# Microsoft Azure での展開



# 前提条件とガイドライン

Microsoft Azure で Nexus ダッシュボード クラスタを展開する前に、次の作業を行う必要があります。

- ファクターから Azure 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。

- 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。
- Azure アカウントとサブスクリプションに適切なアクセス権限を持っている。
- Nexus ダッシュボード クラスタ リソースのリソース グループを作成しました。

（注） リソース グループは空である必要があり、既存のオブジェクトが含まれていない必要があります。既存のオブジェクトを持つリソース グループは、Nexus ダッシュボードの展開には使用できません。

リソース グループを作成するには:

- Azureポータルで、**[すべてのリソース（All Resources）]**>**[リソース グループ（Resource Groups）]** に移動します。

- 新しいメディア リソース グループを作成するには、**[+追加（+Add）]** をクリックします。
- **[リソース グループの作成（Create a resource group）]** 画面で、Nexus ダッシュボード クラスタに使用するサブスクリプションの名前、リソースグループの名前（`nd-cluster` など）、およびリージョンを入力します。

- SSH キー ペアを生成します。

  キー ペアは秘密キーと公開キーで構成され、Nexus ダッシュボード ノードを作成するときに、公開キーを入力するように求められます。

（注） クラスタの展開手順中に一般的な SSH ログインを有効にするには、各ノードへの 1 回限りのログイン用の公開キーを作成するのと同じマシンを使用する必要があります。

SSH キーの作成については、以下の Linux または MacOS での SSH キー ペアの生成 （2 ページ） および Windows での SSH キー ペアの生成 （3 ページ） セクションで説明します。

# Linux または MacOS での SSH キー ペアの生成

次の手順では、Linux または MacOS で SSH 公開キーと秘密キーのペアを生成する方法について説明します。Windows で SSH 公開キーと秘密キーのペアを生成する手順については、を参照してください。Windows での SSH キー ペアの生成 （3 ページ）

**ステップ 1** Linux 仮想マシンまたは Mac で、ssh-keygen を使用して公開キーと秘密キーのペアを作成し、出力をファイルに送信します。

```
# ssh-keygen -f filename
```

次に例を示します。

```
# ssh-keygen -f azure_key
```

次のような出力が表示されます。パスフレーズを入力するように求められたら、テキストを入力せずに Enter キーを押します（パスフレーズがないようにフィールドを空のままにします）。

```
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in azure_key.
Your public key has been saved in azure_key.pub.
The key fingerprint is:
SHA256:gTsQIIAadjgNsgcguifIloh4XGpVWMdcXVV6U0dyBNs
...
```

**ステップ 2** 保存した公開キーファイルと秘密キーファイルを見つけます。

```
# ls
```

2 つのファイルが表示されます。

- 拡張子が .pub のファイルには、公開キー情報が含まれています。
- 同じ名前でサフィックスのないファイルに秘密キー情報が含まれている

たとえば、出力を azure_key という名前のファイルに送信すると、次の出力が表示されます。

```
# ls
azure_key
azure_key.pub
```

その場合、次のようになります。

- azure_key.pub ファイルには、公開キー情報が含まれています。
- azure_key ファイルには秘密キー情報が含まれています。

**ステップ 3** 公開キーファイルを開き、そのファイルから公開キー情報をコピーします。末尾にusername @ hostname情報は含めません。

（注） 秘密キーファイルは、インストールプロセスでは使用されません。ただし、SSH を介して Nexus ダッシュボード ノードにログインするなど、その他の理由で必要になる場合があります。

