Quali による Stack Automation のスタートアップガイド

©2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Stack Automation

Stack Automation by Quali（シスコと Quali が共同開発し、シスコが独自に提供）は、IT の計画、実装、および運用のギャップを埋めるために設計されたエージェント的プラットフォームです。数週間かかる手動の設定作業を自動化されたポリシー主導型の展開に置き換え、信頼性を持ってインフラストラクチャを拡張できるようにします。スタック自動化、計画（Day 0）、実装（Day 1）、運用（Day 2）のライフサイクル全体に対して、検証済みのシスコとサードパーティのソリューションが提供されます。

Stack Automation により、組織は生産を自動化し、クラウド速度でワークロードを準備し、手動エラーを削減し、IT チームは繰り返しの構成タスクではなくイノベーションに集中できます。 機能、利点、初期手順、およびデプロイメントの詳細については、以降のページで詳しく説明します。

ライフサイクルステージ別の機能

Stack Automation は、インフラストラクチャやアプリケーションから、依存関係や運用ワークフローまで、環境全体のライフサイクル管理を提供します。これにより、状態、ポリシー、コスト、Day-2 オペレーション、およびスケジュールを継続的に管理しながら、管理されたセルフサービスのデプロイメントが可能になります。また、定義されたTTL （存続可能時間）の終了時に環境を自動的に切断することで、技術情報効率を保証します。

Stack Automation は、次の機能を使用して環境を管理します。

- 自動化された TTL（存続可能時間）管理。
  - 時間制限付きの環境を適用し、制御された延長を許可します。また、コストを削減して環境のスプロールを防ぐために、TTL の期限が切れると　　技術情報を自動的にデコミッションします。
  - 自動化された TTL の適用と　　""　　デコミッションを備えた時間制限付き環境と、永続的なワークロードや共有サービスの常時接続環境の両方をサポートします。
- 電源管理：VMs の電源状態の開始、停止、再起動、または取得。
- データベース管理：データベース サーバーの起動、停止、再起動、または削除。
- Kubernetes 操作：クラスタの一時停止または再開、ポッドログの取得、ConfigMap の検査、およびシークレットの管理。
- ストレージ管理：インスタンスからブロックストレージ ボリュームを接続または切断します。
- アクセスと消費を管理
  - ロールベースのアクセス、承認、デプロイメント制限、ロケーションルール、インスタンスサイズの制御、　の予想コスト制限、およびその他のカスタム ポリシーを適用します。
  - 起動前と環境ライフサイクル全体の両方で統治を評価します。
- 運用と維持
  - 環境の状態、プロビジョニングの失敗、設定のばらつき、および運用上の問題をモニターします。
  - 更新、　　メンテナンス、スケーリング、修復、設定の変更など、ワンクリック、スケジュール、繰り返し、およびイベント トリガーの Day-2 アクションをサポートします。
  - 環境の更新：環境全体を再構築することなく　　、新しい IaC コードまたは更新された入力値を使用して特定のコンポーネントを再展開します。

©2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

◦ 正常性チェック：サービス、アプリケーション、インフラストラクチャ、および環境の正常性を検証します。

◦ スケーリングとキャパシティの変更：ストレージの追加、技術情報のサイズ変更、または ワークロードのニーズに基づいてインフラストラクチャを調整します。

◦ トラブルシューティング：ログを収集し、ランタイム状態を検査して、診断コマンドを実行します。

◦ カスタム運用ワークフロー：組織固有のスクリプトを実行します。

- スケジュールと予約

  ◦ 将来のウィンドウ用に環境をスケジュールし、 の GPU、ライセンス、静的 VMs、特殊なアセットなどの限定的なインフラストラクチャまたは一覧を予約します。

  ◦ 開発、テスト、デモンストレーション、トレーニング、および AI ワークロード全体で共有キャパシティを調整します。

- コストと使用率を制御する

  ◦ ユーザー、チーム、プロジェクト、環境のコンテキストに応じてデプロイメント コストを追跡します。

  ◦ 最大持続時間を適用し、アイドル状態の環境を特定し、終了の機会を推奨します。また、 は不要な技術情報を自動的にシャットダウンします。

- 拡張、再利用、および共有

  ◦ 再構築ではなく環境を拡張できる。

  ◦ 独立したライフサイクルの所有権と統治を維持しながら、共有サービスや依存関係として再利用できる公開された環境をサポートします。

- クリーンにデコミッションします

  ◦ 制御されたティアダウン ワークフローを実行して、インフラストラクチャと依存技術情報を削除します。

  ◦ Ansible 廃棄時プロセスを含むカスタム クリーンアップ ロジックをサポートし、孤立した 技術情報と設定の残りを削減します。

利点

Stack Automation は、シスコ、ISV、およびパートナー ソフトウェアの検証済みデプロイメント パスを提供します。複雑なソリューションの展開に必要な時間を数週間から数分に短縮します。

Stack Automation を使用すると、次のことが可能です

- 既存のブループリントのカスタマイズ：実績のある再利用可能なブループリントから始めて、特定のユース ケースに合わせてインフラストラクチャ、アプリケーション、ポリシー、入力、およびワークフローを適応させます。
- 独自の自動化の導入：すでに機能しているものを再構築することなく、既存の Terraform、Ansible、Helm、スクリプト、API、および CI/CD の自動化を統合します。
- AI による拡張：AI を活用、ブループリントの作成を加速し、自動化 を生成または変更し、展開をトラブルシュート、インテリジェントなライフサイクル アクションをトリガーします。

©2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Blueprint 管理

Stack Automation は、キュレートされたソリューションのカタログを提供します。既存のブループリントをカスタマイズしたり、新しいブループリントを作成したりできます。独自のコードをインポートしたり、組み込みエージェントの co-Pilot を使用したり、Clade Cowork、Codex、NVIDIA Nemotron などのエージェントのツールを統合したりできます。

Stack Automation は、次の 2 種類のキュレートされたソリューションを提供します：

- ソフトウェアのみ： OS プロビジョニング、VMaaS、GPUaaS、およびシスコおよびサードパーティのアプリケーション（ Nexus Dashboard、NVIDIA NIM、Proxmox、Splunk、Isovalent など）。
- フルスタック：人工知能ポッド、FlexPods、FlashStack などの完全なソリューションは、今後のリリースで利用可能になります。

導入機能

Stack Automation は、次のデプロイメント要件をサポートしています：

- 検証済みソリューション：シスコ、ISV、およびパートナーのソフトウェアのライブラリを提供します。
- 展開速度：手動設定時間を数分に短縮します。
- インフラストラクチャの柔軟性：ユーザーは独自のインフラストラクチャ、クラウド、多様なインフラストラクチャにソリューションを展開できます。
- マーケットプレイス統合：お客様が新しいソリューションをテストまたは導入するための合理化されたパスを提供します。

