Cisco Global Launchpad 1.8 を使用した展開

Cisco Global Launchpad を使用した AWS での Cisco DNA Center の自動展開

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 1.8 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 （2 ページ）を参照してください。
2. （任意）AWS 上の Cisco ISE と Cisco DNA Center VA を統合します。AWS での AWS 上の Cisco ISE と Cisco DNA Center の統合に関するガイドラインを参照してください。
3. 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 （5 ページ）またはホステッド型 Cisco Global Launchpad へのアクセス （7 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 （12 ページ）を参照してください。
5. 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 （24 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 （25 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 （29 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 1.8 管理者ガイド*』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。

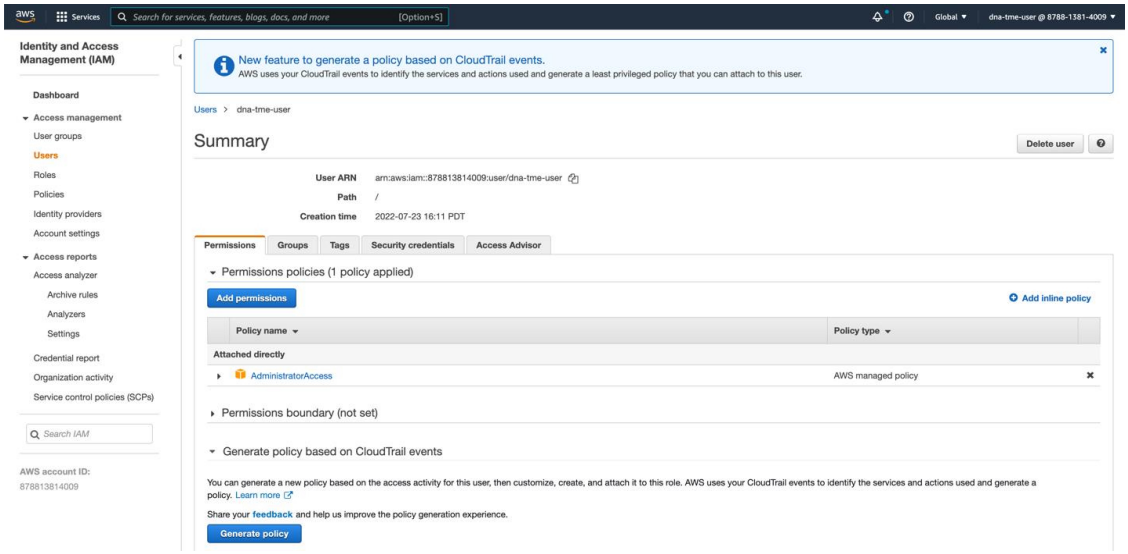
  - **Cisco DNA Center インスタンス**：r5a.8xlarge、32 個の vCPU、256 GB の RAM、4 TB ストレージ

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 1.8.0*』[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 （2 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-1.8.0.tar.gz`
- `Launchpad-desktop-server-1.8.0.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-1.8.0.tar.gz
