



Cisco Catalyst Center 3.1.x on ESXi

Cisco Catalyst Center
Updated March 18, 2026



© 2023–2025 Cisco Systems, Inc. All rights reserved.

短縮されたシスコの商標

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)

第 1 章 : ESXi での Catalyst Center のスタートアップガイド	6
Catalyst Center on ESXi	7
展開の要件	7
Catalyst Center on ESXi パッケージ	9
展開の前提条件	10
VMware vSphere のインストール	10
エンタープライズ インターフェイスの予約	10
IdenTrust 証明書チェーンのインポート	11
DNS、NTP、およびプロキシサーバーの設定	11
必要なインターネット URL と完全修飾ドメイン名	12
ストレージ入出力制御の有効化	16
HA アドミッションコントロールの設定	16
クイック スタート ワークフローの準備	16
第 2 章 : Catalyst Center on ESXi のセットアップ	18
仮想アプライアンス	19
仮想マシンの作成	19
追加のネットワークアダプタの設定	21
Catalyst Center on ESXi 仮想アプライアンスの設定	22
Maglev 構成ウィザード（デフォルトモード）を使用した仮想アプライアンスの設定	22
Maglev 構成ウィザード（詳細モード）を使用した仮想アプライアンスの設定	27
インストール構成ウィザードを使用した仮想アプライアンスの設定	33
詳細インストール構成ウィザードを使用した仮想アプライアンスの設定	38
インタラクティブ CC VA ランチャを使用した仮想アプライアンスの設定	43
CC VA ランチャのサイレントモードを使用した仮想アプライアンスの設定	48
クイック スタート ワークフローの完了	56
エアギャップ展開の有効化	61
第 3 章 : 展開後の変更	62
展開後の設定	63
VM の再起動優先順位の有効化	63
リカバリサイトにおける VM 予約の設定	63
リカバリサイトにおける VM リソースプールの予約	64
第 4 章 : Catalyst Center on ESXi のアップグレード	66
Catalyst Center 3.1.6 on ESXi へのアップグレード	67
エアギャップ展開における Catalyst Center 3.1.6 on ESXi へのアップグレード	67

第

1 ESXi Catalyst Center

章

:

- [Catalyst Center on ESXi](#)
- [□□□□□](#)
- [Catalyst Center on ESXi □□□□□](#)
- [□□□□□□□](#)

Catalyst Center on ESXi

Catalyst Center on ESXi 展開モデルとそのメリット（迅速な仮想展開など）について説明します。

Catalyst Center on ESXi は、以下が特徴の展開モデルです。

- ・ 仮想形式で Catalyst Center のすべての機能を利用できる
- ・ 既存のネットワーク環境に Catalyst Center を迅速に展開できる
- ・ 物理アプライアンスを購入せずに Catalyst Center を評価できる

この展開ガイドでは、以下に関する情報を提供します。

- ・ Catalyst Center on ESXi 仮想アプライアンスを展開するための要件。
- ・ VMware ESXi ホストで仮想マシンを作成する方法、仮想アプライアンスを設定する方法、クイックスタート ワークフローを実行する方法、Catalyst Center on ESXi を使用する前に必要な展開後タスクを完了する方法。

正常に展開するためのベストプラクティス、VM の最小要件、スケール番号、およびその他の要件の概要を説明します。

Catalyst Center on ESXi 仮想アプライアンスを正常に展開するには、次の要件を満たす必要があります。VMware vSphere の最も重要な側面に関するパフォーマンスのヒントを参照してください。

- ・ VMware vSphere Client 7.0 : 『[Performance Best Practices for VMware vSphere 7.0](#)』 (PDF)
- ・ VMware vSphere Client 8.0 : 『[Performance Best Practices for VMware vSphere 8.0](#)』 (PDF)

1:

機能	説明
仮想化プラットフォームおよびハイパーバイザ	VMware vSphere (ESXi および vCenter Server を含む) 7.0.x 以降とすべてのパッチ。
プロセッサ	インテル Xeon スケーラブルプロセッサ (Cascade Lake 以降) または AMD EPYC Gen2 (2.1 GHz 以上のクロック速度)。 64 GHz が予約された 32 の vCPU を VM 専用にする必要があります。
Memory	256 GB が予約された 256 GB の DRAM を VM 専用にする必要があります。
ストレージ	3 TB のソリッドステートドライブ (SSD)。 仮想アプライアンスのバックアップを作成する場合は、追加のデータストア領域を予約してください。詳細については、『 Cisco Catalyst Center Administrator Guide 』の「Backup Server Requirements」を参照してください。
I/O 帯域幅	180 MB/秒
IOPS (1 秒当たりの入出力処理) レート	2,000 ~ 2,500 (5 ミリ秒未満の I/O 完了遅延)。

機能	説明
遅延	Catalyst Center on ESXi からネットワークデバイス接続まで : 200 ミリ秒。

注意

Catalyst Center VM のリソース割り当てまたは予約を変更すると、VM の運用に悪影響を及ぼし、失敗する可能性があります。

Catalyst Center on ESXi がサポートするデバイスおよびサイト要素の数は次のとおりです。

2 :

ネットワークコンポーネント	サポートされる最大数
アクセスポイント	4000
デバイス	1000
エンドポイント	25,000
サイト要素	2500

3 :

ネットワークコンポーネント	サポートされる最大数
エンドポイント	25,000
デバイス	2000
アクセスポイント	3000
サイト要素	2500
ファブリック単位のサイト規模	
ファブリックノード	500
VN	64
IP プール	100

ファブリックおよび非ファブリック展開の場合、ネットワーク管理者が Catalyst Center on ESXi にログインするために最大 10 の同時ユーザー接続がサポートされています。

Cisco Catalyst Assurance は、ほぼリアルタイムのストリーミング分析を使用してデータを処理します。このため、リソースの可用性に関する追加の保証が必要です。Catalyst Center on ESXi を最大規模に近い状態で運用する場合、この機能は、ホストリソースのオーバーサブスクリプションや、リソース使用率の急増を引き起こすエッジのユースケースなど、制御不能な外部イベントの影響を受ける可能性があります。パフォーマンスの低下、データ処理のギャップ、高い I/O 遅延、通常よりも高い CPU 準備率といったさまざまな状況によって、これらのイベントの発生が示される可能性があります。

 注

パフォーマンスに関する問題のトラブルシューティングの詳細については、ご使用のバージョンの VMware vSphere に対応する「[Troubleshoot and Enhance Performance](#)」のトピックを参照してください。

- VMware vSphere Client 7.0 の場合は、[ここ](#)をクリックしてください。
- VMware vSphere Client 8.0 の場合は、[ここ](#)をクリックしてください。

Catalyst Center VA

CCVA ランチャを使用して仮想アプライアンスを展開および設定する場合は、アプリケーションを実行するマシンが次の要件を満たしている必要があります。

機能	説明
RAM	1 GB
ストレージ	• 仮想アプライアンスの OVA ファイル用に 40 GB • ランチャバンドル用に 50 MB
サポートされるオペレーティング システム	• Linux : Ubuntu 20.04 以降 • macOS (Intel および M1) : macOS 14 以降 • Microsoft Windows : Windows 10 以降
スリープ設定	マシンがスリープ状態にならないように設定します。

さらに、次のパターンもあります。

- CCVA ランチャを実行するユーザーが、仮想アプライアンスの OVA ファイルを展開し、アプライアンスの仮想マシン設定を変更するために必要な権限を持っていることを確認します。
- アプリケーションを実行するシステムの HTTP/ネットワークプロキシ設定を指定します（該当する場合）。
- Mozilla Firefox バージョン 65 以降
- Google Chrome バージョン 72 以降

Catalyst Center on ESXi

Catalyst Center on ESXi で使用されるパッケージが一覧表示されている [Cisco Catalyst Center Release Notes](#) にリダイレクトします。

仮想アプライアンスで使用されるパッケージのリストについては、『[Cisco Catalyst Center Release Notes](#)』の「[Package versions in Catalyst Center](#)」を参照してください。

展開を開始する前に完了しておく準備作業について説明します。

Catalyst Center on ESXi 仮想アプライアンスを展開するには、次のタスクを完了します。

- [VMware vSphere のインストール](#) (10ページ)
- [エンタープライズ インターフェイスの予約](#) (10ページ)
- [IdenTrust 証明書チェーンのインポート](#) (11ページ)
- [DNS、NTP、およびプロキシサーバーの設定](#) (11ページ)
- [必要なインターネット URL と完全修飾ドメイン名](#) (12ページ)
- [ストレージ入出力制御の有効化](#) (16ページ)
- [HA アドミッションコントロールの設定](#) (16ページ)
- [クイック スタート ワークフローの準備](#) (16ページ)

VMware vSphere

このページでは、VMware vSphere のインストールおよび設定プロセスの概要を説明します。

VMware vSphere には複数のコンポーネントが含まれています。

Catalyst Center on ESXi を実行する場合は、VMware vSphere 7.0.x 以降（すべてのパッチを含む）を使用してください。VMware vSphere のインストールおよび設定プロセスの概要については、「[VMware のインストールおよびセットアップ](#)」を参照してください。

VMware vSphere をインストールしたら、仮想アプライアンスの OVA ファイルの展開に使用するコンピューターから到達できることを確認します。

仮想アプライアンスで使用するためにエンタープライズ インターフェイスを予約する必要があることを示します。

エンタープライズ インターフェイスの予約は、以下に該当するネットワーク設定要件です。

- 仮想アプライアンスのインターフェイスをエンタープライズ ネットワーク接続専用にする
- 後でアプライアンスの設定時に使用するために、割り当てられた IP アドレスを記録する必要がある
- アプライアンス管理用の管理インターフェイスおよび追加のネットワークインターフェイスをサポートしている場合がある

仮想アプライアンスをセットアップする前に、以下を実行します。

- エンタープライズ ネットワーク接続用に少なくとも 1 つの 1 Gbps または 10 Gbps のエンタープライズ インターフェイスを予約します。
- このインターフェイスの IP アドレスをメモします。後でアプライアンスの設定時にこのアドレスを入力します。
- （任意）Catalyst Center on ESXi GUI アクセス用に 1 つの 1 Gbps または 10 Gbps 管理インターフェイスを予約します。後日設定する場合は、インターフェイスの IP アドレスをメモします。

以下の点に注意してください。

- ・ クラスタ内インターフェイスの IP アドレスは事前に定義されています。デフォルトモードが選択された状態で **Magenv** 構成ウィザードを完了する場合、またはブラウザベースのインストール構成ウィザードを完了する場合、IP アドレスを入力する必要はありません。
- ・ **Catalyst Center on ESXi** は、仮想アプライアンスで使用する 1 つの追加インターフェイスの設定をサポートしています。設定する場合は、**[アダプタタイプ (Adapter Type)]** ドロップダウンリストから **[VMXNET]** を選択してください。他のタイプを選択すると、アプライアンスの設定が正常に完了しません。詳細については、『*vSphere Virtual Machine Administration*』の「[Add a Network Adapter to a Virtual Machine](#)」のトピックを参照してください。

IdenTrust

このタスクトピックでは、IdenTrust 証明書チェーンをインポートする手順について説明します。

Catalyst Center on ESXi OVA ファイルは **IdenTrust CA** 証明書で署名されています。この証明書は、デフォルトの **VMware** トラストストアには含まれていません。

証明書が無効な場合、**[Deploy OVF Template]** ウィザードの **[Review details]** ページに警告が表示されます。この問題を解決するために、OVA ファイルを展開するホストまたはクラスタに **IdenTrust** 証明書チェーンをインポートできます。

1. 仮想アプライアンスを配置する **VMware ESXi** ホストまたはクラスタで、**trustidevcodesigning5-3.1.6-VA.tar.gz** を、**Catalyst Center on ESXi OVA** ファイルと同じ場所からダウンロードします。
2. ダウンロードしたファイルをローカルディレクトリに展開します。
3. **vSphere Web** クライアントにログインします。
4. **[Administration] > [Certificates] > [Certificate Management]** を選択します。
5. **[Trusted Root Certificates]** フィールドで、**[Add]** をクリックします。
6. **[Add Trusted Root Certificate]** ダイアログボックスで、**[Browse]** をクリックします。
7. ステップ 1 でダウンロードしたファイルを抽出し、**trustidevcodesigning5.pem** ファイルを選択します。**[開く (Open)]** ボタンをクリックします。
8. **[Start Root certificate push to vCenter Hosts]** チェックボックスをオンにして、**[Add]** をクリックします。

証明書チェーンが正常にインポートされたことを確認するメッセージが表示されます。

[Deploy OVF Template] ウィザードを完了すると、**[Review details]** ページの **[Publisher]** フィールドに、信頼できる証明書を使用していることが示されます。

DNS NTP

仮想アプライアンスが使用する **DNS**、**NTP** およびプロキシサーバーを準備する方法について説明します。

仮想アプライアンスの設定時には、仮想アプライアンスが使用する **DNS** サーバー、**NTP** サーバー、およびプロキシサーバーを準備する必要があります。

次の 3 項目を指定するように求められます。

- ・ **Catalyst Center on ESXi** がドメイン名を IP アドレスに変換するために使用するドメインネームシステム (DNS) サーバー。
- ・ **Catalyst Center on ESXi** がクロックの同期に使用する **Network Time Protocol (NTP)** サーバー。

- （任意）Catalyst Center on ESXi がインターネット宛ての URL にアクセスするために使用するプロキシサーバー。

仮想アプライアンスを設定する前に、次の手順を実行します。

- 使用するサーバーが使用可能であり、動作中であることを確認します。
- NTPサーバーの場合は、その IP アドレスまたはホスト名を取得します。プロキシサーバーの場合は、URL またはホスト名とそのログイン情報を収集します。

URL

インターネットアドレス Catalyst Center がアクセスできないリスト。

仮想アプライアンスを機能させるには、必要な URL および完全修飾ドメイン名（FQDN）へのセキュアなアクセスを提供する必要があります。

この表では、各 URL と FQDN を使用する機能について説明します。IP トラフィックがアプライアンスとこれらのリソースとの間を移動できるように、ネットワーク ファイアウォールまたはプロキシサーバーのいずれかを設定する必要があります。

注意

リストされた URL および FQDN へのアクセスを提供しない場合、関連する機能は想定どおりに動作しません。

注

サードパーティベンダーの宛先ドメイン名は予告なしに変更される場合があるため、ワイルドカードを使用して指定する必要があります。

プロキシアクセス要件の詳細については、『[Cisco Catalyst Center Third-Generation Installation Guide](#)』の「Provide secure access to the internet」を参照してください。

