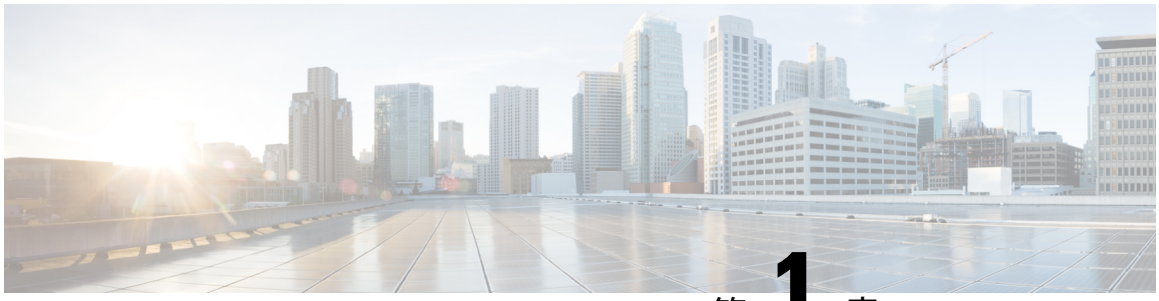
AWS での Cisco DNA Center 2.3.5 導入ガイド

初版：2023 年 8 月 2 日

最終更新：2023 年 12 月 7 日

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/

目 次



第 1 章

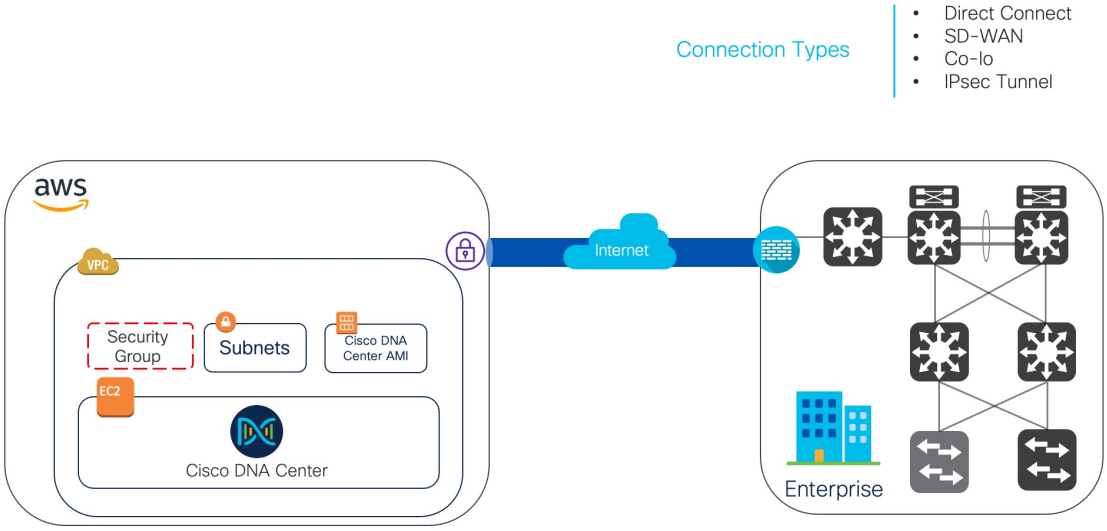
AWS での Cisco DNA Center のスタートアップガイド

AWS 上の Cisco DNA Center の概要

（注） Cisco DNA Center は Catalyst Center にブランド変更され、Cisco DNA Center VA 起動パッドは Cisco Global Launchpad にブランド変更されました。ブランド変更プロセスの進行中、以前の名前とブランド変更後の名前がさまざまな販促アイテムに表示されます。名前が異なっていても、Cisco DNA Center と Catalyst Center は同じ製品を指し、Cisco DNA Center VA 起動パッドと Cisco Global Launchpad は同じ製品を指します。

Cisco DNA Center には直感的な集中管理機能が備わっているため、ご使用のネットワーク環境全体でポリシーを素早く簡単に設計、プロビジョニングして適用できます。Cisco DNA Center のユーザーインターフェイスはネットワークを隅々まで見える化し、ネットワークインサイトを活用してネットワークパフォーマンスの最適化ならびにユーザーエクスペリエンスとアプリケーション エクスペリエンスの最適化を実現します。

Amazon Web Services（AWS） 上の Cisco DNA Center は、Cisco DNA Center アプライアンス環境で提供されるすべての機能を備えています。Cisco DNA Center 上の AWS は、AWS クラウド環境で実行され、クラウドからネットワークを管理します。



展開の概要

AWS に Cisco DNA Center を展開するには、次の 3 つの方法があります。

- **自動展開**：Cisco Global Launchpad が AWS 上の Cisco DNA Center を設定します。自動展開は、クラウドインフラストラクチャに必要なサービスとコンポーネントを作成する場合に便利です。たとえば、仮想プライベートクラウド（VPC）、サブネット、セキュリティグループ、IPSec VPN トンネル、およびゲートウェイの作成に役立ちます。このとき、Cisco DNA Center Amazon Machine Image（AMI）が、指定された設定でサブネット、トランジットゲートウェイ、その他の重要なリソース（モニタリング用の Amazon CloudWatch、ステートストレージ用の Amazon DynamoDB、セキュリティグループなど）とともに、Amazon Elastic Compute Cloud（EC2）として新しい VPC に展開されます。

  Cisco Global Launchpad を使用した 2 つの方法が用意されています。Cisco Global Launchpad をダウンロードしてローカルマシンにインストールすることも、シスコがホストする Cisco Global Launchpad にアクセスすることもできます。どちらの方法を使用するかに関係なく、Cisco Global Launchpad には Cisco DNA Center Virtual Appliance（VA）のインストールと管理に必要なツールが備わっています。

  詳細については、Cisco Global Launchpad 1.7 を使用した展開 （13 ページ）またはCisco DNA Center VA 起動パッド 1.6 を使用した展開 （57 ページ）を参照してください。

- **AWS CloudFormation を使用した手動展開**：AWS で Cisco DNA Center AMI を手動展開します。Cisco Global Launchpad 展開ツールを使用する代わりに、AWS に搭載された展開ツールである AWS CloudFormation を使用します。Cisco DNA Center の手動設定では、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 VA を展開します。詳細については、AWS CloudFormation を使用した展開 （101 ページ）を参照してください。

- **AWS Marketplace を使用した手動展開**：AWS で Cisco DNA Center AMI を手動展開します。Cisco Global Launchpad 展開ツールを使用する代わりに、AWS 内のオンライン ソフトウェア ストアである AWS Marketplace を使用します。Amazon EC2 起動コンソールを使用してソフトウェアを起動します。次に AWS インフラストラクチャの作成、VPN トンネルの確立、および Cisco DNA Center VA の設定を実行して Cisco DNA Center を手動展開します。この展開方式では、EC2 を介した起動のみがサポートされていることに注意してください。他の 2 つの起動オプション（Web サイトから起動およびサービスカタログにコピー）はサポートされていません。詳細については、AWS Marketplace を使用した展開（115 ページ）を参照してください。

AWS の管理経験がほとんどない場合は、Cisco Global Launchpad を使用した自動方式を使用すると、最も合理的なインストール支援プロセスが提供されます。AWS の管理に精通しており、既存の VPC がある場合は、手動方式によりインストールプロセスの別の選択肢が提供されます。

次の表を参照して、それぞれの方法のメリットとデメリットを考慮してください。

Cisco Global Launchpad を使用した自動展開	AWS CloudFormation を使用した手動展開	AWS Marketplace を使用した手動展開
• VPC、サブネット、セキュリティグループ、IPSec VPN トンネル、ゲートウェイなどの AWS インフラストラクチャを AWS アカウントで作成するプロセスがサポートされます。 • Cisco DNA Center のインストールが自動的に完了します。 • VA へのアクセスが提供されます。 • VA の管理性を備えています。 • 展開時間は約 1 ～ 1 時間半です。 • 自動アラートは、Amazon CloudWatch ダッシュボードに送信されます。 • 自動クラウドバックアップまたはエンタープライズ ネットワーク ファイル システム（NFS）バックアップを選択できます。 • AWS での Cisco DNA Center の自動設定ワークフローに手動で変更を加えると、自動展開と競合する可能性があります。	• AWS で Cisco DNA Center VA を作成するために AWS CloudFormation ファイルが必要です。 • ユーザーが VPC、サブネット、セキュリティグループなどの AWS インフラストラクチャを AWS アカウントで作成します。 • ユーザーが VPN トンネルを確立します。 • ユーザーが Cisco DNA Center を展開します。 • 展開には数時間から数日かかります。 • AWS コンソールを使用してモニタリングを手動で設定する必要があります。 • バックアップには、オンプレミス NFS のみを設定できます。	• AWS で Cisco DNA Center VA を作成するために AWS CloudFormation ファイルは必要ありません。 • ユーザーが VPC、サブネット、セキュリティグループなどの AWS インフラストラクチャを AWS アカウントで作成します。 • ユーザーが VPN トンネルを確立します。 • ユーザーが Cisco DNA Center を展開します。 • 展開には数時間から数日かかります。 • AWS コンソールを使用してモニタリングを手動で設定する必要があります。 • バックアップには、オンプレミス NFS のみを設定できます。

展開の準備

AWS で Cisco DNA Center を展開する前に、ネットワーク要件、サポートされている AWS 上の Cisco DNA Center の統合機能を実装する必要があるかどうか、および AWS 上の Cisco DNA Center へのアクセス方法を検討してください。

また、ダウンロードした Cisco DNA Center VA TAR ファイルが正規の Cisco TAR ファイルであることを確認することを強く推奨します。Cisco DNA Center VA の TAR ファイルの確認 （8 ページ）を参照してください。

高可用性と AWS 上の Cisco DNA Center

AWS 上の Cisco DNA Center の高可用性（HA）環境は次のとおりです。

- 可用性ゾーン（AZ）内のシングルノードEC2 HAは、デフォルトで有効になっています。
- Cisco DNA Center の EC2 インスタンスがクラッシュした場合、AWS は同じ IP アドレスを持つ別のインスタンスを自動的に起動します。これにより、中断のない接続が確保され、重要なネットワーク運用の中断が最小限に抑えられます。

（注） Cisco Global Launchpad を使用して AWS で Cisco DNA Center を展開したときに、Cisco DNA Center の EC2 インスタンスがクラッシュした場合、AWS は同じ AZ 内の別のインスタンスを自動的に起動します。この場合、AWS は Cisco DNA Center に別の IP アドレスを割り当てることができます。

- エクスペリエンスと目標復旧時間（RTO）は、ベアメタル Cisco DNA Center アプライアンスの停電シーケンスと同様です。

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

AWS 上の Cisco ISE は AWS 上の Cisco DNA Center と統合できます。これらをクラウドで統合する際、次のガイドラインを遵守してください。

- AWS 上の Cisco ISE は、Cisco Global Launchpad で予約済みの VPC とは別の VPC に展開する必要があります。
- AWS 上の Cisco ISE の VPC は、AWS 上の Cisco DNA Center の VPC と同じリージョンに配置することも、別のリージョンに配置することもできます。
- 環境に応じて、VPC またはトランジットゲートウェイ（TGW）のピアリングを使用できます。
- VPC または TGW ピアリングを使用して AWS 上の Cisco DNA Center と AWS 上の Cisco ISE を接続するには、VPC または TGW ピアリングルートテーブルと、 または AWS または AWS 上の Cisco ISE 上の Cisco DNA Center に関連付けられたサブネットに割り当てられているルートテーブルに、必要なルーティングエントリを追加します。
- Cisco Global Launchpad は、Cisco Global Launchpad によって作成されたエンティティに対するアウトオブバンド変更を検出できません。こうしたエンティティには、VPC、VPN、

TGW、TGW アタッチメント、サブネット、ルーティングなどが含まれます。たとえば、Cisco Global Launchpad によって作成された VA ポッドを別のアプリケーションから削除または変更できますが、この変更が Cisco Global Launchpad で認識されない可能性があります。

基本的なアクセスルールに加えて、クラウド内の Cisco ISE インスタンスにセキュリティグループを割り当てるために、次のインバウンドポートを許可する必要があります。

- AWS 上の Cisco DNA Center と AWS 上の Cisco ISE の統合では、TCP ポート 9060 および 8910 を許可します。
- Radius 認証では、UDP ポート 1812、1813、およびその他の有効なポートを許可します。
- TACACS を介したデバイス管理では、TCP ポート 49 を許可します。
- Datagram Transport Layer Security（DTLS）や Radius 認可変更（CoA）などを AWS 上の Cisco ISE に追加設定する場合は、対応するポートを許可します。

AWS 上の Cisco DNA Center にアクセスする際の注意事項

Cisco DNA Center の仮想インスタンスを作成すると、Cisco DNA Center の GUI および CLI を使用してアクセスできます。

重要 Cisco DNA Center の GUI および CLI には、パブリックネットワークからではなく、エンタープライズネットワークを介してのみアクセスできます。自動展開方式では、Cisco Global Launchpad によって確実に Cisco DNA Center がエンタープライズ イントラネットからのみアクセス可能になります。手動展開方式では、セキュリティ上の理由から、パブリックイントラネット上で Cisco DNA Center にアクセスできないようにする必要があります。

Cisco DNA Center の GUI にアクセスする際の注意事項

Cisco DNA Center GUI にアクセスするには、次の手順を実行します。

- サポートされているブラウザを使用してください。サポートされるブラウザの最新リストについては、『*Release Notes for Cisco Global Launchpad*』[英語] を参照してください。
- 次の形式でブラウザに Cisco DNA Center インスタンスの IP アドレスを入力します。

  http://*ip-address***/dna/home**

  次に例を示します。

  `http://192.0.2.27/dna/home`

- 初回ログイン時に次のログイン情報を使用します。

  ユーザ名：**admin**

  パスワード：**maglev1@3**

（注） Cisco DNA Center に初めてログインすると、このパスワードを変更するよう求められます。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）

Cisco DNA Center の CLI にアクセスする際の注意事項

Cisco DNA Center CLI にアクセスするには、次の手順を実行します。

- Cisco DNA Center の展開方式に応じた IP アドレスとキーを使用します。
  - Cisco Global Launchpad を使用して Cisco DNA Center を展開した場合は、Cisco Global Launchpad によって提供された IP アドレスとキーを使用します。
  - AWS を使用して Cisco DNA Center を手動で展開した場合は、AWS によって提供された IP アドレスとキーを使用します。

（注） キーは .pem ファイルである必要があります。キーファイルが key.cer ファイル形式でダウンロードされている場合は、ファイル名を key.pem に変更する必要があります。

- key.pem ファイルのアクセス権限を手動で 400 に変更します。アクセス権限を変更するには、Linux の **chmod** コマンドを使用します。次に例を示します。

  chmod 400 key.pem

- Cisco DNA Center の CLI にアクセスするには、次の Linux コマンドを使用します。

  ssh -i key.pem maglev@*ip-address* -p 2222

  次に例を示します。

  ```
  ssh -i key.pem maglev@192.0.2.27 -p 2222
  ```

Cisco DNA Center VA の TAR ファイルの確認

Cisco DNA Center VA を展開する前に、ダウンロードした TAR ファイルが正規の Cisco TAR ファイルであるかを確認することを強く推奨します。

始める前に

Cisco DNA Center VA の TAR ファイルは、必ず Cisco ソフトウェアダウンロードサイトからダウンロードする必要があります。

手順

ステップ 1 シスコの指定した場所から署名検証用のシスコ公開キー（cisco_image_verification_key.pub）をダウンロードします。

ステップ 2 シスコが指定した場所から TAR ファイルのセキュア ハッシュ アルゴリズム（SHA512）チェックサムファイルをダウンロードします。

ステップ 3 TAR ファイルの署名ファイル（.sig）をシスコサポートから電子メールで入手するか、セキュアなシスコの Web サイト（利用可能な場合）からダウンロードします。

ステップ 4 （任意） SHA 検証を実行して、不完全なダウンロードによって TAR ファイルが破損していないかを確認します。

オペレーティングシステムに応じて、次のコマンドのいずれかを実行します。

- Linux システムの場合：**sha512sum** <tar-file-filename>
- Mac システムの場合：**shasum -a 512** <tar-file-filename>

Microsoft Windows には組み込みのチェックサムユーティリティはありませんが、certutil ツールを使用できます。

```
certutil -hashfile <filename> sha256
```

次に例を示します。

```
certutil -hashfile D:\Customers\FINALIZE.BIN sha256
```

Windowsでは、Windows PowerShell を使用してダイジェストを生成することもできます。次に例を示します。

```
PS C:\Users\Administrator> Get-FileHash -Path D:\Customers\FINALIZE.BIN
Algorithm Hash Path
SHA256 B84B6FFD898A370A605476AC7EC94429B445312A5EEDB96166370E99F2838CB5
D:\Customers\FINALIZE.BIN
```

コマンドの出力とダウンロードしたSHA512チェックサムファイルを比較します。コマンド出力が一致しない場合は、TARファイルを再度ダウンロードし、もう一度適切なコマンドを実行します。それでも出力が一致しない場合は、シスコサポートにお問い合わせください。

ステップ 5 署名を確認し、TAR ファイルが正規のシスコ製であることを確認します。

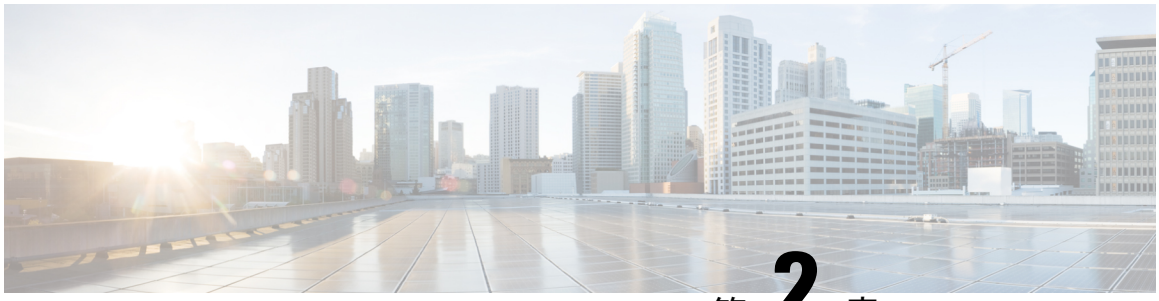
openssl dgst -sha512 -verify cisco_image_verification_key.pub -signature <signature-filename> <tar-file-filename>

（注） このコマンドはMacとLinuxの両方の環境で動作します。Windowsの場合、OpenSSLがまだインストールされていなければ、ダウンロードしてインストールする必要があります（OpenSSL Downloads から入手可能）。

TAR ファイルが正規であれば、このコマンドを実行すると、「Verified OK」というメッセージが表示されます。このメッセージが表示されない場合は、TAR ファイルをインストールせず、シスコサポートにご連絡ください。

第 部

AWS での Cisco DNA Center 2.3.5.3 の展開



第 2 章

Cisco Global Launchpad 1.7 を使用した展開

自動展開メソッドを使用した AWS CloudFormation での Cisco DNA Center の展開

ユーザーは VPC、IPsec VPN トンネル、ゲートウェイ、サブネット、セキュリティグループなど、AWS アカウントで AWS インフラストラクチャを作成するために必要な詳細情報を Cisco Global Launchpad で指定します。これにより、Cisco Global Launchpad は、指定された設定どおりに Cisco DNA Center AMI を Amazon EC2 インスタンスとして個別の VPC に展開します。設定には、サブネット、トランジットゲートウェイのほかに、モニタリング用の AWS CloudFormation、ステートストレージ用の Amazon DynamoDB、セキュリティグループなどの重要なリソースが含まれます。

Cisco Global Launchpad を使用すると、VA にアクセスして管理することも、ユーザー設定を管理することも可能です。詳細については、『*Cisco Global Launchpad 1.7 Administrator Guide*』[英語] を参照してください。

自動展開ワークフロー

自動化されたメソッドを使用して 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。自動展開の前提条件 （14 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 （5 ページ）を参照してください。
3. Cisco Global Launchpad をインストールするか、シスコがホストする Cisco Global Launchpad にアクセスします。Cisco Global Launchpad のインストール （18 ページ）またはホステッド型 Cisco Global Launchpad へのアクセス （19 ページ）を参照してください。
4. Cisco DNA Center VA インスタンスに含める新しい VA ポッドを作成します。新しい VA ポッドの作成 （28 ページ）を参照してください。
5. （任意）優先するオンプレミス接続オプションとして既存の TGW と既存のアタッチメント（VPC など）を使用する場合は、AWS で TGW ルーティングテーブルを手動で設定し、既存のカスタマーゲートウェイ（CGW）にルーティング設定を追加する必要があります。既存のトランジットゲートウェイおよびカスタマーゲートウェイでルーティングを手動設定する （41 ページ）を参照してください。
6. Cisco DNA Center の新しいインスタンスを作成します。Cisco DNA Center VA の新規作成 （42 ページ）を参照してください。
7. （任意）必要に応じて、展開中に発生した問題をトラブルシュートします。展開のトラブルシューティング （48 ページ）を参照してください。
8. Cisco Global Launchpad を使用して Cisco DNA Center VA を管理します。『*Cisco Global Launchpad 1.7 Administrator Guide*』[英語] を参照してください。

自動展開の前提条件

Cisco Global Launchpad を使用して AWS で Cisco DNA Center の展開を開始する前に、次の要件が満たされていることを確認してください。

- プラットフォームに Docker Community Edition（CE） をインストールします。

  Cisco Global Launchpad は、Mac、Windows、および Linux プラットフォーム上の Docker CE をサポートしています。お使いのプラットフォーム固有の手順については、Docker の Web サイトに掲載されているドキュメントを参照してください。

- どの方法で Cisco Global Launchpad にアクセスして Cisco DNA Center VA を展開するかに関係なく、クラウド環境が次の仕様を満たしていることを確認してください。

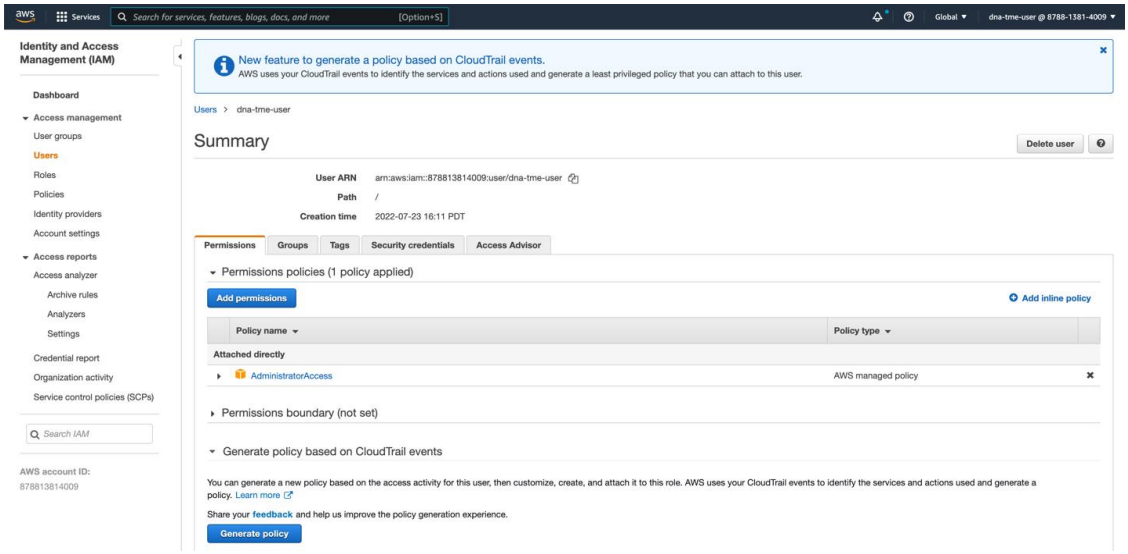
- **Cisco DNA Center インスタンス**：r5a.8xlarge、32 個の vCPU、256 GB の RAM、4 TB ストレージ

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 Release 1.7.0*』[英語]を参照してください。

- **バックアップインスタンス**：T3.micro、2 個の vCPU、500 GB のストレージ、1 GB の RAM

- 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。
- AWS アカウントが、リソースの独立性と分離を維持するためのサブアカウント（子アカウント）であること。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 で Cisco DNA Center 仮想アプライアンスのライセンス持ち込み（BYOL）に登録されていること。
- 管理者ユーザーの場合は、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）。

  管理者アクセスポリシーは、グループではなく、AWS アカウントに直接割り当てる必要があります。このアプリケーションは、グループポリシーを介して列挙を実行しません。そのため、管理者アクセス権限を持つグループに追加されたユーザーであっても、必要なインフラストラクチャを作成できません。



- サブユーザーの場合は、管理者によって CiscoDNACenter ユーザーグループに追加されている必要があります。

  管理者ユーザーが Cisco Global Launchpad に初めてログインすると、必要なすべてのポリシーが割り当てられた CiscoDNACenter ユーザーグループが AWS アカウント上に作成されます。管理者ユーザーがこのグループにサブユーザーを追加すると、サブユーザーが Cisco Global Launchpad にログインできるようになります。

  CiscoDNACenter ユーザーグループには、次のポリシーが割り当てられています。

  - AmazonDynamoDBFullAccess
  - IAMReadOnlyAccess
  - AmazonEC2FullAccess
  - AWSCloudFormationFullAccess
  - AWSLambda_FullAccess
  - CloudWatchFullAccess
  - ServiceQuotasFullAccess
  - AmazonEventBridgeFullAccess
  - service-role/AWS_ConfigRole
  - AmazonS3FullAccess
  - ClientVPNServiceRolePolicy（バージョン：2012-10-17）

    このポリシーでは、次のルールが許可されます。

    - ec2:CreateNetworkInterface
    - ec2:CreateNetworkInterfacePermission
    - ec2:DescribeSecurityGroups
    - ec2:DescribeVpcs
    - ec2:DescribeSubnets
    - ec2:DescribeInternetGateways
    - ec2:ModifyNetworkInterfaceAttribute
    - ec2:DeleteNetworkInterface
    - ec2:DescribeAccountAttributes
    - ds:AuthorizeApplication
    - ds:DescribeDirectories
    - ds:GetDirectoryLimits
    - ds:UnauthorizeApplication
    - logs:DescribeLogStreams

- logs:CreateLogStream
- logs:PutLogEvents
- logs:DescribeLogGroups
- acm:GetCertificate
- acm:DescribeCertificate
- iam:GetSAMLProvider
- lambda:GetFunctionConfiguration

• ConfigPermission（バージョン：2012-10-17、SID：VisualEditor0）

このポリシーでは、次のルールが許可されます。

- config:Get
- config:*
- config:*ConfigurationRecorder
- config:Describe*
- config:Deliver*
- config:List*
- config:Select*
- tag:GetResources
- tag:GetTagKeys
- cloudtrail:DescribeTrails
- cloudtrail:GetTrailStatus
- cloudtrail:LookupEvents
- config:PutConfigRule
- config:DeleteConfigRule
- config:DeleteEvaluationResults

• PassRole（バージョン：2012-10-17、SID：VisualEditor0）

このポリシーでは、次のルールが許可されます。

- iam:GetRole
- iam:PassRole

Cisco Global Launchpad のインストール

この手順では、サーバーおよびクライアント アプリケーションの Docker コンテナを使用して Cisco Global Launchpad をインストールする方法を示します。

始める前に

お使いのマシンに Docker CE がインストールされていることを確認してください。詳細については、自動展開の前提条件 （14 ページ）を参照してください。

手順

ステップ 1 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。

- `Launchpad-desktop-client-1.7.0.tar.gz`
- `Launchpad-desktop-server-1.7.0.tar.gz`

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 （8 ページ）を参照してください。

ステップ 3 ダウンロードしたファイルから Docker イメージを読み込みます。

```
docker load < Launchpad-desktop-client-1.7.0.tar.gz
```

```
docker load < Launchpad-desktop-server-1.7.0.tar.gz
```

ステップ 4 **docker images** コマンドを使用して、リポジトリ内の Docker イメージのリストを表示し、サーバーおよびクライアントアプリケーションの最新コピーがあることを確認します。ファイルには、[TAG] 列に [1.7] から始まる番号が表示されます。

次に例を示します。

```
$ docker images
```

```
REPOSITORY                                                                TAG                 IMAGE ID            CREATED             SIZE
466518672524.dkr.ecr.us-west-2.amazonaws.com/val/valaunchpad-server               1.7.1               854a1630d3a7        3 hours ago         546MB
466518672524.dkr.ecr.us-west-2.amazonaws.com/platform-ui/valaunchpad-client-docker   1.7.1               63ff53f197c9        5 hours ago         1.98GB
```

ステップ 5 サーバーアプリケーションを実行します。

```
docker run -d -p <server-port-number>:8080 -e DEBUG=true --name server
<server_image_id>
```

次に例を示します。

```
$ docker run -d -p 9090:8080 -e DEBUG=true --name server f87ff30d4c6a
```

ステップ 6 クライアント アプリケーションを実行します。

```
docker run -d -p <client-port-number>:80 -e CHOKIDAR_USEPOLLING=true -e
REACT_APP_API_URL=http://localhost:<server-port-number> --name client
<client_image_id>
```

次に例を示します。

```
$ docker run -d -p 90:80 -e CHOKIDAR_USEPOLLING=true -e
REACT_APP_API_URL=http://localhost:9090 --name client dd50d550aa7c
```

（注） 公開されているサーバーのポート番号と REACT_APP_API_URL のポート番号が同じであることを確認します。ステップ 5 とステップ 6 では、両方の例でポート番号 9090 が使用されています。

ステップ 7 **docker ps -a** コマンドを使用して、サーバーとクライアントのアプリケーションが実行されていることを確認します。[STATUS] 列にアプリケーションが稼働中であることが示されている必要があります。

次に例を示します。

```
$ docker ps -a
```

```
CONTAINER ID   IMAGE                                                                                  COMMAND                  CREATED              STATUS              PORTS                    NAMES
ad1b7f7ee6ea   466518672524.dkr.ecr.us-west-2.amazonaws.com/val/valaunchpad-server:1.7.1               "/usr/bin/dumb-init …"   About a minute ago   Up About a minute   0.0.0.0:9494->8080/tcp   server
a6eb2e93f57a   466518672524.dkr.ecr.us-west-2.amazonaws.com/platform-ui/valaunchpad-client-docker:1.7.1   "docker-entrypoint.s…"   2 minutes ago        Up 2 minutes        0.0.0.0:94->80/tcp       client
```

（注） サーバーまたはクライアントアプリケーションの実行中に問題が発生した場合は、Docker エラーのトラブルシュート （48 ページ）を参照してください。

ステップ 8 次の形式で URL を入力して、サーバーアプリケーションにアクセスできることを確認します。

http://<localhost>**:**<server-port-number>**/api/valaunchpad/aws/v1/api-docs/**

次に例を示します。

http://192.0.2.2:9090/api/valaunchpad/aws/v1/api-docs/

Cisco DNA Center VA に使用されているアプリケーション プログラミング インターフェイス（API）がウィンドウに表示されます。

ステップ 9 次の形式で URL を入力して、クライアント アプリケーションにアクセスできることを確認します。

http://<localhost>**:**<client-port-number>**/valaunchpad**

次に例を示します。

http://192.0.2.1:90/valaunchpad

Cisco Global Launchpad ログインウィンドウが表示されます。

（注） クライアントおよびサーバーアプリケーションでアーティファクトが読み込まれるため、Cisco Global Launchpad ログインウィンドウの読み込みに数分かかることがあります。

ホステッド型 Cisco Global Launchpad へのアクセス

Cisco DNA ポータル で Cisco Global Launchpad にアクセスできます。

Cisco DNA ポータル を初めて使用する場合は、シスコアカウントと Cisco DNA ポータル アカウントを作成する必要があります。その後、Cisco DNA ポータル にログインして Cisco Global Launchpad にアクセスできます。

Cisco DNA ポータル を以前から使用し、シスコアカウントと Cisco DNA ポータル アカウントをお持ちの場合は、Cisco DNA ポータル に直接ログインして Cisco Global Launchpad にアクセスできます。