```

```
docker load < Launchpad-desktop-server-1.8.0.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 [1.8] 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       1.8.0     208375910fde   4 hours ago    546MB
466518672524.dkr.ecr.us-west-2.amazonaws.com/platform-ui/valaunchpad-client-docker   1.8.0     68a2452c4dfb   4 hours ago    2.08GB
```

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 208375910fde
```

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 68a2452c4dfb
```

（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 （6 ページ） と ステップ 6 （6 ページ）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
d83bb3df1128   208375910fde   "/usr/bin/dumb-init …"   9 seconds ago    Up 8 seconds    0.0.0.0:9090->8080/tcp   aws-az-server
5de70c6e96f8   68a2452c4dfb   "docker-entrypoint.s…"   36 seconds ago   Up 35 seconds   0.0.0.0:90->80/tcp       aws-az-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 （29 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

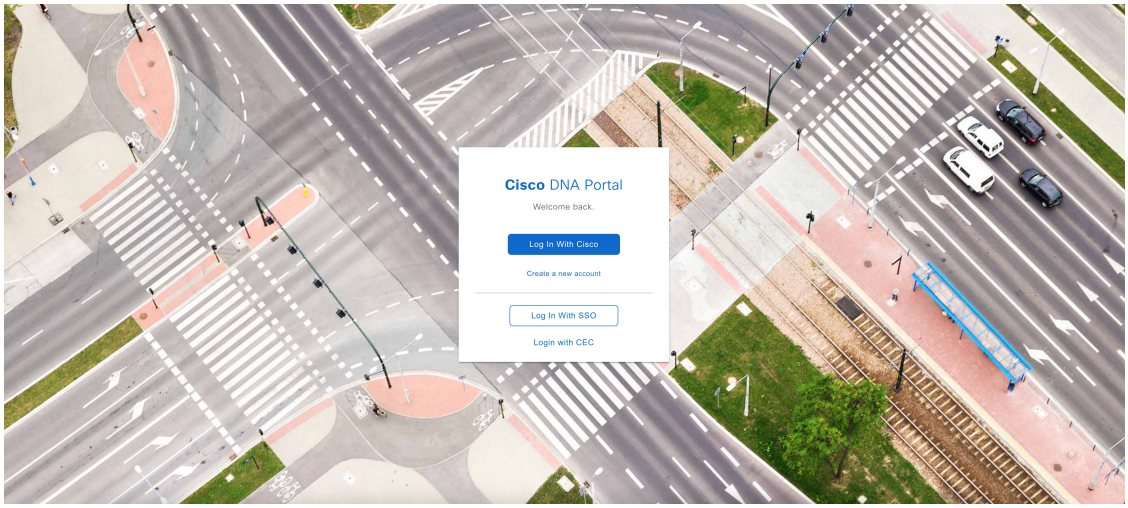
Cisco DNA ポータル を介して Cisco Global Launchpad にアクセスするには、最初にシスコアカウントを作成する必要があります。

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。

