

AWS 上の CiscoDNACenter リリース 1.2.1 導入ガイド

初版：2023 年 4 月 17 日

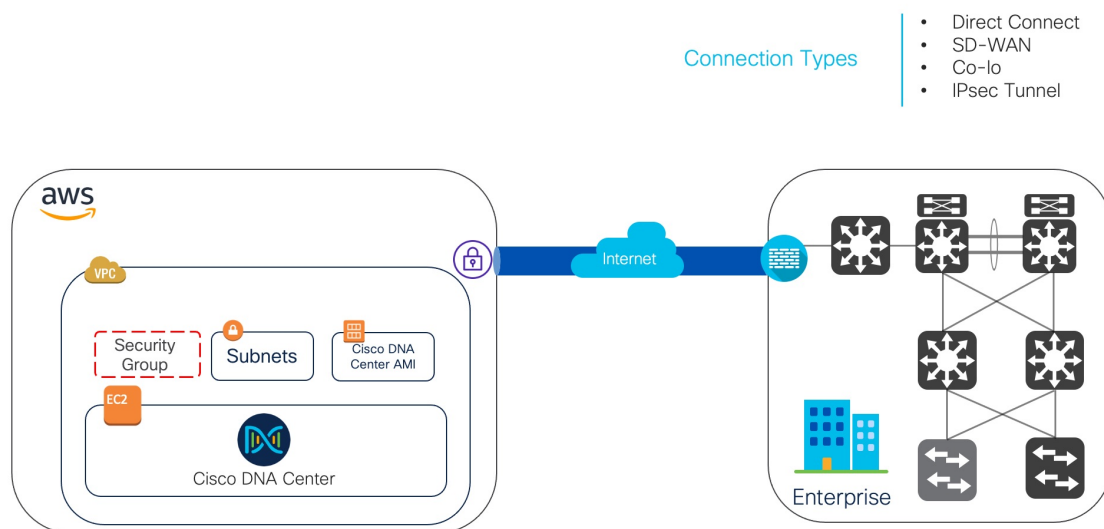
最終更新：2023 年 7 月 6 日

AWS 上の Cisco DNA Center Deployment Guide

AWS 上の Cisco DNA Center の概要

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。

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。AWS 上の Cisco DNA Center は、お客様独自の AWS クラウド環境で実行され、クラウドからお客様の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 DNA Center VA 起動パッドが 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、ステータストレージ用の 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 DNA Center VA 起動パッドを使用した 2 つの方法が用意されています。Cisco DNA Center VA 起動パッド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 DNA Center VA 起動パッド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 DNA Center VA 起動パッドには Cisco DNA Center 仮想アプライアンス (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。

高度な手順については、[自動展開ワークフロー \(8 ページ\)](#) を参照してください。

- **AWS CloudFormation を使用した手動展開**：Cisco DNA Center VA 起動パッドを使用せずに AWS アカウントで Cisco DNA Center AMI を手動展開します。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 を展開します。高度な手順については、[AWS CloudFormation ワークフローを使用した手動展開 \(48 ページ\)](#) を参照してください。
- **AWS Marketplace を使用した手動展開**：Cisco DNA Center VA 起動パッドを使用せずに AWS アカウントで Cisco DNA Center AMI を手動展開します。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 Elastic Compute Cloud (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。手順については、[AWS Marketplace を使用して AWS に Cisco DNA Center を手動展開する \(60 ページ\)](#) 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 DNA Center VA 起動パッド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 DNA Center VA 起動パッド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
<ul style="list-style-type: none"> • 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 のインストーラー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 上の 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。 	<ul style="list-style-type: none"> • 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。 	<ul style="list-style-type: none"> • 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 上の 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 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 \(6 ページ\)](#) 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 AZ 内の別のインスタンスを自動的に起動します。
- 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 上の Cisco ISE と AWS 上の 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 DNA Center VA 起動パッドで予約済みの 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、AWS 上の Cisco DNA Center または AWS 上の Cisco ISE 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 DNA Center VA 起動パッドは、Cisco DNA Center VA 起動パッド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 DNA Center VA 起動パッド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 DNA Center VA 起動パッド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 DNA Center VA 起動パッドによって確実に 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 の GUI にアクセスする際には、次の注意事項を遵守してください。

- サポートされているブラウザを使用してください。サポートされているブラウザの最新リストについては、『[Release Notes for Cisco DNA Center on AWS, Release 1.3.x](#)』 [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。

Cisco DNA Center の CLI にアクセスする際の注意事項

Cisco DNA Center の CLI にアクセスする際には、次の注意事項を遵守してください。

- 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 DNA Center VA 起動パッドを使用して Cisco DNA Center を展開した場合は、Cisco DNA Center VA 起動パッド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い場合は、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。

自動展開方式を使用した AWS 上の 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、ステータストレージ用の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。

自動展開ワークフロー

自動方式を使用して AWS 上の Cisco DNA Center を展開するには、次の手順を実行します。

1. 前提条件が満たされていることを確認します。[自動展開の前提条件 \(8 ページ\)](#) を参照してください。
2. AWS 上の Cisco ISE と Cisco DNA Center VA を統合する場合は、[AWS 上の Cisco ISE と AWS 上の Cisco DNA Center の統合に関するガイドライン \(4 ページ\)](#) 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 \(12 ページ\)](#) または [ホステッド型 Cisco DNA Center VA 起動パッドへのアクセス \(14 ページ\)](#) 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 \(23 ページ\)](#) 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 \(34 ページ\)](#) 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 \(36 ページ\)](#) を参照してください。
7. 必要に応じて、展開中に発生した問題をトラブルシューティングします。[展開のトラブルシューティング \(40 ページ\)](#) を参照してください。
8. Cisco DNA Center VA を正常に展開したら、Cisco DNA Center VA 起動パッドを使用して VA を管理できます。[Cisco DNA Center VA 起動パッドを使用した VA ポッドとユーザー設定の管理 \(69 ページ\)](#) を参照してください。

自動展開の前提条件

ここに記載する前提条件は、自動展開用です。AWS CloudFormation または AWS Marketplace を使用して手動で Cisco DNA Center VA を展開することもできます。それぞれの方法のメリットとデメリットについては、[展開の概要 \(2 ページ\)](#) を参照してください。



-
- (注) リリース 1.3.0 で追加された新しいリージョンへのアクセスを有効にするには、Cisco DNA Center VA 起動パッドリリース 1.3.0 のインストール後に管理者ユーザーが Cisco DNA Center VA 起動パッドにログインする必要があります。管理者ユーザーがログインすると、すべてのリージョンへのアクセス権が他のすべてのユーザーに対して有効になります。
-

AWS 上の 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。

- Cisco DNA Center VA 起動パッドを使用して Cisco DNA Center VA を展開および管理する場合は、Docker Community Edition (CE) をプラットフォームにインストールする必要があります。

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 Community Edition (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 on AWS, Release 1.3.x](#)』[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。

The screenshot shows the AWS IAM console interface. At the top, there is a navigation bar with the AWS logo, a search bar, and the user's profile. Below the navigation bar, the left sidebar contains the 'Identity and Access Management (IAM)' menu with options like Dashboard, Access management, User groups, Users, Roles, Policies, Identity providers, Account settings, Access reports, Access analyzer, Archive rules, Analyzers, Settings, Credential report, Organization activity, and Service control policies (SCPs). The main content area displays the 'Summary' page for the user 'dna-tme-user'. It includes a notification banner about a new feature to generate policies based on CloudTrail events. The user's details are shown: User ARN (arn:aws:iam::878813814009:user/dna-tme-user), Path (/), and Creation time (2022-07-23 16:11 PDT). Below this, there are tabs for Permissions, Groups, Tags, Security credentials, and Access Advisor. The 'Permissions' tab is active, showing a list of permissions policies. One policy, 'AdministratorAccess', is listed as 'Attached directly' and is an 'AWS managed policy'. There is also a section for 'Generate policy based on CloudTrail events' with a 'Generate policy' button.

- 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。



- (注) Cisco DNA Center VA 起動パッドの旧バージョンから Cisco DNA Center VA 起動パッドバージョン 1.3.0 に更新することはできません。Docker Community Edition (CE) を再インストールしてから Cisco DNA Center VA 起動パッドバージョン 1.3.0 をインストールする必要があります。

始める前に

お使いのマシンに Docker Community Edition (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 \(8 ページ\)](#) 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-1.3.0.tar.gz
- Launchpad-desktop-server-1.3.0.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 \(6 ページ\)](#) 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-1.3.0.tar.gz
docker load < Launchpad-desktop-server-1.3.0.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。ファイルの [TAG] 列に [1.3.0] と表示されている必要があります。

次に例を示します。

```
$ docker images

REPOSITORY                                TAG      IMAGE ID      CREATED        SIZE
dockerhub.cisco.com/maglev-docker/server   1.3.0    f87ff30d4c6a 6 days ago    435MB
dockerhub.cisco.com/maglev-docker/client   1.3.0    dd50d550aa7c 6 days ago    832MB
```

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 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
5584b62d4170   dockerhub.cisco.com/maglev-docker/server:1.3.0   "docker-entrypoint.s..." 33 seconds ago Up 32 seconds   0.0.0.0:9090->8080/tcp   server
c771a7eb9c10   dockerhub.cisco.com/maglev-docker/client:1.3.0   "docker-entrypoint.s..." 58 seconds ago Up 57 seconds     0.0.0.0:90->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 問題のトラブルシューティング \(40 ページ\)](#) 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/api-docs/
```

次に例を示します。

```
http://192.0.2.2:9090/api/valaunchpad/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 ポータルを使用して 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

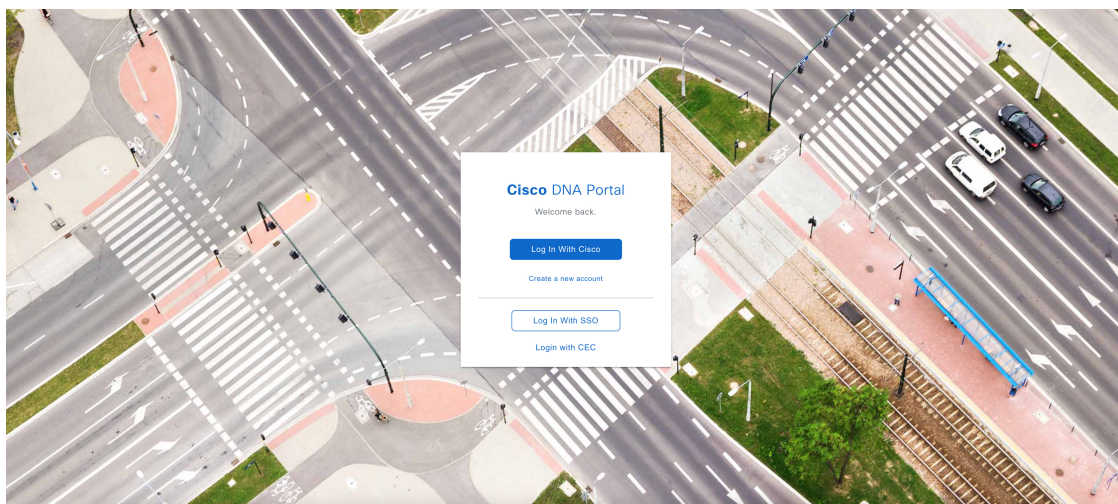
Cisco DNA ポータルを介して Cisco DNA Center VA 起動パッドにアクセスするには、最初にシスコアカウントを作成する必要があります。

手順

ステップ1 ブラウザで次のように入力します。

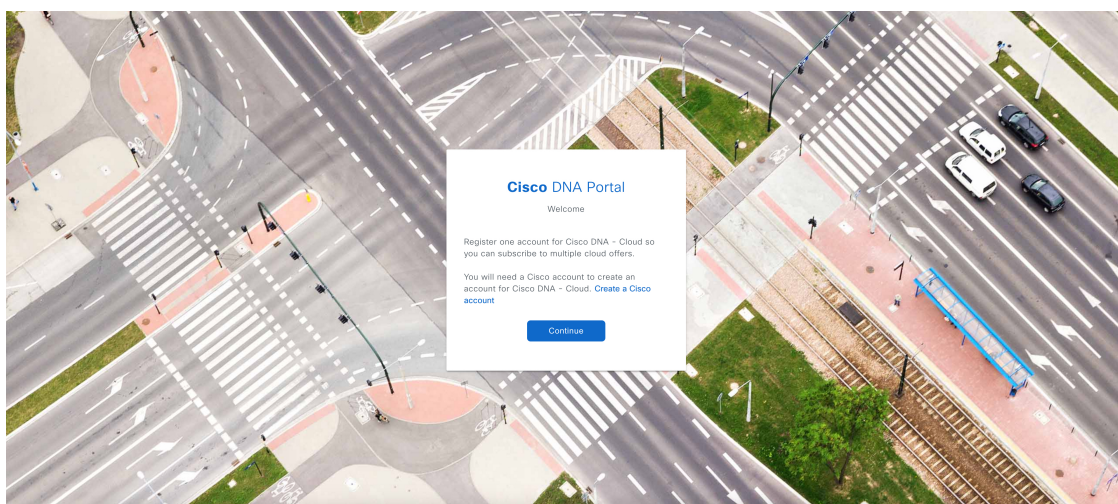
```
dna.cisco.com
```

Cisco DNA ポータル ログインウィンドウが表示されます。

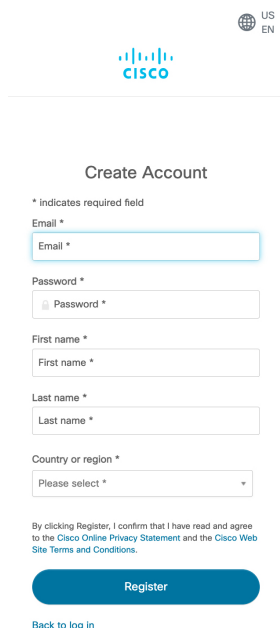


ステップ2 [Create a new account] をクリックします。

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。



US
EN

Create Account

* indicates required field

Email *

Password *

First name *

Last name *

Country or region *

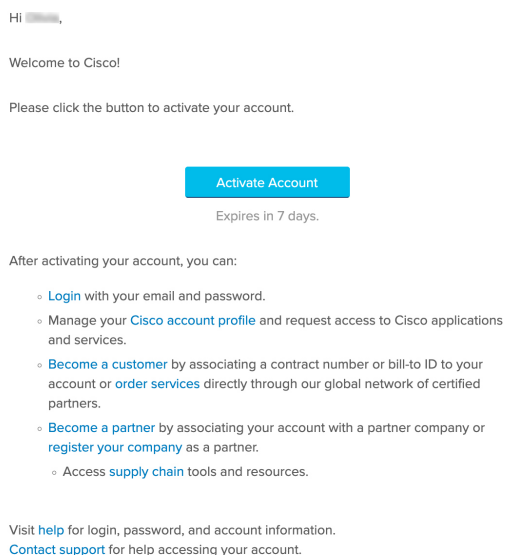
Please select *

By clicking Register, I confirm that I have read and agree to the [Cisco Online Privacy Statement](#) and the [Cisco Web Site Terms and Conditions](#).

Register

[Back to log in](#)

ステップ 5 アカウントに割り当て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。



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

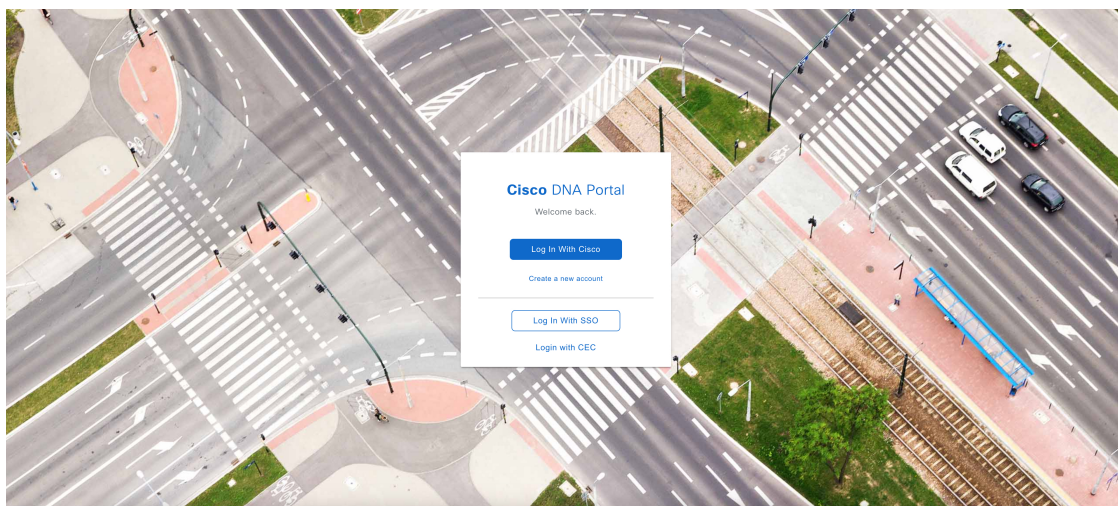
シスコアカウントがあることを確認します。詳細については、[シスコアカウントの作成（14ページ）](#)を参照してください。

手順

ステップ1 ブラウザで次のように入力します。

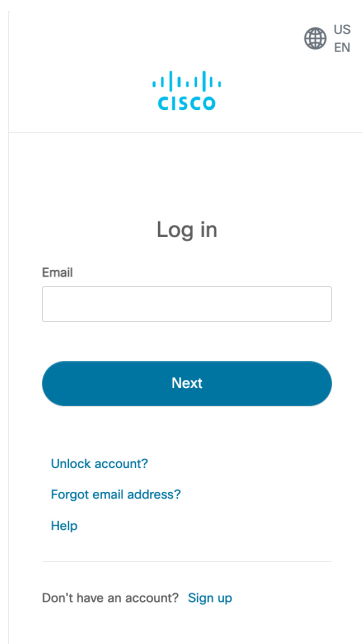
dna.cisco.com

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。



US
EN

CISCO

Log in

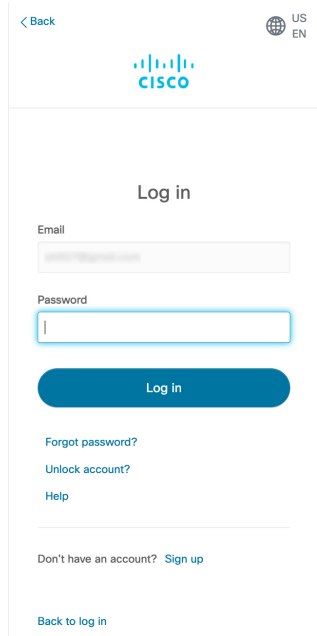
Email

Next

[Unlock account?](#)
[Forgot email address?](#)
[Help](#)

Don't have an account? [Sign up](#)

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、[Log in] をクリックします。



< Back

US
EN

CISCO

Log in

Email

Password

Log in

[Forgot password?](#)
[Unlock account?](#)
[Help](#)

Don't have an account? [Sign up](#)

[Back to log in](#)

ステップ 5 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。

Cisco DNA Portal

Welcome, [redacted]

What's the name of your organization, company, or team?

Name your account*

Ex. Hearst or Hearst Construction

Cancel

Continue

ステップ 6 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。

- 表示される情報が正しいことを確認します。
- 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。
- [Create Account] をクリックします。

Cisco DNA Portal

Confirm CCO Profile

Confirm that this is the Cisco profile you would like to register with, or [login to a different CCO](#).

Your Name [redacted]

Your Email [redacted]

Organization Name SELF

I agree that Cisco DNA Portal is governed by the [Cisco End User License Agreement](#) and that I have read and acknowledge the [Cisco Privacy Statement](#).