Stack Automation プラットフォームのコンポーネント

Stack Automation プラットフォームは、2 つの主要コンポーネントで構成されています：Stack 自動化ポータルと管理サーバー

Stack Automation ポータル

ポータルは、SaaS ベースのインターフェイスです。カタログを参照し、このポータルから展開を開始できます。

管理サーバー

管理サーバーは、 の展開を実行する VM ベースのアプライアンスです。LMP は、これらの機能を実行します：

- カタログの選択に基づいて自動化アーティファクトを取得します。
- Terraform、Ansible、Helm、Shell などのコードツールとしてインフラストラクチャを解釈するランを展開します。
- プライベート インフラストラクチャに自動化を適用します。
- インターネットにアクセスできない隔離された環境に到達するためのプロキシとして機能する。
- スマート デフォルト用に HPING3 などのユーティリティを提供します。
- イメージをローカル Webリポジトリとしてホストおよびキャッシュする。

©2026 Cisco and/or its affiliates. All rights reserved.

クラウドとの通信

ポータルと、AWS、Intersight、Azure などのパブリック クラウド間の通信は、管理サーバーを介してルーティングされません。パブリック クラウド専用のクラウド管理サーバーを生成して、

アカウントの管理をします。このプラットフォームは、従来のクラウドとリモート クラウドの両方をサポートしています。

あなたの Stack Automation の旅

Stack Automation の使用プロセスは、最初のログインから全面的なインフラストラクチャの管理まで続くように設計されています。をオンプレミスで展開する場合も、クラウドで展開する場合でも、このロードマップでは手順を 5 つの明確なフェーズに分割しています。まず、プラットフォームのインターフェイスに慣れてから、インフラストラクチャに適した特定のデプロイメント パスを進み、最終的には、環境を確実に管理および拡張するために必要なライフサイクル管理ツールを習得します。このジャーニーに従って、インフラストラクチャを効率的に計画、実装、および運用するために必要なすべてを確実に実行してください。

フェーズ	目標（Goal）	成功指標
方向	プラットフォームのスキルを身に付けてください。	**Meet Stack Automation** ツアーを完了し、デプロイメントパスを選択します。
パス選択	インフラストラクチャのニーズに合わせましょう。	特定の環境に必要なセットアップ（オンプレミスまたは Cloud）を特定します。
実行	環境の構築します。	オンプレミス： 管理サーバーをプロビジョニングし、統合（Intersight/ vCenter/ Nexus など）を管理して、必要なブループリントを展開します。 Cloud： クラウド サーバー（AWS）をオンボーディングし、必要なブループリントを展開します。
アクティブな管理	サービスを維持します。	オンプレミス： サービスの正常性をモニターし、構成の問題を解決し、稼働時間を維持します。 Cloud： クラウド 技術情報使用率をモニターし、サービスへのアクセスを維持します。
成長と拡張	ライフサイクルを最適化て拡張します。	オンプレミス：インフラストラクチャのばらつきを管理し、ブループリントをバージョン管理し、追加の統合を追加します。 Cloud： より多くのアカウントをオンボーディングし、スペース間で技術情報を共有することで、AWS フットプリントを拡張できます。

Stack Automation GUI

これらのデプロイメント パスのいずれかを選択する前に、Stack Automation GUI にログイン製品について理解し、よく理解する必要があります。

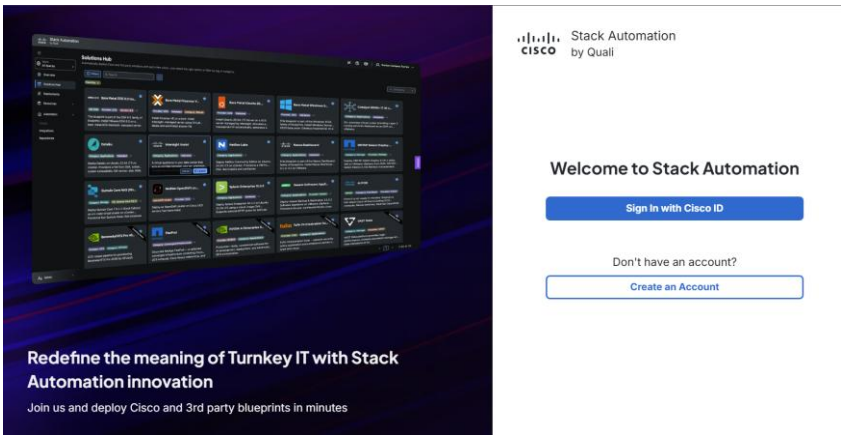
GUI にログインします。

1. Web ブラウザのアドレス バーに、「https://stackautomation.cisco.com」と入力します。

©2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

2. **[Stack Automation へようこそ（Welcome to Stack Automation）]** 画面で、**[アカウントの作成（Create an Account）]**（青い *[Cisco ID を使用した Sign In（Sign In with Cisco ID）]* ボタンの下）をクリックします。