シスコアカウントの作成

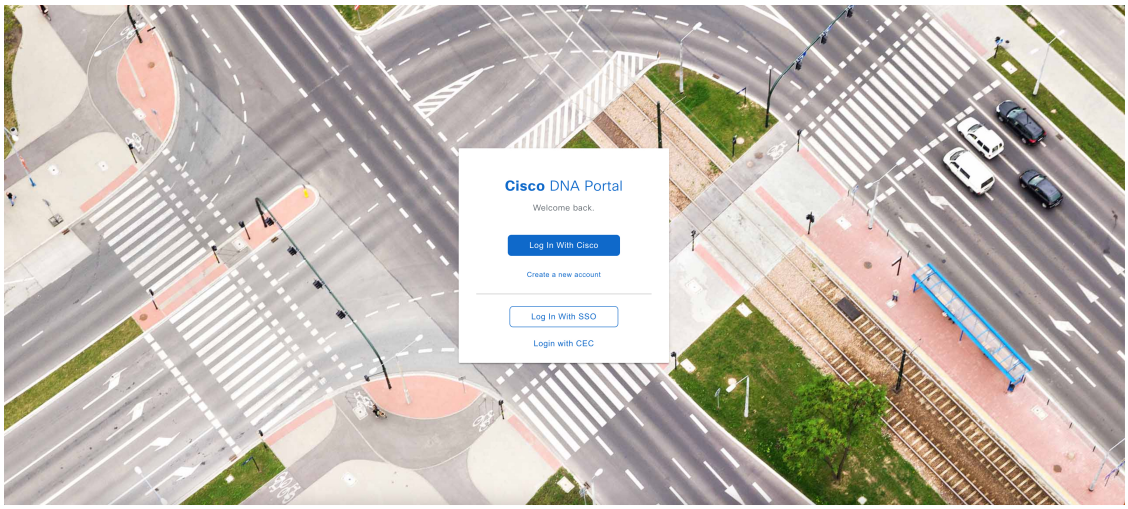
Cisco DNA ポータル を介して Cisco Global Launchpad にアクセスするには、最初にシスコアカウントを作成する必要があります。

手順

ステップ 1 ブラウザで次のように入力します。

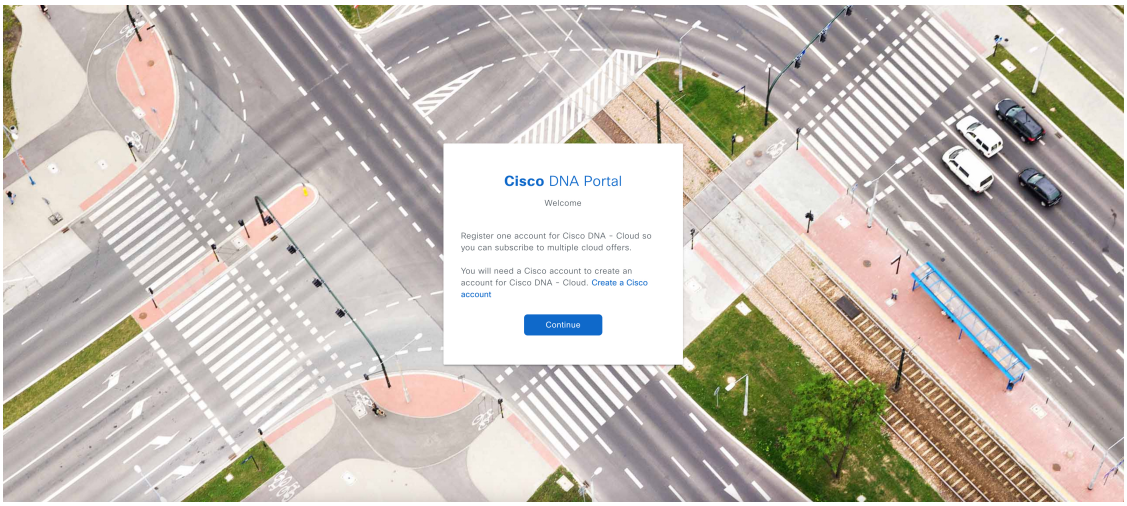
`dna.cisco.com`

Cisco DNA ポータル ログインウィンドウが表示されます。

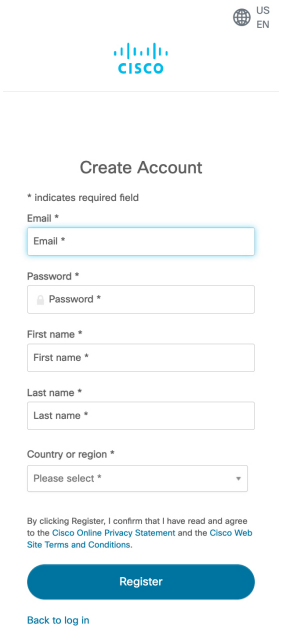


ステップ 2 [Create a new account] をクリックします。

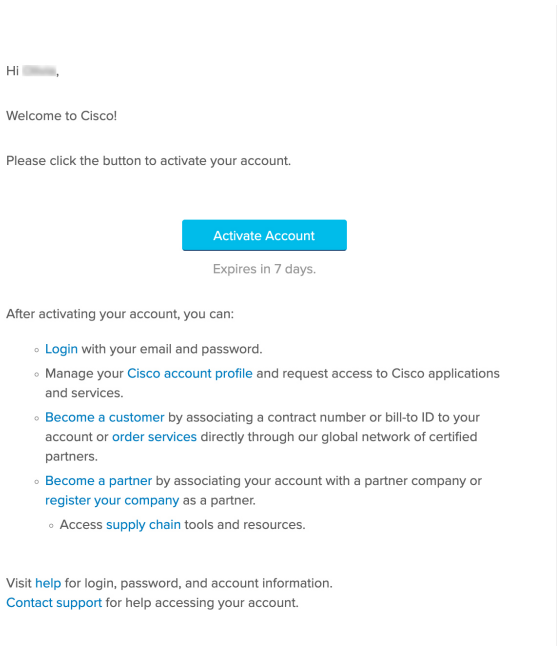
ステップ 3 **Cisco DNA ポータル** の [Welcome] ウィンドウで [Create a Cisco account] をクリックします。



ステップ 4 [Create Account] ウィンドウで必要なフィールドに入力し、[Register] をクリックします。



ステップ 5 アカウントの登録に使用した電子メールに移動し、[Activate Account] をクリックして、アカウントを確認します。


Hi [redacted],

Welcome to Cisco!

Please click the button to activate your account.

Activate Account

Expires in 7 days.

After activating your account, you can:

- Login with your email and password.
- Manage your Cisco account profile and request access to Cisco applications and services.
- Become a customer by associating a contract number or bill-to ID to your account or order services directly through our global network of certified partners.
- Become a partner by associating your account with a partner company or register your company as a partner.
  - Access supply chain tools and resources.

Visit help for login, password, and account information.
Contact support for help accessing your account.

Cisco DNA ポータル アカウントの作成

Cisco DNA ポータル を介して Cisco Global Launchpad にアクセスするには、Cisco DNA ポータル アカウントを作成する必要があります。

始める前に

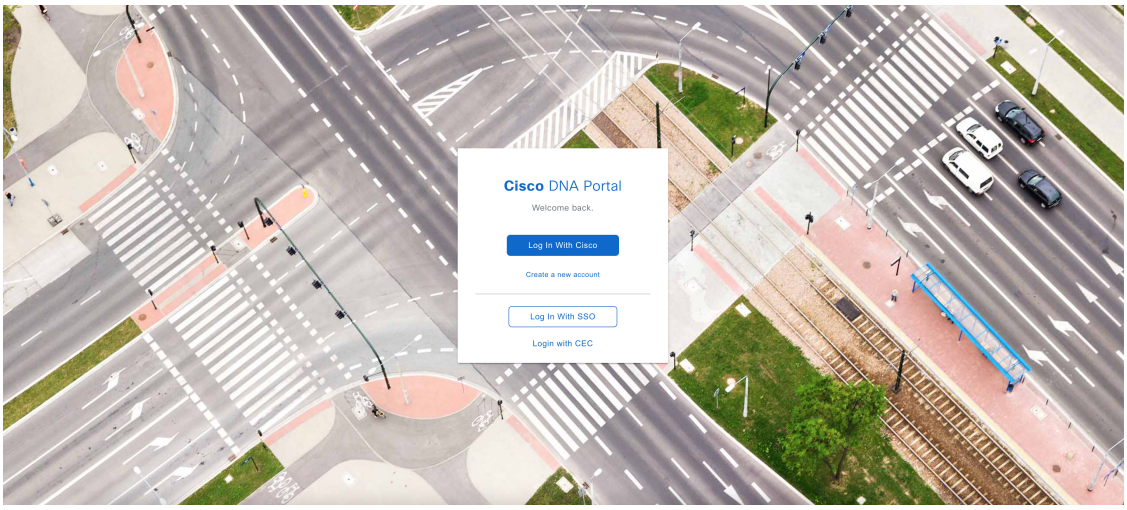
シスコアカウントがあることを確認します。詳細については、シスコアカウントの作成 （20 ページ）を参照してください。

手順

ステップ 1 ブラウザで次のように入力します。

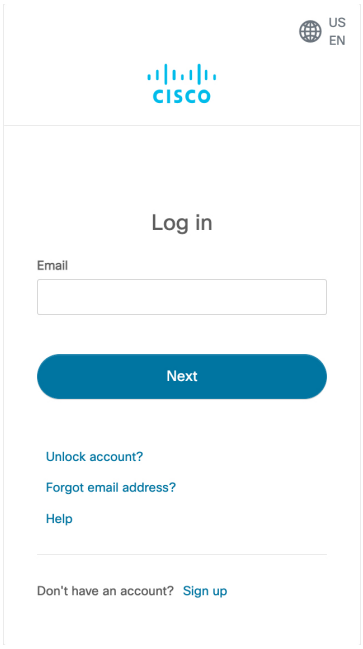
dna.cisco.com

Cisco DNA ポータル ログインウィンドウが表示されます。

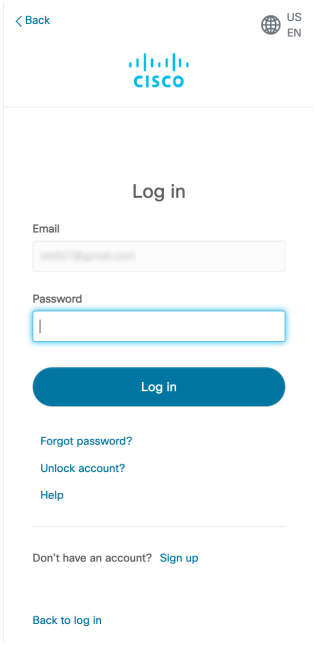


ステップ 2 [Log In With Cisco] をクリックします。

ステップ 3 [Email] フィールドにシスコアカウントの電子メールを入力し、[Next] をクリックします。

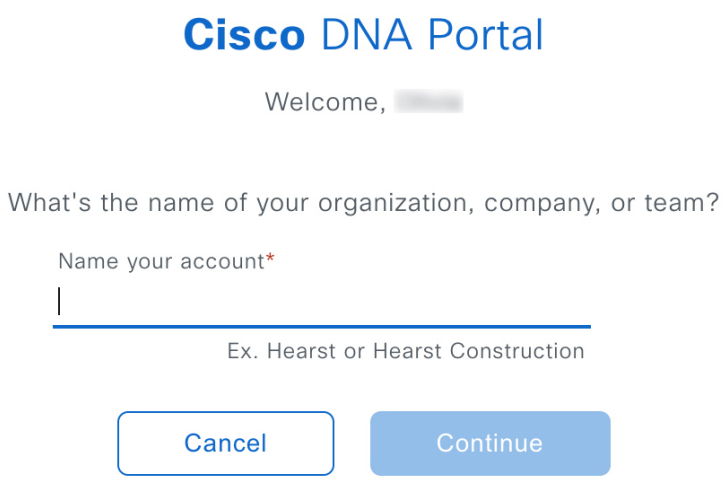


ステップ 4 [Password] フィールドにシスコアカウントのパスワードを入力します。



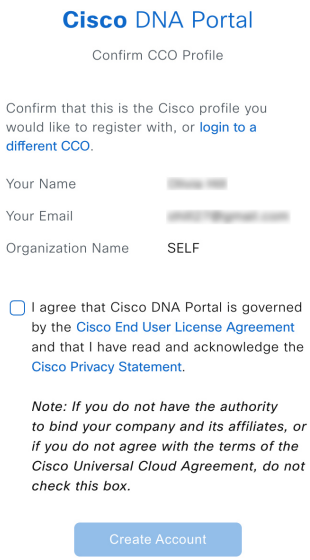
ステップ 5 [Log in] をクリックします。

ステップ 6 **Cisco DNA ポータル** の [Welcome] ウィンドウの [Name your account] フィールドに組織名またはチーム名を入力します。 [Continue] をクリックします。

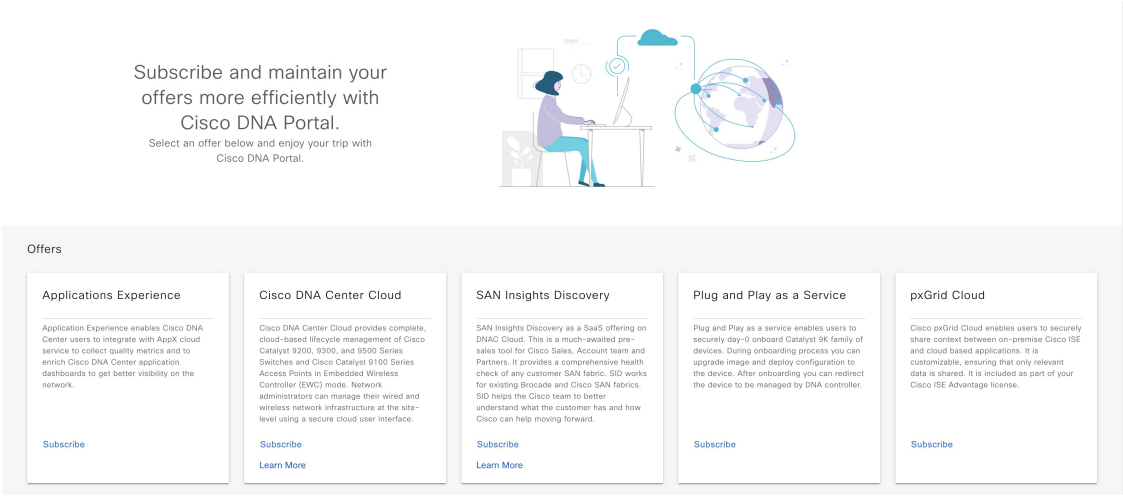


ステップ 7 **Cisco DNA ポータル** の [Confirm CCO Profile] ウィンドウで次の手順を実行します。

a) 表示される情報が正しいことを確認します。
b) 条件を読んで確認し、同意する場合はチェックボックスをオンにします。
c) [Create Account] をクリックします。



アカウントが正常に作成されると、**Cisco DNA ポータル** ホームページが表示されます。



シスコアカウントでの Cisco DNA ポータル へのログイン

Cisco DNA ポータル を介して Cisco Global Launchpad にアクセスするには、Cisco DNA ポータル にログインする必要があります。

始める前に

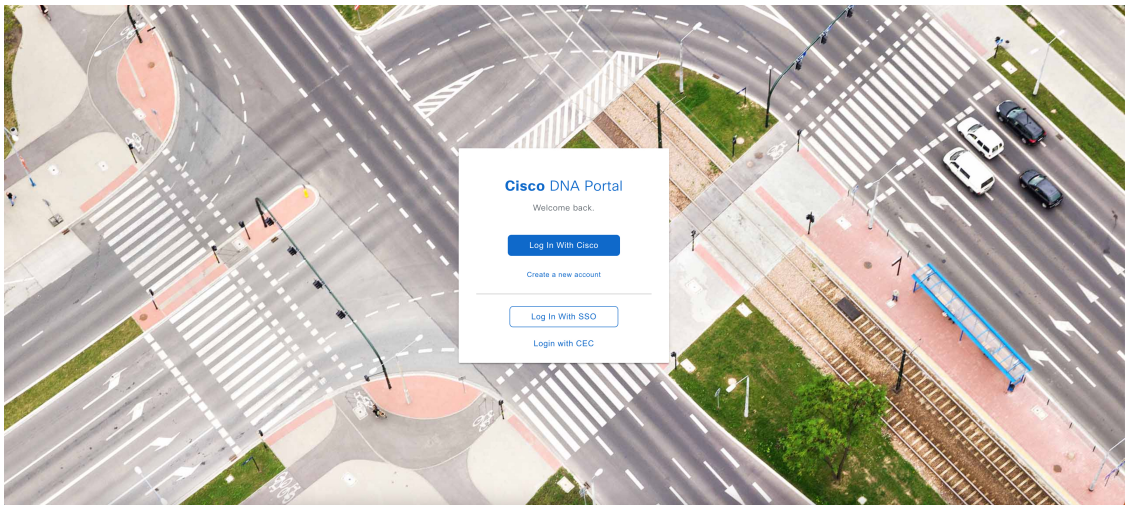
シスコアカウントと Cisco DNA ポータル アカウントがあることを確認します。詳細については、シスコアカウントの作成 （20 ページ）およびCisco DNA ポータル アカウントの作成 （22 ページ）を参照してください。

手順

ステップ 1 ブラウザで次のように入力します。

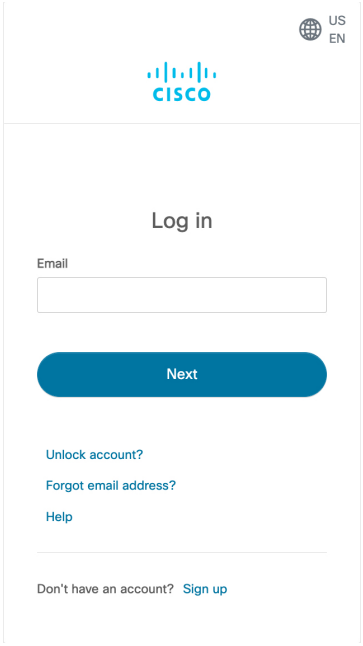
`dna.cisco.com`

Cisco DNA ポータル ログインウィンドウが表示されます。

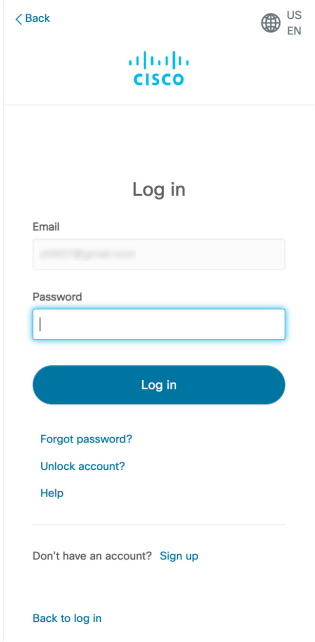


ステップ 2 [Log In With Cisco] をクリックします。

ステップ 3 [Email] フィールドにシスコアカウントの電子メールを入力し、[Next] をクリックします。



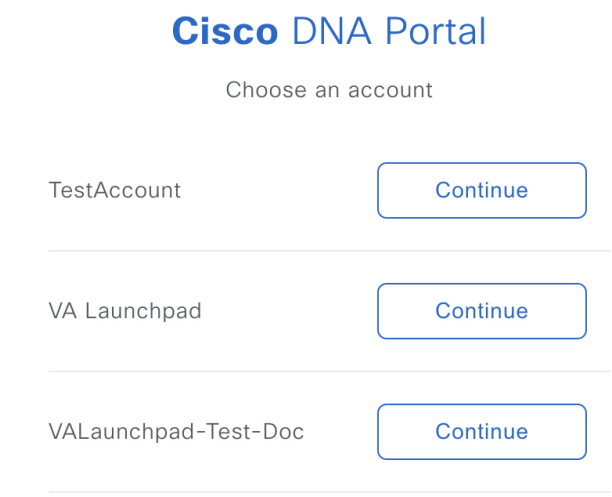
ステップ 4 [Password] フィールドにシスコアカウントのパスワードを入力します。



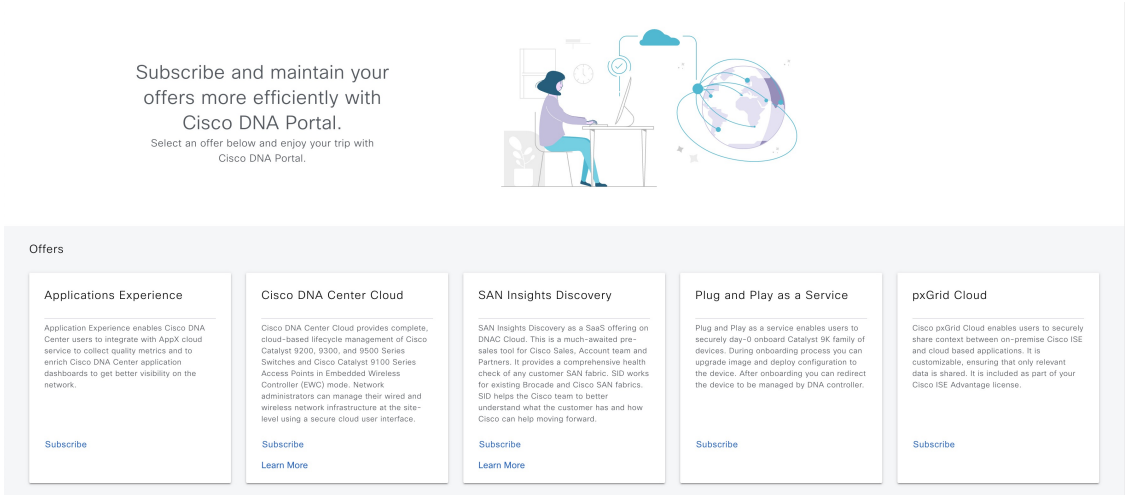
ステップ 5 [Log in] をクリックします。

Cisco DNA ポータル アカウントが 1 つしかない場合は、**Cisco DNA ポータル** ホームページが表示されます。

ステップ 6 （任意）複数の Cisco DNA ポータルアカウントがある場合は、アカウントの横にある [Continue] ボタンをクリックして、ログインするアカウントを選択します。



Cisco DNA ポータル ホームページが表示されます。



新しい VA ポッドの作成

VA ポッドは、Cisco DNA Center VA 向けの AWS ホスティング環境です。このホスティング環境には、Cisco DNA Center VA EC2 インスタンス、Amazon Elastic Block Storage（EBS）、バックアップ NFS サーバー、セキュリティグループ、ルーティングテーブル、Amazon CloudWatch ログ、Amazon Simple Notification Service（SNS）、VPN ゲートウェイ（VPN GW）、TGW などの AWS リソースが含まれます。

Cisco Global Launchpad を使用して、複数の VA ポッド（Cisco DNA Center VA ごとに 1 つの VA ポッド）を作成できます。

（注）

- AWS スーパー管理者ユーザーは、各リージョンで作成できる VA ポッド数の上限を設定できます。Cisco Global Launchpad 以外のリソースに使用される VPC もこの数に含まれます。たとえば、AWS アカウントに設定された VPC の上限が 5 つで、そのうち 2 つが使用中の場合、選択したリージョンでさらに作成できる VA ポッドは 3 つまでです。
- 一部の手順では、すべてのリソースが正しく設定された場合にのみ次の手順に進むことができます。すべてのリソースが正しく設定されていない場合、[Proceed] ボタンは無効になります。すべてのリソースが正しく設定されているにもかかわらず、[Proceed] ボタンが無効になっている場合は、リソースがまだロードされているため、数秒間お待ちください。すべての設定が完了すると、ボタンが有効になります。
- Cisco Global Launchpad を新しいリリースに更新した場合、以前の Cisco Global Launchpad リリースにダウングレードした場合、または VA ポッドが配置されているリージョン設定を更新した場合、VA ポッドの設定は変更されません。

  たとえば、Cisco Global Launchpad リリース 1.7.0 で VA ポッドを作成した場合、バックアップパスワードは、バックアップインスタンスのスタック名とバックアップサーバーの IP アドレスを組み合わせたものになります。リリース 1.6.0 などの以前のリリースでこの VA ポッドにアクセスする場合、バックアップパスワードは変更されません。

ここでは、新しい VA ポッドを作成する方法を順を追って説明します。

始める前に

この手順を実行するには、AWS アカウントに管理者アクセス権限が必要です。詳細については、自動展開の前提条件 （14 ページ）を参照してください。

手順

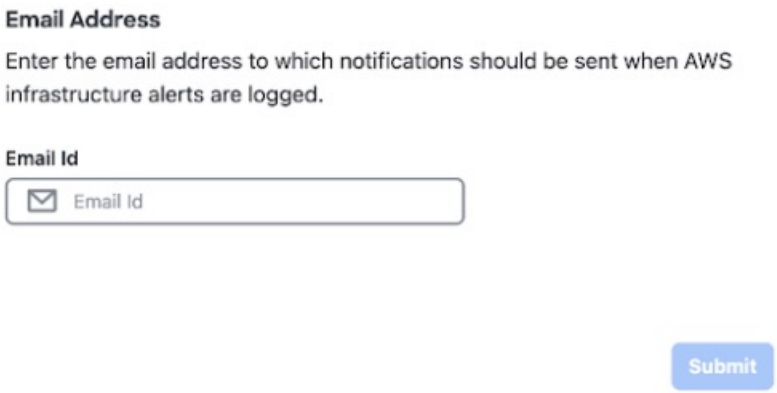
ステップ 1 次のいずれかの方法を使用して、Cisco Global Launchpad にログインします。

- [IAM Login]：この方法では、ユーザーロールを使用してユーザーアクセス権限を定義します。Cisco Global Launchpad は、企業が必要とする場合に、任意の追加認証形式としての多要素認証（MFA）をサポートします。詳細については、『*Cisco Global Launchpad 1.7 Administrator Guide*』の「Log In to Cisco Global Launchpad Using IAM」[英語] を参照してください。
- [Federated Login]：この方法では、1 つのアイデンティティを使用して、他のオペレータが管理するネットワークまたはアプリケーションにアクセスします。詳細については、『*Cisco Global Launchpad1.7 Administrator Guide*』の「Generate Federated User Credentials Using saml2aws」または「Generate Federated User Credentials Using AWS CLI」[英語] を参照してください。

アクセスキー ID とシークレットアクセスキーを取得する方法については、AWS の Web サイトに掲載されている *AWS Tools for PowerShell* ユーザーガイド [英語] の 「AWS Account and Access Keys」を参照してください。

ログインエラーが発生した場合は、エラーを解決して再度ログインする必要があります。詳細については、ログインエラーのトラブルシュート （49 ページ）を参照してください。

ステップ 2 初めてログインする管理者ユーザーの場合は、[Email ID] フィールドに電子メールアドレスを入力し、[Submit] をクリックします。サブユーザーの場合は、ステップ 3 に進みます。



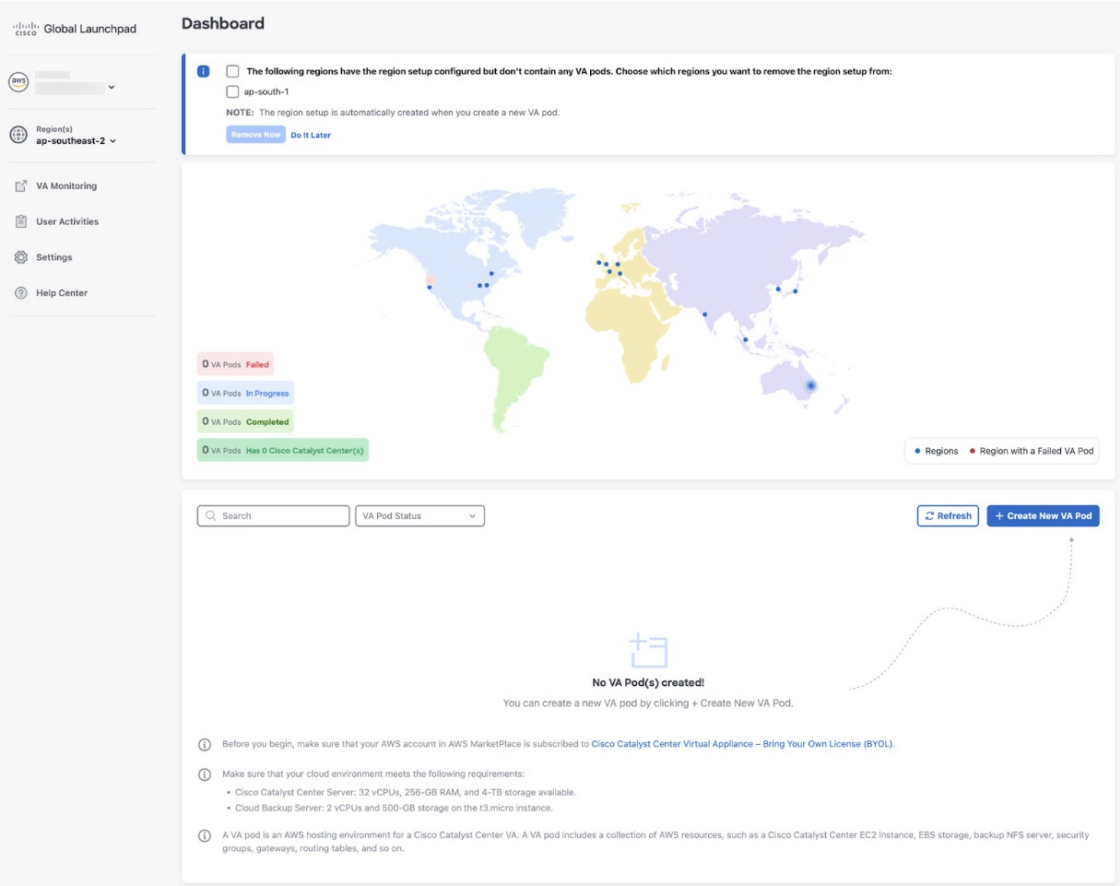
アマゾンSNSに登録して、展開されたリソース、変更、およびリソースの過剰使用に関するアラートを受信できます。さらに、Amazon CloudWatch が Cisco Global Launchpad の異常な動作を検出した場合に通知するようにアラームを設定できます。さらに、AWS Config は設定されたリソースを評価し、結果の監査ログも送信します。詳細については、『*Cisco Global Launchpad 1.7 Administrator Guide*』の「Subscribe to the アマゾンSNS Email Subscription」と「View Amazon CloudWatch Alarms」[英語] を参照してください。

電子メールを入力すると、いくつかのプロセスが実行されます。

- 必要なすべてのポリシーが割り当てられた CiscoDNACenter ユーザーグループが AWS アカウント上に作成されます。管理者ユーザーがこのグループにサブユーザーを追加すると、サブユーザーが Cisco Global Launchpad にログインできるようになります。
- Amazon S3 バケットは、展開の状態を保存するために自動的に作成されます。グローバルでも各リージョンでも、AWS アカウントから S3 バケットや他のバケットを削除しないことを推奨します。バケットを削除すると、Cisco Global Launchpad 展開ワークフローに影響を与える可能性があります。
- リージョンに初めてログインすると、Cisco Global Launchpad によって AWS で複数のリソースが作成されます。リージョンが以前に有効だったかどうかによって、このプロセスは時間がかかる場合があります。プロセスが完了するまで、新しい VA ポッドは作成できません。この間、「**Setting up the initial region configuration. This might take a couple of minutes.（初期リージョンを設定中です。この処理には数分かかる場合があります。）**」というメッセージが表示されます。

正常にログインすると、[**Dashboard**] ペインが表示されます。

（注） リージョンの設定を更新するように求められた場合は、プロンプトに従って更新を完了します。詳細については、『*Cisco Global Launchpad1.7 Administrator Guide*』の「Update a Region Setup」[英語] を参照してください。



ステップ 3 [+ Create New VA Pod] をクリックします。

ステップ 4 [Select a Region] ダイアログボックスで次の手順を実行して、新しい VA ポッドを作成するリージョンを選択します。

1. [Region] ドロップダウンリストから、リージョンを選択します。

   左側のナビゲーションウィンドウの [Region] ドロップダウンリストから 1 つのリージョンをすでに選択している場合は、そのリージョンが自動的に選択されます。

   （注） リージョンの設定を更新するように求められた場合は、プロンプトに従って更新を完了します。詳細については、『*Cisco Global Launchpad1.7 Administrator Guide*』の「Update a Region Setup」[英語] を参照してください。

2. **[Next]** をクリックします。

ステップ 5 次の手順を実行して、VPC、プライベートサブネット、ルーティングテーブル、セキュリティグループ、仮想ゲートウェイ、CGW を含む AWS インフラストラクチャを設定します。

a) [VA Pod Environmental Details] フィールドで、次のフィールドを設定します。

- [VA Pod Name]：新しい VA ポッドに名前を割り当てます。次の制約事項に注意してください。
  - 名前はリージョン内で一意である必要があります（これは複数のリージョンで同じ名前を使用できることを意味します）。
  - 最大 12 文字までの名前を指定できます。
  - 名前には、文字（A－Z）、数字（0－9）、およびダッシュ（-）を含めることができます。
- [Availability Zone]：このドロップダウンリストをクリックして、選択したリージョン内の分離された場所である可用性ゾーンを選択します。
- [AWS VPC CIDR]：AWS リソースの起動に使用する一意の VPC サブネットを入力します。次の注意事項に従ってください。
  - 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。
  - このサブネットは、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。

b) [Transit Gateway (TGW)] で、次のいずれかのオプションを選択します。

- [VPN GW]：VA ポッドが 1 つあり、VPN ゲートウェイを使用する場合は、このオプションを選択します。VPN GW は、サイト間 VPN 接続の Amazon 側の VPN エンドポイントです。1 つの VPC にのみ接続できます。
- [New VPN GW + New TGW]：複数の VA ポッドまたは VPC があり、複数の VPC とオンプレミスネットワークを相互接続するトランジットハブとして TGW を使用する場合は、このオプションを選択します。また、TGW をサイト間 VPN 接続の Amazon 側の VPN エンドポイントとして使用することもできます。