# Windows での SSH キー ペアの生成

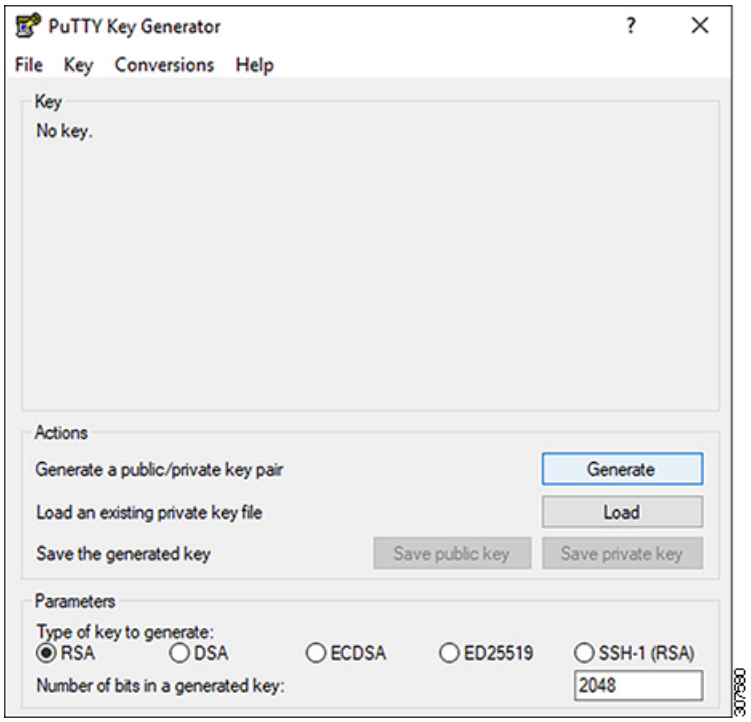
次の手順では、WindowsでSSH公開キーと秘密キーのペアを生成する方法について説明します。LinuxでSSH公開キーと秘密キーのペアを生成する手順については、を参照してください。Linux または MacOS での SSH キー ペアの生成 （2 ページ）

