Amazon Web Services での展開

- 前提条件とガイドライン （1 ページ）
- AWS での Nexus ダッシュボードの展開 （3 ページ）

前提条件とガイドライン

Amazon Web Services（AWS）で Nexus ダッシュボード クラスタを展開する前に、次の手順を実行する必要があります。

- ファクターから AWS が拡張性とサービス要件をサポートしていることを確認します。

  クラスタ フォーム ファクタに基づいて、拡張性とサービス サポートおよび共同ホストは異なります。Nexus ダッシュボード キャパシティ プラン ツールを使用して、仮想フォーム ファクタが展開要件を満たすことを確認できます。

（注） スタンバイ ノードとワーカー ノードは、このクラスタ フォーム ファクタではサポートされていません。

- デプロイ概要 に記載されている一般的な前提条件を確認して完了します。
- 展開する予定のサービスのリリース ノートに記載されている追加の前提条件を確認して完了します。
- AWS アカウントに適切なアクセス権限があること。

  Nexus ダッシュボード クラスタをホストするには、複数の Elastic Compute Cloud（`m5.2xlarge`）のインスタンスを起動できる必要があります。

- 6 つ以上の AWS Elastic IP アドレスが必要です。

  一般的な Nexus ダッシュボードの導入は 3 つのノードで構成され、各ノードには管理およびデータネットワーク用に 2 つの AWS Elastic IP アドレスが必要です。

  デフォルトでは、AWS アカウントの Elastic IP の制限は低いため、増加を要求する必要があります。IP 制限の増加を要求するには、次の手順を実行します。

1. AWS コンソールで、**[Computer]** > **[EC2]** の順に移動します。
2. EC2 ダッシュボードで、**[Network & Security]** > **[Elastic IPs]** をクリックし、すでに使用されている Elastic IP の数を確認します。
3. EC2 ダッシュボードで、**[制限（Limits）]** をクリックし、許可されている **EC2-VPC Elastic IP** の最大数を確認します。

   使用する IP の数を制限から減算します。必要に応じて、**[制限の増加を要求（Request limit 増加）]** をクリックして追加の Elastic IP を要求します。

- VPC（仮想プライベート クラウド）を作成します。

  VPC は、Amazon EC2 インスタンスなどの AWS オブジェクトによって入力される AWS クラウドの分離された部分です。VPC を作成するには:

  1. AWS コンソールで、**[Networking & Content Delivery Tools] [VPC]**に移動します。
  2. VPC ダッシュボードで **[Your VPCs]** をクリックし、**[Create VPC]** を選択します。次に、**名前タグ**と **IPv4 CIDR ブロック** を指定します。

     CIDR ブロックは VPC の IPv4 アドレスの範囲であり、`/16`〜`/24` の範囲である必要があります。たとえば、`10.9.0.0/16` です。

- インターネット ゲートウェイを作成し、VPC に接続します。

  インターネット ゲートウェイは、VPC がインターネットに接続できるようにする仮想ルータです。インターネット ゲートウェイを作成するには:

  - [VPC ダッシュボード（VPC Dashboard）] > **[インターネット ゲートウェイ（Internet Gateway）]** の順にクリックしてから、**[インターネット ゲートウェイの作成（Create Internet Gateway）]** をクリックします。次に、**名前タグ**を入力します。
  - **[インターネット ゲートウェイ（Internet Gateways）]** 画面で、作成したインターネット ゲートウェイを選択し、**[アクション]** > **[VPC をアタッチ]** を選択します。最後に、**[使用可能な VPC（Available VPCs）]** ドロップダウンから、作成した VPC を選択し、**[インターネット ゲートウェイのアタッチ（Attach Internet Gateway）]** をクリックします。

- ルート テーブルを作成します。

  ルートテーブルは、VPC およびインターネット ゲートウェイ内のサブネットを Nexus ダッシュボード クラスタに接続するために使用されます。ルート テーブルを作成するには、次の手順を実行します。

  - VPC ダッシュボードで、**[ルート テーブル（Route Tables）]** をクリックし、**[ルート（Routes）]** タブを選択して、**[ルートの編集（Edit routes）]** をクリックします。
  - **[ルートの編集（Edit routes）]** 画面で、**[ルートの追加（Add route）]** をクリックし、`0.0.0.0/0` の宛先を作成します。**[ターゲット（Target）]** ドロップダウンから `[インターネット ゲートウェイ（Target Internet Gateway）]` から、作成したゲートウェイを選択します。最後に、**[ルートの保存（Save Routes）]** をクリックします。

- キー ペアを作成します。

  キー ペアは、プライベート キーとパブリック キーで構成され、インスタンスへの接続時に ID を証明するために使用されるセキュリティ クレデンシャルとして使用されます。キー ペアを作成するには:

  - **[すべてのサービス（All services）]** > **[コンピュート（Compute）]** > **[EC2]**に移動します。
  - EC2 ダッシュボードで、**[ネットワークとセキュリティ（Network & Security）]** > **[キーペア（Key pairs）]** をクリックします。次に、**[キー ペアの作成 (Create Key Pair)]** をクリックします。
  - キー ペアの名前を入力し、**pem** ファイル形式を選択して、**[キー ペアの作成 (Create Key Pair)]** をクリックします。

    これにより、`.pem` 秘密キー ファイルがシステムにダウンロードされます。ファイルを安全な場所に移動します。EC2インスタンスのコンソールに初めてログインするときに使用する必要があります。

（注） デフォルトでは、PEMベースのログインのみが各ノードで有効になっています。GUI セットアップ ウィザードで要求されるパスワードを使用してノードにSSHで接続できるようにするには、生成されたキーを使用して各ノードにログインし、以下のセットアップセクションの説明に従って必要なコマンドを実行することにより、パスワードベースのログインを明示的に有効にする必要があります。

AWS での Nexus ダッシュボードの展開

ここでは、Amazon Web Services (AWS) で Cisco Nexus ダッシュボード クラスタを展開する方法について説明します。

始める前に

- 前提条件とガイドライン （1 ページ） に記載されている要件とガイドラインを満たしていることを確認します。

手順

ステップ 1 AWS Marketplace で Cisco Nexus ダッシュボード製品に登録します。

a) AWS アカウントにログインし、AWS Management Console に移動します。

管理コンソールは https://console.aws.amazon.com/ で入手できます。

b) **[サービス]** > **[AWS マーケットプレイス サブスクリプション（Services AWS Marketplace Subscriptions）]**に移動します。
c) [Manage Subscriptions] をクリックします。
d) **[製品の検出（Discover products）]** をクリックします。
e) **Cisco Nexus ダッシュボード**を検索し、結果をクリックします。
f) 製品ページで、**[続行して登録（Continue to Subscribe）]** をクリックします。
g) [条件に同意する（Accept Terms）] をクリックします。

サブスクリプションが処理されるまでに数分かかる場合があります。

h) 最後に、**[設定を続行 (Continue to Configuration)]** をクリックします。

ステップ 2 ソフトウェア オプションと地域を選択します。

a) **[配送方法（Delivery Method）]**ドロップダウンから、`[Cisco Nexus Dashboard for Cloud]` を選択します。
b) **[ソフトウェア バージョン（Software Version）]** ドロップダウンから、展開するバージョンを選択します。
c) **[リージョン（Region）]** ドロップダウンから、テンプレートを展開するリージョンを選択します。

これは、VPC を作成したのと同じリージョンである必要があります。

d) **[続行して起動する（Continue to Launch）]** をクリックします

この製品 ページが表示され、設定の概要が表示され、クラウド形成テンプレートを起動できます。

ステップ 3 **[アクションの選択（Choose Action）]** から、`[CloudFormation の起動（Launch CloudFormation）]` を選択し、**[起動（Launch）]** をクリックします。

[Create Stack（スタックの作成）] ページが表示されます。

ステップ 4 スタックを作成します。

a) **[前提条件 - テンプレートの準備（Prerequisite-Prepare template）]** 領域で、`[テンプレート準備完了（Template is ready）]` を選択します。
b) **[テンプレートの指定（Specify Template）]** フィールドで、テンプレート ソースとして `[Amazon S3 URL]` を選択します。

これは、自動的に入力されます。

c) [**次へ（Next）**] をクリックして続行します。

[スタック詳細の指定（Specify stack details）] ページが表示されます。

ステップ 5 スタックの詳細を指定します。

a) **スタック名**を入力します。
b) **[VPC ID]** ドロップダウンから、作成した VPC を選択します。

たとえば、`vpc-038f83026b6a48e98（10.176.176.0/24）` です。

c) **ND クラスタ サブネット ブロック**で、VPC サブネット CIDR ブロックを指定します。

定義した VPC CIDR からサブネットを選択します。より小さいサブネットを提供することも、CIDR 全体を使用することもできます。CIDR は `/24` または `/25` サブネットにすることができ、可用性ゾーン全体で使用されるようにセグメント化されます。

たとえば、`10.176.176.0/24` です。

d) **[可用性ゾーン（Availability Zones）]** ドロップダウンから、1 つ以上の使用可能なゾーンを選択します。

3 つの可用性ゾーンを選択することをお勧めします。2 つの可用性ゾーンのみをサポートするリージョンの場合、クラスタの 2 番目と 3 番目のノードは 2 番目の可用性ゾーンで起動します。

e) **[可用性ゾーンの数（Number of Availability Zones）]** ドロップダウンから、前のサブステップで追加したゾーンの数を選択します。

