cisco.



AWS での Cisco DNA Center 2.3.5 導入ガイド

初版:2023年8月2日 最終更新:2023年12月7日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー http://www.cisco.com/jp お問い合わせ先:シスココンタクトセンター 0120-092-255 (フリーコール、携帯・PHS含む) 電話受付時間:平日10:00~12:00、13:00~17:00 http://www.cisco.com/jp/go/contactcenter/ 【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。

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.



午 1 音	
	AWS CO Cisco DNA Center $O \land \checkmark = \land ? \lor \lor \lor \lor 1$
	AWS上の Cisco DNA Center の概要 1
	展開の機要 2
	展開の準備 4
	高可用性と AWS 上の Cisco DNA Center 5
	AWS での AWS 上の Cisco ISE と Cisco DNA Center の統合に関するガイドライン 5
	AWS 上の Cisco DNA Center にアクセスする際の注意事項 6
	Cisco DNA Center VA の TAR ファイルの確認 8
	AWS での Cisco DNA Center 2.3.5.3 の展開 11
第2章	 Cisco Global Launchpad 1.7 を使用した展開 13
	自動展開メソッドを使用した AWS CloudFormation での Cisco DNA Center の展開 13
	自動展開ワークフロー 14
	自動展開の前提条件 14
	Cisco Global Launchpad のインストール 18
	ホステッド型 Cisco Global Launchpad へのアクセス 19
	シスコアカウントの作成 20
	Cisco DNA ポータル アカウントの作成 22
	シスコアカウントでの Cisco DNA ポータル へのログイン 25
	新しい VA ポッドの作成 28
	既存のトランジットゲートウェイおよびカスタマーゲートウェイでルーティングを手動設定
	する 41
	Cisco DNA Center VA の新規作成 42

展開のトラブルシューティング 48
Docker エラーのトラブルシュート 48
ログインエラーのトラブルシュート 49
ホステッド型 Cisco Global Launchpad エラーのトラブルシューティング 50
リージョンに関する問題のトラブルシュート 50
VA ポッド設定エラーのトラブルシュート 50
ネットワーク接続エラーのトラブルシュート 52
Cisco DNA Center VA 設定エラーのトラブルシュート 53
同時実行エラーのトラブルシュート 53
展開に関するその他の問題のトラブルシュート 54

第3章 Cisco DNA Center VA 起動パッド 1.6 を使用した展開 57

自動展開メソッドを使用した AWS での Cisco DNA Center の展開 57 自動展開ワークフロー 58 自動展開の前提条件 58 Cisco DNA Center VA 起動パッドのインストール 62 ホステッド型 Cisco DNA Center VA 起動パッドへのアクセス 64 シスコアカウントの作成 64 Cisco DNA ポータル アカウントの作成 66 シスコアカウントでの Cisco DNA ポータル へのログイン 69 新しい VA ポッドの作成 72 既存のトランジットゲートウェイおよびカスタマーゲートウェイでルーティングを手動設定 する 84 新しい Cisco DNA Center VA の作成 85 展開のトラブルシューティング 91 Docker エラーのトラブルシュート 91 ログインエラーのトラブルシュート 92 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 93 リージョンに関する問題のトラブルシュート 93 VA ポッド設定エラーのトラブルシュート 94 ネットワーク接続エラーのトラブルシュート 96

Cisco DNA Center VA 設定エラーのトラブルシュート 96 同時実行エラーのトラブルシュート 97 展開に関するその他の問題のトラブルシュート 97

第4章 AWS CloudFormation を使用した展開 101

AWS CloudFormation を使用した AWS での Cisco DNA Center の手動展開 101 AWS CloudFormation ワークフローを使用した手動展開 101 AWS CloudFormation を使用した手動展開の前提条件 102 AWS CloudFormation を使用した AWS での Cisco DNA Center の手動展開 108 展開の検証 113

第5章 AWS Marketplace を使用した展開 115

AWS Marketplace を使用した AWS での Cisco DNA Center の手動展開 115 AWS Marketplace ワークフローを使用した手動展開 115 AWS Marketplace を使用した手動展開の前提条件 116 AWS Marketplace を使用した AWS での Cisco DNA Center の手動展開 122 展開の検証 122

I



AWS での Cisco DNA Center のスタートアッ プガイド

- AWS 上の Cisco DNA Center の概要 (1ページ)
- ・展開の概要 (2ページ)
- •展開の準備 (4ページ)

AWS 上の Cisco DNA Center の概要

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

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

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



展開の概要

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

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

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

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

AWS CloudFormation を使用した手動展開: AWS で Cisco DNA Center AMI を手動展開します。Cisco Global Launchpad 展開ツールを使用する代わりに、AWS に搭載された展開ツールである AWS CloudFormation を使用します。Cisco DNA Center の手動設定では、AWS インフラストラクチャを作成し、VPN トンネルを確立して Cisco DNA Center VA を展開します。詳細については、AWS CloudFormation を使用した展開(101ページ)を参照してください。

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

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

次の表を参照して、それぞれの方法のメリットとデメリットを考慮してください。

Cisco Global Launchpad を使用 した自動展開	AWS CloudFormation を使用し た手動展開	AWS Marketplace を使用した手 動展開
 VPC、サブネット、セ キュリティグループ、 IPSec VPN トンネル、ゲー トウェイなどの AWS イン フラストラクチャを AWS 	 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。 	• 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。
アカウントで作成するプロセスがサポートされます。	 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 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 カウントで佐崎します
・Cisco DIVA Center のイン ストールが自動的に完了 します。	・ユーザーが VPN トンネル を確立します。	・ユーザーが VPN トンネル を確立します。
• VAへのケクセスが提供されます。	・ユーザーが Cisco DNA Center を展開します。	・ユーザーが Cisco DNA Center を展開します。
•VAの管理性を備えていま す。	•展開には数時間から数日 かかります。	•展開には数時間から数日 かかります。
 ・展開時間は約1~1時間 半です。 	• AWS コンソールを使用し てモニタリングを手動で	• AWS コンソールを使用し てモニタリングを手動で
 自動アラートは、Amazon CloudWatch ダッシュボー 	設定する必要がありま す。	設定する必要がありま す。
 トに达信されます。 ・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。 	• バックアップには、オン プレミス NFS のみを設定 できます。	• バックアップには、オン プレミス NFS のみを設定 できます。
 AWS での 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。 		

展開の準備

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

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

高可用性と AWS 上の Cisco DNA Center

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

- ・可用性ゾーン(AZ)内のシングルノードEC2HAは、デフォルトで有効になっています。
- Cisco DNA Center の EC2 インスタンスがクラッシュした場合、AWS は同じ IP アドレスを 持つ別のインスタンスを自動的に起動します。これにより、中断のない接続が確保され、 重要なネットワーク運用の中断が最小限に抑えられます。



- (注) Cisco Global Launchpad を使用して AWS で Cisco DNA Center を展開したときに、Cisco DNA Center の EC2 インスタンスがクラッシュした場合、AWS は同じ AZ 内の別のインスタンスを自動的に起動します。この場合、AWS は Cisco DNA Center に別の IP アドレスを割り当てることができます。
 - エクスペリエンスと目標復旧時間(RTO)は、ベアメタル Cisco DNA Center アプライアン スの停電シーケンスと同様です。

AWS での AWS 上の Cisco ISE と Cisco DNA Center の統合に関するガイ ドライン

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

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

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

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

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

AWS 上の Cisco DNA Center にアクセスする際の注意事項

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

```
¢
```

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

Cisco DNA Center の GUI にアクセスする際の注意事項

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

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

http://ip-address/dna/home

次に例を示します。

http://192.0.2.27/dna/home

•初回ログイン時に次のログイン情報を使用します。

ユーザ名:admin

パスワード: maglev1@3



 (注) Cisco DNA Center に初めてログインすると、このパスワードを変 更するよう求められます。パスワードは、以下のルールに従う必 要があります。

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

Cisco DNA Center の CLI にアクセスする際の注意事項

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

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



- (注) キーは.pem ファイルである必要があります。キーファイルが key.cerファイル形式でダウンロードされている場合は、ファイル 名を key.pem に変更する必要があります。
 - key.pem ファイルのアクセス権限を手動で400に変更します。アクセス権限を変更するには、Linuxのchmodコマンドを使用します。次に例を示します。

chmod 400 key.pem

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

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

次に例を示します。

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

Cisco DNA Center VAの TAR ファイルの確認

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

始める前に

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

手順

- **ステップ1** シスコの指定した場所から署名検証用のシスコ公開キー(cisco_image_verification_key.pub)を ダウンロードします。
- **ステップ2** シスコが指定した場所から TAR ファイルのセキュア ハッシュ アルゴリズム (SHA512) チェッ クサムファイルをダウンロードします。
- **ステップ3** TAR ファイルの署名ファイル (.sig) をシスコサポートから電子メールで入手するか、セキュ アなシスコの Web サイト (利用可能な場合)からダウンロードします。
- ステップ4 (任意) SHA 検証を実行して、不完全なダウンロードによって TAR ファイルが破損していないかを確認します。

オペレーティングシステムに応じて、次のコマンドのいずれかを実行します。

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

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

certutil -hashfile <filename> sha256

次に例を示します。

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

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

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

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

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

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

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

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



第 部

AWS での Cisco DNA Center 2.3.5.3 の展開

- Cisco Global Launchpad 1.7 を使用した展開 (13 ページ)
- Cisco DNA Center VA 起動パッド 1.6 を使用した展開 (57 ページ)
- AWS CloudFormation を使用した展開 (101 ページ)
- AWS Marketplace を使用した展開 (115 ページ)



Cisco Global Launchpad 1.7 を使用した展開

- 自動展開メソッドを使用した AWS CloudFormation での Cisco DNA Center の展開 (13 ページ)
- ・自動展開ワークフロー (14ページ)
- 自動展開の前提条件 (14ページ)
- Cisco Global Launchpad のインストール (18 ページ)
- •ホステッド型 Cisco Global Launchpad へのアクセス (19ページ)
- •新しい VA ポッドの作成 (28 ページ)
- 既存のトランジットゲートウェイおよびカスタマーゲートウェイでルーティングを手動設定する(41ページ)
- Cisco DNA Center VA の新規作成 (42 ページ)
- ・展開のトラブルシューティング(48ページ)

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

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

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

自動展開ワークフロー

自動化されたメソッドを使用して AWS に Cisco DNA Center を展開するには、大まかに言って 次の手順を実行します。

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

自動展開の前提条件

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

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

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

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

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

C/

- 重要 Cisco DNA Center は r5a.8xlarge インスタンスサイズのみをサポートします。この設定は変更できません。さらに、r5a.8xlarge インスタンスサイズは、特定の可用性ゾーンではサポートされていません。サポートされている可用性ゾーンのリストを表示するには、『Release Notes for Cisco Global Launchpad Release 1.7.0』[英語]を参照してください。
 - ・バックアップインスタンス:T3.micro、2個のvCPU、500GBのストレージ、1GB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 Administrator Access 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。

awys III Services Q Search for	services, features, blags, docs, and more [Option+S]	↔ Ø Global •	dna-tme-user @ 8788-1381-4009
Identity and Access Management (IAM)	New feature to generate a policy based on CloudTrail events. Way uses your CloudTrail events to identify the services and actions used and generate a least privileged policy that you can attach to this user.		×
Dashboard			
 Access management 	Users > dna-tme-user		
User groups	Summany		Delete uses
Users	Commany		Delete user
Roles	User ARN arn:aws:lam::878813814009:user/dna-tme-user		
Policies	Path /		
Identity providers	Creation time 2022-07-23 16:11 PDT		
Account settings	Barmissiana Oroume Targe Requeity and antists Assage Advisor		
	Permissions droups rags becuny credentians Access Advisor		
Access analyzer	 Permissions policies (1 policy applied) 		
Archive rules	Add permissions		O Add inline policy
Analyzers			
Settings	Policy name 👻	Policy type 👻	
Credential report	Attached directly		
Organization activity	AdministratorAccess	AWS managed policy	×
Service control policies (SCPs)	Permissions boundary (not set)		
Q Search IAM	 Generate policy based on CloudTrail events 		
AWS account ID: 878813814009	You can generate a new policy based on the access activity for this user, then customize, create, and attach it to this role. AWS uses your CloudTrail events policy. Learn more (2)	to identify the services and actions used	d and generate a
	Share your feedback and help us improve the policy generation experience. Generate policy		

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

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

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

- AmazonDynamoDBFullAccess
- IAMReadOnlyAccess
- AmazonEC2FullAccess
- AWSCloudFormationFullAccess
- AWSLambda_FullAccess
- CloudWatchFullAccess
- ServiceQuotasFullAccess
- AmazonEventBridgeFullAccess
- service-role/AWS ConfigRole
- AmazonS3FullAccess
- ClientVPNServiceRolePolicy (バージョン: 2012-10-17)
 - このポリシーでは、次のルールが許可されます。
 - ec2:CreateNetworkInterface
 - ec2:CreateNetworkInterfacePermission
 - ec2:DescribeSecurityGroups
 - ec2:DescribeVpcs
 - ec2:DescribeSubnets
 - ec2:DescribeInternetGateways
 - ec2:ModifyNetworkInterfaceAttribute
 - ec2:DeleteNetworkInterface
 - ec2:DescribeAccountAttributes
 - ds:AuthorizeApplication
 - ds:DescribeDirectories
 - ds:GetDirectoryLimits
 - ds:UnauthorizeApplication
 - logs:DescribeLogStreams

