Smart Software Manager オンプレミス インストールガイド

バージョン 8 リリース 202006

初版：2015/02/16
最終変更日：2020/7/1

米国本社
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com/jp
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任となります。

対象製品のソフトウェアライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

シスコが導入する TCP ヘッダー圧縮は、カリフォルニア大学バークレー校（UCB）により、UNIX オペレーティング システムの UCB パブリック ドメイン バージョンの一部として開発されたプログラムを適応したものです。

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよび上記代理店は、商品性、特定目的適合、および非侵害の保証、もしくは取り引き、使用、または商慣行から発生する保証を含み、これらに限定することなく、明示または暗黙のすべての保証を放棄します。

いかなる場合においても、シスコおよびその代理店は、このマニュアルに適用できるまたは適用できないことによって、発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコおよびその代理店に知らされていても、それらに対する責任を一切負わないものとします。

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。マニュアル内の例、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。

目次

はじめに

ここでは、このマニュアルの目的、構成、および関連製品やサービスに関する詳細の入手方法について説明します。具体的な内容は次のとおりです。

目的

このドキュメントでは、SSM オンプレミスに固有のソフトウェア機能の概要について説明します。このマニュアルは、実行できるソフトウェア機能のすべてを説明する完全ガイドではなく、このアプリケーションに特化したソフトウェア機能だけを説明します。

関連資料

次のマニュアルも、SSM オンプレミスを設定するうえで役立てることができます。このマニュアルには SSM オンプレミスの重要な情報が記載されており、オンラインで入手できます。

Cisco Smart Software オンプレミスに関連するその他のガイド、リファレンス、リリースノートを次に示します。

- Cisco Smart Software オンプレミス クイック スタート ガイド
- Cisco Smart Software オンプレミスユーザガイド
- Cisco Smart Software オンプレミス コンソール ガイド
- Cisco Smart Software オンプレミスリリースノート（バージョン 8 リリース 202004）

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	説明
太字	太字のテキストは、1 つ以上のステップで使用されるコマンドとキーワードを示します。
イタリック体	イタリック体のテキストは、ユーザが値を入力する引数、または別のドキュメントからの引用を示します。
[x]	省略可能な要素（キーワードまたは引数）は、角カッコで囲んで示しています。

表記法	説明
[x | y]	いずれか 1 つを選択できる省略可能なキーワードや引数は、角カッコで囲み、縦棒で区切って示しています。
{x | y}	必ずいずれか 1 つを選択しなければならない必須キーワードや引数は、波カッコで囲み、縦棒で区切って示しています。
[x {y | z}]	省略可能な要素や必須の要素内に、さらに省略可能な選択肢や必須の選択肢を含める場合は、角カッコや波カッコを入れ子にして示しています。角カッコ内の波カッコと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
変数	ユーザが値を入力する変数であることを表します。イタリック体が使用できない場合に使用されます。
文字列	引用符を付けない文字列。文字列の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて文字列とみなされます。

例では、次の表記法を使用しています。

表記法	説明
screen フォント	スイッチが表示する端末セッションおよび情報は、screen フォントで示しています。
太字の screen フォント	ユーザが入力しなければならない情報は、太字の screen フォントで示しています。
イタリック体の screen フォント	ユーザが値を指定する引数は、イタリック体の screen フォントで示しています。
< >	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[ ]	システムプロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。

表記法	説明
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

このマニュアルでは、次の表記法を使用しています。

注	注釈を意味しています。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。
注意	注意が必要なことを示します。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

マニュアルの入手およびサービスリクエストの送信

マニュアルの入手、Cisco Bug Search Tool（BST）の使用、サービスリクエストの送信、追加情報の収集の詳細については、『更新情報』を参照してください。

シスコの新しい技術情報や改訂された技術情報を直接デスクトップで受信することをご希望の場合は、シスコ製品資料の更新情報RSS フィード（What's New in Cisco Product Documentation RSS feed）にご登録ください。

注： RSS フィードは無料のサービスです。

Smart Software Manager オンプレミスの概要

Cisco Smart Software Manager オンプレミス（Cisco SSM オンプレミス）は、スマートライセンス対応の製品インスタンスを、cisco.com でホストされている Cisco Smart Software Manager に直接接続せずに、お客様が製品およびライセンスをオンプレミスで管理できるようにするためのスマート ライセンシング ソリューションです。