この番号が、前のサブステップで選択した可用性ゾーンの数と一致していることを確認します。

f) **データ インターフェイス EIP サポート**を有効にします。

このフィールドは、ノードの外部接続を有効にします。AWS 以外の Cisco ACI ファブリックとの通信には、外部接続が必要です。

g) **[パスワード（Password）]** および **[パスワードの確認（Confirm Password）]** フィールドに、パスワードを提供します。

このパスワードは、Nexus ダッシュボードのレスキュー ユーザ ログインと、GUI の管理者ユーザの初期パスワードに使用されます。

（注）
すべてのノードに同じパスワードを指定する必要があります。指定しない場合、クラスタ作成に失敗します。

h) **[SSH key pair]** ドロップダウンから、作成したキーペアを選択します。

i) **[アクセス制御（Access control）]** フィールドに、クラスタへのアクセスを許可する外部ネットワークを指定します。

たとえば、`0.0.0.0/0` は、どこからでもクラスタにアクセスできます。

j) [**次へ（Next）**] をクリックして続行します。

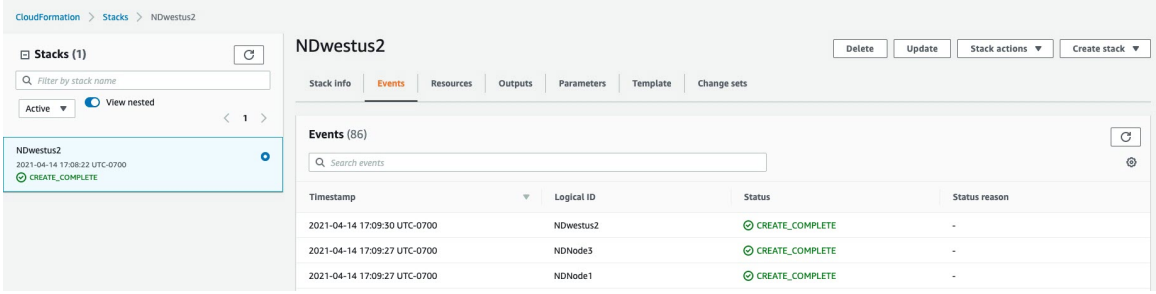
ステップ 6 **[詳細オプション（Advanced options）]** 画面で、**[次へ（Next）]**をクリックします。

ステップ 7 **[レビュー（Review）]** 画面で、テンプレート設定を確認し、**[スタックの作成（Create stack）]** をクリックします。

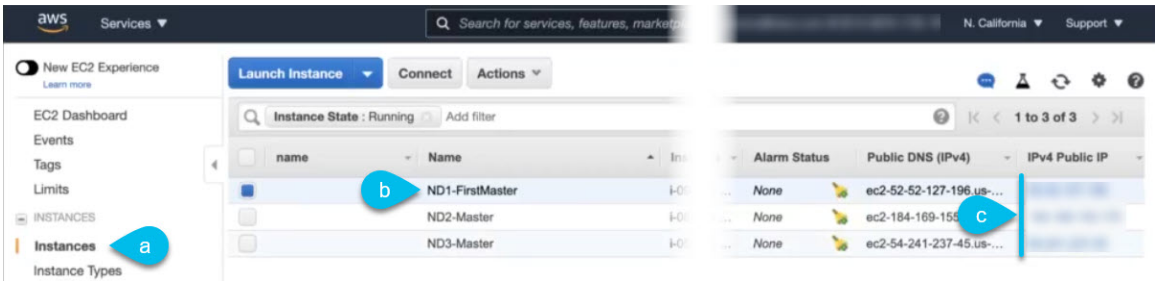
ステップ 8 展開が完了するのを待ってから、VM を起動します。

[CloudFormation] ページでインスタンスの展開のステータス（`CREATE_IN_PROGRESS` など）を表示できます。ページの右上隅にある更新ボタンをクリックすると、ステータスを更新できます。

ステータスが `CREATE_COMPLETE` に変わったら、次の手順に進むことができます。



ステップ 9 すべてのノードのパブリック IP アドレスを書き留めます。



a) すべてのインスタンスが展開されたら、AWS コンソールの **EC2** > **Instances** ページに移動します。

b) `FirstMaster` とラベル付けされているノードを書き留めます。

このノードのパブリック IP アドレスを使用して、クラスタ設定を完了します。

c) すべてのノードのパブリック IP アドレスを書き留めます。

次の手順で、この情報を GUI ブートストラップ ウィザードに提供します。

ステップ 10 すべてのノードでパスワードベースのログインを有効にします。

デフォルトでは、PEM ベースのログインのみが各ノードで有効になっています。パスワードを使用して SSH をノードに接続できるようにするには、GUI セットアップ ウィザードで要求されるように、パスワードベースのログインを明示的に有効にする必要があります。