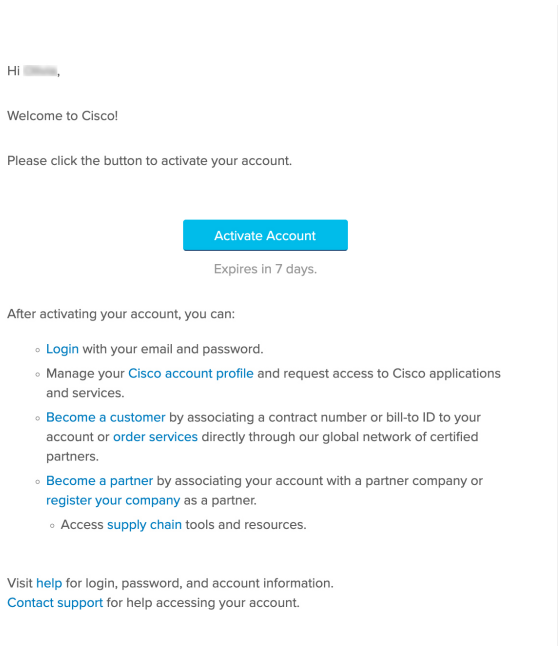


ステップ 2 [Create a new account] をクリックします。

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

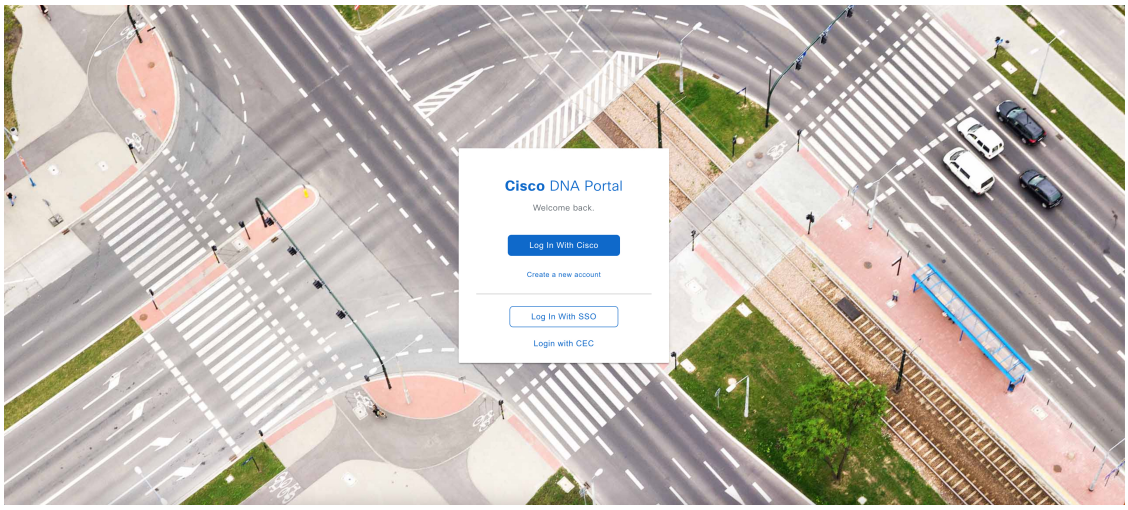
シスコアカウントがあることを確認します。詳細については、シスコアカウントの作成 （8 ページ）を参照してください。

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。

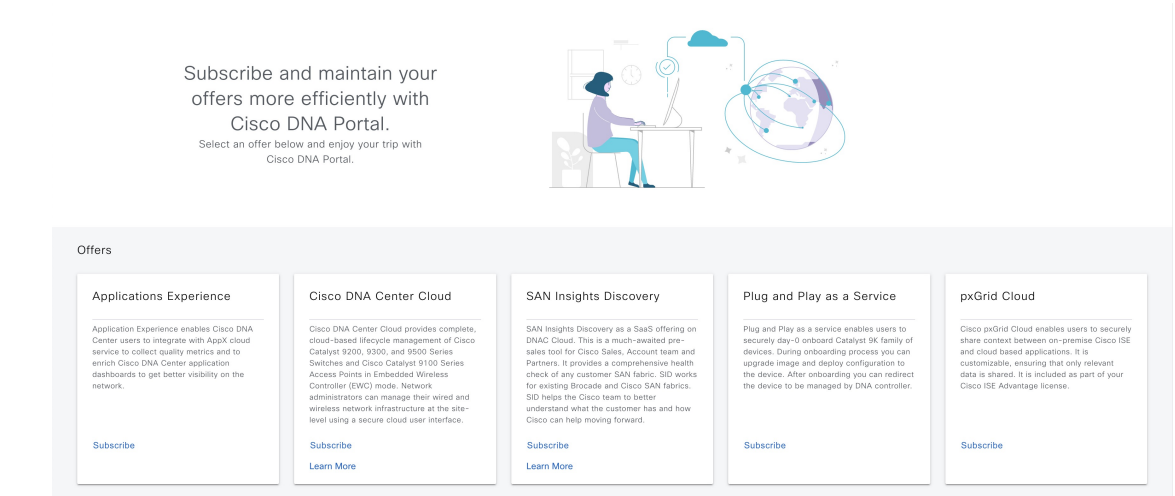
ステップ 7 **Cisco DNA ポータル** の [Confirm CCO Profile] ウィンドウで次の手順を実行します。

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

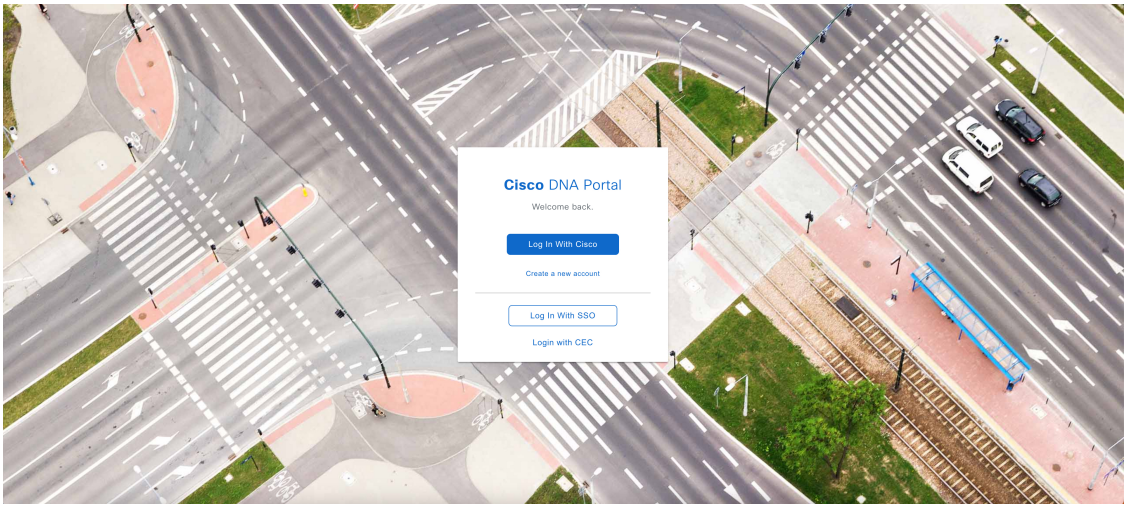
シスコアカウントと Cisco DNA ポータル アカウントがあることを確認します。詳細については、シスコアカウントの作成 （8 ページ）およびCisco DNA ポータル アカウントの作成 （9 ページ）を参照してください。

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。

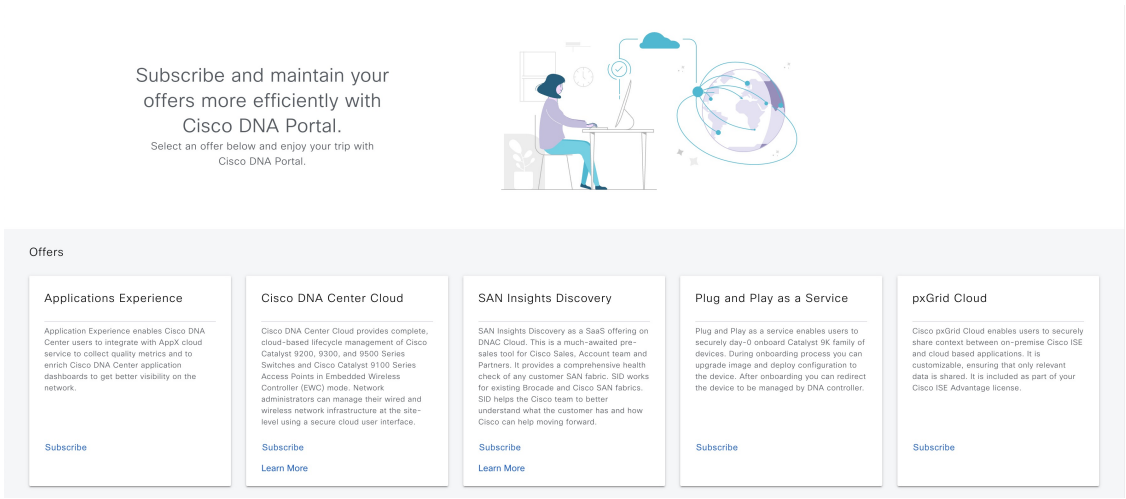
ステップ 4 [Password] フィールドにシスコアカウントのパスワードを入力します。

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 1.8.0 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 1.7.0 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 （2 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* 管理者ガイド 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 Launchpad* 管理者ガイド 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 Identity and Access Management* ユーザーガイド』[英語] の「AWS Managing 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 （30 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 （15 ページ） に進みます。