**ステップ 1** PuTTYキージェネレータ（puttygen）をダウンロードしてインストールします。

https://www.puttygen.com/download-putty

**ステップ 2** **Windows > の[スタート] メニュー > [すべてのプログラム] > [PuTTY] > [PuTTYgen]に移動して、PuTTY キージェネレータを実行します。**

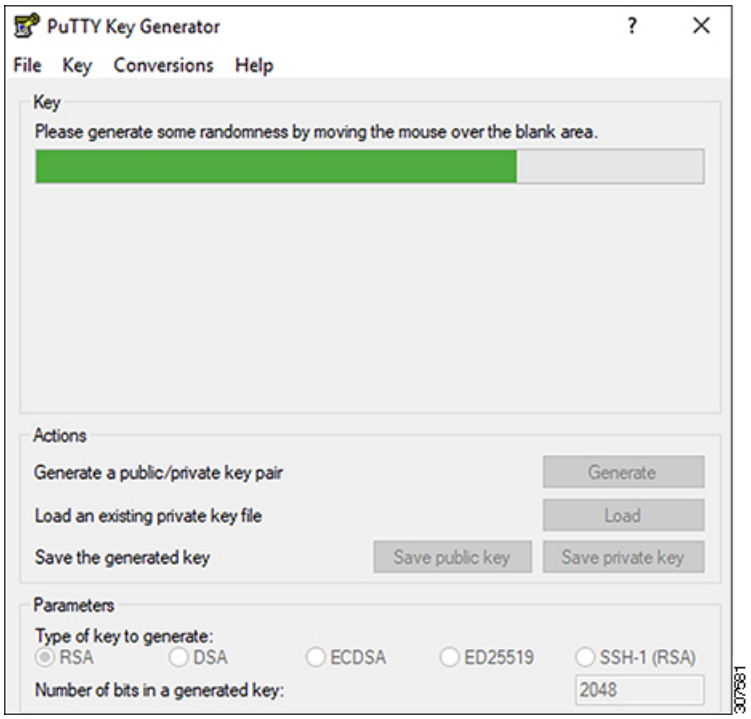
画面にPuTTYキージェネレータのウィンドウが表示されます。




**ステップ 3** **[生成（Generate）]** をクリックします。

公開キーを生成するために空白領域にマウスを移動するように求める画面が表示されます。

**ステップ 4** 空白領域の周囲にカーソルを移動して、公開キーのランダムな文字を生成します。



**ステップ 5** 公開キーを保存します。

a) 公開キーファイルを保存するラップトップ上のフォルダに移動し、この公開キーのテキストファイルを作成します。

b) PuTTYキージェネレータの情報をコピーします。

次の内容を含めて、ウィンドウに公開キー情報をコピーします。

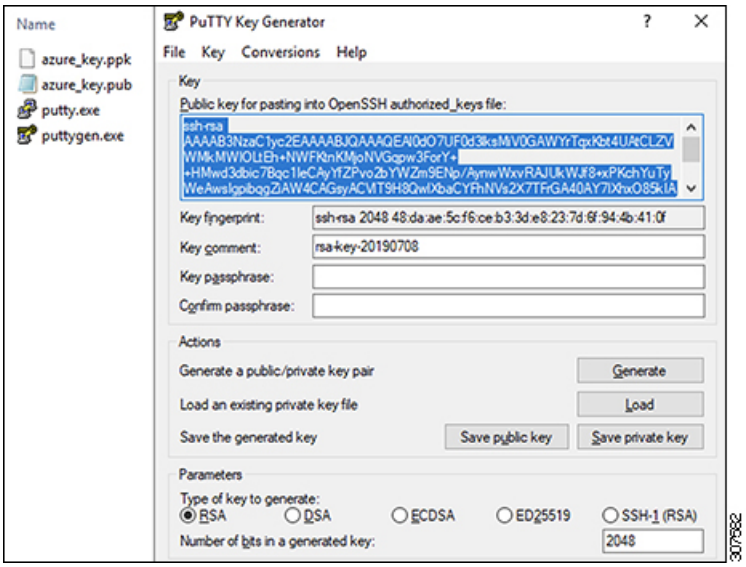
- 公開キーの先頭にssh-rsaテキストを含める。
- 末尾の次のテキスト文字列を除外します。

```
== rsa-key-<date-stamp>
```

== rsa-key-を含まないようにキーを切り捨てます。<date-stamp>末尾のテキスト文字列。

（注） 次の一連の手順では、公開キー情報をAzure ARMテンプレートに貼り付けます。フォームがこの形式のキーを受け入れない場合は、キーの末尾に==を追加します。一部の地域ではこの形式が必要になるためです。

キーが正しい形式でない場合、Nexus ダッシュボードはインストールを完了しません。




c) で作成した公開キーテキストファイルに情報を貼り付け、ファイルを保存して、一意のファイル名を付けます。5.a （5 ページ）

この公開キーテキストファイルには、1行のテキストのキーが含まれています。次の一連の手順では、この公開キーテキストファイルの情報が必要になります。

（注） PuTTYキージェネレータの[公開キーの保存（Save public key）]オプションを使用して公開キーを保存しないでください。これにより、複数行のテキストを含む形式でキーが保存されます。これは、Nexus ダッシュボード展開プロセスと互換性がありません。

**ステップ 6** 秘密キーを保存します。

a) **[プライベート キーの保存（Save private key）]** をクリックします。

パスフレーズなしでファイルを保存するかどうかを確認する画面が表示されます。この画面で **[はい（Yes）]** をクリックします。

b) ラップトップのフォルダに移動し、一意のファイル名を付けて秘密キーファイルを保存します。

（注） 秘密キーファイルは、インストールプロセスでは使用されません。ただし、SSH を介して Nexus ダッシュボード ノードにログインするなど、その他の理由で必要になる場合があります。