  （注） リージョンごとに 1 つの TGW のみを作成できます。

- [Existing TGW]：新しい VA ポッドの作成に使用する既存の TGW がある場合は、このオプションを選択してから、次のいずれかのオプションを選択します。
  - [New VPN GW]：既存の TGW に新しい VPN ゲートウェイを作成する場合は、このオプションを選択します。
  - [Existing Attachment]：既存の VPN または直接接続アタッチメントを使用する場合は、このオプションを選択します。[Select Attachment ID] ドロップダウンリストから、アタッチメント ID を選択します。

    このオプションを選択する場合は、既存の TGW および CGW のルーティングも設定する必要があります。詳細については、既存のトランジットゲートウェイお

よびカスタマーゲートウェイでルーティングを手動設定する （41 ページ）を参照してください。

c) 次のいずれかを実行します。

- 優先する接続オプションとして [Existing TGW] と [Existing Attachments] を選択した場合は、ステップ 5 に進みます。
- [VPN GW]、[New VPN GW + New TGW]、または [Existing TGW + New VPN GW] を選択した場合は、次の VPN 詳細を入力します。
  - [CGW (Enterprise Firewall/Router)]：AWS VPN ゲートウェイとの IPSec トンネルを形成するためのエンタープライズ ファイアウォールまたはルータの IP アドレスを入力します。
  - [VPN Vendor]：ドロップダウンリストから VPN ベンダーを選択します。

    [Barracudo]、[Sophos]、[Vyatta]、および [Zyxel] は、サポートされていない VPN ベンダーです。詳細については、VA ポッド設定エラーのトラブルシュート （50 ページ）を参照してください。
  - [Platform]：ドロップダウンリストからプラットフォームを選択します。
  - [Software]：ドロップダウンリストからソフトウェアを選択します。

d) [Customer Profile] のサイズは、デフォルト設定の [Medium] のままにします。

カスタマープロファイルのサイズは、Cisco DNA Center VA インスタンスとバックアップインスタンスの両方に適用されます。[Medium] を指定すると、インスタンスの構成は次のようになります。

- [Cisco Catalyst Center Instance]：r5a.8xlarge、32 個の vCPU、256 GB RAM、4 TB ストレージ。

  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 Release 1.7.0*』[英語] を参照してください。

- **バックアップインスタンス**：T3.micro、2 個の vCPU、500 GB のストレージ、1 GB の RAM

e) [Backup Target] では、Cisco DNA Center のデータベースとファイルのバックアップ先として次のいずれかのオプションを選択します。

- [Enterprise Backup (NFS)]：バックアップをオンプレミスサーバーに保存する場合は、このオプションを選択します。

- [Cloud Backup (NFS)]：バックアップを AWS に保存する場合は、このオプションを選択します。

  次のバックアップの詳細をメモします。後でこの情報を使用して、クラウド バックアップ サーバーにログインします。

  - **SSH IPアドレス**：<BACKUP VM IP>
  - **SSH ポート**：22
  - **サーバーパス**：/var/dnac-backup/
  - **ユーザー名**：maglev
  - **パスワード**：<xxxx##########>

    バックアップサーバーのパスワードは動的に作成されます。パスワードは、バックアップインスタンスのスタック名の最初の 4 文字とバックアップサーバーの IP アドレス（ピリオドなし）で構成されます。

    たとえば、バックアップインスタンスのスタック名が DNAC-ABC-0123456789987 で、バックアップサーバーの IP アドレスが 10.0.0.1 の場合、バックアップサーバーのパスワードは DNAC10001 になります。

    （注）
    - バックアップインスタンスのスタック名は、[Cisco Catalyst Center Configuration In Progress] ウィンドウ（Cisco DNA Center VA の新規作成 （42 ページ） のステップ 9 を参照）または **[AWS Console]** > **[CloudFormation]** > **[Stacks]** ウィンドウで確認できます。
    - バックアップサーバーの IP アドレスは、[Cisco Catalyst Center Configuration In Progress] ウィンドウ（Cisco DNA Center VA の新規作成 （42 ページ） のステップ 9 を参照）または [View Catalyst Center] ペイン（『*Cisco Global Launchpad1.7 Administrator Guide*』の「View Cisco DNA Center VA Details」[英語] を参照）でも確認できます。

  - **パスフレーズ**：<Passphrase>

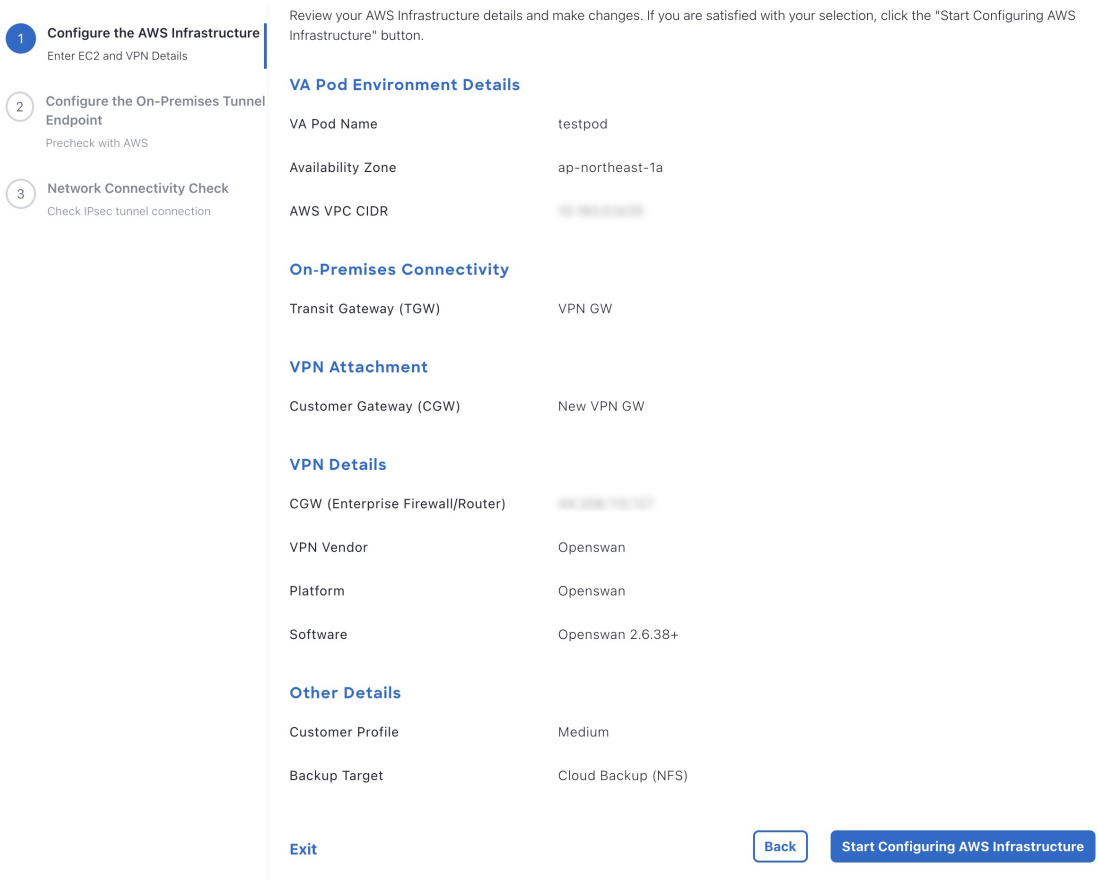
    パスフレーズは、バックアップのセキュリティの影響を受けやすいコンポーネントを暗号化するために使用されます。これらのセキュリティに影響を受けやすいコンポーネントには、証明書とクレデンシャルが含まれます。

    このパスフレーズは必須で、バックアップファイルを復元するときに入力を求められます。このパスフレーズがなければ、バックアップファイルは復元されません。

  - **オープンポート**：22、2049、873、111

f) [Next] をクリックします。

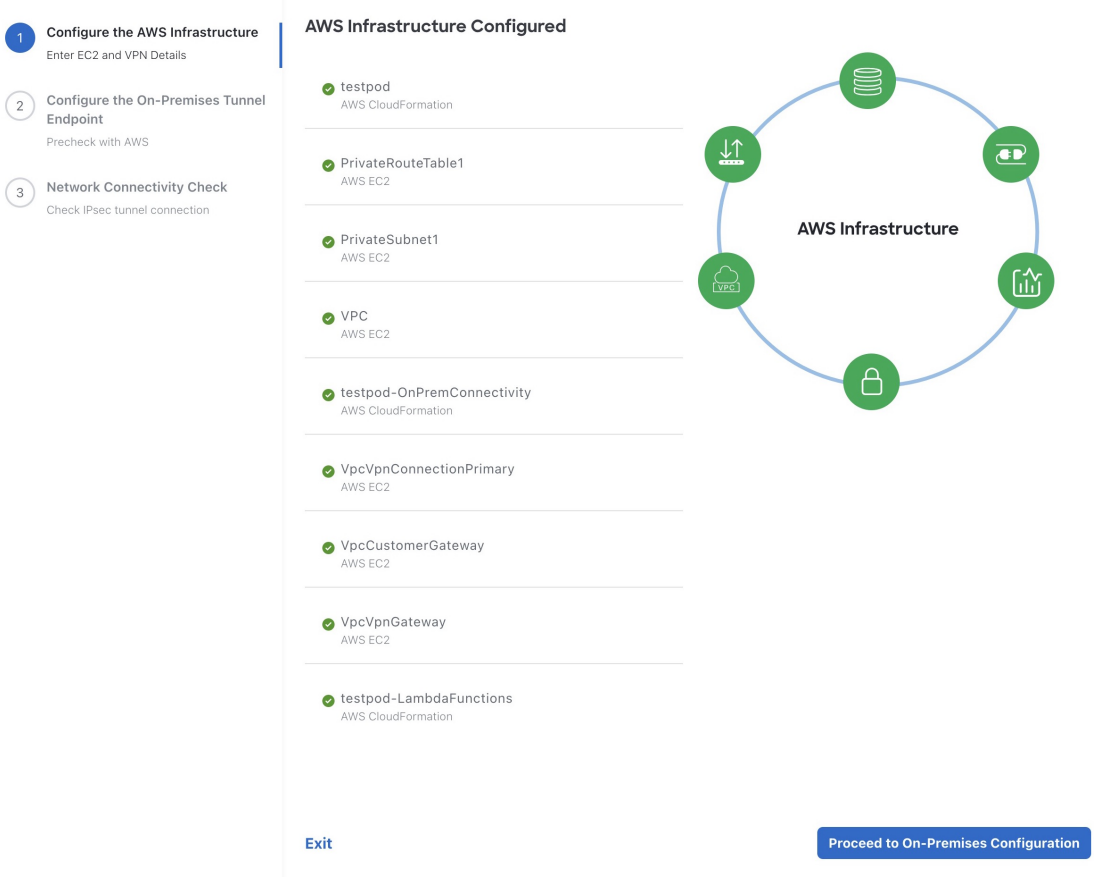
[Summary] ペインが表示されます。



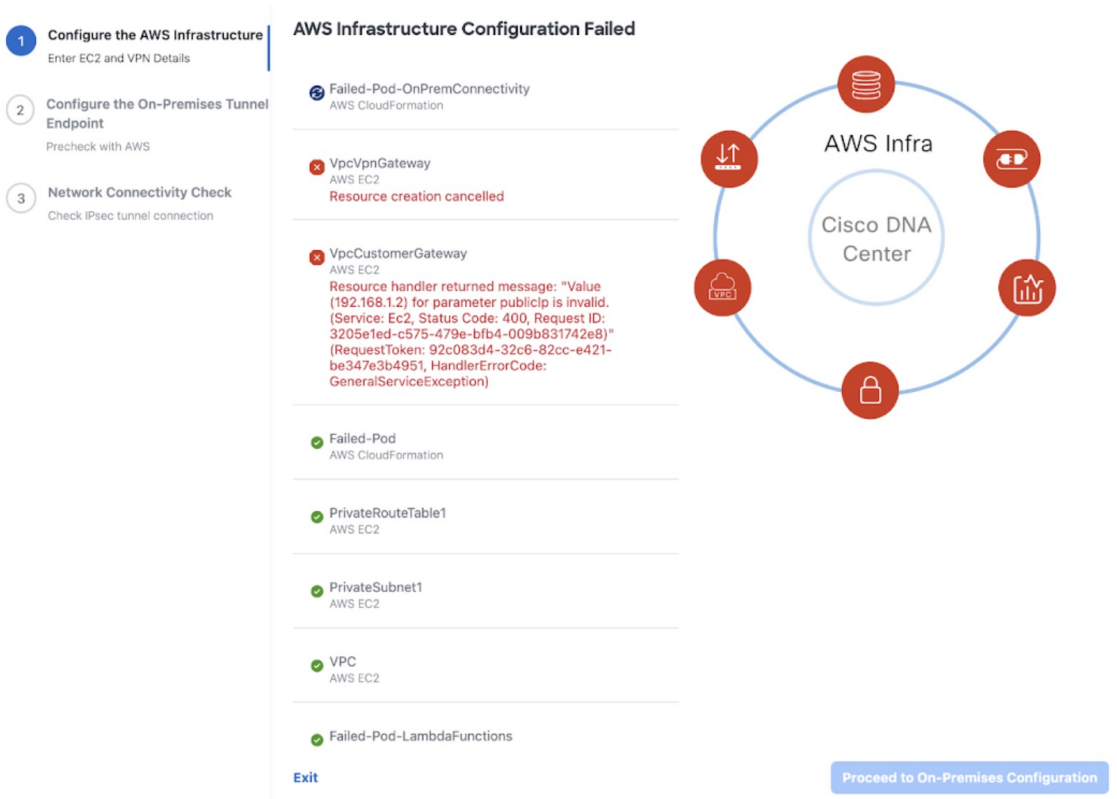
g) 環境と VPN の入力内容を確認します。問題がなければ、[Start Configuring AWS Infrastructure] をクリックします。

重要 設定が完了するまで約 20 分かかります。アプリケーションを終了したり、このウィンドウやタブを閉じたりしないでください。さもないと、設定が一時停止します。

h) AWS インフラストラクチャが正しく設定されると、[AWS Infrastructure Configured] ペインが表示されます。



AWS インフラストラクチャの設定に失敗した場合は、Cisco Global Launchpad を終了します。考えられる原因と解決策については、VA ポッド設定エラーのトラブルシュート （50 ページ）を参照してください。



ステップ 6 次の手順を実行して、オンプレミス構成ファイルをダウンロードします。

a) AWS インフラストラクチャが正しく設定されたら、[Proceed to On-Premises Configuration] をクリックします。

b) [Configure the On-Premises Tunnel Endpoint] ペインで、[Download Configuration File] をクリックします。このファイルをネットワーク管理者に転送して、オンプレミス側の IPSec トンネルを設定します。

ネットワーク管理者が IPSec トンネルを 1 つだけ設定していることを確認してください。

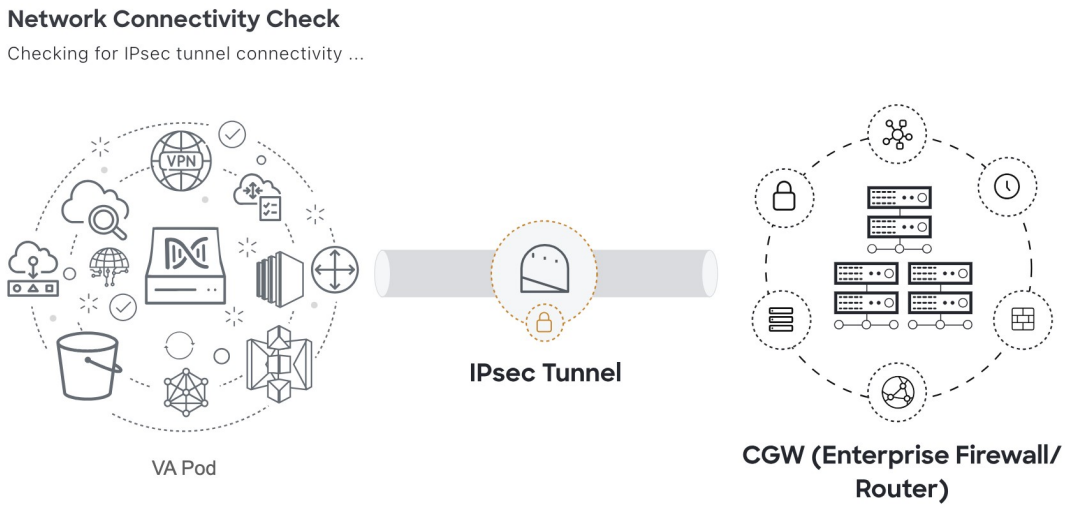
（注）
- ネットワーク管理者がこの構成ファイルに必要な変更を加えてからエンタープライズ ファイアウォールまたはルータに適用すると、IPSec トンネルを起動できます。

  提供されている構成ファイルを使用すると、AWS とエンタープライズルータまたはファイアウォールの間で 2 つのトンネルを起動できます。
- ほとんどの仮想プライベート ゲートウェイ ソリューションでは、1 つのトンネルが稼働し、もう 1 つのトンネルが停止しています。両方のトンネルを稼働すると、等コストマルチパス（ECMP）ネットワーキング機能を使用できます。ECMP 処理では、ファイアウォールまたはルータが等コストルートを使用して同じ宛先にトラフィックを送信できます。このとき、ルータまたはファイアウォールが ECMP をサポートしている必要があります。ECMP を使用しない場合は、1 つのトンネルを停止して手動でフェールオーバーするか、または IP SLA などのソリューションを使用して、フェールオーバーシナリオでトンネルを自動的に起動することを推奨します。

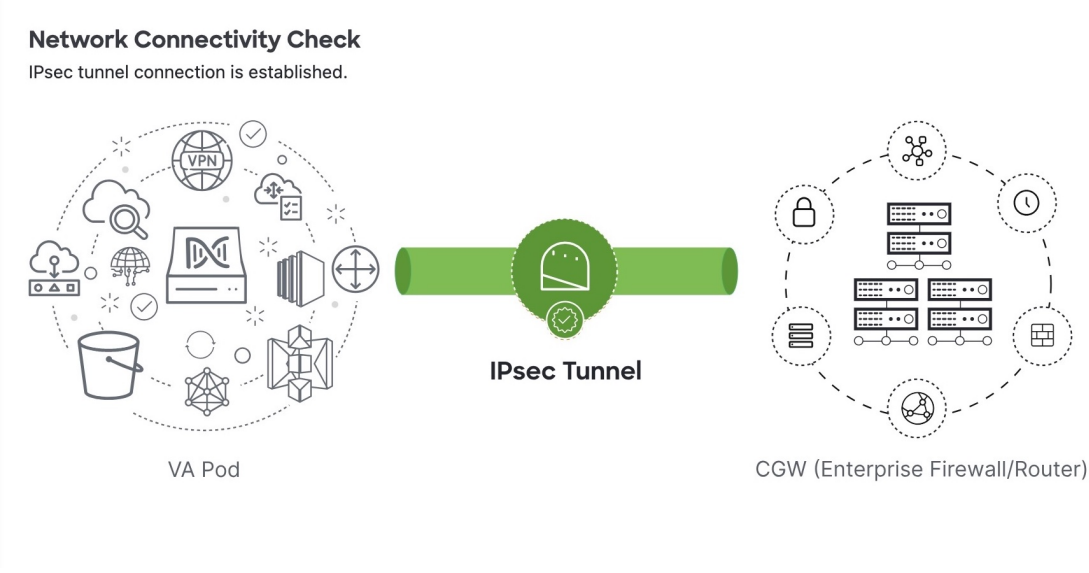
c) [Proceed to Network Connectivity Check] ボタンをクリックします。

ステップ 7 次のいずれかのアクションを実行して、AWS インフラストラクチャの設定時に選択した優先するオンプレミス接続に基づいて、ネットワーク構成のステータスを確認します。

- 優先するオンプレミス接続オプションとして [VPN GW] を選択した場合、IPSec トンネルの設定ステータスが次のように表示されます。
  - ネットワーク管理者が IPSec トンネルをまだ設定していない場合は、IPSec トンネルに鍵アイコンが表示されます。



  - エンタープライズ ファイアウォールまたはルータの IPSec トンネルが稼働していることを確認するようにネットワーク管理者に依頼します。IPSec トンネルが稼働すると、IPSec トンネルが緑色に変わります。



（注） IPsec トンネルが稼働状態になっているのに、CGW から Cisco DNA Center にアクセスできない場合は、IPsec トンネルの設定中に正しい値が渡されたことを確認します。Cisco Global Launchpad は AWS 由来のトンネルステータスを報告し、追加のチェックを実行しません。

- 優先するオンプレミス接続オプションとして [New VPN GW + New TGW] または [Existing TGW and New VPN GW] を選択した場合、Cisco Global Launchpad は、VPC が TGW に接続されているかどうかを確認し、TGW はオンプレミスのファイアウォールまたはルータに接続されます。

  （注） TGW からエンタープライズ ファイアウォールまたはルータへの接続に成功するには、ネットワーク管理者がオンプレミスのファイアウォールまたはルータにこの設定を追加する必要があります。

  接続ステータスは次のように表示されます。

  - TGW からオンプレミスのファイアウォールまたはルータへの接続が確立されていない場合は、グレー表示されます。

  - TGW 接続が正常に確立されると、TGW 接続は緑色になります。

- 優先するオンプレミス接続オプションとして [Existing TGW] と [Existing Attachment] を選択した場合は、既存の TGW と新しく接続された VPC の間でルーティングが設定されていることを確認します。ここで Cisco DNA Center が起動されます。詳細については、既存のトランジットゲートウェイおよびカスタマーゲートウェイでルーティングを手動設定する（41 ページ）を参照してください。

  接続ステータスは次のように表示されます。

  - VPC が TGW に接続されていない場合、TGW 接続はグレー表示されます。

  - TGW 接続が正常に確立されると、TGW 接続は緑色になります。

ステップ 8 [Go to Dashboard] をクリックして [**Dashboard**] ペインに戻ります。ここで、追加の VA ポッドを作成したり、既存の VA ポッドを管理したりすることができます。

既存のトランジットゲートウェイおよびカスタマーゲートウェイでルーティングを手動設定する

新しい VA ポッドの作成時に、優先する接続オプションとして [Existing Transit Gateway] と [Existing Attachments] を選択した場合、Cisco Global Launchpad では Cisco DNA Center を起動するための VPC が作成され、この VPC が既存の TGW に接続されます。

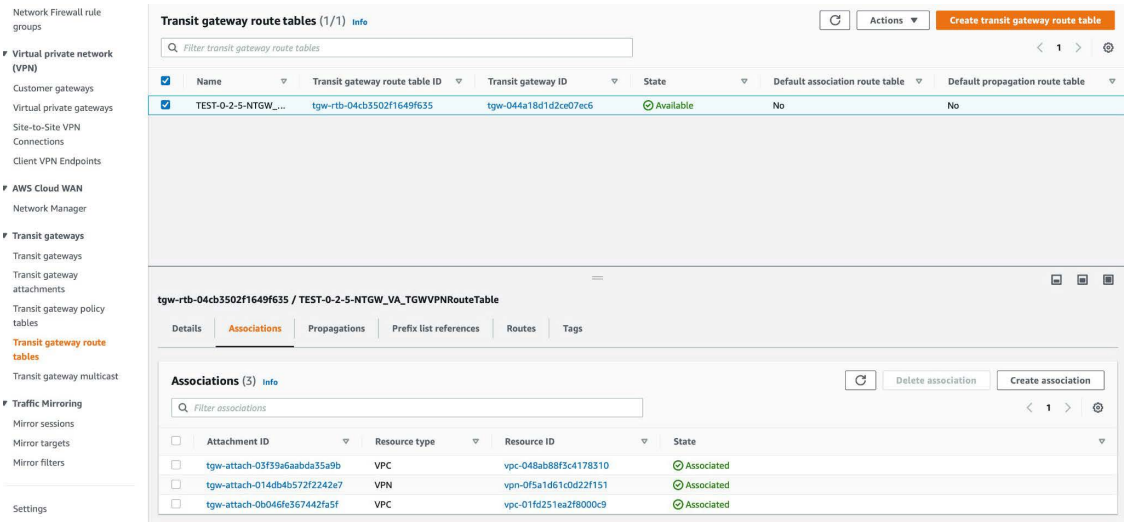
Cisco Global Launchpad で TGW 接続を確立するには、AWS で TGW ルーティングテーブルを手動で設定し、既存の CGW にそのルーティング設定を追加する必要があります。

手順

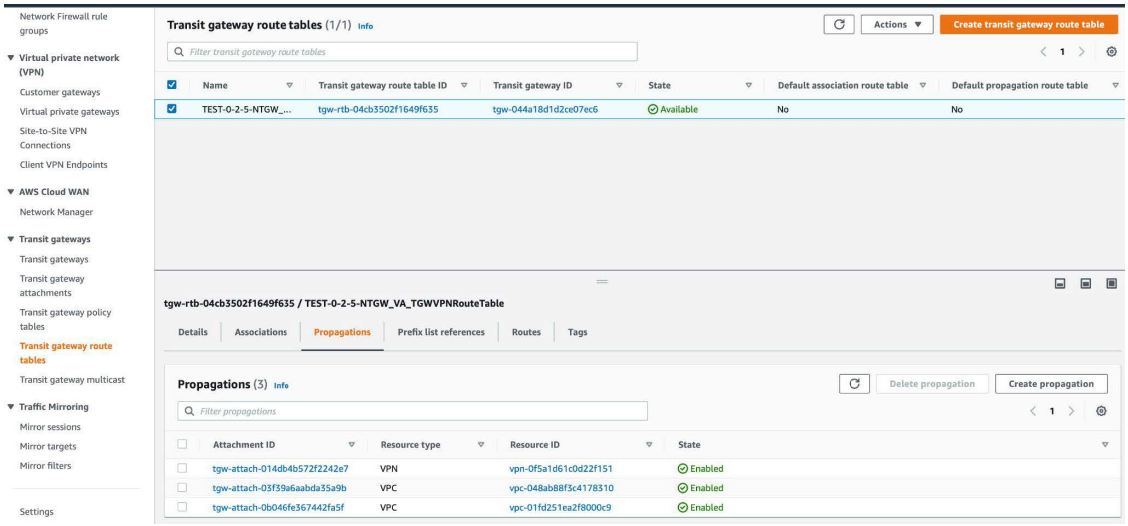
ステップ 1 AWS コンソールから、[VPC service] に移動します。

ステップ 2 左側のナビゲーションウィンドウの [Transit Gateways] で [Transit gateway route table] を選択し、次に既存の TGW ルートテーブルを選択します。

ステップ 3 [Transit gateway route table] ウィンドウで [Associations] タブをクリックし、次に [Create Association] をクリックします。



ステップ 4 [Transit gateway route table] ウィンドウで [Propagations] タブをクリックし、次に [Create propagation] をクリックします。



ステップ 5 それぞれの VPC と VPN 間でスタティックルートを確実にアクティブにするには、[Routes] タブをクリックし、次に [Create static route] をクリックします。

ステップ 6 AWS 環境の CGW に割り当てられた CIDR 範囲に向けてネットワークトラフィックをルーティングするように、オンプレミスルータの設定が更新されていることを確認します。

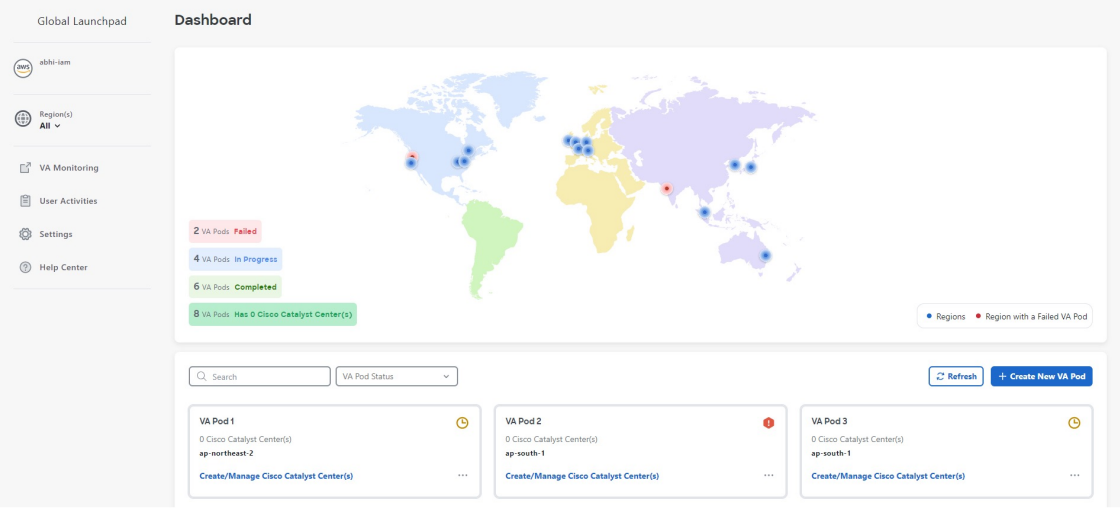
例：`route tunnel-int-vpn-0b57b508d80a07291-1 10.0.0.0 255.255.0.0 192.168.44.37 200`

Cisco DNA Center VA の新規作成

新しい Cisco DNA Center VA を設定するには、次の手順を実行します。

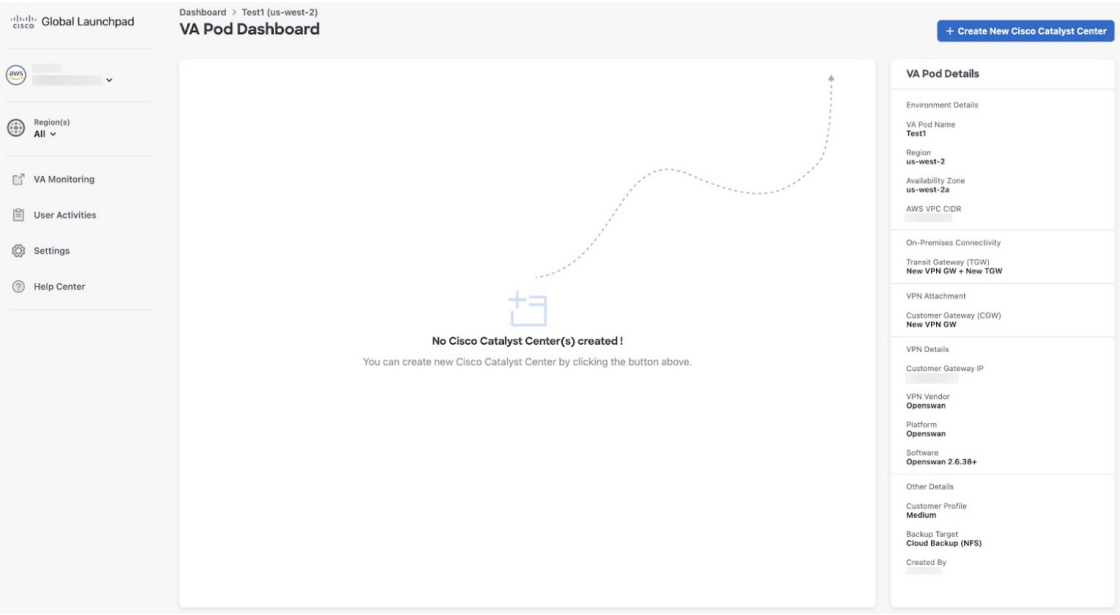
手順

ステップ 1 [**Dashboard**] ペインのマップの下で、Cisco DNA Center VAを作成する VA ポッドを見つけます。



ステップ 2 VA ポッドカードで、[Create/Manage Cisco Catalyst Center(s)] をクリックします。

ステップ 3 [VA Pod Dashboard] ペインで、[+ Create New Cisco Catalyst Center] をクリックします。



ステップ 4 次の詳細を入力します。

- [Cisco Catalyst Center Version]：ドロップダウンリストから、Cisco DNA Center バージョンを選択します。
- [Enterprise DNS]：エンタープライズ DNS の IP アドレスを入力します。このエンタープライズ DNS が、Cisco DNA Center VA を作成する VA ポッドから到達可能であることを確認してください。

（注） Cisco Global Launchpad は、UDP ポート 53 と入力した DNS サーバーの IP アドレスを使用して、オンプレミスのネットワーク接続を確認します。

- [FQDN (Fully Qualified Domain Name)]：DNS サーバーで設定されている Cisco DNA Center VA の IP アドレスを入力します。
- [Proxy Details]：次のいずれかの HTTPS ネットワーク プロキシ オプションを選択します。
  - [No Proxy]：プロキシサーバーは使用されません。
  - [Unauthenticated]：プロキシサーバーは認証を必要としません。プロキシサーバーの URL とポート番号を入力します。
  - [Proxy Authentication]：プロキシサーバーは認証を必要とします。プロキシサーバーの URL、ポート番号、ユーザー名、およびパスワードの詳細を入力します。
- [Cisco Catalyst Center Virtual Appliance Credentials]：Cisco DNA Center VA にログインする際に使用する CLI パスワードを入力します。