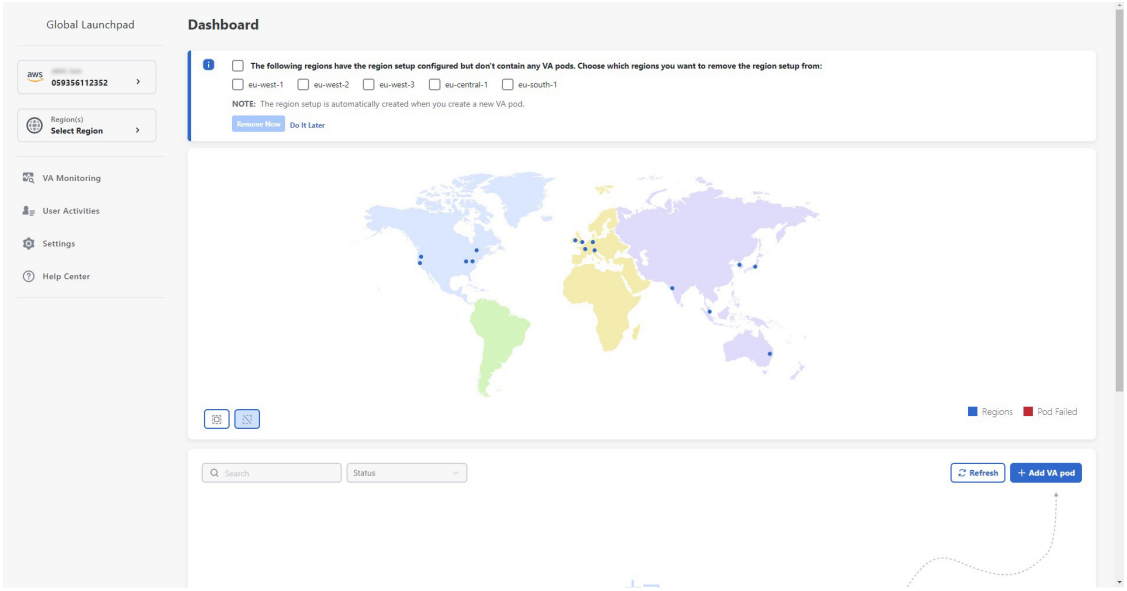
アマゾンSNS に登録して、展開されたリソース、変更、およびリソースの過剰使用に関するアラートを受信できます。さらに、Amazon CloudWatch が Cisco Global Launchpad の異常な動作を検出した場合に通知するようにアラームを設定できます。さらに、AWS Config は設定されたリソースを評価し、結果の監査ログも送信します。詳細については、*Cisco Global Launchpad* 管理者ガイドの「Subscribe to the アマゾンSNS Email Subscription」と「View Amazon CloudWatch Alarms」[英語] 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 Launchpad* 管理者ガイドの「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 Launchpad 管理者ガイド* 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）。
  - 名前は 4 文字以上 12 文字以下にする必要があります。
  - 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 （24 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.d （17 ページ） 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 （31 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 1.8.0*』[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/catalyst-backup/

（注） Cisco Global Launchpad リリース 1.8 では、ディレクトリは自動的に作成されません。バックアップの設定に必要なフォルダを作成する必要があります。詳細については、『*Cisco Global Launchpad* 管理者ガイド』の「NFS サーバーの設定」を参照してください。