- logs:CreateLogStream
- logs:PutLogEvents
- logs:DescribeLogGroups
- acm:GetCertificate
- acm:DescribeCertificate
- iam:GetSAMLProvider
- lambda:GetFunctionConfiguration
- ConfigPermission (バージョン: 2012-10-17、SID: VisualEditor0)

このポリシーでは、次のルールが許可されます。

- config:Get
- config:*
- config:*ConfigurationRecorder
- config:Describe*
- config:Deliver*
- config:List*
- config:Select*
- tag:GetResources
- tag:GetTagKeys
- cloudtrail:DescribeTrails
- cloudtrail:GetTrailStatus
- cloudtrail:LookupEvents
- config:PutConfigRule
- config:DeleteConfigRule
- config:DeleteEvaluationResults
- PassRole (バージョン: 2012-10-17、SID: VisualEditor0)
 - このポリシーでは、次のルールが許可されます。
 - iam:GetRole
 - iam:PassRole

Cisco Global Launchpad のインストール

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

始める前に

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

手順

ステップ1 シスコのソフトウェアダウンロードサイトに移動し、次のファイルをダウンロードします。

- Launchpad-desktop-client-1.7.0.tar.gz
- Launchpad-desktop-server-1.7.0.tar.gz
- **ステップ2** TARファイルがシスコから正規に配布されていることを確認します。手順の詳細については、 Cisco DNA Center VA の TAR ファイルの確認 (8ページ)を参照してください。
- ステップ3 ダウンロードしたファイルから Docker イメージを読み込みます。

docker load < Launchpad-desktop-client-1.7.0.tar.gz</pre>

docker load < Launchpad-desktop-server-1.7.0.tar.gz</pre>

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

次に例を示します。

\$ docker images

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

ステップ5 サーバーアプリケーションを実行します。

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

次に例を示します。

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

ステップ6 クライアントアプリケーションを実行します。

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

次に例を示します。

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

- (注) 公開されているサーバーのポート番号と REACT_APP_API_URL のポート番号が同じであることを確認します。ステップ5とステップ6では、両方の例でポート番号9090が使用されています。
- ステップ7 docker ps -a コマンドを使用して、サーバーとクライアントのアプリケーションが実行さ れていることを確認します。[STATUS] 列にアプリケーションが稼働中であることが示されて いる必要があります。

次に例を示します。

\$ docker ps -a

- (注) サーバーまたはクライアントアプリケーションの実行中に問題が発生した場合は、
 Docker エラーのトラブルシュート (48 ページ) を参照してください。
- ステップ8 次の形式でURLを入力して、サーバーアプリケーションにアクセスできることを確認します。

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

次に例を示します。

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

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

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

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

次に例を示します。

http://192.0.2.1:90/valaunchpad

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

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

ホステッド型 Cisco Global Launchpad へのアクセス

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

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

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

シスコアカウントの作成

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

手順

ステップ1 ブラウザで次のように入力します。

dna.cisco.com

Cisco DNA ポータル ログインウィンドウが表示されます。



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

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



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

C	reate Accou	unt
* indicates req Email *	uired field	
Email *		
Password *		
Password	*	
First name *		
First name *		
Last name *		
Last name *		
Country or reg	ion *	
Please select	*	Ŧ
By clicking Regis to the Cisco Onlin Site Terms and C	ter, I confirm that I have ne Privacy Statement a conditions.	e read and agree nd the Cisco Web
	Deviation	

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

Welc	ome to Cisco!
Plea	se click the button to activate your account.
	Activate Account Expires in 7 days.
After	activating your account, you can:
	 Login with your email and password.
	 Manage your Cisco account profile and request access to Cisco applications and services.
	 Become a customer by associating a contract number or bill-to ID to your account or order services directly through our global network of certified partners.
	 Become a partner by associating your account with a partner company or register your company as a partner.
	Access supply chain tools and resources.
Vicit	hale for login paceword and account information

Cisco DNA ポータル アカウントの作成

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

始める前に

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

手順

ステップ1 ブラウザで次のように入力します。

dna.cisco.com

Cisco DNA ポータル ログインウィンドウが表示されます。



ステップ2 [Log In With Cisco] をクリックします。

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

الله من المناب cisco	US EN
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ます。

< Back	US EN
altalia cisco	
Log in	
Email	
Password	
I	
Log in	
Forgot password?	
Unlock account?	
Help	
Don't have an account? Sign up	
Back to log in	

- ステップ5 [Log in] をクリックします。
- **ステップ6** Cisco DNA ポータル の [Welcome] ウィンドウの [Name your account] フィールドに組織名または チーム名を入力します。 [Continue] をクリックします。

Cisco DNA Portal

Welcome,

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

Name your account*	
Ex. Hearst or	Hearst Construction
Cancel	Continue

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

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



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



シスコアカウントでの Cisco DNA ポータル へのログイン

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

始める前に

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

手順

ステップ1 ブラウザで次のように入力します。

dna.cisco.com

Cisco DNA ポータル ログインウィンドウが表示されます。



ステップ2 [Log In With Cisco] をクリックします。

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

	IS 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ます。

Back		IS EN
	cisco	
	Log in	
Email		
Password		
	Log in	
Forgot pass	word?	
Unlock acco	unt?	
Help		
Don't have an	account? Sign up	
Rock to log in		

ステップ5 [Log in] をクリックします。

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

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



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



ここでは、新しい VA ポッドを作成する方法を順を追って説明します。

始める前に

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

手順

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

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

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

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

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

Email Address

Enter the email address to which notifications should be sent when AWS infrastructure alerts are logged.

Email Id

	Email Id	
--	----------	--

Submit

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

電子メールを入力すると、いくつかのプロセスが実行されます。

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

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



- ステップ3 [+ Create New VA Pod] をクリックします。
- ステップ4 [Select a Region] ダイアログボックスで次の手順を実行して、新しい VA ポッドを作成するリージョンを選択します。
 - 1. [Region]ドロップダウンリストから、リージョンを選択します。

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

- (注) リージョンの設定を更新するように求められた場合は、プロンプトに従って更新を完了します。詳細については、『Cisco Global Launchpad1.7 Administrator Guide』の「Update a Region Setup」[英語]を参照してください。
- 2. [Next] をクリックします。
- ステップ5 次の手順を実行して、VPC、プライベートサブネット、ルーティングテーブル、セキュリティ グループ、仮想ゲートウェイ、CGW を含む AWS インフラストラクチャを設定します。

- a) [VA Pod Environmental Details] フィールドで、次のフィールドを設定します。
 - [VA Pod Name]:新しい VA ポッドに名前を割り当てます。次の制約事項に注意して ください。
 - 名前はリージョン内で一意である必要があります(これは複数のリージョンで同じ名前を使用できることを意味します)。
 - 最大 12 文字までの名前を指定できます。
 - 名前には、文字(A~Z)、数字(0~9)、およびダッシュ(-)を含めることができます。
 - [Availability Zone]: このドロップダウンリストをクリックして、選択したリージョン 内の分離された場所である可用性ゾーンを選択します。
 - [AWS VPC CIDR]: AWS リソースの起動に使用する一意の VPC サブネットを入力します。次の注意事項に従ってください。
 - 推奨されている CIDR 範囲は /25 です。
 - IPv4 CIDR 表記では、IP アドレスの最後のオクテット(4番目のオクテット)の 値に指定できるのは0または128のみです。
 - このサブネットは、企業のサブネットと重複しないようにする必要があります。
- b) [Transit Gateway (TGW)] で、次のいずれかのオプションを選択します。
 - [VPN GW]: VA ポッドが1つあり、VPN ゲートウェイを使用する場合は、このオプ ションを選択します。VPN GW は、サイト間 VPN 接続の Amazon 側の VPN エンドポ イントです。1 つの VPC にのみ接続できます。
 - [New VPN GW + New TGW]:複数の VA ポッドまたは VPC があり、複数の VPC とオンプレミスネットワークを相互接続するトランジットハブとして TGW を使用する場合は、このオプションを選択します。また、TGW をサイト間 VPN 接続の Amazon 側の VPN エンドポイントとして使用することもできます。
 - (注) リージョンごとに1つの TGW のみを作成できます。
 - [Existing TGW]:新しい VA ポッドの作成に使用する既存の TGW がある場合は、この オプションを選択してから、次のいずれかのオプションを選択します。
 - [New VPN GW]:既存の TGW に新しい VPN ゲートウェイを作成する場合は、このオプションを選択します。
 - [Existing Attachment]:既存のVPNまたは直接接続アタッチメントを使用する場合は、このオプションを選択します。[Select Attachment ID]ドロップダウンリストから、アタッチメント ID を選択します。

このオプションを選択する場合は、既存の TGW および CGW のルーティングも 設定する必要があります。詳細については、既存のトランジットゲートウェイお よびカスタマーゲートウェイでルーティングを手動設定する (41ページ)を参照してください。

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

[Barracudo]、[Sophos]、[Vyatta]、および [Zyxel] は、サポートされていない VPN ベンダーです。詳細については、VA ポッド設定エラーのトラブルシュート (50 ページ)を参照してください。

- [Platform]:ドロップダウンリストからプラットフォームを選択します。
- •[Software]:ドロップダウンリストからソフトウェアを選択します。
- d) [Customer Profile] のサイズは、デフォルト設定の [Medium] のままにします。

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

- [Cisco Catalyst Center Instance]: r5a.8xlarge、32 個の vCPU、256 GB RAM、4 TB スト レージ。
 - 重要 Cisco DNA Center は r5a.8xlarge インスタンスサイズのみをサポートします。 この設定は変更できません。さらに、r5a.8xlarge インスタンスサイズは、 特定の可用性ゾーンではサポートされていません。サポートされている可 用性ゾーンのリストを表示するには、『Release Notes for Cisco Global Launchpad Release 1.7.0』[英語] を参照してください。
- ・バックアップインスタンス:T3.micro、2個のvCPU、500GBのストレージ、1GB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

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

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

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

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

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

- •オープンポート: 22、2049、873、111
- f) [Next] をクリックします。

1	Configure the AWS Infrastructure Enter EC2 and VPN Details	Review your AWS Infrastructure details and make changes. If you are satisfied with your selection, click the "Start Configuring AWS Infrastructure" button. VA Pod Environment Details		
2	Configure the On-Premises Tunnel Endpoint Precheck with AWS Network Connectivity Check Check IPsec tunnel connection	VA Pod Name	testpod	
3		Availability Zone	ap-northeast-1a	
\bigcirc		AWS VPC CIDR On-Premises Connectivity Transit Gateway (TGW)	VPN GW	
		VPN Attachment Customer Gateway (CGW)	New VPN GW	
		VPN Details		
		CGW (Enterprise Firewall/Router) VPN Vendor	Openswan	
		Platform	Openswan	
		Software	Openswan 2.6.38+	
		Other Details		
		Customer Profile	Medium	
		Backup Target	Cloud Backup (NFS)	
		Exit	Back Start Configuring AWS Infrastructure	

[Summary] ペインが表示されます。

- g) 環境と VPN の入力内容を確認します。問題がなければ、[Start Configuring AWS Infrastructure] をクリックします。
 - 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 重要 のウィンドウやタブを閉じたりしないでください。さもないと、設定が一時停 止します。
- h) AWS インフラストラクチャが正しく設定されると、[AWS Infrastructure Configured] ペイン が表示されます。



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

1	Configure the AWS Infrastructure Enter EC2 and VPN Details	AWS Infrastructure Configuration Failed	
2	Configure the On-Premises Tunnel Endpoint	Failed-Pod-OnPremConnectivity AWS CloudFormation	
3	Precheck with AWS Network Connectivity Check Check Uses taxed eccentric	VpcVpnGateway AWS EC2 Resource creation cancelled	AWS Infra
		VpcCustomerGateway AWS EC2 Resource handler returned message: "Value (192.168.1.2) for parameter publiclp is invalid. (Service: Ec2, Status Code: 400, Request ID: 3205e1ed-c575-479e-bfb4-009b831742e8)" (RequestToken: 92c083d4-32c6-82cc-e421- be347e3b4951, HandlerErrorCode: GeneralServiceException)	Center
		Selied-Pod AWS CloudFormation	
		PrivateRouteTable1 AWS EC2	
		PrivateSubnet1 AWS EC2	
		VPC AWS EC2	
		Failed-Pod-LambdaFunctions	
		Exit	Proceed to On-Premises Configuration

- ステップ6 次の手順を実行して、オンプレミス構成ファイルをダウンロードします。
 - a) AWS インフラストラクチャが正しく設定されたら、[Proceed to On-Premises Configuration] をクリックします。
 - b) [Configure the On-Premises Tunnel Endpoint] ペインで、[Download Configuration File] をクリッ クします。このファイルをネットワーク管理者に転送して、オンプレミス側の IPSec トン ネルを設定します。
 - ネットワーク管理者が IPSec トンネルを1つだけ設定していることを確認してください。

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

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

- ・ほとんどの仮想プライベートゲートウェイソリューションでは、1つのトンネルが稼働し、もう1つのトンネルが停止しています。両方のトンネルを稼働すると、等コストマルチパス(ECMP)ネットワーキング機能を使用できます。ECMP処理では、ファイアウォールまたはルータが等コストルートを使用して同じ宛先にトラフィックを送信できます。このとき、ルータまたはファイアウォールがECMPをサポートしている必要があります。ECMPを使用しない場合は、1つのトンネルを停止して手動でフェールオーバーするか、または IP SLA などのソリューションを使用して、フェールオーバーシナリオでトンネルを自動的に起動することを推奨します。
- c) [Proceed to Network Connectivity Check] ボタンをクリックします。
- **ステップ7** 次のいずれかのアクションを実行して、AWS インフラストラクチャの設定時に選択した優先 するオンプレミス接続に基づいて、ネットワーク構成のステータスを確認します。
 - 優先するオンプレミス接続オプションとして [VPN GW] を選択した場合、IPSec トンネルの設定ステータスが次のように表示されます。
 - ネットワーク管理者が IPSec トンネルをまだ設定していない場合は、IPSec トンネル に鍵アイコンが表示されます。

Network Connectivity Check

Checking for IPsec tunnel connectivity ...