ソフトウェアのダウンロード

以下のステップに従って SSM オンプレミスソフトウェアをダウンロードしてください。

ステップ	アクション
ステップ 1	次の URL に移動します。 https://software.cisco.com/download/home
ステップ 2	[製品の選択（Select a Product）] フィールドに、「**Smart Software Manager サテライト（Smart software Manager satellite）**」と入力します。
ステップ 3	[最新リリース（Latest Release）] の左側の列で、[8-202004] を選択します。
ステップ 4	次の使用可能なダウンロードファイルから選択します。 • SSM_On-Prem_8-202004.iso SSM オンプレミス ライセンス サーバの新規インストールを実行するために使用します。 • SSM_On-Prem_8-202004_Upgrade.zip 既存の SSM オンプレミス ライセンス サーバをこのバージョンにアップグレードするために使用します。 • SSM_On Prem_8 202004_Full .zip インストールファイル、アップグレードファイルなど、このバージョンの SSM オンプレミス ライセンス サーバに関連するすべてのドキュメントが含まれています。
ステップ 5	ダウンロードが完了したら、zip ファイルが保存されているディレクトリに移動し、**ファイル**を右クリックして、[イメージの解凍（unzip image）] を選択します。

ソフトウェアのパッケージ

SSM オンプレミスのユニバーサル ISO のインストールパッケージは、次のコンポーネントで構成されています。

- SSM オンプレミス

注： このユニバーサル ISO 形式により、さまざまなインストールメディアタイプにエクスポートできます。ISO イメージを他のイメージタイプにエクスポートする際は、お客様の責任で実施してください。シスコはサポートしておりません。

システムの制限と拡張性

製品とユーザの拡張性：

- 最大 500 のローカルアカウント
- 最大 1,000 のローカルのバーチャルアカウント
- 1 つのライセンスを使用して、アカウントごとに最大 25,000 の製品キャパシティで、合計 30 万台まで製品インスタンスを登録できます。30 万台の製品を登録するには、製品を 12 以上のアカウントに分散する必要があります。

注： 25,000 台の製品インスタンスのアップロードには 2 時間弱かかります。

サポートされる Web ブラウザ

次の Web ブラウザがサポートされています。

- Chrome 36.0 以降のバージョン
- Firefox 30.0 以降のバージョン
- Internet Explorer 11.0 以降のバージョン

注： ブラウザで JavaScript を有効にする必要があります。

システム要件

Cisco スマートアカウントへのアクセス

このセクションで説明するタスクを進める前に、Cisco スマートアカウントにアクセスできること、およびスマートアカウント管理者またはバーチャルアカウント管理者のいずれかのロールを持っていることを確認してください。

ハードウェアベースの導入要件

SSM オンプレミスは、Cisco UCS C220 M3 ラックサーバなどの物理サーバ、または次の要件を満たすハードウェアベースのサーバに導入できます。

	小規模	中規模	大規模	最大
製品	4,000	50,000	100,000	300,000
ハードディスク	200 GB	200 GB	200 GB	200 GB
メモリ	8 GB	8 GB	16 GB	16 GB
vCPU	2 vCPU	4 vCPU	6 vCPU	8 vCPU

仮想マシンベースの導入要件

SSM オンプレミスでは、次のバージョンの VMware vSphere Web クライアントがサポートされています。

- VMware vSphere Web クライアント 5.5 ～ 6.5

導入用の仮想マシンを作成する場合は、OS タイプが「Linux」に設定され、ゲスト OS が「CentOS 7 64 ビット」または「その他の Linux 64 ビット」のいずれかに設定されていることを確認します。仮想マシンの構成は、以下の表に示す設定要件を満たしている必要があります。

	小規模	中規模	大規模	最大
製品	4,000	50,000	100,000	300,000
ハードディスク	200 GB	200 GB	200 GB	200 GB
メモリ	8 GB	8 GB	16 GB	16 GB

vCPU	2 vCPU	4 vCPU	6 vCPU	8 vCPU

サポートされている VMware 機能と操作

注： VMware には、アプリケーションをインストールするためのファームウェアオプションが 2 つあります。

- UEFI
- BIOS

SSM オンプレミスのインストールでは、**レガシーBIOS モードのみをサポート**しています。セキュリティ上の理由で EFI を使用してアプリケーションをインストールする必要がある場合は、SSM をインストールすることはできません。

VMware は、仮想アプリケーションを管理し、クローニング、移行、シャットダウン、再開などの操作を実行できるさまざまな機能と操作をサポートしています。

これらの操作の一部では、VM のランタイム状態が保存され、再起動時に復元されます。ランタイム状態にトラフィック関連の状態が含まれている場合、ランタイム状態を再開または再生すると、追加のエラー、統計情報、またはメッセージがユーザのコンソールに表示されます。保存された状態が設定のみに基づいて復元される場合は、これらの機能と操作を問題なく使用できます。

次の VMware 機能と操作は、シスコ クラウド サービス ルータ（CSR）1000v（SSM オンプレミスで使用される製品インスタンス）のすべてのバージョンでサポートされていません。ただし、パケットのドロップ、接続の切断、その他のエラー統計情報が発生するリスクを承知の上で、使用および実行することは可能です。

