AWS CloudFormation を使用した展開

AWS CloudFormation 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 CloudFormation を使用して AWS アカウントで Cisco DNA Center AMIを手動展開するオプションが用意されています。

この方法では、AWS インフラストラクチャを作成し、VPN トンネルを確立して、Cisco DNA Center を展開する必要があります。

AWS CloudFormation 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 CloudFormation 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 CloudFormation を使用して AWS に Cisco DNA Center を展開します。AWS CloudFormation を使用した AWS での Cisco DNA Center の手動展開 （8 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 （13 ページ）を参照してください。

AWS CloudFormation 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、および 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

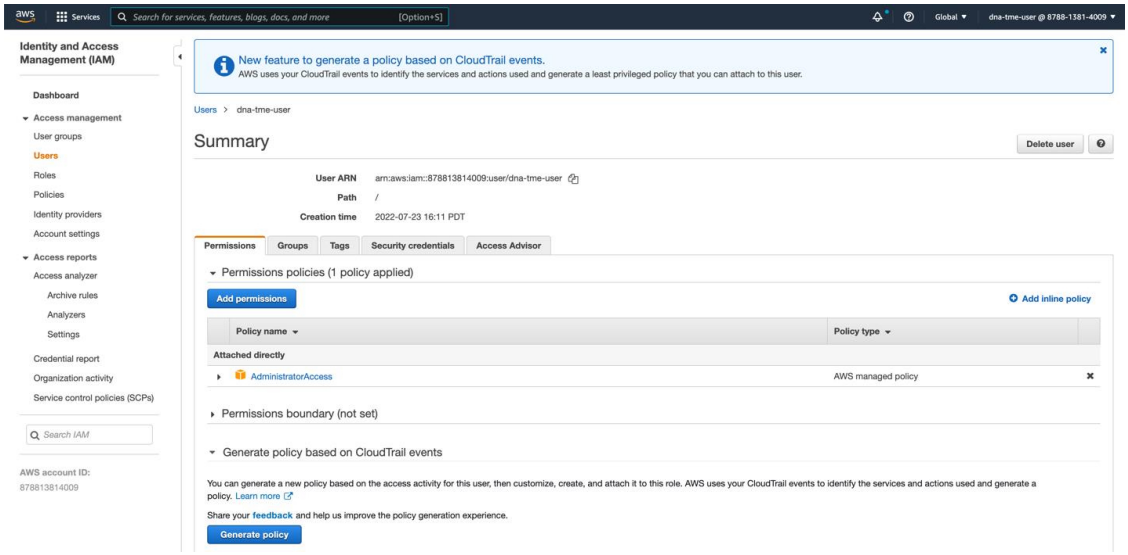
AWS 環境

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。

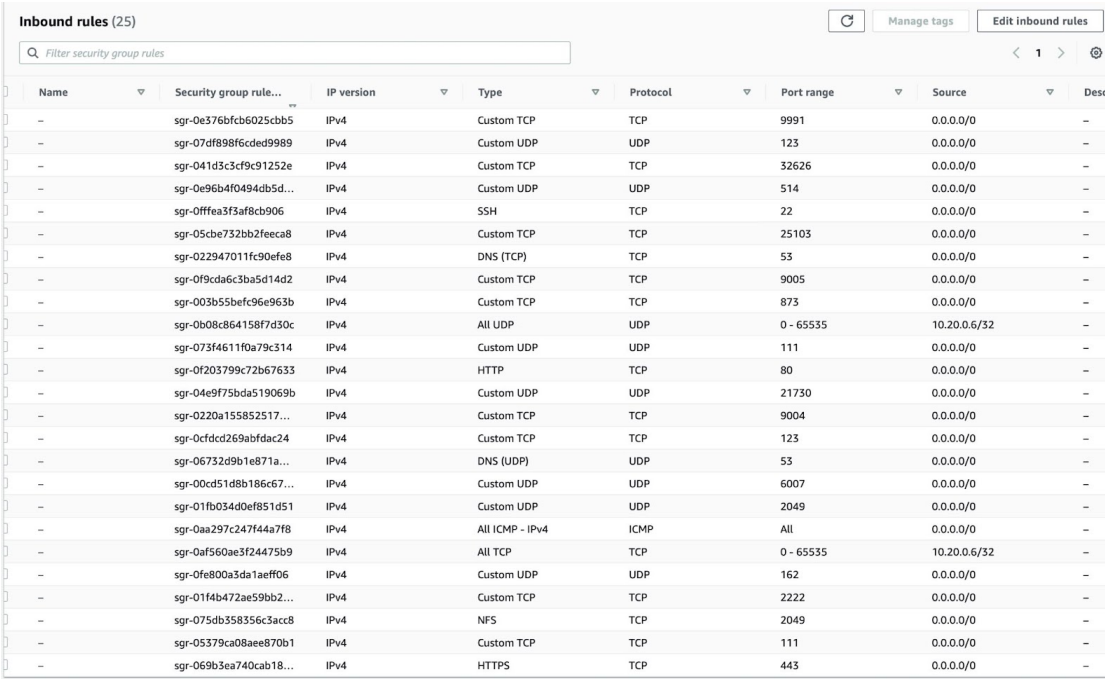
（注） リソースの独立性と分離を維持するために、AWS アカウントをサブアカウント（子アカウント）にすることを推奨します。サブアカウントを使用することで、Cisco DNA Center を展開しても既存のリソースは影響を受けません。