4: URL FQDN

目的	...Catalyst Center がアクセスする必要がある URL と FQDN
システムソフトウェアとアプリケーションパッケージにアップデートをダウンロードし、製品チームにユーザーフィードバックを送信します。	推奨 : https://*.ciscoconnectdna.com/¹ ワイルドカードを回避するには、代わりに次の URL を指定します。 • https://www.ciscoconnectdna.com • https://catalogsvc-cdn.ciscoconnectdna.com • https://catalogsvc-reg.ciscoconnectdna.com • https://catalogsvc-reg-cdn.ciscoconnectdna.com • https://catalogsvc-cm.ciscoconnectdna.com • https://app-cdn.ciscoconnectdna.com
製品チームにユーザーフィードバックを送信します。	https://dnacenter.uservoice.com
スマートアカウントおよび SWIM ソフトウェアのダウンロード	• https://apx.cisco.com • https://cloudsso.cisco.com/as/token.oauth2 • https://*.cisco.com/ • https://download-ssc.cisco.com/
クラウドドメインで認証します。	https://dnaservices.cisco.com
ThousandEyes と統合します。	• app.thousandeyes.com この URL では AWS が使用されており、*.awsglobalaccelerator.com にマッピングされている可能性があります。AWS を使用する可能性のある他のサービスも AWS ドメインにマッピングできます。 • api.thousandeyes.com
API 呼び出しを許可して、Cisco CX Cloud Success Tracks へのアクセスを有効にします。そうしないと、Machine Reasoning Engine (MRE) がサポートする Security Advisories、Bug Identifier、および EOX 機能の拡張構成ベースのスキャンに追加された拡張機能が期待どおりに動作しません。	https://api-cx.cisco.com
Webex と統合します。	• http://analytics.webexapis.com • https://webexapis.com

¹ シスコは ciscoconnectdna.com とそのサブドメインを所有し、維持しています。Cisco Connect DNA インフラストラクチャは、シスコの Security and Trust ガイドラインに準拠しています。セキュリティに関して継続的にテストされています。このインフラストラクチャは、ロードバランスおよび自動化機能が組み込まれた堅牢なインフラストラクチャです。クラウド運用チームがインフラストラクチャをモニターして維持することで、継続的な可用性を確保します。

目的	...Catalyst Center がアクセスする必要がある URL と FQDN
ユーザフィードバック	https://dnacenter.uservoice.com
Cisco Catalyst Cloud およびホストされているアプリケーションとの接続 (AppX MS Teams 統合、Talos 統合など)。	*.cisco.com : 443 それ以外の場合の特定の FQDN は次のとおりです。 ▪ neoffers.cisco.com ▪ neoffers-de.cisco.com ▪ neoffers-sg.cisco.com ▪ dnaservices.cisco.com
Cisco Meraki と統合します。	推奨 : *.meraki.com:443 ワイルドカードを回避したいお客様は、代わりに次の URL を指定できます。 ▪ dashboard.meraki.com:443 ▪ api.meraki.com:443 ▪ n63.meraki.com : 443
OCSP/CRL を使用した SSL/TLS 証明書の失効ステータスを確認します。	▪ http://validation.identrust.com ▪ http://commercial.ocsp.identrust.com
Catalyst Center リモートサポート機能が有効になっている場合、シスコの認定スペシャリストがトラブルシューティングデータを収集できるようにします。	

 注

これらの URL は、直接でも **Catalyst Center** で構成されているプロキシサーバー経由でも到達できるようにする必要があります。

wss://prod.radkit-cloud.cisco.com:443

目的	...Catalyst Center がアクセスする必要がある URL と FQDN
cisco.com とシスコ スマート ライセンス と統合します。	*.cisco.com : 443 ワイルドカードを回避するには、代わりに次の URL を指定します。 - software.cisco.com - cloudsso.cisco.com - cloudsso1.cisco.com - cloudsso2.cisco.com - apiconsole.cisco.com - api.cisco.com - apx.cisco.com - smartreceiver.cisco.com - sso.cisco.com - apmx-prod1-vip.cisco.com - apmx-prod2-vip.cisco.com - tools.cisco.com - tools1.cisco.com - tools2.cisco.com
Network-Based Application Recognition (NBAR) に接続します。	prod.sdavc-cloud-api.com:443
不正なベンダー名を検出するには、不正管理アプリケーションを有効にします。	https://standards-oui.ieee.org/
サイトとロケーションマップで正確な情報をレンダリングします。	- www.mapbox.com *.tiles.mapbox.com/*: 443 プロキシの場合、宛先は *.tiles.mapbox.com/* です。
Cisco AI Network Analytics のデータ収集では、クラウドホストへのアウトバウンド HTTPS (TCP 443) アクセスを許可するようにネットワークまたは HTTP プロキシを設定します。	https://api.use1.prn.kairos.ciscolabs.com (米国東部リージョン) https://api.euc1.prn.kairos.ciscolabs.com (欧州中央リージョン)
GUIから特定のタスクを完了できる対話型ヘルプフローのメニューにアクセスします。	https://ec.walkme.com
ライセンスサービスにアクセスします。	https://swapi.cisco.com
Cisco Spaces と統合します。	https://dnaspaces.io https://dnaspaces.eu https://ciscospaces.sg

仮想アプライアンスを展開する予定のデータストアについては、次の手順を実行して、ネットワークで入出力 (I/O) の輻輳が発生しているときに、アプライアンスの仮想マシンの I/O が他の仮想マシンよりも優先されるようにします。

1. vSphere Client で、仮想アプライアンスを展開する予定のデータストアに移動して、そのデータストアをクリックします。
2. [Configure] タブをクリックし、[General] をクリックします。
3. [Datastore Capabilities] エリアで、[Edit] をクリックします。
4. [Configure Storage I/O Control] ウィンドウで、次の手順を実行します。
 - a) [Enable Storage I/O Control and statistics collection] オプションボタンをクリックします。
 - b) [Storage I/O congestion threshold] エリアで、使用する輻輳しきい値を設定します。
ピークスループットの割合 (%) を指定するか、値 (ミリ秒単位) を入力できます。
 - c) (任意) [Statistic Collection] エリアで、[Include I/O statistics for SDRS] チェックボックスをオンにします。
5. [OK] をクリックします。

HA

Catalyst Center on ESXi VM を接続して 3 ノードクラスタを作成することはできません。高可用性 (HA) を有効にするには、VMware vSphere で HA 機能を使用します。厳格なアドミッションコントロールを有効にして、以下の状態にあることを確認します。

- ・ アクションが可用性の制約に違反する場合、システムは仮想マシンの電源をオンにしない。
- ・ システムで、設定されたフェールオーバー キャパシティ制限が適用されている。
- ・ HA がフェールオーバー時に予期どおりに動作する。

クイック スタート ワークフローを完了する前に実行する必要があるタスクについて説明します。

ESXi ホストで仮想マシンを作成し、Catalyst Center on ESXi 仮想アプライアンスを設定すると、クイック スタート ワークフローを完了するように求められます。このワークフローを完了すると、Catalyst Center on ESXi が管理するデバイスが検出されます。また、それらのデバイスからのテレメトリの収集も有効になります。ワークフローを完了するには、次のタスクを実行します。

- ・ 作成する新しい管理者ユーザーのユーザー名とパスワードを決定します。デフォルトの管理者ユーザー名とパスワード (admin/P@ssword9) は、Catalyst Center on ESXi への初回ログイン時にのみ使用してください。

重要

このパスワードの変更は、特に Catalyst Center on ESXi 仮想アプライアンスをセットアップするユーザーがその管理者となるユーザーと異なる場合に、ネットワークセキュリティにとって重要です。

- ・ Cisco.com へのログインに使用するログイン情報を取得します。

- システムにアクセスする必要があるユーザーを特定します。これらのユーザーについて、そのロール、一意のパスワード、および権限設定を定義します。

仮想アプライアンスで **IPAM** サーバーと **Cisco Identity Services Engine (ISE)** を使用するオプションがあります。これらのいずれかまたは両方を使用する場合は、関連する **URL** とログイン情報も取得する必要があります。

第

2 Catalyst Center on ESXi

章

:

- [Cisco Catalyst Center on ESXi のインストール](#)
- [Cisco Catalyst Center on ESXi のアップグレード](#)
- [Cisco Catalyst Center on ESXi のデプロイ](#)
- [Cisco Catalyst Center on ESXi の管理](#)
- [Cisco Catalyst Center on ESXi のトラブルシューティング](#)
- [Cisco Catalyst Center on ESXi のベストプラクティス](#)

Catalyst Center on ESXi 仮想アプライアンスを展開する方法について、順を追って説明します。

Catalyst Center on ESXi 仮想アプライアンスをセットアップするには、次のタスクを完了します。

1. 仮想マシンを作成します。
2. 仮想アプライアンスを設定します。
3. クイック スタート ワークフローを完了します。

Cisco Catalyst 仮想アプライアンスランチャ（CCVA ランチャ）を使用して仮想アプライアンスをセットアップする場合は、まず、次のいずれかのトピックで説明されている手順を実行します。

- ・ インタラクティブ CC VA ランチャを使用した仮想アプライアンスの設定（43ページ）
- ・ CC VA ランチャのサイレントモードを使用した仮想アプライアンスの設定（48ページ）

次に、クイック スタート ワークフローを完了します。

VMware ESXi ホストに OVA テンプレートを展開する手順（リソースの割り当てやストレージのセットアップなど）について説明します。

仮想アプライアンスが存在する VMware ESXi ホストまたはクラスタで仮想マシンを作成するには、次の手順を実行します。

-
1. シスコが指定する場所から Catalyst Center on ESXi OVA ファイルをダウンロードします。
 2. vSphere Web クライアントにログインします。
 3. ナビゲーションペインで、OVA ファイルを展開するホストまたはクラスタの IP アドレスを右クリックし、[Deploy OVF Template] をクリックします。
 4. [Deploy OVF Template] ウィザードを完了します。
 - a) [Select an OVF Template] ウィザードページで、展開に使用する OVA ファイルを指定し、[Next] をクリックします。次のいずれかの操作を実行できます。
 - ・ [URL] オプションボタンをクリックし、適切なパスおよび OVA ファイル名を入力します。このオプションを選択する場合は、OVA ファイルが Web アクセス可能な場所に保存され、その場所から共有されていることを確認してください。
 - ・ [Local file] オプションボタンをクリックして、[Upload Files] をクリックし、適切な OVA ファイルに移動して、それを選択します。

ウィザードの [Select a name and folder] ページが開きます。デフォルトでは、OVA のファイル名は、作成しようとしている仮想マシンの名前として設定されます。また、手順 3 で選択した ESXi ホストまたはクラスタが存在する場所が、展開場所として設定されます。

- b) デフォルト値を使用する場合は、[Next] をクリックし、手順 4c に進みます。

異なる値を使用する場合は、次の手順を実行します。

1. 作成する仮想マシンの名前を入力します。
2. 仮想マシンが常駐する場所を指定します。

3. **[Next]** をクリックします。

ウィザードの **[Select a compute resource]** ページが開きます。

c) OVA ファイルを展開する ESXi ホストまたはクラスター（手順 3 で右クリックしたもの）をクリックし、**[Next]** をクリックします。

展開テンプレートの詳細が一覧表示されたページが表示されます。

d) テンプレートの詳細を確認し、次のいずれかのタスクを実行します。

- ・ 変更を加える必要がある場合は、必要に応じて **[Back]** をクリックして適切なウィザードページに戻ります。
- ・ 続行する場合は、**[Next]** をクリックします。

注

[Extra configuration] フィールドに表示される情報は無視してください。これは、シスコが **Catalyst Center on ESXi** の OVA ファイルで提供する追加の設定を指します。

ウィザードの **[Select storage]** ページが開きます。

e) ストレージの設定：

1. 使用するストレージデバイスのオプションボタンをクリックします。
2. **[Select virtual disk format]** フィールドで、**[Thick Provision]** または **[Thin Provision]** オプションを選択します。
3. **[Next]** をクリックします。

ウィザードの **[Select networks]** ページが開きます。

f) エンタープライズ ネットワークの宛先ネットワークを設定します。

1. エンタープライズ ネットワークの **[宛先ネットワーク (Destination Network)]** ドロップダウンリストで、**Catalyst Center on ESXi** のエンタープライズ インターフェイスに接続するネットワークを選択します。
2. **[Next]** をクリックします。

入力した展開設定の概要が、**[Ready to complete]** ウィザードページに表示されます。

g) 設定を確認したら、次のいずれかのタスクを実行します。

- ・ 変更を加える必要がある場合は、必要に応じて **[Back]** をクリックして適切なウィザードページに戻ります。
- ・ 展開を続行する場合は、**[Finish]** をクリックします。

重要

通常、展開が完了するまでに約 45 分かかります。vSphere Client の [Recent Tasks] タブで進捗状況をモニターできます。

仮想マシンにセカンダリ ネットワーク インターフェイスを追加して、そのネットワーク設定を行う手順について説明します。

仮想アプライアンスに追加のネットワークアダプタを設定するには、次の手順を実行します。

注

管理インターフェイスはアダプタ上に配置されます。

1. vSphere Web クライアントにログインします。
2. ナビゲーションウィンドウで、作成した仮想マシンを右クリックし、[Power] > [Power Off] を選択します。
3. 仮想マシンを右クリックして、[Actions] > [Edit Settings] を選択します。
4. [仮想ハードウェア (Virtual Hardware)] タブを選択します。[デバイスの新規追加 (Add New Device)] をクリックし、[ネットワークアダプタ (Network Adapter)] を選択します。
5. [新規ネットワーク (New Network)] フィールドのドロップダウンリストで、[ブラウズ (Browse)] をクリックします。
6. [ネットワークの選択 (Select Network)] ダイアログボックスで、仮想アプライアンスの管理インターフェイスに接続するネットワークを選択し、[OK] をクリックします。
7. [Adapter Type] フィールドのドロップダウンリストから、[VMXNET3] を選択し、[OK] をクリックします。
8. ナビゲーションウィンドウで、仮想マシンを右クリックし、[Power] > [Power On] を選択します。
9. 次のいずれか 1 つのタスクを実行します。
 - ・ まだ設定していない場合は、使用可能ないずれかの設定ウィザードまたは CC VA ランチャーを使用して [仮想アプライアンスを設定](#) します。
 - ・ 仮想アプライアンスをすでに設定している場合は、次のステップに進みます。
10. Catalyst Center on ESXi が表示されたら、設定ウィザードを実行して管理インターフェイスの設定を行います。
 - a) 仮想マシンのターミナルウィンドウを開きます。 **sudo maglev-config update** コマンドを実行します。
 構成ウィザードが開き、アプライアンスのエンタープライズインターフェイスにすでに設定されている設定が表示されます。
 - b) [next>>] をクリックします。