（注）
次の手順で説明するクラスタブートストラップに進む前に、すべてのノードでパスワードベースのログインを有効にする必要があります。そうしないと、クラスタ設定を完了できません。

a) パブリック IP アドレスと PEM ファイルを使用して、インスタンスの 1 つに SSH で接続します。

このために作成した PEM ファイルを 前提条件とガイドライン （1 ページ） の一部として使用します。

```
# ssh -i <pem-file-name>.pem rescue-user@<node-public-ip>
```

b) パスワードベースのログインを有効にします。

各ノードで、次のコマンドを実行します。

```
# acs login-prompt enable
```

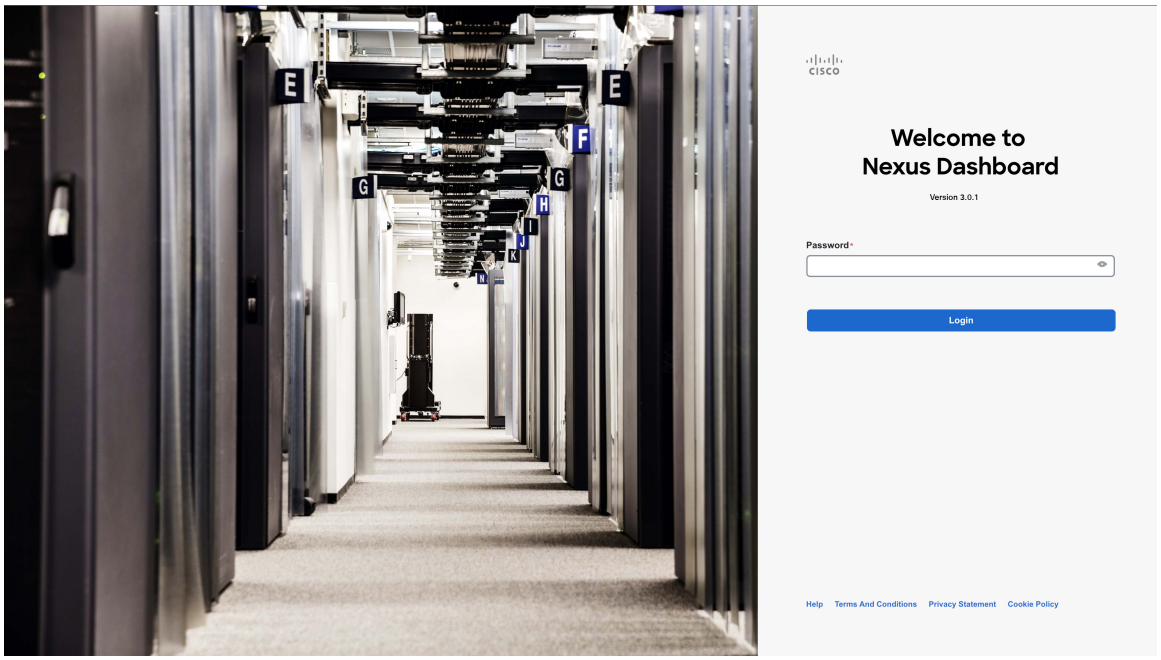
c) 他の 2 つのインスタンスについて、この手順を繰り返します。

ステップ 11 ブラウザを開き、`https://<first-node-public-ip>` に移動して、GUI を開きます。

（注）
最初のノード（`FirstMaster`）のパブリック IP アドレスを使用する必要があります。そうしないと、クラスタ構成を完了できません。

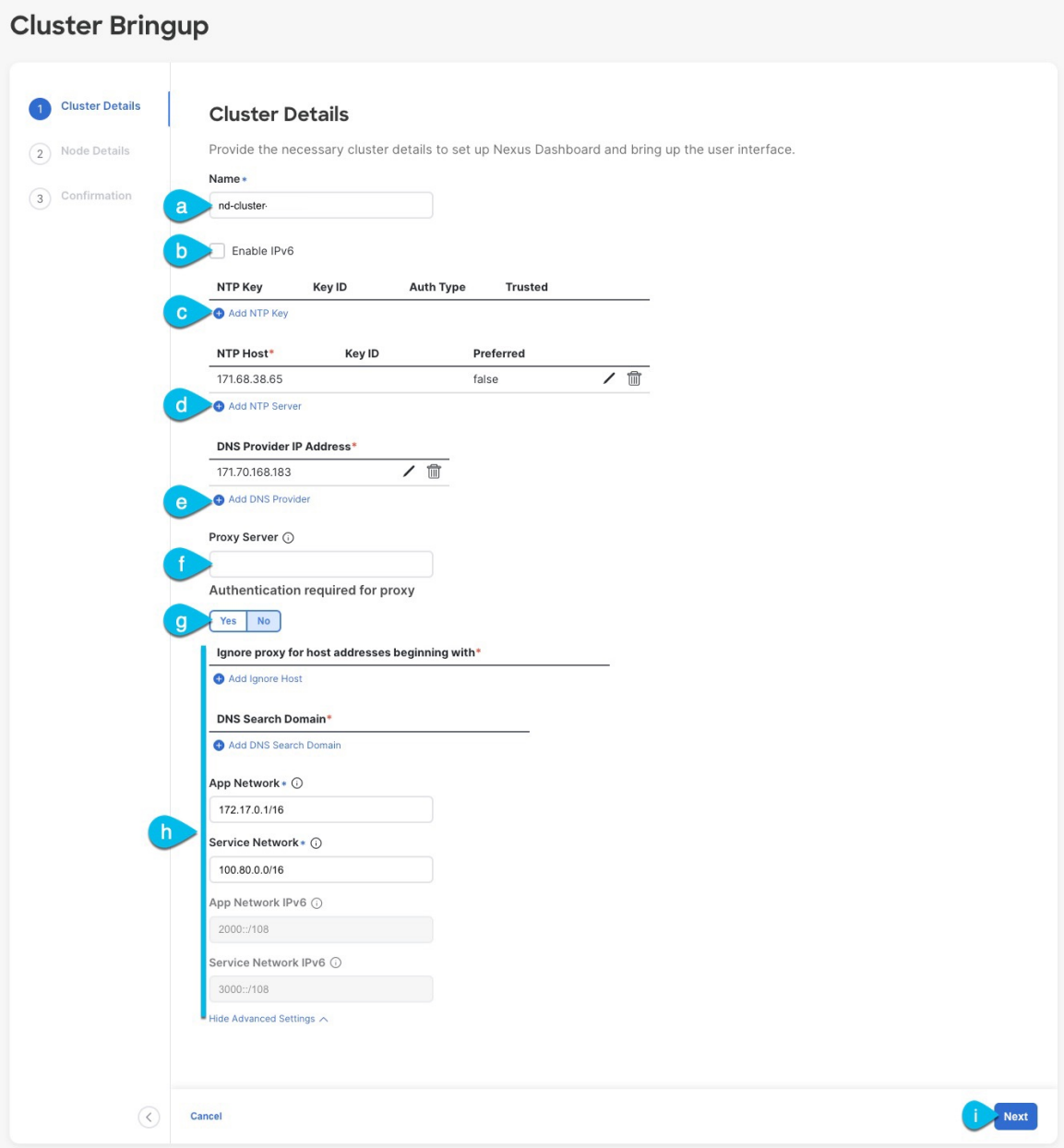
残りの設定ワークフローは、最初のノードの GUI から実行します。他の 2 つのノードに直接ログインまたは設定する必要はありません。

最初のノードに指定したパスワードを入力し、**[ログイン（Login）]** をクリックします。



ステップ 12 **[クラスタの詳細（Cluster Details）]** を入力します。

[クラスタ起動（Cluster Bringup）] ウィザードの **[クラスタの詳細（Cluster Details）]** 画面で、次の情報を入力します。