# Azure での Nexus ダッシュボードの展開

このセクションでは、Microsoft Azure 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。

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

a) Azure アカウントにログインし、https://azuremarketplace.microsoft.com に移動します

b) 検索フィールドに「`Cisco Nexus ダッシュボード`」と入力し、表示されるオプションを選択します。

[Nexus ダッシュボードの Azure Marketplace] ページにリダイレクトされます。

c) **[今すぐ取得（Get it now）]** をクリックします。

d) **[プランを選択（Select a plan）]** ドロップダウンで、バージョンを選択し、**[作成（Create）]** をクリックします。

**ステップ 2** **基本**情報を提供します。

a) **[サブスクリプション（Subscription）]** ドロップダウンから、これに使用するサブスクリプションを選択します。

b) **[リソース グループ（Resource group）]** ドロップダウンから、このために作成したリソース グループを 前提条件とガイドライン （1 ページ） の一部として選択します。

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。

d) **[パスワード (Password)]** および **[パスワードの確認 (Confirm Password)]** フィールドにノードの管理パスワードを入力します。

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。

e) **[SSH 公共キー（SSH public key）]**フィールドに、前提条件とガイドライン （1 ページ） セクションの一部として生成したキーペアの公開キーを貼り付けます。

f) **[次へ (Next)]** をクリックして、次の画面に進みます。

**ステップ 3** **ND 設定**情報を提供します。

a) **クラスタ名** を指定します。

b) **[イメージ バージョン（Image Version）]** ドロップダウンで、正しいバージョンが選択されていることを確認します。

c) **[仮想ネットワーク名（Virtual Network Name）]** フィールドに、クラスタ用に作成される VNET の名前を指定します。

VNET はまだ存在していてはならず、展開時に作成されます。既存の VNET を指定すると、展開を続行できません。

d) **[サブネット アドレス プレフィックス（Subnet Address Prefix）]** フィールドで、VNET 内のサブネットを指定します。

サブネットは `/24` サブネットである必要があり、VNET の作成時に定義したデフォルトの VNET サブネットとは異なる必要があります。

e) **[外部サブネット（External Subnets）]** 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。

f) **[次へ (Next)]** をクリックして、次の画面に進みます。

**ステップ 4** **[確認 + 作成（Review + create）]**ページで情報を確認し、**[作成（Create）]** をクリックします。

**ステップ 5** 展開が完了するのを待ってから、VM を起動します。

**ステップ 6** 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。

すべてのインスタンスが展開されたら、Azure コンソールに移動し、各 VM を選択して、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。

また、どちらが「最初の」ノードであるかに注意してください。これは、ノードの VM 名 `vm-node1-<cluster-name>` によって示されます。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。

**ステップ 7** 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、キーベースの SSH 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) `rescue-user` としてノードの 1 つに SSH でログインします。