ウィザードに、アプライアンスのクラスタ内インターフェイスにすでに設定されている設定が表示されます。

- c) [next>>] をクリックします。
- d) 作成した管理インターフェイス（**NETWORK ADAPTER 3**）について、次のパラメータに必要な値を入力し、[next>>] をクリックします。
 - ・ [Host IPv4/IPv6 Address] フィールド：管理インターフェイスの IP アドレスを入力します。
 - ・ [IPv4 Netmask/IPv6 Prefix Length] フィールド：インターフェイスの IP アドレスのネットマスクを入力します。
 - ・ [Default Gateway IPv4/IPv6 Address] フィールド：インターフェイスに使用するデフォルトゲートウェイの IP アドレスを入力します。
 - ・ [IPv4/IPv6 Static Routes] フィールド：1 つ以上のスタティックルートを次の形式で入力し、スペースで区切ります。 <network>/<netmask>/<gateway>。

Catalyst Center on ESXi

仮想アプライアンスを設定するためのさまざまな方法（**Maglev** 構成ウィザードや **CC VA** ランチャを使用してネットワークとシステムの設定を確立する方法など）について説明します。

VMware ESXi ホスト上の **Catalyst Center on ESXi** 仮想アプライアンスを設定する手順を 1 つ選択します。

- ・ [Maglev 構成ウィザード（デフォルトモード）を使用した仮想アプライアンスの設定（22ページ）](#)
- ・ [Maglev 構成ウィザード（詳細モード）を使用した仮想アプライアンスの設定（27ページ）](#)
- ・ [インストール構成ウィザードを使用した仮想アプライアンスの設定（33ページ）](#)
- ・ [詳細インストール構成ウィザードを使用した仮想アプライアンスの設定（38ページ）](#)
- ・ [インタラクティブ **CC VA** ランチャを使用した仮想アプライアンスの設定（43ページ）](#)
- ・ [CC VA ランチャのサイレントモードを使用した仮想アプライアンスの設定（48ページ）](#)

Maglev

Maglev 構成ウィザードとプリセット設定を使用して仮想アプライアンスをすばやく設定するには、次の手順を実行します。

注

このウィザードを使用する場合、クラスタ内インターフェイスは事前設定されています。このインターフェイスのデフォルト設定を使用しない場合は、[Maglev 構成ウィザード（詳細モードを選択）](#)を完了する必要があります。

この手順を開始する前に、仮想アプライアンスに関する次の情報を収集します。

- ・ スタティック IP アドレス

- ・ サブネット マスク
- ・ デフォルト ゲートウェイ
- ・ DNS アドレス
- ・ NTP サーバーの詳細
- ・ プロキシサーバーの詳細

重要

アプライアンスの管理インターフェイスを設定する場合は、このウィザードを開始する前に、このインターフェイス用に存在する追加のネットワークアダプタも設定します。

1. 展開が完了したら、新しい仮想マシンの電源をオンにします。

- a) vSphere Client で、仮想マシンを右クリックします。
- b) **[Power]** > **[Power On]** を選択します。

仮想マシンは通常 45 分で使用可能になります（帯域幅、RAM、ハードディスク容量、vCPU の数によって異なります）。VMware VM コンソールで進行状況をモニターすることができます。

2. 適切なリンクをクリックして、リモートコンソールまたは Web コンソールを起動します。

3. Maglev 構成ウィザードを完了することにより、仮想マシンを設定します。

- a) ウィザードの **[STATIC IP CONFIGURATION]** ページでは設定を入力する必要がないため、**[skip>>]** をクリックします。

ブラウザベースの WebUI インストールモードを使用して仮想アプライアンスを設定する場合にのみ、静的 IP 設定を入力してください。

- b) **[Create MKS]** をクリックします。
- c) **[MKS事前製造クラスタの使用を開始 (Start using MKS pre manufactured cluster)]** をクリックします。
- d) 次の表に示す **NETWORK ADAPTER #1** の設定値を入力します。**[next>>]** をクリックします。

Catalyst Center on ESXi は、このインターフェイスを使用して、仮想アプライアンスをネットワークにリンクさせます。

[Host IPv4 address] フィールド エンタープライズインターフェイスの IP アドレスを入力します。これは必須です。

[IPv4 Netmask] フィールド インターフェイスの IP アドレスに対応するネットマスクを入力します。

[Default Gateway IPv4 Address] フィールド インターフェイスに使用するデフォルトゲートウェイ IP アドレスを入力します。

重要

アプライアンスの少なくとも 1 つのインターフェイスに対してデフォルトゲートウェイ IP アドレスを入力してください。入力しないと、設定ウィザードを完了できません。

[IPv4 Static Routes] フィールド 1 つ以上のスタティックルートをスペースで区切り、<ネットワーク>/<ネットマスク>/<ゲートウェイ> の形式で入力します。これは、通常、Catalyst Center on ESXi の管理インターフェイスでのみ必要です。

[LACP Mode] フィールド 仮想アプライアンスには適用されないため、このフィールドは空白のままにします。

入力した値がウィザードによって検証され、正しくない値が含まれていた場合にはエラーメッセージが表示されます。エラーメッセージが表示された場合には、入力した値が正しいことを確認してから、再入力します。必要に応じて、[<< back] をクリックして再入力します。

- e) [Host IPv4 Address] フィールドと [IPv4 Netmask] フィールドはクラスタ内インターフェイス用に事前入力されるため、[NETWORK ADAPTER #2] の設定値を入力する必要はありません。[next>>] をクリックして進みます。
- f) 次の表に示す **NETWORK ADAPTER #3** の設定値を入力します。[next>>] をクリックします。

このインターフェイスを使用すると、仮想アプライアンスから Catalyst Center on ESXi GUI にアクセスできます。

注

このウィザードページは、管理インターフェイス用に追加のネットワークアダプタが設定済みの場合にのみ表示されます。

[Host IPv4 address] フィールド 管理インターフェイスの IP アドレスを入力します。これは、このインターフェイスを使用して管理ネットワークから Catalyst Center on ESXi GUI にアクセスする場合にのみ必要です。それ以外の場合は、空白のままにします。

[IPv4 Netmask] フィールド インターフェイスの IP アドレスに対応するネットマスクを入力します。

[Default Gateway IPv4 Address] フィールド インターフェイスに使用するデフォルトゲートウェイ IP アドレスを入力します。

重要

アプライアンスの少なくとも 1 つのインターフェイスに対してデフォルトゲートウェイ IP アドレスを入力してください。入力しないと、設定ウィザードを完了できません。

[IPv4 Static Routes] フィールド 1 つ以上のスタティックルートをスペースで区切り、<ネットワーク>/<ネットマスク>/<ゲートウェイ> の形式で入力します。

検証エラーがある場合は修正し、続行します。ウィザードがネットワークアダプタの設定を適用します。

- g) [DNS Configuration] ページで、優先 DNS サーバーの IP アドレスを入力します。[next>>] をクリックします。複数の DNS サーバを入力する場合には、リスト内の IP アドレスをスペースで区切ります。

重要

- ・ NTP の場合、Catalyst Center on ESXi と NTP サーバの間のポート 123 (UDP) が開いていることを確認します。
- ・ 最大 3 つの DNS サーバーを設定します。仮想アプライアンス 1 台に対して 4 台以上の DNS サーバーを設定すると、問題が発生する可能性があります。

ウィザードが更新され、これまでに入力した設定を検証するためにコントローラをシャットダウンする必要があることが示されます。

h) 次のいずれかの手順を選択します。

- ・ 設定を変更する必要がある場合は、必要に応じて [**<<back**] をクリックし、必要な変更を加えてから、このウィザードページに戻ります。
- ・ 入力した設定に問題がなければ、[**proceed>>**] をクリックします。

i) 検証が正常に完了したら、次のいずれかの手順を選択します。

- ・ ネットワークでプロキシサーバーを使用しないでインターネットにアクセスする場合は、[**skip proxy>>**] をクリックして続けます。
- ・ ネットワークでプロキシサーバーを使用する場合、[**NETWORK PROXY**] ウィザードページに設定値を入力します。[**next>>**] をクリックします。

[HTTPS プロキシ (HTTPS Proxy)] フィールド

インターネットにアクセスする HTTPS ネットワークプロキシの URL またはホスト名を入力します。

注

Catalyst Center on ESXi から HTTPS プロキシへの接続は、このリリースの HTTP 経由のみでサポートされます。

[HTTPS Proxy Username] フィールド

ネットワークプロキシへのアクセスに使用するユーザ名を入力します。プロキシログインが必要ない場合には、このフィールドを空白のままにします。

[HTTPS Proxy Password] フィールド

ネットワークプロキシへのアクセスに使用するパスワードを入力します。プロキシログインが必要ない場合には、このフィールドを空白のままにします。

必要な情報を入力したら、必要に応じて検証エラーを修正し、続行します。

j) 次に、[**MAGLEV CLUSTER DETAILS**] ウィザードページで仮想アプライアンスの仮想 IP アドレスを入力するように求められます。エンタープライズインターフェイスに設定されている仮想 IP アドレスを入力します。管理インターフェイスの仮想 IP アドレスを設定した場合は、そのアドレスも入力します (カンマを使用して 2 つの IP アドレスを区切ります)。

仮想アプライアンスの完全修飾ドメイン名 (FQDN) を指定することもできます。Catalyst Center on ESXi は、このドメイン名を使用して次の手順を実行します。

- このホスト名を使用して、仮想アプライアンスの **Web** インターフェイスと、**Catalyst Center on ESXi** が管理するエンタープライズネットワーク内のデバイスによって使用される **Representational State Transfer (REST) API** にアクセスします。
- Catalyst Center on ESXi** 証明書の **[Subject Alternative Name (SAN)]** フィールドで、**FQDN** を使用して、デバイスのプロビジョニングに使用されるプラグアンドプレイ サーバが定義されます。

必要な情報を入力したら、**[Next >>]** をクリックして続行します。検証エラーが表示された場合は、以前の画面で行ったように修正します。

- k) ウィザードの **[USER ACCOUNT SETTINGS]** ページで提供される設定値を入力します。**[next>>]** をクリックします。

[Linux Password] フィールド maglev ユーザーのパスワードを入力して確認します。

[Re-enter Linux Password] フィールド Linux パスワードをもう一度入力して確認します。

[Password Generation Seed] フィールド Linux パスワードを自分で作成しない場合には、このフィールドにシードフレーズを入力してから、**[パスワードの生成 (Generate password)]** を押してパスワードを生成します。

[Auto Generated Password] フィールド (オプション) シードフレーズは、ランダムで安全なパスワードの一部として表示されます。必要に応じて、このパスワードを「そのまま」使用することも、この自動生成パスワードをさらに編集することもできます。

[<Use Generated Password>] を押してパスワードを保存します。

情報を入力したら、必要に応じて検証エラーを修正し、続行します。

- l) ウィザードの **[NTP SERVER SETTINGS]** ページで提供される設定値を入力します。**[next>>]** をクリックします。

[NTP Server (NTP サーバ)] フィールド 1 つまたは複数の NTP サーバーアドレスまたはホスト名をスペースで区切って入力します。少なくとも 1 つの NTP アドレスまたはホスト名が必要です。実稼働環境への展開では、少なくとも 3 台の NTP サーバを設定することを推奨します。

[NTP Authentication] チェックボックス

Catalyst Center on ESXi と同期する前に NTP サーバーの認証を有効にするには、このチェックボックスをオンにして、次の情報を入力します。

- NTP サーバーのキー ID。有効な値の範囲は 1 ～ 4294967295 ($2^{32}-1$) です。

この値は、NTP サーバーのキーファイルで定義されているキー ID に対応します。

- NTP サーバーのキー ID に関連付けられた SHA-1 キー値。この 40 文字の 16 進文字列は、NTP サーバーのキーファイルにあります。

注

前のフィールドで構成した各 NTP サーバーのキー ID とキー値を入力してください。

情報を入力したら、必要に応じて検証エラーを修正し、続行します。

ウィザードが設定を適用できる状態になったことを示す最終メッセージが表示されます。

- m) 入力した設定を仮想アプライアンスに適用するには、[**proceed>>**] をクリックします。

設定プロセスの完了後に、仮想アプライアンスの電源を再度オンにすると、「**CONFIGURATION SUCCEEDED!**」というメッセージが表示され、**Maglev** ログインページが表示されます。

注

サービスが安定して **Catalyst Center UI** にログイン可能になるまでには 15 ～ 30 分かかります。

4. クイック スタート ワークフローの完了 (56ページ)。

Maglev

Maglev 構成ウィザードを使用して仮想アプライアンスを設定し、事前設定されたアプライアンス設定とは異なる設定を指定する必要がある場合は、次の手順を実行します。

設定を開始する前に、仮想アプライアンスに関する次の情報を収集します。

- スタティック IP アドレス
- サブネット マスク
- デフォルト ゲートウェイ
- DNS アドレス
- NTP サーバーの詳細

- ・ プロキシサーバーの詳細

重要

アプライアンスの管理インターフェイスを設定する場合は、このウィザードを開始する前に、このインターフェイス用に[追加のネットワークアダプタの設定](#)も行います。

1. 展開が完了したら、新しく作成した仮想マシンの電源をオンにします。

- a) vSphere Client で、仮想マシンを右クリックします。
- b) **[Power] > [Power On]** を選択します。

仮想マシンは通常約 45 分で使用可能になります。実際の時間は、使用可能な帯域幅、RAM、ハードディスク容量、vCPU の数によって異なります。vSphere Client の **[Recent Tasks]** タブで進捗状況をモニターできます。

2. 適切なリンクをクリックして、リモートコンソールまたは Web コンソールを起動します。

3. Maglev 構成ウィザードを完了することにより、仮想マシンを設定します。

- a) ウィザードの **[STATIC IP CONFIGURATION]** ページでは設定を入力する必要がないため、**[skip>>]** をクリックします。

ブラウザベースの Web UI を使用して仮想アプライアンスをインストールする場合にのみ、静的 IP アドレスを設定します。

- b) **[Create MKS]** をクリックします。
- c) **[Start configuration of MKS in advanced mode]** オプションをクリックします。

次のウィザードページが開き、事前設定されたすべてのアプライアンス設定（コンテナとクラスタのサブネットを除く）が消去されることが示されます。これらの設定の値を入力する必要があります。

このオプションを選択すると、デフォルトのアプライアンスセットアップワークフローには戻れません。次の手順を完了する前に、この点に留意してください。

- d) **[proceed>>]** をクリックします。

事前設定されたすべてのアプライアンス設定が消去された後、次のウィザードページが開きます。

- e) 次のいずれかまたは複数の手順を実行し、**[next>>]** をクリックします。

- ・ IPv4 または IPv6 アドレッシングを使用するかどうかを選択します。
- ・ FIPS モードを有効にする場合は、対応するオプションをクリックします。FIPS モードの詳細については、『[Cisco Catalyst Center Second-Generation Appliance Installation Guide](#)』の「FIPS Mode Support」のトピックを参照してください。

- f) **[Layer2 mode used for the services]** ウィザードページでは設定を入力する必要はないため、**[next>>]** をクリックします。