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。

Network Connectivity Check

IPsec tunnel connection is established.



- (注) IPsec トンネルが稼働状態になっているのに、CGW から Cisco DNA Center にア クセスできない場合は、IPsec トンネルの設定中に正しい値が渡されたことを 確認します。Cisco Global Launchpad は AWS 由来のトンネルステータスを報告 し、追加のチェックを実行しません。
- 優先するオンプレミス接続オプションとして [New VPN GW + New TGW] または [Existing TGW and New VPN GW] を選択した場合、Cisco Global Launchpad は、VPC が TGW に接続されているかどうかを確認し、TGW はオンプレミスのファイアウォールまたはルータに接続されます。
 - (注) TGW からエンタープライズファイアウォールまたはルータへの接続に成功するには、ネットワーク管理者がオンプレミスのファイアウォールまたはルータにこの設定を追加する必要があります。

接続ステータスは次のように表示されます。



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

•TGW 接続が正常に確立されると、TGW 接続は緑色になります。



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

接続ステータスは次のように表示されます。

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



•TGW 接続が正常に確立されると、TGW 接続は緑色になります。



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

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

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

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

手順

- ステップ1 AWS コンソールから、[VPC service] に移動します。
- ステップ2 左側のナビゲーションウィンドウの [Transit Gateways] で [Transit gateway route table] を選択し、 次に既存の TGW ルートテーブルを選択します。
- **ステップ3** [Transit gateway route table] ウィンドウで [Associations] タブをクリックし、次に [Create Association] をクリックします。

Network Firewall rule groups	Transit gateway route tables (1/1) Info			C Actions V	Create transit gateway route table
 Virtual private network 	te network				< 1 > @
Customer gateways	☑ Name ♥ Transit gateway route table ID ♥	Transit gateway ID 🛛 🗢	State v	7 Default association route table 🔍	Default propagation route table 🛛 🗢
Virtual private gateways	TEST-0-2-5-NTGW tgw-rtb-04cb3502f1649f635	tgw-044a18d1d2ce07ec6	⊘ Available	No	No
Site-to-Site VPN Connections					
Client VPN Endpoints					
AWS Cloud WAN					
Network Manager					
Transit gateways					
Transit gateways					
Transit gateway attachments		-			
Transit gateway policy tables	tgw-rtb-04cb3502t1649t635 / TEST-0-2-5-NTGW_VA_TGWVPNRouteTab	Routes Tags			
Transit gateway route tables					
Transit gateway multicast	Associations (3) Info			C Delet	e association Create association
Traffic Mirroring	Q. Filter associations				< 1 > @
Mirror sessions					
Mirror targets	□ Attachment ID ♥ Resource type ♥	Resource ID			▽
Mirror filters	tgw-attach-03f39a6aabda35a9b VPC	vpc-048ab88f3c4178310	⊘ Associated		
	tgw-attach-014db4b572f2242e7 VPN	vpn-0f5a1d61c0d22f151	⊘ Associated		
	tow-attach-0b046fe367442fa5f VPC	was 01fd251aa2f8000cB	0		

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

Network Firewall rule	Transit gateway route tables (1/1) Info		C Actions 🔻	Create transit gateway route table
 Virtual private network 	Q Filter transit gateway route tables			< 1 > 6
(VPN) Customer gateways	☑ Name ♥ Transit gateway route table ID ♥ Transit gateway ID ♥	State		Default propagation route table
Virtual private gateways	TEST-0-2-5-NTGW tgw-rtb-04cb3502f1649f635 tgw-044a18d1d2ce07ec6	⊘ Available	No	No
Site-to-Site VPN Connections				
Client VPN Endpoints				
W AWS Cloud WAN				
Network Manager				
 Transit gateways 				
Transit gateways				
Transit gateway attachments	=			
Transit gateway policy	tgw-rtb-04cb3502f1649f635 / TEST-0-2-5-NTGW_VA_TGWVPNRouteTable			
tables	Dataile Accordations Propagations Profix list references Pourtes Tage			
Transit gateway route tables				
Transit gateway multicast	Propagations (3) Info		C Delete pro	Opagation Create propagation
▼ Traffic Mirroring	Q. Filter propagations			< 1 > ©
Mirror sessions				
Mirror targets	Attachment ID V Resource type V Resource ID			∇
Mirror filters	tgw-attach-014db4b572f2242e7 VPN vpn-0f5a1d61c0d22f151	@ Enabled		
	tgw-attach-03f39a6aabda35a9b VPC vpc-048ab88f3c4178310	⊘ Enabled		
Settings	tgw-attach-0b046fe367442fa5f 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確実にアクティブにするには、[Routes] タ ブをクリックし、次に [Create static route] をクリックします。
- **ステップ6** AWS 環境の CGW に割り当てられた CIDR 範囲に向けてネットワークトラフィックをルーティ ングするように、オンプレミスルータの設定が更新されていることを確認します。

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

Cisco DNA Center VAの新規作成

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

手順

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

Global Launchpad	Dashboard			
abhi-iam				
Region(s) All ~				
VA Monitoring				
User Activities				
Settings	2 VA Rost Failed 4 VA Rost In Progress			
(?) Help Center				
	6 VA Ross Completed			
	8 VA Pods: Hes 0 Clicco Catalyst Center(s) Regions • Region with a Failed VA Pod			
	Q. Search VA Pod Status v Create New VA Pod			
	VA Pod 1 O VA Pod 2 O VA Pod 3 O			
	0 Cisco Catalyst Center(s) 0 Cisco Catalyst Center(s) 0 Cisco Catalyst Center(s) ap-south=1 ap-south=1 ap-south=1			
	Create/Manage Cisco Catalyst Center(s) ···· Create/Manage Cisco Catalyst Center(s) ··· Create/Manage Cisco Catalyst Center(s) ···			

- ステップ2 VA ポッドカードで、[Create/Manage Cisco Catalyst Center(s)] をクリックします。
- ステップ3 [VA Pod Dashboard] ペインで、[+ Create New Cisco Catalyst Center] をクリックします。

disclo Global Launchpad	Dashboard > Text1 (us-west-2) VA Pod Dashboard	+ Create New Cisco Catalyst Center
(avr5) ~	÷	VA Pod Details
Region(s) All ~		Environment Details VA Pod Name Test1 Region
VA Monitoring		us-west-2 Awailability Zone us-west-2a AWS VPC CIDR
() Settings		On-Premises Connectivity Transit Gateway (TGW) New VPN GW + New TGW
Help Center		VPN Attachment Customer Gateway (CGW) New VPN GW
	You can create new Cisco Catalyst Center (s) created : You can create new Cisco Catalyst Center by clicking the button above.	VPN Details Customer Gateway IP
		VPN Vendor Openswan Platform Openswan
		Software Openswan 2.6.38+ Other Details
		Customer Profile Međium Backup Target Cloud Backup (NFS) Created By

- ステップ4 次の詳細を入力します。
 - [Cisco Catalyst Center Version]: ドロップダウンリストから、Cisco DNA Center バージョン を選択します。
 - •[Enterprise DNS]: エンタープライズ DNS の IP アドレスを入力します。このエンタープラ イズ DNS が、Cisco DNA Center VA を作成する VA ポッドから到達可能であることを確認 してください。
 - (注) Cisco Global Launchpad は、UDP ポート 53 と入力した DNS サーバーの IP アド レスを使用して、オンプレミスのネットワーク接続を確認します。

- [FQDN (Fully Qualified Domain Name)]: DNS サーバーで設定されている Cisco DNA Center VA の IP アドレスを入力します。
- [Proxy Details]:次のいずれかのHTTPSネットワークプロキシオプションを選択します。
 - [No Proxy]: プロキシサーバーは使用されません。
 - [Unauthenticated]: プロキシサーバーは認証を必要としません。プロキシサーバーの URL とポート番号を入力します。
 - [Proxy Authentication]: プロキシサーバーは認証を必要とします。プロキシサーバーの URL、ポート番号、ユーザー名、およびパスワードの詳細を入力します。
- [Cisco Catalyst Center Virtual Appliance Credentials]: Cisco DNA Center VA にログインする際 に使用する CLI パスワードを入力します。
 - パスワードは、次の条件に従う必要があります。
 - タブや改行を含まないこと。
 - ・8 文字以上であること。
 - ・次のうち少なくとも3つのカテゴリの文字を含むこと。
 - ・小文字の英字
 - ・大文字の英字
 - •番号 (Number)
 - 特殊文字

後で参照できるように、このパスワードを保存しておいてください。

- (注) ユーザー名は maglev です。
- **ステップ5** [Validate] をクリックして、DNS サーバーに設定されているエンタープライズ DNS サーバーと FQDN を検証します。
 - (注) Cisco Global Launchpad リリース 1.7.0 で、DNS サーバー、プロキシサーバー、また は FQDN のチェックに失敗した場合は、次の手順で設定を続行します。
 - DNS サーバーの検証に失敗した場合は、Cisco DNA Center VA の作成を続行で きません。入力した DNS サーバーの IP アドレスが VA ポッドから到達可能で あることを確認してください。
 - ・プロキシサーバーの検証に失敗した場合でも、設定を続行できます。無効なプロキシの詳細が修正されなくても、Cisco DNA Center VA は機能します。
 - FQDN の検証に失敗した場合でも、Cisco DNA Center VA の作成を続行できま す。ただし、Cisco DNA Center VA を機能させるには、FQDN 設定を修正する 必要があります。

ステップ6 [Summary] ウィンドウで、設定の詳細を確認します。

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

Summary

Review your Cisco Catalyst Center VA configuration and make any changes as needed. When you're ready, click "Generate PEM key file".

Domain Details		
Enterprise DNS		0
FQDN	dnac-aws01.cisco.com	\mathbf{x}
Cisco Catalyst Center IP Address		
Proxy Details 🥑		
Customer HTTP Network Proxy	No Proxy	
Other Details		
Cisco Catalyst Center Version	2.3.5.3	
Note : You can continue deploying Cisco Cata	lyst Center but you should fix FQDN to make it	work.

(i) Before you can start configuring your Cisco Catalyst Center VA, you need to download the PEM key file.

Exit

Back Generate PEM key file

- ステップ7 設定に問題がない場合は、[Generate PEM Key File] をクリックします。
- **ステップ8** [Download PEM Key File] ダイアログボックスで、[Download PEM Key File] をクリックします。 [Cancel] をクリックすると、[Summary] ウィンドウに戻ります。
 - **重要** PEM キーは AWS アカウントに保存されていないため、ダウンロードする必要があ ります。作成されている Cisco DNA Center VA にアクセスするには、PEM キーが必 要です。

Download PEM key File



DOWNLOAD PEM KEY FILE

Download and save the PEM key file as it isn't stored in your AWS account. You need it later to access the newly configured Cisco Catalyst Center.

Cancel Download PEM key file

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

Summary

Review your Cisco Catalyst Center VA Configuration and make any changes as needed. When you're ready, click "Start Cisco Catalyst Center Configuration".

Domain I	Details
----------	---------

Enterprise DNS		0
FQDN	dnac.cisco.cloud	×
Cisco Catalyst Center IP Address		
Proxy Details 🤣		
Customer HTTP Network Proxy	No Proxy	
Other Details		

Other Details

Cisco Catalyst Center Version

2.3.5.3

Note : You can continue deploying Cisco Catalyst Center but you should fix FQDN to make it work.

Exit

Start Cisco Catalyst Center Configuration

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

Back

(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。

It can take about 45 minutes for the Cisco Catalyst Center VA to boot. Check back again later. Cisco Catalyst Center Details Cisco Catalyst Center URL Cloud Backup Server IP • udpod-1700472553557-InstanceLaunch AWS CloudFormation • udpod-1700472553557-BackupInstance AWS CloudFormation • BackUpInstance AWS EC2

Cisco Catalyst Center Configuration In Progress

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

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

Cisco Catalyst Center Configuration Failed



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

展開のトラブルシューティング

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



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

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

Docker エラーのトラブルシュート

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

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

ログインエラーのトラブルシュート

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

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

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

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

Rate exceeded.