- **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、VA ポッド名の最初の 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、VA ポッド名が DNAC-SJC 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）
  - VA ポッド名は、展開先のリージョンを選択した後に **Dashboard** ペインで確認できます。
  - バックアップサーバーの IP アドレスは、[View Catalyst Center] ペインで確認できます。詳細については、『*Cisco Global Launchpad* 管理者ガイド』の「Catalyst Center VA の詳細の表示」を参照してください。

- **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

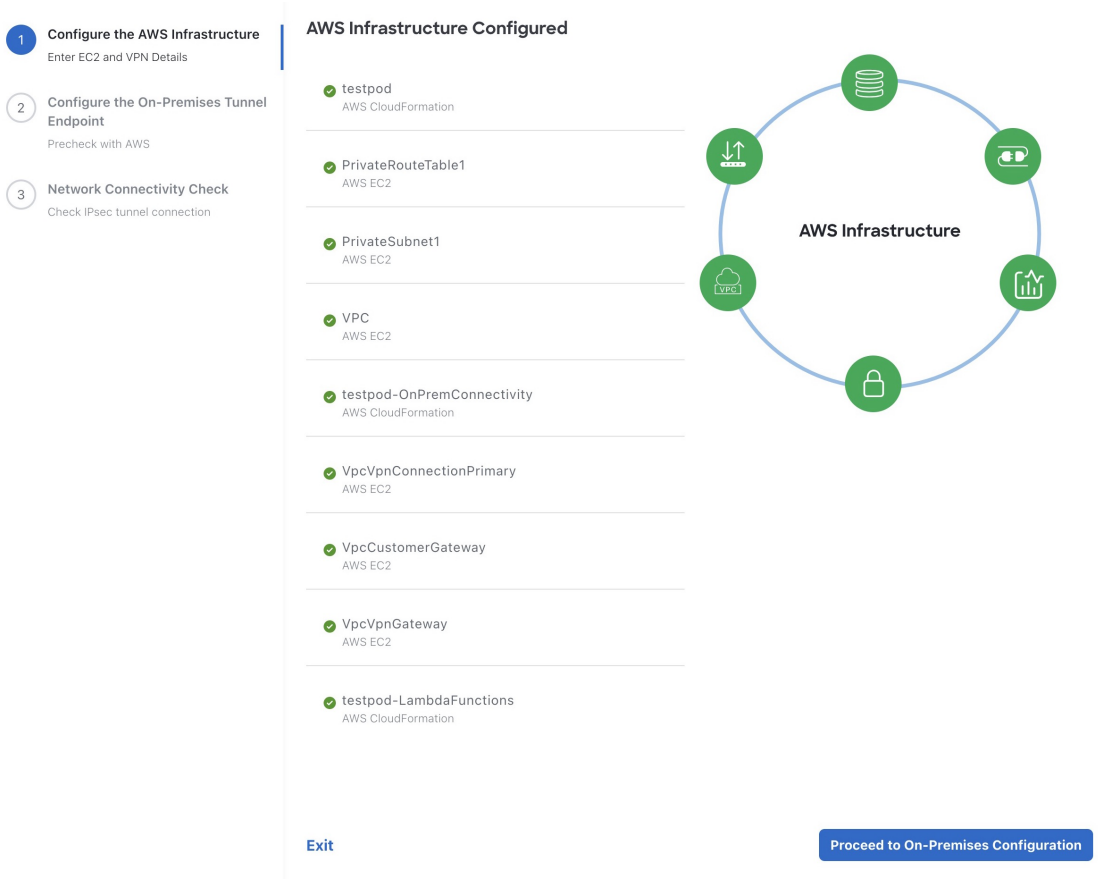
f) [Next] をクリックします。

[Summary] ペインが表示されます。

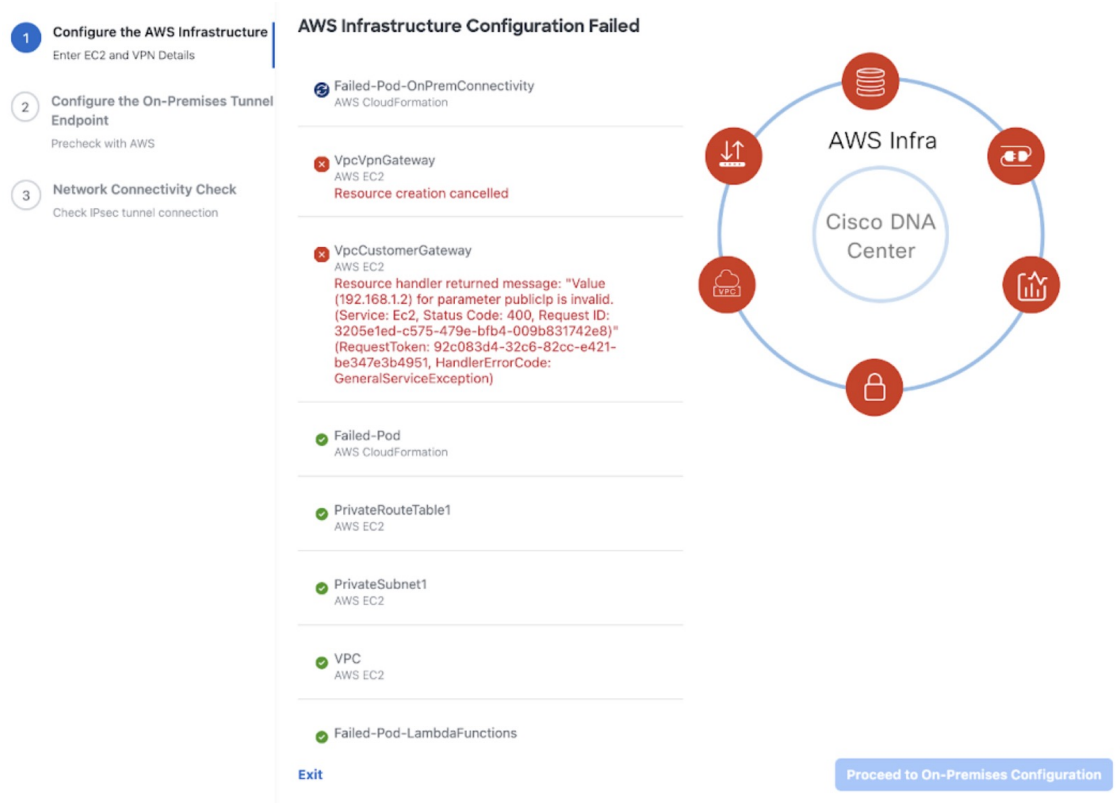
g) 環境と VPN の入力内容を確認します。問題がなければ、[Start Configuring AWS Infrastructure] をクリックします。

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 （31 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。

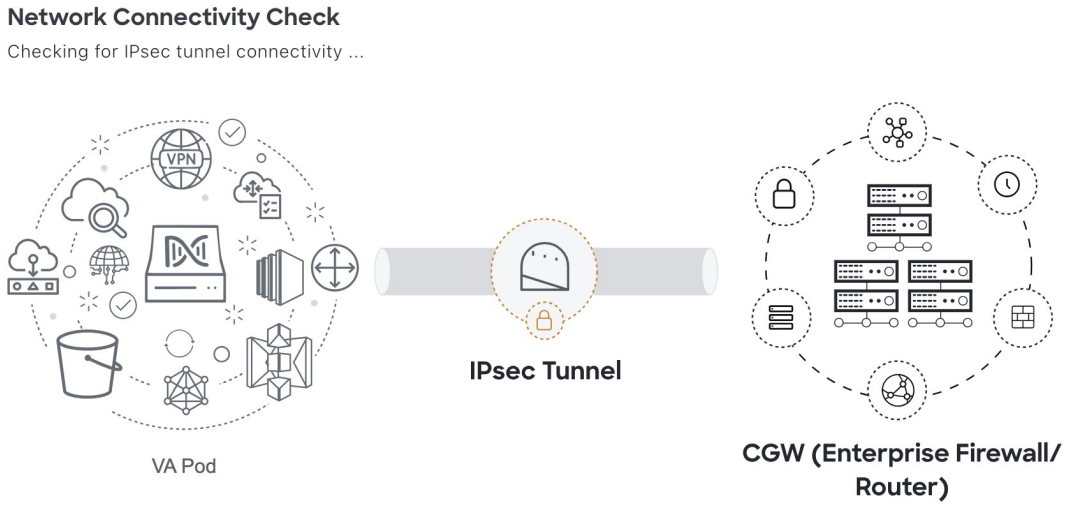
  提供されている構成ファイルを使用すると、AWS とエンタープライズルータまたはファイアウォールの間で 2 つのトンネルを起動できます。

- 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。

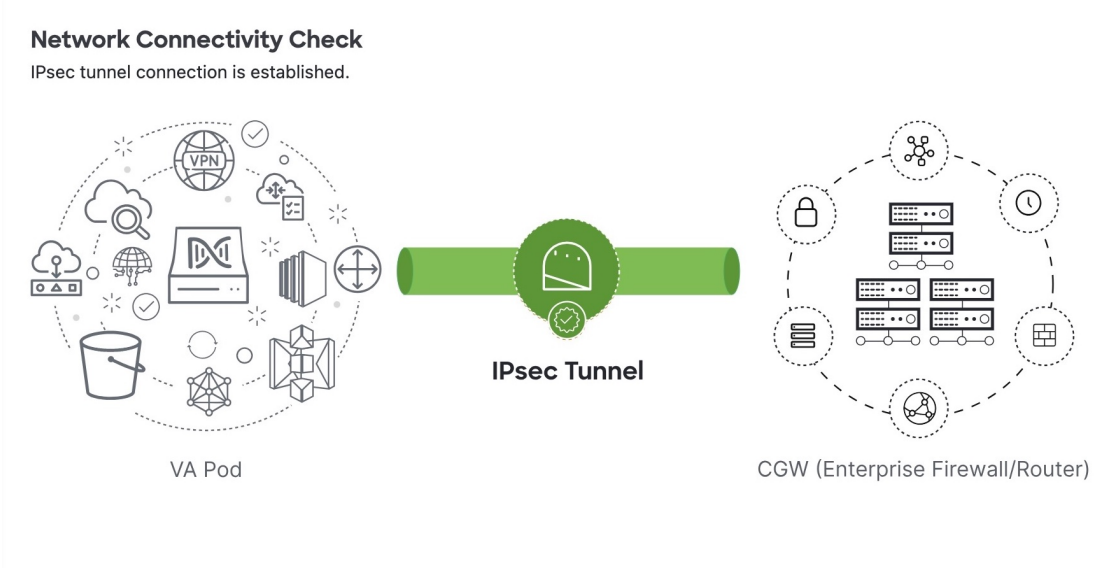
c) [Proceed to Network Connectivity Check] ボタンをクリックします。

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（24 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。

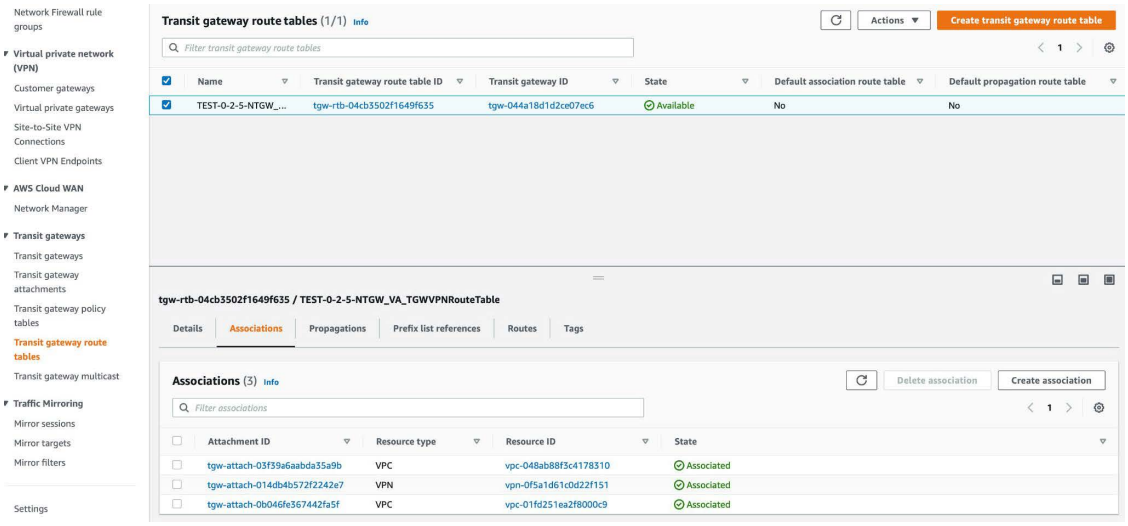
Cisco Global Launchpad で TGW 接続を確立するには、AWS で TGW ルーティングテーブルを手動で設定し、既存の CGW にそのルーティング設定を追加する必要があります。