- g) 次の表に示す **NETWORK ADAPTER #1** の設定値を入力し、**[next>>]** をクリックします。

Catalyst Center on ESXi は、このインターフェイスを使用して、仮想アプライアンスをネットワークにリンクさせます。

[Host IPv4/IPv6 Address] フィールド	エンタープライズ インターフェイスの IP アドレスを入力します。これは必須です。
--	---

[IPv4 Netmask/IPv6 Prefix Length] フィールド

次のいずれかを実行します。

- **IPv4** アドレッシングを選択した場合は、ポートの **IP** アドレスのネットマスクを入力します。これは必須です。
- **IPv6** アドレッシングを選択した場合は、プレフィックス長（ビット単位）を入力します。有効な値の範囲は **10 ~ 127** です。

[Default Gateway IPv4/IPv6 Address] フィールド

インターフェイスに使用するデフォルトゲートウェイ **IP** アドレスを入力します。

重要

アプライアンスの少なくとも **1** つのインターフェイスに対してデフォルトゲートウェイ **IP** アドレスを入力してください。入力しないと、設定ウィザードを完了できません。

[IPv4/IPv6 Static Routes] フィールド

1 つ以上のスタティックルートスペースで区切り、**<ネットワーク>/<ネットマスク>/<ゲートウェイ>** の形式で入力します。これは、通常、管理インターフェイスでのみ必要です。

[Cluster Link] フィールド

このフィールドは空欄のままにします。これは、クラスタ内インターフェイスでのみ必要です。

[LACP Mode] フィールド

仮想アプライアンスには適用されないため、このフィールドは空白のままにします。

入力した値がウィザードによって検証され、正しくない値が含まれていた場合にはエラーメッセージが表示されます。エラーメッセージが表示された場合は、入力した値を確認します。[<< back] をクリックすると再入力できます。

h) 次の表に示す **NETWORK ADAPTER #2** の設定値を入力し、[next>>] をクリックします。

[Host IPv4/IPv6 Address] フィールド

クラスタ内インターフェイスの **IP** アドレスを入力します。これは必須です。クラスタ内インターフェイスのアドレスは後で変更できないことに注意してください。

[IPv4 Netmask/IPv6 Prefix Length] フィールド

次のいずれかを実行します。

- **IPv4** アドレッシングを選択した場合は、ポートの **IP** アドレスのネットマスクを入力します。これは必須です。
- **IPv6** アドレッシングを選択した場合は、プレフィックス長（ビット単位）を入力します。有効な値の範囲は **10 ~ 127** です。

[Default Gateway IPv4/IPv6 Address] フィールド

このフィールドは空欄のままにします。

[IPv4/IPv6 Static Routes] フィールド

このフィールドは空欄のままにします。

[Cluster Link] フィールド

このインターフェイスが **Catalyst Center on ESXi** クラスタへのリンクであるとして設定するには、このチェックボックスをオンにします。これは、クラスタ内インターフェイスでのみ必要です。

[LACP Mode] フィールド 仮想アプライアンスには適用されないため、このフィールドは空白のままにします。

検証エラーが表示された場合は、修正してから続行します。ネットワークアダプタの設定がウィザードによって検証され、適用されます。

- i) 次の表に示す **NETWORK ADAPTER #3** の設定値を入力し、[next>>] をクリックします。

このインターフェイスを使用して、仮想アプライアンスの **Catalyst Center on ESXi GUI** にアクセスします。

注

このウィザードページは、管理インターフェイス用に追加のネットワークアダプタをすでに設定している場合にのみ表示されます。

[Host IPv4/IPv6 Address] フィールド

管理インターフェイスの IP アドレスを入力します。これは、このインターフェイスを使用して管理ネットワークから **Catalyst Center on ESXi GUI** にアクセスする場合にのみ必要です。それ以外の場合は、空白のままにします。

[IPv4 Netmask/IPv6 Prefix Length] フィールド

IP アドレスを入力した場合は、次のいずれかを実行します。

- **IPv4** アドレッシングを選択した場合は、ポートの IP アドレスのネットマスクを入力します。これは必須です。
- **IPv6** アドレッシングを選択した場合は、プレフィックス長（ビット単位）を入力します。有効な値の範囲は 10 ~ 127 です。

[Default Gateway IPv4/IPv6 Address] フィールド

インターフェイスに使用するデフォルトゲートウェイ IP アドレスを入力します。

重要

アプライアンスの少なくとも 1 つのインターフェイスに対してデフォルトゲートウェイ IP アドレスを入力してください。入力しないと、設定ウィザードを完了できません。

[IPv4/IPv6 Static Routes] フィールド

1 つ以上のスタティックルートスペースで区切り、<ネットワーク>/<ネットマスク>/<ゲートウェイ> の形式で入力します。

[Cluster Link] フィールド

このフィールドは空欄のままにします。これは、クラスタ内インターフェイスでのみ必要です。

検証エラーがある場合は、修正して続行します。ネットワークアダプタの設定がウィザードによって検証され、適用されます。

- j) [DNS Configuration] ページで、優先 DNS サーバーの IP アドレスを入力し、[next>>] をクリックします。複数の DNS サーバを入力する場合には、リスト内の IP アドレスをスペースで区切ります。

重要

- NTP の場合、Catalyst Center on ESXi と NTP サーバの間のポート 123 (UDP) が開いていることを確認します。
- 問題を防ぐため、仮想アプライアンス 1 台に対して 3 台以下の DNS サーバーを設定してください。

ウィザードが更新され、これまでに入力した設定を検証するためにコントローラをシャットダウンする必要があることが示されます。

k) 次のいずれかを実行します。

- 設定を変更する必要がある場合は、必要に応じて [**<back**] をクリックし、必要な変更を加えてから、このウィザードページに戻ります。
- 入力した設定に問題がなければ、[**proceed>>**] をクリックします。

l) 検証が正常に完了すると、[**NETWORK PROXY**] ウィザードページが開きます。[**skip proxy>>**] をクリックして続行します。

m) [**skip proxy validation>>**] をクリックすることにより、ネットワークプロキシ設定をスキップすることを確認します。

n) 次に、[**MAGLEV CLUSTER DETAILS**] ウィザードページで仮想アプライアンスの仮想 IP アドレスを入力するように求められます。クラスタは Catalyst Center on ESXi ではサポートされていないため、このページの [**Cluster Virtual IP Address(s)**] フィールドは空白のままにできます。

仮想アプライアンスの完全修飾ドメイン名 (FQDN) を指定することもできます。Catalyst Center on ESXi は、このドメイン名を使用して次のタスクを実行します。

- 仮想アプライアンスの Web インターフェイスと、Catalyst Center on ESXi が管理するエンタープライズネットワーク内のデバイスによって使用される Representational State Transfer (REST) API にアクセスします。
- Catalyst Center on ESXi 証明書の [**Subject Alternative Name (SAN)**] フィールドで、FQDN を使用して、デバイスのプロビジョニングに使用されるプラグアンドプレイサーバーを定義します。

必要な情報を入力したら [**Next >>**] をクリックして続行します。以前の画面でしたように、検証エラーを修正します。

o) ウィザードの [**USER ACCOUNT SETTINGS**] ページで提供される設定値を入力し (次の表を参照)、[**next>>**] をクリックします。

[**Linux Password**] フィールド maglev ユーザーのパスワードを入力して確認します。

[**Re-enter Linux Password**] フィールド Linux パスワードをもう一度入力して確認します。

[**Password Generation Seed**] フィールド Linux パスワードを自分で作成しない場合には、このフィールドにシードフレーズを入力してから、[**パスワードの生成 (Generate password)**] を押してパスワードを生成します。

[**Auto Generated Password**] フィールド (オプション) シードフレーズは、ランダムで安全なパスワードの一部として表示されます。必要に応じて、このパスワードを「そのまま」使用することも、この自動生成パスワードをさらに編集することもできます。

[**<Use Generated Password**] を押してパスワードを保存します。

必要な情報を入力したら、検証エラーを修正して続行します（必要な場合）。

- p) ウィザードの [NTP SERVER SETTINGS] ページで提供される設定値を入力し（次の表を参照）、[next>>] をクリックします。

[NTP Server (NTP サーバ)] フィールド	1つまたは複数の NTP サーバアドレスまたはホスト名をスペースで区切って入力します。1つ以上の NTP アドレスまたはホスト名が必要です。実稼働環境への展開では、少なくとも 3 台の NTP サーバを設定することを推奨します。
[NTP Authentication] チェックボックス	Catalyst Center on ESXi と同期する前に NTP サーバーの認証を有効にするには、このチェックボックスをオンにして、次の情報を入力します。 - NTP サーバーのキー ID。有効な値の範囲は 1 ～ 4294967295 ($2^{32}-1$) です。 この値は、NTP サーバーのキーファイルで定義されているキー ID に対応します。 - NTP サーバーのキー ID に関連付けられた SHA-1 キー値。この 40 文字の 16 進文字列は、NTP サーバーのキーファイルにあります。

注

前のフィールドで構成した各 NTP サーバーのキー ID とキー値を入力してください。

必要な情報を入力したら、検証エラーを修正して続行します（必要な場合）。

設定を適用する準備ができると、ウィザードにメッセージが表示されます。

- q) ウィザードの [MAGLEV ADVANCED SETTINGS] ページで提供される設定値を入力し（次の表を参照）、[next>>] をクリックします。

[Container Subnet] フィールド	内部サービスを管理するために Catalyst Center on ESXi で使用する、ルーティングされない専用の IP サブネット。デフォルトでは、これは 169.254.32.0/20 にあらかじめ設定されています。このサブネットを使用することをお勧めします。別のサブネットを入力する場合は、Catalyst Center on ESXi で使用されている他の内部または外部ネットワークサブネットと競合したり、重複したりしていないことを確認してください。詳細については、『 Catalyst Center Second-Generation Appliance Installation Guide's 』の「Required IP Addresses and Subnets」のトピックにあるコンテナサブネットの説明を参照してください。
[Cluster Subnet] フィールド	内部クラスタサービスを管理するために Catalyst Center on ESXi で使用する、ルーティングされない専用の IP サブネット。デフォルトでは、これは 169.254.48.0/20 にあらかじめ設定されています。このサブネットを使用することをお勧めします。別のサブネットを入力する場合は、Catalyst Center on ESXi の内部ネットワークまたは任意の外部ネットワークで使用されている他のサブネットと競合したり、重複したりしていないことを確認してください。詳細については、『 Catalyst Center Second-Generation Appliance Installation Guide's 』の「Required IP Addresses and Subnets」のトピックにあるクラスタサブネットの説明を参照してください。

必要な情報を入力したら、検証エラーを修正して続行します（必要な場合）。

ウィザードが設定を適用できる状態になったことを示す最終メッセージが表示されます。

- r) 入力した設定を仮想アプライアンスに適用するには、**[proceed>>]** をクリックします。

設定プロセスの完了後に、仮想アプライアンスの電源を再投入すると、「**CONFIGURATION SUCCEEDED!**」というメッセージが表示されます。

仮想マシンが動作可能になるまでに約 **180～210** 分かかります。実際の時間は、使用可能な帯域幅、**RAM**、ハードディスク容量、**vCPU** の数などによって異なります。**vSphere Client** の **[Recent Tasks]** タブで進捗状況をモニターできます。

4. クイック スタート ワークフローの完了 (56ページ)。

インストール構成ウィザードを使用すると、**Catalyst Center on ESXi** 仮想アプライアンスをより簡単に設定できます。

ブラウザベースのインストール構成ウィザードを使用して仮想アプライアンスをできるだけ迅速に設定する必要があります、事前設定されたアプライアンス設定を使用しても問題ない場合は、次の手順を実行します。

重要

この手順の実行中に入力するすべての **IP** アドレスが有効な **IPv4** ネットマスクを持つ有効な **IPv4** アドレスであることを確認してください。また、アドレスと対応するサブネットが重複していないことを確認してください。重複している場合、サービスの通信に問題が発生する可能性があります。

以下の必須情報を収集します。

- スタティック **IP** アドレス
- サブネット マスク
- デフォルト ゲートウェイ
- **DNS** アドレス
- **NTP** サーバーの詳細
- プロキシサーバーの詳細

サポートされているブラウザを使用してください。[展開の要件](#) (7ページ) を参照してください。

次の手順で指定する **DNS** サーバーと **Catalyst Center on ESXi** の間のファイアウォールで **ICMP** を有効にします。このウィザードでは、ユーザの指定する **DNS** サーバを **ping** で確認します。**Catalyst Center on ESXi** と **DNS** サーバーの間のファイアウォールが **ICMP** を許可する設定になっていないと、**ping** がブロックされる可能性があります、ウィザードを正常に完了できない場合があります。

 注

このウィザードを使用する場合、クラスタ内インターフェイスは事前設定されています。このインターフェイスのデフォルト設定を使用しない場合は、[ブラウザベースの詳細インストール構成ウィザード](#)を完了する必要があります。

1. 展開が完了したら、新しく作成した仮想マシンの電源をオンにします。

- a) vSphere Web Client で、仮想マシンを右クリックします。
- b) **[Power]** > **[Power On]** を選択します。

仮想マシンは通常約 45 分で使用可能になります。この時間は、帯域幅、RAM、ハードディスク容量、および vCPU の数によって異なります。vSphere Client の **[Recent Tasks]** タブで進捗状況をモニターできます。

2. 適切なリンクを選択して、リモートコンソールまたは Web コンソールを起動します。

3. インストール構成ウィザードを表示します。

- a) **[STATIC IP CONFIGURATION]** ページで、次のいずれかのタスクを実行します。

- DHCP サーバーが IP アドレス、サブネットマスク、デフォルトゲートウェイを仮想アプライアンスのエンタープライズインターフェイスに割り当てるようにするには、**[skip>>]** をクリックします。
- 独自の IP アドレス、サブネットマスク、デフォルトゲートウェイを仮想アプライアンスのエンタープライズインターフェイスに割り当てる場合は、次の表に記載されている情報を入力し、**[Configure]** をクリックします。

 注

[IPv6 Mode] チェックボックスは、拡張モードでのみ IPv6 アドレッシングを有効にするためのものです。IPv4 展開の場合は、このチェックボックスをオフにする必要があります。

[IPv6 Mode] チェックボックス IPv6 アドレッシングを有効にする場合は、[高度なインストール設定ウィザード](#)を使用して有効にする必要があります。IPv4 アドレッシングを使用するには、このチェックボックスをオフのままにします。

[IP Address] フィールド 使用する静的 IP アドレスを入力します。

[ネットマスク (Netmask)] フィールド 前のフィールドに指定した IP アドレスのネットマスクを入力します。ネットマスクまたは CIDR アドレスのいずれかを入力できます。

[Default Gateway Address] フィールド トラフィックのルーティングに使用されるデフォルトゲートウェイを指定します。

[Static Routes] フィールド このウィザードではスタティックルートの設定ができないため、**[Static Routes]** フィールドは空欄のままにします。