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

リージョンに関する問題のトラブルシュート

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

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

VA ポッド設定エラーのトラブルシュート

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

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

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

ネットワーク接続エラーのトラブルシュート

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

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



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

Cisco DNA Center VA 設定エラーのトラブルシュート

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

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

同時実行エラーのトラブルシュート

考えられる次の解決策を使用して、同時実行エラーをトラブルシュートします。

エラー	考えられる解決策
Unable to delete a Pod or a Cisco DNA Center created by another user. (別のユーザーが作成	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。
したポッドや Cisco DNA Center は削除でき	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。
ません。) 	・別のユーザーが Cisco DNA Center VA を作成中である。
	•別のユーザーが Cisco DNA Center VA を削除中である。
	・削除を試行して、Cisco DNA Center VA がエラー状態である。
The status of a Pod has been changed recently. (ポッドのステータス が見に亦更されまし	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。
か取 <u></u> 近変 文 C 4 しま し た。)	VA ポッドの更新されたステータスを表示するには、[Refresh] をクリックします。

展開に関するその他の問題のトラブルシュート

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

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

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



Cisco DNA Center VA 起動パッド 1.6 を使用 した展開

- 自動展開メソッドを使用した AWS での Cisco DNA Center の展開 (57 ページ)
- ・自動展開ワークフロー (58ページ)
- 自動展開の前提条件(58ページ)
- Cisco DNA Center VA 起動パッドのインストール (62 ページ)
- ・ホステッド型 Cisco DNA Center VA 起動パッドへのアクセス (64ページ)
- •新しい VA ポッドの作成 (72 ページ)
- 既存のトランジットゲートウェイおよびカスタマーゲートウェイでルーティングを手動設定する(84ページ)
- •新しい Cisco DNA Center VA の作成 (85ページ)
- •展開のトラブルシューティング (91 ページ)

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

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

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

自動展開ワークフロー

自動化されたメソッドを使用して AWS に Cisco DNA Center を展開するには、大まかに言って 次の手順を実行します。

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

自動展開の前提条件

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

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

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

 ・どの方法で Cisco DNA Center VA 起動パッド にアクセスして Cisco DNA Center VA を展開 するかに関係なく、クラウド環境が次の仕様を満たしていることを確認してください。 • **Cisco DNA Center インスタンス**: r5a.8xlarge、32 個の vCPU、256 GB の RAM、4 TB ストレージ

C/

- 重要 Cisco DNA Center は r5a.8xlarge インスタンスサイズのみをサポートします。この設定は変更できません。さらに、r5a.8xlarge インスタンスサイズは、特定の可用性ゾーンではサポートされていません。サポートされている可用性ゾーンのリストを表示するには、『Release Notes for Cisco DNA Center VA 起動パッド Release 1.6.0』[英語]を参照してください。
 - •バックアップインスタンス:T3.micro、2 個の vCPU、500 GB のストレージ、1 GB の RAM
 - ・AWS アカウントにアクセスするための有効なログイン情報を保有していること。
 - AWS アカウントが、リソースの独立性と分離を維持するためのサブアカウント(子アカウント)であること。サブアカウントを使用することで、Cisco DNA Center を展開しても既存のリソースは影響を受けません。
 - 重要:お使いの AWS アカウントが AWS Marketplace の Cisco DNA Center Virtual Appliance - Bring Your Own License (BYOL) に登録されていること。
 - ・管理者ユーザーの場合は、AWS アカウントに管理者アクセス権限が割り当てられている こと(AWS では、ポリシー名は Administrator Access 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。

awys III Services Q Search for	services, features, blags, docs, and more [Option+S]	↔ Ø Global •	dna-tme-user @ 8788-1381-4009
Identity and Access Management (IAM)	New feature to generate a policy based on CloudTrail events. Way uses your CloudTrail events to identify the services and actions used and generate a least privileged policy that you can attach to this user.		×
Dashboard			
 Access management 	Users > dna-tme-user		
User groups	Summany		Delete uses
Users	Commany		Delete user
Roles	User ARN arn:aws:lam::878813814009:user/dna-tme-user		
Policies	Path /		
Identity providers	Creation time 2022-07-23 16:11 PDT		
Account settings	Barmissiana Oroume Targe Requeity and antists Assage Advisor		
	Permissions droups rags becuny credentians Access Advisor		
Access analyzer	 Permissions policies (1 policy applied) 		
Archive rules	Add permissions		O Add inline policy
Analyzers			
Settings	Policy name 👻	Policy type 👻	
Credential report	Attached directly		
Organization activity	AdministratorAccess	AWS managed policy	×
Service control policies (SCPs)	 Permissions boundary (not set) 		
Q Search IAM	 Generate policy based on CloudTrail events 		
AWS account ID: 878813814009	You can generate a new policy based on the access activity for this user, then customize, create, and attach it to this role. AWS uses your CloudTrail events policy. Learn more C	to identify the services and actions used	d and generate a
	Share your feedback and help us improve the policy generation experience. Generate policy		

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

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

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

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

このポリシーでは、次のルールが許可されます。

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

- logs:CreateLogStream
- logs:PutLogEvents
- logs:DescribeLogGroups
- acm:GetCertificate
- acm:DescribeCertificate
- iam:GetSAMLProvider
- lambda:GetFunctionConfiguration
- ConfigPermission (バージョン: 2012-10-17、SID: VisualEditor0)

このポリシーでは、次のルールが許可されます。

- config:Get
- config:*
- config:*ConfigurationRecorder
- config:Describe*
- config:Deliver*
- config:List*
- config:Select*
- tag:GetResources
- tag:GetTagKeys
- cloudtrail:DescribeTrails
- cloudtrail:GetTrailStatus
- cloudtrail:LookupEvents
- config:PutConfigRule
- config:DeleteConfigRule
- config:DeleteEvaluationResults
- PassRole (バージョン: 2012-10-17、SID: VisualEditor0)
 - このポリシーでは、次のルールが許可されます。
 - iam:GetRole
 - iam:PassRole

Cisco DNA Center VA 起動パッド のインストール

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

始める前に

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

手順

ステップ1 シスコのソフトウェアダウンロードサイトに移動し、次のファイルをダウンロードします。

- Launchpad-desktop-client-1.6.0.tar.gz
- Launchpad-desktop-server-1.6.0.tar.gz
- **ステップ2** TARファイルがシスコから正規に配布されていることを確認します。手順の詳細については、 Cisco DNA Center VA の TAR ファイルの確認 (8ページ)を参照してください。
- ステップ3 ダウンロードしたファイルから Docker イメージを読み込みます。

docker load < Launchpad-desktop-client-1.6.0.tar.gz</pre>

docker load < Launchpad-desktop-server-1.6.0.tar.gz</pre>

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

次に例を示します。

\$ docker images

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

ステップ5 サーバーアプリケーションを実行します。

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

次に例を示します。

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

ステップ6 クライアントアプリケーションを実行します。

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

次に例を示します。

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

- (注) 公開されているサーバーのポート番号と REACT_APP_API_URL のポート番号が同じであることを確認します。ステップ5とステップ6では、両方の例でポート番号9090が使用されています。
- ステップ7 docker ps -a コマンドを使用して、サーバーとクライアントのアプリケーションが実行されていることを確認します。[STATUS] 列にアプリケーションが稼働中であることが示されている必要があります。

次に例を示します。

\$ docker ps -a

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

- (注) サーバーまたはクライアントアプリケーションの実行中に問題が発生した場合は、
 Docker エラーのトラブルシュート (91 ページ) を参照してください。
- ステップ8 次の形式でURLを入力して、サーバーアプリケーションにアクセスできることを確認します。

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

次に例を示します。

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

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

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

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

次に例を示します。

http://192.0.2.1:90/valaunchpad

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

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

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

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

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

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

シスコアカウントの作成

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

手順

ステップ1 ブラウザで次のように入力します。

dna.cisco.com

[Cisco DNA Portal] ログインウィンドウが表示されます。



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

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



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

C	reate Acco	unt
* indicates req Email *	uired field	
Email *		
Password *		
Password	*	
First name *		
First name *		
Last name *		
Last name *		
Country or reg	ion *	
Please select	*	-
By clicking Regis to the Cisco Onlin Site Terms and C	ter, I confirm that I hav ne Privacy Statement a conditions.	e read and agree and the Cisco Web
	Desister	

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

Welc	come to Cisco!
Pleas	se click the button to activate your account.
	Activate Account
	Expires in 7 days.
After	activating your account, you can:
	 Login with your email and password.
	 Manage your Cisco account profile and request access to Cisco applications and services.
	 Become a customer by associating a contract number or bill-to ID to your account or order services directly through our global network of certified partners.
	 Become a partner by associating your account with a partner company or register your company as a partner.
	Access supply chain tools and resources.

Cisco DNA ポータル アカウントの作成

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

始める前に

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

手順

ステップ1 ブラウザで次のように入力します。

dna.cisco.com

[Cisco DNA Portal] ログインウィンドウが表示されます。


ステップ2 [Log In With Cisco] をクリックします。

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

الله من المعالم CISCO	US EN
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ます。

Back	US EN
cisco	
Loa in	
Email	
and the gradient	
Descuverd	
Password	
Log in	
5	
Forgot password?	
Help	
Don't have an account? Sign up	
Back to log in	

- ステップ5 [Log in] をクリックします。
- **ステップ6** [Cisco DNA Portal Welcome] ウィンドウの [Name your account] フィールドに組織名またはチー ム名を入力します。[Continue] をクリックします。

Cisco DNA Portal

Welcome,

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

Name your account*	
Ex. Hearst or	Hearst Construction
Cancel	Continue

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

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



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



シスコアカウントでの Cisco DNA ポータル へのログイン

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

始める前に

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

手順

ステップ1 ブラウザで次のように入力します。

dna.cisco.com

[Cisco DNA Portal] ログインウィンドウが表示されます。



ステップ2 [Log In With Cisco] をクリックします。

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

	IS 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ます。

Back	IS EN
cisco	
Log In	
Email	
Password	
Log in	
Forgot password?	
Unlock account?	
Help	
Don't have an account? Sign up	
P. L. L. L.	

ステップ5 [Log in] をクリックします。

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

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

Choose an account

TestAccount	Continue
VA Launchpad	Continue
VALaunchpad-Test-Doc	Continue

[Cisco DNA Portal] ホームページが表示されます。

新しい VA ポッドの作成

VA ポッドは、Cisco DNA Center VA 向けの AWS ホスティング環境です。このホスティング環境には、Cisco DNA Center VA EC2 インスタンス、Amazon Elastic Block Storage (EBS)、バッ クアップ NFS サーバー、セキュリティグループ、ルーティングテーブル、Amazon CloudWatch ログ、Amazon Simple Notification Service (SNS)、VPN ゲートウェイ (VPN GW)、TGW な どの AWS リソースが含まれます。 Cisco DNA Center VA 起動パッドを使用して、複数の VA ポッド (Cisco DNA Center VA ごと に 1 つの VA ポッド)を作成できます。

始める前に

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

手順

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

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

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

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

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

Email to Notify

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

Email ID (i)

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

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

電子メールを入力すると、いくつかのプロセスが実行されます。

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

正常にログインすると、[Dashboard] ペインが表示されます。

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

- ステップ3 [+ Create New VA Pod] をクリックします。
- **ステップ4** [Region Selection] ダイアログボックスで次の手順を実行して、新しいVAポッドを作成するリージョンを選択します。
 - 1. [Region]ドロップダウンリストから、リージョンを選択します。

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

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

- ステップ5 次の手順を実行して、VPC、プライベートサブネット、ルーティングテーブル、セキュリティ グループ、仮想ゲートウェイ、CGW を含む AWS インフラストラクチャを設定します。
 - a) [Environmental Details] フィールドで、次のフィールドを設定します。
 - [VA Pod Name]:新しい VA ポッドに名前を割り当てます。次の制約事項に注意して ください。
 - 名前はリージョン内で一意である必要があります(これは複数のリージョンで同じ名前を使用できることを意味します)。
 - 最大12文字までの名前を指定できます。
 - 名前には、文字(A~Z)、数字(0~9)、およびダッシュ(-)を含めることができます。
 - [Availability Zone]: このドロップダウンリストをクリックして、選択したリージョン 内の分離された場所である可用性ゾーンを選択します。
 - [AWS VPC CIDR]: AWS リソースの起動に使用する一意の VPC サブネットを入力し ます。次の注意事項に従ってください。
 - ・推奨されている CIDR 範囲は /25 です。
 - IPv4 CIDR 表記では、IP アドレスの最後のオクテット(4 番目のオクテット)の 値に指定できるのは0 または 128 のみです。
 - このサブネットは、企業のサブネットと重複しないようにする必要があります。
 - b) [Transit Gateway (TGW)] で、次のいずれかのオプションを選択します。
 - [VPN GW]: VA ポッドが 1 つあり、VPN ゲートウェイを使用する場合は、このオプ ションを選択します。VPN GW は、サイト間 VPN 接続の Amazon 側の VPN エンドポ イントです。1 つの VPC にのみ接続できます。
 - [New VPN GW + New TGW]: 複数の VA ポッドまたは VPC があり、複数の VPC とオンプレミスネットワークを相互接続するトランジットハブとして TGW を使用する場合は、このオプションを選択します。また、TGW をサイト間 VPN 接続の Amazon 側の VPN エンドポイントとして使用することもできます。
 - (注) リージョンごとに1つのTGWのみを作成できます。
 - [Existing TGW]:新しい VA ポッドの作成に使用する既存の TGW がある場合は、この オプションを選択してから、次のいずれかのオプションを選択します。
 - [New VPN GW]:既存の TGW に新しい VPN ゲートウェイを作成する場合は、このオプションを選択します。
 - [Existing Attachment]:既存のVPNまたは直接接続アタッチメントを使用する場合は、このオプションを選択します。[Select Attachment ID]ドロップダウンリストから、アタッチメント ID を選択します。