Note: If you do not have the authority to bind your company and its affiliates, or if you do not agree with the terms of the Cisco Universal Cloud Agreement, do not check this box.

Create Account

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。

シスコアカウントを使用した Cisco DNA ポータルへのログイン

シスコアカウントを使用した 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

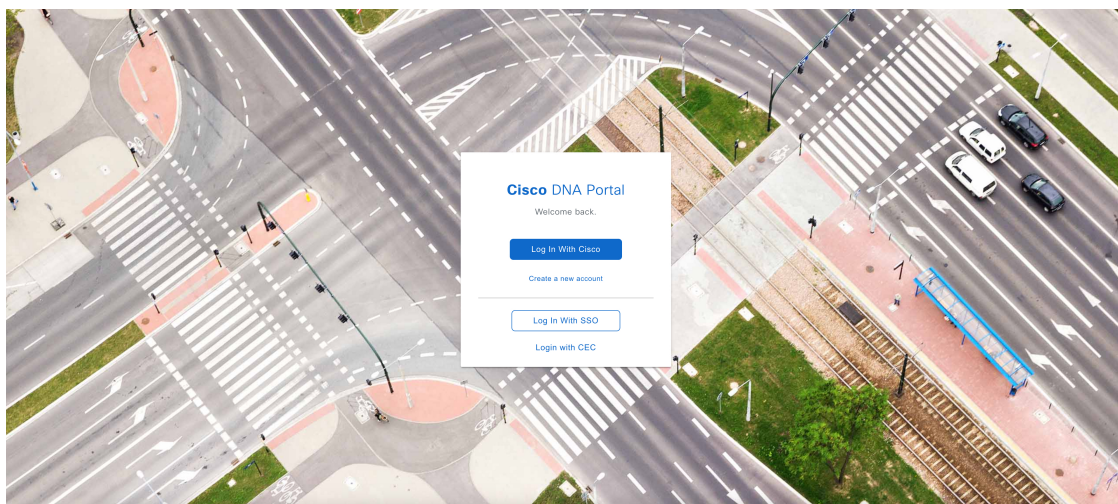
シスコアカウントと Cisco DNA ポータルアカウントがあることを確認します。詳細については、[シスコアカウントの作成 \(14 ページ\)](#) および [Cisco DNA ポータルアカウントの作成 \(16 ページ\)](#) を参照してください。

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、[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 5** (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

Choose an account

TestAccount	Continue
VA Launchpad	Continue
VALaunchpad-Test-Doc	Continue

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 DNA Center VA 起動パッドでは、複数の VA ポッドを作成できます。各 VA ポッドを使用して、Cisco DNA Center VA インスタンスを作成および管理できます。



- (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 つがすでに使用されている場合、選択したリージョンに対してさらに作成できる VA ポッドは最大 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 起動パッドの現行リリースで作成されたリソースは、旧リリースではサポートされません。たとえば、リリース 1.3.0 で作成された VA ポッドは、リリース 1.2.0 では削除できません。

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 \(8 ページ\)](#) を参照してください。

手順

ステップ 1 Cisco DNA Center VA 起動パッドにログインします。

(注) 複数のブラウザタブ、複数のブラウザウィンドウ、または複数のブラウザアプリケーションで同時にこのアプリケーションを開かないでください。

a) ブラウザウィンドウから、次のいずれかを実行します。

- Cisco DNA Center VA 起動パッドをローカルにインストールした場合、Cisco DNA Center VA 起動パッドの URL を次の形式で入力します。

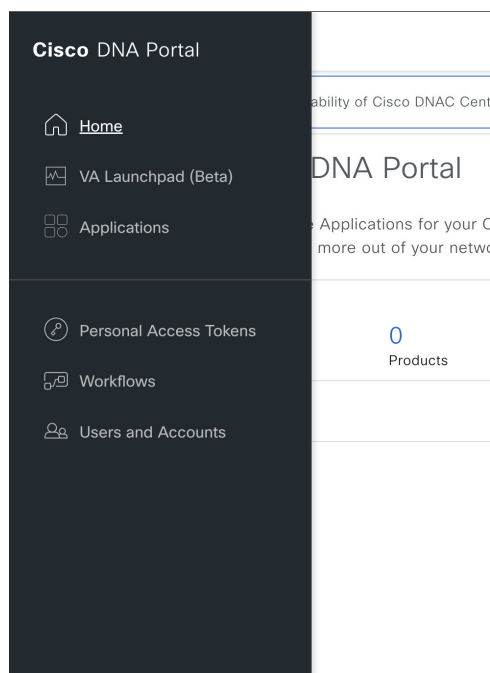
http://<localhost>:<client-port-number>/valaunchpad

次に例を示します。

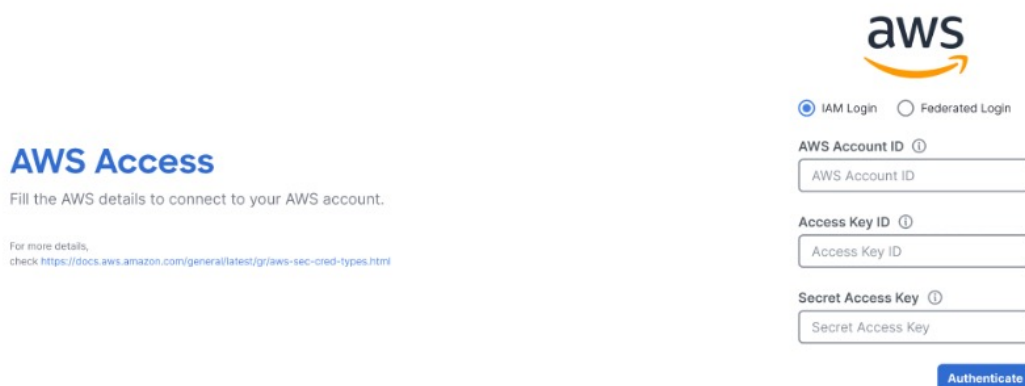
http://192.0.2.1:90/valaunchpad

- ホステッド型 Cisco DNA Center VA 起動パッドにアクセスする場合は、**dna.cisco.com** と入力し、表示される手順に従ってログインします (詳細については、[シスコアカウントを使用した Cisco DNA ポータルへのログイン \(20 ページ\)](#) を参照してください)。

Cisco DNA ポータル のホームページでメニューアイコンをクリックして選択 [VA Launchpad (Beta)] を選択します。



AWS ログインウィンドウが表示されます。



b) ユーザーログインを選択し、次のフィールドにログイン情報を入力します。

- [IAM Login]

詳細については、[シスコアカウントでのログイン \(69 ページ\)](#) を参照してください。

- [Federated Login]

詳細については、[saml2aws で生成したログイン情報を使用してフェデレーテッドユーザーとしてログインする \(72 ページ\)](#) または [AWS CLI で生成したログイン情報を使用してフェデレーテッドユーザーとしてログインする \(76 ページ\)](#) 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。

- c) [Authenticate] をクリックします。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 \(40 ページ\)](#) を参照してください。

管理者ユーザーの初回ログイン時に、いくつかのプロセスが発生します。

- 電子メールアドレスを入力するように求められます。[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。

Email to Notify

Please enter the Email address where notification needs to be sent if there are any Alerts on AWS Infrastructure.

Email ID ⓘ

Updating the email address will be used for newer VA Pods and not for existing VA Pods

電子メールアドレスは、アラームの通知と、設定されたリソースの監査ログの送信に使用されます。Amazon CloudWatch が Cisco DNA Center VA 起動パッドで異常な動作を検出すると、アラームがトリガーされます。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。電子メールアドレスの更新の詳細については、[Amazon CloudWatch 通知の設定 \(94 ページ\)](#) を参照してください。Amazon CloudWatch アラームの詳細については、[Amazon CloudWatch アラームの表示 \(96 ページ\)](#) を参照してください。

- AWS アカウント上に作成される CiscoDNACenter ユーザーグループには、必要なすべてのポリシーが割り当てられています。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。
- 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。
- また、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複数のリソースが AWS で作成されます。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** が表示されます。

リージョンのバージョン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。リリース 1.3.0 をインストールしてリージョンのバージョンを更新するには、その前にリリース 1.0.4（限定利用可能リリース）以上にする必要があることに注意してください。詳細については、[リージョンのバージョンの更新（83 ページ）](#) を参照してください。



ステップ 2 デフォルト（us-east-1）以外のリージョンに新しい VA ポッドを作成するには、[Region] ドロップダウンリストをクリックしてリージョンを選択します。

(注) リリース 1.3.0 で追加された新しいリージョンへのアクセスを有効にするには、Cisco DNA Center VA 起動パッドリリース 1.3.0 のインストール後に管理者ユーザーが Cisco DNA Center VA 起動パッドにログインする必要があります。管理者ユーザーがログインすると、すべてのリージョンへのアクセス権が他のすべてのユーザーに対して有効になります。

リージョンのバージョン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。リリース 1.3.0 をインストールしてリージョンのバージョンを更新するには、その前にリリース 1.0.4（限定利用可能リリース）以上にする必要があることに注意してください。詳細については、[リージョンのバージョンの更新（83 ページ）](#) 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 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、カスタマーゲートウェイを含む 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。名前はすべてのリージョンで一貫である必要があります。英字（A～Z と a～z）、数字（0～9）、ダッシュ（-）を使用できます。

- [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。
 - CIDR の推奨範囲は /25 です。
 - CIDR の最後のオクテットには、0 または 128 のみを使用できます。つまり、xxx0 または xxx128 になります。
 - 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、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 \(34 ページ\)](#) 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 ポッド設定の問題のトラブルシューティング \(43 ページ\)](#) 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 on AWS, Release 1.3.x](#)』[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 : maglev1@3
- パスフレーズ : maglev1@
- オープンポート : 22、2049、873、111

- f) [Next] をクリックします。
概要ページが表示されます。

Summary	
Review your AWS Infrastructure details and make changes. If you are satisfied with your selection, click the "Start Configuring AWS Infrastructure"	
VA Pod Environment Details	
VA Pod Name	LA-101-1a
Region	us-east-1
Availability Zone	us-east-1a
AWS VPC CIDR	172.16.0.0/16
On-prem Connectivity	
Transit Gateway (TGW)	VPN GW
VPN Attachment	
Customer Gateway (CGW)	New VPN GW
VPN DETAILS	
CGW (Enterprise Firewall/Router)	172.16.0.0/16
VPN Vendor	Cisco Systems, Inc.
Platform	ASA 5500 Series
Software	ASA 9.7+ VTI
Other Details	
Customer Profile	Medium
Backup Target	Cloud Backup (NFS)

- 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] ページが表示されます。

AWS Infrastructure Configured

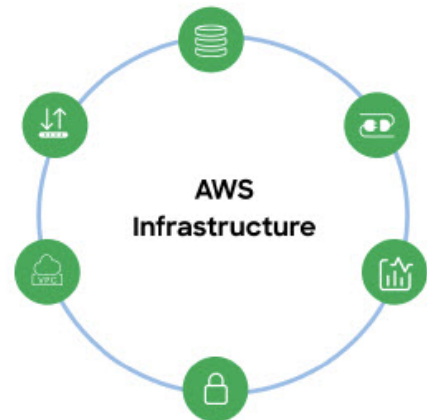
AWS::EC2::VPNGatewayRoutePropagation

AWS::EC2::VPNGatewayAttachment

AWS::EC2::VPNGateway

AWS::EC2::CustomerGateway

AWS::EC2::VPNConnectionRoute



(注) 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 \(40 ページ\)](#) を参照してください。

AWS Infrastructure Configured

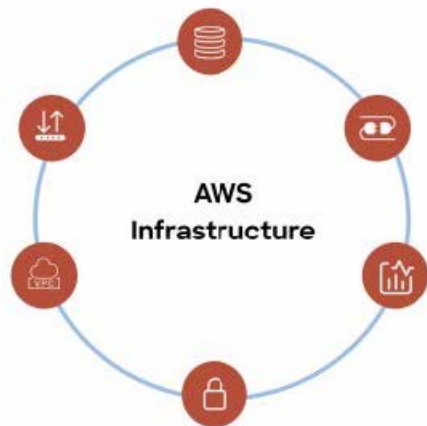
AWS::EC2::VPNGatewayRoutePropagation

AWS::EC2::VPNGatewayAttachment

AWS::EC2::VPNGateway

AWS::EC2::CustomerGateway

AWS::EC2::VPNConnectionRoute



ステップ 5 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] 画面で、[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 6 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。



- 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 起動ポッドは、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 (34 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 7 [Go to Dashboard] をクリックして Cisco DNA Center VA 起動パッドに戻ります。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 [Association] タブをクリックし、次に [Create Association] をクリックします。

The screenshot shows the AWS Transit Gateway console. The left sidebar is expanded to 'Transit gateway route tables'. The main content area shows the 'Associations' tab for the route table 'tgw-rtb-04cb3502f1649f635 / TEST-0-2-5-NTGW_VA_TGWVPNRouteTable'. The 'Associations' table is as follows:

Attachment ID	Resource type	Resource ID	State
tgw-attach-03f39a6abdb35a9b	VPC	vpc-048ab88f3c4178310	Associated
tgw-attach-014db4b572f2242e7	VPN	vpn-0f5a1d61c0d22f151	Associated
tgw-attach-0b046e367442fa5f	VPC	vpc-01fd251ea2f8000c9	Associated

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

The screenshot shows the AWS Transit Gateway console with the 'Propagations' tab selected for the same route table. The 'Propagations' table is as follows:

Attachment ID	Resource type	Resource ID	State
tgw-attach-014db4b572f2242e7	VPN	vpn-0f5a1d61c0d22f151	Enabled
tgw-attach-03f39a6abdb35a9b	VPC	vpc-048ab88f3c4178310	Enabled
tgw-attach-0b046e367442fa5f	VPC	vpc-01fd251ea2f8000c9	Enabled

- 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実際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 環境に割り当てられた CIDR 範囲宛てのネットワークトラフィックを CGW に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

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



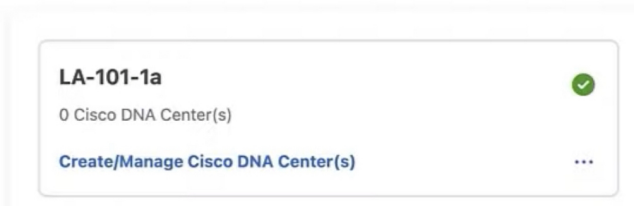
- (注) Cisco DNA Center VA 起動パッドの現行リリースで作成されたリソースは、旧リリースではサポートされません。たとえば、リリース 1.3.0 で作成された Cisco DNA Center VA は、リリース 1.2.0 では削除できません。

手順

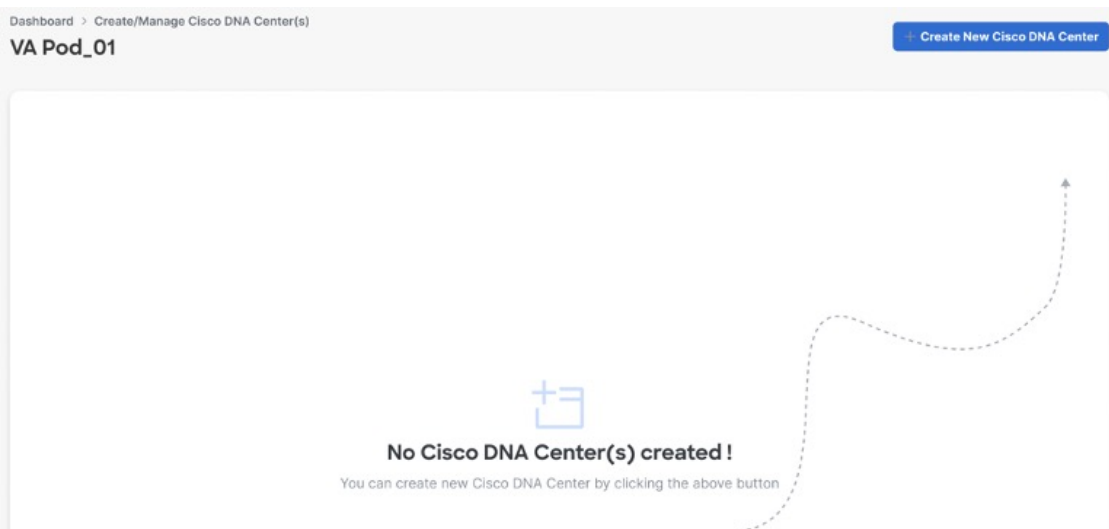
ステップ 1 Cisco DNA Center VA 起動パッドにログインします。

ステップ 2 作成した任意の VA ポッドを **Dashboard** で見つけ、VA ポッドカードで [Create/Manage Cisco DNA Center(s)] をクリックします。

Dashboard



ステップ 3 VA ポッドの [Create/Manage Cisco DNA Center(s)] ページで、[+ 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。
- [FQDN (Fully Qualified Domain Name)] : DNS サーバーで設定されている Cisco DNA Center 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 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 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 起動パッドリリース 1.0.4 以前では、DNS、プロキシ、および FQDN チェックが無効であっても、Cisco DNA Center VA の作成を続行できましたが、Cisco DNA Center VA 起動パッドリリース 1.3.0 では、DNS、プロキシ、または FQDN チェックに失敗した場合に設定を続行できるかどうかは、次に基づいて決まります。

- DNS 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 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 設定内容を確認します。

Summary

Review your Cisco DNA Center Virtual Appliance Configuration details and make any changes if needed. If you are satisfied, Start Cisco DNA Center Configuration now.

DOMAIN DETAILS

Enterprise DNS		✓
FQDN (Fully Qualified Domain Name)	dnac01.ciscodnacenter.com	✓

PROXY DETAILS ✓

Customer HTTP Network Proxy	No Proxy
-----------------------------	----------

[Exit](#)

[Back](#)

[Start Cisco DNA Center Configuration](#)

ステップ 7 設定に問題がない場合は、[Start Cisco DNA Center Configuration] をクリックします。

Cisco DNA Center VA 起動パッドで環境設定が開始されます。

環境設定が完了すると、Cisco DNA Center が起動します。最初は、Cisco DNA Center VA 起動パッド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。

Done! Cisco DNA Center Virtual Appliance Configured

It will take around 45 - 60 minutes to complete the setup.

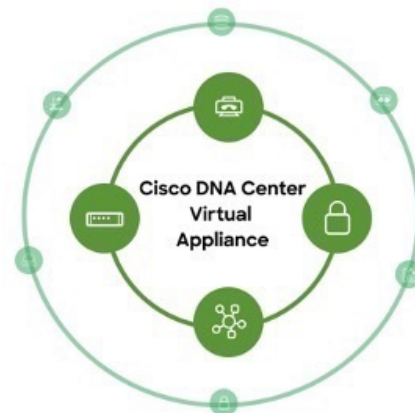
**Please do not leave the application or close the tab/window.
Otherwise, the setup will pause.**

Cisco DNA Center is booting up...

IP Address	[REDACTED]	
SSH Key	[REDACTED]	📄
PEM File	VA_Instance01.pem	📄

① Note: Please download and save the PEM file to accessing Cisco DNA Center. This is the only time that you will have access to download the pem file.