- **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 VA 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 VA 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

    着信ポートと発信ポートも設定する必要があります。着信ポートを設定するには、次の図を参照してください。



Inbound rules (25)

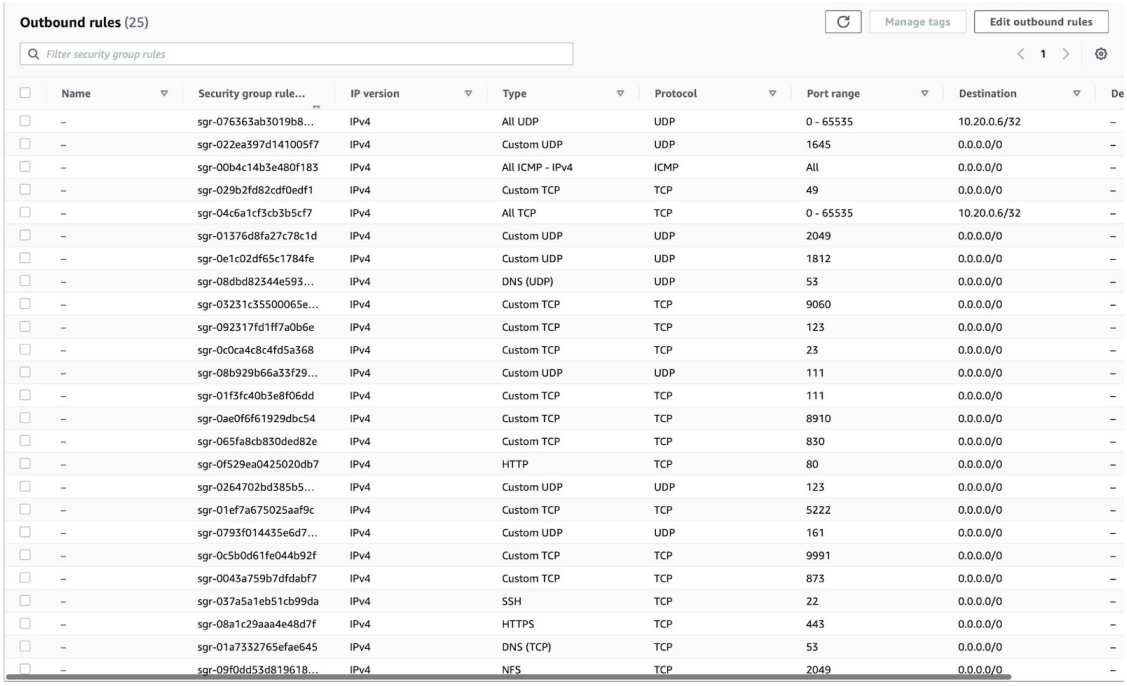
Manage tags | Edit inbound rules

Filter security group rules

1

Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Desc
–	sgr-0e376bfcb6025cbb5	IPv4	Custom TCP	TCP	9991	0.0.0.0/0	–
–	sgr-07df898f6cded9989	IPv4	Custom UDP	UDP	123	0.0.0.0/0	–
–	sgr-041d3c3cf9c91252e	IPv4	Custom TCP	TCP	32626	0.0.0.0/0	–
–	sgr-0e96b4f0494db5d...	IPv4	Custom UDP	UDP	514	0.0.0.0/0	–
–	sgr-0fffea3f3af8cb906	IPv4	SSH	TCP	22	0.0.0.0/0	–
–	sgr-05cbe732bb2feeca8	IPv4	Custom TCP	TCP	25103	0.0.0.0/0	–
–	sgr-022947011fc90efe8	IPv4	DNS (TCP)	TCP	53	0.0.0.0/0	–
–	sgr-0f9cda6c3ba5d14d2	IPv4	Custom TCP	TCP	9005	0.0.0.0/0	–
–	sgr-003b55befc96e963b	IPv4	Custom TCP	TCP	873	0.0.0.0/0	–
–	sgr-0b08c864158f7d30c	IPv4	All UDP	UDP	0 - 65535	10.20.0.6/32	–
–	sgr-073f4611f0a79c314	IPv4	Custom UDP	UDP	111	0.0.0.0/0	–
–	sgr-0f203799c72b67633	IPv4	HTTP	TCP	80	0.0.0.0/0	–
–	sgr-04e9f75bda519069b	IPv4	Custom UDP	UDP	21730	0.0.0.0/0	–
–	sgr-0220a155852517...	IPv4	Custom TCP	TCP	9004	0.0.0.0/0	–
–	sgr-0cfdcd269abfdac24	IPv4	Custom TCP	TCP	123	0.0.0.0/0	–
–	sgr-06732d9b1e871a...	IPv4	DNS (UDP)	UDP	53	0.0.0.0/0	–
–	sgr-00cd51d8b186c67...	IPv4	Custom UDP	UDP	6007	0.0.0.0/0	–
–	sgr-01fb034d0ef851d51	IPv4	Custom UDP	UDP	2049	0.0.0.0/0	–
–	sgr-0aa297c247f44a7f8	IPv4	All ICMP - IPv4	ICMP	All	0.0.0.0/0	–
–	sgr-0af560ae3f24475b9	IPv4	All TCP	TCP	0 - 65535	10.20.0.6/32	–
–	sgr-0fe800a3da1aeff06	IPv4	Custom UDP	UDP	162	0.0.0.0/0	–
–	sgr-01f4b472ae59bb2...	IPv4	Custom TCP	TCP	2222	0.0.0.0/0	–
–	sgr-075db358356c3acc8	IPv4	NFS	TCP	2049	0.0.0.0/0	–
–	sgr-05379ca08aee870b1	IPv4	Custom TCP	TCP	111	0.0.0.0/0	–
–	sgr-069b3ea740cab18...	IPv4	HTTPS	TCP	443	0.0.0.0/0	–

発信ポートを設定するには、次の図を参照してください。


Outbound rules (25)