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

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

[Barracudo]、[Sophos]、[Vyatta]、および [Zyxel] は、サポートされていない VPN ベンダーです。詳細については、VA ポッド設定エラーのトラブルシュート (94 ページ)を参照してください。

- [Platform]:ドロップダウンリストからプラットフォームを選択します。
- ・[Software]:ドロップダウンリストからソフトウェアを選択します。
- d) [Customer Profile] のサイズは、デフォルト設定の [Medium] のままにします。

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

- Cisco DNA Center インスタンス: r5a.8xlarge、32 個の vCPU、256 GB の RAM、4 TB ストレージ
 - 重要 Cisco DNA Center は r5a.8xlarge インスタンスサイズのみをサポートします。 この設定は変更できません。さらに、r5a.8xlarge インスタンスサイズは、 特定の可用性ゾーンではサポートされていません。サポートされている可 用性ゾーンのリストを表示するには、『Release Notes for Cisco DNA Center VA 起動パッド Release 1.6.0』[英語] を参照してください。
- ・バックアップインスタンス:T3.micro、2個のvCPU、500GBのストレージ、1GB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

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

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

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

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

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

- •オープンポート: 22、2049、873、111
- f) [Next] をクリックします。

[Summary] ペインが表示されます。

Configure AWS Infrastructure	Summary	
Vith EC2, VPN Details Configure On-premise Precheck with AWS	Review your AWS Infrastructure deta Configuring AWS Infrastructure"	ails and make changes. If you are satisfied with your selection, click the "Star
	VA Pod Environment Details	
Check IPSec tunnel connection	VA Pod Name	LA-101-1a
	Region	us-east-1
	Availability Zone	us-east-1a
	AWS VPC CIDR	112.162.005
	On-prem Connectivity	
	Transit Gateway (TGW)	VPN GW
	VPN Attachment	
	Customer Gateway (CGW)	New VPN GW
	VPN DETAILS	
	CGW (Enterprise Firewall/Router)	175.06.045.276
	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] ペイン が表示されます。

AWS Infrastructure Configured

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

- ステップ6 次の手順を実行して、オンプレミス構成ファイルをダウンロードします。
 - a) AWS インフラストラクチャが正しく設定されたら、[Proceed to On-Prem Configuration] をク リックします。
 - b) [Configure On-premise] ペインで、[Download Configuration File] をクリックします。このファ イルをネットワーク管理者に転送して、オンプレミス側の IPSec トンネルを設定します。

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

 ・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1** 次のいずれかのアクションを実行して、AWS インフラストラクチャの設定時に選択した優先 するオンプレミス接続に基づいて、ネットワーク構成のステータスを確認します。
 - 優先するオンプレミス接続オプションとして [VPN GW] を選択した場合、IPSec トンネルの設定ステータスが次のように表示されます。
 - ネットワーク管理者が IPSec トンネルをまだ設定していない場合は、IPSec トンネル に鍵アイコンが表示されます。

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

- (注) IPsecトンネルが稼働状態になっているのに、CGWから Cisco DNA Center にア クセスできない場合は、IPsecトンネルの設定中に正しい値が渡されたことを 確認します。Cisco Global Launchpad は AWS 由来のトンネルステータスを報告 し、追加のチェックを実行しません。
- 優先するオンプレミス接続オプションとして [New VPN GW + New TGW] または [Existing TGW and New VPN GW] を選択した場合、Cisco DNA Center VA 起動パッドは、VPC が TGWに接続されているかどうかを確認し、TGW はオンプレミスのファイアウォールまた はルータに接続されます。
 - (注) TGW からエンタープライズ ファイアウォールまたはルータへの接続に成功するには、ネットワーク管理者がオンプレミスのファイアウォールまたはルータにこの設定を追加する必要があります。

接続ステータスは次のように表示されます。

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

•TGW 接続が正常に確立されると、TGW 接続は緑色になります。

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

接続ステータスは次のように表示されます。

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

•TGW 接続が正常に確立されると、TGW 接続は緑色になります。

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

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

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

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

手順

- ステップ1 AWS コンソールから、[VPC service] に移動します。
- **ステップ2** 左側のナビゲーションウィンドウの [Transit Gateways] で [Transit gateway route table] を選択し、 次に既存の TGW ルートテーブルを選択します。
- **ステップ3** [Transit gateway route table] ウィンドウで [Associations] タブをクリックし、次に [Create Association] をクリックします。

Network Firewall rule groups	Transit gateway route tables (1/1) Info	C Actions V Create transit gateway route table
 Virtual private network 	Q Filter transit gateway route tables	< 1 > @
Customer gateways	✓ Name	State $ abla$ Default association route table $ abla$ Default propagation route table $ abla$
Virtual private gateways	TEST-0-2-5-NTGW tgw-rtb-04cb3502f1649f635 tgw-044a18d1d2ce07ec6	O Available No No
Site-to-Site VPN		
Connections		
Client VPN Endpoints		
AWS Cloud WAN		
Network Manager		
Transit gateways		
Transit gateways		
Transit gateway attachments	=	n U Ø
Transit gateway policy	tgw-rtb-04cb3502r1649f635 / TEST-0-2-5-NTGW_VA_TGWVPNRouteTable	
tables	Details Associations Propagations Prefix list references Routes Tags	
tables		
Transit gateway multicast	Associations (3) Info	C Delete association Create association
Traffic Mirroring	Q Filter associations	< 1 > @
Mirror sessions		
Mirror targets	□ Attachment ID ♥ Resource type ♥ Resource ID	v State v
Mirror filters	tgw-attach-03f39a6aabda35a9b VPC vpc-048ab88f3c4178310	⊘ Associated
	tgw-attach-014db4b572f2242e7 VPN vpn-0f5a1d61c0d22f151	⊘ Associated
Settings	tgw-attach-0b046fe367442fa5f VPC vpc-01fd251ea2f8000c9	⊘ Associated

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

Network Firewall rule groups	Transit gateway route tables (1/1) Info		C Actions 🔻	Create transit gateway route table
 Virtual private network (VPN) 	Q Filter transit gateway route tables			< 1 > ©
Customer gateways	✓ Name \[\nothing Transit gateway route table ID \[\nothing Transit gateway ID \[\not	State 🗢	Default association route table 🛛 🗸	Default propagation route table ∇
Virtual private gateways	TEST-0-2-5-NTGW tgw-rtb-04cb3502f1649f635 tgw-044a18d1d2ce07ec6	⊘ Available	No	No
Site-to-Site VPN Connections				
Client VPN Endpoints				
AWS Cloud WAN				
Network Manager				
Transit gateways				
Transit gateways				
Transit gateway attachments	-			- 8 8
Transit gateway policy tables	tgw-rtb-04cb5502r1649f655 / TEST-0-2-5-NTGW_VA_TGWVPNRouteTable Details Associations Propagations Prefix list references Routes Tags			
Transit gateway route tables				
Transit gateway multicast	Propagations (3) Info		C Delete propa	gation Create propagation
▼ Traffic Mirroring	Q. Filter propagations			< 1 > @
Mirror sessions				
Mirror targets	Attachment ID V Resource type V Resource ID	♥ State		∇
Mirror filters	tgw-attach-014db4b572f2242e7 VPN vpn-0f5a1d61c0d22f151	⊘ Enabled		
	tgw-attach-03f39a6aabda35a9b VPC vpc-048ab88f3c4178310	⊘ Enabled		
Settings	tgw-attach-0b046fe367442fa5f 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確実にアクティブにするには、[Routes] タ ブをクリックし、次に [Create static route] をクリックします。
- **ステップ6** AWS 環境の CGW に割り当てられた CIDR 範囲に向けてネットワークトラフィックをルーティ ングするように、オンプレミスルータの設定が更新されていることを確認します。

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

新しい Cisco DNA Center VA の作成

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

手順

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

cisco Cisco DNA Center	Dashboard			
VA Launchpad	Region serves in floand in the following regions will ap-northeast-1 ap-aouth-1 NOTE: Region setup will be automatically seased with	out the VA pods. Choose the regions to remove the ARK setup files. In you attempt to create a new VX.Pod.		Duit Later Dennis
😨 Unior Activities	Upgrade Available The regional satup-opgrade is now available. Upgrade time (in it Later			
	-	57. 220	-	
	æ			
	O un Proces - Audited O un Proces - Un Prespreses B un Proces - Georgeneted		A	
	T sk huls - Nex & Gare Disk Cantery Q. Search by 1A Pod Name	SA Pod Status		1) Barlmach + Croaste Name Vill Paul
	Ve-120 1 Closs DNA Center(s) us wash Create/Manage Disco DNA Center(s)	TEST2 Cross Disk Center(s) warran 2 Cress(Manage Disco Disk Center(s)	Feet Cours DNA Contents) servesh-2 Create(Manager Class-DNA C	enter(s)
regterer	Wilandpat 182			© 2023 Class Aysteins, in Princey - Term

- ステップ2 VA ポッドカードで、[Create/Manage Cisco DNA Center(s)] をクリックします。
- ステップ3 [Create/Manage Cisco DNA Center(s)] ペインで、[+ Create New Cisco DNA Center] をクリックしま す。

ステップ4 次の詳細を入力します。

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

- •[Enterprise DNS]: エンタープライズ DNS の IP アドレスを入力します。このエンタープラ イズ DNS が、Cisco DNA Center VA を作成する VA ポッドから到達可能であることを確認 してください。
 - (注) Cisco DNA Center VA Launchpad は、UDP ポート 53 と入力した DNS サーバーの IP アドレスを使用して、オンプレミスのネットワーク接続を確認します。
- [FQDN (Fully Qualified Domain Name)]: DNS サーバーで設定されている Cisco DNA Center VA の IP アドレスを入力します。
- [Proxy Details]: 次のいずれかの HTTPS ネットワーク プロキシオプションを選択します。
 - [No Proxy]: プロキシサーバーは使用されません。
 - [Unauthenticated]: プロキシサーバーは認証を必要としません。プロキシサーバーの URL とポート番号を入力します。
 - [Proxy Authentication]: プロキシサーバーは認証を必要とします。プロキシサーバーの URL、ポート番号、ユーザー名、およびパスワードの詳細を入力します。
- [Cisco DNA Center Virtual Appliance Credentials]: Cisco DNA Center VA へのログインに使用 する CLIパスワードを入力します。パスワードは、以下のルールに従う必要があります。
 - ・タブまたは改行を省略する
 - ・8 文字以上にする
 - ・次のうち少なくとも3つのカテゴリの文字を含める
 - •小文字 (a~z)
 - 大文字 (A ~ Z)
 - 数字 (0~9)
 - 特殊文字(!や#など)

後で参照できるように、このパスワードを保存しておいてください。

(注) ユーザー名は maglev です。

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

- (注) Cisco DNA Center VA Launchpad のリリース 1.6.0 で、DNS サーバー、プロキシサー バー、または FQDN のチェックに失敗した場合は、次の手順に従って設定を続行し ます。
 - DNS サーバーの検証に失敗した場合は、Cisco DNA Center VA の作成を続行で きません。入力した DNS サーバーの IP アドレスが VA ポッドから到達可能で あることを確認してください。
 - プロキシサーバーの検証に失敗した場合でも、設定を続行できます。無効なプロキシの詳細が修正されなくても、Cisco DNA Center VA は機能します。
 - FQDNの検証に失敗した場合でも、Cisco DNA Center VAの作成を続行できます。ただし、Cisco DNA Center VAを機能させるには、FQDN設定を修正する必要があります。
- **ステップ6** [Summary] ウィンドウで、設定の詳細を確認します。
 - (注) Cisco DNA Center の IP アドレスは静的に割り当てられた IP アドレスであり、中断のない接続を確保し、重要なネットワーク運用中の障害を最小限に抑えるため、 AWS 可用性ゾーンの停止後もそのままに保たれます。

DOMAIN DETAILS			
Enterprise DNS		0	
FQDN (Fully Qualified Domain Name)	dnac.example.com	8	
Cisco DNA Center IP Address	10.193.0.5		
PROXY DETAILS 🥥			
Customer HTTPS Network Proxy	No Proxy		
OTHER DETAILS			
Cisco DNA Center Version	2.3.5.3		
Note : You can continue deploying Cisco D	NA Center but you should fix FQDN to	make it work.	

- ステップ7 設定に問題がない場合は、[Generate PEM Key File] をクリックします。
- **ステップ8** [Download PEM Key File] ダイアログボックスで、[Download PEM Key File] をクリックします。 [Cancel] をクリックすると、[Summary] ウィンドウに戻ります。

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

\sim	<u>L</u>
DOWNLOA	AD PEM KEY FILE
Download and save the PEM Key file need it later to access the ne	as it isn't stored in your AWS account. Yo ewly configured Cisco DNA Center.

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

Summary

Review your Cisco DNA Center VA configuration and make any changes if needed. When you're ready, click Start Cisco DNA Center Configuration

DOMAIN DETAILS			
Enterprise DNS		0	
FQDN (Fully Qualified Domain Name)	cis.co	8	
Cisco DNA Center IP Address			
PROXY DETAILS			
Customer HTTPS Network Proxy	No Proxy		
OTHER DETAILS			
Cisco DNA Center Version	2.3.5.3		
Note : You can continue deploying Cisco D	NA Center but you should fix FQDN	to make it work.	

