要 Cisco DNA Center は r5a.8xlarge インスタンスサイズのみをサポートします。この設定は変更できません。さらに、r5a.8xlarge インスタンスサイズは、特定の可用性ゾーンではサポートされていません。サポートされている可用性ゾーンのリストを表示するには、『*Release Notes for Cisco Global Launchpad*』[英語] を参照してください。

  - 32 vCPU
  - 256 GB RAM
  - 4 TB ストレージ
  - 2500 ディスク入出力処理/秒（IOPS）
  - 180 MBps のディスク帯域幅

- 次の AWS 情報を用意します。
  - サブネット ID
  - セキュリティ グループ ID

- キーペア ID
- 環境名
- CIDR 予約

Cisco DNA Center 環境

Cisco DNA Center 環境が次の要件を満たす必要があります。

- Cisco DNA Center GUI にアクセスできること。
- 次の Cisco DNA Center 情報を用意します。
  - NTP 設定
  - デフォルトゲートウェイ設定
  - CLI パスワード
  - UI のユーザー名とパスワード
  - スタティック IP
  - Cisco DNA Center IP アドレスの FQDN

AWS Marketplace を使用した AWS での Cisco DNA Center の手動展開

AWS Marketplace を使用して AWS で Cisco DNA Center を展開する方法については、次のいずれかを実行してください。

- シスコのソフトウェアダウンロードサイトに移動し、次のファイルをダウンロードします。

  `Deploy-cisco-dna-center-using-aws-marketplace-1.8.0.tar.gz`

- シスコのソフトウェアダウンロードサイトに移動し、次のファイルをダウンロードします。

  `Deploy-cisco-dna-center-on-aws-using-aws-marketplace-1.7.0.zip`

展開の検証

環境のセットアップと Cisco DNA Center VA の設定が正常に機能していることを確認するには、次の検証チェックを実行します。

始める前に

AWS Marketplace でスタックの作成時にエラーが発生していないことを確認します。

手順

ステップ 1 Amazon EC2 コンソールから、ネットワークとシステムの設定を検証し、Cisco DNA Center IP アドレスが正しいことを確認します。

ステップ 2 Cisco DNA Center の IP アドレスに ping を送信して、ホストの詳細とネットワーク接続が有効であることを確認します。

ステップ 3 Cisco DNA Center との SSH 接続を確立して、Cisco DNA Center が認証されていることを確認します。

ステップ 4 次のいずれかのメソッドを使用して、Cisco DNA Center GUI への HTTPS アクセシビリティをテストします。

- ブラウザを使用します。

  ブラウザの互換性の詳細については、『*Cisco DNA Center Release Notes*』[英語] を参照してください。

- CLI で Telnet を使用します。
- CLI で curl を使用します。

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。