Manage tags | Edit outbound rules

Filter security group rules

1

Name	Security group rule...	IP version	Type	Protocol	Port range	Destination	De
–	sgr-076363ab3019b8...	IPv4	All UDP	UDP	0 - 65535	10.20.0.6/32	–
–	sgr-022ea397d141005f7	IPv4	Custom UDP	UDP	1645	0.0.0.0/0	–
–	sgr-00b4c14b3e480f183	IPv4	All ICMP - IPv4	ICMP	All	0.0.0.0/0	–
–	sgr-029b2fd82cdf0edf1	IPv4	Custom TCP	TCP	49	0.0.0.0/0	–
–	sgr-04c6a1cf3cb3b5cf7	IPv4	All TCP	TCP	0 - 65535	10.20.0.6/32	–
–	sgr-01376d8fa27c78c1d	IPv4	Custom UDP	UDP	2049	0.0.0.0/0	–
–	sgr-0e1c02df65c1784fe	IPv4	Custom UDP	UDP	1812	0.0.0.0/0	–
–	sgr-08dbd82344e593...	IPv4	DNS (UDP)	UDP	53	0.0.0.0/0	–
–	sgr-03231c35500065e...	IPv4	Custom TCP	TCP	9060	0.0.0.0/0	–
–	sgr-092317fd1ff7a0b6e	IPv4	Custom TCP	TCP	123	0.0.0.0/0	–
–	sgr-0c0ca4c8c4fd5a368	IPv4	Custom TCP	TCP	23	0.0.0.0/0	–
–	sgr-08b929b66a33f29...	IPv4	Custom UDP	UDP	111	0.0.0.0/0	–
–	sgr-01f3fc40b3e8f06dd	IPv4	Custom TCP	TCP	111	0.0.0.0/0	–
–	sgr-0ae0f6f61929dbc54	IPv4	Custom TCP	TCP	8910	0.0.0.0/0	–
–	sgr-065fa8cb830ded82e	IPv4	Custom TCP	TCP	830	0.0.0.0/0	–
–	sgr-0f529ea0425020db7	IPv4	HTTP	TCP	80	0.0.0.0/0	–
–	sgr-0264702bd385b5...	IPv4	Custom UDP	UDP	123	0.0.0.0/0	–
–	sgr-01ef7a675025aaf9c	IPv4	Custom TCP	TCP	5222	0.0.0.0/0	–
–	sgr-0793f014435e6d7...	IPv4	Custom UDP	UDP	161	0.0.0.0/0	–
–	sgr-0c5b0d61fe044b92f	IPv4	Custom TCP	TCP	9991	0.0.0.0/0	–
–	sgr-0043a759b7dfdabf7	IPv4	Custom TCP	TCP	873	0.0.0.0/0	–
–	sgr-037a5a1eb51cb99da	IPv4	SSH	TCP	22	0.0.0.0/0	–
–	sgr-08a1c29aaa4e48d7f	IPv4	HTTPS	TCP	443	0.0.0.0/0	–
–	sgr-01a7332765efae645	IPv4	DNS (TCP)	TCP	53	0.0.0.0/0	–
–	sgr-09f0dd53d819618...	IPv4	NFS	TCP	2049	0.0.0.0/0	–

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 VA IP アドレスの FQDN

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

AWS CloudFormation を使用して手動で AWS に Cisco DNA Center を展開することもできます。提供されている AWS CloudFormation のテンプレートには、すべての必須パラメータに関連する詳細情報が含まれています。

展開プロセスの一環として、Cisco DNA Center インスタンスの AWS CloudFormation テンプレートによって次の Amazon CloudWatch ダッシュボードとアラームが自動的に作成されます。

- **DNACDashboard（VA_Instance_MonitoringBoard）**：このダッシュボードには、Cisco DNA Center インスタンスの `CPUUtilization`、`NetworkIn`、`NetworkOut`、`DiskReadOps`、および `DiskWriteOps` に関するモニタリング情報が表示されます。
- **DnacCPUAlarm**：Cisco DNA Center インスタンスの CPU 使用率が 80% 以上になると、このアラームがトリガーされます。CPU 使用率のデフォルトのしきい値は 80% です。
- **DnacSystemStatusAlarm**：Cisco DNA Center インスタンスのシステムステータスチェックに失敗すると、リカバリプロセスが開始されます。システムステータスチェックのデフォルトのしきい値は 0 です。

始める前に

- 必要なすべてのコンポーネントを使用して AWS 環境がセットアップされていること。詳細については、AWS CloudFormation 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。
- VPN トンネルが稼働していること。

手順

ステップ 1 ダウンロードするファイルに応じて、次のいずれかを実行します。

- 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。

  `DNA_Center_VA_InstanceLaunch_CFT-1.7.0.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。

  `DNA_Center_VA_InstanceLaunch_CFT-1.6.0.tar.gz`

両方の TAR ファイルに、Cisco DNA Center VA インスタンスの作成に使用する AWS CloudFormation テンプレートが含まれています。AWS CloudFormation テンプレートには複数の AMI が含まれており、それぞれの AMI には特定のリージョンに基づいて異なる AMI ID が割り当てられています。リージョンに適した AMI ID を使用してください。

リージョン	Cisco DNA Center AMI ID
ap-northeast-1（東京）	ami-0e15eb31bcb994472
ap-northeast-2（ソウル）	ami-043e1b9f3ccace4b2
ap-south-1（ムンバイ）	ami-0bbdbd7bcc1445c5f
ap-southeast-1（シンガポール）	ami-0c365aa4cfb5121a9
ap-southeast-2（シドニー）	ami-0d2d9e5ebb58de8f7
ca-central-1（カナダ）	ami-0485cfdbda5244c6e
eu-central-1（フランクフルト）	ami-0677a8e229a930434
eu-south-1（ミラノ）	ami-091f667a02427854d
eu-west-1（アイルランド）	ami-0a8a59b277dff9306
eu-west-2（ロンドン）	ami-0cf5912937286b42e
eu-west-3（パリ）	ami-0b12cfdd092ef754e