Cisco DNA Center VA Launchpad により、Cisco DNA Center 環境が設定されます。環境が設定さ れると、Cisco DNA Center が起動します。最初は、Cisco DNA Center VA 起動パットの外側の リングが灰色で表示されます。ポート 2222 が検証されると、イメージがオレンジに変わりま す。ポート 443 が検証されると、イメージが緑色に変わります。 (注) このプロセスは45~60分かかります。アプリケーションを終了したり、このウィ ンドウやタブを閉じたりしないでください。さもないと、設定が一時停止します。

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

Cisco DNA Center Configuration In Progress

Exit

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

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

Cisco DNA Center Configuration In progress

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

展開のトラブルシューティング

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

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

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

Docker エラーのトラブルシュート

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

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

ログインエラーのトラブルシュート

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

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

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。

Deshibeard > A-1 Trigger RCA	Rate exceeded	×
RCA Logs The RCA bundle will consist of Server API logs, AWS resources, event logs and AWS r		
Acce ACA Trigger AWS Logs		
<u>1678341533569-</u>		
	Close	

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

リージョンに関する問題のトラブルシュート

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

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

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

VA ポッド設定エラーのトラブルシュート

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

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

I

エラー	考えられる解決策
Your VPN configuration is invalid. At this step you cannot update it so please delete the instance and create a new one. (VPN の設定が無効で す。このステップでは設定を更新 できないため、インスタンスを削 除してから新しいインスタンスを 作成してください。)	VA ポッドを設定する場合、次の VPN ベンダーはサポートされません。 ・Barracuda ・Sophos ・Vyatta ・Zyxel サポートされていない VPN ベンダーを使用している場合は、次のエラーメッセー ジが Cisco DNA Center VA 起動パッド に表示されます。 Modify VPN Details ② Modify VPN Details ③ Modify VPN Details ③ Modify VPN Details ③ Configure On-premise Please use the configuration file to complete the on-prem configuration ④ Modify Conserving ④ Modify Conserving ⑤ Modify Conserving ⑥ Modify Conserving ⑥ Modify Conserving ⑧ Details ⑥ Network Connectivity Check ⑤ Network Connectivity Check ⑧ Details ⑥ Network Connectivity Check ⑧ Details ⑧ Details 0 D
CustomerGateway with type "ipsec.1", ip-address "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」、 bgp-asn「65000」 のカスタマーゲートウェイはすで に存在します)	ー度に複数の VA ポッドを作成しようとすると、このエラーが発生する可能性が あります。 このエラーを解決するには、障害が発生した VA ポッドを削除して再作成します。 一度に1つの VA ポッドのみを作成するようにしてください。
AWS Infrastructure Failed. (AWSイ ンフラストラクチャで障害が発生 しました。)	 AWS の設定に失敗した場合は、[Dashboard] ペインに戻り、新しい VA ポッドを 作成します。詳細については、新しい VA ポッドの作成 (72 ページ) を参照して ください。 (注) 設定に失敗した VA ポッドを削除できます。
AWS Configuration fails when editing a VA Pod (VA ポッドの編集中に AWS の設定に失敗しました)	 AWS コンソールでの手動プロセスが正常に完了したことを確認し、この手順を再 試行してください。問題が解決しない場合は、TAC にご連絡ください。 (注) このような競合状態を回避するには、VA ポッドを手動で変更しない ことを推奨します。代わりに、すべてのアクションに Cisco DNA Center VA 起動パッドを使用してください。
Deleting VA Pod has failed (VA ポッ ドの削除に失敗しました)	 AWS コンソールでの手動プロセスが正常に完了したことを確認し、この手順を再 試行してください。問題が解決しない場合は、TAC にご連絡ください。 (注) このような競合状態を回避するには、VA ポッドを手動で変更しない ことを推奨します。代わりに、すべてのアクションに Cisco DNA Center VA 起動パッドを使用してください。

エラー	考えられる解決策
The resource you are trying to delete	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
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。)	

ネットワーク接続エラーのトラブルシュート

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

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

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

Cisco DNA Center VA 設定エラーのトラブルシュート

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

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

同時実行エラーのトラブルシュート

考えられる次の解決策を使用して、同時実行エラーをトラブルシュートします。

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

展開に関するその他の問題のトラブルシュート

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

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

問題	考えられる原因と解決策
セッションが終了する	RCAのトリガーなどの操作の進行中にセッションがタイムアウトすると、操作が突然終 了し、次の通知が表示されることがあります。
	Session ended Your session has ended. You'll be redirected to the login page. O K 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。

AWS CloudFormation を使用した展開

- AWS CloudFormation を使用した AWS での Cisco DNA Center の手動展開 (101 ページ)
- AWS CloudFormation ワークフローを使用した手動展開 (101 ページ)
- AWS CloudFormation を使用した手動展開の前提条件 (102 ページ)
- AWS CloudFormation を使用した AWS での Cisco DNA Center の手動展開 (108 ページ)
- •展開の検証(113ページ)

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

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

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

AWS CloudFormation ワークフローを使用した手動展開

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

- 前提条件を満たします。AWS CloudFormation を使用した手動展開の前提条件(102ページ)を参照してください。
- (任意) AWS 上の Cisco ISE と Cisco DNA Center VA を統合します。AWS での AWS 上の Cisco ISE と Cisco DNA Center の統合に関するガイドライン (5ページ) を参照してくだ さい。
- **3.** AWS CloudFormation を使用して AWS に Cisco DNA Center を展開します。AWS CloudFormation を使用した AWS での Cisco DNA Center の手動展開 (108 ページ) を参照し てください。

4. 環境のセットアップと Cisco DNA Center VA の設定が正しく行われ、想定どおりに動作していることを確認します。展開の検証(113ページ)を参照してください。

AWS CloudFormation を使用した手動展開の前提条件

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

ネットワーク環境

ご使用のネットワーク環境に関する次の情報を把握しておく必要があります。

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

AWS 環境

次の AWS 環境要件を満たす必要があります。

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

- リソースの独立性と分離を維持するために、AWSアカウントをサ ブアカウント(子アカウント)にすることを推奨します。サブア カウントを使用することで、Cisco DNA Center を展開しても既存 のリソースは影響を受けません。
 - 重要:お使いの AWS アカウントが AWS Marketplace の Cisco DNA Center Virtual Appliance - Bring Your Own License (BYOL) に登録されていること。
 - AWS アカウントに管理者アクセス権限が割り当てられていること(AWS では、ポリシー 名は Administrator Access と表示されます)。
| Services Q Search for se | rvices, features, blags, docs, and more [Option+5] | ⇔ ® Global ▼ | dna-tme-user @ 8788-1381-400 |
|--|---|---|------------------------------|
| dentity and Access
Management (IAM) | New feature to generate a policy based on CloudTrail events. Wis uses your CloudTrail events to identify the services and actions used and generate a least privileged policy that you can attach to this user. | | \$ |
| Dashboard | | | |
| Access management | Users > dna-tme-user | | |
| User groups | Summany | | |
| Users | Summary | | Delete user |
| Roles | User ARN am:aws:lam::878813814009:user/dna-tme-user @q | | |
| Policies | Path / | | |
| Identity providers | Creation time 2022-07-23 16:11 PDT | | |
| Account settings | | | |
| Access reports | Permissions Groups Tags Security credentials Access Advisor | | |
| Access analyzer | Permissions policies (1 policy applied) | | |
| Archive rules | Add permissions | | O Add inline policy |
| Analyzers | | | |
| Settings | Policy name 👻 | Policy type 👻 | |
| Credential report | Attached directly | | |
| Organization activity | AdministratorAccess | AWS managed policy | × |
| Service control policies (SCPs) | | | |
| | Permissions boundary (not set) | | |
| Q Search IAM | | | |
| | Generate policy based on CloudTrail events | | |
| WS account ID:
76813814009 | You can generate a new policy based on the access activity for this user, then customize, create, and attach it to this role. AWS uses your CloudTrail events
policy. Learn more 12* | s to identify the services and actions used | and generate a |
| | Share your feedback and help us improve the policy generation experience. | | |
| | Generate policy | | |

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

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

Inbound rule	es (25)						C Manage tags	Edit inbound rules
Q Filter secur	ity group rules							< 1 > ©
Name		IP version	▽	Туре	⊽ Proto	col 🗢 Port r	ange 🗢 Source	⊽ Descr
1 -	sgr-0e376bfcb6025cbb5	IPv4		Custom TCP	TCP	9991	0.0.0.0/0	-
p –	sgr-07df898f6cded9989	IPv4		Custom UDP	UDP	123	0.0.0.0/0	
1 -	sgr-041d3c3cf9c91252e	IPv4		Custom TCP	TCP	32626	0.0.0.0/0	-
p _	sgr-0e96b4f0494db5d	IPv4		Custom UDP	UDP	514	0.0.0/0	-
p _	sgr-Offfea3f3af8cb906	IPv4		SSH	TCP	22	0.0.0.0/0	-
p –	sgr-05cbe732bb2feeca8	IPv4		Custom TCP	ТСР	25103	0.0.0.0/0	-
p. –	sgr-022947011fc90efe8	IPv4		DNS (TCP)	тср	53	0.0.0/0	-
p –	sgr-0f9cda6c3ba5d14d2	IPv4		Custom TCP	ТСР	9005	0.0.0/0	-
1 -	sgr-003b55befc96e963b	IPv4		Custom TCP	ТСР	873	0.0.0/0	
D -	sgr-0b08c864158f7d30c	IPv4		All UDP	UDP	0 - 65	535 10.20.0.6,	/32 –
p -	sgr-073f4611f0a79c314	IPv4		Custom UDP	UDP	111	0.0.0.0/0	-
p -	sgr-0f203799c72b67633	IPv4		HTTP	TCP	80	0.0.0/0	-
p =	sgr-04e9f75bda519069b	IPv4		Custom UDP	UDP	21730	0.0.0/0	-
p –	sgr-0220a155852517	IPv4		Custom TCP	TCP	9004	0.0.0.0/0	-
1 -	sgr-0cfdcd269abfdac24	IPv4		Custom TCP	TCP	123	0.0.0.0/0	-
p –	sgr-06732d9b1e871a	IPv4		DNS (UDP)	UDP	53	0.0.0.0/0	-
p _	sgr-00cd51d8b186c67	IPv4		Custom UDP	UDP	6007	0.0.0.0/0	
p _	sgr-01fb034d0ef851d51	IPv4		Custom UDP	UDP	2049	0.0.0.0/0	-
p –	sgr-0aa297c247f44a7f8	IPv4		All ICMP - IPv4	ICMP	All	0.0.0/0	-
D	sgr-0af560ae3f24475b9	IPv4		All TCP	TCP	0 - 65	535 10.20.0.6,	/32 –
D -	sgr-Ofe800a3da1aeff06	IPv4		Custom UDP	UDP	162	0.0.0/0	-
þ –	sgr-01f4b472ae59bb2	IPv4		Custom TCP	TCP	2222	0.0.0/0	-
p _	sgr-075db358356c3acc8	IPv4		NFS	TCP	2049	0.0.0.0/0	-
p –	sgr-05379ca08aee870b1	IPv4		Custom TCP	TCP	111	0.0.0/0	-
p –	sgr-069b3ea740cab18	IPv4		HTTPS	TCP	443	0.0.0.0/0	-)

発信ポートを設定するには、次の図を参照してください。

Out	bound rules	(25)								C	Manage tags	Edit out	bound rules	s
Q	Q Filter security group rules												< 1 > 6	
	Name	∇	Security group rule	IP version	∇	Туре	∇	Protocol	∇	Port range	▽	Destination	⊽	De
	-		sgr-076363ab3019b8	IPv4		All UDP		UDP		0 - 65535		10.20.0.6/32		-
	-		sgr-022ea397d141005f7	IPv4		Custom UDP		UDP		1645		0.0.0.0/0		-
	-		sgr-00b4c14b3e480f183	IPv4		All ICMP - IPv4		ICMP		All		0.0.0.0/0		-
	-		sgr-029b2fd82cdf0edf1	IPv4		Custom TCP		TCP		49		0.0.0.0/0		-
	-		sgr-04c6a1cf3cb3b5cf7	IPv4		All TCP		TCP		0 - 65535		10.20.0.6/32		-
	-		sgr-01376d8fa27c78c1d	IPv4		Custom UDP		UDP		2049		0.0.0.0/0		-
	-		sgr-0e1c02df65c1784fe	IPv4		Custom UDP		UDP		1812		0.0.0.0/0		-
	-		sgr-08dbd82344e593	IPv4		DNS (UDP)		UDP		53		0.0.0.0/0		-
	-		sgr-03231c35500065e	IPv4		Custom TCP		TCP		9060		0.0.0.0/0		-
	-		sgr-092317fd1ff7a0b6e	IPv4		Custom TCP		TCP		123		0.0.0.0/0		-
	-		sgr-0c0ca4c8c4fd5a368	IPv4		Custom TCP		TCP		23		0.0.0.0/0		-
	-		sgr-08b929b66a33f29	IPv4		Custom UDP		UDP		111		0.0.0.0/0		-
	-		sgr-01f3fc40b3e8f06dd	IPv4		Custom TCP		TCP		111		0.0.0.0/0		-
	- 1		sgr-0ae0f6f61929dbc54	IPv4		Custom TCP		TCP		8910		0.0.0.0/0		-
	-		sgr-065fa8cb830ded82e	IPv4		Custom TCP		TCP		830		0.0.0.0/0		-
	-		sgr-0f529ea0425020db7	IPv4		HTTP		TCP		80		0.0.0.0/0		-
	-		sgr-0264702bd385b5	IPv4		Custom UDP		UDP		123		0.0.0.0/0		-
	-		sgr-01ef7a675025aaf9c	IPv4		Custom TCP		TCP		5222		0.0.0.0/0		-
	-		sgr-0793f014435e6d7	IPv4		Custom UDP		UDP		161		0.0.0.0/0		-
	-		sgr-0c5b0d61fe044b92f	IPv4		Custom TCP		TCP		9991		0.0.0.0/0		-
	н.		sgr-0043a759b7dfdabf7	IPv4		Custom TCP		TCP		873		0.0.0.0/0		-
	-		sgr-037a5a1eb51cb99da	IPv4		SSH		TCP		22		0.0.0.0/0		-
	-		sgr-08a1c29aaa4e48d7f	IPv4		HTTPS		TCP		443		0.0.0.0/0		-
	-		sgr-01a7332765efae645	IPv4		DNS (TCP)		TCP		53		0.0.0.0/0		-
	-		sgr-09f0dd53d819618	IPv4		NFS		тср		2049		0.0.0.0/0		-