✔ Environment Setup completed

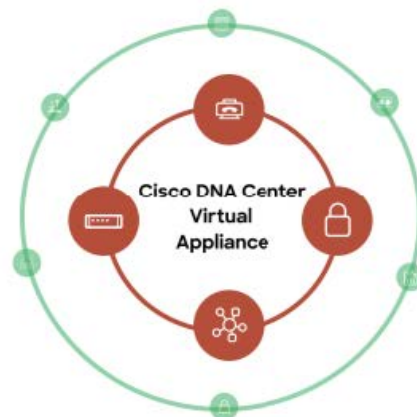


Exit [Go to Manage Cisco DNA Center\(s\)](#)

Cisco DNA Center の設定に失敗した場合は、[Create/Manage Cisco DNA Center(s)] ページに戻ります。詳細については、[展開のトラブルシューティング \(40 ページ\)](#) を参照してください。

Cisco DNA Center Configuration In progress

⊗ Environment Setup failed



ステップ 8 コピーアイコン (📄) をクリックして SSH キーをコピーし、ダウンロードアイコン (↓) をクリックして、後で参照できるように PEM ファイルをダウンロードします。

重要 SSH キーは後でダウンロードできないため、必ずダウンロードしてください。

ステップ 9 VA ポッドページに戻るには、[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 上の Cisco DNA Center の展開時の一般的な問題をトラブルシューティングする方法について説明します。



(注) 特に指定がない限り、AWS コンソールから手動で変更を行うことは避けてください。手動で変更すると、Cisco DNA Center VA 起動パッドで問題が発生することがあります。

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 問題のトラブルシューティング

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 (ポートがすでに使用されています)」というエラーが表示された場合は、次の考えられる解決策を使用して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
<p>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：</p> <p>port is already in use (ポートがすでに使用されています)</p>	<p>Docker でサーバーアプリケーションを実行します。</p> <pre>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</pre> <p>(注) 使用可能なサーバーポートをどれでも使用できます。</p> <p>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。</p> <pre>docker run -d -p 3001:3000 -e REACT_APP_API_URL=http://localhost:<client-port-number> --name client --pull=always dockerhub.cisco.com/maglev-docker/client:x.x.x</pre> <p>(注) サーバーアプリケーションの実行で使用したのと同じポート番号を使用する必要があります。</p>
<p>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：</p> <p>port is already in use (ポートがすでに使用されています)</p>	<p>Docker でクライアントアプリケーションを実行します。</p> <pre>docker run -d -p <client-port-name>:3000 --name client --pull=always dockerhub.cisco.com/maglev-docker/client:x.x.x</pre> <p>(注) 使用可能なサーバーポートをどれでも使用できます。</p>

ログインエラーのトラブルシューティング

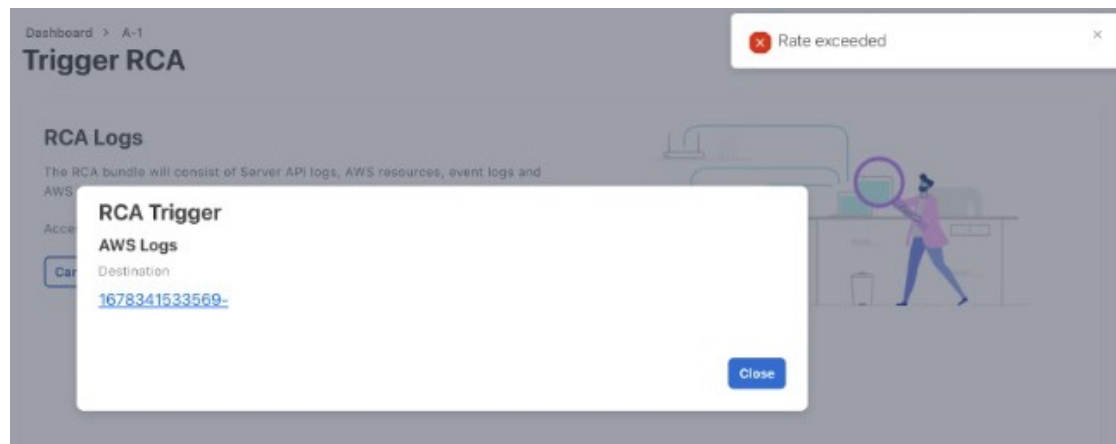
Cisco DNA Center VA 起動パッドにログインする際に、ログインエラーが発生する場合があります。次の一般的なログイン問題に対するトラブルシューティング方法を提供します。

エラーとその解決策は以下のとおりです。

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、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。

フリーズしたリージョン設定画面のトラブルシューティング

[Create a VA Pod] をクリックして新しいリージョンに新しい VA ポッドを作成すると、Cisco DNA Center VA 起動パッドによってリージョンが設定されます。この設定には約 2～3 分かかり、次の設定中のメッセージが表示されます。



Setting up the initial region configurations.
This might take a few minutes.

エラーメッセージが表示される場合や、画面が 5 分以上フリーズしたままで、設定中のメッセージが表示されない場合は、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。



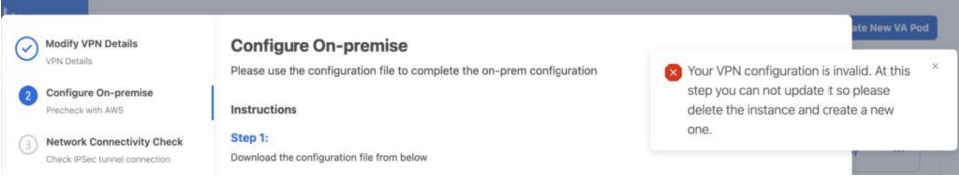
(注) このような競合状態を回避するには、VA ポッドを手動で変更しないことを推奨します。代わりに、すべてのアクションに Cisco DNA Center VA 起動パッドを使用してください。

VA ポッド設定の問題のトラブルシュート

新しい VA ポッドの作成に関連する VA ポッド設定の問題をトラブルシュートできます。

新しい VA ポッドを作成しようとしたときに次のエラーが発生した場合は、次の手順を実行します。

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)	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> • 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。 <p>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に対してさらに作成できる VA ポッドは 3 つまでです。</p> <p>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。</p> <ul style="list-style-type: none"> • 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 ポッドの作成を再実行します。
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。)	<p>[+ 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。</p> <p>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。</p>

エラー	考えられる解決策
<p>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。)</p>	<p>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。</p> <ul style="list-style-type: none"> • Barracuda • Sophos • Vyatta • Zyxel <p>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、次の警告が Cisco DNA Center VA 起動パッドに表示されます。</p> 
<p>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)</p>	<p>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。</p> <p>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。</p>
<p>AWS Infrastructure Failed. (AWS インフラストラクチャで障害が発生しました。)</p>	<p>AWS の設定に失敗した場合は、Dashboard 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 (23 ページ) を参照してください。</p> <p>(注) 設定に失敗した VA ポッドを削除できます。</p>
<p>AWS Configuration fails when editing a VA Pod (VA ポッドの編集時に AWS の設定に失敗しました)</p>	<p>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。</p> <p>(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。</p>
<p>Deleting VA Pod has failed (VA ポッドの削除に失敗しました)</p>	<p>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。</p> <p>(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。</p>

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ティング

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 へのトンネルがグレーの場合は、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 \(34 ページ\)](#) 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ティング

Cisco DNA Center VA の設定中に発生したエラーをトラブルシューティングできます。

エラーとその解決策は以下のとおりです。

同時実行エラーのトラブルシュート

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)	<ol style="list-style-type: none"> 1. Cisco DNA Center VA 起動パッドの [Create/Manage Cisco DNA Center(s)] ページに戻ります。 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

次の表は、以下に記載する同時実行エラーのトラブルシュートに役立ちます。

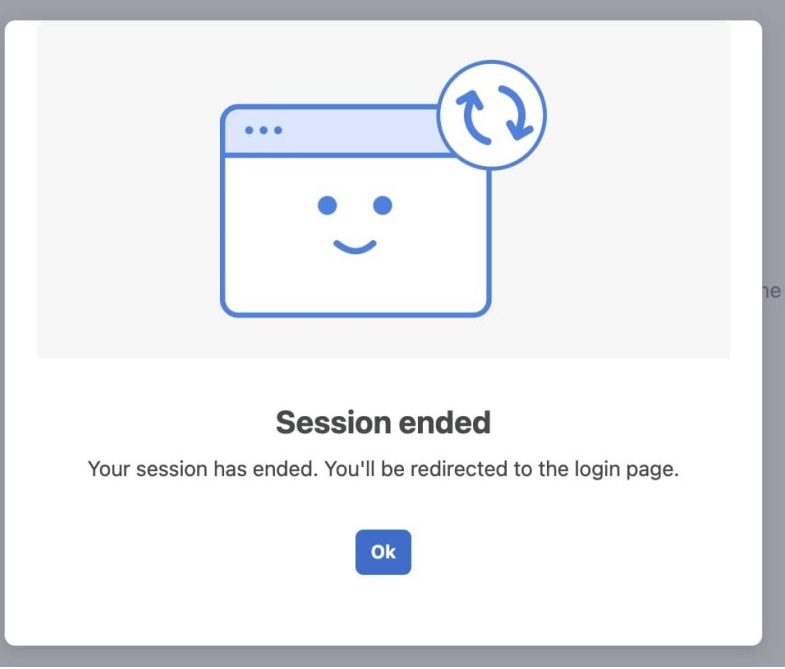
エラー	考えられる解決策
Unable to delete a Pod or a Cisco DNA Center created by another user. (別のユーザーが作成したポッドや Cisco DNA Center は削除できません。)	<p>別のユーザーが作成した VA ポッドや Cisco DNA Center VA などコンポーネントは、そのコンポーネントで別のアクションが進行中は削除できません。アクションが完了すると、自分または他のユーザーがそのコンポーネントを削除できます。</p> <p>たとえば、VA ポッドや Cisco DNA Center VA が次のプロセス中または状態にある場合は削除できません。</p> <ul style="list-style-type: none"> • 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。)	<p>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。</p> <p>VA ポッドの更新ステータスを表示するには、[Refresh] をクリックします。</p>

展開に関するその他の問題のトラブルシュート

AWS に Cisco DNA Center VA を展開する際に発生するその他の問題をトラブルシュートできます。

問題とその解決策は以下のとおりです。

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。	<p>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。</p> <p>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され、ロードされると、[Proceed] ボタンが有効になります。</p>
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。	<p>次のことを確認してください。</p> <ul style="list-style-type: none"> • 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 アドレスがこの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	<p>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。</p> <div data-bbox="451 380 1247 1045" style="border: 1px solid #ccc; padding: 10px; text-align: center;">  <p>Session ended</p> <p>Your session has ended. You'll be redirected to the login page.</p> <p>Ok</p> </div> <p>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。</p>

AWS CloudFormation を使用した AWS 上の 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

この方法で AWS 上の Cisco DNA Center を展開するには、次の手順を実行します。

1. 前提条件が満たされていることを確認します。[AWS CloudFormation を使用した手動展開の前提条件 \(49 ページ\)](#) を参照してください。
2. AWS 上の Cisco ISE と Cisco DNA Center VA を統合する場合は、[AWS 上の Cisco ISE と AWS 上の Cisco DNA Center の統合に関するガイドライン \(4 ページ\)](#) を参照してください。

3. AWS CloudFormation を使用して AWS 上の Cisco DNA Center を展開します。[AWS CloudFormation を使用した AWS 上の Cisco DNA Center の手動展開 \(55 ページ\)](#) 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 \(59 ページ\)](#) 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

ここで紹介する前提条件は、AWS CloudFormation を使用した手動展開に適用されます。自動方式または AWS Marketplace を使用した手動の展開方式でも Cisco DNA Center を展開できます。それぞれの方法のメリットとデメリットについては、[展開の概要 \(2 ページ\)](#) を参照してください。

AWS 上の 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 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

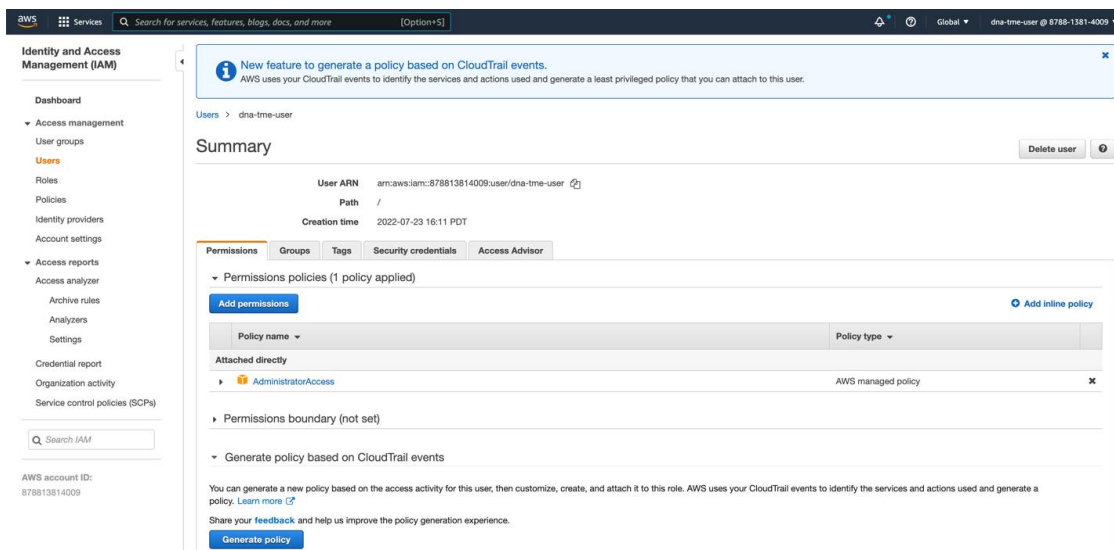
次の AWS 環境要件を満たす必要があります。

- 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 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。
- 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] : CIDR の推奨範囲は /25 です。CIDR の最後のオクテットには、0 または 128 のみを使用できます（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 (22)

Filter security group rules

Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
-	sgr-0482eb11896826fec	IPv4	Custom TCP	TCP	111	0.0.0.0/0	-
-	sgr-06112d895e265c2...	IPv4	Custom TCP	TCP	9005	0.0.0.0/0	-
-	sgr-0e6511be2e699ad...	IPv4	All TCP	TCP	0 - 65535	172.16.2.0/28	-
-	sgr-0c67e0ac5b8dffde3	IPv4	Custom UDP	UDP	21750	0.0.0.0/0	-
-	sgr-04bd504b473ccd7c6	IPv4	Custom UDP	UDP	162	0.0.0.0/0	-
-	sgr-09f72040be517ac12	IPv4	HTTPS	TCP	443	0.0.0.0/0	-
-	sgr-0a7098c3b2bab6a1	IPv4	NFS	TCP	2049	0.0.0.0/0	-
-	sgr-07ac7f99f8c942056	IPv4	Custom TCP	TCP	9004	0.0.0.0/0	-
-	sgr-04840db2face92a23	IPv4	Custom TCP	TCP	25103	0.0.0.0/0	-
-	sgr-0a2ba3dea618510...	IPv4	Custom UDP	UDP	2049	0.0.0.0/0	-
-	sgr-01b8e84fa1d0e9031	IPv4	Custom TCP	TCP	9991	0.0.0.0/0	-
-	sgr-065328ee42f1fbfd	IPv4	Custom UDP	UDP	6007	0.0.0.0/0	-
-	sgr-0e0f86cb88d098324	IPv4	SSH	TCP	22	0.0.0.0/0	-
-	sgr-0015c86702bd994f3	IPv4	Custom TCP	TCP	2222	0.0.0.0/0	-
-	sgr-0901d46c360997...	IPv4	All UDP	UDP	0 - 65535	172.16.2.0/28	-
-	sgr-0d5787d5a0646fae8	IPv4	All ICMP - IPv4	ICMP	All	0.0.0.0/0	-
-	sgr-0530e136dfe73d8d9	IPv4	Custom TCP	TCP	873	0.0.0.0/0	-
-	sgr-0af12dadde93f014	IPv4	Custom UDP	UDP	111	0.0.0.0/0	-
-	sgr-0d3f55a192c8fb4a	IPv4	HTTP	TCP	80	0.0.0.0/0	-
-	sgr-0897d44466641b...	IPv4	Custom TCP	TCP	32626	0.0.0.0/0	-
-	sgr-05e4179da8996b0fb	IPv4	Custom UDP	UDP	514	0.0.0.0/0	-
-	sgr-0b45333d5134f8a...	IPv4	Custom UDP	UDP	123	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 (23)

Filter security group rules

Name	Security group rule...	IP version	Type	Protocol	Port range	Destination	Description
-	sgr-0e208c10731f66fde	IPv4	NFS	TCP	2049	0.0.0.0/0	-
-	sgr-0a67f0e542c9e8d3e	IPv4	Custom UDP	UDP	123	0.0.0.0/0	-
-	sgr-02e060f15d6998...	IPv4	Custom TCP	TCP	49	0.0.0.0/0	-
-	sgr-0d51e1643d50f72a	IPv4	Custom TCP	TCP	9991	0.0.0.0/0	-
-	sgr-03b22337742ea6...	IPv4	Custom UDP	UDP	111	0.0.0.0/0	-
-	sgr-0c1d1d9a7e4f55bbf	IPv4	Custom UDP	UDP	1812	0.0.0.0/0	-
-	sgr-0b5c884f021d0b99	IPv4	Custom TCP	TCP	23	0.0.0.0/0	-
-	sgr-0795765cabe1c2095	IPv4	HTTPS	TCP	443	0.0.0.0/0	-
-	sgr-097cc931b815b43...	IPv4	Custom UDP	UDP	1645	0.0.0.0/0	-
-	sgr-0fada929aecd05db	IPv4	Custom TCP	TCP	8910	0.0.0.0/0	-
-	sgr-0c9d0454fc1c8bb2e	IPv4	All TCP	TCP	0 - 65535	172.16.2.0/28	-
-	sgr-0341f0b3e872b73...	IPv4	HTTP	TCP	80	0.0.0.0/0	-
-	sgr-014ced79443b904fc	IPv4	Custom TCP	TCP	9060	0.0.0.0/0	-
-	sgr-01abd82ce50608...	IPv4	Custom UDP	UDP	2049	0.0.0.0/0	-
-	sgr-0c22f51a7396d4f25	IPv4	Custom TCP	TCP	873	0.0.0.0/0	-
-	sgr-0f0a1426fabee5234	IPv4	DNS (UDP)	UDP	53	0.0.0.0/0	-
-	sgr-0d70c7499320d3...	IPv4	Custom TCP	TCP	5222	0.0.0.0/0	-
-	sgr-0c78bb5393f7fb78	IPv4	Custom UDP	UDP	161	0.0.0.0/0	-
-	sgr-01973931a8d884...	IPv4	SSH	TCP	22	0.0.0.0/0	-
-	sgr-061ef5612e74dad4b	IPv4	Custom TCP	TCP	111	0.0.0.0/0	-
-	sgr-0b3d8aa9ef6abd56	IPv4	Custom TCP	TCP	830	0.0.0.0/0	-
-	sgr-06e5b34277c7da2...	IPv4	All ICMP - IPv4	ICMP	All	0.0.0.0/0	-
-	sgr-06e40371754c806...	IPv4	All UDP	UDP	0 - 65535	172.16.2.0/28	-

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	<p>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。</p> <p>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。</p> <p>(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。</p>	<p>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。</p> <p>(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。</p>
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 アシユアランス 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 アシユアランス 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か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](#)』[英語]の「Plan the Deployment」の章に記載されている「Required Network Ports」を参照してください。

- [Site-to-Site VPN Connection] : トランジット ゲートウェイ アタッチメントとトランジット ゲートウェイ 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 (AWS インスタンスタイプは、推奨される最小サイジング仕様の一例です)



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 on AWS, Release 1.3.x](#)』[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 ユーザー名/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 上の Cisco DNA Center の手動展開

Cisco DNA Center VA の展開は、AWS CloudFormation を使用して手動で実行できます。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)**
- **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 \(49 ページ\)](#) 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 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-1.3.0.tar.gz