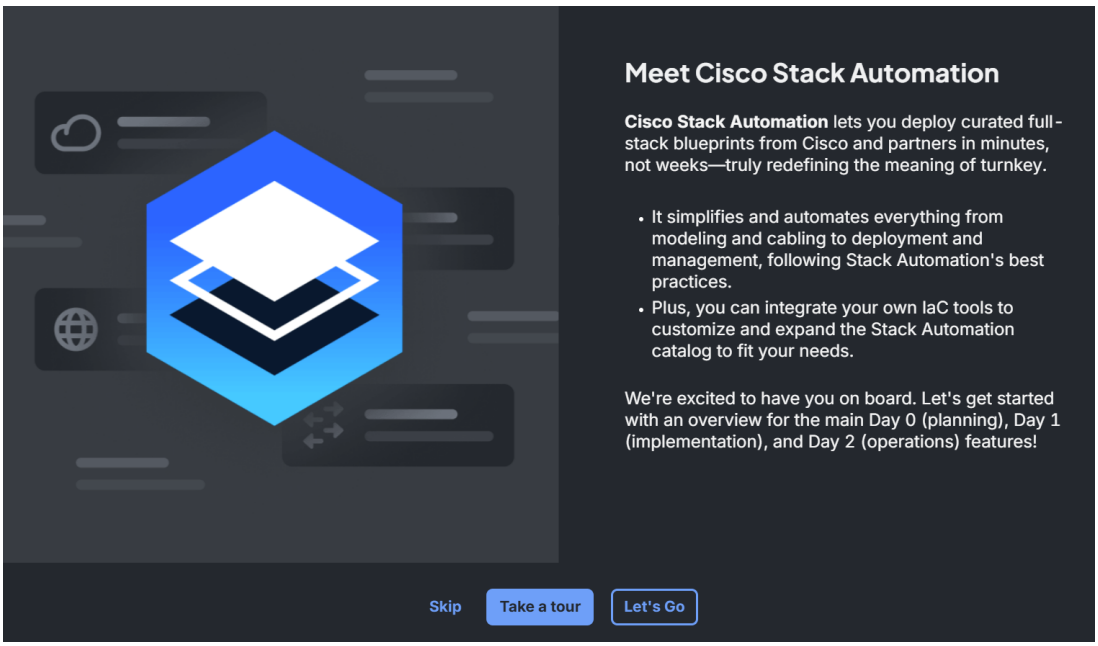


3. 「*利用規約*」を読んだことを示すチェックボックスを選択、**[Cisco ID でサインアップ（Sign-up with Cisco ID）]** をクリックします。
4. **[アカウントの作成（Create Account）]** 画面では、Cisco の電子メール ID が自動的に使用可能になり、**[アカウント名の設定（Set Account Name）]** フィールドに名前を入力するだけで済みます。
5. [登録（Register）] をクリックします。

ロード プロセスが完了すると、ポータルへのアクセスが許可されます。

Stack Automation をご紹介します

ジャーニー セクション（左側のナビゲーション メニューの概要からいつでもアクセスできます）は、デフォルトで、 **Meet Cisco Stack Automation** ポップアップとともにロードされます。これは、 *[ジャーニー（Journey）]*の最初のステップです。



©2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

主な目的は、Stack Automation のスキルを習得し　　、短期間で効果的に強化することです。現在の目標に最も一致するパスを以下から選択します：

パス選択の詳細

- ガイド付き学習の場合： プラットフォームの構造化されたウォークスルーを受信するには、**[進む（Let's Go）]** を 選択 します。
- 即時アクションの場合：**[スキップ（Skip）]**を 選択 して管理サーバーのインストールに直接進みます。オンプレミス環境を構成する準備ができているユーザーに最適です。
- ハンズオン検証の場合：ツアーに参加選択て、サンプル Linux EC2 インスタンスと S3 バケットをプロビジョニングします。これは、お客様自身のインフラストラクチャの準備を必要とせずに、プラットフォームの機能を確認する最良の方法です。

推奨開始点：Stack Automation を初めて使用する場合は、**[ツアーの実施（Take a Tour）]** を選択します。サンドボックス環境を 10 分間で提供し、実稼働インフラインフラストラクチャを危険にさらすことなくセットアップを検証できます。

Stack Automation GUI にログインし、ツアーを参加済みである。ご質問はありますか?

よく寄せられる質問（FAQ）

Q：今すぐ「 スキップ」を選択した場合、後でガイド付きの概要に戻ることはできますか。

A：はい。*[ジャーニー（Journey）]* は、柔軟性があるように設計されています基本的な知識を見逃さなかった場合、「スタートアップ ガイド 」の手順をいつでも再訪問できます。

Q：「ツアーを実施」オプションの利点は何ですか?

A：リスクのないサンドボックス化された　　環境を提供します。サンプルのLinux EC2　　インスタンスと S3 バケットを展開することで、実稼働機器の管理を開始する前に、接続と権限が　　正しく設定されていることを確認できます。

Q： すべてのユーザーに管理サーバーが必要ですか。

A：主にオンプレミス環境で必要です。管理されたクラウド環境　　で排他的に作業している場合は、インストール手順が異なることがあります。お使いのセットアップに基づく特定の手順については、 ジャーニーのプロンプトに従います。

Q：進捗はどのように追跡されますか。

A：「スタートアップガイド」の完了率によって進捗状況が追跡されます。　　タスクを完了すると、その割合が増加し、　基本的なセットアップの習得に どれだけ近づいているか　　を明確に把握できます。

展開パス

Stack Automation は、次の 2 つのプライマリ デプロイメント パスをサポートします：

- オンプレミス（オンプレミス）： ブループリントをオンプレミス環境（Intersight を介した vCenter、ESXi、 UCS 、 Nexus Dashboard、Kubernetes など）に展開します。
- Cloud： AWS や Azure などのパブリック クラウド アカウントにブループリントを展開します。

©2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

- オプション パス：GitOps リポジトリを統合することで、デプロイメント ワークフローを強化できます。このオプションでは、組み込みの共同パイロットまたは外部エージェント ツールを使用してブループリントをカスタマイズまたは作成できます。

オンプレミス展開

オンプレミス デプロイメントには、次の手順が含まれます：

手順	目標（Goal）	成功指標
管理サーバーの展開	SaaS ポータルとプライベート インフラストラクチャの間にセキュアなローカル ブリッジを確立するには、次の手順を実行します：	**[技術情報（Resources）] > [管理サーバー（Management Servers）]** に移動します。展開ステータスが **[接続済み（Connected）]** であることを確認してください。
統合の追加	検出のために既存のインフラストラクチャ（vCenter、 UCS など）にプラットフォームを接続するため。	**[技術情報（Resources）] > [インベントリ（Inventory）]** に移動します。アカウント ステータスが「 **接続済み** 」であり、技術情報が *[表示されている（visible）]* ことを確認します。
ブループリントの展開	最初の OS、VM、またはアプリケーション ソリューションのプロビジョニングを自動化するには、次の手順を実行します。	**[ソリューション ハブ（Solutions Hub）]** の展開ステータスが *[アクティブ（Active）]* です。

管理サーバーの展開

管理サーバーを展開する前に、管理サーバーの概要とアクセス方法について理解しておきます。

管理サーバ

管理サーバーは、ポータルから自動化アーティファクトを取得し、ソリューショ ンハブの選択に基づいてターゲットに対して自動化を展開するオンプレミスのリモート対応マシン（または物理アプライアンス）です。

標準規格のオンプレミス管理サーバーに加えて、システムは Kubernetes クラスタのエージェントもサポートします。

- **自動デプロイメント**：スタック自動化を使用して Kubernetes クラスタを作成すると、システムはこのエージェントを自動的に組み込みます。
- **手動インストール**：オンボーディング プロセスの一環として、既存の Kubernetes クラスタ（オンプレミス、パブリック クラウド、または neocloud）にエージェントを手動でインストールできます。詳細については、「*Kubernetes または Openshift アカウントの追加*」セクションを参照してください。

サーバーは、**[概要（Overview）] > [ジャーニー（Journey）]** ページで管理および表示できます。Stack Automation 管理サーバーをインストール ステップを選択すると、**[技術情報（Resources）]** and **[管理サーバー（Management Servers）]** セクションが表示されます。