a) Nexus ダッシュボード クラスタの **[クラスタ名（Cluster Name）]** を入力します。

クラスタ名は、 RFC-1123 の要件に従う必要があります。

b) （オプション）クラスタの IPv6 機能を有効にする場合は、**[IPv6 を有効にする（Enable IPv6）]** チェックボックスをオンにします。

c) （オプション）NTP サーバー認証を有効にする場合は、**[NTP キーの追加（Add NTP Key）]** をクリックします。

次のフィールドで、以下の情報を提供します。

- **NTP キー**：Nexus ダッシュボードと NTP サーバ間の NTP トラフィックを認証するために使用される暗号キー。次の手順で NTP サーバーを定義します。複数の NTP サーバで同じ NTP キーを使用できます。
- **キー ID**：各 NTP キーに一意のキー ID を割り当てる必要があります。この ID は、NTP パケットの検証時に使用する適切なキーを識別するために使用されます。
- **認証タイプ**：このリリースでは、`MD5`、`SHA`、および `AES128CMAC` 認証タイプがサポートされています。
- このキーが**信頼**できるかどうかを選択します。信頼できないキーはNTP認証に使用できません。

（注）
NTP 認証の要件とガイドラインの完全なリストについては、前提条件とガイドライン を参照してください。

情報を入力した後、チェックマーク アイコンをクリックして保存します。

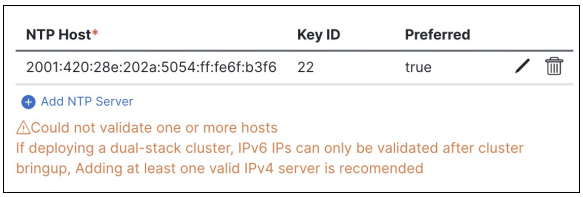
d) **[+ NTP ホストの追加（+Add NTP Host）]** をクリックして、1 つ以上の NTP サーバを追加します。