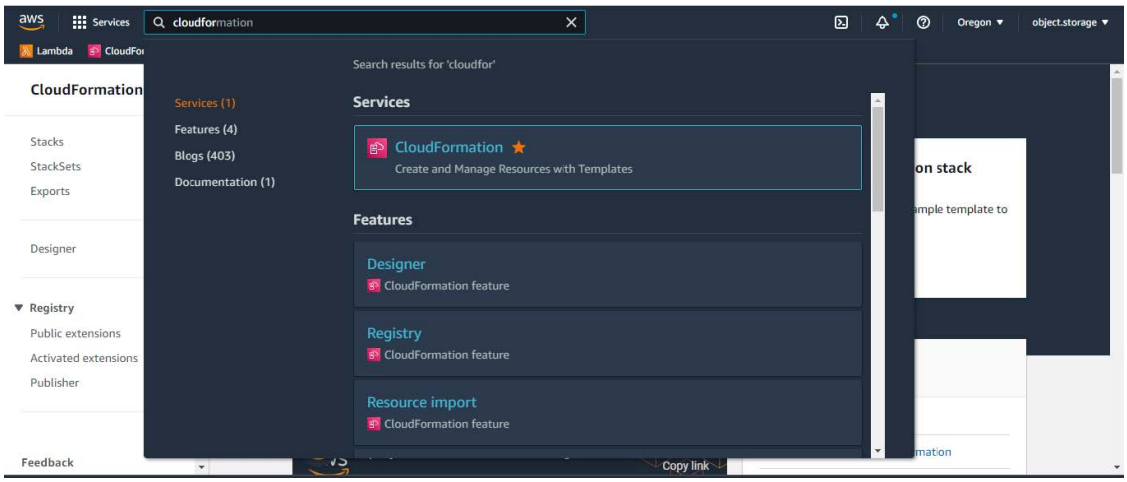
リージョン	Cisco DNA Center AMI ID
us-east-1（バージニア）	ami-08ad555593196c1de
us-east-2（オハイオ）	ami-0c52ce38eb8974728
us-west-1（北カリフォルニア）	ami-0b83a898072e12970
us-west-2（オレゴン）	ami-02b6cd5eee1f3b521

ステップ 2 TAR ファイルがシスコから正規に配布されていることを確認します。手順の詳細については、Cisco DNA Center VA の TAR ファイルの確認を参照してください。