  パスワードは、次の条件に従う必要があります。
  - タブや改行を含まないこと。
  - 8 文字以上であること。
  - 次のうち少なくとも 3 つのカテゴリの文字を含むこと。
    - 小文字の英字
    - 大文字の英字
    - 番号（Number）
    - 特殊文字

  後で参照できるように、このパスワードを保存しておいてください。

  （注） ユーザー名は maglev です。

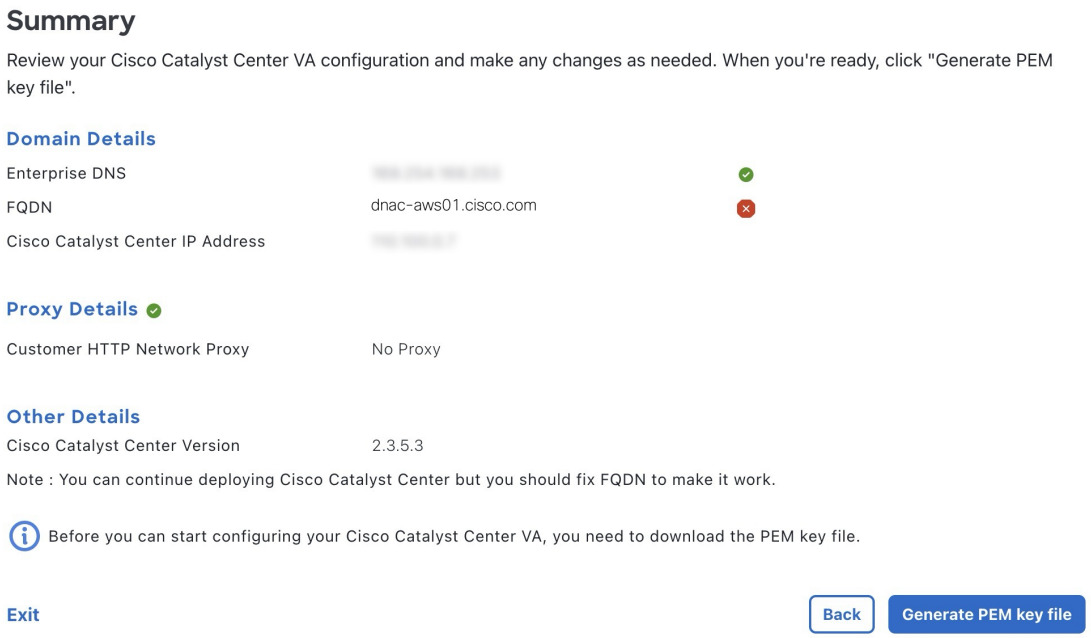
ステップ 5 [Validate] をクリックして、DNS サーバーに設定されているエンタープライズ DNS サーバーと FQDN を検証します。

（注） Cisco Global Launchpad リリース 1.7.0 で、DNS サーバー、プロキシサーバー、または FQDN のチェックに失敗した場合は、次の手順で設定を続行します。

- DNS サーバーの検証に失敗した場合は、Cisco DNA Center VA の作成を続行できません。入力した DNS サーバーの IP アドレスが VA ポッドから到達可能であることを確認してください。
- プロキシサーバーの検証に失敗した場合でも、設定を続行できます。無効なプロキシの詳細が修正されなくても、Cisco DNA Center VA は機能します。
- FQDN の検証に失敗した場合でも、Cisco DNA Center VA の作成を続行できます。ただし、Cisco DNA Center VA を機能させるには、FQDN 設定を修正する必要があります。

ステップ 6 [Summary] ウィンドウで、設定の詳細を確認します。

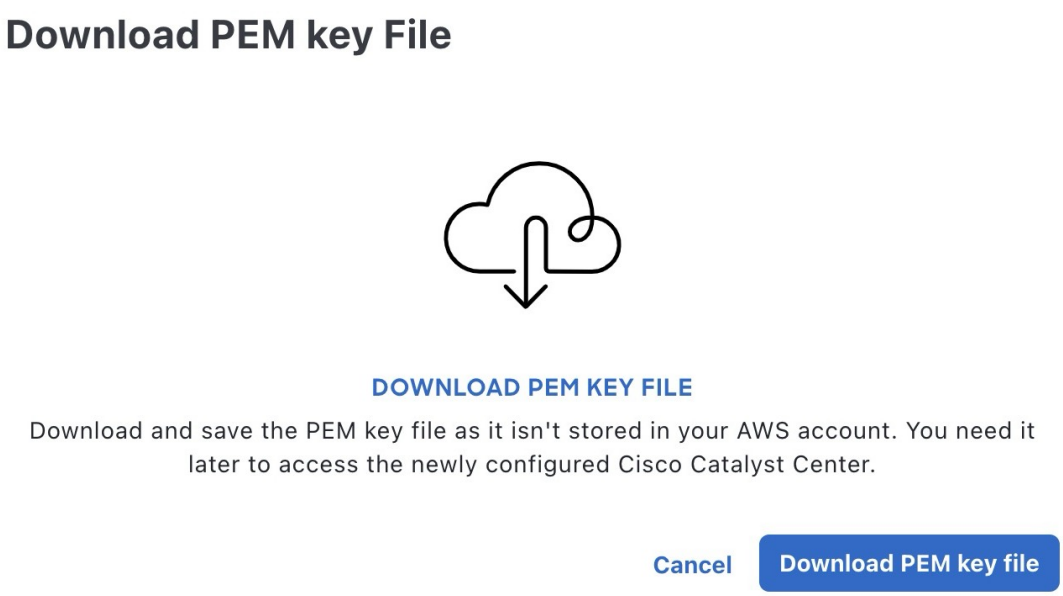
（注） Cisco DNA Center の IP アドレスは静的に割り当てられた IP アドレスであり、中断のない接続を確保し、重要なネットワーク運用中の障害を最小限に抑えるため、AWS 可用性ゾーンの停止後もそのまま保たれます。



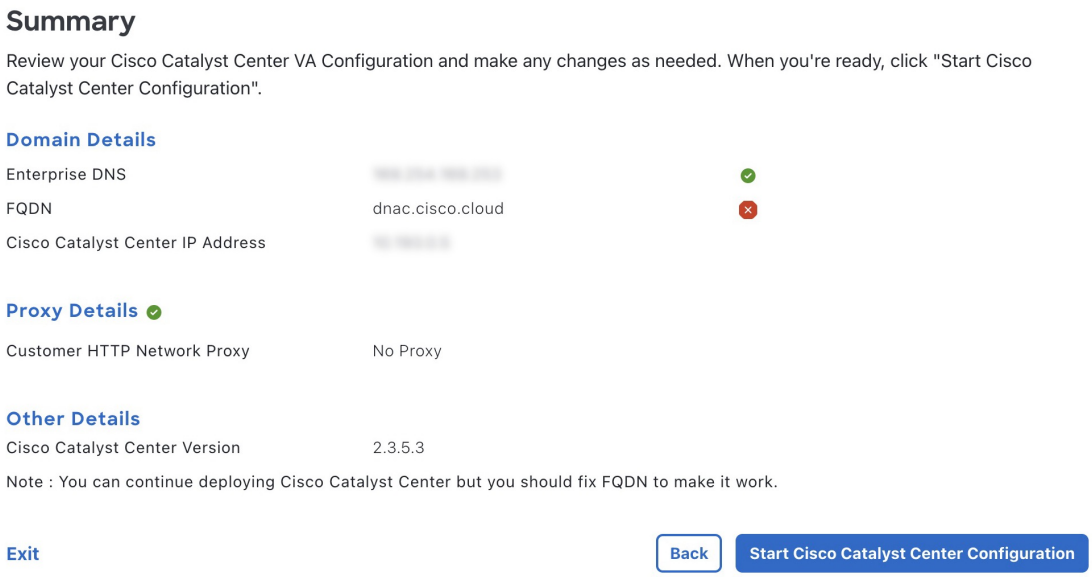
ステップ 7 設定に問題がない場合は、[Generate PEM Key File] をクリックします。

ステップ 8 [Download PEM Key File] ダイアログボックスで、[Download PEM Key File] をクリックします。[Cancel] をクリックすると、[Summary] ウィンドウに戻ります。

重要 PEM キーは AWS アカウントに保存されていないため、ダウンロードする必要があります。作成されている Cisco DNA Center VA にアクセスするには、PEM キーが必要です。



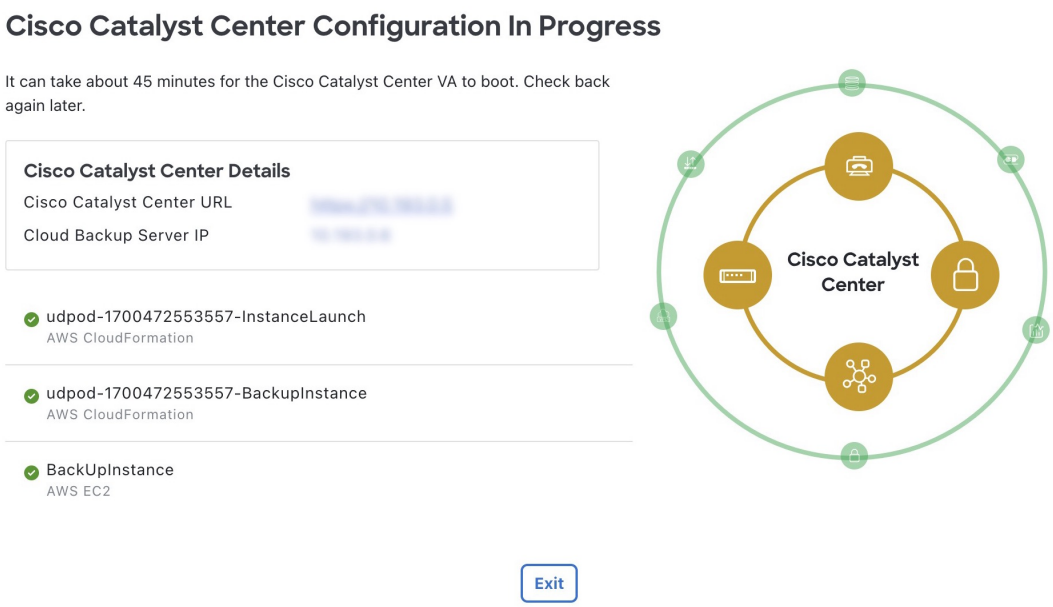
ステップ 9 PEM ファイルをダウンロードしたら、[Start Cisco Catalyst Center Configuration] をクリックします。



Cisco Global Launchpad により Cisco DNA Center 環境が設定されます。環境設定が完了すると、Cisco DNA Center が起動します。最初は、Cisco Global Launchpad で外側のリングがグレー表示されます。ポート 2222 が検証されると、イメージがオレンジに変わります。ポート 443 が検証されると、イメージが緑色に変わります。

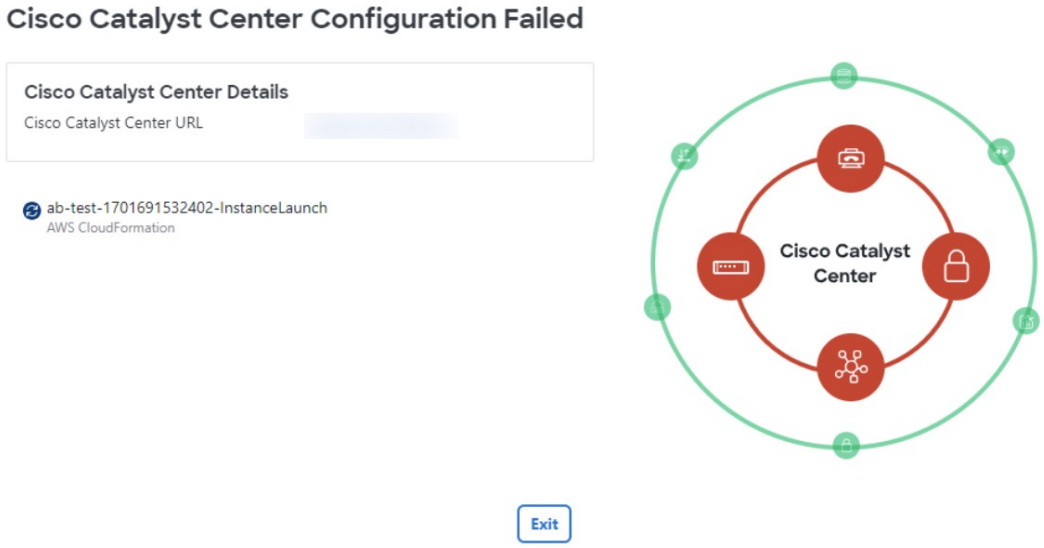
（注） このプロセスは 45 ～ 60 分かかります。アプリケーションを終了したり、このウィンドウやタブを閉じたりしないでください。さもないと、設定が一時停止します。

Cisco DNA Center が起動すれば、設定は完了です。これで、Cisco DNA Center VA の詳細を表示できるようになります。



ヒント　[Cisco Catalyst Center Configuration In Progress] ウィンドウが表示されている間に、バックアップサーバーの IP アドレスとバックアップインスタンスのスタック名を後で使用できるように記録します。バックアップサーバーのパスワードは、バックアップインスタンスのスタック名の最初の 4 文字とバックアップサーバーの IP アドレス（ピリオドを除く）を組み合わせたものです。

Cisco DNA Center の設定に失敗した場合は、[VA Pod Dashboard] ペインに戻ります。詳細については、Cisco DNA Center VA 設定エラーのトラブルシュート （53 ページ）を参照してください。



ステップ 10 [VA Pod Dashboard] ペインに戻るには、[Go to Manage Cisco Catalyst Center(s)] をクリックします。

展開のトラブルシューティング

Cisco Global Launchpad は、最小限の介入で AWS に Cisco DNA Center をシームレスに設定できるように設計されています。ここでは、AWS での Cisco DNA Center の展開時の一般的な問題をトラブルシュートする方法について説明します。

（注） Cisco Global Launchpad では解決できない問題が発生する可能性があるため、AWS コンソールを介して Cisco Global Launchpad でワークフローを手動で変更することは推奨できません。

ここに記載されていない問題がある場合は、Cisco TAC にご連絡ください。

Docker エラーのトラブルシュート

Cisco Global Launchpad の Docker イメージの実行中に「`port is already in use`」というエラーメッセージが表示された場合は、考えられる次の解決策を使用してトラブルシュートできます。

エラー	考えられる解決策
サーバーアプリケーションの実行中に次のエラーが表示された場合： port is already in use（ポートがすでに使用されています）	Docker でサーバーアプリケーションを実行します。 **docker run -d -p** <server-port-number>**:8080 -e SECRET_KEY=**<your-secret-key> **--name server --pull=always dockerhub.cisco.com/maglev-docker/server:x.x.x-latest** （注） 使用可能なサーバーポートをどれでも使用できます。 サーバーアプリケーションの実行中に、クライアントアプリケーションを実行します。 **docker run -d -p 90:80 -e REACT_APP_API_URL=http://localhost:**<client-port-number> **--name client --pull=always dockerhub.cisco.com/maglev-docker/client:x.x.x** （注） サーバーアプリケーションの実行で使用したものと同じポート番号を使用する必要があります。
クライアントアプリケーションの実行中に次のエラーが表示された場合： port is already in use（ポートがすでに使用されています）	Docker でクライアントアプリケーションを実行します。 **docker run -d -p** <client-port-name>**:80 --name client --pull=always dockerhub.cisco.com/maglev-docker/client:x.x.x** （注） 使用可能なサーバーポートをどれでも使用できます。

ログインエラーのトラブルシュート

Cisco Global Launchpad にログインする際に、ログインエラーが発生する場合があります。考えられる次の解決策を使用して、一般的なログインエラーをトラブルシュートできます。

エラー	考えられる解決策
Invalid credentials.（無効なログイン情報です。）	ログイン情報を再入力し、正しく入力されていることを確認します。
You don't have enough access.（十分なアクセス権がありません。）	管理者ユーザーの場合は、アカウントに管理者アクセス権があることを確認します。 サブユーザーの場合は、管理者によって CiscoDNACenter ユーザーグループに追加されていることを確認します。
An operation to delete is in progress, please try again after some time.（削除操作が進行中です。しばらくしてからもう一度お試しください。）	管理者ユーザーが AWS アカウントから <AccountId>-cisco-dna-center グローバルバケットを削除した後にログインしようとすると、このログインエラーが発生することがあります。削除が完了するまで 5 分待ちます。

ホステッド型 Cisco Global Launchpad エラーのトラブルシューティング

ホステッド型 Cisco Global Launchpad では、[Trigger RCA] ペインから根本原因分析（RCA）をトリガーすると、**Rate exceeded** エラーが発生する可能性があります。このエラーが発生すると、次のメッセージが [Trigger RCA] ペインの右上隅に表示されます。

```
Rate exceeded.
```

このエラーメッセージは、1 つのリージョンで最大数の API 要求（1 秒あたり 10,000）を受信した場合に表示されます。このエラーを解決するには、サービスクォータを使用して AWS の制限値を増やすか、数秒後に操作を再試行します。

リージョンに関する問題のトラブルシュート

考えられる次の解決策を使用して、リージョンに関する問題をトラブルシュートできます。

問題	考えられる解決策
新しいリージョンで新しい VA ポッドを作成しているときに、Cisco Global Launchpad にエラーメッセージが表示されるか、画面が 5 分を超えてフリーズし、設定中であることを示すメッセージが表示されません。	AWS コンソールでの手動プロセスが正常に完了したことを確認してから、この手順を再試行してください。問題が解決しない場合は、TAC にご連絡ください。 （注） このような競合状態を回避するため、VA ポッドを手動で変更しないことを推奨します。代わりに、すべてのアクションに Cisco Global Launchpad を使用してください。
リージョンのセットアップが失敗し、Cisco Global Launchpad に次のような [Bucket [name] did not stabilize] エラーが表示されます。 Bucket 059356112352-cisco-dna-center-eu-south-1.va.storage did not stabilize	AWS でケースを開き、失敗したリソースをバックエンドから削除するように依頼します。

VA ポッド設定エラーのトラブルシュート

考えられる次の解決策を使用して、VA ポッド設定エラーをトラブルシュートできます。

エラー	考えられる解決策
+ Create VA Pod button disabled（[+ Create VA Pod] ボタンが無効です）	無効になっているボタンにカーソルを合わせると、無効になっている理由の詳細が表示されます。 新しい VA ポッドを作成できない理由として、次のことが考えられます。 • **VPC サービスクォータの上限数に達した**：すべてのリージョンにおいて、作成できる VPC 数の上限が AWS 管理者によって設定されています。通常、リージョンごとに 5 つの VPC があり、各 VPC に VA ポッドを 1 つだけ配置できます。ただし、正確な数値については、AWS 管理者にお問い合わせください。 Cisco Global Launchpad 以外のリソースに使用される VPC も、この上限数に含まれることに注意してください。たとえば、AWS アカウントに設定された VPC の上限が 5 つで、そのうち 2 つが使用中の場合、選択したリージョンでさらに作成できる VA ポッドは 3 つまでです。 新しい VA ポッドを作成するには、AWS 管理者に上限数の変更を依頼するか、AWS アカウントで既存の VA ポッドまたは VPC の一部を削除します。詳細については、 AWS の Web サイトで『*AWS Support User Guide*』 の AWS「Creating a service quota increase」[英語] のトピックを参照してください。 • **ポッドの削除が進行中**：リージョン内の最後の VA ポッドの削除が進行中です。数分待ってから、新しい VA ポッドの作成を再試行します。
AMI ID for this region is not available for your account.（このリージョンの AMI IDは、お使いのアカウントでは使用できません。）	[+ Create New VA Pod] をクリックすると、Cisco Global Launchpad は選択したリージョンの AMI ID を検証します。 このエラーが発生した場合、検証に失敗しており、このリージョンで新しいポッドを作成できません。この問題を解決するには、Cisco TAC にご連絡ください。
Your VPN configuration is invalid. At this step you cannot update it so please delete the instance and create a new one.（VPN の設定が無効です。このステップでは設定を更新できないため、インスタンスを削除してから新しいインスタンスを作成してください。）	VA ポッドを設定する場合、次の VPN ベンダーはサポートされません。 • **Barracuda** • **Sophos** • **Vyatta** • **Zyxel** サポートされていない VPN ベンダーを使用している場合は、[Configure the On-Premises Tunnel Endpoint] ウィンドウに次のエラーメッセージが表示されます。 `Your VPN configuration is invalid. At this step, you cannot update it, so please delete the instance and create a new one.`

エラー	考えられる解決策
CustomerGateway with type "ipsec.1", ip-address "xx.xx.xx.xx", and bgp-asn "65000" already exists (RequestToken: f78ad45d-b4f8-d02b-9040-f29e5f5f86cf, HandlerErrorCode: AlreadyExists)（タイプ「ipsec.1」、IP アドレス「xx.xx.xx.xx」、bgp-asn「65000」のカスタマーゲートウェイはすでに存在します）	一度に複数の VA ポッドを作成しようとすると、このエラーが発生する可能性があります。 このエラーを解決するには、障害が発生した VA ポッドを削除して再作成します。一度に 1 つの VA ポッドのみを作成するようにしてください。
AWS Infrastructure Failed.（AWSインフラストラクチャで障害が発生しました。）	AWS の設定に失敗した場合は、[**Dashboard**] ペインに戻り、新しい VA ポッドを作成します。詳細については、新しい VA ポッドの作成 （28 ページ）を参照してください。 （注） 設定に失敗した VA ポッドを削除できます。
AWS Configuration fails when editing a VA Pod（VA ポッドの編集中に AWS の設定に失敗しました）	AWS コンソールでの手動プロセスが正常に完了したことを確認し、この手順を再試行してください。問題が解決しない場合は、TAC にご連絡ください。 （注） このような競合状態を回避するには、VA ポッドを手動で変更しないことを推奨します。代わりに、すべてのアクションに Cisco Global Launchpad を使用します。
Deleting VA Pod has failed（VA ポッドの削除に失敗しました）	AWS コンソールでの手動プロセスが正常に完了したことを確認し、この手順を再試行してください。問題が解決しない場合は、TAC にご連絡ください。 （注） このような競合状態を回避するには、VA ポッドを手動で変更しないことを推奨します。代わりに、すべてのアクションに Cisco Global Launchpad を使用します。
The resource you are trying to delete has been modified recently. Please refresh the page get the latest changes and try again.（削除しようとしているリソースは最近変更されました。ページを更新して最新の変更内容を表示してから、もう一度お試しください。）	VA ポッドの削除中にこのエラーが発生した場合は、Cisco TAC にご連絡ください。

ネットワーク接続エラーのトラブルシュート

VA ポッドの作成中に IPSec トンネルや TGW 接続が確立されていない場合は、オンプレミスのファイアウォールまたはルータでトンネルが稼働していることを確認します。

VA ポッドから TGW へのトンネルが緑色で、TGW から CGW へのトンネルが灰色の場合は、次のことを確認します。

- 正しい構成ファイルがネットワーク管理者に転送されている。
- ネットワーク管理者が構成ファイルに必要な変更を加えている。
- ネットワーク管理者がエンタープライズファイアウォールやルータに対してこの構成を適用している。
- 優先するネットワーク接続として [Existing TGW] と [Existing Attachments] を選択した場合は、既存のトランジットゲートウェイおよびカスタマーゲートウェイでルーティングを手動設定する （41 ページ） に正しく従っていることを確認してください。

Cisco DNA Center VA 設定エラーのトラブルシュート

考えられる次の解決策を使用して、Cisco DNA Center VA の設定中に発生したエラーをトラブルシュートできます。

エラー	考えられる解決策
Environment Setup failed（環境設定に失敗しました）	1. Cisco Global Launchpad の [Create/Manage Cisco Catalyst Center(s)] ペインに戻ります。 2. Cisco DNA Center VA を削除します。 3. 新しい Cisco DNA Center VA を作成します。
Delete Failed（削除に失敗しました）	Cisco DNA Center VA の削除に失敗した場合は、Cisco TAC にご連絡ください。

同時実行エラーのトラブルシュート

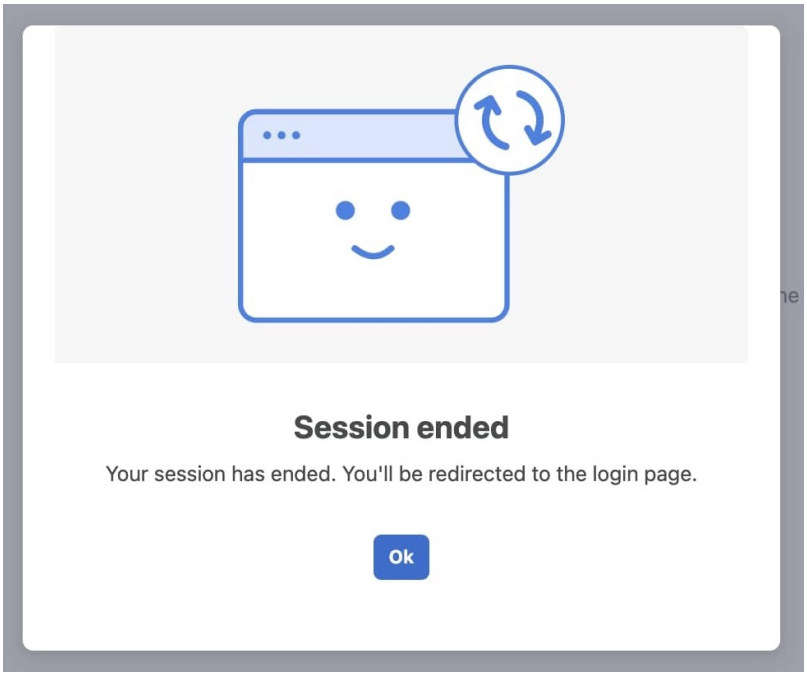
考えられる次の解決策を使用して、同時実行エラーをトラブルシュートします。

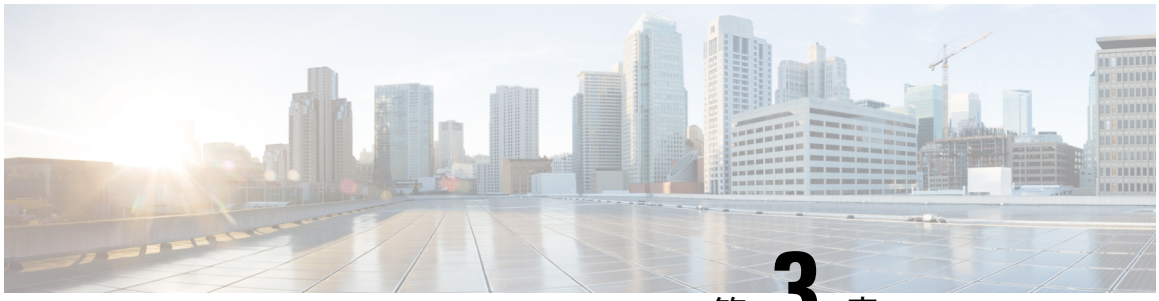
エラー	考えられる解決策
Unable to delete a Pod or a Cisco DNA Center created by another user.（別のユーザーが作成したポッドや Cisco DNA Center は削除できません。）	別のユーザーが作成した VA ポッドや Cisco DNA Center VA などコンポーネントは、そのコンポーネントで別のアクションが進行中は削除できません。アクションが完了すると、自分または他のユーザーがそのコンポーネントを削除できます。 たとえば、VA ポッドや Cisco DNA Center VA が次のプロセス中または状態にある場合は削除できません。 • 別のユーザーが Cisco DNA Center VA を作成中である。 • 別のユーザーが Cisco DNA Center VA を削除中である。 • 削除を試行して、Cisco DNA Center VA がエラー状態である。
The status of a Pod has been changed recently.（ポッドのステータスが最近変更されました。）	VA ポッドを削除しようとした場合、VA ポッドを作成した元のユーザーアカウントが同時アクションを実行した可能性があります。このような同時実行の問題が発生すると、選択した VA ポッドのステータスが変更されます。 VA ポッドの更新されたステータスを表示するには、[Refresh] をクリックします。

展開に関するその他の問題のトラブルシュート

考えられる次の解決策を使用して、AWS での Catalyst Center VA の展開中に発生した他の問題をトラブルシュートできます。

問題	考えられる原因と解決策
リソースは緑色だが、[Proceed] ボタンが無効になる。	一部の手順は、すべてのリソースが正常にセットアップされている場合にのみ続行できます。展開の完全性を確保するため、セットアップが完了し、すべてのリソースが設定およびロードされるまで、[Proceed] ボタンは無効のままになります。 リソースが正常にセットアップされたことが画面に表示されても、[Proceed] ボタンが無効のままになることがあります。この場合、一部のリソースがロードされるまでさらに数秒待つ必要があります。すべてのリソースが設定およびロードされると、[Proceed] ボタンが有効になります。
1 つのリージョンで同じ CGW を持つ複数の VA ポッドを展開するとエラーが発生する。	次のことを確認してください。 • CGW IP アドレスがエンタープライズ ファイアウォールまたはルータの IP アドレスであること。 • CGW IP アドレスが有効なパブリックアドレスであること。 • CGW IPアドレスが同じリージョン内の別の VA ポッドに使用されていないこと。現在、各リージョンでは、複数の VA ポッドが同じ CGW IP アドレスを持つことはできません。複数の VA ポッドで同じ CGW IP アドレスを使用するには、各 VA ポッドを異なるリージョンに展開してください。

問題	考えられる原因と解決策
Cisco DNA Center VA に SSH または ping を実行できない。	トンネルが稼働しており、アプリケーションのステータスが完了（緑色）であっても、Catalyst Center VA に対して SSH 接続や ping を実行できない場合があります。この問題は、オンプレミスの CGW が正しく設定されていない場合に発生する可能性があります。CGW の設定を確認して、再試行してください。
セッションが終了する	RCA のトリガーなどの操作の進行中にセッションがタイムアウトすると、操作が突然終了し、次の通知が表示されることがあります。  セッションがタイムアウトした場合は、再度ログインして操作を再開してください。



第 3 章

Cisco DNA Center VA 起動パッド 1.6 を使用した展開

自動展開メソッドを使用した AWS での Cisco DNA Center の展開

ユーザーは VPC、IPsec VPN トンネル、ゲートウェイ、サブネット、セキュリティグループなど、AWS アカウントで AWS インフラストラクチャを作成するために必要な詳細情報を Cisco DNA Center VA 起動パッド で指定します。これにより、Cisco DNA Center VA 起動パッド は、指定された設定どおりに Cisco DNA Center AMI を Amazon EC2 インスタンスとして個別の VPC に展開します。設定には、サブネット、トランジットゲートウェイのほかに、モニタリング用の Amazon CloudWatch、ステートストレージ用の Amazon DynamoDB、セキュリティグループなどの重要なリソースが含まれます。

Cisco DNA Center VA 起動パッド を使用すると、VA にアクセスして管理することも、ユーザー設定を管理することも可能です。詳細については、*Cisco DNA Center VA Launchpad 1.6 Administrator Guide*を参照してください。

自動展開ワークフロー

自動化されたメソッドを使用して 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。自動展開の前提条件 （58 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 （5 ページ）を参照してください。
3. Cisco DNA Center VA 起動パッドをインストールするか、シスコがホストする Cisco DNA Center VA 起動パッドにアクセスします。Cisco DNA Center VA 起動パッドのインストール （62 ページ）またはホステッド型 Cisco DNA Center VA 起動パッドへのアクセス （64 ページ）を参照してください。
4. Cisco DNA Center VA インスタンスに含める新しい VA ポッドを作成します。新しい VA ポッドの作成 （72 ページ）を参照してください。
5. （任意）優先するオンプレミス接続オプションとして既存の TGW と既存のアタッチメント（VPC など）を使用する場合は、AWS で TGW ルーティングテーブルを手動で設定し、既存のカスタマーゲートウェイ（CGW）にルーティング設定を追加する必要があります。既存のトランジットゲートウェイおよびカスタマーゲートウェイでルーティングを手動設定する （84 ページ）を参照してください。
6. Cisco DNA Center の新しいインスタンスを作成します。新しい Cisco DNA Center VA の作成 （85 ページ）を参照してください。
7. （任意）必要に応じて、展開中に発生した問題をトラブルシュートします。展開のトラブルシューティング （91 ページ）を参照してください。
8. Cisco DNA Center VA 起動パッドを使用して Cisco DNA Center VA を管理します。*Cisco DNA Center VA Launchpad 1.6 Administrator Guide*を参照してください。

自動展開の前提条件

Cisco DNA Center VA 起動パッドを使用して AWS で Cisco DNA Center の展開を開始する前に、次の要件が満たされていることを確認してください。

- プラットフォームに Docker Community Edition（CE） をインストールします。

  Cisco DNA Center VA 起動パッドは、Mac、Windows、および Linux プラットフォーム上の Docker CE をサポートしています。お使いのプラットフォーム固有の手順については、Docker の Web サイトに掲載されているドキュメントを参照してください。

- どの方法で Cisco DNA Center VA 起動パッドにアクセスして Cisco DNA Center VA を展開するかに関係なく、クラウド環境が次の仕様を満たしていることを確認してください。