手順

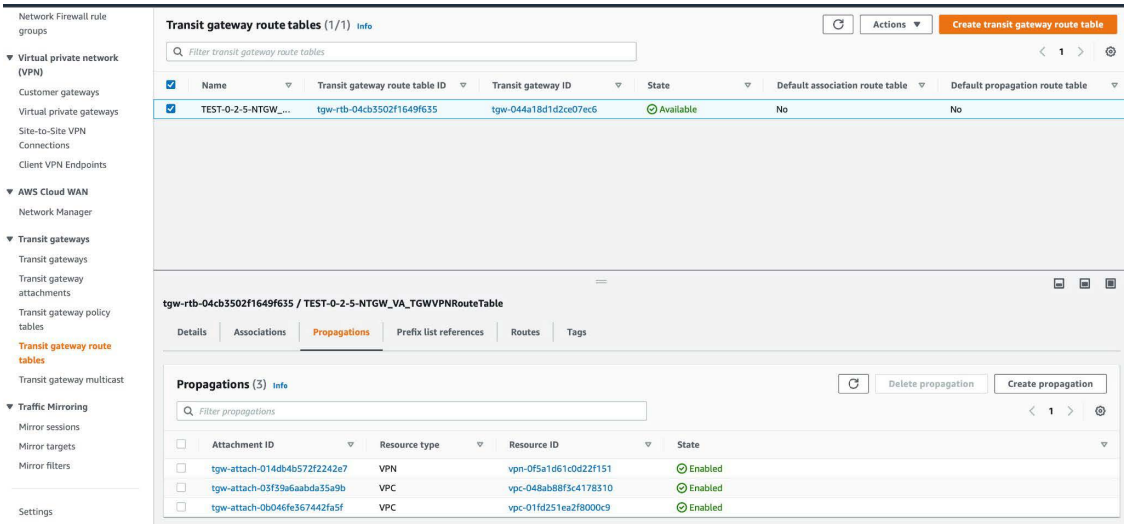
ステップ 1 AWS コンソールから、[VPC service] に移動します。

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。

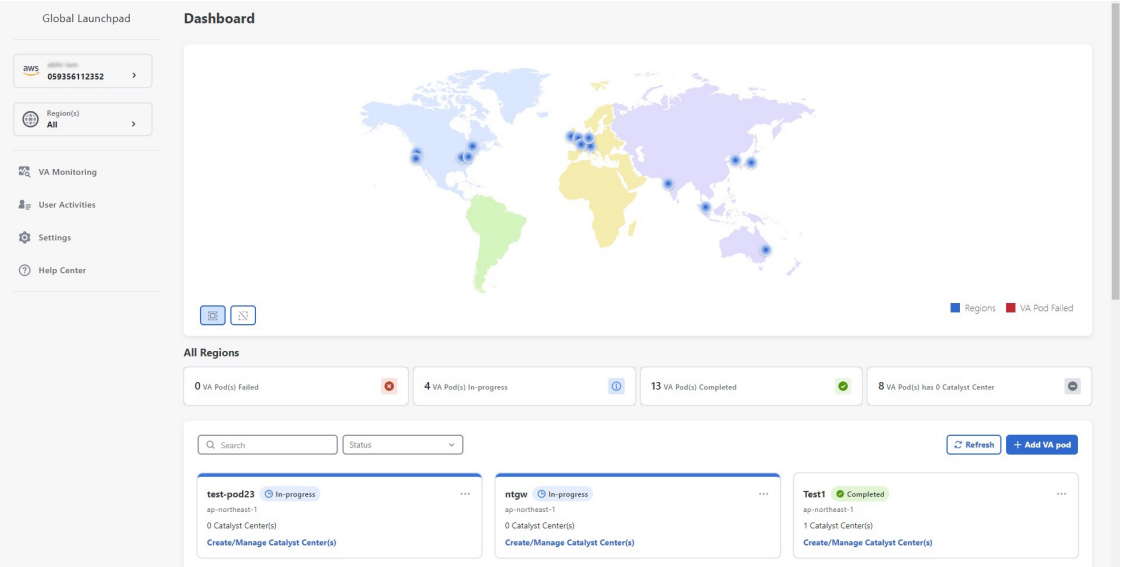
例：`route tunnel-int-vpn-0b57b508d80a07291-1 10.0.0.0 255.255.0.0 192.168.44.37 200`

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。
  - Cisco DNA Center を AWS に展開した後、Cisco Global Launchpad を使用して DNS サーバーを更新することはできません。ただし、AWS コンソールを使用すると DNS サーバーを更新できます。詳細については、AWS コンソールを使用した Cisco DNA Center VA での DNS サーバーの更新 （34 ページ）を参照してください。

- [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 1.8.0 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。

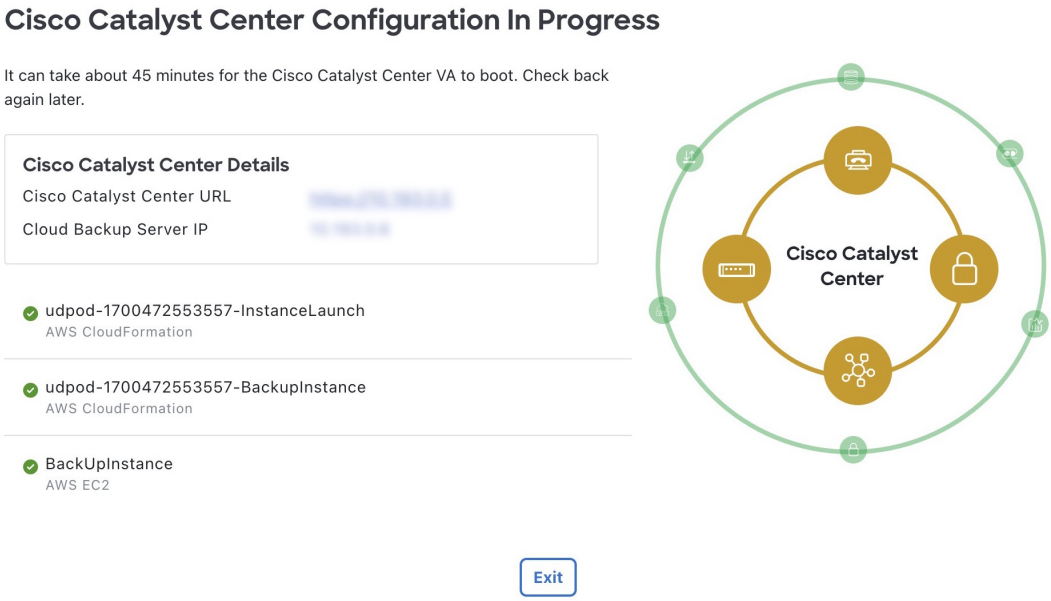
重要 PEM キーは AWS アカウントに保存されていないため、ダウンロードする必要があります。作成されている Cisco DNA Center VA にアクセスするには、PEM キーが必要です。

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。

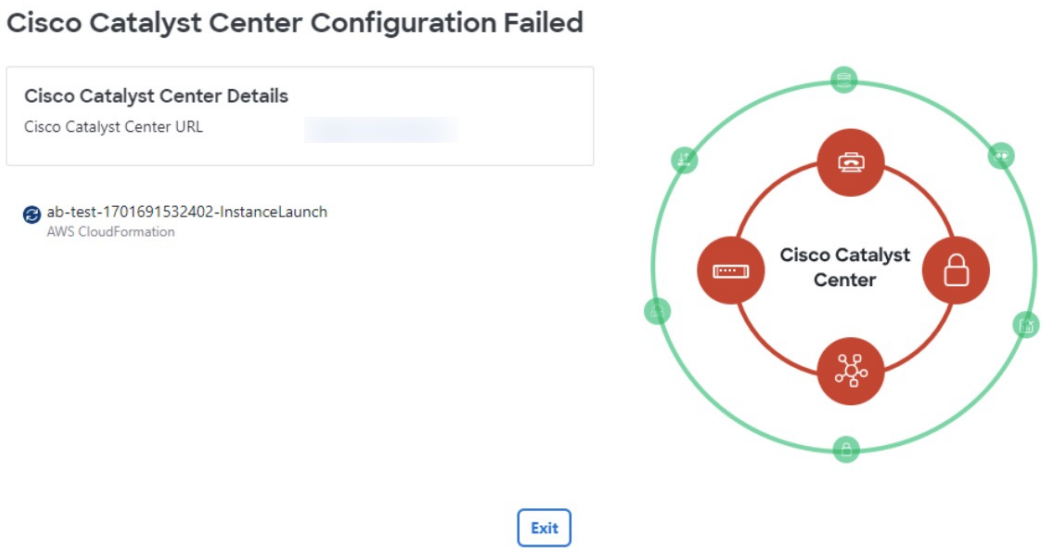
（注） このプロセスは 45 ～ 60 分かかります。アプリケーションを終了したり、このウィンドウやタブを閉じたりしないでください。さもないと、設定が一時停止します。

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、VA ポッド名の最初の 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 （34 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 （12 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 （24 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。