この TAR ファイルには、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。

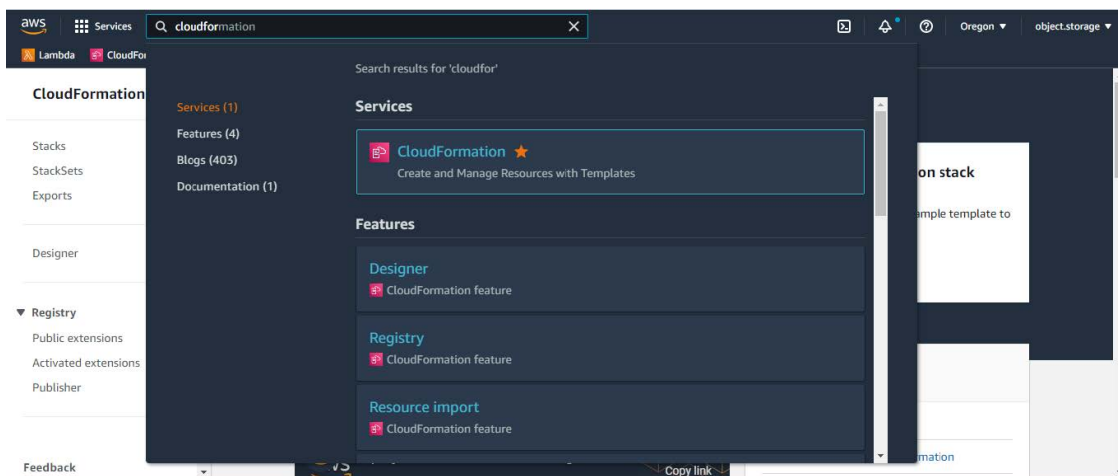
リージョン	Cisco DNA Center AMI ID
ap-northeast-1 (東京)	ami-0e15eb31bcb994472
ap-northeast-2 (ソウル)	ami-043e1b9f3ccace4b2
ap-south-1 (ムンバイ)	ami-0bbdbd7bcc1445c5f
ap-southeast-1 (シンガポール)	ami-0c365aa4cfb5121a9
ap-southeast-2 (シドニー)	ami-0d2d9e5ebb58de8f7
ca-central-1 (カナダ)	ami-0485cfd8da5244c6e
eu-central-1 (フランクフルト)	ami-0677a8e229a930434
eu-south-1 (ミラノ)	ami-091f667a02427854d
eu-west-1 (アイルランド)	ami-0a8a59b277dff9306
eu-west-2 (ロンドン)	ami-0cf5912937286b42e
eu-west-3 (パリ)	ami-0b12cfdd092ef754e
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 \(6 ページ\)](#) 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。

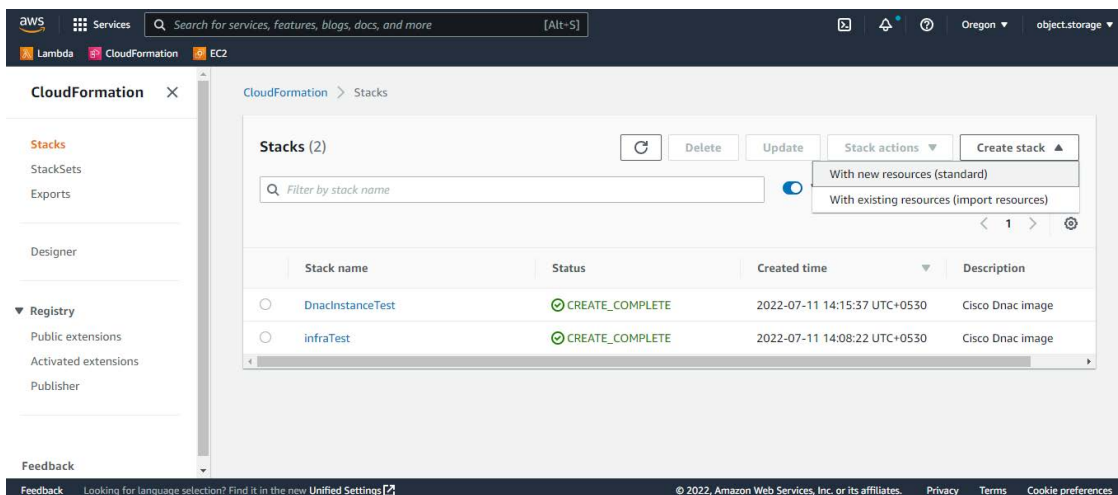
AWS コンソールが表示されます。

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

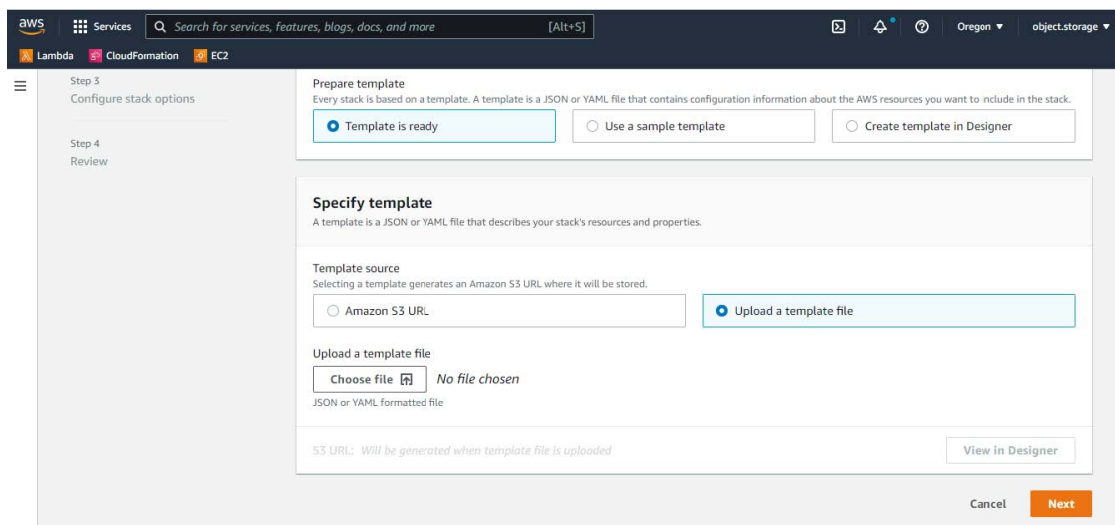


ステップ5 ドロップダウンメニューから [CloudFormation] を選択します。

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。

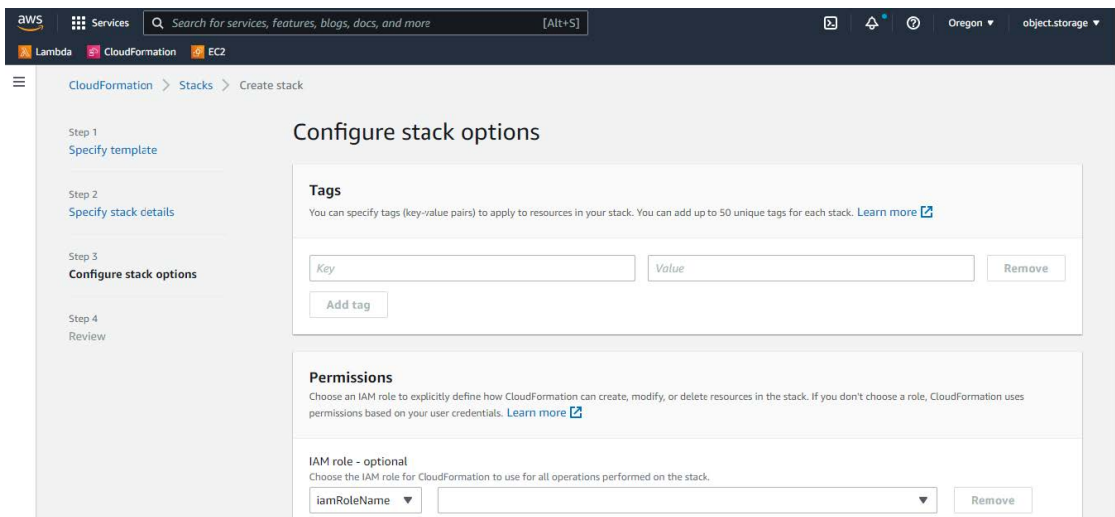
- [DnacInstanceIP] : Cisco DNA Center の IP アドレス。
- [DnacNetmask] : Cisco DNA Center のネットマスク。
- [DnacGateway] : Cisco DNA Center のゲートウェイアドレス。
- [DnacDnsServer] : エンタープライズ DNS サーバー。
- [DnacPassword] : Cisco DNA Center のパスワード。

(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。

- [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。

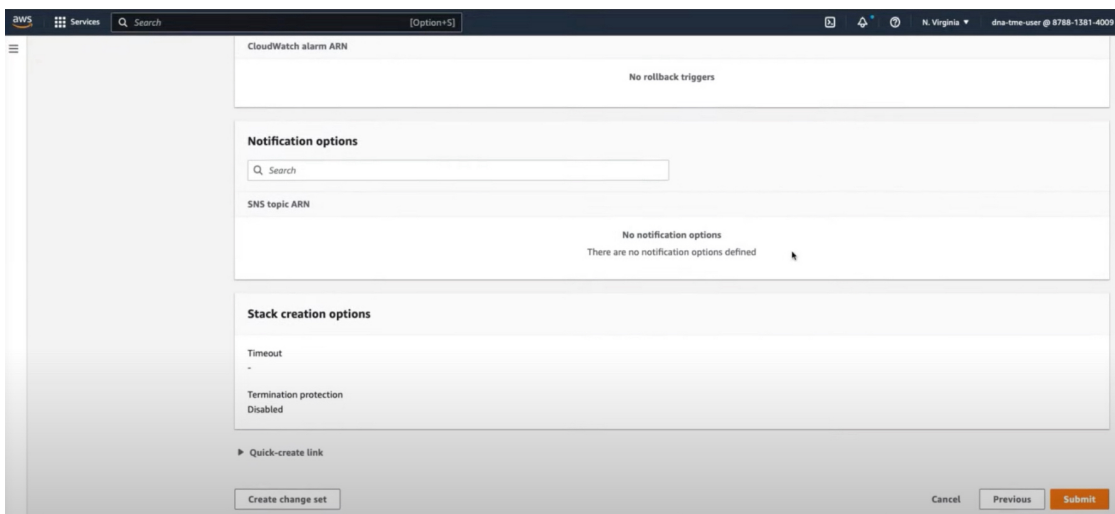
- [DnacHttpsProxyPassword] : (オプション) HTTPS プロキシのパスワード。

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** 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 2** 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 3** ブラウザを使用して、Cisco DNA Center GUI への HTTPS アクセスをテストします。
- ブラウザの互換性の詳細については、『[Release Notes for AWS 上の Cisco DNA Center, Release 1.3.x](#)』[英語]を参照してください。
-

AWS Marketplace を使用して AWS に Cisco DNA Center を手動展開する

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

この方法で AWS 上の Cisco DNA Center を展開するには、次の手順を実行します。

1. 前提条件が満たされていることを確認します。[AWS Marketplace を使用した手動展開の前提条件 \(60 ページ\)](#) を参照してください。
2. AWS 上の Cisco ISE と Cisco DNA Center VA を統合する計画がある場合は、[AWS 上の Cisco ISE と AWS 上の Cisco DNA Center の統合に関するガイドライン \(4 ページ\)](#) を参照してください。
3. AWS Marketplace を使用して AWS 上の Cisco DNA Center を展開します。[AWS Marketplace を使用して AWS に Cisco DNA Center を手動展開する \(67 ページ\)](#) 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 \(67 ページ\)](#) 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

ここで紹介する前提条件は、AWS Marketplace を使用した手動展開に適用されます。自動方式または AWS Marketplace を使用した手動の展開方式でも Cisco DNA Center を展開できます。そ

それぞれの方法のメリットとデメリットについては、[展開の概要（2 ページ）](#) を参照してください。

AWS 上の 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 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 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。
- 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）。

The screenshot shows the AWS IAM console interface. On the left is the navigation menu for Identity and Access Management (IAM). The main content area displays the 'Summary' page for a user named 'dna-tme-user'. Key details include: User ARN: arn:aws:iam::878813814009:user/dna-tme-user, Path: /, and Creation time: 2022-07-23 16:11 PDT. Under the 'Permissions' tab, it shows 'Permissions policies (1 policy applied)' with a table listing the attached policy 'AdministratorAccess' as an 'AWS managed policy'. At the bottom, there is a section for 'Generate policy based on CloudTrail events' with a 'Generate policy' button.

- 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] : CIDR の推奨範囲は /25 です。CIDR の最後のオクテットには、0 または 128 のみを使用できます（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。

Name	Security group rule	IP version	Type	Protocol	Port range	Source	Description
-	sg-0482eb1896826fec	IPv4	Custom TCP	TCP	111	0.0.0.0	-
-	sg-06112d899e265c2...	IPv4	Custom TCP	TCP	9005	0.0.0.0	-
-	sg-0e6511be2e699ad...	IPv4	All TCP	TCP	0 - 65535	172.16.2.0/28	-
-	sg-0c67e0ac5b8dffde3	IPv4	Custom UDP	UDP	21730	0.0.0.0	-
-	sg-04bd504b473ccd7c6	IPv4	Custom UDP	UDP	162	0.0.0.0	-
-	sg-09f720408e517ac12	IPv4	HTTPS	TCP	443	0.0.0.0	-
-	sg-0a7098c3b2babca1	IPv4	NFS	TCP	2049	0.0.0.0	-
-	sg-07ac7f99fb942056	IPv4	Custom TCP	TCP	9004	0.0.0.0	-
-	sg-048d0db2face92a23	IPv4	Custom TCP	TCP	25103	0.0.0.0	-
-	sg-0a2ba3dea618510...	IPv4	Custom UDP	UDP	2049	0.0.0.0	-
-	sg-01b8e84fa1d0e9031	IPv4	Custom TCP	TCP	9991	0.0.0.0	-
-	sg-065328ee42f1fbfd	IPv4	Custom UDP	UDP	6007	0.0.0.0	-
-	sg-0b0f86cb88d098324	IPv4	SSH	TCP	22	0.0.0.0	-
-	sg-0015c86702bd994f3	IPv4	Custom TCP	TCP	2222	0.0.0.0	-
-	sg-0901d46c360997...	IPv4	All UDP	UDP	0 - 65535	172.16.2.0/28	-
-	sg-0d5787d5a064fae8	IPv4	All ICMP - IPv4	ICMP	All	0.0.0.0	-
-	sg-0530e136dfe73d8d9	IPv4	Custom TCP	TCP	873	0.0.0.0	-
-	sg-0af12dadde93f014	IPv4	Custom UDP	UDP	111	0.0.0.0	-
-	sg-0d3f55a192c58fb4a	IPv4	HTTP	TCP	80	0.0.0.0	-
-	sg-0897d44466641b...	IPv4	Custom TCP	TCP	32626	0.0.0.0	-
-	sg-05e4179da8996b0fb	IPv4	Custom UDP	UDP	514	0.0.0.0	-
-	sg-0b4533d3134f8a...	IPv4	Custom UDP	UDP	123	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。

Name	Security group rule...	IP version	Type	Protocol	Port range	Destination	Description
-	sgr-0e208c10731166fde	IPv4	NFS	TCP	2049	0.0.0.0/0	-
-	sgr-0a67f0e5429e8d3e	IPv4	Custom UDP	UDP	123	0.0.0.0/0	-
-	sgr-02e060f15d6998...	IPv4	Custom TCP	TCP	49	0.0.0.0/0	-
-	sgr-0d51e1643d50f672a	IPv4	Custom TCP	TCP	9991	0.0.0.0/0	-
-	sgr-03b22337742ea6...	IPv4	Custom UDP	UDP	111	0.0.0.0/0	-
-	sgr-0c1d1d9a7e4f55bbf	IPv4	Custom UDP	UDP	1812	0.0.0.0/0	-
-	sgr-0b5c8844021dd0b9	IPv4	Custom TCP	TCP	23	0.0.0.0/0	-
-	sgr-0795765cabe1c2095	IPv4	HTTPS	TCP	443	0.0.0.0/0	-
-	sgr-097c931b815b43...	IPv4	Custom UDP	UDP	1645	0.0.0.0/0	-
-	sgr-0fada929aef05db	IPv4	Custom TCP	TCP	8910	0.0.0.0/0	-
-	sgr-0c9d0454fc1c8bb2e	IPv4	All TCP	TCP	0 - 65535	172.16.2.0/28	-
-	sgr-0341fdb5e872b73...	IPv4	HTTP	TCP	80	0.0.0.0/0	-
-	sgr-014ced79443b904fc	IPv4	Custom TCP	TCP	9060	0.0.0.0/0	-
-	sgr-01abd82ce5b06d8...	IPv4	Custom UDP	UDP	2049	0.0.0.0/0	-
-	sgr-0c22f51a7396d4f25	IPv4	Custom TCP	TCP	875	0.0.0.0/0	-
-	sgr-0f0a1426fabee5234	IPv4	DNS (UDP)	UDP	53	0.0.0.0/0	-
-	sgr-0d70c7499320d3...	IPv4	Custom TCP	TCP	5222	0.0.0.0/0	-
-	sgr-0c78bb53937f7b78	IPv4	Custom UDP	UDP	161	0.0.0.0/0	-
-	sgr-01973931a8d884...	IPv4	SSH	TCP	22	0.0.0.0/0	-
-	sgr-061ef5612e74dad4b	IPv4	Custom TCP	TCP	111	0.0.0.0/0	-
-	sgr-0b3d8aa9ef60abd56	IPv4	Custom TCP	TCP	850	0.0.0.0/0	-
-	sgr-06e5b34277c7da2...	IPv4	All ICMP - IPv4	ICMP	All	0.0.0.0/0	-
-	sgr-06e40371754c806...	IPv4	All UDP	UDP	0 - 65535	172.16.2.0/28	-

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	<p>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。</p> <p>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。</p> <p>(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。</p>	<p>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。</p> <p>(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。</p>

ポート	サービス名	目的	推奨処置
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。
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 アシユアランス 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 アシユアランス 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](#)』[英語]の「Plan the Deployment」の章に記載されている「Required Network Ports」を参照してください。

- [Site-to-Site VPN Connection] : トランジット ゲートウェイ アタッチメントとトランジット ゲートウェイ 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 (AWS インスタンスタイプは、推奨される最小サイジング仕様の一例です)



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 on AWS, Release 1.3.x](#)』 [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 Setting]
 - デフォルトゲートウェイ設定
 - CLI パスワード
 - UI ユーザー名/パスワード
 - スタティック IP (Static IP)
 - Cisco DNA Center VA IP アドレスの FQDN

AWS Marketplace を使用して AWS に Cisco DNA Center を手動展開する

AWS 上の Cisco DNA Center を使用して AWS Marketplace 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 を使用して AWS に Cisco DNA Center を展開する

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 でのスタック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** 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 2** 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 3** ブラウザを使用して、Cisco DNA Center GUI への HTTPS アクセスをテストします。
ブラウザの互換性の詳細については、『[Release Notes for AWS 上の Cisco DNA Center, Release 1.3.x](#)』[英語]を参照してください。

バックアップと復元

バックアップおよび復元機能を使用して、バックアップファイルを作成し、別のアプライアンスに復元できます。Cisco DNA Center VA では、次の 2 つの方法でデータをバックアップおよび復元できます。

- Cisco DNA Center ハードウェアアプライアンスからデータをバックアップし、Cisco DNA Center VA にデータを復元します。
- 任意の Cisco DNA Center VA からデータをバックアップし、別の Cisco DNA Center VA にデータを復元します。