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

ポート	サービス名	目的	推奨処置
	ICMP	デバイスは ICMP メッセージを使 用してネットワーク接続の問題を 通知します。	ICMP を有効にします。
TCP 22、80、443	HTTPS、SFTP、HTTP	 Cisco DNA Center からのソフトウェ アイメージのダウンロードに HTTPS 443、SFTP 22、HTTP 80を 使用します。 Cisco DNA Center からの証明書の ダウンロードにHTTPS 443、HTTP 80 (Cisco 9800 ワイヤレスコント ローラ、PnP)、センサー/テレメ トリを使用します。 (注) ポート 80 について は、プラグアンドプレ イ (PnP)、ソフト ウェアイメージ管理 (SWIM)、組み込み イベント管理 (EEM)、デバイス登 録、Cisco 9800 ワイヤ レスコントローラを使 用しない場合はブロッ クしてください。 	 これらのポートでCisco DNA Center にアクセスできるホストまたは ネットワークデバイスの送信元 IP がファイアウォールルールで制限 されていることを確認してください。 (注) HTTP 80 の使用は推奨 されません。可能な限 り HTTPS 443 を使用し てください。
UDP 123	NTP	デバイスは時刻の同期にNTPを使 用します。	デバイスが時刻を同期できるよう にポートを開いておく必要があり ます。
UDP 162	SNMP	Cisco DNA Center はデバイスから SNMP ネットワークテレメトリを 受信します。	SNMP に基づくデータ分析用に ポートを開いておく必要がありま す。
UDP 514	Syslog	Cisco DNA Center はデバイスから syslog メッセージを受信します。	syslogに基づくデータ分析用にポー トを開いておく必要があります。
UDP 6007	NetFlow	Cisco DNA Center はデバイスから NetFlow ネットワークテレメトリ を受信します。	NetFlow に基づくデータ分析用に ポートを開いておく必要がありま す。

ポート	サービス名	目的	推奨処置
TCP 9991	Wide Area Bonjour サー ビス	Cisco DNA Center は、Bonjour 制御 プロトコルを使用して、サービス 検出ゲートウェイ(SDG)エー ジェントからマルチキャストドメ インネームシステム(mDNS)ト ラフィックを受信します。	Bonjour アプリケーションがインス トールされている場合、Cisco DNA Center でポートを開いておく必要 があります。
UDP 21730	アプリケーション可視 性サービス	アプリケーション可視性サービス の CBAR デバイス通信。	ネットワークデバイスで CBAR が 有効になっている場合、ポートを 開いておく必要があります。
TCP 25103	ストリーミングテレメ トリが有効になってい る Cisco 9800 ワイヤレ スコントローラおよび Cisco Catalyst 9000 ス イッチ	テレメトリに使用されます。	Cisco DNA Center と Catalyst 9000 デバイス間のテレメトリ接続用に ポートが開いている必要がありま す。
TCP 32626	インテリジェントキャ プチャ (gRPC) コレ クタ	Cisco DNA アシュアランスインテ リジェントキャプチャ(gRPC)機 能で使用されるトラフィック統計 情報とパケットキャプチャデータ の受信に使用されます。	Cisco DNA アシュアランス インテ リジェントキャプチャ(gRPC)機 能を使用する場合、ポートを開い ておく必要があります。

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

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

- [Site-to-Site VPN Connection]: TGW アタッチメントと TGW ルートテーブルを使用で きます。
- ・AWS環境は、次のいずれかのリージョンで設定する必要があります。
 - ap-northeast-1 (東京)
 - ap-northeast-2 (ソウル)
 - ap-south-1 (ムンバイ)

- ap-southeast-1 (シンガポール)
- ap-southeast-2 (シドニー)
- ca-central-1 (カナダ)
- eu-central-1 (フランクフルト)
- eu-south-1 (ミラノ)
- ・eu-west-1(アイルランド)
- eu-west-2 (ロンドン)
- eu-west-3 (パリ)
- us-east-1 (バージニア)
- us-east-2 (オハイオ)
- •us-west-1(北カリフォルニア)
- us-west-2 (オレゴン)
- 複数のIAM ユーザーが同じ環境設定を使用して Cisco DNA Center を設定できるようにするには、次のポリシーを持つグループを作成し、該当するユーザーをそのグループに追加する必要があります。
 - IAMReadOnlyAccess
 - AmazonEC2FullAccess
 - AWSCloudFormationFullAccess
- Cisco DNA Center インスタンスのサイズは、次の最小リソース要件を満たす必要があります。
 - r5a.8xlarge

C)

- 重要 Cisco DNA Center は r5a.8xlarge インスタンスサイズのみをサポートします。この設定は変更できません。さらに、r5a.8xlarge インスタンスサイズは、特定の可用性ゾーンではサポートされていません。サポートされている可用性ゾーンのリストを表示するには、『Release Notes for Cisco Global Launchpad』[英語]を参照してください。
 - 32 vCPU
 - 256 GB RAM
 - •4 TB ストレージ
 - •2500 ディスク入出力処理/秒 (IOPS)

- •180 MBps のディスク帯域幅
- 次のAWS 情報を用意します。
 - ・サブネット ID
 - ・セキュリティ グループ ID
 - ・キーペア ID
 - 環境名
 - CIDR 予約

Cisco DNA Center 環境

Cisco DNA Center 環境が次の要件を満たす必要があります。

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

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

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

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

 DNACDashboard (VA_Instance_MonitoringBoard) : このダッシュボードには、Cisco DNA Center インスタンスの CPUUtilization、NetworkIn、NetworkOut、 DiskReadOps、および DiskWriteOps に関するモニタリング情報が表示されます。

- DnacCPUAlarm: Cisco DNA Center インスタンスの CPU 使用率が 80% 以上になると、このアラームがトリガーされます。CPU 使用率のデフォルトのしきい値は 80% です。
- DnacSystemStatusAlarm: Cisco DNA Center インスタンスのシステムステータスチェック に失敗すると、リカバリプロセスが開始されます。システムステータスチェックのデフォ ルトのしきい値は0です。

始める前に

- ・必要なすべてのコンポーネントを使用して AWS 環境がセットアップされていること。詳細については、AWS CloudFormation を使用した手動展開の前提条件(102ページ)を参照してください。
- VPN トンネルが稼働していること。

手順

- **ステップ1** ダウンロードするファイルに応じて、次のいずれかを実行します。
 - シスコのソフトウェアダウンロードサイトに移動し、次のファイルをダウンロードします。

DNA_Center_VA_InstanceLaunch_CFT-1.7.0.tar.gz

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

DNA_Center_VA_InstanceLaunch_CFT-1.6.0.tar.gz

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

リージョン	Cisco DNA Center AMI ID
ap-northeast-1(東京)	ami-0e15eb31bcb994472
ap-northeast-2 (ソウル)	ami-043e1b9f3ccace4b2
ap-south-1 (ムンバイ)	ami-0bbdbd7bcc1445c5f
ap-southeast-1(シンガポール)	ami-0c365aa4cfb5121a9
ap-southeast-2 (シドニー)	ami-0d2d9e5ebb58de8f7
ca-central-1 (カナダ)	ami-0485cfdbda5244c6e
eu-central-1 (フランクフルト)	ami-0677a8e229a930434

リージョン	Cisco DNA Center AMI ID
eu-south-1 (ミラノ)	ami-091f667a02427854d
eu-west-1(アイルランド)	ami-0a8a59b277dff9306
eu-west-2 (ロンドン)	ami-0cf5912937286b42e
eu-west-3 (パリ)	ami-0b12cfdd092ef754e
us-east-1 (バージニア)	ami-08ad555593196c1de
us-east-2 (オハイオ)	ami-0c52ce38eb8974728
us-west-1 (北カリフォルニア)	ami-0b83a898072e12970
us-west-2 (オレゴン)	ami-02b6cd5eee1f3b521

- **ステップ2** TARファイルがシスコから正規に配布されていることを確認します。手順の詳細については、 Cisco DNA Center VA の TAR ファイルの確認 (8ページ)を参照してください。
- ステップ3 AWS コンソールにログインします。

AWS コンソールが表示されます。

ステップ4 検索バーに「cloudformation」と入力します。

aws Services	Q cloudformation	×	D	\$ °	⑦ Oregon ▼	object.storage 🔻
Lambda 🗿 CloudFor		Search results for 'cloudfor' Services				Â
Stacks StackSets Exports	Features (4) Blogs (403) Documentation (1)	CloudFormation * Create and Manage Resources with Templates			on stack	
Designer		Designer				
 Registry Public extensions Activated extensions 		Registry S CloudFormation feature				
Publisher		Resource import			mation	

- 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。

CloudFormation ×	CloudFormation > Stacks			
Stacks	Stacks (2)	C Delete	e Update Stack actions 🔻 Create stack	
StackSets			With new resources (standard)	
Exports	Q Filter by stack name		With existing resources (import resources)	
Designer			< 1 >	۲
Designer	Stack name	Status	Created time	
Registry	O DnacInstanceTest	Ø CREATE_COMPLETE	2022-07-11 14:15:37 UTC+0530 Cisco Dnac imag	e
Public extensions	O infraTest	⊘ CREATE_COMPLETE	2022-07-11 14:08:22 UTC+0530 Cisco Dnac imag	e
Activated extensions	4			
² ublisher				
Activated extensions Publisher	<pre>intralest </pre>	CREATE_COMPLETE	2022-07-11 14:08:22 UTC+0550 CLISCO UNAC IMA	9

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。

WS Services Q Search for se	rvices, features, blogs, docs, and more [Alt+S]		D 4 0	Oregon 🔻 object.stora
Lambda 🔗 CloudFormation 🧕 EC2				
Step 3 Configure stack options Step 4 Review	Prepare template Every stack is based on a template. A template is a JSON or YAML file that Template is ready Use a sar	contains configuration inform	ation about the AWS resources you	a want to include in the stack.
	Specify template A template is a JSON or YAML file that describes your stack's resources and	properties.		
	Template source Selecting a template generates an Amazon S3 URL where it will be stored.			
	Upload a template file Choose file JSON or YAML formatted file	• Upload a	template file	
				View in Designer
				Cancel Next

ステップ8 スタック名を入力し、次のパラメータを確認します。

・EC2 インスタンスの設定

• [Environment Name]: 一意の環境名を割り当てます。

環境名は、展開を区別するために使用され、AWS リソース名の前に追加されます。 以前の展開と同じ環境名を使用すると、現在の展開でエラーが発生します。

- [Private Subnet ID]: Cisco DNA Center で使用する VPC サブネットを入力します。
- [Security Group]:展開する Cisco DNA Center VA に割り当てるセキュリティグループ を入力します。
- [Keypair]:展開する Cisco DNA Center VA の CLI へのアクセスに使用する SSH キーペ アを入力します。

- Cisco DNA Center の設定: 次の情報を入力します。
 - [DnacInstanceIP] : Cisco DNA Center の IP アドレス。
 - [DnacNetmask]: Cisco DNA Center のネットマスク。
 - [DnacGateway] : Cisco DNA Center のゲートウェイアドレス。
 - [DnacDnsServer]: エンタープライズ DNS サーバー。
 - [DnacPassword] : Cisco DNA Center のパスワード。
 - (注) Cisco DNA Center のパスワードを使用して、AWS EC2 シリアルコンソー ルから Cisco DNA Center VA CLI にアクセスできます。パスワードは、以下のルールに従う必要があります。
 - タブまたは改行を省略する
 - ・8 文字以上にする
 - ・次のうち少なくとも3つのカテゴリの文字を含める
 - •小文字 (a~z)
 - •大文字 (A~Z)
 - 数字 (0~9)
 - ・特殊文字(!や#など)

• [DnacFQDN] : Cisco DNA Center 𝕂 FQDN₀

- [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。

NS Services Q Search for se	rices, features, blogs, docs, and more [Alt+S] Description → Object.storage →
Lambda 👩 CloudFormation 🙋 EC2	
CloudFormation > Stacks >	ireate stack
Step 1 Specify template	Configure stack options
Step 2 Specify stack details	Tags You can specify tags (key-value pairs) to apply to resources in your stack. You can add up to 50 unique tags for each stack. Learn more 🔀
Step 3 Configure stack options	Key Value Remove
Step 4 Review	Add tag
	Permissions Choose an IAM role to explicitly define how CloudFormation can create, modify, or delete resources in the stack. If you don't choose a role, CloudFormation uses permissions based on your user credentials. Learn more 🖄
	IAM role - optional Choose the IAM role for CloudFormation to use for all operations performed on the stack.
	iamRoleName V Remove