（注） 前提条件とガイドライン （1 ページ） セクションで展開用の公開キーを作成するために使用したのと同じマシンを使用する必要があります。

テンプレートの基本設定で指定したパスワードを使用して、**rescue-user** としてログインできます。

```
# ssh 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。

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

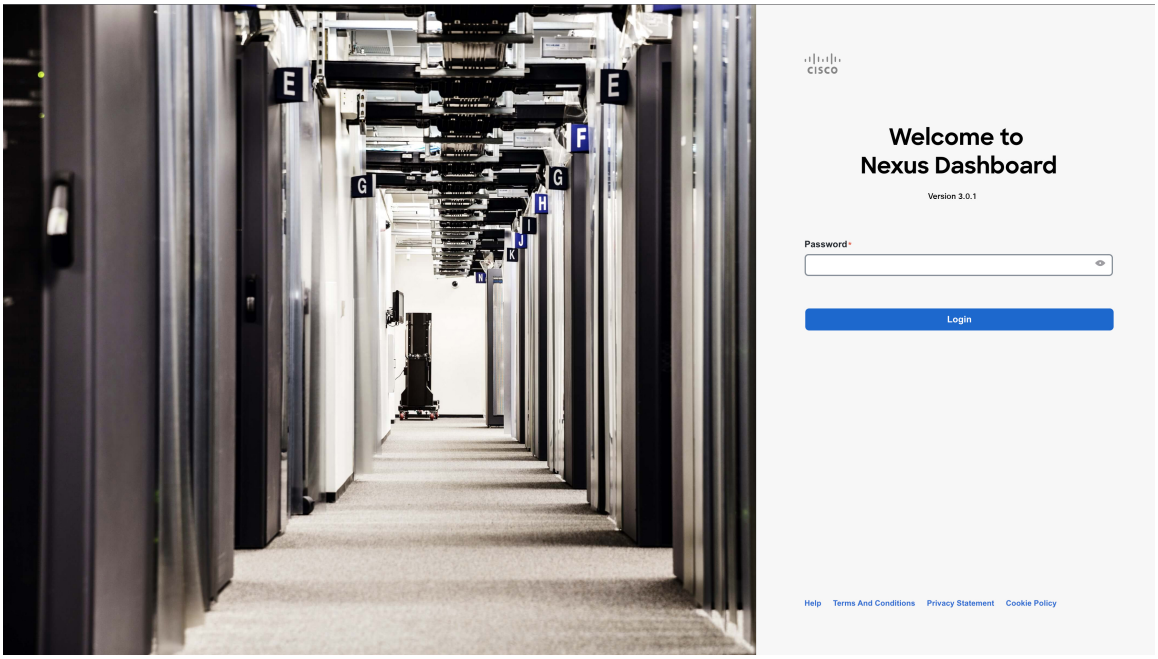
c) 他の 2 つのノードについて、この手順を繰り返します。

**ステップ 8** 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（vm-**node1**-*<cluster-name>*）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、クラスタ設定を完了できません。

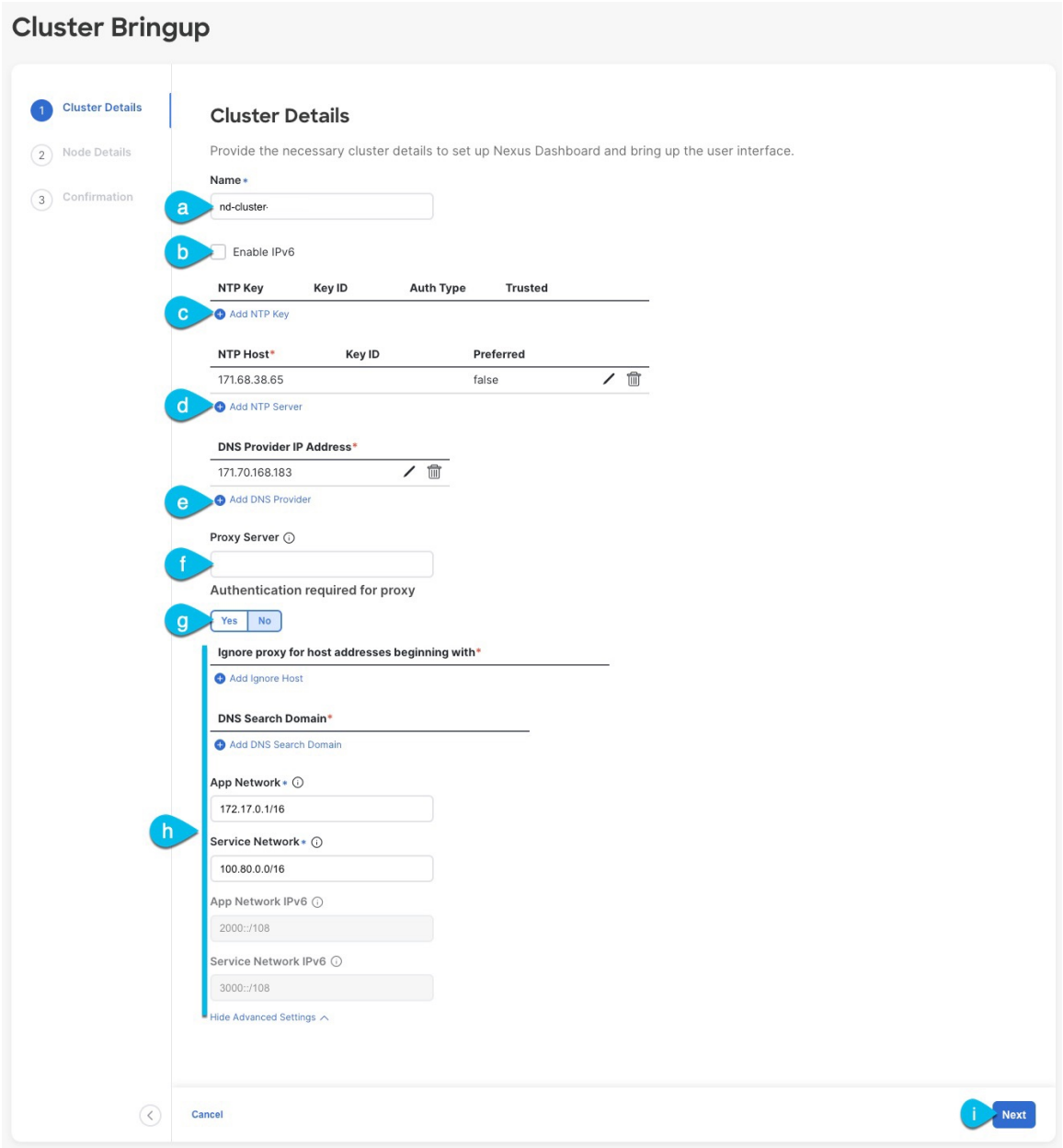
残りの設定ワークフローは、最初のノードの GUI から実行します。他の 2 つのノードに直接ログインまたは設定する必要はありません。

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 9** **[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。

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 Dashboard と NTP サーバー間の 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 サーバーで同じ 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。

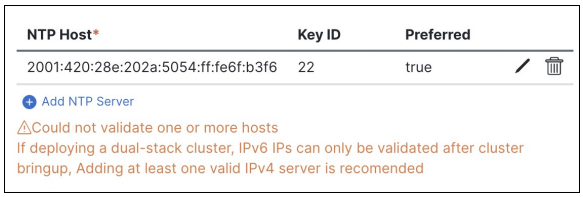
d) **[+ NTP ホストの追加（+Add NTP Host）]** をクリックして、1 つ以上の NTP サーバを追加します。

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 アドレスのみが構成されているが、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 サーバー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。