[Web Installation] フィールドに表示されている URL を書き留めます。この URL は次のステップで必要になります。

- b) [Static IP Configuration] ページに表示された URL を開きます。
- c) [Start a Catalyst Center Virtual Appliance] オプションボタンをクリックし、[Next] をクリックします。
- d) [Install] オプションボタンをクリックし、[Start] をクリックします。

[Overview] スライダが開きます。[>] をクリックして、ウィザードで実行するタスクの概要を表示します。

- e) [Start Workflow] をクリックしてウィザードを起動します。

[Virtual Appliance Interfaces] ページが開きます。

4. インストール構成ウィザードを完了することにより、仮想アプライアンスを設定します。

- a) [Next] をクリックします。

[DNS Configuration] ページが開きます。

- b) [DNS] フィールドに、優先 DNS サーバーの IP アドレスを入力します。追加の DNS サーバーを入力するには、[Add] (+) アイコンをクリックします。

重要

最大 3 つの DNS サーバーを設定できます。問題を防ぐため、アプライアンス 1 台に対して 3 台以下の DNS サーバーを設定してください。

- c) [Next] をクリックします。

[Configure Proxy Server Information] ページが開きます。

- d) 次のいずれか 1 つのタスクを実行します。

- ・ ネットワークでプロキシサーバーを使用しないでインターネットにアクセスする場合は、[No] オプションボタンをクリックし、[Next] をクリックします。
- ・ ネットワークでプロキシサーバーを使用してインターネットにアクセスする場合は、この表に示す値を入力し、[Next] をクリックします。

[プロキシサーバ (Proxy Server)] フィールド	インターネットにアクセスする HTTPS ネットワークプロキシの URL またはホスト名を入力します。
---------------------------------------	---



注

Catalyst Center on ESXi から HTTPS プロキシへの接続は、このリリースの HTTP 経由のみでサポートされます。

[Port] フィールド	アプライアンスがネットワークプロキシにアクセスするために使用したポートを入力します。
--------------	--

[Username] フィールド	ネットワークプロキシへのアクセスに使用するユーザー名を入力します。プロキシログインが必要ない場合には、このフィールドを空白のままにします。
------------------	---

Password フィールド	ネットワークプロキシへのアクセスに使用するパスワードを入力します。プロキシログインが必要ない場合には、このフィールドを空白のままにします。
----------------	---

ウィザードの **[Advanced Appliance Settings]** ページが開きます。

- e) アプライアンスの構成値を入力し、**[Next]** をクリックします。

クラスタ仮想 IP アドレス

[Enterprise Network] および **[For Intracluster Access]** フィールドからアクセスする場合

エンタープライズインターフェイスに設定されている仮想 IP アドレスを入力します。管理インターフェイスの仮想 IP アドレスを設定した場合は、そのアドレスも入力します（カンマを使用して 2 つの IP アドレスを区切ります）。

[Fully Qualified Domain Name (FQDN)] フィールド

仮想アプライアンスの完全修飾ドメイン名（FQDN）を指定することもできます。**Catalyst Center on ESXi** は、このドメイン名を使用して次のタスクを実行します。

- このホスト名を使用して、仮想アプライアンスの **Web** インターフェイスと、エンタープライズネットワーク内で **Catalyst Center on ESXi** が管理するデバイスによって使用される **Representational State Transfer (REST) API** にアクセスします。
- Catalyst Center on ESXi** 証明書の **[Subject Alternative Name (SAN)]** フィールドで、FQDN を使用して、デバイスのプロビジョニングに使用されるプラグアンドプレイサーバが定義されます。

NTP サーバー設定

[NTP Server] フィールド

少なくとも 1 つの NTP サーバーアドレスまたはホスト名を入力します。追加の NTP サーバーアドレスまたはホスト名を入力するには、**[Add] (+)** アイコンをクリックします。

実稼働環境への展開では、少なくとも 3 台の NTP サーバーを設定することをお勧めします。

[Turn on NTP Authentication] チェックボックス

Catalyst Center on ESXi と同期する前に NTP サーバーの認証を有効にするには、このチェックボックスをオンにして、次の情報を入力します。

- NTP サーバーのキー ID。有効な値の範囲は 1 ～ 4294967295 ($2^{32}-1$) です。
この値は、NTP サーバーのキーファイルで定義されているキー ID に対応します。
- NTP サーバーのキー ID に関連付けられた SHA-1 キー値。この 40 文字の 16 進文字列は、NTP サーバーのキーファイルにあります。

注

前のフィールドで構成した各 NTP サーバーのキー ID とキー値を入力してください。

サブネット設定

[Container Subnet] フィールド 内部サービスを管理するために **Catalyst Center on ESXi** で使用する、ルーティングされない専用の IP サブネット。デフォルトでは、これは **169.254.32.0/20** に設定されているため、別のサブネットは入力できません。

[Cluster Subnet] フィールド 内部クラスタサービスを管理するために **Catalyst Center on ESXi** で使用する、ルーティングされない専用の IP サブネット。デフォルトでは、これは **169.254.48.0/20** に設定されているため、別のサブネットは入力できません。

[Enter CLI Password] ページが開きます。

- f) maglev ユーザーのパスワードを入力して確認した後、**[Next]** をクリックします。

これは、仮想アプライアンスの設定後に初めて **Catalyst Center on ESXi** にログインするときに使用するパスワードです。ログインすると、（セキュリティ対策として）新しい管理者ユーザーを設定するように求められます。「[クイックスタートワークフローの完了（56ページ）](#)」を参照してください。

入力した情報がウィザードで検証され、ウィザードの操作を続行する前に変更の必要な設定があれば、通知されます。入力した設定が有効な場合、ウィザードの **[Summary]** ページが開きます。



注

アプライアンスの設定を **JSON** ファイルとしてダウンロードするには、対応するリンクをクリックします。

- g) 画面の下部までスクロールし、ウィザードの完了時に入力したすべての設定を確認します。設定を更新するには、関連する **[Edit]** リンクをクリックします。
- h) **Catalyst Center on ESXi** 仮想アプライアンスの設定を完了するには、**[Start Configuration]** をクリックします。

プロセス中もウィザード画面が継続的に更新され、実行中のタスクとその進行状況、エラーが表示されます。この情報のローカルコピーをテキストファイルとして保存するには、**[Download]** アイコンをクリックします。

5. アプライアンスの設定が完了したら、コピーアイコンをクリックして、デフォルトの管理者スーパーユーザーパスワードをコピーします。

重要

インストール構成ウィザードを完了すると、**Catalyst Center on ESXi** はこのパスワードを自動的に設定します。続行する前に、必ずコピーアイコンをクリックしてください。クリックしないと、**Catalyst Center on ESXi** への最初のログインができません。

 注

セキュリティ対策として、ログイン後にこのパスワードを変更するよう求められます。詳細については、[クイック スタート ワークフローの完了](#) (56ページ) を参照してください。

このガイドでは、詳細インストール構成ウィザードを使用して仮想アプライアンスを設定する方法について説明します。

ブラウザベースの詳細インストール構成ウィザードを使用して仮想アプライアンスを設定し、事前設定されたアプライアンス設定とは異なる設定にする場合は、次の手順を実行します。

重要

正しい **IPv4** サブネットマスクを持つ有効な **IPv4** アドレスのみを入力してください。アドレスと対応するサブネットが重複していないことを確認します。サブネットが重複すると、サービスの通信に問題が発生する場合があります。

次の情報を収集します。

- スタティック IP アドレス
- サブネット マスク
- デフォルト ゲートウェイ
- DNS アドレス
- NTP サーバーの詳細
- プロキシサーバーの詳細

サポート対象のブラウザを使用していることを確認します。詳細については、[展開の要件](#) (7ページ) を参照してください。

次の手順で指定するデフォルトゲートウェイおよび DNS サーバーと Catalyst Center on ESXi の間のファイアウォールで **ICMP** が有効になっていることを確認します。ウィザードでは、ユーザの指定する DNS サーバを **ping** で確認します。ファイアウォールが配置されており、そのファイアウォールで **ICMP** が許容されていない場合、この **ping** がブロックされる可能性があります。ブロックされた場合、ウィザードを完了できません。

1. 展開が完了したら、新しい仮想マシンの電源をオンにします。

- a) vSphere Web Client で、仮想マシンを右クリックします。
- b) **[Power]** > **[Power On]** を選択します。

仮想マシンが動作可能になるまでに約 **90 ～ 120 分** かかります。合計時間は、使用可能な帯域幅、RAM、ハードディスク容量、vCPU の数によって異なります。vSphere Client の **[最近のタスク (Recent Tasks)]** タブで進行状況をモニターします。

2. リモートコンソールまたは **Web** コンソールのリンクをクリックして起動します。

3. 詳細インストール構成ウィザードを表示します。

a) **[STATIC IP CONFIGURATION]** ページで、次のいずれかのタスクを実行します。

- DHCP サーバーが IP アドレス、サブネットマスク、デフォルトゲートウェイを仮想アプライアンスのエンタープライズインターフェイスに割り当てるようにするには、**[skip>>]** をクリックします。
- 独自の IP アドレス、サブネットマスク、デフォルトゲートウェイを仮想アプライアンスのエンタープライズインターフェイスに割り当てる場合は、次の表に記載されている情報を入力し、**[Configure]** をクリックします。

オプション	説明
[IPv6 Mode] チェックボックス	IPv6 アドレスを使用する場合は、このチェックボックスをオンにします。代わりに IPv4 アドレスを使用する場合は、このチェックボックスを空白のままにします。
[IP Address] フィールド	使用する静的 IP アドレスを入力します。
[ネットマスク (Netmask)] フィールド	前のフィールドに指定した IP アドレスのネットマスクを入力します。 • IPv4 アドレスを入力した場合は、ネットマスクまたは CIDR アドレスのいずれかを入力できます。 • IPv6 アドレスを入力した場合は、CIDR アドレスのみを入力できます。
[Default Gateway Address] フィールド	トラフィックのルーティングに使用されるデフォルトゲートウェイを指定します。
[Static Routes] フィールド	1 つ以上のスタティックルートをスペースで区切り、<ネットワーク>/<ネットマスク>/<ゲートウェイ> の形式で入力します。これは、通常、管理インターフェイスでのみ必要です。

[Webインストール (Web Installation)] フィールドに記載されている URL をメモします。この URL は次のステップで必要になります。

b) **[Static IP Configuration]** ページに表示された URL を開きます。

c) **[Start a Catalyst Center Virtual Appliance]** オプションボタンをクリックし、**[Next]** をクリックします。

d) **[Advanced Install]** オプションボタンをクリックし、**[Start]** をクリックします。

[Advanced Install Overview] スライドが開きます。**[>]** をクリックして、ウィザードで実行するタスクの概要を表示します。

e) **[Start Workflow]** をクリックしてウィザードを起動します。

[Virtual Appliance Interface Overview] ページが開き、設定可能な 4 つのアプライアンス インターフェイスの説明が表示されます。

4. 詳細インストール構成ウィザードを完了することにより、仮想アプライアンスを設定します。

a) **[Next]** をクリックします。

[How would you like to set up your appliance interfaces?] ページが開きます

ネットワークがファイアウォールの背後にある場合は、次のアクションを実行します。

- ・ [これら URL へのアクセスを許可 (allow access to these URLs)] リンクをクリックすると、**Catalyst Center on ESXi** がアクセスする必要がある URL が一覧表示されたウィンドウが開きます。
- ・ [これらのポートを開く (open these ports)] リンクをクリックすると、**Catalyst Center on ESXi** に必要なネットワークサービスポートが一覧表示されたウィンドウが開きます。

デフォルトでは、[Enterprise Network Interface] チェックボックスがすでにオンになっています。また、[STATIC IP CONFIGURATION] ページで入力した値も事前に入力されています。

- b) 使用するアプライアンスインターフェイスごとに次の手順を実行し、[次へ (Next)] をクリックします。

- ・ 対応するチェックボックスをオンにして、適切な設定値を入力します。
- ・ 必要に応じて、対応する [Add/Edit Static Route] リンクをクリックし、スタティックルートを設定します。必要に応じて [+] をクリックし、追加のルートを設定します。完了したら、[Add] をクリックします。

[DNS Configuration] 画面が開きます。

- c) 優先 DNS サーバーの IP アドレスを入力して、[Next] をクリックします。追加の DNS サーバーを入力するには、[Add] (+) アイコンをクリックします。

重要

- ・ クラスタ内の各ノードに対して、最大 3 つの DNS サーバーを設定します。1 台のアプライアンスに対して 4 台以上の DNS サーバーを設定すると、問題が発生する可能性があります。
- ・ NTP の場合、**Catalyst Center on ESXi** と NTP サーバーの間のポート 123 (UDP) が開いていることを確認します。

[Configure Proxy Server Information] 画面が開きます。

- d) 次のいずれかの手順を実行して、[Next] をクリックします。

- ・ ネットワークでプロキシサーバーを使用しないでインターネットにアクセスする場合は、[No] オプションボタンをクリックします。
- ・ ネットワークでプロキシサーバーを使用してインターネットにアクセスする場合は、次の表に示す値を入力します。

フィールド	説明
[Proxy Server]	インターネットにアクセスする HTTPS ネットワークプロキシの URL またはホスト名を入力します。
	 注 Catalyst Center on ESXi から HTTPS プロキシへの接続は、このリリースの HTTP 経由のみでサポートされます。
Port	アプライアンスがネットワークプロキシにアクセスするために使用したポートを入力します。

フィールド	説明
Username	ネットワークプロキシへのアクセスに使用するユーザー名を入力します。プロキシログインが必要ない場合には、このフィールドを空白のままにします。
Password	ネットワークプロキシへのアクセスに使用するパスワードを入力します。プロキシログインが必要ない場合には、このフィールドを空白のままにします。

ウィザードが入力した情報を確認し、続行する前に変更が必要な設定を表示します。入力した設定が有効で、ポートが稼働している場合は、ウィザードの [詳細アプライアンス設定 (Advanced Appliance Settings)] 画面が開きます。

- e) アプライアンスの構成値を入力し、[Next] をクリックします。

オプション	説明
クラスタ仮想 IP アドレス	
[Enterprise Network] および [For Intracluster Access] フィールドからアクセスする場合	エンタープライズ インターフェイスに設定されている仮想 IP アドレスを入力します。管理インターフェイスの仮想 IP アドレスを設定した場合は、そのアドレスも入力します（カンマを使用して 2 つの IP アドレスを区切ります）。
[Fully Qualified Domain Name (FQDN)] フィールド	仮想アプライアンスの完全修飾ドメイン名 (FQDN) を指定することもできます。Catalyst Center on ESXi は、このドメイン名を使用して次のタスクを実行します。 - このホスト名を使用して、仮想アプライアンスの Web インターフェイスと、Catalyst Center on ESXi が管理するエンタープライズ ネットワーク内のデバイスによって使用される Representational State Transfer (REST) API にアクセスします。 - Catalyst Center on ESXi 証明書の [Subject Alternative Name (SAN)] フィールドで、FQDN を使用して、デバイスのプロビジョニングに使用されるプラグ アンドプレイ サーバが定義されます。