バックアップと復元（ハードウェアアプライアンスから VA）

Cisco DNA Center ハードウェアアプライアンスからデータをバックアップし、Cisco DNA Center VA にデータを復元します。

始める前に

ハードウェアアプライアンスの場合は、44 コア Cisco DNA Center アプライアンスを使用してデータをバックアップおよび復元します。

手順

-
- ステップ 1** Cisco DNA Center ハードウェアアプライアンスからデータをバックアップします。手順については、『[Cisco DNA Center Administrator Guide, Release 2.3.5](#)』 [英語] の「Backup and Restore」の章を確認してください。
- バックアップサーバーが VPN を介して Cisco DNA Center に接続されていることを確認します。
- ステップ 2** Cisco DNA Center VA を作成します。詳細については、[新しい Cisco DNA Center VA の作成 \(36 ページ\)](#) を参照してください。
- Cisco DNA Center VA が稼働していることを確認します。
- ステップ 3** Cisco DNA Center VA をステップ 1 のバックアップサーバーに接続します。
- バックアップサーバーが Cisco DNA Center VA から到達可能であることを確認します。
- ステップ 4** Cisco DNA Center VA でバックアップサーバーを設定します。
- ステップ 5** データを Cisco DNA Center VA に復元します。
-

バックアップと復元 (VA から VA)

任意の Cisco DNA Center VA からデータをバックアップして、別の Cisco DNA Center VA にデータを復元できます。

始める前に

Cisco DNA Center VA 起動パッドまたは AWS CloudFormation を使用して 2 つの Cisco DNA Center VA が正常に展開されていることを確認します。詳細については、[自動展開方式を使用した AWS 上の Cisco DNA Center の展開 \(7 ページ\)](#) または [AWS CloudFormation を使用した AWS 上の Cisco DNA Center の手動展開 \(48 ページ\)](#) を参照してください。

手順

-
- ステップ 1** Cisco DNA Center VA からデータをバックアップします。手順については、『[Cisco DNA Center Administrator Guide, Release 2.3.5](#)』 [英語] の「Backup and Restore」の章を確認してください。
- バックアップサーバーが VPN を介して Cisco DNA Center VA に接続されていることを確認します。
- ステップ 2** 復元する Cisco DNA Center VA を起動します。

この Cisco DNA Center VA が稼働していることを確認します。

- ステップ 3** 復元する Cisco DNA Center VA をステップ 1 のバックアップサーバーに接続します。
バックアップサーバーが Cisco DNA Center VA から到達可能であることを確認します。
- ステップ 4** 復元する Cisco DNA Center VA のバックアップサーバーを設定します。
- ステップ 5** データを Cisco DNA Center VA に復元します。

Cisco DNA Center VA 起動パッドを使用した VA ポッドとユーザー設定の管理

Cisco DNA Center VA 起動パッドでは、VA ポッド、Cisco DNA Center VA、およびユーザー設定を管理できます。

Cisco Launchpad へのログイン

Cisco DNA Center VA 起動パッドは次の認証方式をサポートしています。

- [シスコアカウントを使用した Cisco DNA ポータル へのログイン](#) : この方法では、シスコアカウントのログイン情報を使用します。
- [フェデレーテッドユーザーとしてログイン](#) : フェデレーテッドアクセスでは、組織などのアイデンティティプロバイダー (IdP) がユーザー認証と Cisco DNA Center VA 起動パッドへの情報送信を実行し、ログイン後に付与されるリソースへのアクセス権の範囲決定をサポートします。初回ログイン時に、ユーザーには CiscoDNACenter ロールを作成する管理者ユーザーロールが割り当てられます。管理者は CiscoDNACenter ロールを後続のユーザーに割り当てることができます。CiscoDNACenter ロールには、CiscoDNACenter ユーザーグループと同じ権限が付与されます。CiscoDNACenter ロールによって付与される権限の詳細については、[自動展開の前提条件 \(8 ページ\)](#) を参照してください。

saml2aws CLI または AWS CLI を使用して、フェデレーテッドユーザーとして Cisco DNA Center VA 起動パッドにログインするためのトークンを生成できます。詳細については、次のトピックを参照してください。

- [saml2aws で生成したログイン情報を使用してフェデレーテッドユーザーとしてログインする \(72 ページ\)](#)
- [AWS CLI で生成したログイン情報を使用してフェデレーテッドユーザーとしてログインする \(76 ページ\)](#)

シスコアカウントでのログイン

この手順では、Cisco DNA Center VA 起動パッドにログインする方法を示します。

始める前に

次の要件が満たされていることを確認します。

- 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。詳細については、[自動展開の前提条件 \(8 ページ\)](#) を参照してください。
- Cisco DNA Center VA 起動パッドがインストールされているか、ホステッド型 Cisco DNA Center VA 起動パッドにアクセスできる。
- AWS のアカウント ID、アクセスキー ID、およびシークレットアクセスキーが用意されている。

手順

ステップ 1 ブラウザウィンドウから、次のいずれかを実行します。

- Cisco DNA Center VA 起動パッドをローカルにインストールした場合、Cisco DNA Center VA 起動パッドの URL を次の形式で入力します。

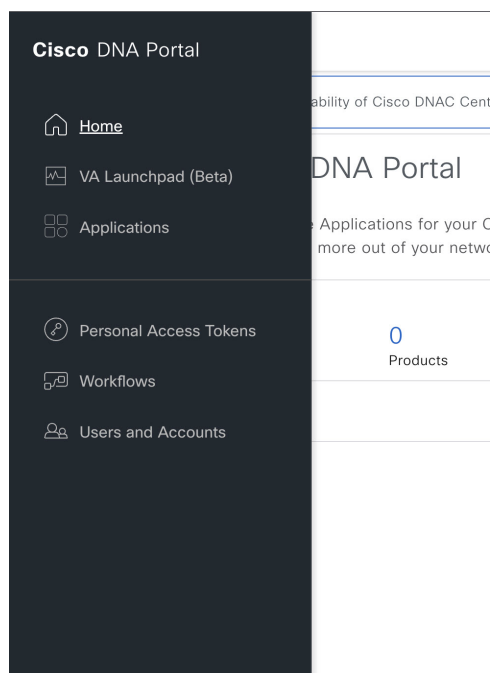
http://<localhost>:<client-port-number>/valaunchpad

次に例を示します。

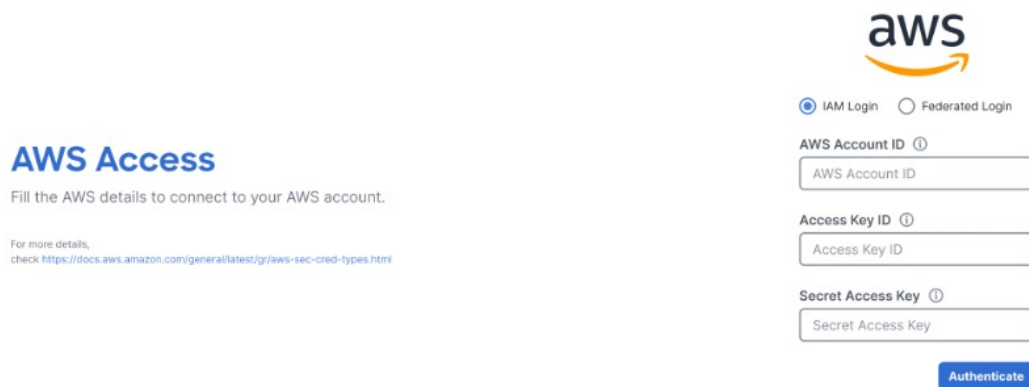
http://192.0.2.1:90/valaunchpad

- ホステッド型 Cisco DNA Center VA 起動パッドにアクセスする場合は、**dna.cisco.com** と入力し、画面に表示される指示に従ってログインします（詳細については、[シスコアカウントを使用した Cisco DNA ポータルへのログイン \(20 ページ\)](#) を参照してください）。

Cisco DNA ポータル のホームページでメニューアイコンをクリックして選択 [VA Launchpad (Beta)] を選択します。



AWS ログインウィンドウが表示されます。



ステップ 2 ユーザーログインを選択し、次のフィールドにログイン情報を入力します。

- [IAM Login]
- [Federated Login]

詳細については、[saml2aws](#) で生成したログイン情報を使用してフェデレーテッドユーザーとしてログインする (72 ページ) または [AWS CLI](#) で生成したログイン情報を使用してフェデレーテッドユーザーとしてログインする (76 ページ) を参照してください。

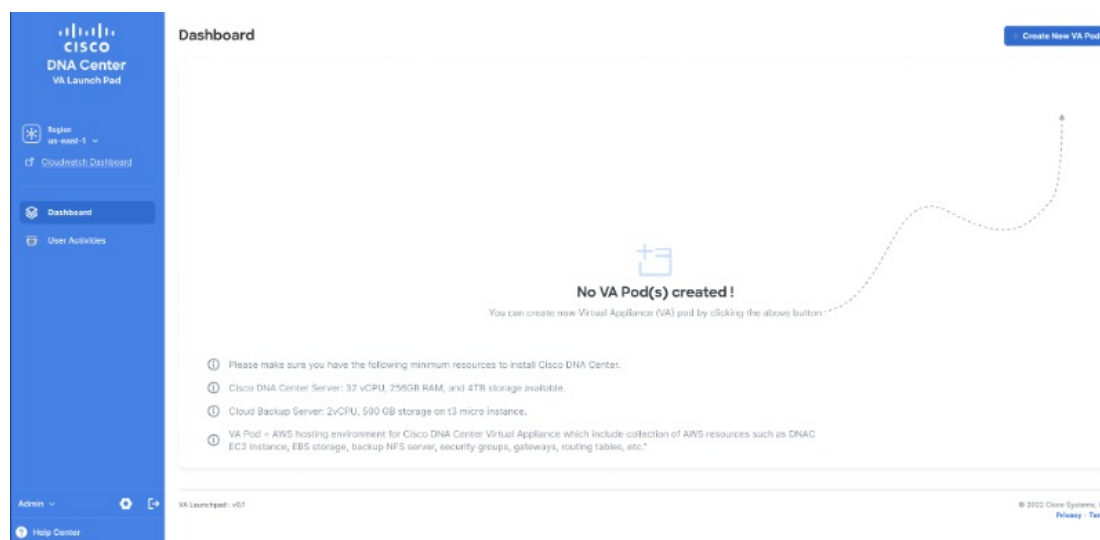
saml2aws で生成したログイン情報を使用してフェデレーテッドユーザーとしてログインする

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。

ステップ 3 [Authenticate] をクリックします。

正常にログインすると、**Dashboard**が表示され、us-east-1 リージョンがデフォルトで選択されます。

リージョンのバージョン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、[リージョンのバージョンの更新 \(83ページ\)](#) を参照してください。



ステップ 4 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ティング \(41ページ\)](#) を参照してください。

saml2aws で生成したログイン情報を使用してフェデレーテッドユーザーとしてログインする

コマンドライン インターフェイス (CLI) ツールを使用して一時的な AWS ログイン情報を生成し、その生成したログイン情報を使用して Cisco DNA Center VA 起動パッドにログインできます。

手順

ステップ 1 CLI から saml2aws をインストールします。詳細については、[Github](#) に関する詳細な手順を参照してください。

ステップ 2 saml2aws と入力して、インストールを確認します。

インストールに成功すると、次の出力が表示されます。

```

[redacted] ~ % saml2aws
usage: saml2aws [<flags>] <command> [<args> ...]

A command line tool to help with SAML access to the AWS token service.

Flags:
  --help                Show context-sensitive help (also try --help-long
                        and --help-man).
  --version             Show application version.
  --verbose             Enable verbose logging
  --quiet              silences logs
  -i, --provider=PROVIDER This flag is obsolete. See:
                        https://github.com/Versent/saml2aws#configuring-i
dp-accounts
  --config=CONFIG      Path/filename of saml2aws config file (env:
                        SAML2AWS_CONFIGFILE)
  -a, --idp-account="default" The name of the configured IDP account. (env:
                        SAML2AWS_IDP_ACCOUNT)
  --idp-provider=IDP-PROVIDER The configured IDP provider. (env:
                        SAML2AWS_IDP_PROVIDER)
  --mfa=MFA            The name of the mfa. (env: SAML2AWS_MFA)
  -s, --skip-verify    Skip verification of server certificate. (env:

```

ステップ 3 アカウントを設定します。

- a) **saml2aws configure** と入力します。
- b) [Please choose a provider] プロンプトでプロバイダーを選択し、Enter を押します。

```

[redacted] ~ % saml2aws configure
? Please choose a provider: [Use arrows to move, type to filter]
  Akamai
  Auth0
  AzureAD
> Browser
  F5APM
  GoogleApps
  JumpCloud

```

- c) [AWS Profile] プロンプトで Enter を押して、デフォルトの AWS プロファイルを使用します。

```

[redacted] ~ % saml2aws configure
? Please choose a provider: Browser
? AWS Profile (saml) █

```

- d) [URL] プロンプトで、アイデンティティプロバイダー (IdP) の URL を入力し、Enter を押します。

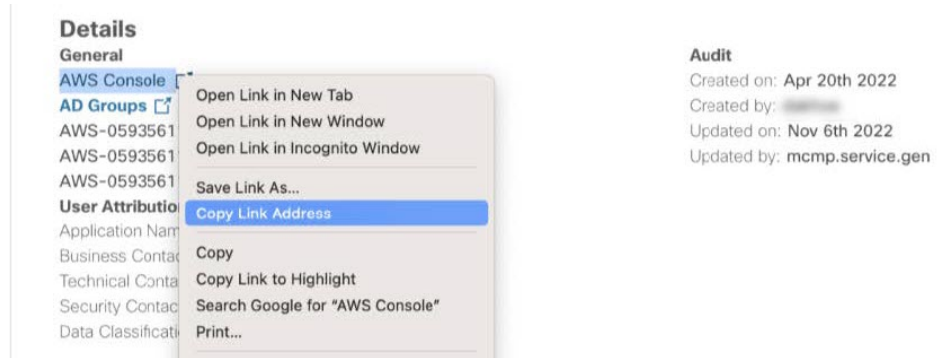
saml2aws で生成したログイン情報を使用してフェデレーテッドユーザーとしてログインする

```

[redacted] ~ % saml2aws configure
? Please choose a provider: Browser
[?] AWS Profile saml
? URL (https://cloudsso.cisco.com/idp/startSSO.ping?PartnerSpId=https://signin.a
ws.amazon.com/saml)

```

(注) この情報は、ご使用の IdP から取得してください。



e) プロンプトでユーザー名とパスワードを入力し、Enter を押します。

```

[redacted] — saml2aws configure — 80x24

exec [<flags>] [<command>...]
  Exec the supplied command with env vars from STS token.

console [<flags>]
  Console will open the aws console after logging in.

list-roles [<flags>]
  List available role ARNs.

script [<flags>]
  Emit a script that will export environment variables.

[redacted] ~ % saml2aws configure
? Please choose a provider: Browser
[?] AWS Profile saml
[?] URL https://cloudsso.cisco.com/idp/startSSO.ping?PartnerSpId=https://signin.a
s.amazon.com/saml
[?] Username [redacted]
? Password

```

ステップ 4 フェデレーテッドユーザーのログイン情報を生成します。

a) **saml2aws login** と入力します。

- b) プロンプトでユーザー名とパスワードを入力します。
- c) プロンプトで [Admin] または [CiscoDNACenter] ロールを選択し、Enter を押します。
 - (注) これらのロール用に作成されたトークンの有効期限が 180 分 (3 時間) 以上であることを確認します。

ログイン情報が生成されると、~/aws/credentials に保存されます。

```

~ % saml2aws script
export AWS_ACCESS_KEY_ID=
export AWS_SECRET_ACCESS_KEY=
export AWS_SESSION_TOKEN=

export AWS_SECURITY_TOKEN=IQoJb3JpZ21uX2VjEAQaCXVzLWVhc3QtMSJIMEYCIQC57/JKbcFRmVhjeAC/48J6VXn3anqxs/LhFqy1ERf2twIhAJft15wqZ83sHyBE
rPnbu6xMZPjSj9+r5EwY73PRNEpKvoCCLz//////////wEQABoMMDU5MzU2MTEyMzUyIgx/PgNuyGmIFxpRKJcqzGJx+973k27K54YewpvBmF0MbAmiZUCT3txuqkUb0
qju0WzXPjRAi19bgBLC2jXe19q9VJIFeQYUGnQ+8WuuECXzy1tXF+/ZaDpjVnyzy4Bw30ggZhpRJJiohT2T0+KxTZPLshMdhPGTqi2U/Jf1g1IAipRDux/Myd1LDKveSIP
ptVkpTnAMgLvA0tYpzDmTGNwKc9Hs66S0qcreTWpGSuCNxjzvuENsky6uAZV0TivtgmEFzk6VjiXYOaoBLWLEk+LGziXeVucpyGSugCjzJVzNACZF0FFePb21KjJzra
EX7ioLc07LbomZ0UP6ME2pza5uWZ0/AEicPUhpvRfkn5fS+fSu0syHdvprYIDWLX25zmNrqzhxT6vqR7EjJMnL20GfsYRheJQFDIBY0/5dyian4zPJGFhtaG5WHX74T
HfZyCfzu+yAr9b0zMMaGvKAG0poBBkUU70tSu4raGjuu8W81DhXuqEhvkvt0qhPzmpcjjgV25MKyL4rM1aGCXXtIpoJ9/IVEfuRIwL123qYDyLYptNn9x0qDDghh/Ys0gd
+Nu+BPNYG4qjMCRGni1oypwN1Bj6TCLNmWQjYQG5d17owrFCPquoRoas+80mE86GHKYlu0siCeeA9SCMsf8+2zoJvyvAJME0tXPFgvVA==
export SAML2AWS_PROFILE=saml
export AWS_CREDENTIAL_EXPIRATION=2023-03-13T17:34:38+05:30

```

ステップ 5 `saml2aws script` と入力してログイン情報をダウンロードします。

ステップ 6 フェデレーテッドユーザーとして Cisco DNA Center VA 起動パッドにログインする際に使用する次のパラメータの値をメモします。

- AWS_ACCESS_KEY_ID
- AWS_SECRET_ACCESS_KEY
- AWS_SESSION_TOKEN

ステップ 7 Cisco DNA Center VA 起動パッド ログインウィンドウで、[Federated Login] を選択します。

AWS CLI で生成したログイン情報を使用してフェデレーテッドユーザーとしてログインする

The screenshot shows the AWS Access console. On the left, there is a heading "AWS Access" and instructions to fill in AWS details. On the right, there are radio buttons for "IAM Login" and "Federated Login", with "Federated Login" selected. Below are three input fields: "Access Key ID", "Secret Access Key", and "Session Token". An "Authenticate" button is located at the bottom right of the form.