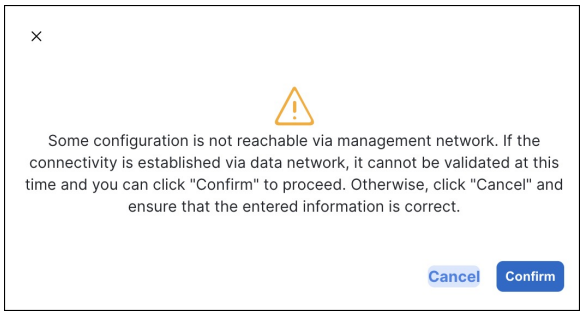
  サービス ネットワークは、Nexus ダッシュボードとそのプロセスで使用される内部ネットワークです。このフィールドには、デフォルトの `100.80.0.0/16` 値が事前に入力されています。

  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 10** **[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VNET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 VNET 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 11** **[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 12** 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 13** **[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 14** [**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 15** 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。

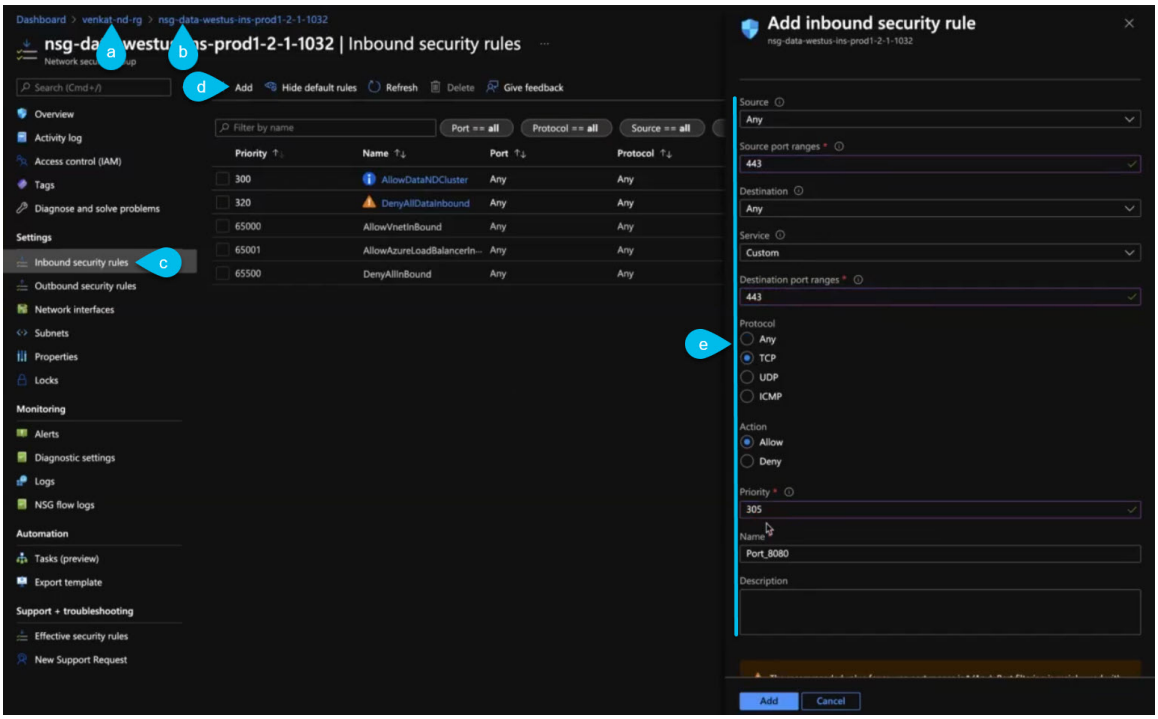
```
$ acs health
All components are healthy
```

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 16** 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。




a) Azure ポータルで、Nexus ダッシュボードを展開したリソース グループに移動します。

これは、手順 2 で選択したのと同じリソース グループです。

b) ノードのデータ インターフェイスにアタッチされているセキュリティ グループを選択します。