NTP サーバー設定

[NTP Server] フィールド

少なくとも 1 つの NTP サーバーアドレスまたはホスト名を入力します。追加の NTP サーバーアドレスまたはホスト名を入力するには、[Add] (+) アイコンをクリックします。

実稼働環境への展開では、少なくとも 3 台の NTP サーバを設定するようお勧めします。

オプション	説明
[Turn On NTP Authentication] チェックボックス	NTP サーバーが同期する前に Catalyst Center on ESXi NTP サーバーの認証を有効にするには、このチェックボックスをオンにして、次の情報を入力します。 • NTP サーバーのキー ID。有効な値の範囲は 1 ～ 4294967295 ($2^{32}-1$) です。 この値は、NTP サーバーのキーファイルで定義されているキー ID に対応します。 • NTP サーバーのキー ID に関連付けられた SHA-1 キー値。この 40 文字の 16 進文字列は、NTP サーバーのキーファイルにあります。

注

前のフィールドで構成した各 NTP サーバーのキー ID とキー値を入力してください。

サブネット設定

[Container Subnet] フィールド

内部サービスを管理するために **Catalyst Center on ESXi** で使用する、ルーティングされない専用の IP サブネット。デフォルトでは、これは **169.254.32.0/20** にあらかじめ設定されています。このサブネットを使用することをお勧めします。

[Cluster Subnet] フィールド

内部クラスタサービスを管理するために **Catalyst Center on ESXi** で使用する、ルーティングされない専用の IP サブネット。デフォルトでは、これは **169.254.48.0/20** にあらかじめ設定されています。このサブネットを使用することをお勧めします。

[Enter CLI Password] ページが開きます。

- f) maglev ユーザーのパスワードを入力して確認した後、[Next] をクリックします。

入力した情報がウィザードで検証され、変更の必要な設定があれば、ウィザードの操作を続行する前に通知されます。入力した設定が有効な場合、ウィザードの [Summary] ページが開きます。

 注

アプライアンスの設定を JSON ファイルとしてダウンロードするには、対応するリンクをクリックします。

- g) 画面の下部までスクロールし、ウィザードの完了時に入力したすべての設定を確認します。必要に応じて、適切な **[Edit]** リンクをクリックして、更新を行うウィザード画面を開きます。
- h) **Catalyst Center on ESXi** 仮想アプライアンスの設定を完了するには、**[Start Configuration]** をクリックします。

プロセス中もウィザード画面が更新され、実行中のタスクとその進行状況、エラーが表示されます。この情報をテキストファイルとして保存するには、**[ダウンロード (Download)]** リンクをクリックします。

仮想マシンは **180 ~ 210** 分で使用可能になります。この時間は、使用可能な帯域幅、RAM、ハードディスク容量、vCPU の数によって異なります。vSphere Client の **[Recent Tasks]** タブで進捗状況をモニターできます。

5. アプライアンスの設定が完了したら、コピーアイコンをクリックして、デフォルトの管理者スーパーユーザーパスワードをコピーします。

サービスが安定してユーザーインターフェイスにログインできるようになるまで **15 ~ 30** 分かかる場合があります。

重要

インストール構成ウィザードを完了すると、**Catalyst Center on ESXi** はこのパスワードを自動的に設定します。続行する前に、必ずコピーアイコンをクリックしてください。クリックしないと、**Catalyst Center on ESXi** への最初のログインができません。

 注

セキュリティ対策として、ログイン後にこのパスワードを変更するよう求められます。詳細については、[クイック スタート ワークフローの完了 \(56 ページ\)](#) を参照してください。

CC VA

インタラクティブ **CC VA** ランチャーを使用した仮想アプライアンスの設定方法について説明します。

CC VA ランチャーを使用して **Catalyst Center on ESXi** 仮想アプライアンスを設定するには、次の手順を実行します。

 注

CC VA ランチャは、デフォルトのルートディレクトリ内のすべての VM 展開をプロビジョニングしますが、ユーザー定義のフォルダへの VM の展開はサポートしていません。

1. シスコのソフトウェアダウンロードサイトに移動して、Catalyst Center on ESXi OVA ファイルをダウンロードします。
2. 同じ場所から CC VA ランチャバンドル (CatC-SW-Launcher-*<release number>*-VA.tar.gz) をダウンロードして解凍します。
バンドルには次のファイルが含まれています。
 - ランチャアプリケーション : **dnac-esxi-launcher**
 - 単一ネットワーク インターフェイス コントローラ (NIC) 展開用の構成ファイル : **config.json**
 - デュアルネットワーク インターフェイス コントローラ (NIC) 展開用の構成ファイル : **config_dual_nic.json**
 - ロガー構成ファイル : **log_config.json**
 - ライセンス : **LICENSE**
3. オペレーティングシステムに固有のコマンドを入力して、CC VA ランチャーをインタラクティブモードで起動します。
 - macOS : **./dnac-esxi-launcher**
 - Microsoft Windows : **dnac-esxi-launcher.exe**
 - Linux : **./dnac-esxi-launcher**
4. CC VA ランチャーを完了します。
 - a) 仮想アプライアンスを展開するホスト/vCenter サーバーの IP アドレス、ログイン情報、および SSL ポート番号を入力します。
ランチャーはホスト/vCenter サーバーとの接続を確認します。
 - b) Catalyst Center on ESXi OVA ファイルへのパスを入力します。
Microsoft Windows パスを指定する場合は、デリミタとして「\\」を使用します。パスは次のようになります。C:\\Users\\dnac\\downloads\\esxi_10.ova
 - c) 作成する仮想マシンの名前を入力します。
 - d) 仮想ディスクが使用するプロビジョニング形式を選択し、**Enter** を押します。
シンプロビジョニング形式とシックプロビジョニング形式の両方がサポートされています。デフォルトはシックプロビジョニング形式です。

 注

NFS データストアのシックプロビジョニングは、ストレージベンダーが許可している場合にのみサポートされます。許可していない場合、システムはインポート時にデータストアのデフォルトのプロビジョニング形式を使用します。

- e) 次のいずれかの検出モードを選択し、**Enter** を押します。

 注

この手順は、スタンドアロン **ESXi** ホストには適用されません。ステップ **4h** に進みます。

- ・ **[Discover all VMware Datacenters]** : 選択すると、アクセス権があり、**Catalyst Center on ESXi** のメモリ、CPU 予約、およびディスク容量の要件を満たすデータセンターのみがリストされます。
- ・ **[List all available VMware Datacenters]** : 選択すると、使用可能なすべてのデータセンターがリストされます。

- f) 使用するデータセンターを選択し、**Enter** を押します。

検出時間は、ネットワーク速度と、ホスト、クラスタ、仮想マシン、またはデータストアの数によって異なります。

- g) クラスタまたは直接接続されたホストが使用可能な場合は、対応する展開ターゲットオプションを選択するように求められます。

- ・ クラスタオプションを選択した場合は、適切なクラスタとその予約されていないリソースがリストされます。使用するクラスタを指定し、ステップ **4h** に進みます。

 注

選択したクラスタで **vSphere HA** が有効になっていない場合は、警告メッセージが、クラスタの分散リソーススケジューラ (**DRS**) のステータスとともに表示されます。

- ・ 直接接続ホストオプションを選択した場合（またはクラスタオプションを選択し、**DRS** が無効になっている場合）、適切なホストがリストされます。使用するホストを指定し、ステップ **4h** に進みます。

 注

DRS が有効になっていて、リソースプールが見つかった場合は、展開でのリソースプールの使用を確認するように求められます。

- h) 以前に選択したディスクプロビジョニング形式に基づいて、使用可能な適切なデータストアがリストされます。使用するデータストアを指定します。

 注

NFS データストアの場合、シックプロビジョニングは、基盤となるストレージベンダーがサポートしている場合にのみサポートされます。そうでない場合は、データストアのデフォルトのプロビジョニングがインポート時に選択されます。

- i) **y** または **n** を入力して、仮想アプライアンスの管理インターフェイスを設定するかどうかを指定します。
- 使用可能なネットワークのリストが表示されます。
- j) アプライアンスのエンタープライズ インターフェイスに使用するネットワークを選択します。
- 前の手順で **y** を選択した場合、アプライアンスの管理インターフェイスに使用するネットワークを選択します。
- k) エンタープライズ インターフェイスの IP アドレスおよびサブネットマスクを入力します。
- エンタープライズ インターフェイスのみを設定する場合（ステップ 4i で **n** を入力）、エンタープライズ インターフェイスで使用するゲートウェイの IP アドレスを入力します。
 - ステップ 4i で **y** を入力した場合は、**y** と入力して、エンタープライズ インターフェイスが使用するデフォルトゲートウェイを設定します。

 注

デフォルトゲートウェイは、アプライアンスのインターフェイスの 1 つに対してのみ設定できます。管理インターフェイスでデフォルトゲートウェイを設定する場合は、**n** と入力します。

- l) **y** または **n** を入力して、エンタープライズ インターフェイスのスタティックルートを設定するかどうかを指定します。
- y** と入力した場合は、設定するスタティックルートの数を入力します。また、各ルートを次の形式で入力します：<network>/<netmask>/<gateway>。
- m) （ステップ 4i で **y** と入力して）アプライアンスの管理インターフェイスを設定することを選択した場合は、その IP アドレスとサブネットマスクを入力します。
- n) ステップ 4k で **n** を入力した場合は、管理インターフェイスが使用するデフォルトゲートウェイを入力します。

- o) **y** または **n** を入力して、管理インターフェイスのスタティックルートを設定するかどうかを指定します。

y と入力した場合は、設定するスタティックルートの数を入力します。また、各ルートを次の形式で入力します：<network>/<netmask>/<gateway>。

- p) **y** または **n** を入力して、プロキシサーバーを設定するかどうかを指定します。

 注

HTTP プロキシサーバーのみがサポートされています。

- q) 前の手順で **y** を入力した場合は、**y** または **n** を入力して、プロキシサーバーに対して認証が有効になっているかどうかを指定します。

- r) **y** を入力した場合は、プロキシサーバーのログイン情報を入力します。

- s) 設定する DNS サーバーの数を入力します。

少なくとも 1 台のサーバーを設定する必要があり、最大 3 台を設定できます。プロンプトが表示されたら、設定する DNS サーバーの IP アドレスを入力します。

- t) 設定する NTP サーバーの数を入力します。

少なくとも 1 台のサーバーを設定する必要があり、最大 3 台を設定できます。プロンプトが表示されたら、設定する NTP サーバーの IP アドレスを入力します。

- u) **y** または **n** を入力して、完全修飾ドメイン名 (FQDN) を設定するかどうかを指定します。

y と入力した場合は、適切な FQDN を入力します。

 注

FQDN にはハイフン以外の特殊文字を含めることはできません。

- v) **Maglev** ユーザーのパスワードを入力して確認します。このパスワードを使用してシェルにアクセスし、SSH アクセスを有効にします。

パスワードは次の要件を満たす必要があります。

- ・ 8 文字以上とすること。
- ・ タブや改行を含まないこと。
- ・ 次のうち少なくとも 3 つのカテゴリの文字を含むこと。
 - ・ 大文字の英字 (A ~ Z)
 - ・ 小文字の英字 (a ~ z)
 - ・ 数字 (0 ~ 9)
 - ・ 特殊文字 (! や # など)

設定の概要が表示されます。

- w) 「**y**」 と入力して、展開および設定プロセスを開始します。

ランチャが次のタスクを実行します。

1. OVA ファイルをインポートします。
2. 管理インターフェイスの設定を選択した場合は、仮想マシンにインターフェイスを追加します。
3. Catalyst Center on ESXi のネットワーク設定を仮想マシンに適用します。
4. [Enable Storage I/O Control and statistics collection] オプションが有効になっているかどうかを確認し、有効になっていない場合はメッセージを表示します。
5. 展開された仮想マシンの電源をオンにします。

注

展開の完了に必要な時間は、使用可能なネットワーク帯域幅とデータストアのスループットによって異なります。

5. Catalyst Center on ESXi 仮想アプライアンスの電源がオンになったら、その仮想アプライアンスを展開したホスト/vCenter サーバーにログインします。仮想アプライアンスの **VMware** コンソールを開きます。
仮想アプライアンスが起動すると、ターミナルシェルが開くまで最大 **60 分** かかります。
6. ステップ 4v で入力した **Maglev** パスワードを使用してログインします。
デフォルトのユーザー名は **maglev** です。
7. すべての Catalyst Center on ESXi サービスが実行されているときに、サポートされているブラウザを使用し、先ほど指定した IP アドレスを使用してエンタープライズインターフェイスにアクセスします。管理インターフェイスを設定した場合は、その IP アドレスを使用します。
8. Catalyst Center on ESXi GUI で求められたら、デフォルトのログイン情報 (**admin/P@ssword9**) を入力してログインします。

CC VA

CC VA ランチャーをサイレントモードで使用した仮想アプライアンスの設定方法について説明します。

CC VA ランチャのサイレントモードを使用して、**config.json** ファイルで指定された設定で Catalyst Center on ESXi 仮想アプライアンスを展開します。このモードは、展開の自動化ワークフローにランチャーを統合する場合に便利です。ランチャのサイレントモードを使用して仮想アプライアンスを設定するには、次の手順を実行します。

 注

CC VA ランチャは、デフォルトのルートディレクトリ内のすべての VM 展開をプロビジョニングしますが、ユーザー定義のフォルダへの VM の展開はサポートしていません。

1. シスコのソフトウェアダウンロードサイトに移動して、Catalyst Center on ESXi OVA ファイルをダウンロードします。
2. 同じ場所からランチャバンドル (CatC-SW-Launcher- <release number>-VA.tar.gz) をダウンロードして解凍します。
バンドルには、次のファイルが含まれています。
 - ・ ランチャアプリケーション : dnac-esxi-launcher
 - ・ エンタープライズ インターフェイスのみを設定する場合の構成ファイル : config.json
 - ・ エンタープライズ インターフェイスと管理インターフェイスの両方を設定する場合の構成ファイル : config_dual_nic.json
 - ・ ロガー構成ファイル : log_config.json
 - ・ ライセンス : LICENSE
3. CCVA ランチャーバンドルファイルが解凍されたディレクトリに移動し、構成ファイルをテキストエディタで開きます。
 - ・ 単一の NIC 展開で、アプライアンスのエンタープライズ インターフェイスのみを設定する場合は、config.json を開きます。
 - ・ アプライアンスのエンタープライズ インターフェイスと管理インターフェイスを設定するデュアル NIC 展開の場合は、config_dual_nic.json を開きます。
4. 構成ファイルで提供されるパラメータについては、展開に固有の値を入力します。
詳細については、[設定ファイルのパラメータ](#) (51 ページ) を参照してください。