ステップ 8 生成されたログイン情報を対応するフィールドに入力します。

- [Access Key ID] : AWS_ACCESS_KEY_ID パラメータから取得した値を入力します。
- [Secret Access Key] : AWS_SECRET_ACCESS_KEY パラメータから取得した値を入力します。
- [Session Token] : AWS_SESSION_TOKEN パラメータから取得した値を入力します。

ステップ 9 [Authenticate] をクリックします。

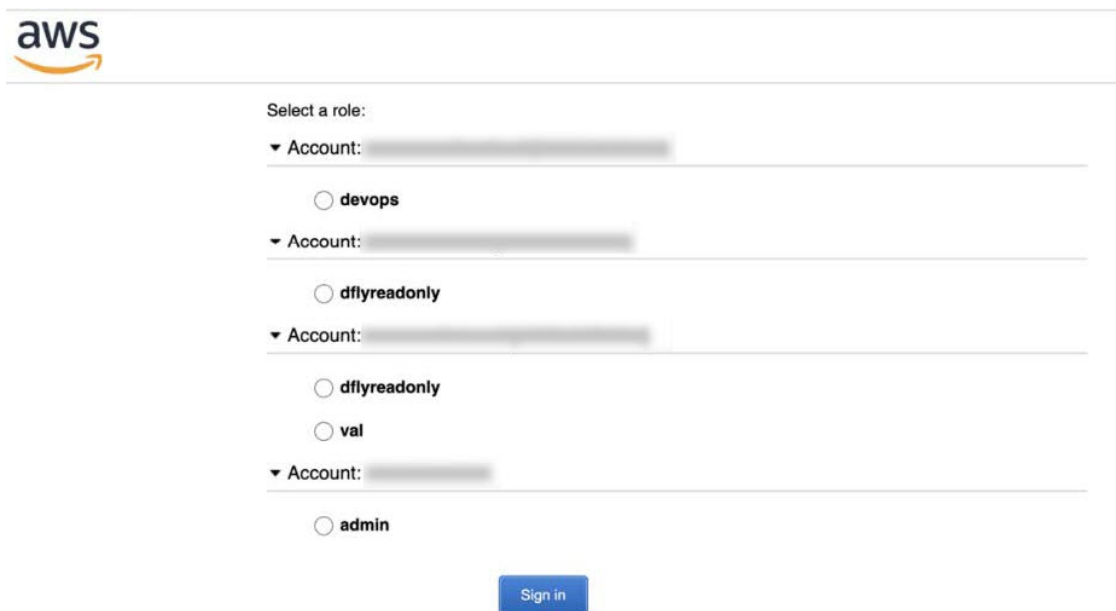
AWS CLI で生成したログイン情報を使用してフェデレーテッドユーザーとしてログインする

AWS コマンドライン インターフェイス (CLI) を使用して一時的な AWS ログイン情報を生成し、そのログイン情報を使用して Cisco DNA Center VA 起動パッドにログインできます。

手順

- ステップ 1** ブラウザウィンドウで、[AWS Single Sign On (SSO)/Active Directory (AD)] ウィンドウに移動します。
- ステップ 2** [AWS Single Sign On (SSO)/Active Directory (AD)] ウィンドウで、AWS コンソールのリンクをクリックします。

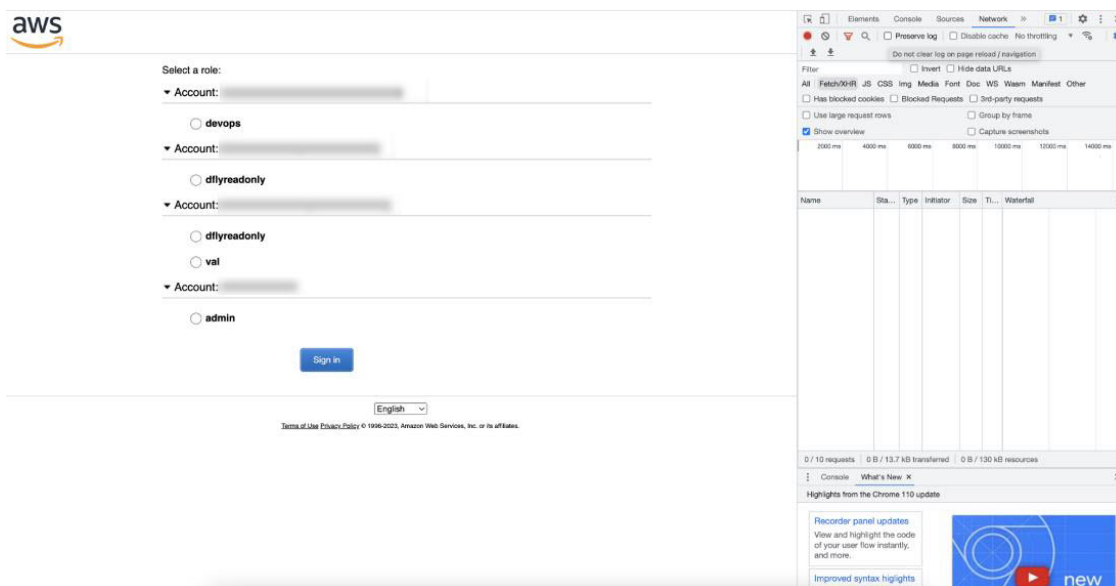
次のウィンドウが表示されます。



ステップ 3 ウィンドウ内の任意の場所を右クリックし、ドロップダウンメニューから [Inspect Element] または [Inspect] (ブラウザに応じて) を選択します。

(注) F12 キーを押して [Developer Tools] パネルを開くこともできます。

次のウィンドウのような [Developer Tools] パネルが表示されます。

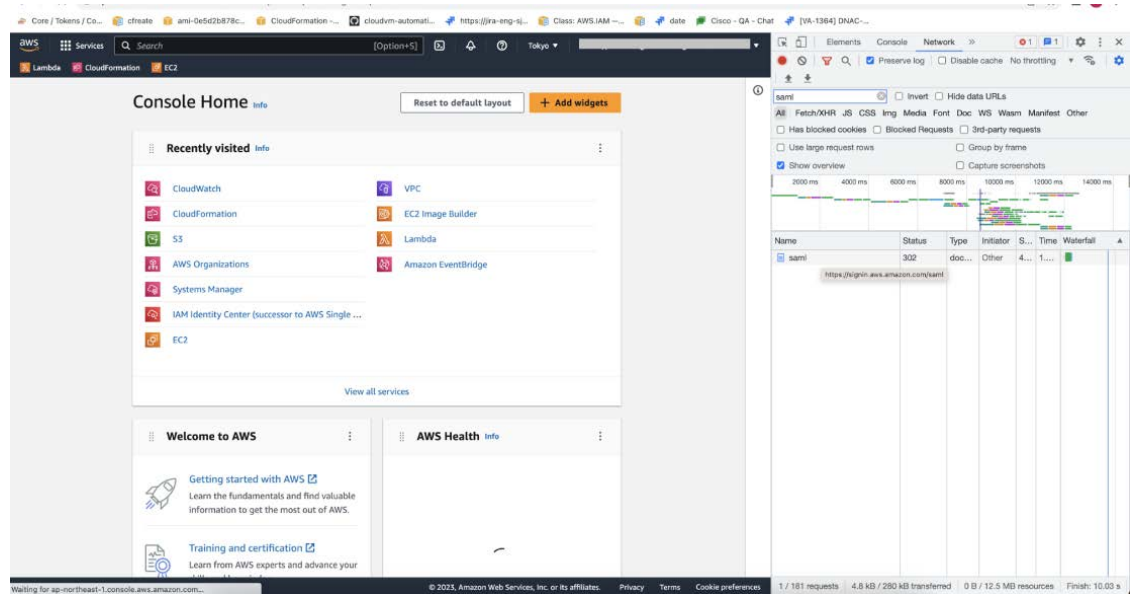


ステップ 4 [Developer Tools] パネルで [Network] タブをクリックし、[Preserve Log] チェックボックスをオンにします (このオプションは、ツールパネルの虫眼鏡アイコンの横にあります)。

AWS CLI で生成したログイン情報を使用してフェデレーテッドユーザーとしてログインする

ステップ 5 AWS コンソールで [Sign In] をクリックします。

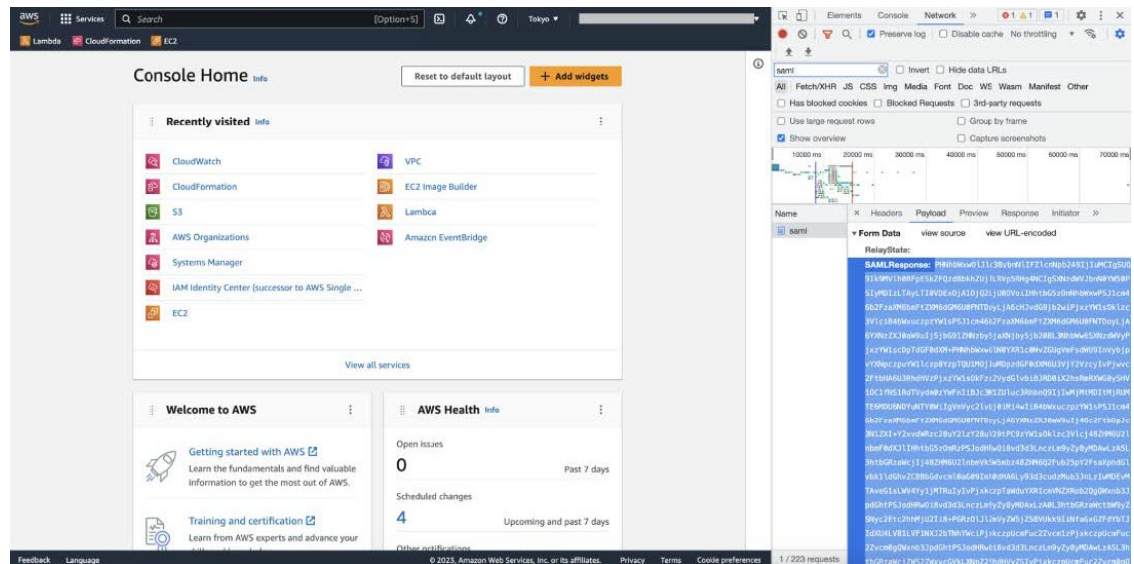
ステップ 6 [Developer Tools] パネルで、[Filter] フィールドに **saml** と入力して、必要な API コールをフィルタ処理します。



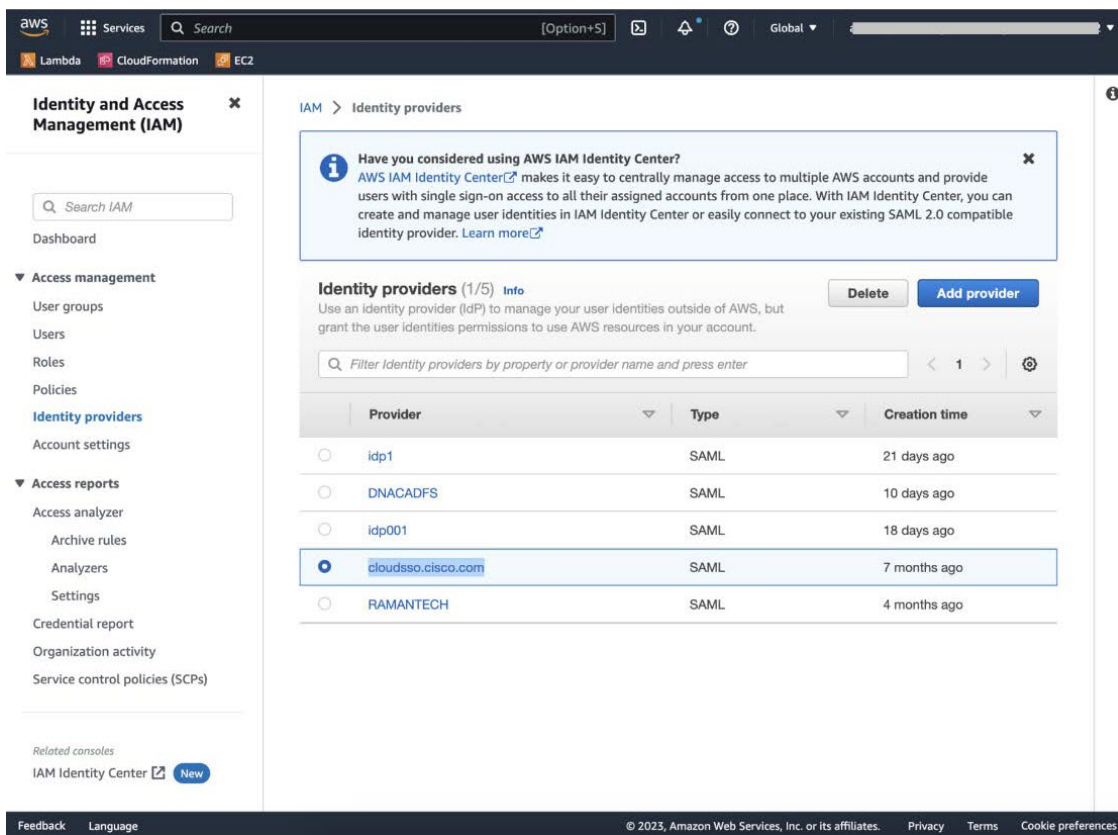
ステップ 7 **saml** という名前の API 要求をクリックします。

ステップ 8 [Payload] タブをクリックします。

ステップ 9 SAML 応答の値をコピーします。



ステップ 10 AWS コンソールに移動して、[IAM] > [Access Management] > [Identity Providers]の順に選択し、該当する IdP を選択します。



ステップ 11 IdP に関する次の詳細を取得します。

- IdP に割り当てられたロール
- IdP の Amazon リソース名 (ARN)

ステップ 12 AWS CLI から次のコマンドを入力します。

```
aws sts assume-role-with-saml --role-arn <Role-Arn> --principal-arn <IDP-Arn> --saml-assertion <SAML response>
```

次に示すように、このコマンドの変数は以前に取得した値を参照します。

- **<Role-Arn>** : ステップ 11 で取得した、IdP に割り当てられたロール。
- **<IDP-Arn>** : ステップ 11 で取得した、IdP の Amazon リソース名 (ARN) 。
- **<SAML response>** : ステップ 9 で取得した SAML 応答の値。

次に例を示します。

AWS CLI で生成したログイン情報を使用してフェデレーテッドユーザーとしてログインする

```
aws sts assume-role-with-saml --role-arn
arn:aws:iam::059356109852:role/ADFS-AWS-ADMIN --principal-arn
arn:aws:iam::059356109852:saml-provider/cloudsso.cisco.com --saml-
assertion
MIIC6jCCAdKgAwIBAgIQPP5He1K6QoZPQrIuPjzCUTANBqkqhkiG9w0BAQsFADAxMS8wLQY
DVQDEyZBREZTIFNpZ25pbmcgLSBFQzJBTUFaLU1IMUYzQ0Quc3NvLmNvbTAeFw0yMzAyMDY
wNTUyNDJaFw0yNDAYMDYwNTUNDJaMDEXLzAtBgNVBAMTJkFERlMgU2lnbmluZyAtIEVDMkF
NQVotTUgxRjNDRC5zc28uY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAs1
Sx/rQJ/wAOJ6ZRBbgYkfe7TMPsnOTqX0C+dh+yQ30+X9xqRDPVKuSDHrv72bsGwk/
2VRdb38xdVueuFYRavyVPzjsSF95fkjC3qFDN+R5Dk1Cnba7GT6i+HGfacEpL8Vqd3jzNgh
guskM1OrHDHKDv5ksNMxppHIDPlVhyRCdKEtP1PG5gBftoKvBZX+RxYcTaVUK/
NrMfkWmklyQTNRmpUDj+NAwGGjr4byjH8hUu59cFJetatzJo8qxuWWtPBtd+ESs/
DVR5dpilfyEBi4Dc22X91kOShJpeDu08EGfR605/nmRErlyy/p5f2sPKM0/
ix+XlQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQA7kt4HeU/
zohOSDnnfmXYpYi8WrJFxmVtS6CjwE8eYZ6BwByEI4PjxcjPOu+sVNXrtBzJUwyPM+LKKMs
zYn5VQ/skrwc1jW5P4msUMj4/J5K4vuYcKbJS4VyASKVZmWUWC23WhpC3U8ft6F7Jynp/
omrEh6Xrc4f4SqFdvIz35h2Sd/
HbcDp+sHZzm4TgnA2XuSuvv0NJPF2VsRHMCMsn3eBTQfbbD5naLEpitju8Zy5qW+Ic8Up51
ATNzPP+kmaQY6SxPLeuAarrnp4vDrD7hphzneRfWX8h9v/Fg+w1nOsEed1FYyLRoc
```

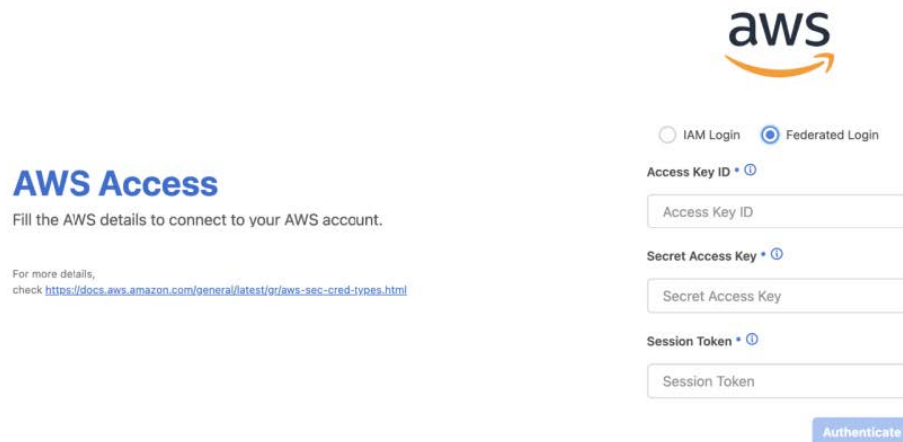
次のような出力が表示されます。

```
{
  "Credentials": {
    "AccessKeyId": "xxxx",
    "SecretAccessKey": "xxxxxx",
    "SessionToken": "xxxxxxxxxx",
    "Expiration": "2023-03-10T18:07:15+00:00"
  },
  "AssumedRoleUser": {
    "AssumedRoleId": "xxx:user@sso.com",
    "Arn": "arn:aws:sts::059356109852:assumed-role/ADFS-AWS-ADMIN/user@sso.com"
  },
  "Subject": "SSO\\USER",
  "SubjectType": "transient",
  "Issuer": "http://EC2AMAZ-MH1F3CD.sso.com/adfs/services/trust",
  "Audience": "https://signin.aws.amazon.com/saml",
  "NameQualifier": "POIUyTRFVNmkJGfKJHJHJcYlQCePSAZg="
}
```

ステップ 13 生成された次のログイン情報の値をメモします。

- AccessKeyId
- SecretAccessKey
- SessionToken

ステップ 14 Cisco DNA Center VA 起動パッド ログインウィンドウで、[Federated Login] を選択します。



aws

IAM Login Federated Login

Access Key ID * ⓘ

Access Key ID

Secret Access Key * ⓘ

Secret Access Key

Session Token * ⓘ

Session Token

Authenticate

ステップ 15 ステップ 13 で取得した、生成されたクレデンシャルを対応するフィールドに入力します。

- [Access Key ID] : AccessKeyId クレデンシャルの値を入力します。
- [Secret Access Key] : SecretAccessKey クレデンシャルの値を入力します。
- [Session Token] : SessionToken クレデンシャルの値を入力します。

ステップ 16 [Authenticate] をクリックします。

Cisco DNA Center VA 起動パッド リージョンの設定

Cisco DNA Center VA 起動パッド でサポートされているリージョンのリストからリージョンを選択できます。

始める前に

Cisco DNA Center VA 起動パッド が正常にインストールされていることを確認します。詳細については、[Cisco DNA Center VA 起動パッド のインストール \(12 ページ\)](#) を参照してください。

関連するリージョンが AWS で有効になっていることを AWS 管理者に確認します。Cisco DNA Center VA 起動パッド の [Region] ドロップダウンリストには、有効なリージョンのみが表示されます。