次のフィールドで、以下の情報を提供します。

- **NTP ホスト**：IP アドレスを指定する必要があります。完全修飾ドメイン名（FQDN）はサポートされていません。
- **キー ID**：このサーバーの NTP 認証を有効にする場合は、前の手順で定義した NTP キーのキー ID を指定します。
- この NTP サーバーを **[優先（Preferred）]** にするかどうかを選択します。

情報を入力した後、チェックマーク アイコンをクリックして保存します。

（注）
ログインしているノードに IPv4 アドレスのみが設定されているが、前の手順で [IPv6 を有効にする（Enable IPv6）] をオンにして NTP サーバーの IPv6 アドレスを指定した場合は、次の検証エラーが表示されます。



これは、ノードに IPv6 アドレスがまだなく（次の手順で指定します）、NTP サーバーの IPv6 アドレスに接続できないためです。

この場合、次の手順の説明に従って他の必要な情報の入力を完了し、**[次へ（Next）]** をクリックして次の画面に進み、ノードの IPv6 アドレスを入力します。

追加の NTP サーバーを指定する場合は、**[+NTP ホストの追加（+Add NTP Host）]** を再度クリックし、このサブステップを繰り返します。

e) **[+DNS プロバイダの追加（+Add DNS Provider）]** をクリックして、1 つ以上の DNS サーバを追加します。

情報を入力した後、チェックマーク アイコンをクリックして保存します。

f) **[プロキシ サーバ（Proxy Server）]** を指定します。

Cisco Cloud に直接接続できないクラスタの場合は、接続を確立するためにプロキシ サーバを構成することをお勧めします。これにより、ファブリック内の非適合ハードウェアおよびソフトウェアにさらされるリスクを軽減できます。

プロキシ サーバーでは、次の URL が有効になっている必要があります。

```
dcappcenter.cisco.com
svc.intersight.com
svc.ucs-connect.com
svc-static1.intersight.com
svc-static1.ucs-connect.com
```

プロキシ構成をスキップする場合は、フィールドの横にある情報 **(i)** アイコンにマウスを置いてから、**[スキップ（Skip）]** をクリックします。

g) (オプション) プロキシ サーバで認証が必要な場合は、**[プロキシに必要な認証（Authentication required for Proxy）]** を [はい（Yes）] に変更し、ログイン資格情報を指定します。

h) (オプション) **[詳細設定（Advanced Settings）]** カテゴリを展開し、必要に応じて設定を変更します。

詳細設定では、次の設定を行うことができます。

- **[+DNS 検索ドメインを追加（+Add DNS Search Domain）]** をクリックして、1 つ以上の検索ドメインを指定します。

  情報を入力した後、チェックマーク アイコンをクリックして保存します。

- カスタム **App Network** と **Service Network** を提供します。

  アプリケーション オーバーレイ ネットワークは、Nexus ダッシュボードで実行されるアプリケーションのサービスで使用されるアドレス空間を定義します。このフィールドには、デフォルトの 172.17.0.1/16 値が事前に入力されています。

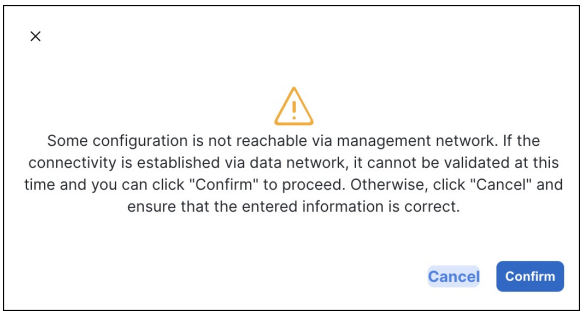
  サービス ネットワークは、Nexus ダッシュボードとそのプロセスで使用される内部ネットワークです。このフィールドには、デフォルトの 100.80.0.0/16 値が事前に入力されています。

  以前に **[IPv6 を有効にする（Enable IPv6）]** オプションをオンにした場合は、アプリケーション ネットワークとサービス ネットワークの IPv6 サブネットを定義することもできます。

  アプリケーションおよびサービスネットワークについては、このドキュメントの前の 前提条件とガイドライン の項で説明します。

i) [**次へ（Next）**] をクリックして続行します。

（注）
ノードに IPv4 管理アドレスしかないが、**[IPv6 を有効にする（Enabled IPv6）]** をオンにして IPv6 NTP サーバーアドレスを指定した場合は、NTP アドレスが正しいことを確認し、**[確認（Confirm）]** をクリックして次の画面に進み、ノードの IPv6 アドレスを指定します。