 注

使用しないオプションパラメータについては、空の文字列 ("") を入力します。たとえば、仮想アプライアンスの FQDN を指定しない場合、エントリは次のようになります。"fqdn": ""

5. 構成ファイルで指定した値を使用して、CC VA ランチャを実行します。
 - a. 必要に応じて、ランチャー バンドル ファイルが解凍されたディレクトリに戻ります。
 - b. オペレーティングシステムに固有のコマンドを入力します。
 - ・ macOS : `./dnac-esxi-launcher -c configuration-filename -u vCenter-or-host-username -p vCenter-or-host-password -l Maglev-password --proxy_user proxy-username --proxy_password proxy-password`

- Microsoft Windows : `dnac-esxi-launcher.exe -c configuration-filename -u vCenter-or-host-username -p vCenter-or-host-password -l Maglev-password --proxy_user proxy-username --proxy_password proxy-password`
- Linux : `./dnac-esxi-launcher -c configuration-filename -u vCenter-or-host-username -p vCenter-or-host-password -l Maglev-password --proxy_user proxy-username --proxy_password proxy-password`

注

- ホストまたは vCenter サーバーが自己署名証明書を使用してインストールされている場合は、次のコマンドを入力して SSL 証明書の検証をスキップします。`./dnac-esxi-launcher config.json -d -u vCenter-or-host-username -p vCenter-or-host-password -l Maglev-password`（単一 NIC 展開）または `./dnac-esxi-launcher config_dual_nic.json -d -u vCenter-or-host-username -p vCenter-or-host-password -l Maglev-password`（デュアル NIC 展開）
- `--proxy_user` および `--proxy_password` パラメータはオプションであり、認証ベースのプロキシが使用されている場合にのみ入力する必要があります。
- このコマンドで指定するパスワードのいずれかに OS 固有の特殊文字が含まれている場合は、エスケープシーケンスとして入力することを推奨します。エスケープシーケンスは、バックslash (\) の後に文字または対応する 8 進または 16 進数を続けたものです。

CC VAランチャが起動すると、次のタスクを実行します。

- ホストまたは vCenter サーバーとの接続を確認する
- ターゲット環境と設定パラメータを検証する
- 検証が成功したら、設定の概要を表示する
- OVA ファイルをインポートする
- 管理インターフェイスの設定が選択されている場合は、このインターフェイスをインポートされた仮想マシンに追加する
- Catalyst Center on ESXi のネットワーク設定を仮想マシンに適用する
- [Enable Storage I/O Control and statistics collection] オプションが有効になっているかどうかを確認し、有効になっていない場合はメッセージを表示する
- 展開された仮想マシンの電源をオンにします。

展開にかかる時間は、使用可能なネットワーク帯域幅とターゲットデータストアのスループットによって異なります。

6. 仮想アプライアンスの電源がオンになったら、ホスト/vCenter サーバーのログイン情報を入力し、アプライアンスの VMware コンソールを開きます。

端末シェルが開くまでに最大 1 時間かかることがあります。

7. ステップ 5 で指定したユーザー名とパスワードとして **maglev** を使用してログインします。
8. Catalyst Center on ESXi サービスが起動したら、サポートされているブラウザを使用して、構成ファイルでエンタープライズ インターフェイスに指定した IP アドレスを開きます。
9. ユーザー名に **admin**、パスワードに **P@ssword9** を使用してログインします。

次の表は、`config.json` ファイルで値を入力する必要があるパラメータを示しています。

 注

使用しないオプションパラメータについては、空の文字列（""）を入力します。たとえば、仮想アプライアンスの完全修飾ドメイン名（FQDN）を指定しない場合、エントリは次のようになります。"fqdn": ""

カテゴリ	設定パラメータ	説明
ホスト/vCenter 情報 (host_info)	IP (ip) ²	オープン仮想アプライアンス（OVA）がインポートされる vCenter またはスタンドアロン ESXi ホストの IP アドレスまたは FQDN。
	SSL ポート (ssl_port) ¹	vCenter または ESXi ホストで HTTPS が設定されているポート。デフォルトのポートは 443 です。

 注

vCenter によって管理されているホストは指定できません。

² 必須パラメータ

カテゴリ	設定パラメータ	説明
インポート設定 (import_info)	OVA ファイルのパス (ova_path) ¹	Catalyst Center on ESXi OVA ファイルがダウンロードされたディレクトリ。
		📄 注 Microsoft Windows パスを指定する場合は、デリミタとして二重バックスラッシュを使用します。パスは次の例のようになります。 <pre>C:\Users\dnac\downloads\esxi_10.ova</pre>
	仮想マシン (VM) 名 (vm_name) ¹	VM の名前。
	データセンター (data_center) ³	仮想アプライアンス OVA ファイルのインポート先となるデータセンターの名前。このパラメータは、スタンドアロン ESXi ホストの展開には適用されません。
	クラスタ名 (cluster) ⁴	仮想マシンが存在するクラスタの名前。
	リソースプール (resource_pool) ³	インポートされた VM を配置する必要があるリソースプール。このパラメータは、ESXi ホストの展開には適用されません。
	ホスト名 (host_name) ²	VM を配置する必要がある ESXi ホスト (vCenter によって管理)。このパラメータは、スタンドアロン ESXi ホストの展開には適用されません。
	データベース (datastore) ¹	VMDK およびその他のサポートファイルを配置する必要があるデータストアの名前。
	ディスクのプロビジョニング (disk_provision) ¹	仮想ディスクのプロビジョニング形式。シックプロビジョニング形式がデフォルトで設定されていますが、シンプロビジョニング形式とシックプロビジョニング形式の両方がサポートされています。
	エンタープライズネットワーク (network: enterprise_network) ¹	仮想マシンのエンタープライズ ネットワークにマッピングされるホストネットワークの名前。
	管理ネットワーク (network: management_network) ⁵	Catalyst Center on ESXi のグラフィカルユーザー インターフェイス (GUI) へのアクセスに使用される、仮想マシンの管理ネットワークにマッピングされるホストネットワークの名前。

³ vCenter Server にのみ適用される必須のパラメータ

⁴ vCenter にのみ適用され、スタンドアロン ESXi ホストには適用されないオプションのパラメータ

⁵ デュアル NIC 展開にのみ適用される必須パラメータ

カテゴリ	設定パラメータ	説明
Catalyst Center on ESXi 設定情報 (dnac_info)	IP アドレス (address) ¹	仮想アプライアンスのエンタープライズネットワークインターフェイスの IP アドレス。
	サブネットマスク (netmask) ¹	仮想アプライアンスのエンタープライズネットワークインターフェイスのサブネットマスク。
	ゲートウェイ (gateway) ¹ 、 ⁶	エンタープライズネットワークインターフェイスのゲートウェイの IP アドレス。
	ルート (routes) ⁵	エンタープライズ インターフェイスのスタティックルート。次の形式でルートを入力します。 <network-IP-address> <netmask> <gateway-IP-address>。複数のルートを指定する場合は、カンマ (,) で区切ります。
	IP アドレス (address) ⁴	仮想アプライアンスの管理インターフェイスの IP アドレス。
	サブネットマスク (netmask) ⁴	仮想アプライアンスの管理ネットワーク インターフェイスのサブネットマスク。
	ゲートウェイ (gateway) ¹ 、 ⁵	管理ネットワーク インターフェイスのゲートウェイの IP アドレス。
	ルート (routes) ⁵	管理インターフェイスのスタティックルート。次の形式でルートを入力します。 <network-IP-address> <netmask> <gateway-IP-address>。複数のルートを指定する場合は、カンマ (,) で区切ります。
	ドメイン ネーム システム (DNS) サーバー (dns_servers) ¹	仮想アプライアンスが使用する DNS サーバー。少なくとも 1 つのサーバーを指定します。最大 3 つのサーバーをカンマで区切って指定できます。
	HTTP プロキシ (http_proxy) ⁷	仮想アプライアンスが使用する HTTP プロキシ。プロキシを指定する場合は、次の形式を使用します。 http://IP-address-or-FQDN:port-number
	NTP サーバー (ntp) ¹	仮想アプライアンスが使用する NTP サーバー。少なくとも 1 つのサーバーを指定します。最大 3 つのサーバーをカンマで区切って指定できます。
	FQDN (fqdn) ⁶	仮想アプライアンスに設定する完全修飾ドメイン名。この名前には、ハイフン以外の特殊文字は使用できません。

注

認証が有効になっている場合は、プロキシのユーザー名とパスワードを手元に置いておいてください。

⁶ デュアル NIC 展開にのみ適用されるオプションパラメータ
⁷ オプションパラメータ

CC VA

このガイドは、**progress.json** ファイルに表示される情報を理解するのに役立ちます。

Catalyst Center on ESXi 仮想アプライアンスのサイレントモード設定中に、**progress.json** ファイルを表示して設定プロセスをモニターできます。このファイルは、**CCVA** ランチャと同じディレクトリにあります。構成プロセスについて詳しく説明しています。

フィールド	説明
stage	アプライアンス構成プロセスの現在のステージ： • launcher_start : ランチャーが開始されました。 • config_file_validation : 構成ファイルを検証しています。 • connectivity_verification : vCenter/ ESXi ホストとの接続を検証しています。 • import_information_validation : インポート情報（データストア、リソースプール、OVA パスなど）を検証しています。 • import_ova : Catalyst Center on ESXi OVA ファイルをインポートしています。 • post_import_configuration : インポート手順の後に、システムが構成を行います。 • power_on : 仮想マシンの電源がオンになっています。 • deployment : 仮想アプライアンスの展開はほぼ完了しています。
status	構成ステージの現在のステータス： • in-progress • 「completed（完了）」 • failed • waiting • aborted
percentage	インポートされた Catalyst Center on ESXi OVA ファイルのパーセンテージ。
error_code	失敗した操作に関連付けられているエラーコード。テーブルを使用して、これらのコードの説明を見つけることができます。
error_desc	発生したエラーの説明。

エラー コード	説明
0	操作に成功しました。
101	操作が手動で終了しました。
102	構成ファイルが見つかりませんでした。
103	構成ファイルのエントリが正しくありません。
104	vCenter/ESXi ホストへの接続に失敗しました。
105	インポート操作に失敗しました。
106	指定された OVA ファイルパスが無効です。

エラー コード	説明
107	データストアフィールドが空です。
108	インポート情報が無効です。
109	データストアが無効です。
110	データセンターが無効です。
111	データストアの空き容量が不足しています。
112	ディスクプロビジョニングが無効です。
113	クラスタが無効です。
114	仮想マシンが見つかりません。
115	電源オン操作に失敗しました。
116	展開の確認メッセージで「 No 」を選択しました。
117	コマンドライン引数が正しくありません。
118	管理インターフェイスの追加に失敗しました。
119	json ファイルが無効です。
120	必須のサイレントモードフィールドが空です。
121	指定された OVA ファイルは別のファイルタイプです。
122	仮想マシン名フィールドが空です。
123	エンタープライズ ネットワーク名フィールドが空です。
124	リソースプールが無効です。
125	管理ネットワークが無効です。
126	仮想名が文字数の上限を超えています。
127	Maglev パスワードがパスワードの要件を満たしていません。
129	ESXi ホストが無効です。
130	vCenter ベースのインポートに空のデータセンターが指定されています。
131	vCenter ベースのインポートに空のホスト名が指定されています。
132	vCenter/ESXi ホストに無効なネットワークが指定されました。
133	仮想マシンの CPU またはメモリが不足しています。
134	入力された Catalyst Center on ESXi の情報が正しくありません。
135	検出中に適切なデータセンターが見つかりませんでした。
136	空の OVA ファイルパスが指定されました。

Catalyst Center の使用を開始するために必要な初期ログイン、セキュリティ設定、およびデバイス検出プロセスについて説明します。

Catalyst Center on ESXi 仮想アプライアンスを展開して設定したら、その GUI にログインできます。Catalyst Center on ESXi にアクセスするには、互換性のある HTTPS 対応ブラウザを使用してください。

(ユーザー名 `admin` と `SUPER-ADMIN-ROLE` が割り当てられた) 管理者スーパーユーザーとして初めてログインすると、クイックスタートワークフローが自動的に開始されます。このワークフローを完了すると、Catalyst Center on ESXi が管理するデバイスが検出されます。また、それらのデバイスからのテレメトリの収集も有効になります。

Catalyst Center on ESXi にログインしてクイックスタートワークフローを完了するには、次の内容が必要です。

- ・ 詳細インストール構成ウィザードを完了した場合は、スーパーユーザーのユーザー名 (`admin`) と、指定したパスワードを入力します。
- ・ 『[Cisco Catalyst Center Second-Generation Appliance Installation Guide](#)』の「Required First-Time Setup Information」のトピックで説明されている情報。

1. 次のいずれかを実行します。

- ・ いずれかの Maglev 構成ウィザードを完了した場合は、`https://` と、設定プロセスの最後に表示された Catalyst Center on ESXi GUI の IP アドレスを使用して、Catalyst Center on ESXi GUI にアクセスします。
- ・ いずれかのブラウザベースの構成ウィザードを完了した場合は、ウィザードの最後のページで **[Open Catalyst Center Virtual Appliance]** をクリックします。

次のいずれかのメッセージが表示されます (使用しているブラウザによって異なります)。

- ・ **Google Chrome** : 接続のプライバシーは保護されません
- ・ **Mozilla Firefox** : 警告 : 今後セキュリティリスクが見つかる潜在的可能性があります

2. メッセージを無視して **[詳細設定 (Advanced)]** をクリックします。

次のいずれかのメッセージが表示されます (使用しているブラウザによって異なります)。

- ・ **Google Chrome** :

```
This server could not prove that it is GUI-IP-address; its security
certificate is not trusted by your computer's
operating system. This may be caused by a misconfiguration or an attacker
intercepting your connection.
```

- ・ **Mozilla Firefox** :

```
Someone could be trying to impersonate the site and you should not continue.
Websites prove their identity via certificates.
Firefox does not trust GUI-IP-address because its certificate issuer is
unknown,
```

```
the certificate is self-signed, or the server is not sending the correct intermediate certificates.
```

こうしたメッセージが表示されるのは、コントローラが自己署名証明書を使用しているためです。Catalyst Center on ESXi での証明書の使用方法については、『[Cisco Catalyst Center Administrator Guide](#)』の「Certificate and Private Key Support」セクションを参照してください。

3. メッセージを無視し、次のいずれかを実行します。

- Google Chrome : *GUI-IP-address* (安全でない) リンクをクリックして開きます。
- Mozilla Firefox : [リスクを理解して続行する (Accept the Risk and Continue)] をクリックします。