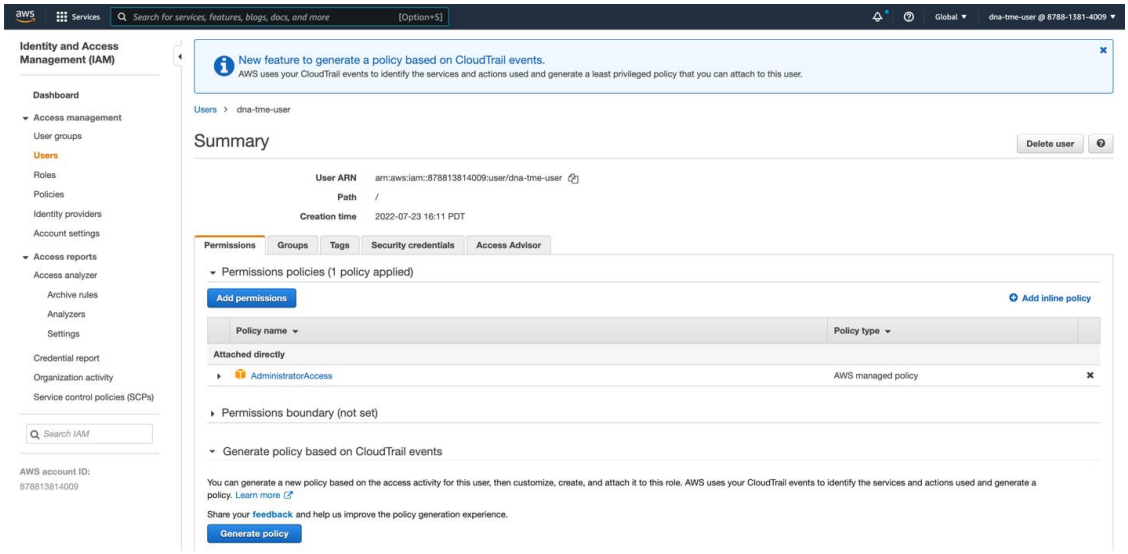
- **Cisco DNA Center インスタンス**：r5a.8xlarge、32 個の vCPU、256 GB の RAM、4 TB ストレージ

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 DNA Center VA 起動パッド Release 1.6.0*』[英語] を参照してください。

- **バックアップインスタンス**：T3.micro、2 個の vCPU、500 GB のストレージ、1 GB の RAM

- 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。
- AWS アカウントが、リソースの独立性と分離を維持するためのサブアカウント（子アカウント）であること。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。
- 管理者ユーザーの場合は、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）。

  管理者アクセスポリシーは、グループではなく、AWS アカウントに直接割り当てる必要があります。このアプリケーションは、グループポリシーを介して列挙を実行しません。そのため、管理者アクセス権限を持つグループに追加されたユーザーであっても、必要なインフラストラクチャを作成できません。



- サブユーザーの場合は、管理者によって CiscoDNACenter ユーザーグループに追加されている必要があります。

  管理者ユーザーが Cisco DNA Center VA 起動パッドに初めてログインすると、必要なすべてのポリシーが割り当てられた CiscoDNACenter ユーザーグループが AWS アカウント上に作成されます。管理者ユーザーがこのグループにサブユーザーを追加すると、サブユーザーが Cisco DNA Center VA 起動パッドにログインできるようになります。

  CiscoDNACenter ユーザーグループには、次のポリシーが割り当てられています。

  - AmazonDynamoDBFullAccess
  - IAMReadOnlyAccess
  - AmazonEC2FullAccess
  - AWSCloudFormationFullAccess
  - AWSLambda_FullAccess
  - CloudWatchFullAccess
  - ServiceQuotasFullAccess
  - AmazonEventBridgeFullAccess
  - service-role/AWS_ConfigRole
  - AmazonS3FullAccess
  - ClientVPNServiceRolePolicy（バージョン：2012-10-17）

    このポリシーでは、次のルールが許可されます。

    - ec2:CreateNetworkInterface
    - ec2:CreateNetworkInterfacePermission
    - ec2:DescribeSecurityGroups
    - ec2:DescribeVpcs
    - ec2:DescribeSubnets
    - ec2:DescribeInternetGateways
    - ec2:ModifyNetworkInterfaceAttribute
    - ec2:DeleteNetworkInterface
    - ec2:DescribeAccountAttributes
    - ds:AuthorizeApplication
    - ds:DescribeDirectories
    - ds:GetDirectoryLimits
    - ds:UnauthorizeApplication
    - logs:DescribeLogStreams

- logs:CreateLogStream
- logs:PutLogEvents
- logs:DescribeLogGroups
- acm:GetCertificate
- acm:DescribeCertificate
- iam:GetSAMLProvider
- lambda:GetFunctionConfiguration

• ConfigPermission（バージョン：2012-10-17、SID：VisualEditor0）

このポリシーでは、次のルールが許可されます。

- config:Get
- config:*
- config:*ConfigurationRecorder
- config:Describe*
- config:Deliver*
- config:List*
- config:Select*
- tag:GetResources
- tag:GetTagKeys
- cloudtrail:DescribeTrails
- cloudtrail:GetTrailStatus
- cloudtrail:LookupEvents
- config:PutConfigRule
- config:DeleteConfigRule
- config:DeleteEvaluationResults

• PassRole（バージョン：2012-10-17、SID：VisualEditor0）

このポリシーでは、次のルールが許可されます。

- iam:GetRole
- iam:PassRole

Cisco DNA Center VA 起動パッドのインストール

この手順では、サーバーおよびクライアント アプリケーションの Docker コンテナを使用して Cisco DNA Center VA 起動パッドをインストールする方法を示します。

始める前に

お使いのマシンに Docker CE がインストールされていることを確認してください。詳細については、自動展開の前提条件 （58 ページ）を参照してください。

手順

ステップ 1 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。

- `Launchpad-desktop-client-1.6.0.tar.gz`
- `Launchpad-desktop-server-1.6.0.tar.gz`

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 （8 ページ）を参照してください。

ステップ 3 ダウンロードしたファイルから Docker イメージを読み込みます。

```
docker load < Launchpad-desktop-client-1.6.0.tar.gz
```

```
docker load < Launchpad-desktop-server-1.6.0.tar.gz
```

ステップ 4 **docker images** コマンドを使用して、リポジトリ内の Docker イメージのリストを表示し、サーバーおよびクライアントアプリケーションの最新コピーがあることを確認します。ファイルには、[TAG] 列に [1.6] から始まる番号が表示されます。

次に例を示します。

```
$ docker images

REPOSITORY                                                          TAG       IMAGE ID       CREATED       SIZE
466518672524.dkr.ecr.us-west-2.amazonaws.com/val/valaunchpad-server              1.6.2     d210a13ab40c   3 hours ago   470MB
466518672524.dkr.ecr.us-west-2.amazonaws.com/platform-ui/valaunchpad-client-docker   1.6.2     d22f4eb51e31   4 hours ago   1.12GB
```

ステップ 5 サーバーアプリケーションを実行します。

docker run -d -p <server-port-number>**:8080 -e DEBUG=true --name server** <server_image_id>

次に例を示します。

```
$ docker run -d -p 9090:8080 -e DEBUG=true --name server f87ff30d4c6a
```

ステップ 6 クライアント アプリケーションを実行します。

docker run -d -p <client-port-number>**:80 -e CHOKIDAR_USEPOLLING=true -e REACT_APP_API_URL=http://localhost:**<server-port-number> **--name client** <client_image_id>

次に例を示します。

```
$ docker run -d -p 90:80 -e CHOKIDAR_USEPOLLING=true -e
REACT_APP_API_URL=http://localhost:9090 --name client dd50d550aa7c
```

（注） 公開されているサーバーのポート番号と REACT_APP_API_URL のポート番号が同じであることを確認します。ステップ 5 とステップ 6 では、両方の例でポート番号 9090 が使用されています。

ステップ 7 **docker ps -a** コマンドを使用して、サーバーとクライアントのアプリケーションが実行されていることを確認します。[STATUS] 列にアプリケーションが稼働中であることが示されている必要があります。

次に例を示します。

```
$ docker ps -a

CONTAINER ID   IMAGE          COMMAND                  CREATED       STATUS       PORTS                    NAMES
cfa24728a490   d210a13ab40c   "/usr/bin/dumb-init …"   2 hours ago   Up 2 hours   0.0.0.0:9090->8080/tcp   server-aws
4fedc555f1f5   d22f4eb51e31   "docker-entrypoint.s…"   2 hours ago   Up 2 hours   0.0.0.0:90->80/tcp       client-aws
```

（注） サーバーまたはクライアントアプリケーションの実行中に問題が発生した場合は、Docker エラーのトラブルシュート （91 ページ）を参照してください。

ステップ 8 次の形式でURLを入力して、サーバーアプリケーションにアクセスできることを確認します。

http://<localhost>**:**<server-port-number>**/api/valaunchpad/aws/v1/api-docs/**

次に例を示します。

http://192.0.2.2:9090/api/valaunchpad/aws/v1/api-docs/

Cisco DNA Center VA に使用されているアプリケーション プログラミング インターフェイス（API）がウィンドウに表示されます。

ステップ 9 次の形式で URL を入力して、クライアント アプリケーションにアクセスできることを確認します。

http://<localhost>**:**<client-port-number>**/valaunchpad**

次に例を示します。

http://192.0.2.1:90/valaunchpad

Cisco DNA Center VA 起動パッド ログインウィンドウが表示されます。

（注） クライアントおよびサーバーアプリケーションでアーティファクトが読み込まれるため、Cisco DNA Center VA 起動パッド ログインウィンドウの読み込みに数分かかることがあります。

ホステッド型 Cisco DNA Center VA 起動パッド へのアクセス

Cisco DNA ポータル で Cisco DNA Center VA 起動パッド にアクセスできます。

Cisco DNA ポータル を初めて使用する場合は、シスコアカウントと Cisco DNA ポータル アカウントを作成する必要があります。その後、Cisco DNA ポータル にログインして Cisco DNA Center VA 起動パッド にアクセスできます。

Cisco DNA ポータル を以前から使用し、シスコアカウントと Cisco DNA ポータル アカウントをお持ちの場合は、Cisco DNA ポータル に直接ログインして Cisco DNA Center VA 起動パッド にアクセスできます。

シスコアカウントの作成

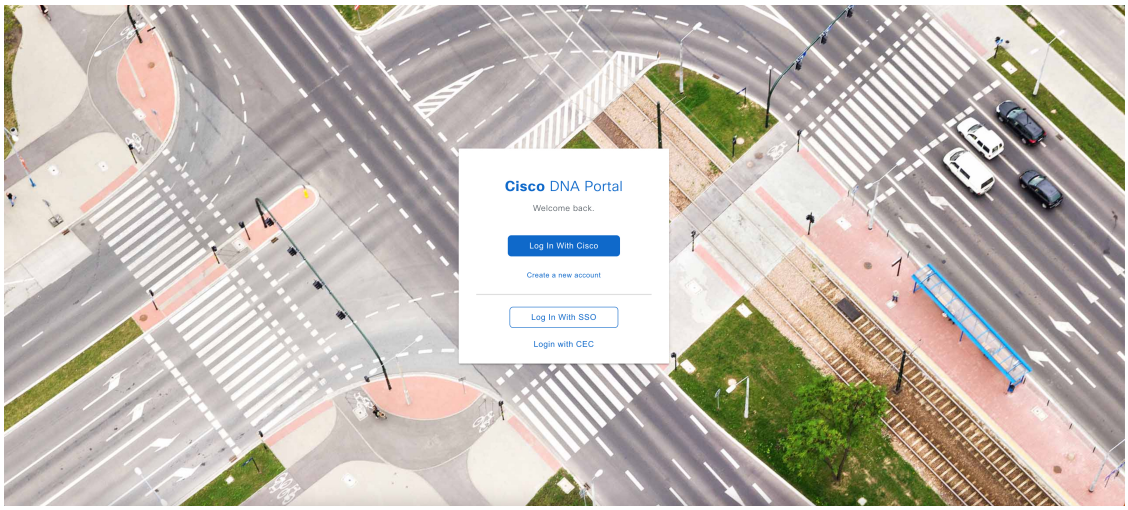
Cisco DNA ポータル を介して Cisco DNA Center VA 起動パッド にアクセスするには、最初にシスコアカウントを作成する必要があります。

手順

ステップ 1 ブラウザで次のように入力します。

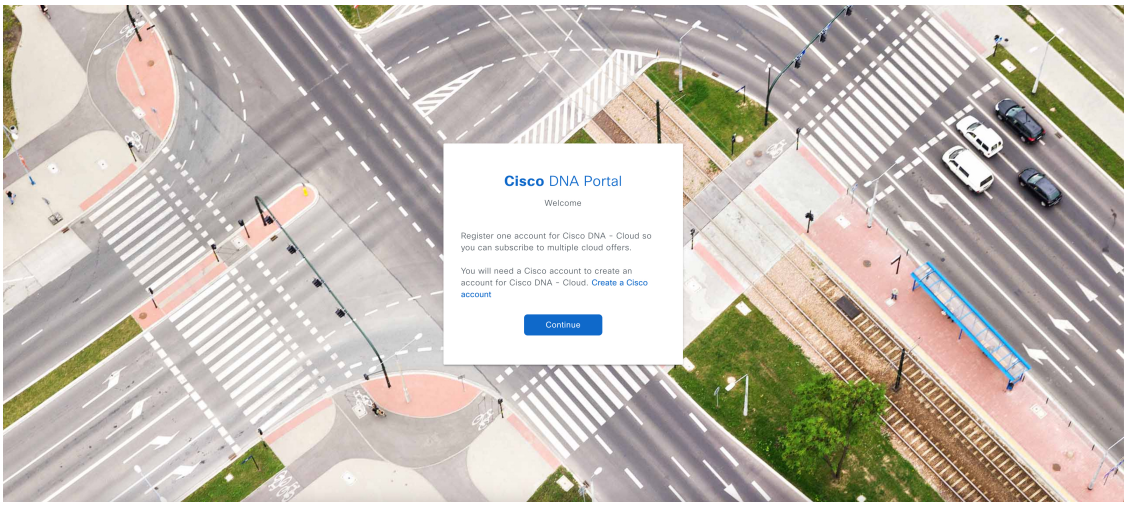
dna.cisco.com

[Cisco DNA Portal] ログインウィンドウが表示されます。

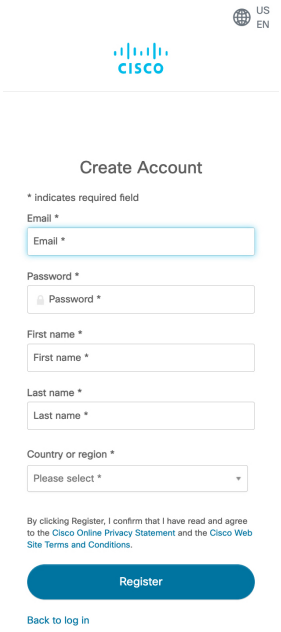


ステップ 2 [Create a new account] をクリックします。

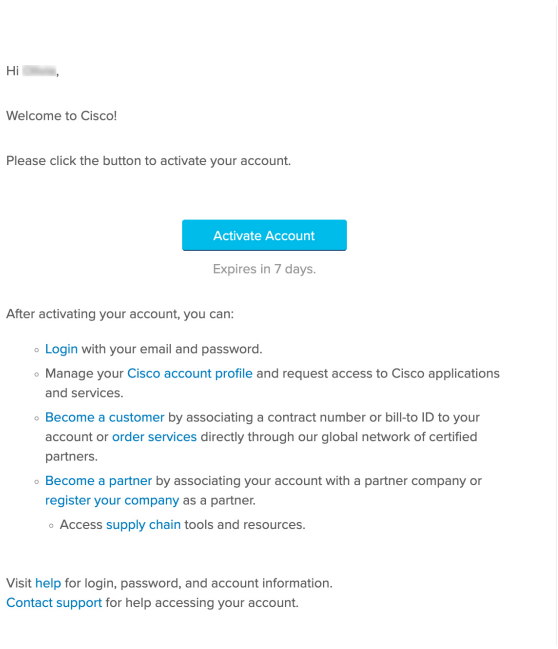
ステップ 3 [Cisco DNA Portal Welcome] ウィンドウで [Create a Cisco account] をクリックします。



ステップ 4 [Create Account] ウィンドウで必要なフィールドに入力し、[Register] をクリックします。



ステップ 5 アカウントの登録に使用した電子メールに移動し、[Activate Account] をクリックして、アカウントを確認します。


Hi [redacted],

Welcome to Cisco!

Please click the button to activate your account.

Activate Account

Expires in 7 days.

After activating your account, you can:

- Login with your email and password.
- Manage your Cisco account profile and request access to Cisco applications and services.
- Become a customer by associating a contract number or bill-to ID to your account or order services directly through our global network of certified partners.
- Become a partner by associating your account with a partner company or register your company as a partner.
  - Access supply chain tools and resources.

Visit help for login, password, and account information.
Contact support for help accessing your account.

Cisco DNA ポータル アカウントの作成

Cisco DNA ポータル を介して Cisco DNA Center VA 起動パッド にアクセスするには、Cisco DNA ポータル アカウントを作成する必要があります。

始める前に

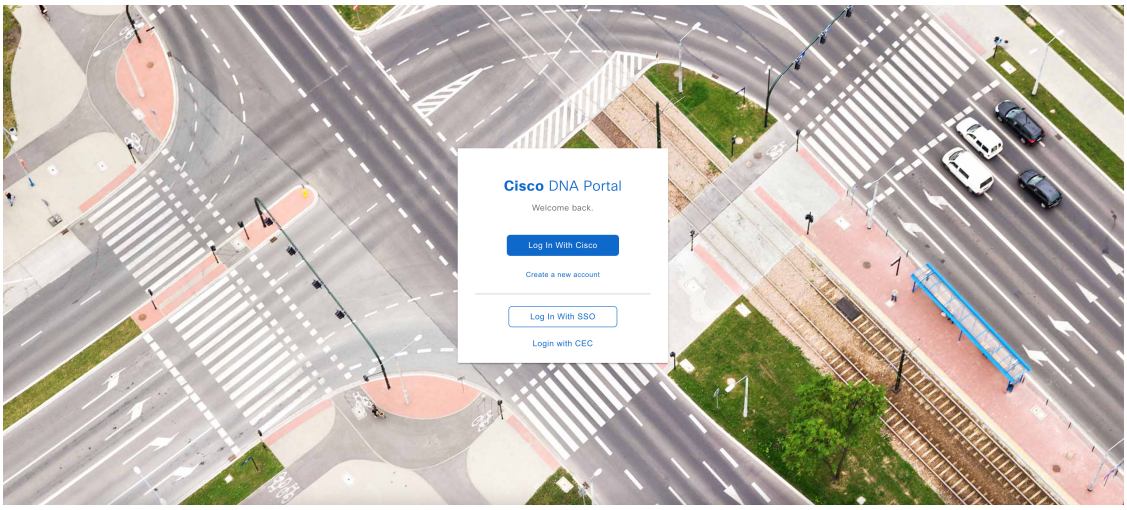
シスコアカウントがあることを確認します。詳細については、シスコアカウントの作成 （64 ページ）を参照してください。

手順

ステップ 1 ブラウザで次のように入力します。

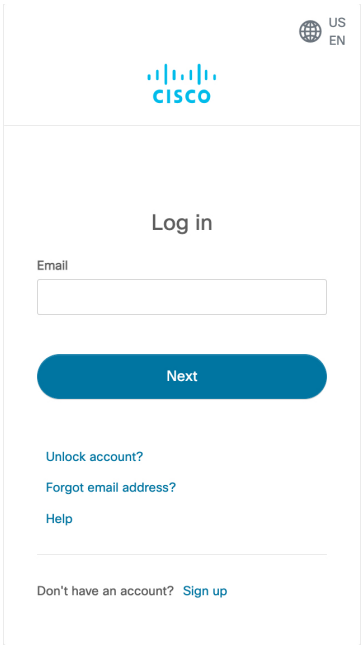
`dna.cisco.com`

[Cisco DNA Portal] ログインウィンドウが表示されます。

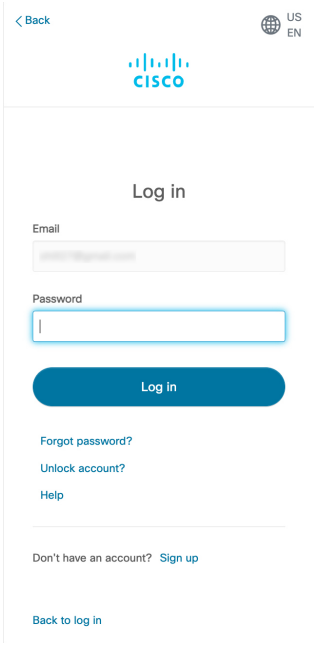


ステップ 2 [Log In With Cisco] をクリックします。

ステップ 3 [Email] フィールドにシスコアカウントの電子メールを入力し、[Next] をクリックします。

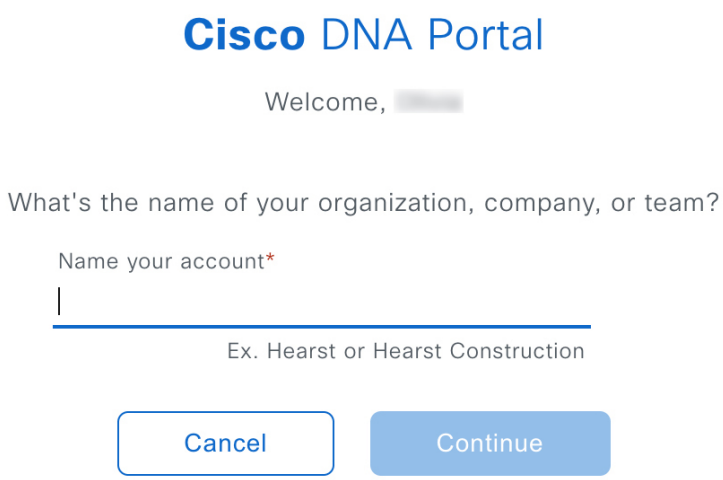


ステップ 4 [Password] フィールドにシスコアカウントのパスワードを入力します。



ステップ 5 [Log in] をクリックします。

ステップ 6 [Cisco DNA Portal Welcome] ウィンドウの [Name your account] フィールドに組織名またはチーム名を入力します。[Continue] をクリックします。

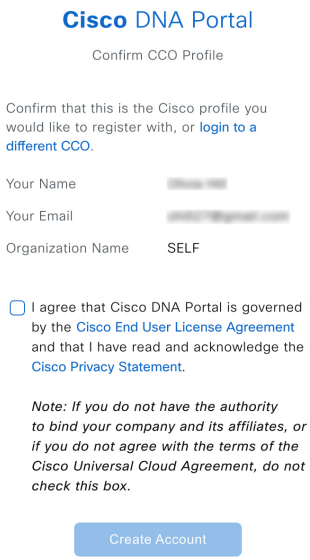


ステップ 7 [Cisco DNA Portal Confirm CCO Profile] ウィンドウで、次の手順を実行します。

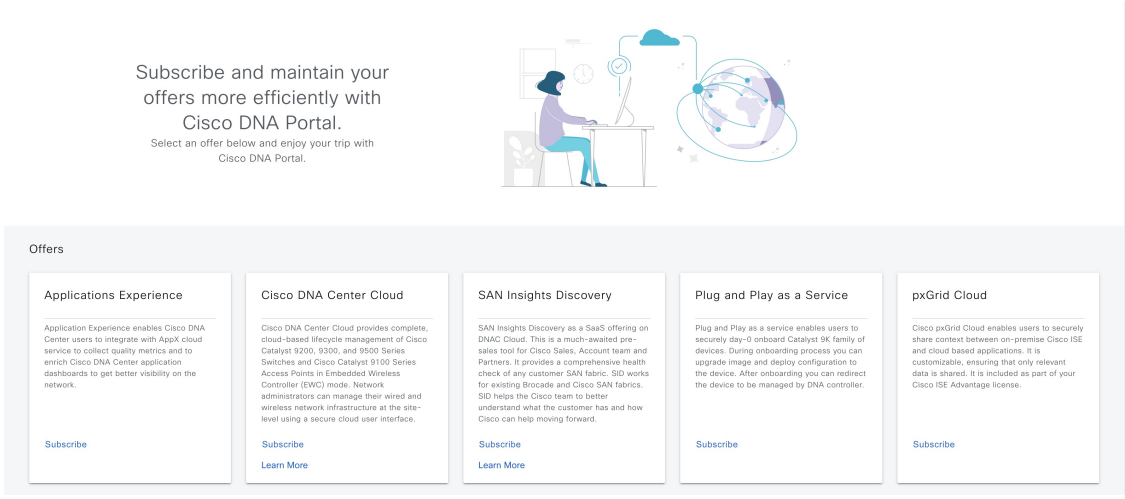
a) 表示される情報が正しいことを確認します。

b) 条件を読んで確認し、同意する場合はチェックボックスをオンにします。

c) [Create Account] をクリックします。



アカウントが正常に作成されると、[Cisco DNA Portal] ホームページが表示されます。



シスコアカウントでの Cisco DNA ポータル へのログイン

Cisco DNA ポータル を介して Cisco DNA Center VA 起動パッド にアクセスするには、Cisco DNA ポータル にログインする必要があります。

始める前に

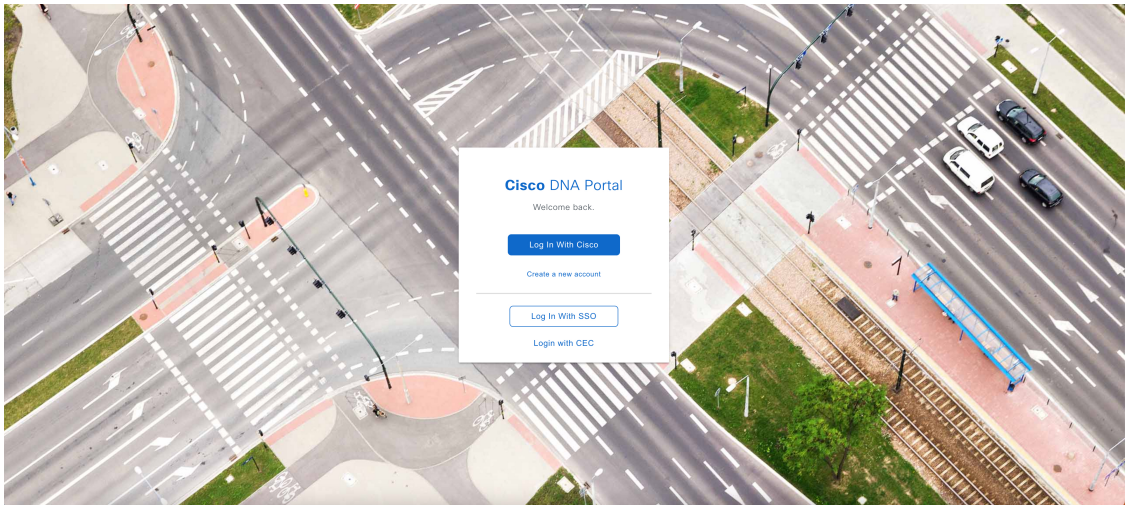
シスコアカウントと Cisco DNA ポータル アカウントがあることを確認します。詳細については、シスコアカウントの作成 （64 ページ）およびCisco DNA ポータル アカウントの作成 （66 ページ）を参照してください。

手順

ステップ 1 ブラウザで次のように入力します。

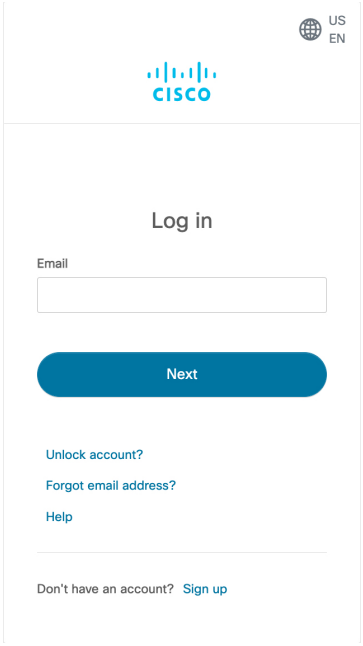
dna.cisco.com

[Cisco DNA Portal] ログインウィンドウが表示されます。

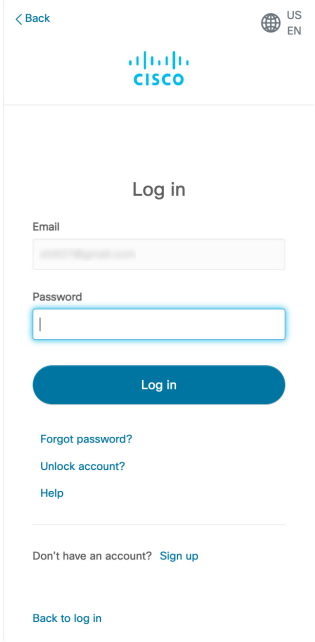


ステップ 2 [Log In With Cisco] をクリックします。

ステップ 3 [Email] フィールドにシスコアカウントの電子メールを入力し、[Next] をクリックします。



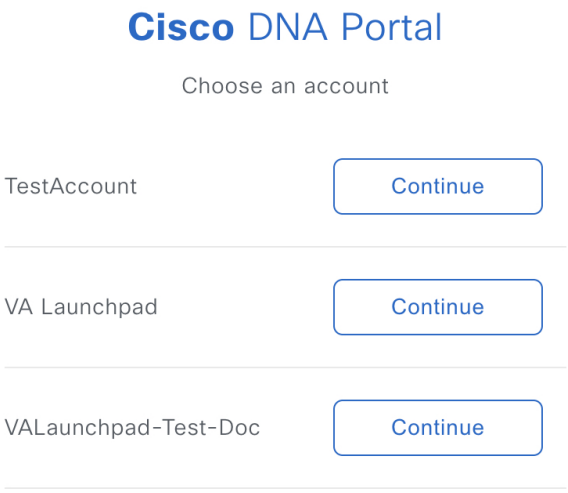
ステップ 4 [Password] フィールドにシスコアカウントのパスワードを入力します。



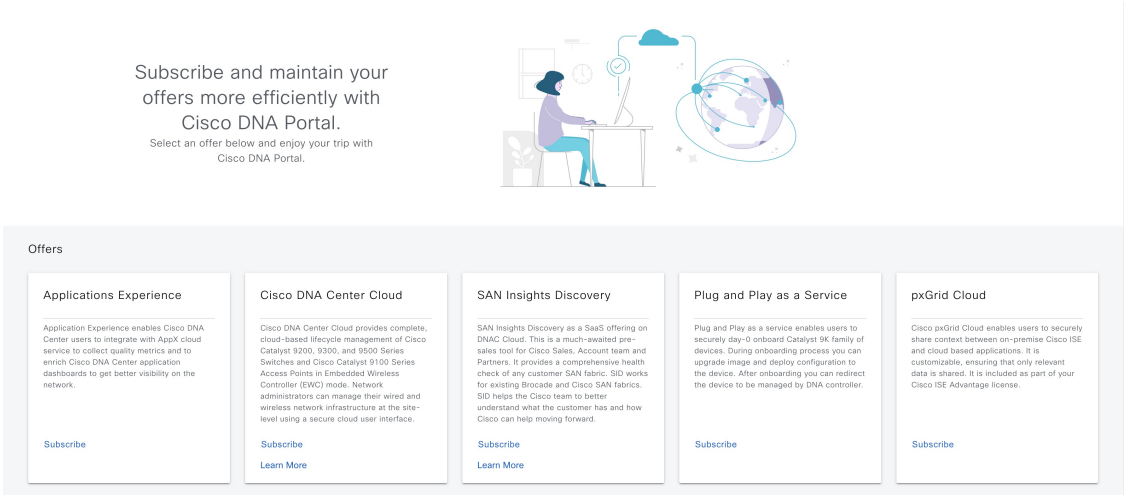
ステップ 5 [Log in] をクリックします。

Cisco DNA ポータル アカウントが 1 つしかない場合は、[Cisco DNA Portal] ホームページが表示されます。

ステップ 6 （任意）複数の Cisco DNA ポータルアカウントがある場合は、アカウントの横にある [Continue] ボタンをクリックして、ログインするアカウントを選択します。



[Cisco DNA Portal] ホームページが表示されます。



新しい VA ポッドの作成

VA ポッドは、Cisco DNA Center VA 向けの AWS ホスティング環境です。このホスティング環境には、Cisco DNA Center VA EC2 インスタンス、Amazon Elastic Block Storage（EBS）、バックアップ NFS サーバー、セキュリティグループ、ルーティングテーブル、Amazon CloudWatch ログ、Amazon Simple Notification Service（SNS）、VPN ゲートウェイ（VPN GW）、TGW などの AWS リソースが含まれます。

Cisco DNA Center VA 起動パッドを使用して、複数の VA ポッド（Cisco DNA Center VA ごとに 1 つの VA ポッド）を作成できます。