- 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。

aws	Services Q Search	[Option+S]		Þ	\$*	0	N. Virginia 🔻	dna-tme-user @ 8788-1381-4009
≡		CloudWatch alarm ARN						
			No rollback triggers					
		Notification options						
		Q. Search						
		SNS topic ARN						
			No notification options There are no notification options defined					
		Stack creation options						
		Timeout						
		Termination protection Disabled						
		Quick-create link						
		Create change set					Cancel	Previous Submit

スタックの作成プロセスには、通常45~60分かかります。

展開の検証

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

始める前に

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

手順

- **ステップ1** Amazon EC2 コンソールから、ネットワークとシステムの設定を検証し、Cisco DNA Center IP アドレスが正しいことを確認します。
- **ステップ2** Cisco DNA Center の IP アドレスに ping を送信して、ホストの詳細とネットワーク接続が有効 であることを確認します。
- **ステップ3** Cisco DNA Center との SSH 接続を確立して、Cisco DNA Center が認証されていることを確認し ます。
- **ステップ4** 次のいずれかのメソッドを使用して、Cisco DNA Center GUI への HTTPS アクセシビリティを テストします。
 - ブラウザを使用します。

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

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



AWS Marketplace を使用した展開

- AWS Marketplace を使用した AWS での Cisco DNA Center の手動展開 (115 ページ)
- AWS Marketplace ワークフローを使用した手動展開 (115 ページ)
- AWS Marketplace を使用した手動展開の前提条件 (116ページ)
- AWS Marketplace を使用した AWS での Cisco DNA Center の手動展開 (122 ページ)
- •展開の検証(122ページ)

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

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

AWS Marketplace ワークフローを使用した手動展開

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

- 前提条件を満たします。AWS Marketplace を使用した手動展開の前提条件(116ページ)を 参照してください。
- (任意) AWS 上の Cisco ISE と Cisco DNA Center VA を統合します。「AWS での AWS 上の Cisco ISE と Cisco DNA Center の統合に関するガイドライン (5 ページ)」を参照してください。
- **3.** AWS Marketplace を使用して AWS に Cisco DNA Center を展開します。AWS Marketplace を 使用した AWS での Cisco DNA Center の手動展開 (122 ページ) を参照してください。
- **4.** 環境のセットアップと Cisco DNA Center VA の設定が正しく行われ、想定どおりに動作していることを確認します。展開の検証(122ページ)を参照してください。

AWS Marketplace を使用した手動展開の前提条件

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

ネットワーク環境

ご使用のネットワーク環境に関する次の情報を把握しておく必要があります。

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

AWS 環境

次の AWS 環境要件を満たす必要があります。

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



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

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

antity and Accase				
anagement (IAM)	New feature to generate a policy based on Cloud	Trail events.		
-	AWS uses your CloudTrail events to identify the services and ac	tions used and generate a least privileged policy that you can attach to this user.		
Dashboard	Users > dna-tme-user			
Access management				
User groups	Summary			Delete user
Users				
Roles	User ARN arn:aws:iam::878813814009:	:user/dna-tme-user 🖉		
olicies	Path /			
dentity providers	Creation time 2022-07-23 16:11 PDT			
ccount settings	Demainsione Course Trees Coursity and entirely Ar			
ccess reports	Permissions Groups lags Security credentials Ac	Cess Advisor		
ccess analyzer	 Permissions policies (1 policy applied) 			
Archive rules	Add permissions			O Add inline policy
Analyzers				
Settings	Policy name 👻		Policy type 👻	
Credential report	Attached directly			
Drganization activity	AdministratorAccess		AWS managed policy	
Service control policies (SCPs)				
	 Permissions boundary (not set) 			
Search IAM				
	 Generate policy based on CloudTrail events 			
account ID:				
13814009	You can generate a new policy based on the access activity for this user	r, then customize, create, and attach it to this role. AWS uses your CloudTrail events	to identify the services and actions used	i and generate a
	Photo your feadback and halo us improve the pallou generation superior	-		
	onare your recuback and help us improve the policy generation expension	en.e.		

・次のリソースとサービスを AWS で設定する必要があります。

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

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

Inbound rules	s (25)				C	Manage tags Edit i	nbound rules
Q Filter security	y group rules					<	1 > 6
Name	▽ Security group rule	IP version \bigtriangledown	Туре		▽ Port range		⊽ De
-	sgr-0e376bfcb6025cbb5	IPv4	Custom TCP	TCP	9991	0.0.0/0	-
-	sgr-07df898f6cded9989	IPv4	Custom UDP	UDP	123	0.0.0/0	-
-	sgr-041d3c3cf9c91252e	IPv4	Custom TCP	TCP	32626	0.0.0/0	-
-	sgr-0e96b4f0494db5d	IPv4	Custom UDP	UDP	514	0.0.0/0	-
-	sgr-Offfea3f3af8cb906	IPv4	SSH	TCP	22	0.0.0/0	-
-	sgr-05cbe732bb2feeca8	IPv4	Custom TCP	TCP	25103	0.0.0/0	-
-	sgr-022947011fc90efe8	IPv4	DNS (TCP)	TCP	53	0.0.0/0	-
-	sgr-Of9cda6c3ba5d14d2	IPv4	Custom TCP	TCP	9005	0.0.0/0	-
-	sgr-003b55befc96e963b	IPv4	Custom TCP	TCP	873	0.0.0/0	-
-	sgr-0b08c864158f7d30c	IPv4	All UDP	UDP	0 - 65535	10.20.0.6/32	-
-	sgr-073f4611f0a79c314	IPv4	Custom UDP	UDP	111	0.0.0/0	-
-	sgr-0f203799c72b67633	IPv4	HTTP	TCP	80	0.0.0/0	-
-	sgr-04e9f75bda519069b	IPv4	Custom UDP	UDP	21730	0.0.0/0	-
-	sgr-0220a155852517	IPv4	Custom TCP	TCP	9004	0.0.0/0	-
-	sgr-0cfdcd269abfdac24	IPv4	Custom TCP	TCP	123	0.0.0/0	-
-	sgr-06732d9b1e871a	IPv4	DNS (UDP)	UDP	53	0.0.0/0	-
-	sgr-00cd51d8b186c67	IPv4	Custom UDP	UDP	6007	0.0.0/0	-
-	sgr-01fb034d0ef851d51	IPv4	Custom UDP	UDP	2049	0.0.0/0	-
-	sgr-0aa297c247f44a7f8	IPv4	All ICMP - IPv4	ICMP	All	0.0.0/0	-
-	sgr-0af560ae3f24475b9	IPv4	All TCP	TCP	0 - 65535	10.20.0.6/32	-
-	sgr-Ofe800a3da1aeff06	IPv4	Custom UDP	UDP	162	0.0.0/0	-
-	sgr-01f4b472ae59bb2	IPv4	Custom TCP	TCP	2222	0.0.0/0	-
-	sgr-075db358356c3acc8	IPv4	NFS	тср	2049	0.0.0/0	-
-	sgr-05379ca08aee870b1	IPv4	Custom TCP	тср	111	0.0.0/0	-
-	sgr-069b3ea740cab18	IPv4	HTTPS	TCP	443	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。

Out	Outbound rules (25) Q. Filter security group rules						C Manage tags Edit outbou			
Q									< 1 > @	
	Name	∇	Security group rule	IP version	▽	Туре	⊽ Protoc	col 🗢 Port ra	nge 🗢 Destination	⊽ De
	-		sgr-076363ab3019b8	IPv4		All UDP	UDP	0 - 655	35 10.20.0.6/3	2 –
	-		sgr-022ea397d141005f7	IPv4		Custom UDP	UDP	1645	0.0.0/0	-
	-		sgr-00b4c14b3e480f183	IPv4		All ICMP - IPv4	ICMP	All	0.0.0/0	-
	-		sgr-029b2fd82cdf0edf1	IPv4		Custom TCP	TCP	49	0.0.0/0	-
	-		sgr-04c6a1cf3cb3b5cf7	IPv4		All TCP	TCP	0 - 655	35 10.20.0.6/3	2 –
	-		sgr-01376d8fa27c78c1d	IPv4		Custom UDP	UDP	2049	0.0.0/0	-
	-		sgr-0e1c02df65c1784fe	IPv4		Custom UDP	UDP	1812	0.0.0/0	-
	-		sgr-08dbd82344e593	IPv4		DNS (UDP)	UDP	53	0.0.0/0	-
	-		sgr-03231c35500065e	IPv4		Custom TCP	TCP	9060	0.0.0/0	-
	-		sgr-092317fd1ff7a0b6e	IPv4		Custom TCP	TCP	123	0.0.0/0	-
	-		sgr-0c0ca4c8c4fd5a368	IPv4		Custom TCP	TCP	23	0.0.0/0	-
	-		sgr-08b929b66a33f29	IPv4		Custom UDP	UDP	111	0.0.0/0	-
	-		sgr-01f3fc40b3e8f06dd	IPv4		Custom TCP	TCP	111	0.0.0/0	-
	-		sgr-0ae0f6f61929dbc54	IPv4		Custom TCP	TCP	8910	0.0.0/0	-
	-		sgr-065fa8cb830ded82e	IPv4		Custom TCP	TCP	830	0.0.0/0	-
	-		sgr-0f529ea0425020db7	IPv4		HTTP	TCP	80	0.0.0/0	-
	-		sgr-0264702bd385b5	IPv4		Custom UDP	UDP	123	0.0.0/0	-
	-		sgr-01ef7a675025aaf9c	IPv4		Custom TCP	TCP	5222	0.0.0/0	-
	-		sgr-0793f014435e6d7	IPv4		Custom UDP	UDP	161	0.0.0/0	-
	-		sgr-0c5b0d61fe044b92f	IPv4		Custom TCP	TCP	9991	0.0.0/0	-
	-		sgr-0043a759b7dfdabf7	IPv4		Custom TCP	TCP	873	0.0.0/0	-
	-		sgr-037a5a1eb51cb99da	IPv4		SSH	TCP	22	0.0.0/0	-
	-		sgr-08a1c29aaa4e48d7f	IPv4		HTTPS	TCP	443	0.0.0.0/0	-
	-		sgr-01a7332765efae645	IPv4		DNS (TCP)	TCP	53	0.0.0.0/0	-
	_		sgr-09f0dd53d819618	IPv4		NFS	TCP	2049	0.0.0.0/0	-

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

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

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

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

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

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

- [Site-to-Site VPN Connection]: TGW アタッチメントと TGW ルートテーブルを使用できます。
- •AWS環境は、次のいずれかのリージョンで設定する必要があります。
 - ap-northeast-1 (東京)
 - ap-northeast-2 (ソウル)
 - ap-south-1 (ムンバイ)
 - ap-southeast-1 (シンガポール)
 - ap-southeast-2 (シドニー)
 - ca-central-1 (カナダ)
 - eu-central-1 (フランクフルト)
 - eu-south-1 (ミラノ)

- ・eu-west-1 (アイルランド)
- eu-west-2 (ロンドン)
- eu-west-3 (パリ)
- us-east-1 (バージニア)
- •us-east-2 (オハイオ)
- •us-west-1(北カリフォルニア)
- us-west-2 (オレゴン)
- 複数のIAM ユーザーが同じ環境設定を使用して Cisco DNA Center を設定できるようにするには、次のポリシーを持つグループを作成し、該当するユーザーをそのグループに追加する必要があります。
 - IAMReadOnlyAccess
 - AmazonEC2FullAccess
 - AWSCloudFormationFullAccess
- Cisco DNA Center インスタンスのサイズは、次の最小リソース要件を満たす必要があります。
 - r5a.8xlarge

¢

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

• 32 vCPU

- 256 GB RAM
- •4 TB ストレージ
- •2500 ディスク入出力処理/秒(IOPS)
- •180 MBps のディスク帯域幅
- 次の AWS 情報を用意します。
 - ・サブネット ID
 - ・セキュリティグループ ID

- ・キーペア ID
- 環境名
- CIDR 予約

Cisco DNA Center 環境

Cisco DNA Center 環境が次の要件を満たす必要があります。

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

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

AWS Marketplace を使用して AWS で Cisco DNA Center を展開する方法については、シスコの ソフトウェアダウンロードサイトにアクセスし、次のファイルをダウンロードしてください。

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

展開の検証

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

始める前に

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

手順

- ステップ1 Amazon EC2 コンソールから、ネットワークとシステムの設定を検証し、Cisco DNA Center IP アドレスが正しいことを確認します。
- **ステップ2** Cisco DNA Center の IP アドレスに ping を送信して、ホストの詳細とネットワーク接続が有効 であることを確認します。
- **ステップ3** Cisco DNA Center との SSH 接続を確立して、Cisco DNA Center が認証されていることを確認し ます。
- ステップ4 次のいずれかのメソッドを使用して、Cisco DNA Center GUI への HTTPS アクセシビリティを テストします。
 - ブラウザを使用します。

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

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

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては 、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている 場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容につい ては米国サイトのドキュメントを参照ください。