4. [Log In] をクリックします。

Catalyst Center on ESXi ログイン画面が表示されます。

5. 次のいずれかを実行し、[Login] をクリックします。

- Maglev 構成ウィザードまたはブラウザベースのインストール構成ウィザードのいずれかを完了したら、管理者のユーザー名 (admin) とパスワード (P@ssword9) を入力します。
- ブラウザベースの詳細インストール構成ウィザードを完了した場合は、管理者のユーザー名 (admin) と、Catalyst Center on ESXi アプライアンスの設定時に設定したパスワードを入力します。

次の画面で、新しい管理者ユーザーを設定するように求められます (初回ログインに使用したデフォルトのログイン情報は削除されます)。

6. 表示されるダイアログボックスで次の手順を実行し、[Submit] をクリックします。

- [Roles] ドロップダウンリストで、[SUPER-ADMIN] ユーザーロールが選択されていることを確認します。
- 新しい管理ユーザーのユーザー名を入力します。
- 新しい管理ユーザーのパスワードを入力して確認します。

7. [Log In] をクリックします。

Catalyst Center on ESXi ログイン画面が表示されます。

8. 新しい管理者ユーザーに関して設定したユーザー名とパスワードを入力し、[Login] をクリックします。

9. [cisco.com](#) のユーザー名とパスワード (ソフトウェアダウンロードの登録とシステム通信の受信に使用される) を入力し、[Next] をクリックします。

 注

現時点でこれらのログイン情報を入力したくない場合は、代わりに [Skip] をクリックします。

[Terms & Conditions] 画面が開き、ソフトウェアのシスコ エンドユーザー ライセンス契約 (EULA) および現在利用可能な補足条件へのリンクが表示されます。

10. 各ドキュメントを確認したら、[Next] をクリックして EULA に同意します。

[Quick Start Overview] スライドが開きます。[>] をクリックすると、Catalyst Center on ESXi の使用を開始するために、クイック スタート ワークフローで完了までサポートされるタスクの説明が表示されます。

11. クイック スタート ワークフローを完了します。

- a) [Let's Do it] をクリックします。
- b) [Discover Devices: Provide IP Ranges] ページで、次の情報を入力し、[Next] をクリックします。
- ・ デバイス検出ジョブの名前。
 - ・ 検出するデバイスの IP アドレスの範囲。追加の範囲を入力するには、[+] をクリックします。
 - ・ アプライアンスのループバックアドレスを優先管理 IP アドレスとして指定するかどうかを指定します。詳細については、『[Cisco Catalyst Center User Guide](#)』の「Preferred Management IP Address」を参照してください。
- c) [Discover Devices: Provide Credentials] 画面で、設定するログイン情報のタイプに関する情報（次の表を参照）を入力し、[Next] をクリックします。

GUI コンポーネント	説明
[CLI (SSH) Credentials]	
[Username] フィールド	ネットワーク内のデバイスの CLI にログインするために使用するユーザー名。
Password フィールド	ネットワーク内のデバイスの CLI にログインするために使用するパスワード。入力するパスワードは、8 文字以上にする必要があります。
[Name/Description] フィールド	CLI ログイン情報の名前または説明。
[Enable Password] フィールド	CLI でより高い権限レベルを有効にするために使用するパスワード。ネットワークデバイスで必要な場合にのみ、このパスワードを設定します。
[SNMP Credentials]	
[SNMPv2c] オプションボタン	SNMPv2c のログイン情報を使用する場合にクリックします。
[SNMPv3] オプションボタン	SNMPv3 のログイン情報を使用する場合にクリックします。
[SNMP Credentials: SNMPv2c]	
[SNMPv2c Type] ドロップダウンリスト	SNMPv2c のログイン情報が使用されている場合は、読み取りまたは書き込みコミュニティ文字列を選択します。
[Name/Description] フィールド	SNMPv2c 読み取りまたは書き込みコミュニティストリングの名前または説明。
[Community String] フィールド	デバイス上の SNMP 情報を表示するためにのみ使用される読み取り専用コミュニティストリングパスワード。
[SNMP Credentials: SNMPv3]	
[Name/Description] フィールド	SNMPv3 ログイン情報の名前または説明。
[Username] フィールド	SNMPv3 ログイン情報に関連付けられているユーザー名。

GUI コンポーネント	説明
[Mode] フィールド	SNMP メッセージを必要とするセキュリティレベル。 ▪ [No Authentication, No Privacy] (noAuthnoPriv) : 認証も暗号化も行いません。 ▪ [Authentication, No Privacy] (authNoPriv) : 認証は行いますが、暗号化は行いません。 ▪ [Authentication and Privacy] (authPriv) : 認証と暗号化の両方を行います。
[認証パスワード (Authentication Password)] フィールド	SNMPv3 を使用するデバイスから情報にアクセスするために必要なパスワード。パスワードの長さは、最低 8 文字である必要があります。以下の点に注意してください。 ▪ 一部のワイヤレスコントローラでは、パスワードは少なくとも 12 文字以上にする必要があります。ワイヤレスコントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスでは Catalyst Center on ESXi による検出、監視、管理が行われなくなります。 ▪ パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
[Authentication Type] フィールド	[Authentication and Privacy] または [Authentication, No Privacy] が認証モードとして設定されている場合に使用されるハッシュベースのメッセージ認証コード (HMAC) タイプ。 ▪ [SHA] : HMAC-SHA 認証。 ▪ [MD5] : HMAC-MD5 認証。

GUI コンポーネント	説明
[Privacy Type] フィールド	プライバシー タイプ。 ([Mode] として [Authentication and Privacy] を選択した場合に有効になります)。次のいずれかのプライバシータイプを選択します。 • [AES128]: 暗号化の 128 ビット CBC モード AES。 • [AES192]: シスコのデバイス上での暗号化の 192 ビット CBC モード AES。 • [AES256]: シスコのデバイス上での暗号化の 256 ビット CBC モード AES。

注

- 検出機能とインベントリ機能の使用は、プライバシータイプ **AES192** および **AES256** のみでサポートされています。 **Assurance** 機能はサポートされていません。
- プライバシー タイプ **AES128** は、検出、インベントリ、および **Assurance** でサポートされています。

[Privacy Password] フィールド AES128、AES192、および AES256 暗号化標準規格でサポートされているデバイスで交換されるメッセージを暗号化するための秘密鍵を生成するために使用される **SNMPv3** プライバシーパスワード。パスワード（またはパスフレーズ）は、**8 文字以上**にする必要があります。

以下の点に注意してください。

- 一部のワイヤレスコントローラでは、パスワードは少なくとも **12 文字以上**にする必要があります。ワイヤレスコントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスでは **Catalyst Center on ESXi** による検出、監視、管理が行われなくなります。
- パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

NETCONF

[Port] フィールド Cisco IOS-XE を実行するワイヤレスコントローラを検出するために Catalyst Center on ESXi が使用する必要がある **NETCONF** ポート。

d) [Create Site] 画面で、テレメトリを容易にするために検出するデバイスを 1 つのサイトにグループ化し、[Next] をクリックします。

サイトの情報を手動で入力することも、マッピングインターフェイスを使用して構成プロセスの最後に表示された優先 GUI を選択することもできます。

e) [Enable Telemetry] 画面で、Catalyst Center on ESXi にテレメトリを収集させるネットワークコンポーネントを選択し、[Next] をクリックします。

f) [Summary] 画面で、入力した設定を確認し、次のいずれかを実行します。

- ・ 変更を加える場合は、該当する **[Edit]** リンクをクリックして、関連画面を開きます。
- ・ 設定に問題がなければ、**[検出とテレメトリの開始 (Start Discovery and Telemetry)]** をクリックします。**Catalyst Center on ESXi** により設定が検証され、問題が発生しないことが確認されます。検証が完了すると、画面が更新されます。

Catalyst Center on ESXi により、ネットワークのデバイスを検出し、選択したネットワークコンポーネントのテレメトリを有効にするプロセスが開始されます。このプロセスには少なくとも **30 分 (0.5 時間)** かかります。大規模なネットワークでは、さらに時間がかかる場合があります。

g) **[Launch Homepage]** をクリックして、**Catalyst Center on ESXi** のホームページを開きます。

ここから、デバイス検出とテレメトリ有効化の進捗状況をモニターできます。これらのタスクを実行中に、次のいずれかまたは複数を実行します。

- ・ **[Discoveries]** ページを開いて、ネットワーク内のデバイスが検出されたことを確認するには、**[Tools] > [Discovery]** メニューアイコンをクリックして次を選択します。
- ・ 以前に入力したログイン情報がサイトに設定されていることを確認するには、**[Design] > [Network Settings]** メニューアイコンをクリックして次を選択します。。その後、**[Device Credentials]** タブをクリックします。
- ・ **Catalyst Center on ESXi** ですでに実行がスケジュールされているタスク（セキュリティアドバイザリの毎週のネットワークスキャンなど）を表示するには、**[Activities]** メニューアイコンをクリックして次を選択します。。その後、**[Tasks]** タブをクリックします。
- ・ ネットワークのセットアップと維持に役立つガイド付きワークフローにアクセスするには、**[Workflows]** メニューアイコンをクリックして次を選択します。。

エアギャップ展開でネットワークを隔離し、手動でデータ転送を実行するプロセスについて説明します。

エアギャップは、ネットワークを分離し、そのネットワークが外部接続を確立できないようにするセキュリティ対策です。エアギャップネットワークにデータを転送するには、リムーバブルメディア（USB ドライブなど）を挿入するか、ラップトップを接続します。**Catalyst Center on ESXi** 展開のエアギャップを有効にするには、次の手順を実行します。

1. **仮想アプライアンスを展開**し、プロキシサーバーは未設定のままにします。
2. ネットワークのエアギャップを有効にする場合は、**Cisco Technical Assistance Center (TAC)** にお問い合わせください。

第3

章

- :

- □□□□□□
 - VM □□□□□□□□□□□□
 - □□□□□□□□□□ VM □□□□□
 - □□□□□□□□□□ VM □□□□□□□□□□

基本的な運用の調整（VM再起動の優先順位の設定、ディザスタリカバリ用のVMリソース予約の設定など）について説明します。

仮想アプライアンスを展開したら、次のタスクを完了してからアプライアンスを実行します。

VM

VMware vSphere の HA 設定で、HA フェールオーバー時の VM の優先順位を設定する方法について説明します。

ご使用の環境で VMware vSphere の HA が有効になっている場合は、次の手順を実行して、HA フェールオーバー時に仮想アプライアンスの VM の電源が優先的に（最初に）オンになるようにします。

-
1. vSphere Client のナビゲーションウィンドウで、HA クラスタをクリックします。
 2. [Configure] タブをクリックします。
 3. [設定 (Configuration)] > [VMオーバーライド (VM Overrides)] を選択し、[追加 (Add)] をクリックします。
 4. オーバーライドを適用する仮想マシンをクリックし、[OK] をクリックします。
 5. [vSphere HA] エリアの [VM再起動の優先順位 (VM Restart Priority)] フィールドで、次の手順を実行します。
 - a. [Override] チェックボックスにマークを付けます。
 - b. ドロップダウンリストから、[High] を選択します。
 6. [Finish] をクリックします。
-

VM

ディザスタリカバリ プレースホルダ VM に必要な手動リソース割り当て手順について詳しく説明します。

vSphere の Site Recovery Manager (SRM) を使用して Catalyst Center on ESXi のディザスタリカバリを有効にする場合は、フェールオーバー時に必要なリソースが予約されていることを確認します。リソースを予約するには、次の手順を実行します。仮想アプライアンスで vSphere レプリケーションを設定する場合、リカバリサイトの VM（「プレースホルダ VM」とも呼ばれる）には、メインサイトで設定された予約がありません。レプリケーションの完了後に、手動で予約を設定します。

-
1. vSphere Client のナビゲーションウィンドウで、セカンダリサイトのプレースホルダ VM をクリックします。
 2. [Actions] をクリックし、[Edit Settings] を選択します。
 3. [Virtual Hardware] タブを選択した状態で、[CPU] パラメータに 64 GHz の予約を設定し、[Memory] パラメータに 256 GB の予約を設定します。

4. [OK] をクリックします。

VM

セカンダリサイトで**SRM**を使用する場合のリソースプールのマッピングと予約の管理について説明します。

リソースプールに仮想アプライアンスを展開し、**vSphere** の **Site Recovery Manager (SRM)** を使用してプライマリサイトのリソースプールをセカンダリサイトのリソースプールにマッピングした場合は、仮想アプライアンスに必要なリソースをセカンダリサイトのリソースプールが予約していることを確認します。

第

4 Catalyst Center on ESXi

章

- :
- [Catalyst Center 3.1.6 on ESXi](#) □□
□□□□□□
 - [□□□□□□□□□□ Catalyst Center 3.1.6 on ESXi](#) □□□□□□□□
□

Catalyst Center 3.1.6 on ESXi

[ソフトウェア管理 (Software Management)] ページからシステムソフトウェアをアップグレードする手順について説明します。

- ・ Catalyst Center on ESXi データベースのバックアップを作成します。
- ・ 展開でファイアウォールを使用する場合は、Catalyst Center on ESXi が各クラスターノードのこの場所にアクセスして、<https://www.ciscoconnectdna.com:443> からシステムおよびパッケージファイルをダウンロードできることを確認します。

注

この手順を実行できるのは、SUPER-ADMIN-ROLE ユーザーのみです。

1. 右上隅にポップアップウィンドウが開き、新しいバージョンの Catalyst Center on ESXi が使用可能であることが示されます。[Go to Software Management] リンクをクリックします。

注

このポップアップウィンドウが表示されない場合は、左上隅にあるメニューアイコンをクリックし、**[System] > [Software Management]** を選択することもできます。

2. [Software Management] ページで、[Upgrade] をクリックします。
 3. [Upgrade Release] ダイアログボックスで、[Install] をクリックします。
 4. [Schedule Upgrade] ダイアログボックスで、アップグレードを開始するタイミングを指定し、[Download] をクリックします。
- [Activities] ページからアップグレードの進捗状況を追跡できます。

Catalyst Center 3.1.6 on ESXi

エアギャップ環境で Catalyst Center on ESXi 仮想アプライアンスを手動でアップグレードする方法について説明します。

1. シスコが指定する場所から *.tar.gz ファイルをダウンロードします。

2. 次のコマンドを入力して、ファイルを仮想アプライアンスの **/airgap** フォルダにコピーします。

```
scp -P 2222 *.tar.gz maglev@<appliance-IP-address>:/airgap
```

3. Catalyst Center on ESXi GUI にログインします。
 4. **[System]** > **[Software Management]** メインメニューから次を選択します。。
 5. **[Scan]** をクリックします。
 6. アップグレードを完了するために必要なファイルをシステムが認識したら、次のいずれかのオプションを選択します。
 - **[PreLoad]** をクリックしてアップグレードファイルをダウンロードします。このオプションを選択した場合は、アップグレード時間をスケジュールします。
 - **[Upgrade]** をクリックして関連ファイルをダウンロードし、すぐにアップグレードを開始します。
-

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。