（注）

- AWS スーパー管理者ユーザーは、各リージョンで作成できる VA ポッド数の上限を設定できます。Cisco DNA Center VA 起動パッド以外のリソースに使用される VPC もこの数に含まれます。たとえば、AWS アカウントに設定された VPC の上限が 5 つで、そのうち 2 つが使用中の場合、選択したリージョンでさらに作成できる VA ポッドは 3 つまでです。
- 一部の手順では、すべてのリソースが正しく設定された場合にのみ次の手順に進むことができます。すべてのリソースが正しく設定されていない場合、[Proceed] ボタンは無効になります。すべてのリソースが正しく設定されているにもかかわらず、[Proceed] ボタンが無効になっている場合は、リソースがまだロードされているため、数秒間お待ちください。すべての設定が完了すると、ボタンが有効になります。
- Cisco DNA Center VA 起動パッドを新しいリリースに更新した場合、以前の Cisco DNA Center VA 起動パッドリリースにダウングレードした場合、または VA ポッドが配置されているリージョン設定を更新した場合、VA ポッドの設定は変更されません。

  たとえば、Cisco DNA Center VA 起動パッドリリース 1.6.0 で VA ポッドを作成した場合、バックアップパスワードは、バックアップインスタンスのスタック名とバックアップサーバーの IP アドレスを組み合わせたものになります。リリース 1.5.0 などの以前のリリースでこの VA ポッドにアクセスする場合、バックアップパスワードは変更されません。

ここでは、新しい VA ポッドを作成する方法を順を追って説明します。

始める前に

この手順を実行するには、AWS アカウントに管理者アクセス権限が必要です。詳細については、自動展開の前提条件 （58 ページ）を参照してください。

手順

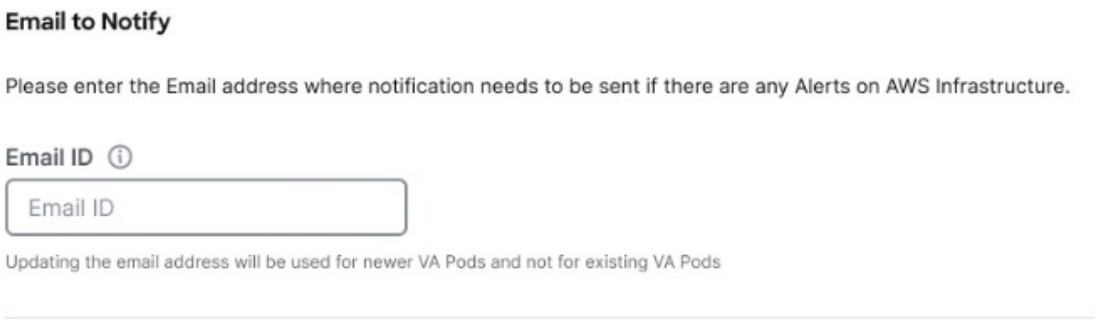
ステップ 1 次のいずれかの方法を使用して、Cisco DNA Center VA 起動パッドにログインします。

- [IAM Login]：この方法では、ユーザーロールを使用してユーザーアクセス権限を定義します。Cisco DNA Center VA 起動パッドは、企業が必要とする場合に、任意の追加認証形式としての多要素認証（MFA）をサポートします。詳細については、*Cisco DNA Center VA Launchpad 1.6 Administrator Guide* の「Log In to Cisco DNA Center VA 起動パッド Using IAM」[英語] を参照してください。
- [Federated Login]：この方法では、1 つのアイデンティティを使用して、他のオペレータが管理するネットワークまたはアプリケーションにアクセスします。詳細については、*Cisco DNA Center VA Launchpad 1.6 Administrator Guide* の「Generate Federated User Credentials Using saml2aws」または「Generate Federated User Credentials Using AWS CLI」[英語] を参照してください。

アクセスキー ID とシークレットアクセスキーを取得する方法については、AWS の Web サイトに掲載されている *AWS Tools for PowerShell* ユーザーガイド [英語] の 「AWS Account and Access Keys」を参照してください。

ログインエラーが発生した場合は、エラーを解決して再度ログインする必要があります。詳細については、展開のトラブルシューティング （91 ページ）を参照してください。

ステップ 2 初めてログインする管理者ユーザーの場合は、[Email ID] フィールドに電子メールアドレスを入力し、[Submit] をクリックします。サブユーザーの場合は、ステップ 3 に進みます。



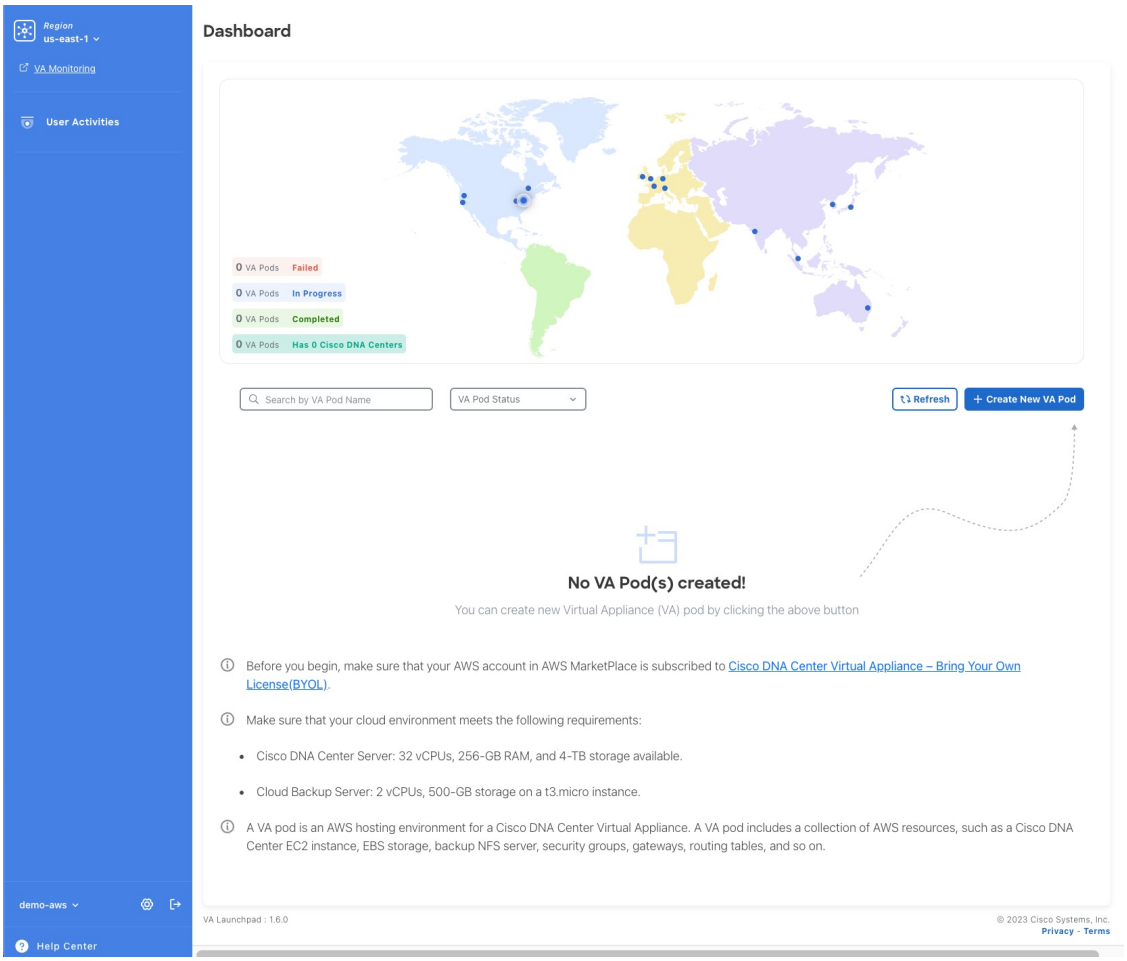
Amazon Simple Notification Service（SNS） に登録して、展開されたリソース、変更、およびリソースの過剰使用に関するアラートを受信できます。さらに、Amazon CloudWatch が Cisco DNA Center VA 起動パッド の異常な動作を検出した場合に通知するようにアラームを設定できます。さらに、AWS Config は設定されたリソースを評価し、結果の監査ログも送信します。詳細については、*Cisco DNA Center VA Launchpad 1.6 Administrator Guide* の「Subscribe to the アマゾンSNS Email Subscription」と「View Amazon CloudWatch Alarms」[英語] を参照してください。

電子メールを入力すると、いくつかのプロセスが実行されます。

- 必要なすべてのポリシーが割り当てられた CiscoDNACenter ユーザーグループが AWS アカウント上に作成されます。管理者ユーザーがこのグループにサブユーザーを追加すると、サブユーザーが Cisco DNA Center VA 起動パッド にログインできるようになります。
- Amazon S3 バケットは、展開の状態を保存するために自動的に作成されます。グローバルでも各リージョンでも、AWS アカウントから S3 バケットや他のバケットを削除しないことを推奨します。バケットを削除すると、Cisco DNA Center VA 起動パッド 展開ワークフローに影響を与える可能性があります。
- リージョンに初めてログインすると、Cisco DNA Center VA 起動パッド によって AWS で複数のリソースが作成されます。リージョンが以前に有効だったかどうかによって、このプロセスは時間がかかる場合があります。プロセスが完了するまで、新しい VA ポッドは作成できません。この間、「**Setting up the initial region configuration. This might take a couple of minutes.（初期リージョンを設定中です。この処理には数分かかる場合があります。）**」というメッセージが表示されます。

正常にログインすると、[**Dashboard**] ペインが表示されます。

（注） リージョンの設定を更新するように求められた場合は、プロンプトに従って更新を完了します。詳細については、*Cisco DNA Center VA Launchpad 1.6 Administrator Guide* の「Update a Region Setup」[英語] を参照してください。



ステップ 3 [+ Create New VA Pod] をクリックします。

ステップ 4 [Region Selection] ダイアログボックスで次の手順を実行して、新しい VA ポッドを作成するリージョンを選択します。

1. [Region] ドロップダウンリストから、リージョンを選択します。

   左側のナビゲーションウィンドウの [Region] ドロップダウンリストから 1 つのリージョンをすでに選択している場合は、そのリージョンが自動的に選択されます。

   （注） リージョンの設定を更新するように求められた場合は、プロンプトに従って更新を完了します。詳細については、*Cisco DNA Center VA Launchpad 1.6 Administrator Guide* の「Update a Region Setup」[英語] を参照してください。

2. [Next] をクリックします。

ステップ 5 次の手順を実行して、VPC、プライベートサブネット、ルーティングテーブル、セキュリティグループ、仮想ゲートウェイ、CGW を含む AWS インフラストラクチャを設定します。

a) [Environmental Details] フィールドで、次のフィールドを設定します。

- [VA Pod Name]：新しい VA ポッドに名前を割り当てます。次の制約事項に注意してください。
  - 名前はリージョン内で一意である必要があります（これは複数のリージョンで同じ名前を使用できることを意味します）。
  - 最大 12 文字までの名前を指定できます。
  - 名前には、文字（A〜Z）、数字（0〜9）、およびダッシュ（-）を含めることができます。
- [Availability Zone]：このドロップダウンリストをクリックして、選択したリージョン内の分離された場所である可用性ゾーンを選択します。
- [AWS VPC CIDR]：AWS リソースの起動に使用する一意の VPC サブネットを入力します。次の注意事項に従ってください。
  - 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。
  - このサブネットは、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。

b) [Transit Gateway (TGW)] で、次のいずれかのオプションを選択します。

- [VPN GW]：VA ポッドが 1 つあり、VPN ゲートウェイを使用する場合は、このオプションを選択します。VPN GW は、サイト間 VPN 接続の Amazon 側の VPN エンドポイントです。1 つの VPC にのみ接続できます。
- [New VPN GW + New TGW]：複数の VA ポッドまたは VPC があり、複数の VPC とオンプレミスネットワークを相互接続するトランジットハブとして TGW を使用する場合は、このオプションを選択します。また、TGW をサイト間 VPN 接続の Amazon 側の VPN エンドポイントとして使用することもできます。

  （注） リージョンごとに 1 つの TGW のみを作成できます。

- [Existing TGW]：新しい VA ポッドの作成に使用する既存の TGW がある場合は、このオプションを選択してから、次のいずれかのオプションを選択します。
  - [New VPN GW]：既存の TGW に新しい VPN ゲートウェイを作成する場合は、このオプションを選択します。
  - [Existing Attachment]：既存の VPN または直接接続アタッチメントを使用する場合は、このオプションを選択します。[Select Attachment ID] ドロップダウンリストから、アタッチメント ID を選択します。

このオプションを選択する場合は、既存の TGW および CGW のルーティングも設定する必要があります。詳細については、既存のトランジットゲートウェイおよびカスタマーゲートウェイでルーティングを手動設定する （84 ページ）を参照してください。

c) 次のいずれかを実行します。

- 優先する接続オプションとして [Existing TGW] と [Existing Attachments] を選択した場合は、ステップ 5 に進みます。
- [VPN GW]、[New VPN GW + New TGW]、または [Existing TGW + New VPN GW] を選択した場合は、次の VPN 詳細を入力します。
  - [Customer Gateway IP]：AWS VPN ゲートウェイとの IPSec トンネルを形成するためのエンタープライズ ファイアウォールまたはルータの IP アドレスを入力します。
  - [VPN Vendor]：ドロップダウンリストから VPN ベンダーを選択します。

    [Barracudo]、[Sophos]、[Vyatta]、および [Zyxel] は、サポートされていない VPN ベンダーです。詳細については、VA ポッド設定エラーのトラブルシュート （94 ページ）を参照してください。
  - [Platform]：ドロップダウンリストからプラットフォームを選択します。
  - [Software]：ドロップダウンリストからソフトウェアを選択します。

d) [Customer Profile] のサイズは、デフォルト設定の [Medium] のままにします。

カスタマープロファイルのサイズは、Cisco DNA Center VA インスタンスとバックアップ インスタンスの両方に適用されます。[Medium] を指定すると、インスタンスの構成は次のようになります。

- **Cisco DNA Center インスタンス**：r5a.8xlarge、32 個の vCPU、256 GB の RAM、4 TB ストレージ

  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 DNA Center VA 起動パッド Release 1.6.0*』[英語] を参照してください。

- **バックアップインスタンス**：T3.micro、2 個の vCPU、500 GB のストレージ、1 GB の RAM

e) [Backup Target] では、Cisco DNA Center のデータベースとファイルのバックアップ先として次のいずれかのオプションを選択します。

- [Enterprise Backup (NFS)]：バックアップをオンプレミスサーバーに保存する場合は、このオプションを選択します。

- [Cloud Backup (NFS)]：バックアップを AWS に保存する場合は、このオプションを選択します。

  次のバックアップの詳細をメモします。後でこの情報を使用して、クラウド バックアップ サーバーにログインします。

  - **SSH IPアドレス**：<BACKUP VM IP>
  - **SSH ポート**：22
  - **サーバーパス**：/var/dnac-backup/
  - **ユーザー名**：maglev
  - **パスワード**：<xxxx##########>

    バックアップサーバーのパスワードは動的に作成されます。パスワードは、バックアップインスタンスのスタック名の最初の 4 文字とバックアップサーバーの IP アドレス（ピリオドなし）で構成されます。

    たとえば、バックアップインスタンスのスタック名が DNAC-ABC-0123456789987 で、バックアップサーバーの IP アドレスが 10.0.0.1 の場合、バックアップサーバーのパスワードは DNAC10001 になります。

    （注）
    - バックアップインスタンスのスタック名は、[Cisco DNA Center Configuration In Progress] ウィンドウ（新しい Cisco DNA Center VA の作成 （85 ページ） のステップ 9 を参照）または **[AWS Console]** > **[CloudFormation]** > **[Stacks]** ウィンドウで確認できます。
    - バックアップサーバーの IP アドレスは、[Cisco DNA Center Configuration In Progress] ウィンドウ（新しい Cisco DNA Center VA の作成 （85 ページ） のステップ 9 を参照）または [Cisco DNA Center Virtual Appliance Details] ウィンドウ（*Cisco DNA Center VA Launchpad 1.6 Administrator Guide* の「View Cisco DNA Center VA Details」[英語] を参照）でも確認できます。

  - **パスフレーズ**：<Passphrase>

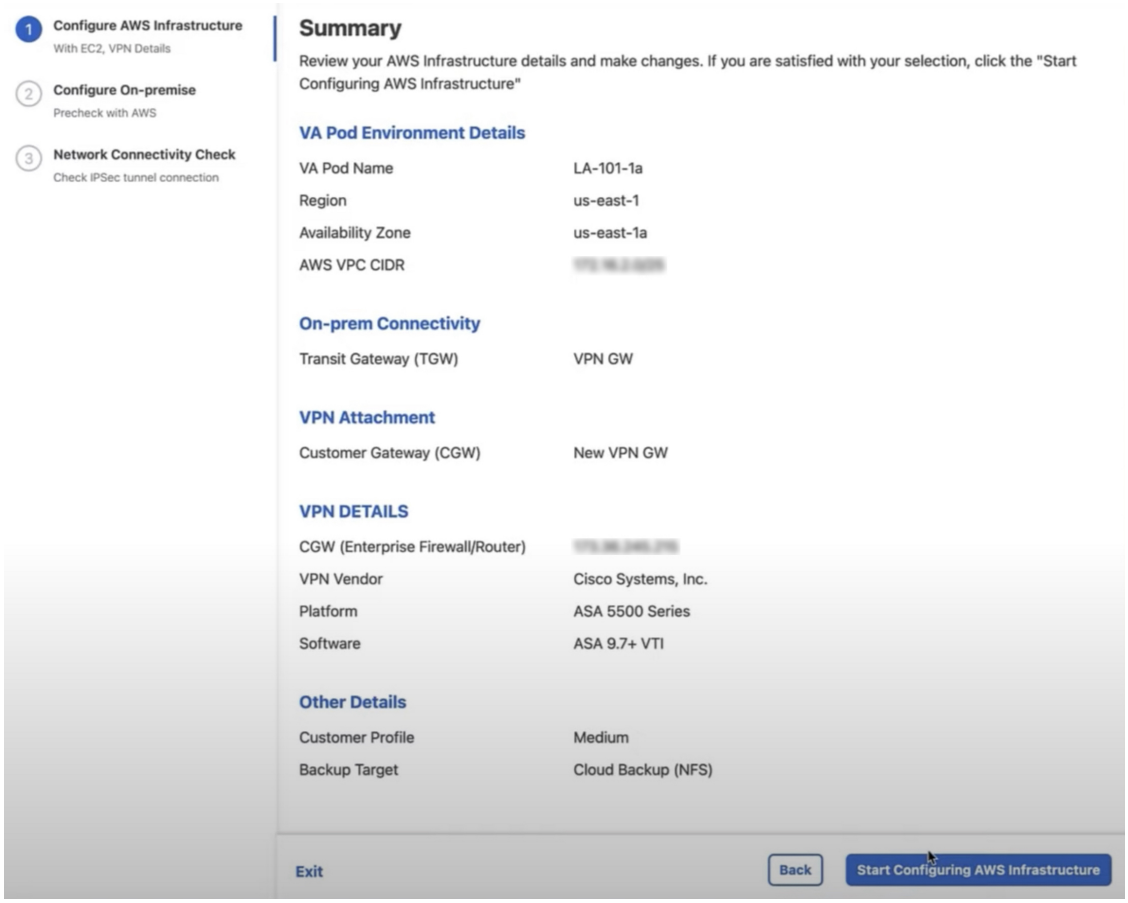
    パスフレーズは、バックアップのセキュリティの影響を受けやすいコンポーネントを暗号化するために使用されます。これらのセキュリティに影響を受けやすいコンポーネントには、証明書とクレデンシャルが含まれます。

    このパスフレーズは必須で、バックアップファイルを復元するときに入力を求められます。このパスフレーズがなければ、バックアップファイルは復元されません。

  - **オープンポート**：22、2049、873、111

f) [Next] をクリックします。

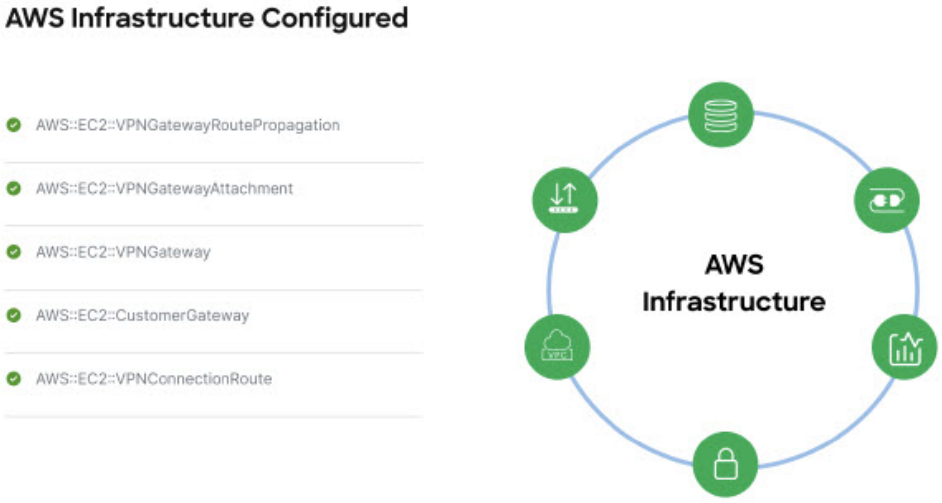
[Summary] ペインが表示されます。



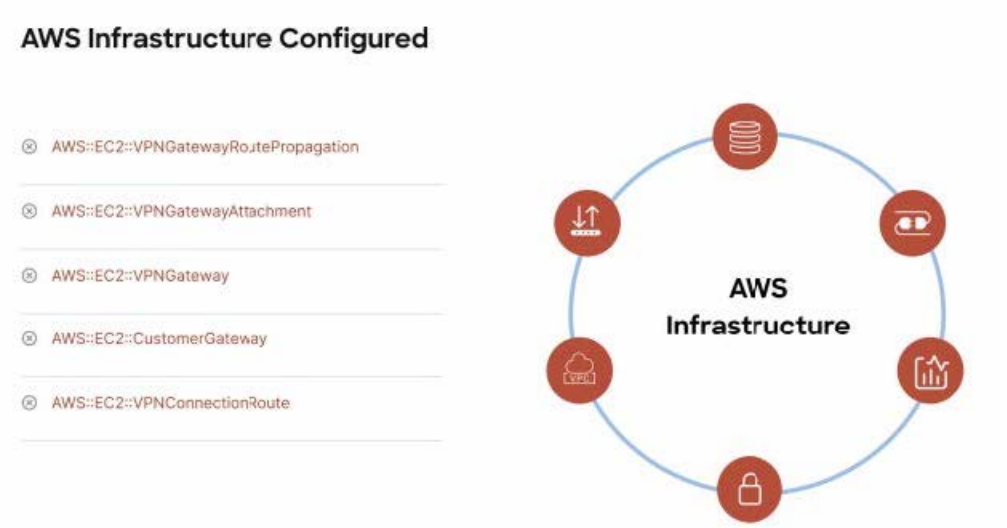
g) 環境と VPN の入力内容を確認します。問題がなければ、[Start Configuring AWS Environment] をクリックします。

重要 設定が完了するまで約 20 分かかります。アプリケーションを終了したり、このウィンドウやタブを閉じたりしないでください。さもないと、設定が一時停止します。

h) AWS インフラストラクチャが正しく設定されると、[AWS Infrastructure Configured] ペインが表示されます。



AWS インフラストラクチャの設定に失敗した場合は、Cisco DNA Center VA 起動パッドを終了します。考えられる原因と解決策については、展開のトラブルシューティング （91 ページ）を参照してください。



ステップ 6 次の手順を実行して、オンプレミス構成ファイルをダウンロードします。

a) AWS インフラストラクチャが正しく設定されたら、[Proceed to On-Prem Configuration] をクリックします。

b) [Configure On-premise] ペインで、[Download Configuration File] をクリックします。このファイルをネットワーク管理者に転送して、オンプレミス側の IPSec トンネルを設定します。

ネットワーク管理者が IPSec トンネルを 1 つだけ設定していることを確認してください。

（注）
- ネットワーク管理者がこの構成ファイルに必要な変更を加えてからエンタープライズ ファイアウォールまたはルータに適用すると、IPSec トンネルを起動できます。

  提供されている構成ファイルを使用すると、AWS とエンタープライズルータまたはファイアウォールの間で 2 つのトンネルを起動できます。

- ほとんどの仮想プライベート ゲートウェイ ソリューションでは、1 つのトンネルが稼働し、もう 1 つのトンネルが停止しています。両方のトンネルを稼働すると、等コストマルチパス（ECMP）ネットワーキング機能を使用できます。ECMP 処理では、ファイアウォールまたはルータが等コストルートを使用して同じ宛先にトラフィックを送信できます。このとき、ルータまたはファイアウォールが ECMP をサポートしている必要があります。ECMP を使用しない場合は、1 つのトンネルを停止して手動でフェールオーバーするか、または IP SLA などのソリューションを使用して、フェールオーバーシナリオでトンネルを自動的に起動することを推奨します。

c) [Proceed to Network Connectivity Check] ボタンをクリックします。

ステップ 7 次のいずれかのアクションを実行して、AWS インフラストラクチャの設定時に選択した優先するオンプレミス接続に基づいて、ネットワーク構成のステータスを確認します。

- 優先するオンプレミス接続オプションとして [VPN GW] を選択した場合、IPSec トンネルの設定ステータスが次のように表示されます。
  - ネットワーク管理者が IPSec トンネルをまだ設定していない場合は、IPSec トンネルに鍵アイコンが表示されます。

  - エンタープライズ ファイアウォールまたはルータの IPSec トンネルが稼働していることを確認するようにネットワーク管理者に依頼します。IPSec トンネルが稼働すると、IPSec トンネルが緑色に変わります。

（注） IPsec トンネルが稼働状態になっているのに、CGW から Cisco DNA Center にアクセスできない場合は、IPsec トンネルの設定中に正しい値が渡されたことを確認します。Cisco Global Launchpad は AWS 由来のトンネルステータスを報告し、追加のチェックを実行しません。

- 優先するオンプレミス接続オプションとして [New VPN GW + New TGW] または [Existing TGW and New VPN GW] を選択した場合、Cisco DNA Center VA 起動パッドは、VPC が TGW に接続されているかどうかを確認し、TGW はオンプレミスのファイアウォールまたはルータに接続されます。

（注） TGW からエンタープライズ ファイアウォールまたはルータへの接続に成功するには、ネットワーク管理者がオンプレミスのファイアウォールまたはルータにこの設定を追加する必要があります。

接続ステータスは次のように表示されます。

- TGW からオンプレミスのファイアウォールまたはルータへの接続が確立されていない場合は、グレー表示されます。

- TGW 接続が正常に確立されると、TGW 接続は緑色になります。

- 優先するオンプレミス接続オプションとして [Existing TGW] と [Existing Attachment] を選択した場合は、既存の TGW と新しく接続された VPC の間でルーティングが設定されていることを確認します。ここで Cisco DNA Center が起動されます。詳細については、既存のトランジットゲートウェイおよびカスタマーゲートウェイでルーティングを手動設定する（84 ページ）を参照してください。

  接続ステータスは次のように表示されます。

  - VPC が TGW に接続されていない場合、TGW 接続はグレー表示されます。

  - TGW 接続が正常に確立されると、TGW 接続は緑色になります。

ステップ 8 [Go to Dashboard] をクリックして [**Dashboard**] ペインに戻ります。ここで、追加の VA ポッドを作成したり、既存の VA ポッドを管理したりすることができます。

既存のトランジットゲートウェイおよびカスタマーゲートウェイでルーティングを手動設定する

新しい VA ポッドの作成時に、優先する接続オプションとして [Existing Transit Gateway] と [Existing Attachments] を選択した場合、Cisco DNA Center VA 起動パッド では Cisco DNA Center を起動するための VPC が作成され、この VPC が既存の TGW に接続されます。

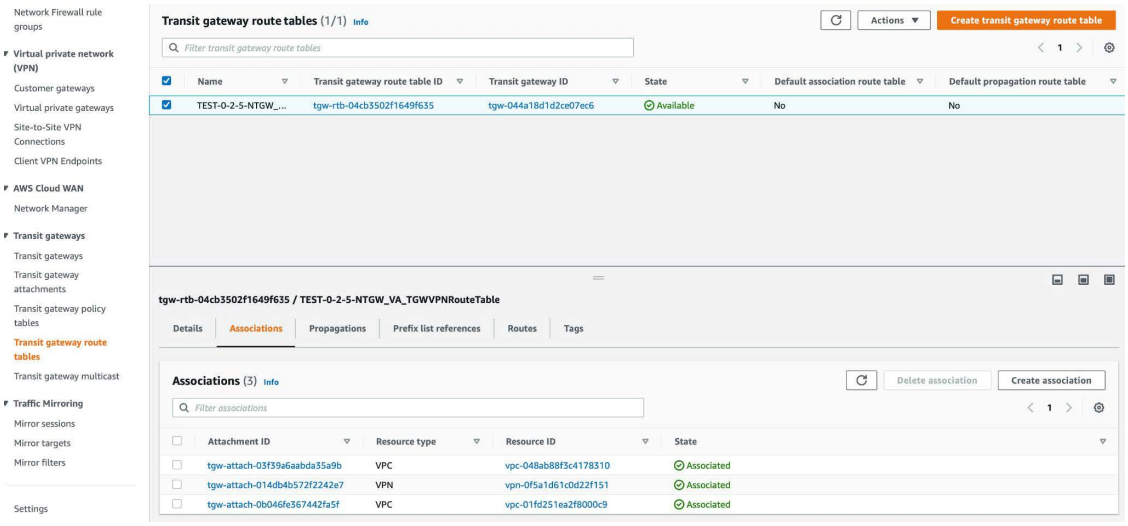
Cisco DNA Center VA 起動パッド で TGW 接続を確立するには、AWS で TGW ルーティングテーブルを手動で設定し、既存の CGW にそのルーティング設定を追加する必要があります。

手順

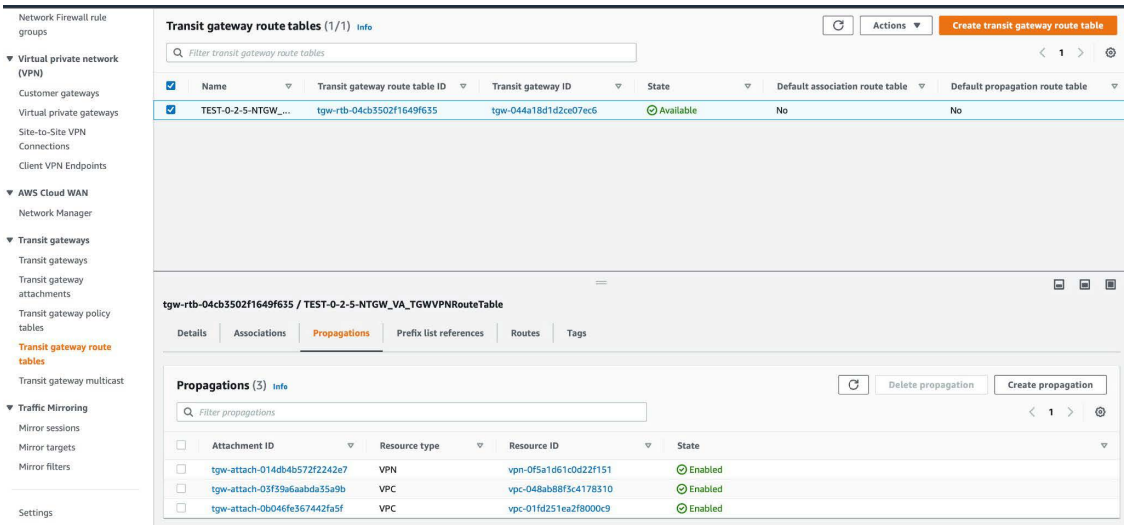
ステップ 1 AWS コンソールから、[VPC service] に移動します。

ステップ 2 左側のナビゲーションウィンドウの [Transit Gateways] で [Transit gateway route table] を選択し、次に既存の TGW ルートテーブルを選択します。

ステップ 3 [Transit gateway route table] ウィンドウで [Associations] タブをクリックし、次に [Create Association] をクリックします。



ステップ 4 [Transit gateway route table] ウィンドウで [Propagations] タブをクリックし、次に [Create propagation] をクリックします。



ステップ 5 それぞれの VPC と VPN 間でスタティックルートを確実にアクティブにするには、[Routes] タブをクリックし、次に [Create static route] をクリックします。

ステップ 6 AWS 環境の CGW に割り当てられた CIDR 範囲に向けてネットワークトラフィックをルーティングするように、オンプレミスルータの設定が更新されていることを確認します。