ステップ 13 **[ノードの詳細（Node Details）]** 画面で、ノードの情報を入力します。

a) 最初のノードの横にある **[編集（Edit）]**ボタンをクリックします。

b) ノードの**名前**を入力します。

管理ネットワークと**データ ネットワーク**の情報は、クラスタを展開する前に構成した VPC サブネットから既に入力されています。

クラスタは、指定された VPC CIDR から 6 つのサブネットを作成し、そこからデータと管理ネットワークがクラスタの 3 つのノードに割り当てられます。

c) IPv6 アドレスと VLAN フィールドは空白のままにします。

Cloud Nexus ダッシュボード クラスタは、これらのオプションをサポートしていません。

d) **[Save]**をクリックして、変更内容を保存します。

ステップ 14 **[ノードの追加（Add Node）]** をクリックして、クラスタに 2 番目のノードを追加します。

[ノードの詳細（Node Details）] ウィンドウが開きます。

a) ノードの**名前**を入力します。

b) **[資格情報（Credentials）]** セクションで、ノードの**パブリック IP アドレス**とテンプレートの展開時に指定したパスワードを入力し、**[検証（Verify）]** をクリックします。

IP アドレスとパスワードは、そのノードの**管理ネットワーク**と**データ ネットワーク**情報を取得するために使用され、下のフィールドに入力されます。

c) **[保存 (Save)]**をクリックして、変更内容を保存します。

ステップ 15 前の手順を繰り返して、3番目のノードを追加します。

ステップ 16 **[ノードの詳細（Node Details）]** ページで、**[次へ（Next）]** をクリックして続行します。

ステップ 17 [**確認（Confirmation）**] 画面で設定情報を確認し、[**構成（Configure）**] をクリックしてクラスタを作成します。

ノードのブート ストラップとクラスタの起動中に、全体的な進捗状況と各ノードの個々の進捗状況がUIに表示されます。ブートストラップの進行状況が表示されない場合は、ブラウザでページを手動で更新し、ステータスを更新してください。

クラスタが形成され、すべてのサービスが開始されるまでに最大30分かかる場合があります。クラスタの設定が完了すると、ページが Nexus ダッシュボード GUI にリロードされます。

ステップ 18 クラスタが健全であることを検証します。

クラスタが形成され、すべてのサービスが開始されるまでに最大 30 分かかる場合があります。

3 つすべてのノードの準備ができたら、ノード展開中に指定した `rescue-user` を使用して、SSH を介して任意の 1 つのノードにログインし、次のコマンドを実行してクラスタの状態を確認できます。

a) クラスタが稼働していることを確認します。

任意のノードにログインし、`acs health` コマンドを実行することで、クラスタ展開の現在のステータスを確認できます。

クラスタが収束している間、次の出力が表示されることがあります。

```
$ acs health
k8s install is in-progress
```

```
$ acs health
k8s services not in desired state - [...]
```

```
$ acs health
k8s: Etcd cluster is not ready
```