初期セットアップ中に **[ツアーの実施（Take a Tour）]** オプションを選択した場合は、リストに管理サーバーが 1 つ表示されます。このサーバーは、特にサンプル ブループリントを展開するために使用されます。ジャーニー ステップで **[さらに表示（View More）]** をクリックすると、そのコンポーネントの詳細な説明を含むペイン内のスライドを開くことができます。

目標：管理サーバーを展開する

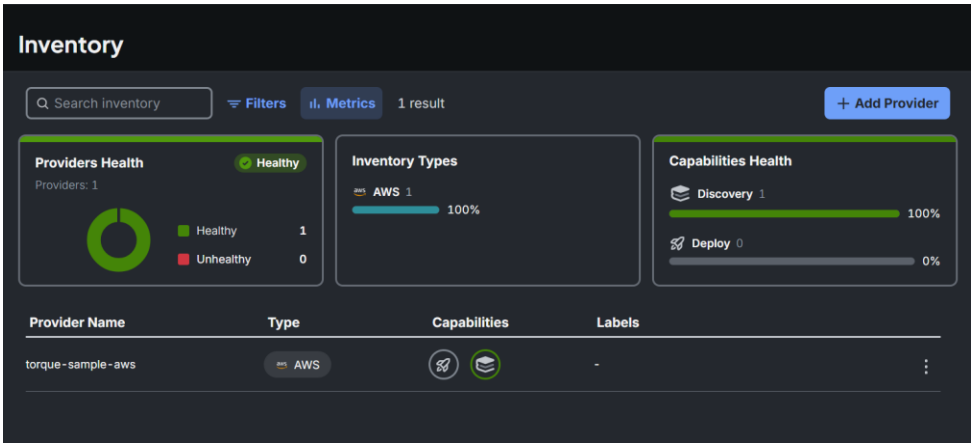
©2026 Cisco and/or its affiliates. All rights reserved.

目的は、VMware を使用してオンプレミス管理サーバーをプロビジョニングして接続することです。このタスクを完了すると、サーバーが自動化アーティファクトを取得してインフラインフラストラクチャに展開できるようになります。

前提条件

- vCenter のログイン情報の準備ができていることを確認します。
- ハイパーバイザへのネットワーク接続を確認します。

接続を確認するには、**[技術情報（Resources）] > [インベントリ（Inventory）]**に移動します。プロバイダーの場合は、**[機能（Capabilities）]** の列を確認します。**[展開（Deploy）]** 要素と **[検出（Discover）]** 要素の両方が 緑色の円で示されていることを確認します。詳細については、アイコンにカーソルを合わせてください。



手順

- **サーバーのプロビジョニング**：ポータルでデプロイメント ファイルを生成します。
- **ログイン情報の保護**： SSH 秘密キーを保存して構成します。
- **OVF テンプレートを展開します**VMware でリモート対応マシンをインポートし、電源をオンにします。

サーバーのプロビジョニング

1. [新しい管理サーバ（New Management Server）] をクリックします。
2. [オンプレミス（On-Premises）] > [VM] > [VMware] を選択します。
   注：現時点では、Nutanix AHV と RedHat KVM はサポートされていません。
3. [Next] をクリックします。
4. 管理サーバーの詳細を指定します。
   - NTP： NTPサーバーの詳細を入力します。このフィールドは必須です。
   - プロキシ：プロキシを使用する場合は、 vCenter/ ESXi サブネットで No プロキシフィールドを設定し、管理サーバーがハイパーバイザに直接接続するようにします。
5. [次へ（Next）] をクリックして、システムがダウンロード可能な .ova ファイルを生成するのを待ちます。

ログイン情報の保護

©2026 Cisco and/or its affiliates. All rights reserved.

1. 提供された SSH 秘密キーをコピーします。これは管理サーバー構成の一部です。
2. テキスト エディタ（メモ帳、TextEdit、nano）を使用して、キーを新しいファイルに貼り付けます。
3. macOS または Linux では、 chmod 600 デモキー.pem を実行して正しいファイル権限を設定します。

OVF テンプレートの展開

1. VMware vCenter にログインします。
2. サーバーをインストールするホスト、サーバー、またはクラスタを右クリックします。
3. [OVF テンプレートの展開（Deploy OVF Template）] を選択します。
4. ウィザードに従って、ダウンロードした .ovf ファイルをインポートします。
5. 管理サーバー仮想マシンの電源をオンにします。

検証

[技術情報（Resources）] > [管理サーバー（Management Servers）]に移動します。デプロイメント ステータスが **[接続済み（Connected）]** であることを確認します。

注：帯域幅幅によっては、ステータスの更新に約 5 分かかる場合があります。

FAQ

Q：元の .ovf ファイルを消失した場合はどうすればよいですか。

A：サーバーを再作成する必要はありません。[技術情報（Resources）] > [管理サーバー（Management Servers）]に移動し、リストでサーバーを見つけて、... をクリックします。（その他のオプション）ボタンをクリックし、「管理サーバ ファイルのダウンロード」を選択して、ファイルを再度取得します。

Q：管理サーバのステータスが「*切断（Disconnected）*」と表示されるのはなぜですか。

A：ネットワーク帯域幅幅によっては、電源をオンにしてからサーバーが接続を確立するまでに最大 5 分かかる場合があります。5 分たってもステータスが「切断（Disconnected）」のままの場合は、 NTP とプロキシの設定を確認してください。

Q：なぜプロキシなしフィールドが重要ですか?

A： vCenter/ ESXiサブネットで No プロキシフィールドを設定することで、管理サーバーはプロキシをバイパスしてハイパーバイザと直接通信します。これは、正常なデプロイメントと継続的な管理に不可欠です。

オンプレミスの技術情報と統合

技術情報一覧は、Intersight、 Nexus Dashboard、Kubernetes、VCenter、AWS、Azure などのインフラストラクチャ アカウントを Stack Automation プラットフォームに接続する管理インターフェイスです。

技術情報一覧には、**[概要（Overview）] > [ジャーニー（Journey）]** ページで **[技術情報 インベントリの追加（Add Resources Inventory）]** ステップを選択することでアクセスできます。このアクションにより、特定のインフラストラクチャ アカウントを接続できる **[技術情報（Resources）] > [インベントリ（Inventory）]** セクションにリダイレクトされます。

一覧には、シスコが管理する AWS クラウド アカウントがデフォルトで含まれています。このアカウントは、クイック ツアー中にサンプル ブループリントを展開するために必要な環境を提供します。

オンプレミス デプロイメントでは、これらの 5 つの統合がサポートされており、それぞれの手順については詳しく説明しています。

- Intersight アカウントを追加

©2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

- vCenter アカウントの追加
- Nexus Dashboard アカウントの追加
- Kubernetes または OpenShift アカウントの追加
- 他の統合

Intersight アカウントを追加

目標： UCSサーバーでオペレーティング システムとプラットフォームのインストール ブループリントをテストするために、Intersight アカウントを追加します。