AWS コンソールを使用した Cisco DNA Center VA での DNS サーバーの更新

Cisco DNA Center VAで設定されている DNS サーバーの IP アドレスを更新するには、Cisco TAC から取得した同意トークンを使用し、次の手順に従います。

始める前に

Cisco TAC サポートに連絡して、シェルへのフルアクセスを取得できる同意トークンを取得してください。

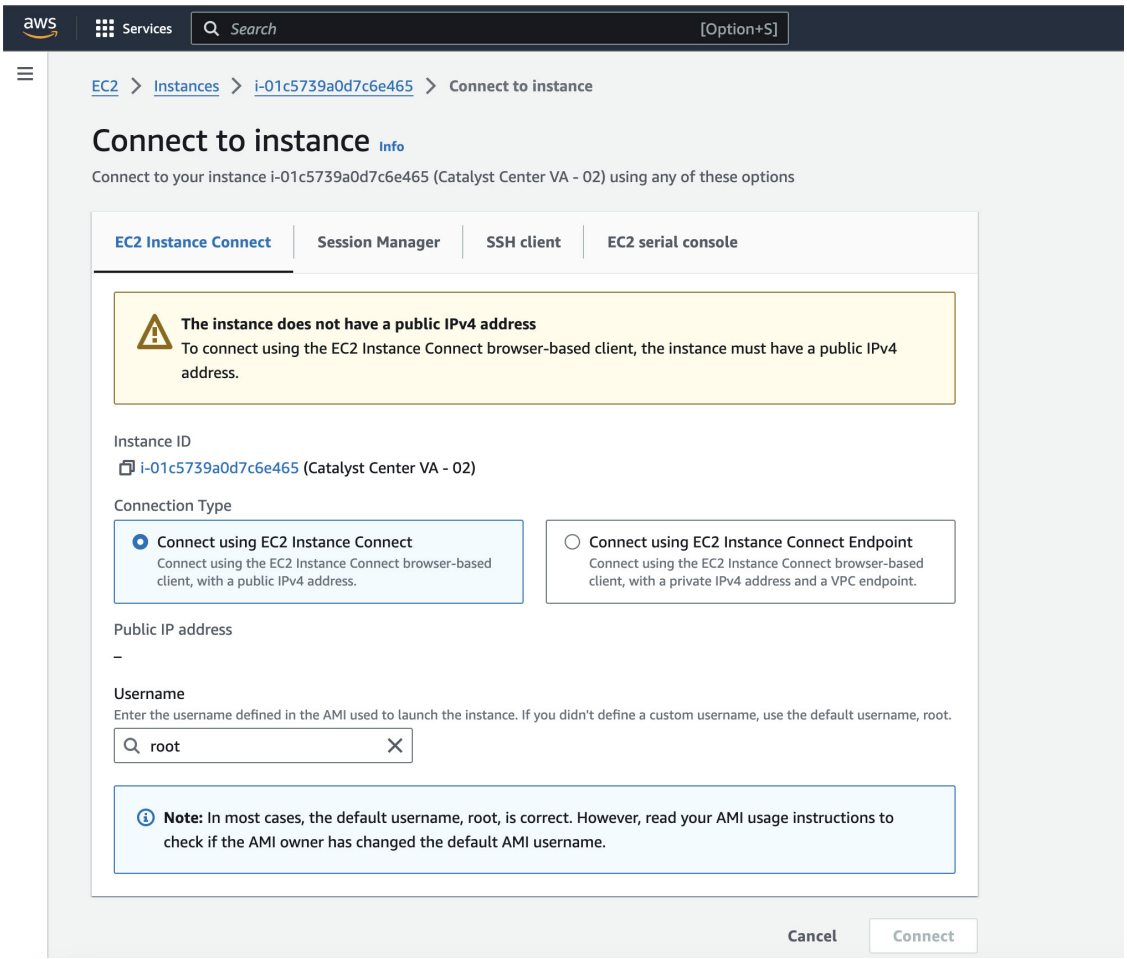
手順

ステップ 1 AWS コンソールにログインします。

ステップ 2 **[EC2]** > **[Instances]** を選択します。

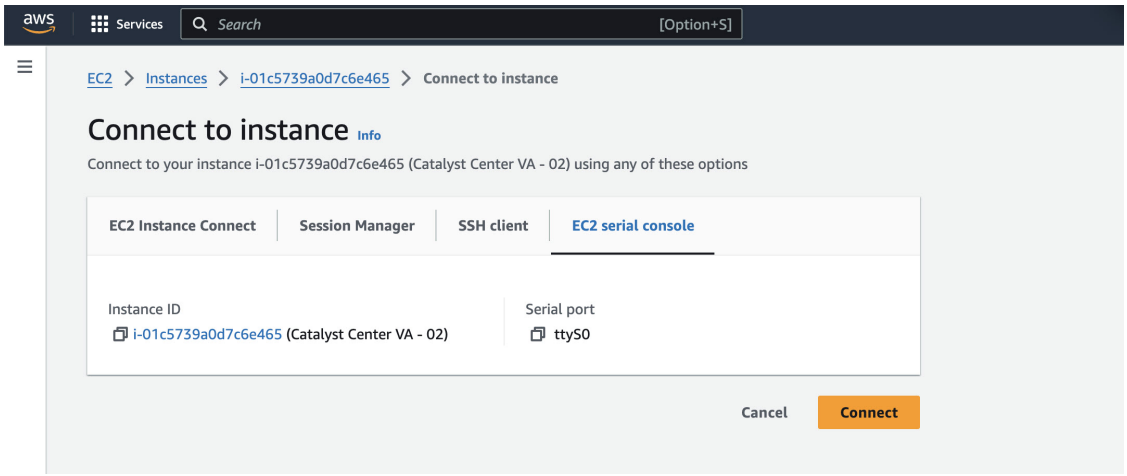
ステップ 3 変更する Cisco DNA Center のインスタンス ID を選択して、[Connect] をクリックします。

[EC2 Instance Connect] タブがデフォルトで選択された状態で、[Connect to instance] ページが表示されます。



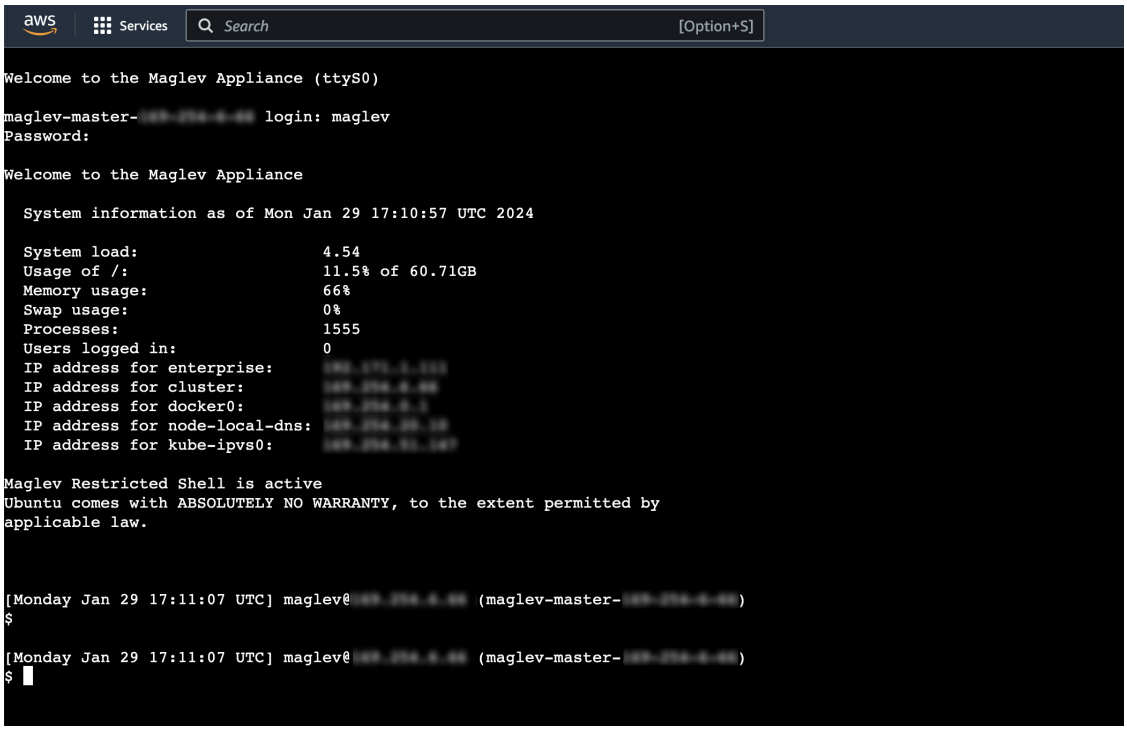
ステップ 4 [EC2 serial console] タブをクリックします。

Cisco DNA Center VA のインスタンス ID とシリアルポートが表示されます。



ステップ 5 [接続（Connect）] をクリックします。

Maglev コンソールが表示されます。



ステップ 6 ログインプロンプトで **maglev** と入力します。

ステップ 7 [Password] プロンプトには、Cisco Global Launchpad、AWS CloudFormation、または AWS Marketplace を使用して Cisco DNA Center VA を展開したかどうかに関係なく、初期展開時に設定したパスワードを入力します。

ステップ 8 Cisco TAC から取得した同意トークンを使用して、シェルへのフルアクセスを取得します。

```
$ _shell -v _shell -vconsent-token
```

次に例を示します。

```
_shell -v _shell  -v n1+hPAAAAQ000AQAAAABAgAEAAAAAAMBYkk2bmhXcW14OGtqUXoy
a09UTXlzM252UnNlUnFwTEFEQVQvejJjQm9kNXloN2thSFk3MzZBek9CMEJRUUZad2QNCkhPNVZMNjhMUXMyb0h