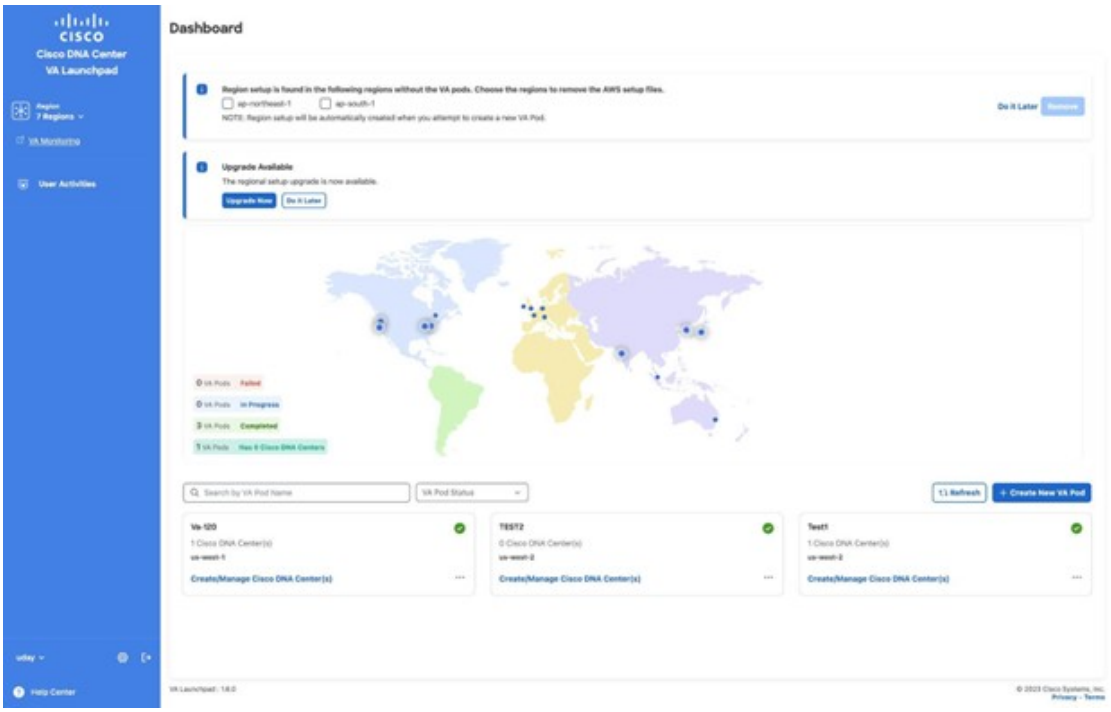
例：`route tunnel-int-vpn-0b57b508d80a07291-1 10.0.0.0 255.255.0.0 192.168.44.37 200`

新しい Cisco DNA Center VA の作成

次の手順に従って、新しい Cisco DNA Center VA を設定します。

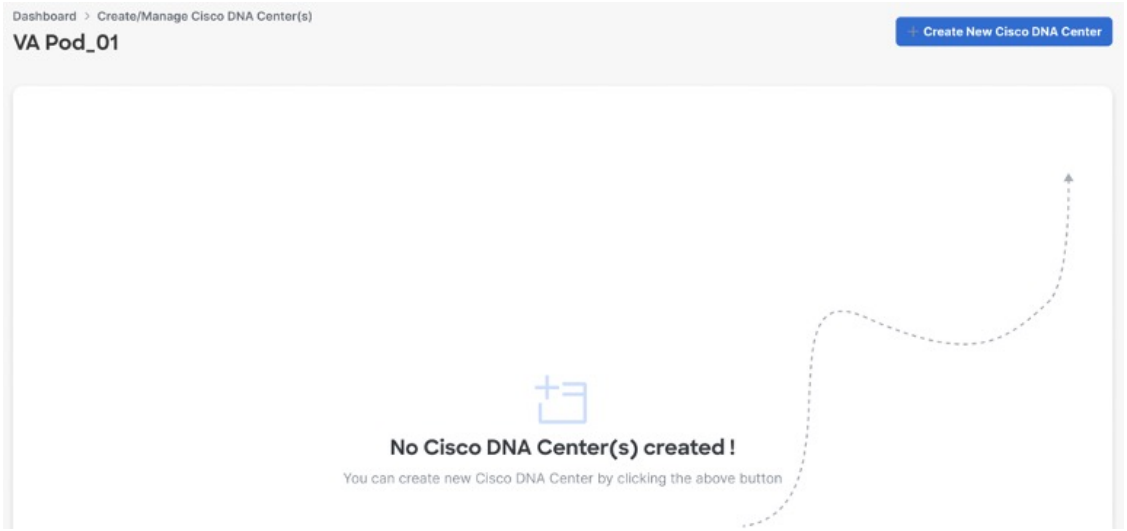
手順

ステップ 1 [**Dashboard**] ペインのマップの下で、Cisco DNA Center VA を作成する VA ポッドを見つけます。



ステップ 2 VA ポッドカードで、[Create/Manage Cisco DNA Center(s)] をクリックします。

ステップ 3 [Create/Manage Cisco DNA Center(s)] ペインで、[+ Create New Cisco DNA Center] をクリックします。



ステップ 4 次の詳細を入力します。

- [Cisco DNA Center Version]：ドロップダウンリストから、Cisco DNA Center バージョンを選択します。

- [Enterprise DNS]：エンタープライズ DNS の IP アドレスを入力します。このエンタープライズ DNS が、Cisco DNA Center VA を作成する VA ポッドから到達可能であることを確認してください。

  （注） Cisco DNA Center VA Launchpad は、UDP ポート 53 と入力した DNS サーバーの IP アドレスを使用して、オンプレミスのネットワーク接続を確認します。

- [FQDN (Fully Qualified Domain Name)]：DNS サーバーで設定されている Cisco DNA Center VA の IP アドレスを入力します。
- [Proxy Details]：次のいずれかの HTTPS ネットワーク プロキシ オプションを選択します。
  - [No Proxy]：プロキシサーバーは使用されません。
  - [Unauthenticated]：プロキシサーバーは認証を必要としません。プロキシサーバーの URL とポート番号を入力します。
  - [Proxy Authentication]：プロキシサーバーは認証を必要とします。プロキシサーバーの URL、ポート番号、ユーザー名、およびパスワードの詳細を入力します。
- [Cisco DNA Center Virtual Appliance Credentials]：Cisco DNA Center VA へのログインに使用する CLI パスワードを入力します。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）

  後で参照できるように、このパスワードを保存しておいてください。

  （注） ユーザー名は maglev です。

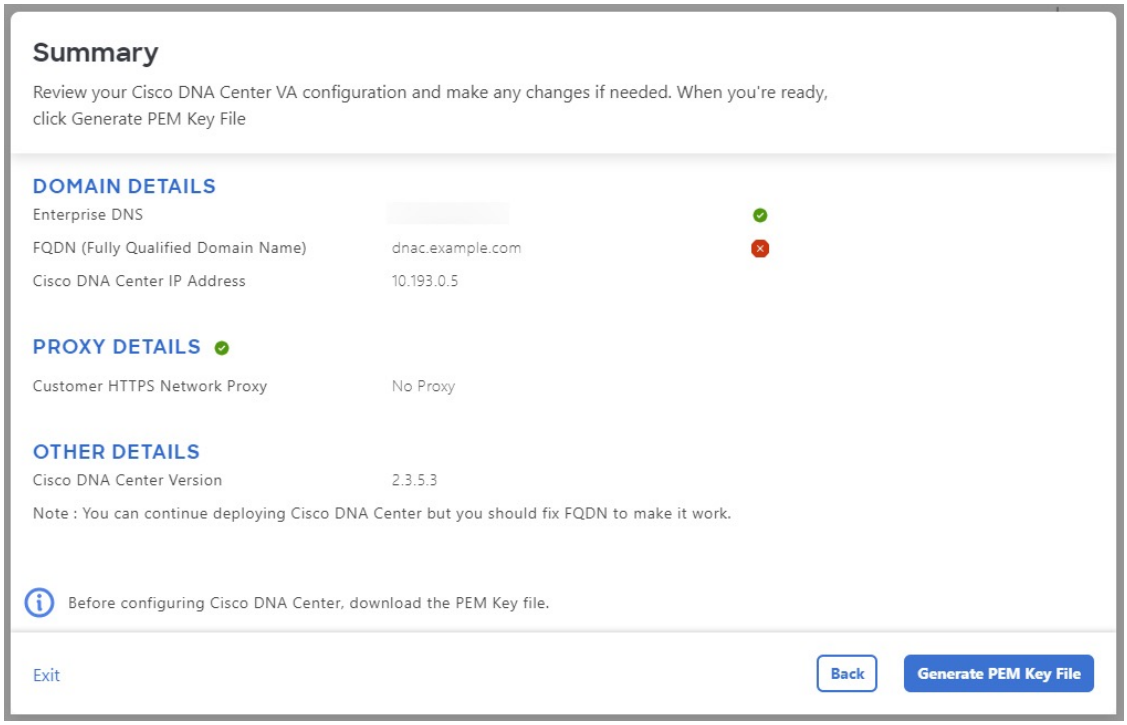
ステップ 5 [Validate] をクリックして、DNS サーバーに設定されているエンタープライズ DNS サーバーと FQDN を検証します。

（注） Cisco DNA Center VA Launchpad のリリース 1.6.0 で、DNS サーバー、プロキシサーバー、またはFQDNのチェックに失敗した場合は、次の手順に従って設定を続行します。

- DNS サーバーの検証に失敗した場合は、Cisco DNA Center VA の作成を続行できません。入力した DNS サーバーの IP アドレスが VA ポッドから到達可能であることを確認してください。
- プロキシサーバーの検証に失敗した場合でも、設定を続行できます。無効なプロキシの詳細が修正されなくても、Cisco DNA Center VA は機能します。
- FQDN の検証に失敗した場合でも、Cisco DNA Center VA の作成を続行できます。ただし、Cisco DNA Center VA を機能させるには、FQDN 設定を修正する必要があります。

ステップ 6 [Summary] ウィンドウで、設定の詳細を確認します。

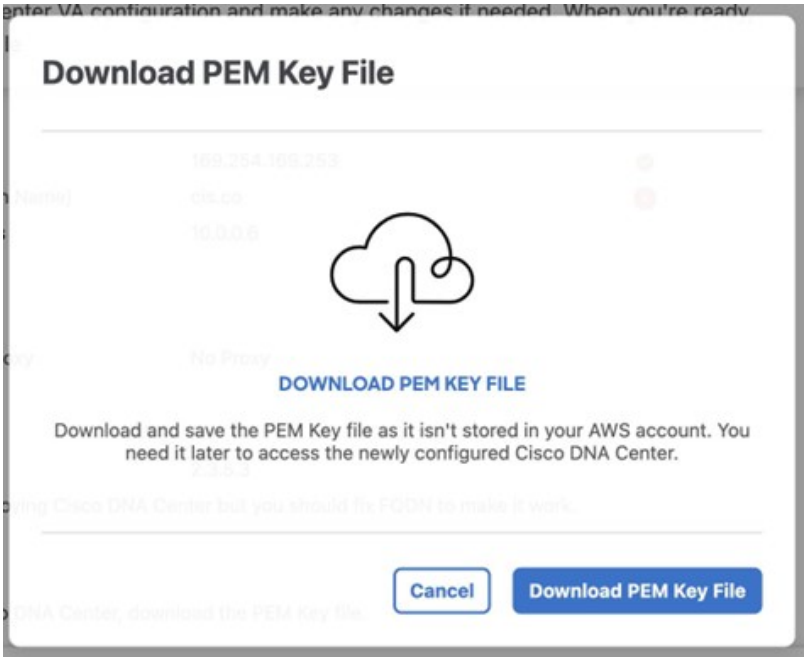
（注） Cisco DNA Center の IP アドレスは静的に割り当てられた IP アドレスであり、中断のない接続を確保し、重要なネットワーク運用中の障害を最小限に抑えるため、AWS 可用性ゾーンの停止後もそのままに保たれます。



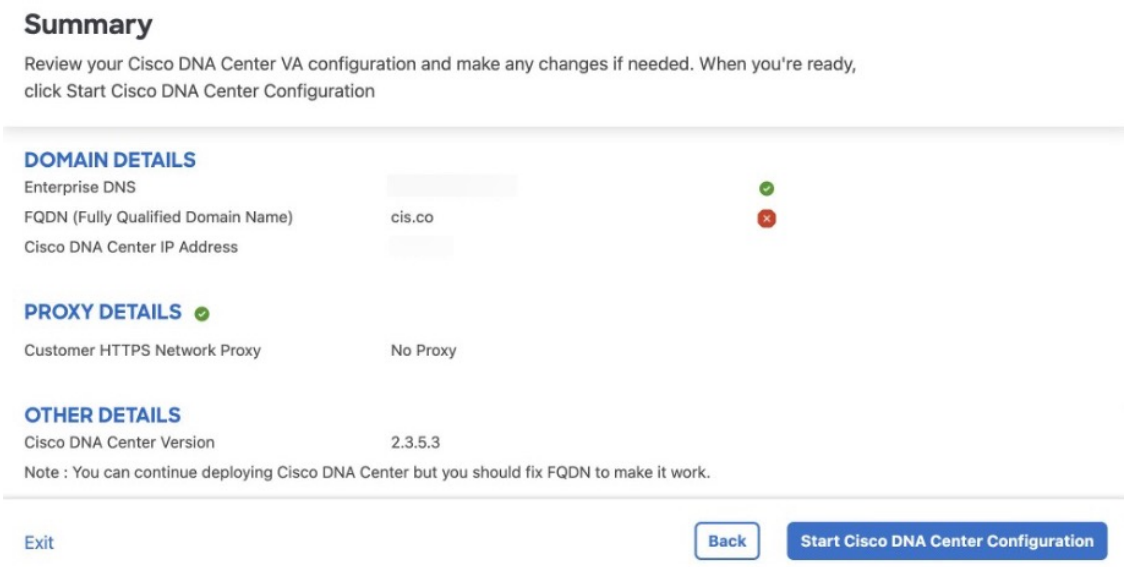
ステップ 7 設定に問題がない場合は、[Generate PEM Key File] をクリックします。

ステップ 8 [Download PEM Key File] ダイアログボックスで、[Download PEM Key File] をクリックします。[Cancel] をクリックすると、[Summary] ウィンドウに戻ります。

重要 PEM キーは AWS アカウントに保存されていないため、ダウンロードする必要があります。作成されている Cisco DNA Center VA にアクセスするには、PEM キーが必要です。



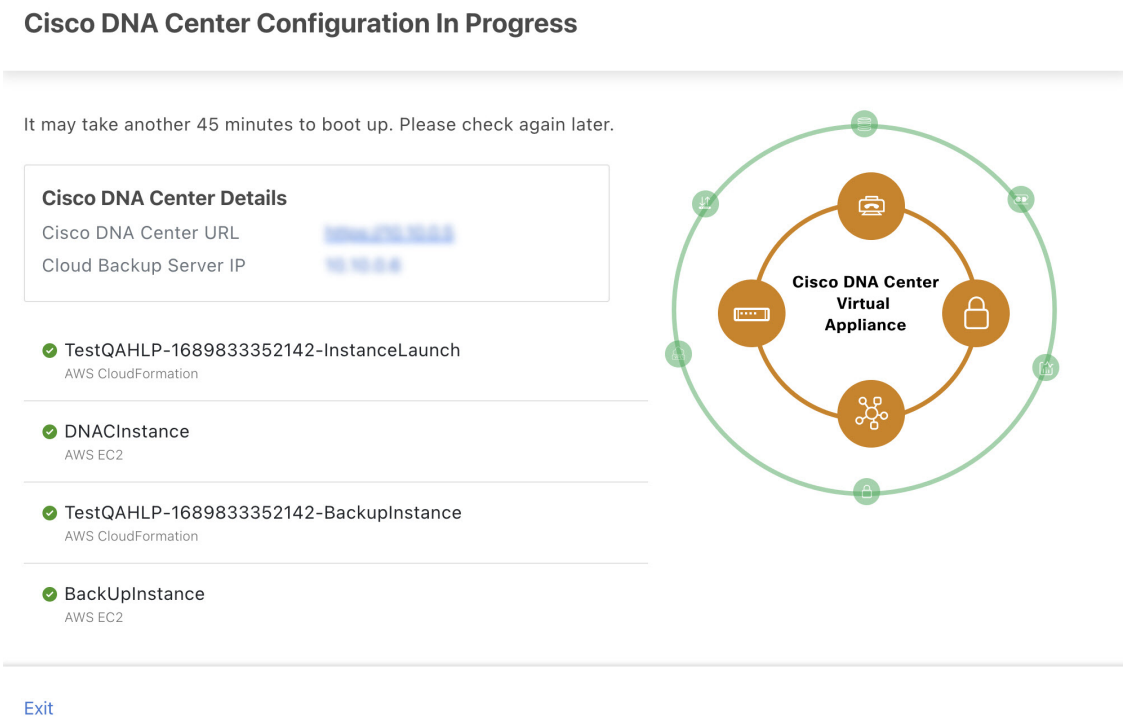
ステップ 9 PEM ファイルをダウンロードしたら、[Start Cisco DNA Center Configuration] をクリックします。



Cisco DNA Center VA Launchpad により、Cisco DNA Center 環境が設定されます。環境が設定されると、Cisco DNA Center が起動します。最初は、Cisco DNA Center VA 起動パットの外側のリングが灰色で表示されます。ポート 2222 が検証されると、イメージがオレンジに変わります。ポート 443 が検証されると、イメージが緑色に変わります。

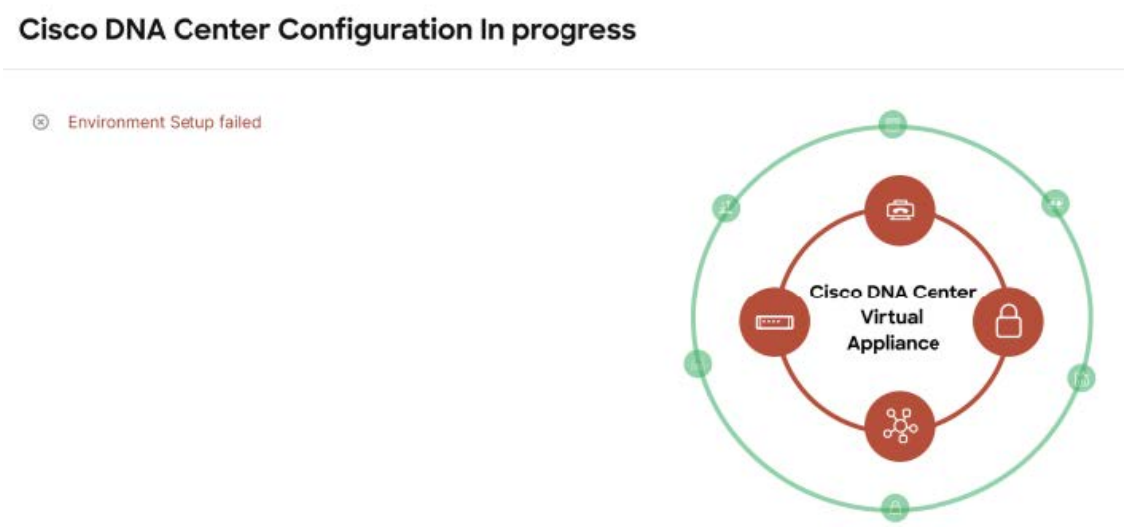
（注） このプロセスは 45 ～ 60 分かかります。アプリケーションを終了したり、このウィンドウやタブを閉じたりしないでください。さもないと、設定が一時停止します。

Cisco DNA Center が起動すると、設定は完了です。Cisco DNA Center VA の詳細を表示できるようになりました。



ヒント [Cisco DNA Center Configuration In Progress] ウィンドウが表示されている間に、バックアップサーバーの IP アドレスとバックアップインスタンスのスタック名を後で使用できるように記録します。バックアップサーバーのパスワードは、バックアップインスタンスのスタック名の最初の 4 文字とバックアップサーバーの IP アドレス（ピリオドを除く）を組み合わせたものです。

Cisco DNA Center の設定に失敗した場合は、[Create/Manage Cisco DNA Center(s)] ペインに戻ります。詳細については、展開のトラブルシューティング （91 ページ）を参照してください。



ステップ 10 [Create/Manage Cisco DNA Center(s)] ペインに戻るには、[Go to Manage Cisco DNA Center(s)] をクリックします。

展開のトラブルシューティング

Cisco DNA Center VA 起動パッドは、最小限の介入で AWS に Cisco DNA Center をシームレスに設定できるように設計されています。ここでは、AWS での Cisco DNA Center の展開時の一般的な問題をトラブルシュートする方法について説明します。

（注） Cisco DNA Center VA 起動パッドでは解決できない問題が発生する可能性があるため、AWS コンソールを介して Cisco DNA Center VA 起動パッドでワークフローを手動で変更することは推奨できません。

ここに記載されていない問題がある場合は、Cisco TAC にご連絡ください。

Docker エラーのトラブルシュート

Cisco DNA Center VA 起動パッドの Docker イメージの実行中に「`port is already in use`」というエラーメッセージが表示された場合は、考えられる次の解決策を使用してトラブルシュートできます。

エラー	考えられる解決策
サーバーアプリケーションの実行中に次のエラーが表示された場合： port is already in use（ポートがすでに使用されています）	Docker でサーバーアプリケーションを実行します。 **docker run -d -p** <server-port-number>**:8080 -e SECRET_KEY=**<your-secret-key> **--name server --pull=always dockerhub.cisco.com/maglev-docker/server:x.x.x-latest** （注） 使用可能なサーバーポートをどれでも使用できます。 サーバーアプリケーションの実行中に、クライアント アプリケーションを実行します。 **docker run -d -p 90:80 -e REACT_APP_API_URL=http://localhost:**<client-port-number> **--name client --pull=always dockerhub.cisco.com/maglev-docker/client:x.x.x** （注） サーバーアプリケーションの実行で使用したものと同じポート番号を使用する必要があります。
クライアント アプリケーションの実行中に次のエラーが表示された場合： port is already in use（ポートがすでに使用されています）	Docker でクライアント アプリケーションを実行します。 **docker run -d -p** <client-port-name>**:80 --name client --pull=always dockerhub.cisco.com/maglev-docker/client:x.x.x** （注） 使用可能なサーバーポートをどれでも使用できます。

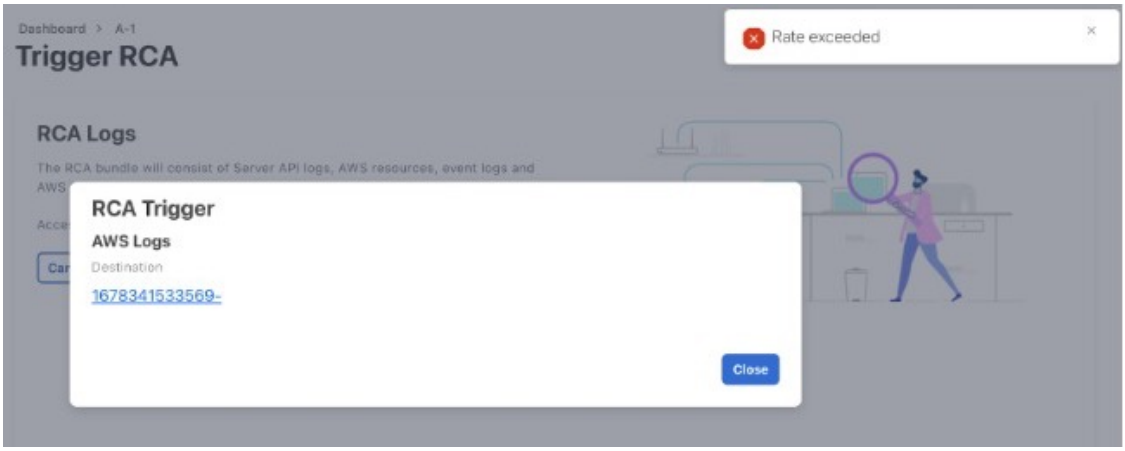
ログインエラーのトラブルシュート

Cisco DNA Center VA 起動パッドにログインする際に、ログインエラーが発生する場合があります。考えられる次の解決策を使用して、一般的なログインエラーをトラブルシュートできます。

エラー	考えられる解決策
Invalid credentials.（無効なログイン情報です。）	ログイン情報を再入力し、正しく入力されていることを確認します。
You don't have enough access.（十分なアクセス権がありません。）	管理者ユーザーの場合は、アカウントに管理者アクセス権があることを確認します。 サブユーザーの場合は、管理者によって CiscoDNACenter ユーザーグループに追加されていることを確認します。
An operation to delete is in progress, please try again after some time.（削除操作が進行中です。しばらくしてからもう一度お試しください。）	管理者ユーザーが AWS アカウントから <AccountId>-cisco-dna-center グローバルバケットを削除した後にログインしようとすると、このログインエラーが発生することがあります。削除が完了するまで 5 分待ちます。

ホステッド型 Cisco DNA Center VA 起動パッド エラーのトラブルシューティング

ホステッド型 Cisco DNA Center VA 起動パッド では、根本原因分析（RCA）をトリガーすると、**レート超過**エラーが発生する可能性があります。このエラーが発生すると、次のバナーが表示されます。



このエラーバナーは、1 つのリージョンで最大数の API 要求（1 秒あたり 10,000）を受信した場合に表示されます。このエラーを解決するには、サービスクォータを使用して AWS の制限値を増やすか、数秒後に操作を再試行します。

リージョンに関する問題のトラブルシュート

考えられる次の解決策を使用して、リージョンに関する問題をトラブルシュートできます。

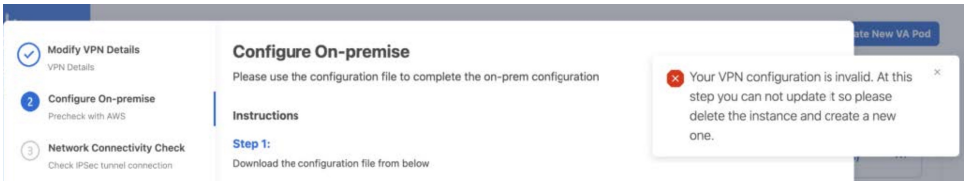
問題	考えられる解決策
新しいリージョンで新しい VA ポッドを作成しているときに、Cisco DNA Center VA 起動パッドにエラーメッセージが表示されるか、画面が 5 分を超えてフリーズし、設定中であることを示すメッセージが表示されません。	AWS コンソールでの手動プロセスが正常に完了したことを確認してから、この手順を再試行してください。問題が解決しない場合は、TAC にご連絡ください。 （注） このような競合状態を回避するため、VA ポッドを手動で変更しないことを推奨します。代わりに、すべてのアクションに Cisco DNA Center VA 起動パッド を使用してください。

問題	考えられる解決策
リージョンのセットアップが失敗し、Cisco DNA Center VA 起動パッドに次のような [Bucket [name] did not stabilize] エラーが表示されます。 Bucket 059356112352-cisco-dna-center-eu-south-1.va.storage did not stabilize	AWS でケースを開き、失敗したリソースをバックエンドから削除するように依頼します。

VA ポッド設定エラーのトラブルシュート

考えられる次の解決策を使用して、VA ポッド設定エラーをトラブルシューティングできます。

エラー	考えられる解決策
+ Create VA Pod button disabled（[+ Create VA Pod] ボタンが無効です）	無効になっているボタンにカーソルを合わせると、無効になっている理由の詳細が表示されます。 新しい VA ポッドを作成できない理由として、次のことが考えられます。 • **VPC サービスクォータの上限数に達した**：すべてのリージョンにおいて、作成できる VPC 数の上限が AWS 管理者によって設定されています。通常、リージョンごとに 5 つの VPC があり、各 VPC に VA ポッドを 1 つだけ配置できます。ただし、正確な数値については、AWS 管理者にお問い合わせください。 Cisco DNA Center VA 起動パッド以外のリソースに使用される VPC も、この上限数に含まれることに注意してください。たとえば、AWS アカウントに設定された VPC の上限が 5 つで、そのうち 2 つが使用中の場合、選択したリージョンでさらに作成できる VA ポッドは 3 つまでです。 新しい VA ポッドを作成するには、AWS 管理者に上限数の変更を依頼するか、AWS アカウントで既存の VA ポッドまたは VPC の一部を削除します。詳細については、AWS の Web サイトで『*AWS Support User Guide*』の AWS「Creating a service quota increase」[英語] のトピックを参照してください。 • **ポッドの削除が進行中**：リージョン内の最後の VA ポッドの削除が進行中です。数分待ってから、新しい VA ポッドの作成を再試行します。
AMI ID for this region is not available for your account.（このリージョンの AMI IDは、お使いのアカウントでは使用できません。）	[+ Create New VA Pod] をクリックすると、Cisco DNA Center VA 起動パッドは選択したリージョンの AMI ID を検証します。 このエラーが発生した場合、検証に失敗しており、このリージョンで新しいポッドを作成できません。この問題を解決するには、Cisco TAC にご連絡ください。

エラー	考えられる解決策
Your VPN configuration is invalid. At this step you cannot update it so please delete the instance and create a new one.（VPN の設定が無効です。このステップでは設定を更新できないため、インスタンスを削除してから新しいインスタンスを作成してください。）	VA ポッドを設定する場合、次の VPN ベンダーはサポートされません。 • **Barracuda** • **Sophos** • **Vyatta** • **Zyxel** サポートされていないVPNベンダーを使用している場合は、次のエラーメッセージが Cisco DNA Center VA 起動パッド に表示されます。 
CustomerGateway with type "ipsec.1", ip-address "xx.xx.xx.xx", and bgp-asn "65000" already exists (RequestToken: f78ad45d-b4f8-d02b-9040-f29e5f5f86cf, HandlerErrorCode: AlreadyExists)（タイプ「ipsec.1」、IP アドレス「xx.xx.xx.xx」、 bgp-asn「65000」のカスタマーゲートウェイはすでに存在します）	一度に複数の VA ポッドを作成しようとすると、このエラーが発生する可能性があります。 このエラーを解決するには、障害が発生した VA ポッドを削除して再作成します。一度に 1 つの VA ポッドのみを作成するようにしてください。
AWS Infrastructure Failed.（AWSインフラストラクチャで障害が発生しました。）	AWS の設定に失敗した場合は、[**Dashboard**] ペインに戻り、新しい VA ポッドを作成します。詳細については、新しい VA ポッドの作成 （72 ページ）を参照してください。 （注） 設定に失敗した VA ポッドを削除できます。
AWS Configuration fails when editing a VA Pod（VA ポッドの編集中に AWS の設定に失敗しました）	AWS コンソールでの手動プロセスが正常に完了したことを確認し、この手順を再試行してください。問題が解決しない場合は、TAC にご連絡ください。 （注） このような競合状態を回避するには、VA ポッドを手動で変更しないことを推奨します。代わりに、すべてのアクションに Cisco DNA Center VA 起動パッド を使用してください。
Deleting VA Pod has failed（VA ポッドの削除に失敗しました）	AWS コンソールでの手動プロセスが正常に完了したことを確認し、この手順を再試行してください。問題が解決しない場合は、TAC にご連絡ください。 （注） このような競合状態を回避するには、VA ポッドを手動で変更しないことを推奨します。代わりに、すべてのアクションに Cisco DNA Center VA 起動パッド を使用してください。

エラー	考えられる解決策
The resource you are trying to delete has been modified recently. Please refresh the page get the latest changes and try again.（削除しようとしているリソースは最近変更されました。ページを更新して最新の変更内容を表示してから、もう一度お試しください。）	VA ポッドの削除中にこのエラーが発生した場合は、Cisco TAC にご連絡ください。

ネットワーク接続エラーのトラブルシュート

VA ポッドの作成中に IPSec トンネルや TGW 接続が確立されていない場合は、オンプレミスのファイアウォールまたはルータでトンネルが稼働していることを確認します。

VA ポッドから TGW へのトンネルが緑色で、TGW から CGW へのトンネルが灰色の場合は、次のことを確認します。

- 正しい構成ファイルがネットワーク管理者に転送されている。
- ネットワーク管理者が構成ファイルに必要な変更を加えている。
- ネットワーク管理者がエンタープライズファイアウォールやルータに対してこの構成を適用している。
- 優先するネットワーク接続として [Existing TGW] と [Existing Attachments] を選択した場合は、既存のトランジットゲートウェイおよびカスタマーゲートウェイでルーティングを手動設定する （84 ページ） に正しく従っていることを確認してください。

Cisco DNA Center VA 設定エラーのトラブルシュート

考えられる次の解決策を使用して、Cisco DNA Center VA の設定中に発生したエラーをトラブルシュートできます。

エラー	考えられる解決策
Environment Setup failed（環境設定に失敗しました）	**1.** Cisco DNA Center VA 起動パッド の [Create/Manage Cisco DNA Center(s)] ペインに戻ります。 **2.** Cisco DNA Center VA を削除します。 **3.** 新しい Cisco DNA Center VA を作成します。
Delete Failed（削除に失敗しました）	Cisco DNA Center VA の削除に失敗した場合は、Cisco TAC にご連絡ください。