前提条件

Intersight アカウントからアクセス キーと秘密鍵を取得します（**[設定（Settings ）] → [API キー（API Keys）]**）。

管理サーバーを作成します（このドキュメントで前述したとおり）。

手順

1. 右上隅にある **[プロバイダを追加（Add Provider）]** をクリックします。
2. **[Intersight]** を選択し、**[プロバイダー エイリアス名（Provider Alias Name）]** フィールドにアカウントの名前を入力します。
3. **[シングル ログイン情報設定（Single Credentials Set）]** を選択し、**[次へ（Next）]**をクリックします。
4. 適切な Intersight リージョンを選択、**[アクセス キー（Access Key）]** と **[秘密キー（Secret Key）]** を入力します。
5. スループットを最大化し、デプロイメント時間を短縮するために、技術情報の場所に最も近い管理サーバーを選択。
6. **[完了（Done）]** をクリックします。

[技術情報（Resources）] → [インベントリ（Inventory）] セクションにリダイレクトされます。Intersight アカウントのステータスが「**接続済み**」と表示されます。

検証

Intersight アカウントの「...」オプションをクリックし、技術情報の表示を選択して、Intersight アカウントに登録されている UCS サーバが取得されることを検証します。

UCS サーバーを プラットフォームと統合しましたが、ご質問はありますか。

FAQ

Q： アクセス キーと秘密キーはどこで入手できますか。

A： Intersight アカウントにログインし、[設定（Settings ）] → [API キー（API Keys）] に移動します。詳細な関連情報については、 [Intersight のヘルプ（Intersight Help）] ページを参照してください。

Q：技術情報に近い管理サーバーを選択する必要があるのはなぜですか。

A：地理的または論理的に技術情報に近いサーバーを選択すると、スループットが最大化され、ブループリントデプロイメントに必要な時間が短縮されます。

©2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Q： アカウント ステータスが「接続済み」に変わらない場合はどうすればよいですか。

A：アクセス キーと秘密キーが正しいことを確認してください。キーを活用管理サーバーに接続し、Stack Automation へのインターネット接続を検証します。

Q： UCS サーバが正常に登録されたことを確認するにはどうすればよいですか。

A：**[技術情報（Resources）] > [インベントリ（Inventory）]** セクションに移動し、Intersight アカウントの横にある「...」アイコンをクリックして、**[技術情報の表示（View Resources）]** を選択します。サーバーがリストに表示されている場合は、登録が成功しています。

vCenter アカウントの追加

目標： シスコおよびサードパーティのソリューション用の VMaaS ブループリントとリモート対応アプライアンスを VMware環境に展開するための vCenter アカウントを追加します。

このタスクにより、 VMware 環境が統合され、仮想化ソリューションのデプロイメントが可能になります。開始する前にログイン情報を準備します。

前提条件

- vCenter Server URL（ https://[IP] または https://[domain]の形式）。
- 一覧を検出し、リモート対応マシンを展開する権限を持つユーザー名とパスワード。
- 管理サーバー。

手順

1. 右上隅にある **[プロバイダを追加（Add Provider）]** をクリックします。
2. **[vCenter]** を選択、 **[プロバイダー エイリアス名（Provider Alias Name ）]**フィールドにアカウントの名前を入力します。
3. **シングルログイン情報設定** を選択、 **次へ**をクリックします。
4. お使いの **[vCenter サーバー URL（vCenter Server URL）]**、 **[ユーザー名（Username）]**、および **[パスワード（Password）]** を入力します。
5. **[証明書の検証（Validate Certificate ）]のトグル**を設定します。
   - 有効のままにしてサーバーの証明書を検証します。
   - 自己署名証明書を使用するラボ環境でのみ無効にしてください。
6. スループットを最大化し、デプロイメント時間を短縮するために、リソースの場所に最も近い管理サーバーを選択。
7. **[完了（Done）]** をクリックします。

検証

vCenter アカウントが追加され、両方のステータス アイコンが緑色で強調表示されます。

FAQ

Q： vCenter のユーザー名に必要な権限は何ですか。

A：このアカウントには、 VMware 環境内で一覧を検出し、リモート対応マシンを展開する権限が必要です。

Q： vCenter Server の URL をフォーマットするにはどうすればよいですか。

©2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

A: URL は、https:// で始まり、その後に IP アドレスまたはドメイン名が続く必要があります(例：https://vcenter.example.com)。

Q：「証明書の検証（Validate Certificate）」トグルは、いつ無効にすべきですか。

A：自己署名証明書を使用するラボ環境でのみ、このトグルを無効にしてください。実稼働環境では、セキュアな通信を確保するために有効に維持します。

Q： アカウントが正常に追加されたかどうかを確認するにはどうすればよいですか。

A：両方のステータスアイコンが緑色で強調表示されている場合、望ましい状態になっています。

Q：技術情報に近い管理サーバーを選択する必要があるのはなぜですか。

A： VMware技術情報に地理的または論理的に近い管理サーバーを選択すると、スループットが最大になり、ブループリント デプロイメントに必要な時間が短縮されます。

Nexus Dashboard アカウントの追加

目標： ファブリック インフラインフラストラクチャのブループリントと統合を展開するための Nexus ダッシュボード アカウントを追加するには、以下の手順を実行します。

前提条件：

- Nexus Dashboard URL を取得します。
- API キーの生成： Nexus Dashboard にログインし、管理メニュー（右上）> [API キーの管理（Manage API keys）] > + [API キーの追加（Add API key）] の順に選択します。生成したキーをコピーします。

手順

1. 右上隅にある **[プロバイダを追加（Add Provider）]** をクリックします。
2. **[Nexus Dashboard]** を選択、 **[プロバイダー エイリアス名（Provider Alias Name）]** フィールドにアカウントの名前を入力します。
3. **シングルログイン情報設定** を選択、 **次へ**をクリックします。
4. **[Nexus Dashboard URL]**、 **[ユーザー名（Username）]**、および **[API キー（API Key）]** を入力します。
5. **[証明書の検証（Validate Certificate）]** のトグルを構成します：
   - 有効のままにしてサーバーの証明書を検証します。
   - 自己署名証明書を使用するラボ環境でのみ無効にしてください。
6. スループットを最大化するために、技術情報の場所に最も近い管理サーバーを選択します。
7. **[完了（Done）]** をクリックします。

検証

- [技術情報（Resources）] → [インベントリ（Inventory）] セクションにリダイレクトされ、 Nexus Dashboard アカウントのステータスが接続済みと表示されます。
- アカウントの「...」オプションをクリックし、技術情報の表示を選択して、 Nexus Dashboard によって管理されているスイッチがシステムによって取得されることを検証します。

©2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

FAQ

Q： Nexus Dashboard の API キーはどこで入手しますか?