クラスタが稼働している場合は、次の出力が表示されます。

```
$ acs health
All components are healthy
```

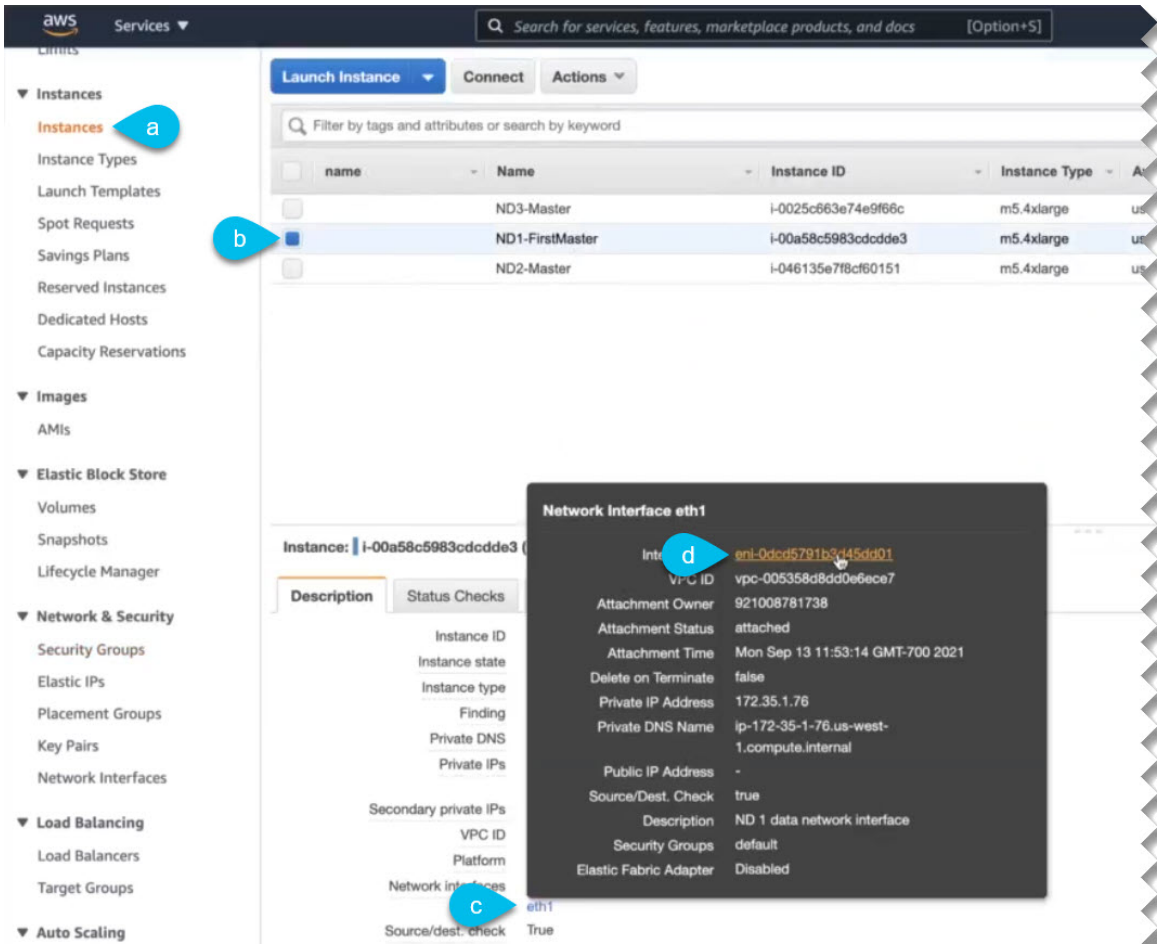
b) Nexus ダッシュボード GUI にログインします。

クラスタが使用可能になったら、ノードの管理 IP アドレスのいずれかを参照してアクセスできます。管理者ユーザのデフォルト パスワードは、Nexus ダッシュボード クラスタの最初のノードに選択した レスキュー ユーザ パスワードと同じです。

ステップ 19 必要なポートでノードのセキュリティ グループを更新します。

この手順では、Cisco NDFC サイトのオンボーディングに必要なポート設定で Nexus ダッシュボード ノードのインスタンスを更新する方法について説明します。Nexus ダッシュボード クラスタへの NDFC サイトのオンボーディングを計画していない場合は、この手順をスキップできます。

いずれかのノードのデータ インターフェイスに移動します。



a) AWS コンソールで、**[インスタンス（Instances）]** に移動します。

b) Nexus ダッシュボード インスタンスの 1 つを選択します。

デフォルトのセキュリティ グループに変更を加えるため、ノードの 1 つを選択するだけで済みます。

c) データ インターフェイスをクリックします（`eth1`）。

d) **[インターフェイス ID（Interface ID）]** をクリックします。

[ネットワークインターフェイス（Network Interface）] ページが開きます。

e) **[ネットワーク インターフェイス（Network Interface）]** ページで、インターフェイスの [セキュリティ グループ（`Security groups`）] 列の **[デフォルト（default）]** をクリックします。

新しいルールを追加します。

a) デフォルトのセキュリティ グループのページで、**[インバウンド ルール（Inbound rules）]** タブを選択します。

b) **[インバウンド ルールの編集（Edit Inbound Rules）]** をクリックします。

c) **[インバウンド ルールの編集（Edit inbound rules）]** ページで、**[ルールの追加（Add rule）]** をクリックして新しいインバウンド セキュリティ ルールを追加し、ポート 443 でのインバウンド通信を許可するための詳細を指定します。

新しいルールについて、次の情報を提供します。

- **[タイプ（Type）]** で、[カスタム TCP（Custom TCP）] を選択します。
- **[ポート範囲（Port range）]** に 443 を入力します。
- **[ソース（Source）]** には、Nexus ダッシュボードにオンボードする予定の NDFC コントローラの IP アドレスを指定します。

d) 引き続き **[インバウンド ルールの編集（Edit inbound rules）]** ページで、**[ルールの追加（Add rule）]** をクリックして別のインバウンド セキュリティ ルールを追加し、ポート 9092 でのインバウンド通信を許可するための詳細を指定します。

新しいルールについて、次の情報を提供します。

- **[タイプ（Type）]** で、[カスタム TCP（Custom TCP）] を選択します。
- **[ポート範囲（Port range）]** には、9092 と入力します。
- **[ソース（Source）]** には、Nexus ダッシュボードにオンボードする予定の NDFC コントローラの IP アドレスを指定します。

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。