ステップ 3 AWS コンソールにログインします。

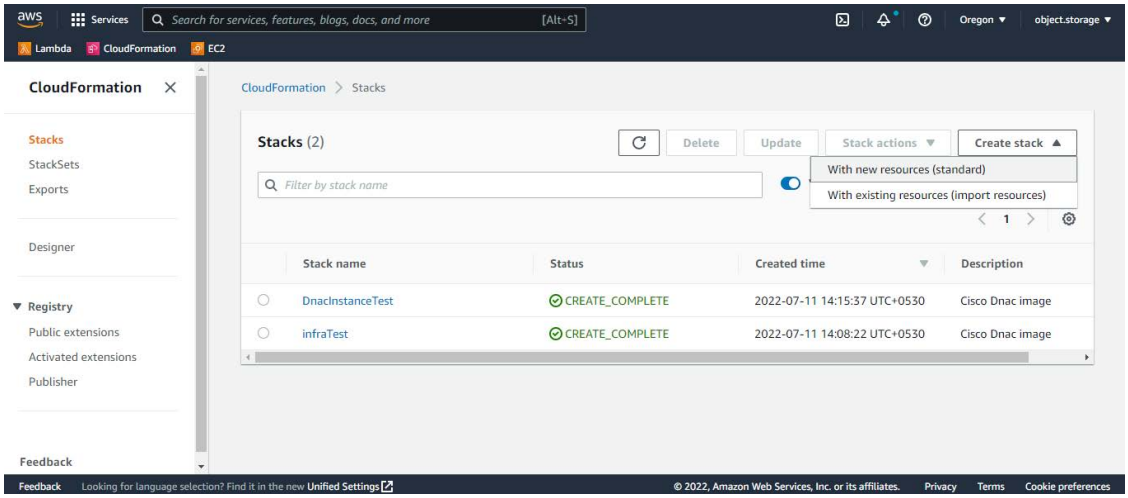
AWS コンソールが表示されます。

ステップ 4 検索バーに「**cloudformation**」と入力します。

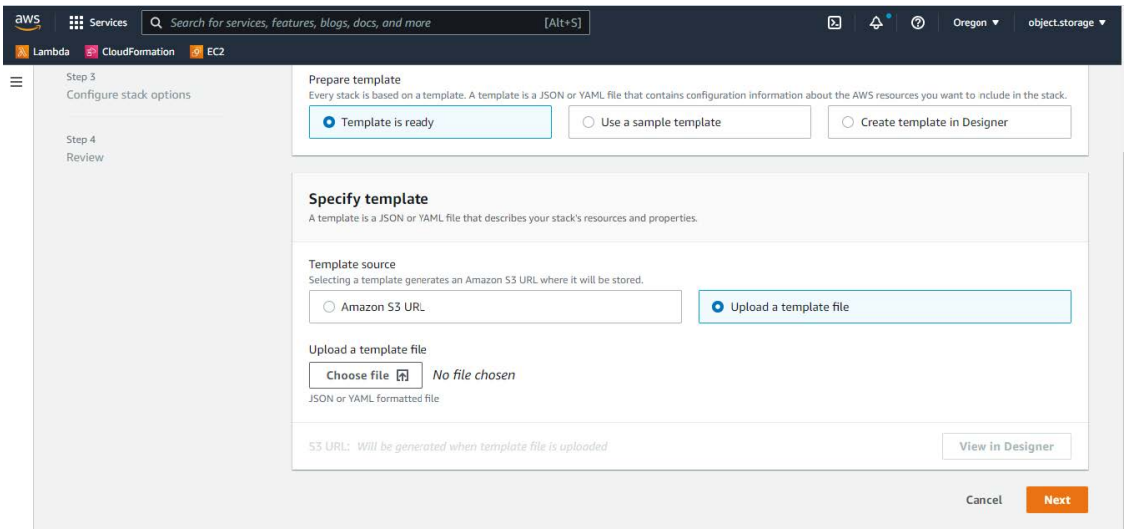


ステップ 5 ドロップダウンメニューから [CloudFormation] を選択します。

ステップ 6 [Create stack] をクリックして [With new resources (standard)] を選択します。



ステップ 7 [Specify template] で、[Upload a template file] を選択し、ステップ 1 でダウンロードした AWS CloudFormation テンプレートを選択します。



ステップ 8 スタック名を入力し、次のパラメータを確認します。

- **EC2 インスタンスの設定**
  - [Environment Name]：一意の環境名を割り当てます。

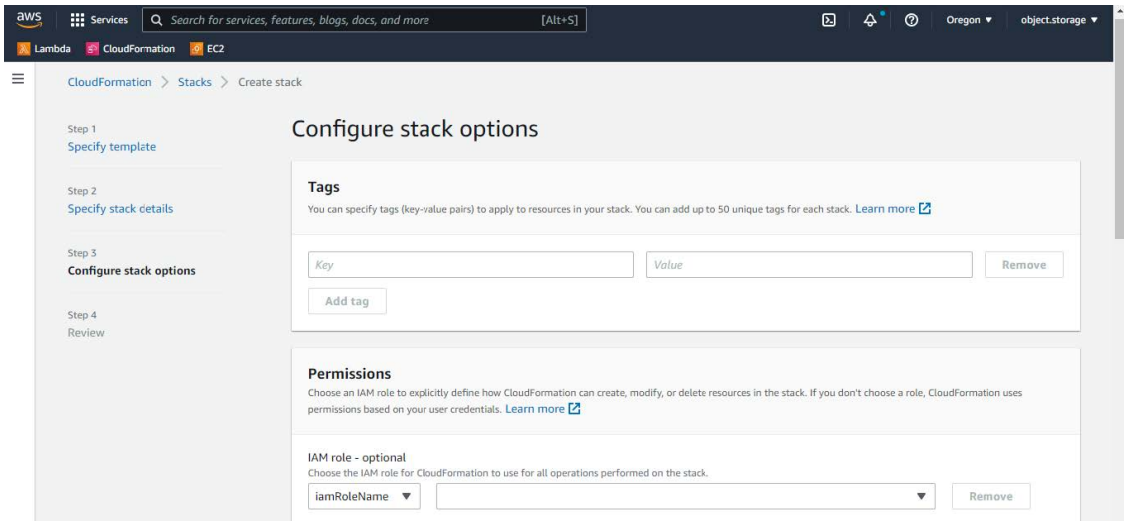
    環境名は、展開を区別するために使用され、AWS リソース名の前に追加されます。以前の展開と同じ環境名を使用すると、現在の展開でエラーが発生します。
  - [Private Subnet ID]：Cisco DNA Center で使用する VPC サブネットを入力します。
  - [Security Group]：展開する Cisco DNA Center VA に割り当てるセキュリティグループを入力します。
  - [Keypair]：展開する Cisco DNA Center VA の CLI へのアクセスに使用する SSH キーペアを入力します。
- **Cisco DNA Center の設定**：次の情報を入力します。
  - [DnacInstanceIP]：Cisco DNA Center の IP アドレス。
  - [DnacNetmask]：Cisco DNA Center のネットマスク。
  - [DnacGateway]：Cisco DNA Center のゲートウェイアドレス。
  - [DnacDnsServer]：エンタープライズ DNS サーバー。
  - [DnacPassword]：Cisco DNA Center のパスワード。