A： Nexus Dashboard にログインし、右上隅の管理メニューをクリックして、Manage API キーを選択します。[+ API キーの追加（Add API Key）] をクリックして、キーを生成とコピーします。

Q：すべてのスペースに同じ管理サーバーを使用できますか。

A：はい。ただし、 Nexus Dashboard の場合は、スループットを最大化してデプロイメント時間を短縮するために、技術情報にできるだけ近い管理サーバーを選択することをお勧めします。

Kubernetes または OpenShift クラスタを追加します

目標： エージェントベースのアプローチを使用して、既存の Kubernetes または OpenShift クラスタを Stack Automation にオンボードする。

Kubernetes は、エージェントベースのアプローチを使用し、ポッドがクラスタ内で実行されて Stack Automation への接続を確立します。

前提条件

既存の Kubernetes または OpenShift クラスタ。

- ターゲット クラスタへの kubectl アクセス権があることを確認します。
- 名前空間、サービス アカウント、およびクラスタ ロールを作成する権限。これらは、Kubernetes/OpenShift クラスタで作成されます。kubectl auth can-i コマンドを使用します。

手順

1. 右上隅にある **[プロバイダを追加（Add Provider）]** をクリックします。
2. [Kubernetes] を選択、 **[プロバイダー エイリアス名（Provider Alias Name）]** フィールドにアカウントの名前を入力します。
3. **[すべての機能（All Capabilities）]** のステップで生成された kubectl apply コマンドをコピーします。
4. ターゲット クラスタにログインし、コピーしたコマンドを実行して必要な技術情報を作成します。
5. **kubectl get pod -A**を実行して、エージェントのインストールを確認します。2 つの torque-agent-rs ポッドが **[実行中（1/1）（Running (1/1)）]** 状態であることを確認します。
6. Stack Automation に戻り、ドロップダウン リストから適切な **[サービス アカウント（Service Account）** と **[名前空間（Namespace）**を選択して、 **[完了（Done）]**をクリックします。

検証

- **接続ステータス** バーが緑色に変わり、「管理サーバーが正常に接続されました（management server connected successfully）」と表示されます。**[技術情報（Resources）]→ [インベントリ（Inventory）]** のアカウント ステータスは、 **[接続済み（Connected）]**と表示されます。
- Kubernetes アカウントの「...」オプションをクリックし、技術情報の表示を選択して、システムがクラスタから技術情報を取得することを検証します。

FAQ

Q：Kubernetes 接続ステータスに「接続の待機中」と表示されるのはなぜですか。

A：クラスタで **kubectl apply** コマンドを実行するまでは、これは正常な動作です。エージェントポッドの準備が整い、レポートが返されると、ステータスが緑色で表示されます。

©2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Q：Kubernetes エージェントが正しく動作していることを確認するにはどうすればよいですか。

A：クラスタで **kubectl get pod -A** を実行します。実行中（1/1）状態の 2 つの bulk-agent-rs ポッドが表示されます。

スタック自動化用の RedHat ログイン情報の追加

目標： RedHat プル シークレットを Stack Automation Credentials ストアに追加し、ライセンス取得済み OpenShift クラスタのデプロイメントを可能にする。

前提条件

- [RedHat ハイブリッド クラウド コンソール（RedHat Hybrid Cloud Console）] へのアクセス権を持つアクティブな RedHat アカウント。
- RedHat コンソールから取得した有効な RedHat プル秘密。
- Stack Automation インターフェイスの 自動化 メニューにアクセスします。

手順

1. プル シークレットを取得します。

   a) [RedHat ハイブリッド クラウド コンソール（RedHat Hybrid Cloud Console）] にログインします。

   b) **[OpenShift] > [ダウンロード（Download）]**（またはクラスタ作成フロー）に移動します。

   c) **[トークン（Tokens）] > [シークレットをプル（Pull secret）]** を見つけ、**[コピー（Copy）]** または **[ダウンロード（Copy）]** をクリックします。

2. ログイン情報を Stack Automation に追加します。

   a) **[自動化（Automation）] > [統合（Integrations）]**に移動します。

   b)右上隅の **[ログイン情報の追加（+ Add Credentials）]** をクリックします。

   c)適切な **[ログイン情報の種類(Credential Type）]** を選択し、**[次へ（Next）]**をクリックします。

   d) **[ライセンス サブスクリプション（Licensing Subscriptions）]**で、 RedHat を選択して、**[次へ（Next）]**をクリックします。

   e)ログイン情報の一意の [名前（Name）]（ログイン情報エイリアス）を入力します。

   f) プルシークレットを認証フィールドに貼り付けます。

   g) **概要** を確認し、**[完了（Done）]** をクリックします。

FAQ

Q：なぜこれを Stack Automation Credential ストアに保存する必要があるのですか。

A：シークレットをログイン情報ストアに保存すると、自動化アセットがランタイム時にライセンス ログイン情報を安全に取得して使用できるため、手動による介入なしで展開の準拠を維持できます。

Q：ログイン情報が正常に追加されたことを確認するにはどうすればよいですか。

A：完了をクリックすると、ログイン情報が統合リストに表示されます。統合がアクティブな場合、ブループリントデプロイメントの設定時にこのログイン情報エイリアスを選択できます。

Q：複数の RedHat アカウントがある場合はどうすればよいですか。

©2026 Cisco and/or its affiliates. All rights reserved.

A：この手順を繰り返して、複数のログイン情報を追加できます。それぞれに固有のクレデンシャルエイリアスを指定して、デプロイメントプロセス中にそれらを簡単に区別できるようにします。

NVIDIA アカウントの追加

目標： スタック自動化用に NVIDIA（NVAIE）ログイン情報を追加する

前提条件

- NVIDIA 開発者ポータル（NGC）のアクティブなアカウント。
- 生成された GTC/NGC API キー。
- Stack Automation インターフェイスの 自動化 メニューにアクセスします。

手順

1. NVIDIA **GTC API キー**を取得します。

a) NVIDIA アカウントで NVIDIA デベロッパーポータル（NGC） にログインします。

b) アカウントの「**API キー**」セクションに移動します。

c) **[API キーの生成（Generate API Key）]**（GTC/NGC APIキー）をクリックします。

d) 生成されたキーをコピー、安全に保管します。

2. ログイン情報を Stack Automation に追加します。

a) **[自動化（Automation）] > [統合（Integrations）]**に移動します。

b) 右上隅の **[ログイン情報の追加（+ Add Credentials）]** をクリックします。

c) 適切な **[ログイン情報の種類(Credential Type）]** を選択し、 **[次へ（Next）]**をクリックします。

d) **[ライセンス サブスクリプション（Licensing Subscriptions）]**の下の **[NVAIE]**を選択して、 **[次へ（Next）]**をクリックします。

e) ログイン情報の一意の 名前 （**ログイン情報エイリアス**）を入力します。

f) 認証 フィールドに、 **NVIDIA GTC APIキー を**貼り付けます。

g) **概要** を確認し、 **[完了（Done）]** をクリックします。

FAQ

Q： スタックの自動化に NVIDIA GTC APIキーが必要なのはなぜですか。

A：このキーにより、Stack Automation は NVIDIA サービスで認証できます。NVIDIA サービスは、コンテナ イメージをプルして、NIM や GPUaaS などの NVIDIA 固有のブループリントを展開するために必要です。