手順

ステップ 1 Cisco DNA Center VA 起動パッドにログインします。

詳細については、[シスコアカウントでのログイン \(69 ページ\)](#) を参照してください。

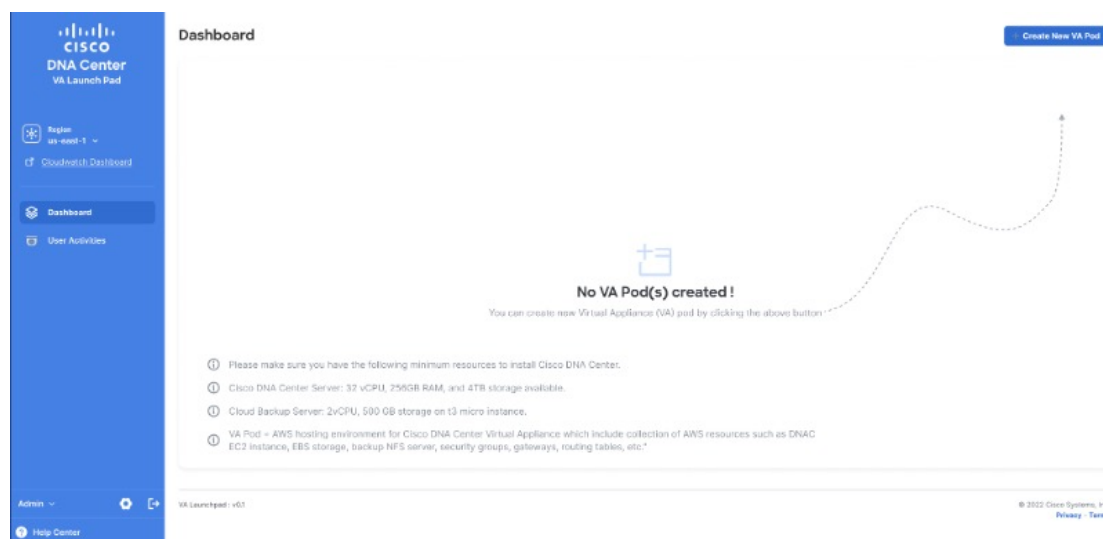
Dashboard が表示されます。

リージョンのバージョン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。リリース 1.3.0 をインストールしてリージョンのバージョンを更新するには、その前にリリース 1.0.4 (限定利用可能リリース) 以上にすることが必要であることを注意してください。詳細については、[リージョンのバージョンの更新 \(83 ページ\)](#) を参照してください。

(注) 更新されたバージョンが利用可能になったら、リージョンを更新する必要があります。ログインするか、選択したリージョンを変更するたびに、更新されたリージョンバージョンが利用可能かどうかを Cisco DNA Center VA 起動パッドによって自動的にチェックされます。更新された地域バージョンが検出された場合、Cisco DNA Center VA 起動パッドに更新を求めるプロンプトが表示されます。画面に表示される指示に従って操作します。

更新には数分かかる場合があります。プロセスが完了するまで、タブまたはウィンドウを閉じないでください。

更新が失敗した場合、Cisco DNA Center VA 起動パッドにより、機能する最新のバージョンに地域が復元され、エラーが表示されます。この場合は、Cisco TAC までお問い合わせください。



ステップ 2 **Dashboard** の左上隅にある [Region] ドロップダウンリストから、次のリージョンのいずれかを選択します。

- 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)

リージョンのバージョン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。リリース 1.3.0 をインストールしてリージョンのバージョンを更新するには、その前にリリース 1.0.4 (限定利用可能リリース) 以上にする必要があることに注意してください。詳細については、[リージョンのバージョンの更新 \(83 ページ\)](#) を参照してください。

- (注)
- [Region] ドロップダウンリストには、有効なリージョンのみが表示されます。
 - リリース 1.3.0 で追加された新しいリージョンへのアクセスを有効にするには、Cisco DNA Center VA 起動パッドリリース 1.3.0 のインストール後に管理者ユーザーが Cisco DNA Center VA 起動パッドにログインする必要があります。管理者ユーザーがログインすると、すべてのリージョンへのアクセス権が他のすべてのユーザーに対して有効になります。

リージョンのバージョンの更新

更新されたバージョンが利用可能になったら、リージョンを更新する必要があります。ログインするか、選択したリージョンを変更するたびに、更新されたリージョンバージョンが利用可能かどうかは Cisco DNA Center VA 起動パッドによって自動的にチェックされます。更新されたリージョンバージョンが検出された場合、Cisco DNA Center VA 起動パッドにより、更新を求めるプロンプトが表示されます。画面に表示される指示に従って操作します。



-
- (注) リリース 1.3.0 をインストールしてリージョンのバージョンを更新するには、その前にリリース 1.0.4 (限定利用可能リリース) 以上にする必要があります。
-

更新には数分かかる場合があります。プロセスが完了するまで、タブまたはウィンドウを閉じないでください。

更新が成功したら、[OK] をクリックして続行します。

更新が失敗した場合、Cisco DNA Center VA 起動パッドにより、機能する最新のバージョンに地域が復元され、エラーが表示されます。この場合は、Cisco TAC までお問い合わせください。

リージョン設定の削除

アクティブなリージョン設定内に VA ポッドが作成されていない場合、そのリージョン設定を削除するには、次の手順を実行します。

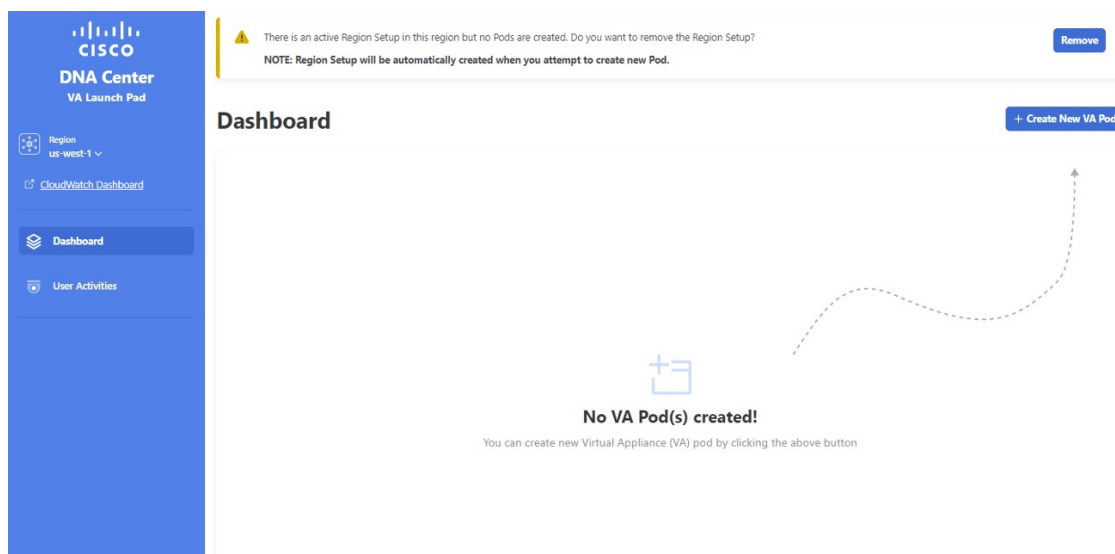


-
- (注) リージョンで最後の VA ポッドが削除されても、リージョンスタック (cisco-dna-center) は削除されません。つまり、[+ Create New VA Pod] は有効のままになり、そのリージョンに新しい VA ポッドを作成できます。
-

手順

ステップ 1 選択したリージョン内のすべての VA ポッドが削除されていることを確認します。詳細については、[VA ポッドの削除 \(87 ページ\)](#) を参照してください。

選択したリージョンに VA ポッドが存在しない場合は、**Dashboard** の上部にバナーが表示されます。



ステップ2 バナーで [Remove] をクリックします。

削除プロセスには、最大 1 分間かかります。このプロセス中に新しい VA ポッドを作成することはできません。

リージョン設定が正常に削除されると、右上隅に成功通知メッセージが表示されます。

(注) 選択したリージョンで新しい VA ポッドを初めて作成すると、新しいリージョン設定が自動的に作成されます。

VA ポッドの編集

VA ポッドの作成時に優先する VPN として [VPN GW] を選択した場合にのみ、VA ポッドを編集できます。



(注) VA ポッドの編集中は、Amazon EventBridge（電子メール通知をトリガーするために使用される AWS サービス）が無効になっているため、VA ポッドに関する電子メール通知が届かなくなります。VA ポッドの編集が正常に実行されると、Amazon EventBridge が再度有効になるため、この VA ポッドに関する電子メール通知が届きます。

始める前に

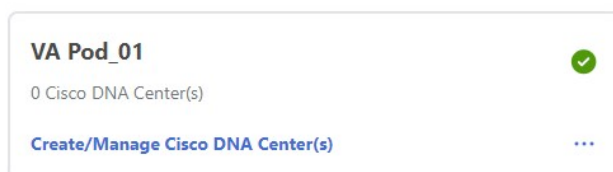
Cisco DNA Center VA 起動パッドが正常にインストールされていることを確認します。詳細については、[Cisco DNA Center VA 起動パッドのインストール（12 ページ）](#)を参照してください。

手順

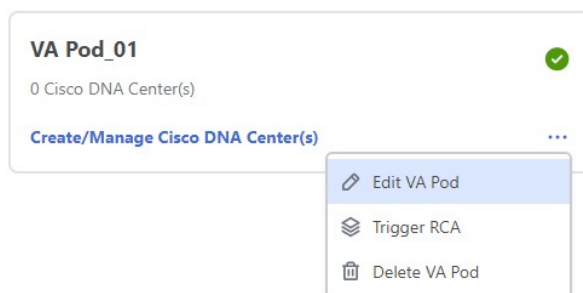
ステップ 1 Cisco DNA Center VA 起動パッドにログインします。

詳細については、[シスコアカウントでのログイン \(69 ページ\)](#) を参照してください。

ステップ 2 **Dashboard**で VA ポッドを見つけます。



ステップ 3 VA ポッドカードの右下隅にある省略記号アイコン ([...]) をクリックし、[Edit VA Pod] を選択します。



ステップ 4 [Modify VPN Details] ページで、次の VPN の詳細を必要に応じて編集し、[Next] をクリックします。

- カスタマーゲートウェイ IP
カスタマーゲートウェイ IP は有効なパブリックアドレスにする必要があります。
- VPN ベンダー
- プラットフォーム
- ソフトウェア

ステップ 5 編集内容を確認し、準備ができたなら [Proceed to On-Prem Configuration] をクリックします。

ステップ 6 オンプレミス接続を設定します。

- a) [Configure On-premise] 画面で、[Download Configuration File] をクリックします。
- b) 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 トンネルの設定を依頼します。

ネットワーク管理者がこの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この設定を適用すると、IPsec トンネルを起動できます。

詳細については、[新しい VA ポッドの作成 \(23 ページ\)](#) を参照してください。

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

ステップ 7 ネットワーク設定のステータスを確認します。

ネットワーク管理者が IPsec トンネルを設定している間、IPsec トンネルの設定ステータスは未設定（鍵アイコン）として表示されます。



ネットワーク管理者が設定を完了し、IPsec トンネルが正常に設定されると、IPsec トンネルの設定ステータスが成功アイコンとともに緑色で表示されます。



ステップ 8 （任意） **Dashboard** に戻るには、[Go to Dashboard] をクリックします。

VA ポッドの削除

Cisco DNA Center VA 起動パッドで VA ポッドを削除できます。



- (注)
- ポッド内の Cisco DNA Center VA を削除している間は、VA ポッドを削除できません。最初に Cisco DNA Center VA が削除されるのを待つ必要があります。
 - TGW は既存の VPN または VPC によって使用されている可能性があるため、VA ポッドを削除しても TGW は削除されません。

始める前に

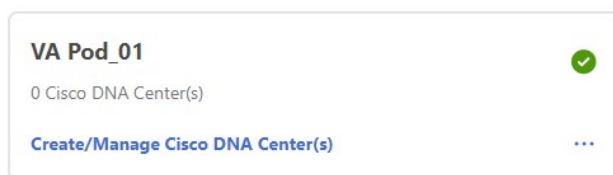
Cisco DNA Center VA 起動パッドが正常にインストールされていることを確認します。詳細については、[Cisco DNA Center VA 起動パッドのインストール \(12 ページ\)](#) を参照してください。

手順

ステップ 1 Cisco DNA Center VA 起動パッドにログインします。

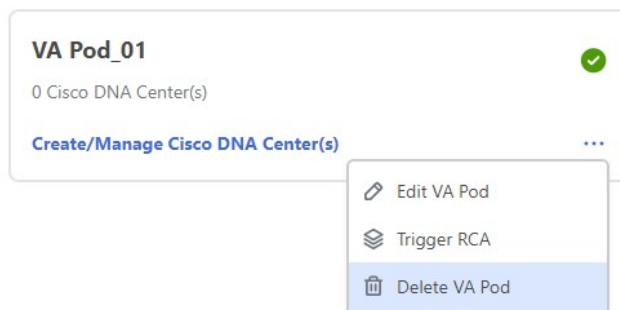
詳細については、[シスコアカウントでのログイン \(69 ページ\)](#) を参照してください。

ステップ 2 **Dashboard** で VA ポッドを見つけます。



ステップ 3 VA ポッドの右下隅にある省略記号アイコン ([...]) をクリックし、[Delete VA Pod] を選択します。

VA ポッド内にある Cisco DNA Center VA を削除する場合、[Delete VA Pod] オプションは使用できないことに注意してください。



ステップ 4 [Confirmation] ダイアログボックスのテキストフィールドに **DELETE** と入力します。

Confirmation

Are you sure you want to delete **VA Pod_01**?
This will permanently delete all the DNAC instances in this VA Pod.

Please type **DELETE** to confirm the operation

Cancel Delete

- ステップ 5** [Delete] をクリックして、Cisco DNA Center VA 起動パッドで VA ポッドの削除を実行します。VA ポッドの削除には約 20 ~ 40 分かかります。

Cisco DNA Center VA 詳細の表示

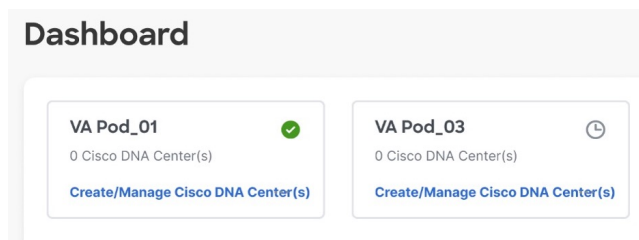
Cisco DNA Center VA 起動パッドで Cisco DNA Center VA の詳細を表示できます。

始める前に

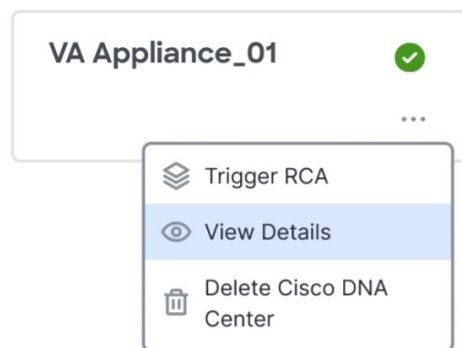
Cisco DNA Center VA 起動パッドが正常にインストールされていることを確認します。詳細については、[Cisco DNA Center VA 起動パッドのインストール \(12 ページ\)](#) を参照してください。

手順

- ステップ 1** Cisco DNA Center VA 起動パッドにログインします。
詳細については、[シスコアカウントでのログイン \(69 ページ\)](#) を参照してください。
- ステップ 2** 表示対象の Cisco DNA Center VA を含む VA ポッドを **Dashboard** で見つけ、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** Cisco DNA Center VA カードの右下隅にある省略記号アイコン ([...]) をクリックし、[View Details] を選択します。



ステップ 4 Cisco DNA Center 仮想アプライアンスの詳細 ウィンドウで、次の Cisco DNA Center VA 詳細を表示します。

Cisco DNA Center Virtual Appliance Details

DOMAIN DETAILS

Enterprise DNS	[Redacted]
FQDN (Fully Qualified Domain Name)	www.google.com

PROXY DETAILS

Customer HTTPS Network Proxy	No Proxy
Cisco DNA Center URL	[Redacted]
Cisco DNA Center AMI	ami-06ebf482b1cd486ef
Cloud Backup Server IP	[Redacted]
Cloud Backup Server AMI	ami-0dfcb1ef8550277af

OTHER DETAILS

Created By	[Redacted]
Cisco DNA Center Version	2.3.5.0

Close

ステップ 5 (任意) ウィンドウを終了するには、[Close] をクリックします。

既存の Cisco DNA Center VA の削除

Cisco DNA Center VA 起動パッドで既存の Cisco DNA Center VA を削除できます。

始める前に

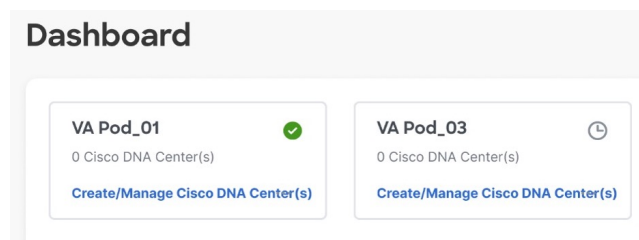
Cisco DNA Center VA 起動パッドが正常にインストールされていることを確認します。詳細については、[Cisco DNA Center VA 起動パッドのインストール \(12 ページ\)](#) を参照してください。

手順

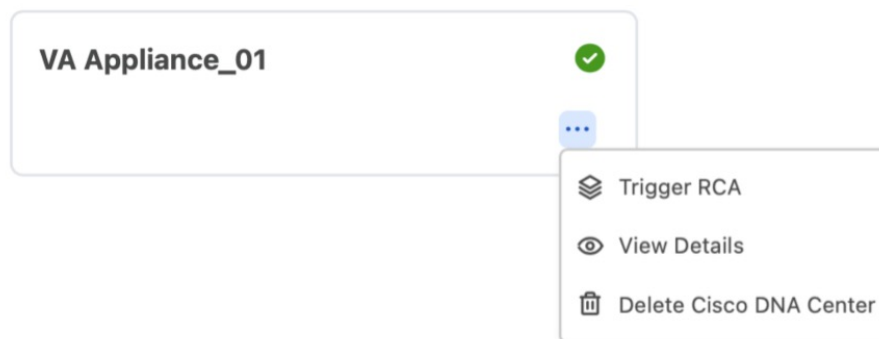
ステップ 1 AWS アカウントにログインします。

詳細については、[シスコアカウントでのログイン \(69 ページ\)](#) を参照してください。

ステップ 2 削除対象の Cisco DNA Center VA を含む VA ポッドを **Dashboard** で見つけ、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 Cisco DNA Center VA カードの右下隅にある省略記号アイコン ([...]) をクリックし、[Delete Cisco DNA Center] を選択します。



ステップ 4 [Confirmation] ダイアログボックスのテキストフィールドに **DELETE** と入力します。

Confirmation

Are you sure you want to delete **VA Appliance_01**
This will permanently delete the DNAC instance.