セキュリティ グループの名前は `nsg-data-<region>-...` で始まります。。

c) セキュリティ グループの設定ナビゲーション バーで、**[受信セキュリティ ルール（Inbound security rules）]** を選択します。

d) **[+ 追加（+Add）]** 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。

- **[送信元（Source）]** で、`[任意（Any）]` を選択します。
- **[送信元ポート範囲（Source port ranges）]** には、`443` と入力します。
- **[宛先（Destination）]** で、`[任意（Any）]` を選択します。
- **[宛先ポート範囲（Destination port ranges）]** に、`443` と入力します。
- **[プロトコル（Protocol）]** には、`[TCP]` を選択します。
- **[アクション（Action）]** で、`[許可（Allow）]` を選択します。
- **[優先度（Priority）]** で、`300` ～ `320` の優先度を選択します。

  たとえば、`305` です。
- ルールの**名前**を指定します。

e) **[+ 追加（+Add）]** 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 9092 でのインバウンド通信を許可する詳細を指定します。

前のサブステップを繰り返して、次の詳細を含む別のルールを追加します。

- **[送信元（Source）]** で、[任意（Any）] を選択します。
- **[送信元ポート範囲（Source port ranges）]** には、9092 と入力します。
- **[宛先（Destination）]** で、[任意（Any）] を選択します。
- **[宛先ポート範囲（Destination port ranges）]** に、9092 と入力します。
- **[プロトコル（Protocol）]** には、[TCP] を選択します。
- **[アクション（Action）]** で、[許可（Allow）] を選択します。
- **[優先度（Priority）]** で、300 ～ 320 の優先度を選択します。

  例えば、310。
- ルールの**名前**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。