（注） Cisco DNA Center のパスワードを使用して、AWS EC2 シリアルコンソールから Cisco DNA Center VA CLI にアクセスできます。パスワードは、以下のルールに従う必要があります。

- タブまたは改行を省略する
- 8 文字以上にする
- 次のうち少なくとも 3 つのカテゴリの文字を含める
  - 小文字（a ～ z）
  - 大文字（A ～ Z）
  - 数字（0 ～ 9）
  - 特殊文字（! や # など）

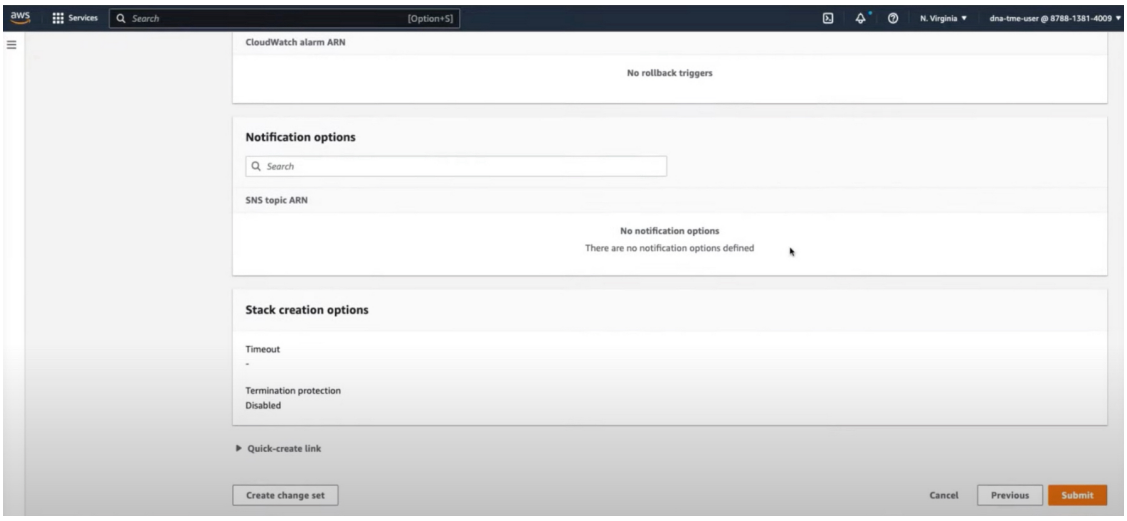
- [DnacFQDN]：Cisco DNA Center の FQDN。
- [DnacHttpsProxy]：（オプション）エンタープライズ HTTPS プロキシ。
- [DnacHttpsProxyUsername]：（オプション）HTTPS プロキシのユーザー名。
- [DnacHttpsProxyPassword]：（オプション）HTTPS プロキシのパスワード。

ステップ 9 （任意）[Next] をクリックして、スタックオプションを設定します。



ステップ 10 [Next] をクリックして、スタック情報を確認します。

ステップ 11 設定に問題なければ、[Submit] をクリックして終了します。



スタックの作成プロセスには、通常 45 ～ 60 分かかります。

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 CloudFormation 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。