Please type **DELETE** to confirm the operation

ステップ 5 [Delete] をクリックして、Cisco DNA Center VA 起動パッドで Cisco DNA Center VA の削除を実行します。

根本原因分析 (RCA) のトリガー

Cisco DNA Center VA 起動パッドで根本原因分析をトリガーして、AWS インフラストラクチャや Cisco DNA Center VA の展開に関連する問題の根本原因を特定できます。RCA 操作により AWS からログが収集されて、AWS の S3 バケットに保存されます。RCA バンドルには、バックアップログ、バックエンドログ、Amazon CloudWatch アラームログ、AWS リソースとイベントログが含まれます。

始める前に

Cisco DNA Center VA 起動パッドが正常にインストールされていることを確認します。詳細については、[Cisco DNA Center VA 起動パッドのインストール \(12 ページ\)](#) を参照してください。

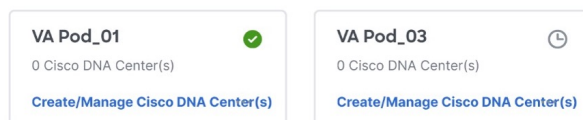
手順

ステップ 1 AWS アカウントにログインします。

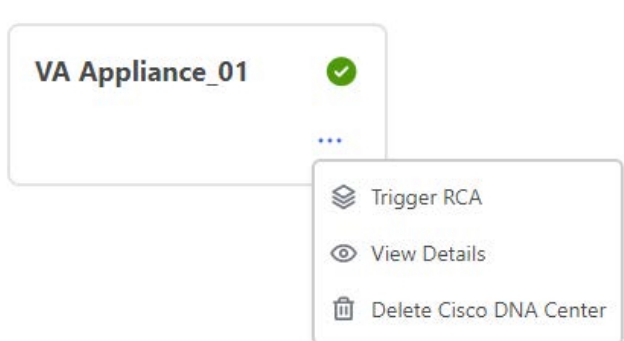
詳細については、[シスコアカウントでのログイン \(69 ページ\)](#) を参照してください。

ステップ 2 RCA をトリガーする Cisco DNA Center VA を含む VA ポッドを **Dashboard** で見つけ、VA ポッドカードで [Create/Manage Cisco DNA Center(s)] をクリックします。

Dashboard



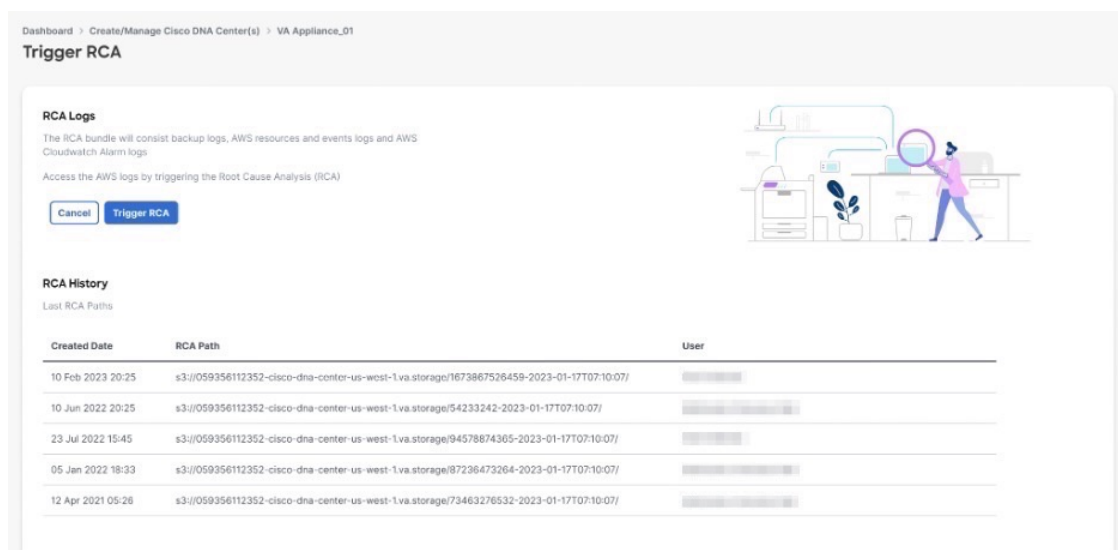
ステップ 3 Cisco DNA Center VA カードの右下隅にある省略記号アイコン ([...]) をクリックし、[Trigger RCA] を選択します。



ステップ 4 [Trigger RCA] ウィンドウの [RCA Logs] エリアで、[Trigger RCA] をクリックして AWS ログを収集してバンドルします。

Cisco DNA Center VA 起動パッドは、使用されたリソースを記録、評価、および監査するために AWS Config と Amazon CloudWatch を使用します。

(注) [Trigger RCA] ウィンドウでは、最後に正常にトリガーされた 5 つの RCA が [RCA Logs] テーブルに表示されます。



このプロセスには数分かかります。

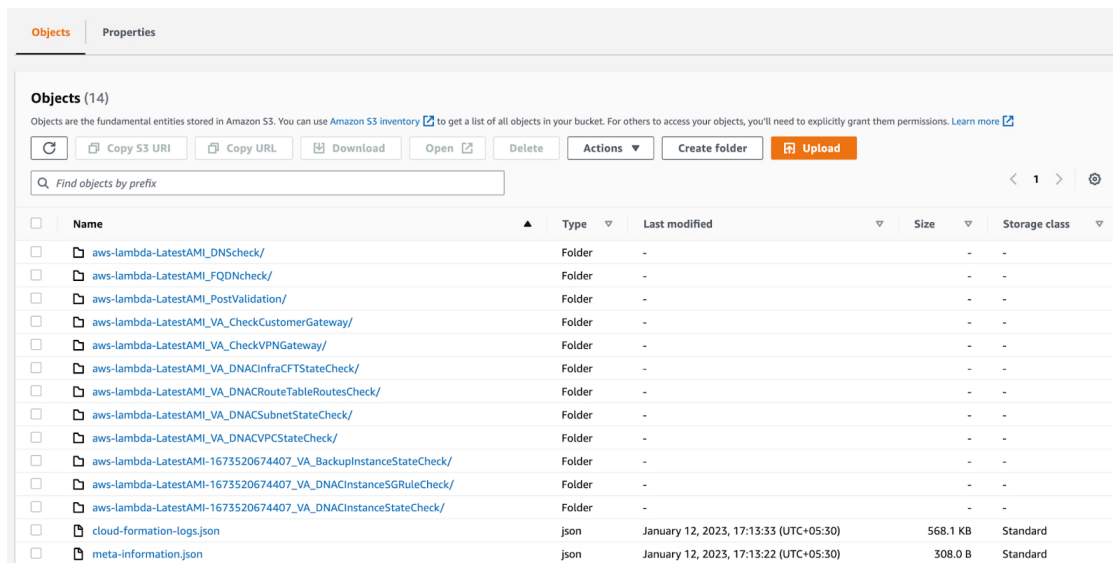


Please wait for few minutes until RCA Trigger is completed.

プロセスが完了すると、AWS ログが保存されている S3 バケットへの URL が表示されます。



ステップ 5 [Destination] の下に表示される URL をクリックして AWS の S3 バケットに移動します。S3 バケットの内容が表示されます。



作成されたリソースに応じて、ロググループの数は異なります。

AWS Config と監査ログの詳細

AWS Config は、リソース設定を継続的に評価、監視、および評価する AWS ツールであり、設定変更を指定のイベントや状態に関連付けることで、運用時のトラブルシューティングを支援します。Cisco DNA Center VA 起動パッドは AWS Config を使用して設定を監視します。AWS Config が設定の変更を検出すると、Cisco DNA Center VA 起動パッドは設定変更を通知する電子メールを生成します。

Amazon CloudWatch 通知の設定

Amazon CloudWatch 通知を受信するには、ユーザー設定で電子メールアドレスを更新します。Amazon CloudWatch は、展開されたリソース、変更、またはリソースの過剰使用に関するアラートを、指定された電子メールに送信します。

始める前に

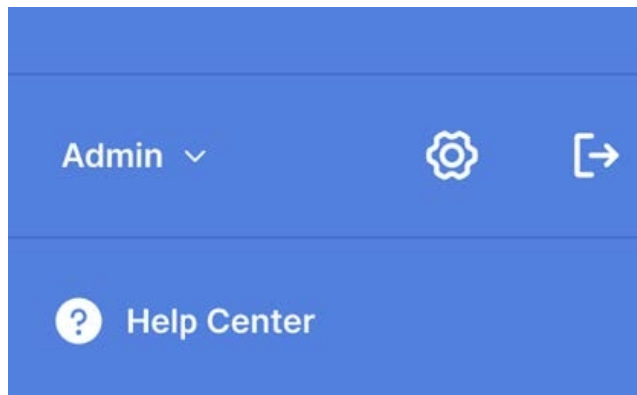
Cisco DNA Center VA 起動パッドが正常にインストールされていることを確認します。詳細については、[Cisco DNA Center VA 起動パッドのインストール \(12 ページ\)](#) を参照してください。

手順

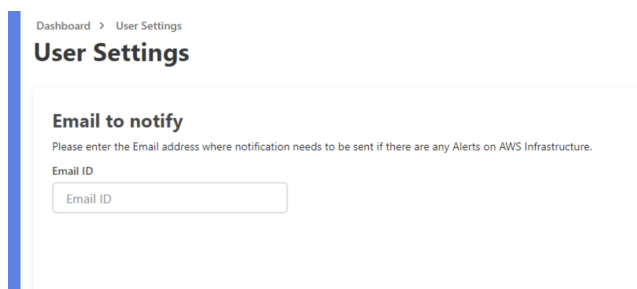
ステップ 1 Cisco DNA Center VA 起動パッドにログインします。

詳細については、[シスコアカウントでのログイン \(69 ページ\)](#) を参照してください。

ステップ 2 **Dashboard**の左下隅にあるユーザー アカウント ドロップダウン リストからユーザーアカウントを選択し、設定アイコンをクリックします。



ステップ 3 [User Settings] ウィンドウの [User Email Configuration] エリアで、[Email ID] フィールドに優先する電子メールアドレスを入力します。



古い電子メールアドレスは登録解除され、電子メールの変更後に作成された VA ポッドには新しい電子メールアドレスが使用されます。新しい電子メールアドレスは、既存の VA ポッドには使用されません。

既存のユーザーアカウントで電子メールサブスクリプションが確認されず、新しい電子メールアドレスでサブスクリプションが更新されると、古い電子メールアドレスと新しい電子メールアドレスの両方が登録され、Amazon Simple Notification System (SNS) で設定されたままになります。

- (注) 複数のユーザーアカウントで同時に電子メール ID を更新しないでください。この場合、更新された最新の電子メール ID が電子メール通知に使用されます。

ステップ 4 [Submit] をクリックします。

Amazon CloudWatch アラームの表示

Cisco DNA Center VA 起動パッドは Amazon CloudWatch アラームを使用してリソースの使用状況をモニターし、異常な動作がないかを確認します。AWS の RCA 機能でも Amazon CloudWatch アラームが使用されます。

しきい値に達すると、最初の Cisco DNA Center VA 起動パッド ログイン時に設定した電子メール ID またはユーザー設定の電子メール ID（更新した場合）にアラートが送信されます。詳細については、[Amazon CloudWatch 通知の設定](#)（94 ページ）を参照してください。



- (注)
- ラムダ関数の Amazon CloudWatch アラームは、対応するラムダ関数の実行でエラーが発生しない限り、不十分なデータ状態のままになります。ラムダ関数でエラーが発生すると、Amazon CloudWatch はメトリックを収集し、アラームをトリガーします。すべてのラムダアラームのしきい値は 1 であるため、障害が発生した場合に Amazon CloudWatch はアラートをキャプチャできます。
 - S3 などの一部のアラームでは、グリニッジ標準時 (GMT) の午前 0 時に 1 日 1 回のみメトリックが報告されます。そのため、ダッシュボードのメトリックが更新されるまでに 24 ~ 48 時間かかる場合がありますが、これは予想される動作です。

始める前に

AWS アカウントが正常に設定されていることを確認します。詳細については、[自動展開の前提条件](#)（8 ページ）を参照してください。

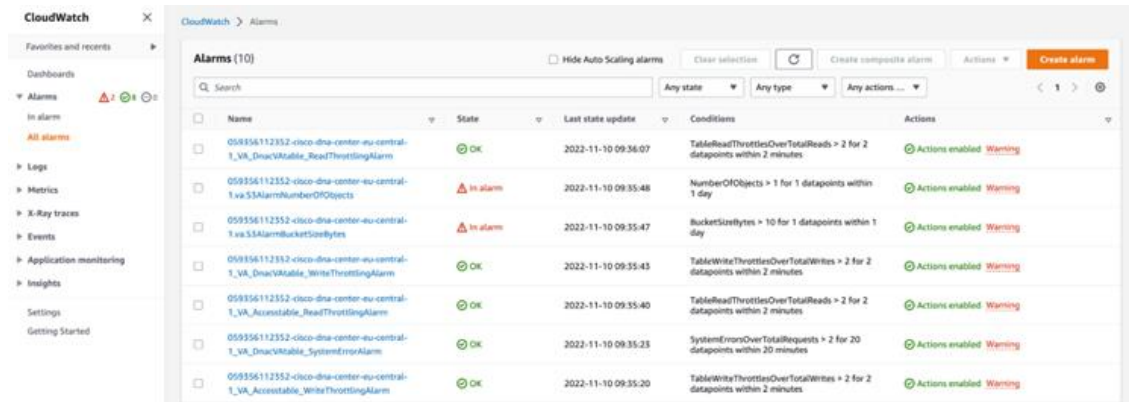
手順

ステップ 1 AWS コンソールにログインします。

AWS コンソールが表示されます。

ステップ 2 AWS ダッシュボードから **[CloudWatch]** > **[Alarms]** > **[All Alarms]** の順に選択します。

[Alarms] ページには、すべてのアラームのステータスが表示されます。

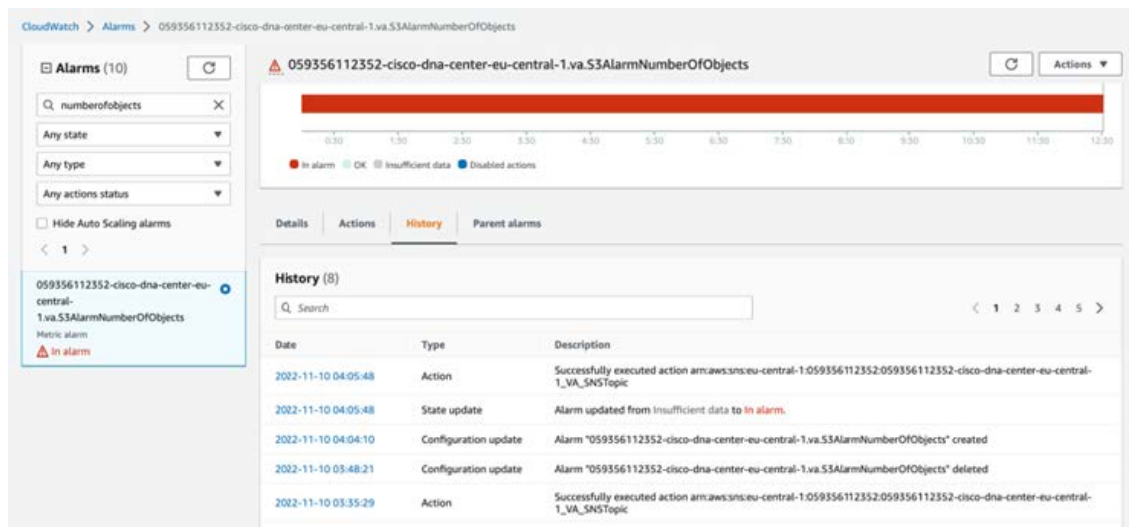


ステップ 3 [Alarms] ページの [Search] フィールドに Cisco DNA Center の展開で使用する環境名を入力します。

指定した環境名の Cisco DNA Center インスタンスに関連するアラームが表示されます。

ステップ 4 アラーム名をクリックします。

アラームの詳細が [Details] タブに表示されます。他の情報を表示するには、[Actions]、[History]、または [Parent alarms] タブをクリックします。



ユーザーアクティビティの表示

[User Activities] ウィンドウでは、選択したリージョンで実行したすべてのアクティビティを表示できます。

手順

ステップ 1 **Dashboard** の左ペインで、[User Activities] をクリックします。

[User Activities] ウィンドウには、ユーザーアクティビティが表形式で表示されます。

Dashboard > User Activities

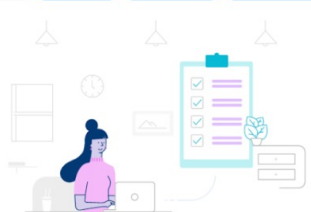
User Activities

All User ▾
↺ Reset
↻ Refresh
↓ Download

Date	Activity	User
18 May 2023 11:32	VA Pod Pa1Test-03 creation has been initiated.	
18 May 2023 11:24	Cisco DNA Center creation for VA Pod Pa1Test-02 has been initiated.	
18 May 2023 09:26	Cisco DNA Center creation for VA Pod Pa1Test-01 has been initiated.	
18 May 2023 08:32	Cisco DNA Center for VA Pod Pa1Test-02 has been deleted successfully.	
18 May 2023 08:22	Cisco DNA Center deletion for VA Pod Pa1Test-02 has been initiated.	

<
1
2
3
4
5
...
45
>

1 - 5 of 221
Rows per page
5



ステップ 2 [User Activities] ウィンドウで次の手順を実行すると、[User Activities] テーブルのデータを表示、検索、およびフィルタ処理できます。

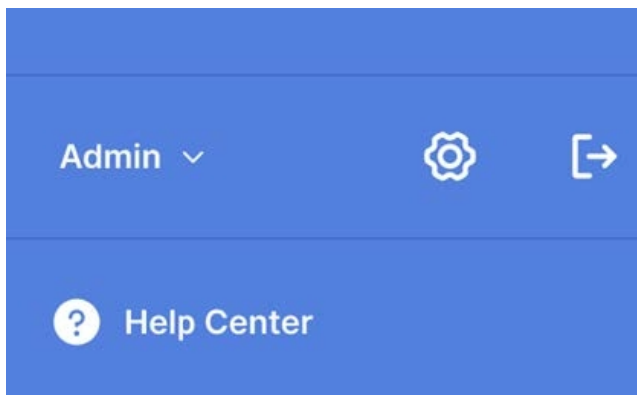
- アクティビティを検索するには、[Search on Activity] バーを使用します。
- 日付でアクティビティをフィルタ処理するには、[Select Start Date] をクリックして開始日を選択し、[Select End Date] をクリックして終了日を選択します。
- ユーザーでアクティビティをフィルタ処理するには、[All User] ドロップダウンリストからユーザーアカウントを選択します。
- フィルタをリセットするには、[Reset] をクリックします。
- 表示内容を更新するには、[Refresh] をクリックします。
- すべてのユーザーアクティビティデータを CSV ファイル形式でダウンロードするには、[Download] をクリックします。

ログアウト

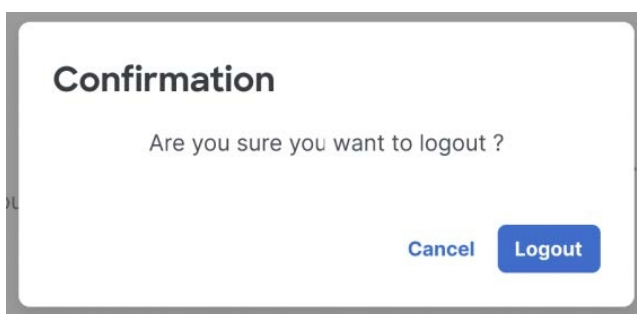
Cisco DNA Center VA 起動パッドアカウントへのアクセス方法に応じて、Cisco DNA Center VA 起動パッドからのみログアウトするか、Cisco DNA Center VA 起動パッドと Cisco DNA ポータルの両方からログアウトする必要があります。

手順

ステップ 1 Cisco DNA Center VA 起動パッドからログアウトするには、**Dashboard**の左下隅にあるユーザーアカウントをクリックしてから、ログアウトアイコンをクリックします。

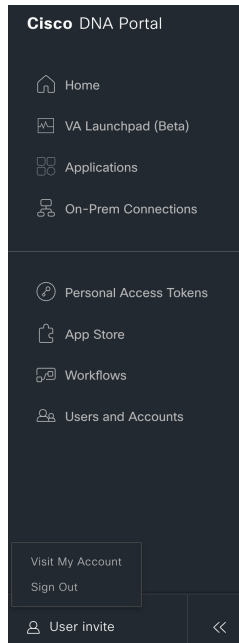


ステップ 2 [Confirmation] ダイアログボックスで、[Logout] をクリックします。
ログアウトすると、進行状況が自動的に保存されます。



ステップ 3 (任意) Cisco DNA ポータル経由で Cisco DNA Center VA 起動パッドにアクセスした場合は、Cisco DNA ポータルからもログアウトする必要があります。次の手順を実行します。

- a) メニューアイコン (☰) をクリックします。
- b) ユーザーアカウントにカーソルを合わせます。
- c) [Sign out] をクリックします。



【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2023 Cisco Systems, Inc. All rights reserved.

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。