1OXQ2eWlTR01yT1hwZkRPSmNuc1c2QUJ5ZGtVZ0N2OU1mMXZtTC90em1MNldWcVdjY2gNCkh3eEd5MytZWmRVUTN
kek1xOWNiWi9rLzVlTkozQ2RrYy9SMXEya2NOV09uMEdvZE11c1lZN01ENjZvVk5zZlMNCktseHZxTi9tVXF0cW1
vaG9NZFY4SnVOY3NBcXkxQkZOMzZHdS9XQ2N4S2tpdlNUV1VOTVVrRXU1TjVRUDl6d1YNCmYyWW1ZdUFnSGNOcnV
veUhoTzZYYjRIWnJWNDdxSG5qR0REUjV3TE90bnNXalpBL2tsRzNzN0lIa1ZaY0VzMVENCkVoc3FZUGU5Z2ZoTWF
6YXVKRmtxVmc9PQ==
```

ステップ 9 端末を色で表示するように設定します。

```
export TERM=xterm
```

ステップ 10 **sudo-maglev-config** コマンドを実行します。

設定ウィザードでは、『*Cisco DNA Center* 第 *2* 世代アプライアンス リリース *2.2.3* 設置ガイド』の「Maglev ウィザードを使用したセカンダリ ノードの設定」に示される一連の画面のセッションが簡略化されています。

DNS サーバーの IP アドレス設定が表示されたら、DNS サーバーの IP アドレスを優先アドレスに変更します。画面ごとに変更を終えたら [next>>] を選択して設定ウィザードを続行します。

ステップ 11 設定プロセスの最後に、設定ウィザードが変更の適用を実行できる状態になったことを示すメッセージが表示されます。次のオプションを使用できます。

- [<<back]：変更を確認して検証します。
- [<cancel>]：変更を破棄して設定ウィザードを終了します。
- [proceed>>]：変更を保存して、それらの適用を開始します。

ステップ 12 変更を完了するには、[proceed>>] を選択します。設定ウィザードで変更が適用されます。

設定プロセスの最後に、「CONFIGURATION SUCCEEDED」というメッセージが表示されます。

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、**セッション終了**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、[OK] をクリックし、再度ログインして操作を再開してください。

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。