Q： NVIDIA AP Iキーは安全に保存されますか。

A：はい。ログイン情報を追加すると、キーが Stack Automation ログイン情報ストアに保存され、自動化アセットがブループリントでキーを公開することなく、ランタイム時に安全に取得して使用できるようになります。

Q：NVIDIA API キーが失効または期限切れになった場合はどうすればよいですか。

A： API キーが有効でなくなった場合、 ブループリント の展開は失敗します。[自動化（Automation）] > [統合（Integrations）] メニューに戻り、既存の NVIDIA ログイン情報を見つけて、新しいアクティブな API キーで更新する必要があります。

©2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

オンプレミス ブループリントの展開

Stack Automation GUI で、**[ジャーニー（Journey）]** に移動し、**[ソリューション ハブ（Solutions Hub）]**から **[最初のソリューション ブループリントを展開する（Deploy your first solution blueprint）]**をクリックします。OSプロビジョニング、 VMs、コンテナ、アプリケーションなど、使用可能なブループリントのいずれかを自由に試すことができます。一般的にどのように動作するかを理解する例を次に示します。

ベアメタル Windowsソリューションの展開

目標： Intersight 管理モード（IMM）または Intersight スタンドアロンモード（ISM）のいずれかを使用して、ベアメタルWindowsソリューションのデプロイメントを設定および開始すること。

前提条件：

- Intersight アカウントが Stack Automation に追加されました。
- 管理サーバ。
- デプロイメントに使用できるターゲットサーバー。

手順

1. ソリューションの選択します。

a) **[ソリューションズ ハブ (Solutions Hub)]** の順に移動します。

b)展開するソリューション（ベア メタル Windows など）をクリックします。

c)実装モード（[Intersight 管理モード（Intersight Managed Mode）] または [Intersight スタンドアロン モード（Intersight Standalone Mode）]）を選択します。 ワークフローはどちらのモードでも同じです。

2. 展開設定を構成します。

a) **展開名**を入力します。

b)デプロイメントの **[期間（Duration）]** を設定します。

c)通常、 OS プロビジョニングは持続するため、設定を *常にオンのままに* します。

d) **[ターゲット（Target）]** （前の手順で追加したIntersightアカウント）を選択します。

e)前の手順で構成した **[管理サーバー（Management Server）]** を選択します。

f) 使用可能なサーバーのリストから **[ターゲット サーバー（Target Server）]** を選択します。

3. サーバー設定を設定。

サーバーの設定 セクションで、**[管理者パスワード（Administrator Password）]**を入力します。

4. ネットワークの設定を構成します。

a)ネットワーク設定 セクションで、 **ターゲット サブネット**を入力します。

b)ネットワーク デフォルトの確認：サブネットを指定すると、スマート デフォルトが有効になり、次の表に示す要素が自動的に設定されます。

設定	動作
IP アドレス（IP Address）	ターゲット サブネットから自動的に割り当てられます。
ゲートウェイ	自動検出。

©2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

設定	動作
IMC IP アドレス	自動計算。
VLAN/vNIC（IMM のみ）	デフォルトはネイティブアップリンクVLAN です。

5. （オプション）手動ネットワーク要件を指定します。

   次の表を確認して、追加の設定を手動で指定する必要があるかどうかを判断します。

設定	動作
DNS サーバー	必要に応じて手動で指定します。
VLAN ID	ISM ： Windows 上のタグ管理 VLAN。 IMM： アップリンク VLAN。ネイティブを使用しない場合にのみ指定します。
vNIC A/B VLAN	IMM のみ： 別の VLAN が必要な場合にのみ指定します。

6. 展開を完了させます。**[次へ（Next）]** をクリックして概要を表示します。

   展開するには、お使いの構成を確認し、**[終了（Finish）]** をクリックします。

FAQ

Q： Intersight 管理モードとスタンドアロン モードのどちらを選択しても問題はありませんか。

A：デプロイメント ワークフローはどちらも同じです。既存のインフラストラクチャ管理戦略に合わせてモードを選択します。

Q： ターゲット サブネットを指定しない場合はどうなりますか。

A：サブネットを指定しない場合、 IP アドレス、ゲートウェイ、および IMC IP アドレスを手動で設定する必要があります。これにより、ネットワーク設定エラーや IP アドレスの重複のリスクが高まります。

Q：vNIC VLAN は、いつ手動で指定する必要がありますか。

A：これらを手動で指定する必要があるのは、アップリンクで検出されたネイティブ VLAN とは異なる特定の VLAN が環境に必要な場合のみです。ほとんどの場合、スマート デフォルトにより、これが自動的に処理されます。

クラウド展開

クラウドサーバー（AWS）の導入準備

導入準備 AWS リソース

目標： AWS アカウントを一覧に追加し、プラットフォーム内の AWS 技術情報の管理とモニタリングを可能にすること。

前提条件：

- 管理サーバー
- AWS アカウント情報：

©2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

- アカウント番号
- アクセスキー
- 秘密キー
- ARN の表示

手順

1. オンボーディングの開始

   a)左側のメニューに移動し、**[技術情報（Resources）] > [インベントリ（Inventory）] > [AWS]**を選択します。

   b)アカウントを識別するための **[プロバイダー エイリアス名（Provider Alias Name）]** を入力します。

   c)すべてのスペースでこのアカウントにアクセスできるようにする場合は、「すべてのスペースと共有」 を切り替えます。

   d) **[シングル ログイン情報設定（Single Credentials Set）]** を選択し、**[次へ（Next）]**をクリックします。
2. ログイン情報の設定。

   a) [基本（Basic）] オプション ボタンを選択します。

   b)AWS アカウント情報を使用して、次のフィールドに入力します。

   - アカウント番号
   - アクセスキー
   - 秘密キー
   - ARN の表示
3. 前の手順で作成した [管理サーバー（Management Server）] を選択します。
4. **[完了（Done）]** をクリックして、ウィザードを終了します。

確認

[インベントリ（Inventory）] に移動します。新しいプロバイダー名が **[プロバイダー名（Provider Name）]** のリストに表示されていることを確認します。