同時実行エラーのトラブルシュート

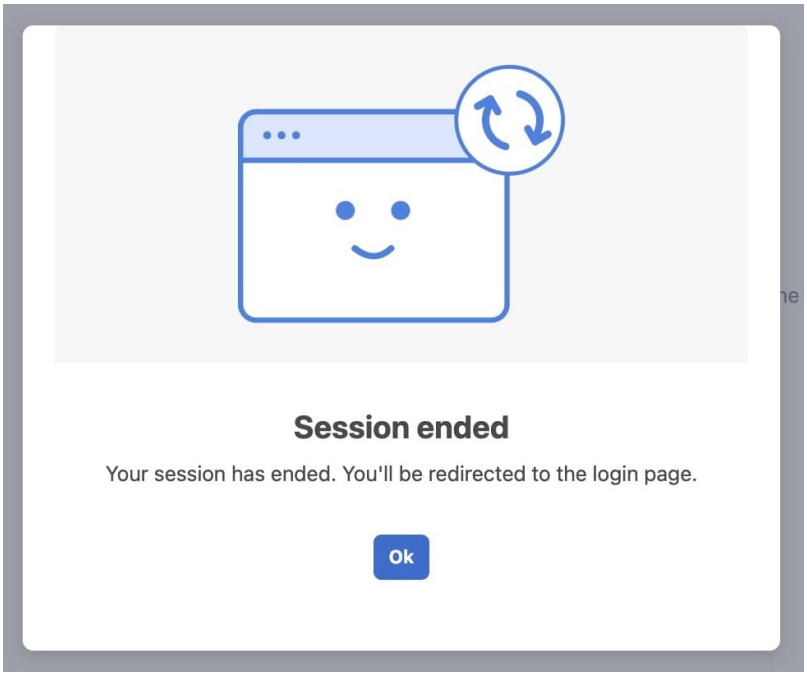
考えられる次の解決策を使用して、同時実行エラーをトラブルシュートします。

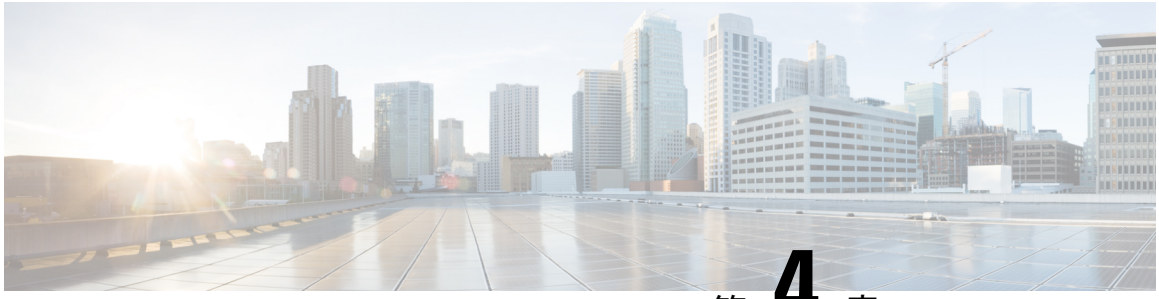
エラー	考えられる解決策
Unable to delete a Pod or a Cisco DNA Center created by another user.（別のユーザーが作成したポッドや Cisco DNA Center は削除できません。）	別のユーザーが作成した VA ポッドや Cisco DNA Center VA などコンポーネントは、そのコンポーネントで別のアクションが進行中は削除できません。アクションが完了すると、自分または他のユーザーがそのコンポーネントを削除できます。 たとえば、VA ポッドや Cisco DNA Center VA が次のプロセス中または状態にある場合は削除できません。 • 別のユーザーが Cisco DNA Center VA を作成中である。 • 別のユーザーが Cisco DNA Center VA を削除中である。 • 削除を試行して、Cisco DNA Center VA がエラー状態である。
The status of a Pod has been changed recently.（ポッドのステータスが最近変更されました。）	VA ポッドを削除しようとした場合、VA ポッドを作成した元のユーザーアカウントが同時アクションを実行した可能性があります。このような同時実行の問題が発生すると、選択した VA ポッドのステータスが変更されます。 VA ポッドの更新されたステータスを表示するには、[Refresh] をクリックします。

展開に関するその他の問題のトラブルシュート

考えられる次の解決策を使用して、AWS での Cisco DNA Center VA の展開中に発生した他の問題をトラブルシュートできます。

問題	考えられる原因と解決策
リソースは緑色だが、**[Proceed]** ボタンが無効になる。	一部の手順は、すべてのリソースが正常にセットアップされている場合にのみ続行できます。展開の完全性を確保するため、セットアップが完了し、すべてのリソースが設定およびロードされるまで、[Proceed] ボタンは無効のままになります。 リソースが正常にセットアップされたことが画面に表示されても、[Proceed] ボタンが無効のままになることがあります。この場合、一部のリソースがロードされるまでさらに数秒待つ必要があります。すべてのリソースが設定およびロードされると、[Proceed] ボタンが有効になります。
1 つのリージョンで同じ **CGW** を持つ複数の **VA** ポッドを展開するとエラーが発生する。	次のことを確認してください。 • CGW IP アドレスがエンタープライズ ファイアウォールまたはルータの IP アドレスであること。 • CGW IP アドレスが有効なパブリックアドレスであること。 • CGW IPアドレスが同じリージョン内の別の VA ポッドに使用されていないこと。現在、各リージョンでは、複数の VA ポッドが同じ CGW IP アドレスを持つことはできません。複数の VA ポッドで同じ CGW IP アドレスを使用するには、各 VA ポッドを異なるリージョンに展開してください。
Cisco DNA Center VA に **SSH** または **ping** を実行できない。	トンネルが稼働しており、アプリケーションのステータスが完了（緑色）であっても、Cisco DNA Center VA に対して SSH 接続や ping を実行できない場合があります。この問題は、オンプレミスの CGW が正しく設定されていない場合に発生する可能性があります。CGW の設定を確認して、再試行してください。

問題	考えられる原因と解決策
セッションが終了する	RCA のトリガーなどの操作の進行中にセッションがタイムアウトすると、操作が突然終了し、次の通知が表示されることがあります。  セッションがタイムアウトした場合は、再度ログインして操作を再開してください。



第 4 章

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 （102 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 （5 ページ）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 （108 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 （113 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

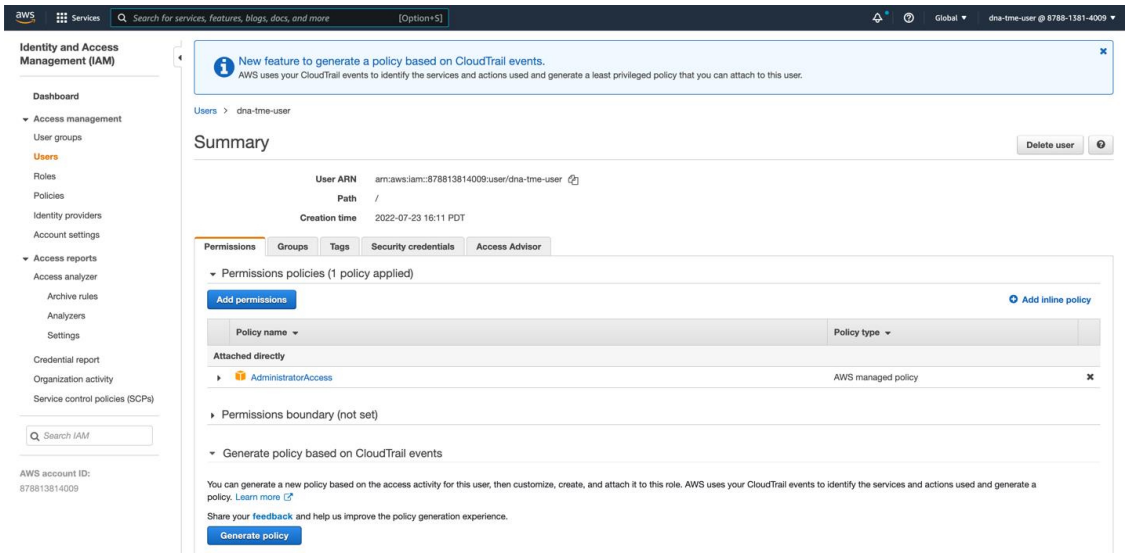
AWS 環境

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。

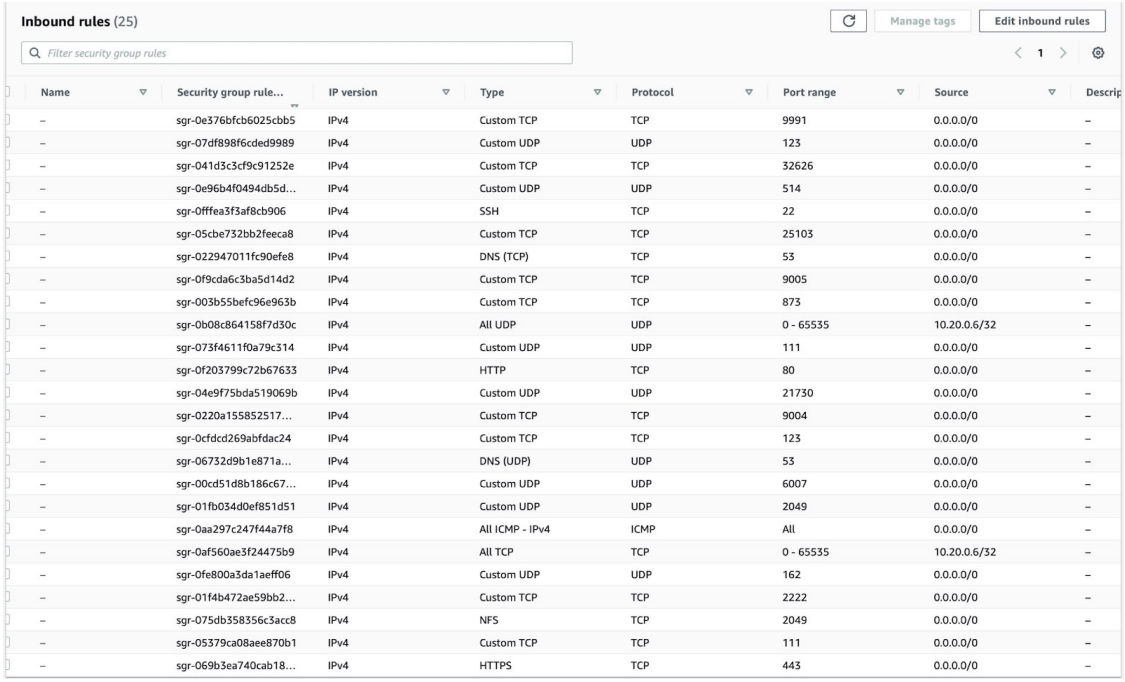
（注） リソースの独立性と分離を維持するために、AWS アカウントをサブアカウント（子アカウント）にすることを推奨します。サブアカウントを使用することで、Cisco DNA Center を展開しても既存のリソースは影響を受けません。

- **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。



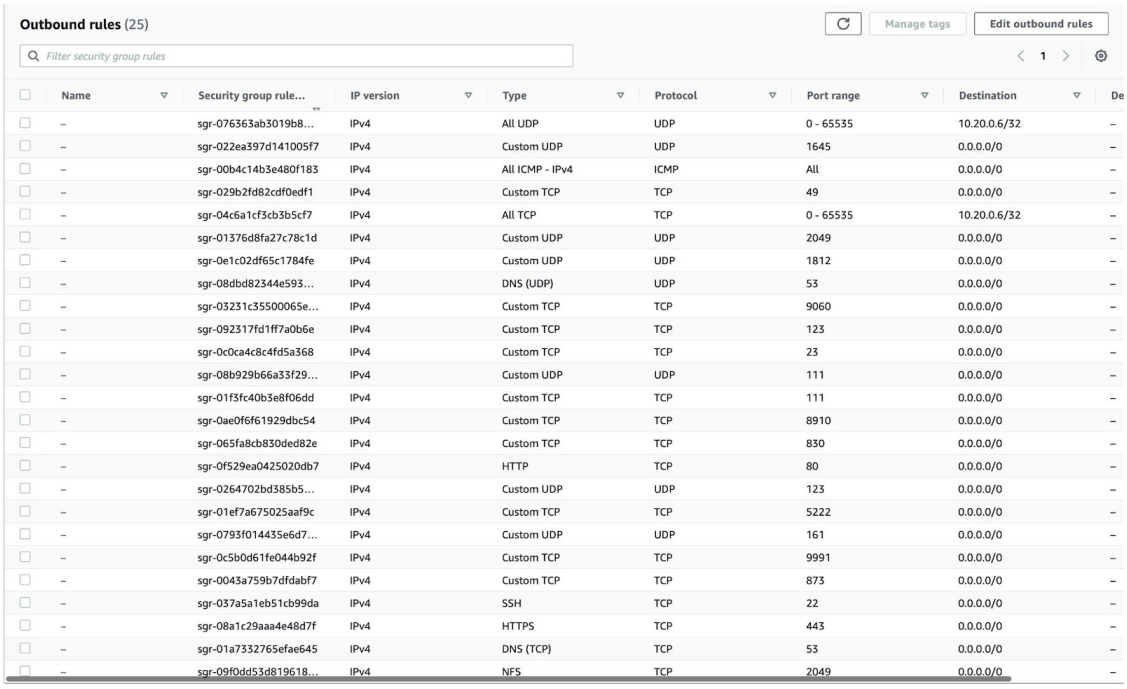
Inbound rules (25)

Manage tags | Edit inbound rules

Filter security group rules

Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Descrip
–	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

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-022ea397d1141005f7	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。
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。

ポート	サービス名	目的	推奨処置
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。
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 （102 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

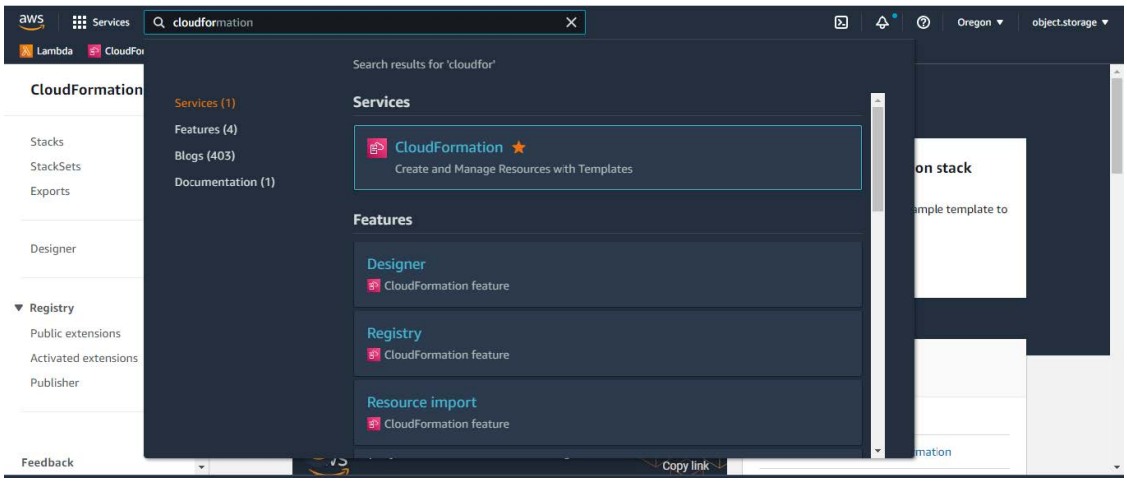
リージョン	Cisco DNA Center AMI ID
eu-south-1（ミラノ）	ami-091f667a02427854d
eu-west-1（アイルランド）	ami-0a8a59b277dff9306
eu-west-2（ロンドン）	ami-0cf5912937286b42e
eu-west-3（パリ）	ami-0b12cfdd092ef754e
us-east-1（バージニア）	ami-08ad555593196c1de
us-east-2（オハイオ）	ami-0c52ce38eb8974728
us-west-1（北カリフォルニア）	ami-0b83a898072e12970
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 （8 ページ）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。

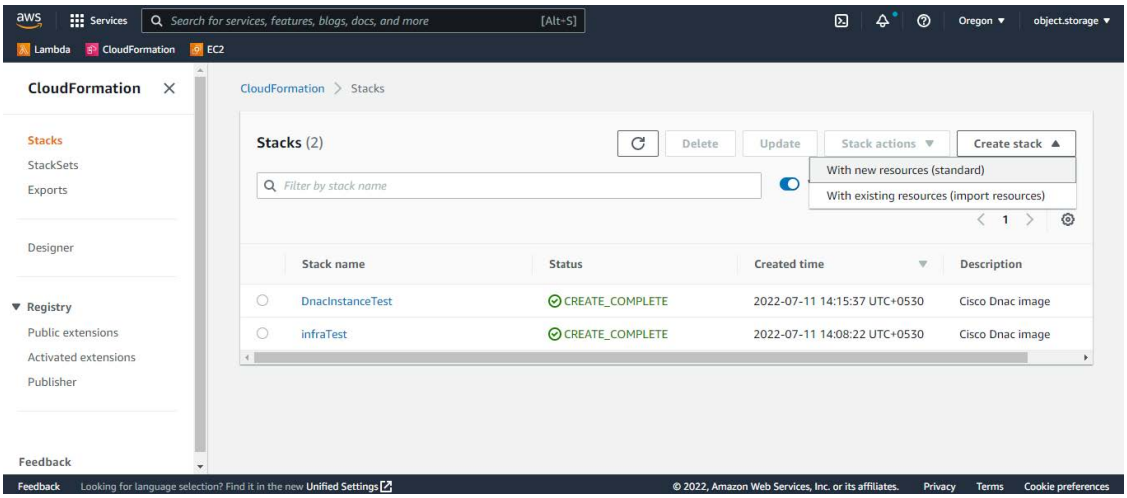
AWS コンソールが表示されます。

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

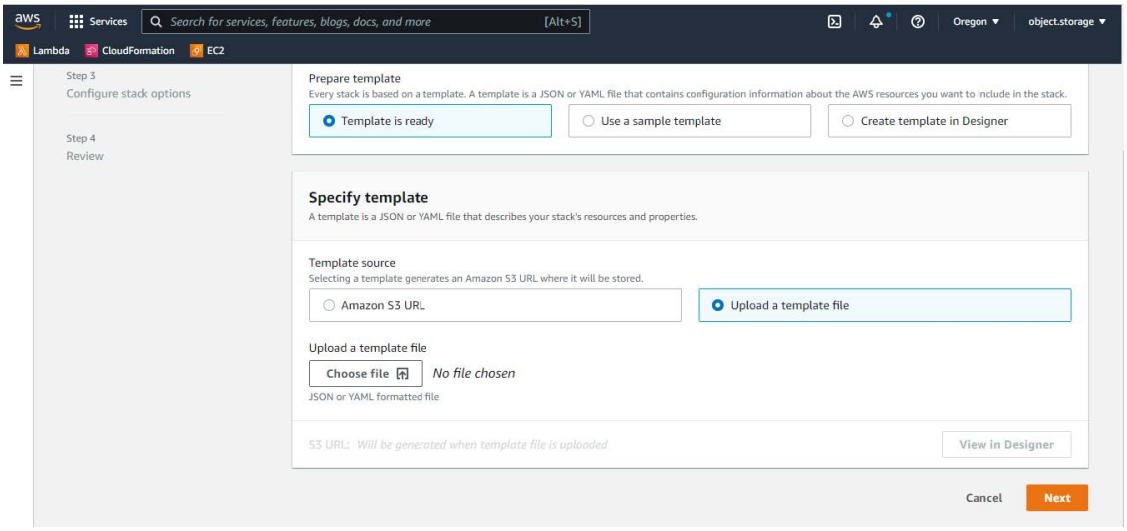


ステップ 5 ドロップダウンメニューから [CloudFormation] を選択します。

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。

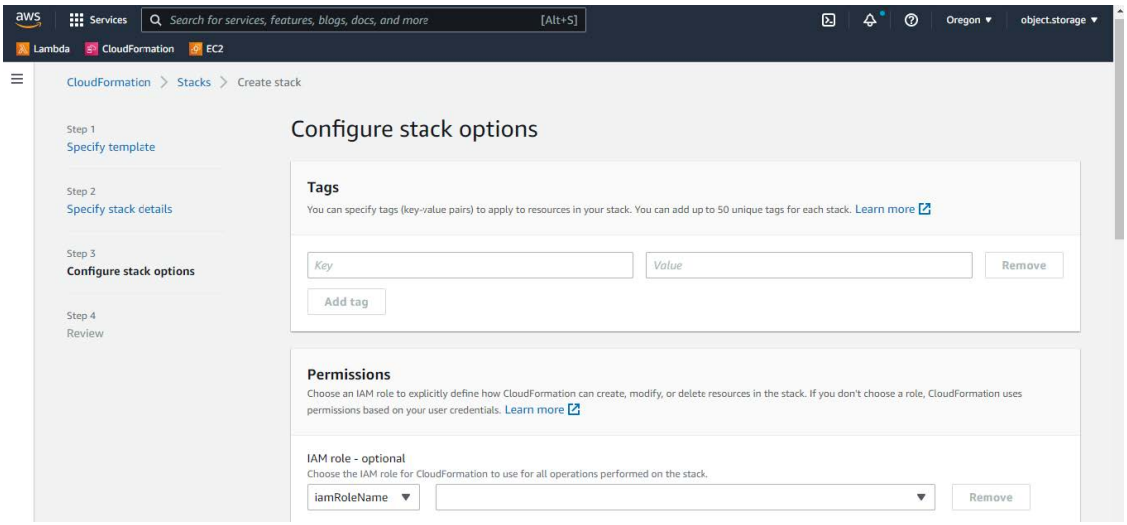
    環境名は、展開を区別するために使用され、AWS リソース名の前に追加されます。以前の展開と同じ環境名を使用すると、現在の展開でエラーが発生します。
  - [Private Subnet ID]：Cisco DNA Center で使用する VPC サブネットを入力します。
  - [Security Group]：展開する Cisco DNA Center VA に割り当てるセキュリティグループを入力します。
  - [Keypair]：展開する Cisco DNA Center VA の CLI へのアクセスに使用する SSH キーペアを入力します。

- **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）

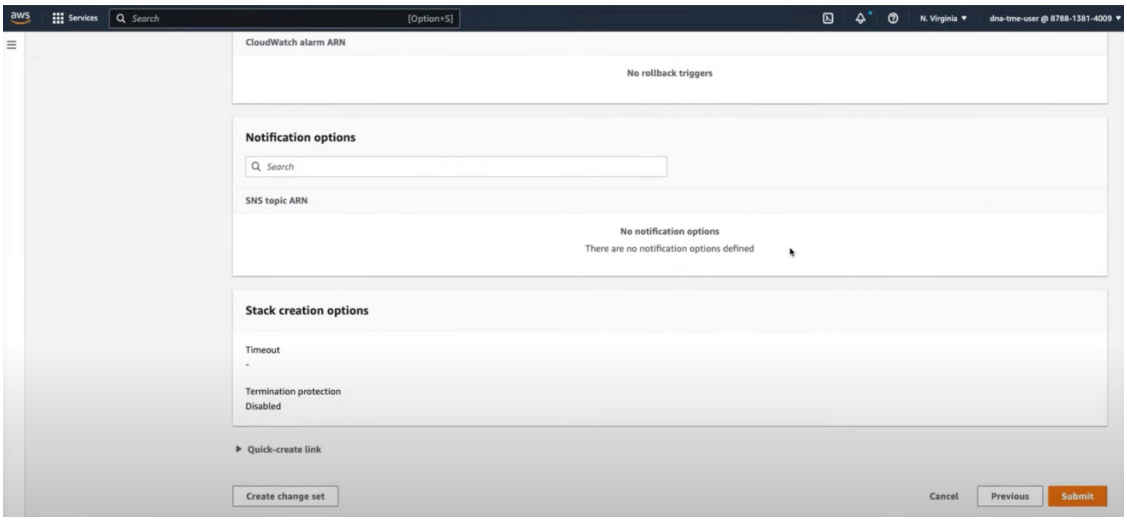
  - [DnacFQDN]：Cisco DNA Center の FQDN。
  - [DnacHttpsProxy]：（オプション）エンタープライズ HTTPS プロキシ。
  - [DnacHttpsProxyUsername]：（オプション）HTTPS プロキシのユーザー名。
  - [DnacHttpsProxyPassword]：（オプション）HTTPS プロキシのパスワード。

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。

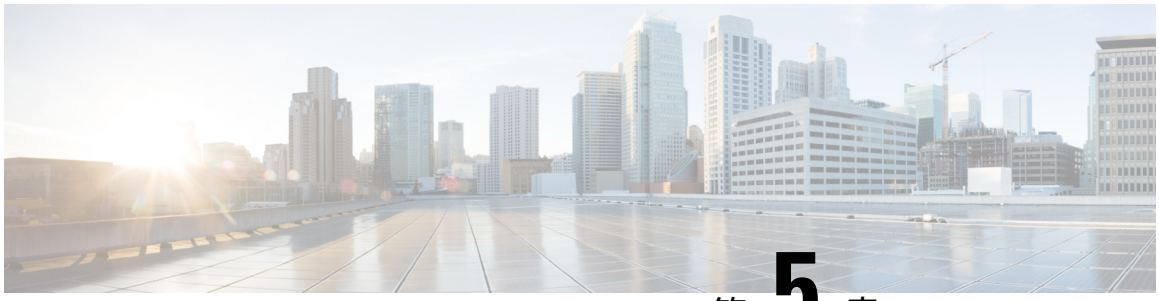
ステップ 3 Cisco DNA Center との SSH 接続を確立して、Cisco DNA Center が認証されていることを確認します。

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。



第 5 章

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 （116 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 （5 ページ）」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 （122 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 （122 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

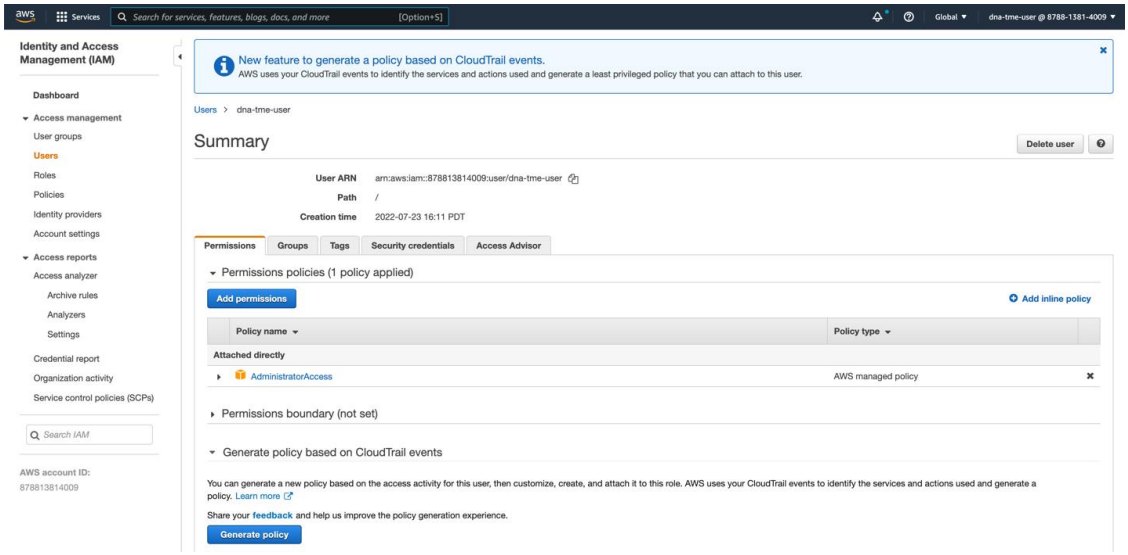
AWS 環境

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。

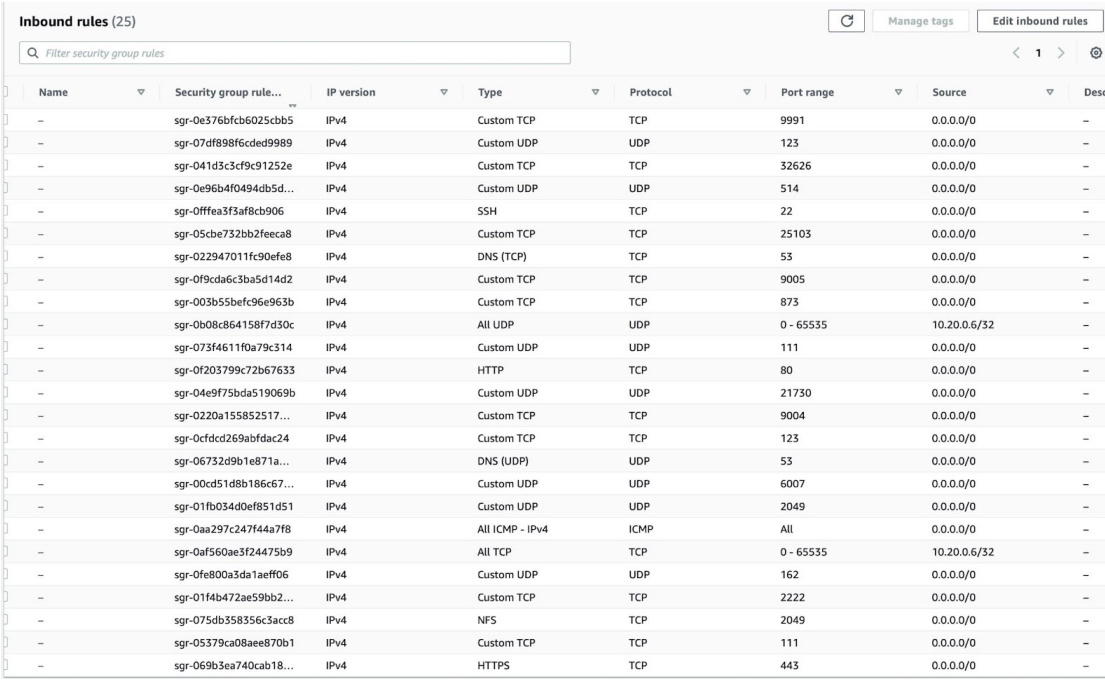
（注） リソースの独立性と分離を維持するために、AWS アカウントをサブアカウント（子アカウント）にすることを推奨します。サブアカウントを使用することで、Cisco DNA Center を展開しても既存のリソースは影響を受けません。

- **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

    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。



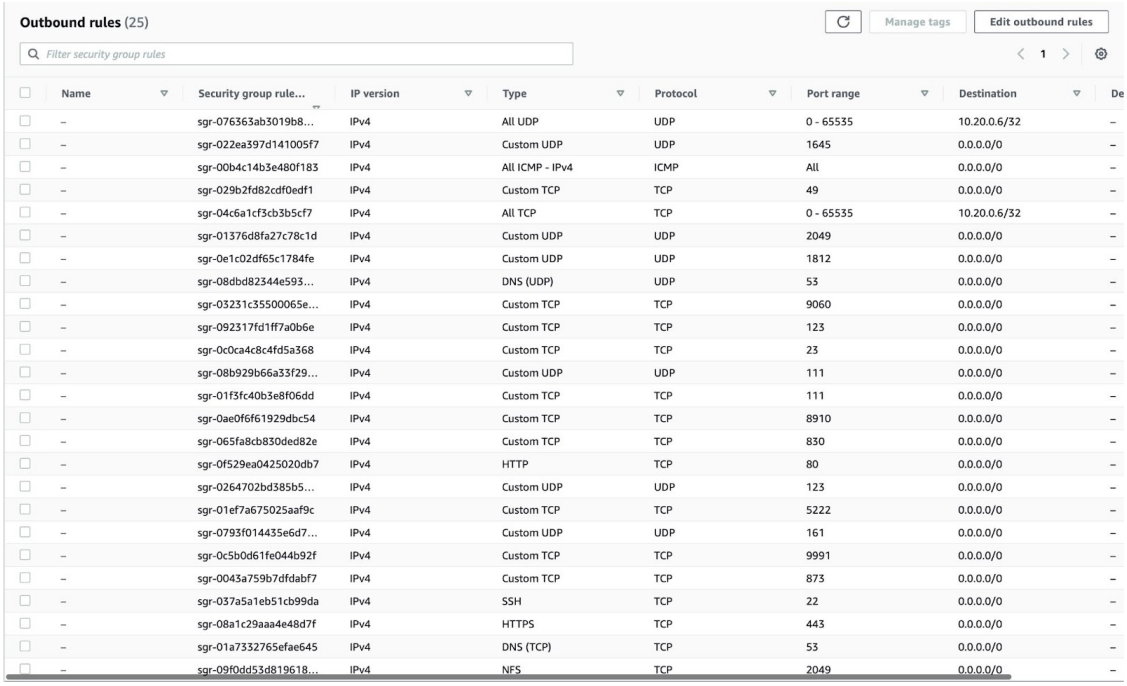
Inbound rules (25)

Manage tags | Edit inbound rules

Filter security group rules

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

Name	Security group rule...	IP version	Type	Protocol	Port range	Destination
–	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 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、シスコのソフトウェアダウンロードサイトにアクセスし、次のファイルをダウンロードしてください。

AWS Marketplace を使用した *AWS* での *Cisco DNA Center* の展開

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。