FAQ

Q：「View ARN」とは何ですか。また、どこに表示されますか。

A：View ARN（Amazon 技術情報ネーム）は、AWS 技術情報の一意の識別子です。通常、これは、AWS IAM コンソールのアカウントに関連付けられた特定のロールまたはポリシーの下にあります。

ARN 詳細については、公式の「*AWS ドキュメント*」を参照してください。

Q：「すべてのスペースと共有」を切り替えない場合はどうなりますか。

A：これをオフのままにすると、AWS 技術情報は現在作業している特定のスペース内でのみ表示および管理可能になります。オンに切り替えると、すべてのスペースでグローバルにアカウントを使用できるようになります。

Q：「完了」をクリックしましたが、インベントリ リストにプロバイダー名が表示されません。どうすればよいでしょうか。

©2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

A：インベントリページを更新します。それでもプロバイダーが表示されない場合は、AWS ログイン情報（アクセス キーと秘密キー）が有効であり、管理サーバーが正しく構成されていることを確認します。

ブループリントの展開

Nexusブループリントの展開

目標： Cloudカテゴリから**Nexus**ブループリントを AWS 環境に展開し、 Nexus Dashboard UI にアクセスする。

前提条件

- インベントリ に AWS 技術情報を導入準備（「AWS 技術情報のオンボーディング」の手順を参照します）。
- プラットフォームの **[ソリューションズ ハブ（Solutions Hub）]** にアクセスします。

手順

1. ブループリントを選択
   - **[ソリューションズ ハブ (Solutions Hub)]** の順に移動します。
   - [すべてのスペース（All Spaces）] を選択し、値 Nexus を検索して、ブループリントをフィルタ処理します。
   - Cloud カテゴリを開きます。
   - 目的のブループリントにカーソルを合わせて、 [起動（Launch）] をクリックします。
2. 展開設定を構成します。
   - 展開の **[名前（Name）]** を入力します。
   - ブループリントの **[期間（Duration）]** を選択します。
   - **[次へ（Next）]** をクリックします。
3. クラウド パラメータを設定します。
   - それぞれのドロップダウンリストから **[リージョン（Region）]** と **[VPC]** を選択します。
   - AWS 環境から取得した値に基づいて、残りのフィールドに入力します。
   - [Next] をクリックします。
4. 展開を検証と開始します。
   - ブループリントの設定 が正しいことを確認します。
   - **[完了（Finish）]** をクリックしてデプロイメントを開始します。
5. ダッシュボードを監視してアクセスする。
   - デプロイメントが完了するまで数分待ちます。 *チェック*のステータスが アクティブ に移行します。
   - **[概要（Overview）]** をクリックしてデプロイメントの詳細を視覚化します。
   - **アクセスの詳細** カードを見つけて、**[ログイン（Login）]** リンクをクリックします。
   - ユーザー名 *[管理（admin）]* と、 の構成で定義したパスワードを使用して**Nexus**ダッシュボードにログインします。

FAQ

©2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Q：「エージェント」フィールドが事前に入力されているのはなぜですか。

A：Cloud カテゴリのベータ展開の場合、システムは「ホステッド エージェント モード」を使用します。これは、エージェントを手動で設定することなく CloudFormation の自動化がサポートされるスマート デフォルトです。

Q：「チェック」がアクティブになるまでにどのくらい時間がかかりますか。

A：通常、デプロイメントでは数分以内にアクティブな状態への移行がチェックされます。10 分以上非アクティブのままである場合は、AWS 接続を確認し、VPC 設定が正しいことを確認します。

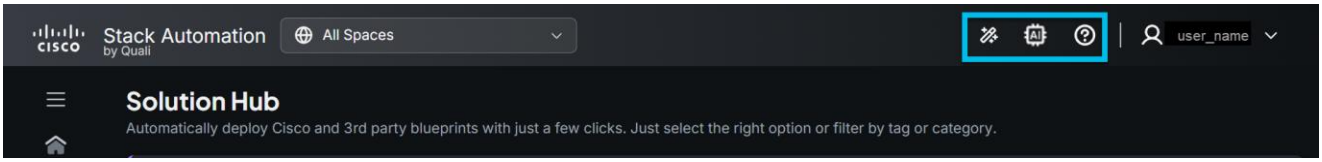
Q：「完了」をクリックした後、デプロイメント名を変更できますか。

A：いいえ。デプロイメントが開始されると、名前はロックされます。変更する必要がある場合は、デプロイメントをキャンセルして、再度起動プロセスを開始する必要があります。

付録

ヘッダー アイコン

青いボックスに示されているヘッダーアイコンを使用すると、タスクが簡単になります。



- **[Copilot]** アイコンをクリックして、スタック自動化 AI の一部であるコパイロットアシスタントを呼び出すことができます。ヘルプを利用するには、[チャットを開始する（Start a chat）] をクリックします。
- **[AI 統合（AI integrations）]** アイコンをクリックして、AI ツールを Stack Automation に接続します。

  [サポート（Support）] アイコンをクリックし、使用可能なオプションから選択します。**ドキュメントの確認（Explore Documentation）]** をクリックして、[Stack Automation のヘルプ ページ（Stack Automation help page）] に移動します。ヘルプ ページには、Stack Automation のすべての側面に関する詳細情報と技術情報が表示されます。

チェックリスト

曜日	アクティビティ	成功指標
基準日	アカウントとスペースの作成	ユーザーはログインして、割り当てられたスペースにアクセスできます Click or tap to enter a date.

法的情報

シスコおよびシスコのロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の国における登録商標または商標です。シスコの商標の一覧については、https://www.cisco.com/c/ja_jp/about/legal/trademarks.html をご覧ください。記載されているサードパーテ

ィの商標は、それぞれの所有者に帰属します。「パートナー」という言葉が使用されていても、シスコと他社の間にパートナー関係が存在することを意味するものではありません。（1110R）。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアルの中の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際の IP アドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

© 2026 Cisco Systems, Inc. All rights reserved.

米国本社
Cisco Systems, Inc.
カリフォルニア州サンノゼ

アジア太平洋本社
Cisco Systems (USA), Pte. Ltd.
シンガポール

ヨーロッパ本社
Cisco Systems International BV
Amsterdam, The Netherlands

2023 年 11 月発行

© 2023 Cisco and/or its affiliates. All rights reserved.

Cisco および Cisco ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の国における商標または登録商標です。シスコの商標の一覧については、www.cisco.com/jp/go/trademarks をご覧ください。記載されているサードパーティの商標は、それぞれの所有者に帰属します。「パートナー」または「partner」という言葉が使用されていても、シスコと他社の間にパートナーシップ関係が存在することを意味するものではありません。1175152207 10/23

Printed in USA

Cxx-xxxxxx-xx 01/20

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。