- クローニング
- 移行

VMware ESXi 設定のパフォーマンス向上

次の手順を実行することで、VMware ESXi 設定のパフォーマンスを向上させることができます。

- VMware ESXi の電源管理を無効にします。
- VMware ESXi で電源管理を無効にするには、[高パフォーマンス（High-Performance）] 設定を選択します。

詳細については、VMware のマニュアル [英語] を参照してください。

Cisco Smart Software Manager オンプレミスの導入

注： SSM オンプレミスの導入とインストールに関する簡潔な説明については、『Cisco Smart Software オンプレミス クイック スタート ガイド』を参照してください。

SSM オンプレミス（Enhanced Edition 6.x 以降）では、以前のバージョン（Classic Edition 5.x まで）と比較してアーキテクチャおよびユーザインターフェイスが一新されています。SSM オンプレミスでは次のことが可能です。

- https://< IP アドレス >:8443/ からライセンスワークスペースにアクセスする
- https://< IP アドレス >:8443/admin から管理ワークスペースにアクセスする

SSM オンプレミスでは、新しい登録および同期手順、ライセンス管理用の新しいシステムロールおよびロールベース アクセス コントロール（RBAC）、外部認証、syslog、プロキシ、およびその他の機能を用意しています。Cisco Smart Software Manager オンプレミスユーザガイドを確認して、新しいシステムアーキテクチャ、ユーザインターフェイス、アカウント、セットアップ、および操作の変更点について理解することを推奨します。

導入シーケンスの概要

開始前の準備

SSM オンプレミスをインストールして導入する前に以下のリソースを確認してください。

1. Software.cisco.com から ISO イメージをダウンロードする。
2. １つの専用の IP アドレスの確保（HA クラスタ構成の場合は複数の IP アドレス）
3. 適切なネットマスク
4. DNS (Domain Name Server) アドレス
5. 大文字と小文字、数字、特殊文字を混合した 15 文字以上のパスワード(例えば CiscoAdmin!2345）
6. NTP サーバアドレス

更に、ハードウェア上にインストールする場合は以下のものが必要です。

7. ISO からの USB イメージ
8. 最初に USB から、次にハードディスクからブートする様に設定されたハードウェア BIOS

9. マスターブートレコードを使ってブートする様に設定されたハードウェア BIOS（レガシーBIOS モード）

SSM オンプレミスの運用を開始し、スマートライセンス機能にアクセスするためには、次の 5 つのフェーズを（リストされた順序で）完了する必要があります。

1. **メディアのインストール**：インストールガイドのインストール手順に従って、オンプレミスを導入します（以下を参照）。
2. **SSM オンプレミスの設定**：このフェーズでは、次の手順を実行します。
   a. SSM オンプレミスで共通名を設定（[セキュリティ（Security）] ウィジェット > [証明書（Certificates）]）
   b. NTP サーバの同期（[設定（Settings）] ウィジェット > [時刻設定（Time Settings）]）
3. **新規ローカルアカウントの登録**：新規ローカルアカウントが設定されたら、少なくとも 1 つのローカルアカウントを作成し、それをシスコに登録する必要があります。これは、オンプレミス管理ワークスペースの [アカウント（Account）] ウィジェットにある [新規アカウント（New Account）] タブで実行します（『Smart Software Manager オンプレミスユーザガイド』を参照）。または、ライセンスワークスペースにログインした後に新しいローカルアカウントを要求することもできます。
4. **新規ローカルアカウントの承認**：新規ローカルアカウントが要求されると、オンプレミス管理ワークスペースの [アカウント（Account）] ウィジェットにある [アカウント要求（Account Request）] タブにリストされます。次に、スマートアカウントを使用している Cisco Smart Software Manager のバーチャルアカウントを使用して、ローカルアカウントの登録を完了するための適切な方法を選択する必要があります（『Smart Software Manager オンプレミスユーザガイド』を参照）。
5. **アカウントの同期**（[同期（Synchronization）] ウィジェット）

このプロセスが完了すると、製品の登録、ローカルのバーチャルアカウントまたはユーザの作成、製品とライセンスのステータスの表示/転送など、スマートライセンス機能の使用を開始できます。

メディアのインストール

インストールを開始するには、Cisco Smart Software Manager オンプレミス ソフトウェア パッケージの **ISO ファイル**をダウンロードする必要があります。https://software.cisco.com/download/home で Cisco Smart Software Manager を検索し、パッケージを入手します。

.iso ファイル（USB）を使用してハードウェアに手動で展開する

USB ドライブを使用して ISO ファイルを手動で展開するには、次の手順を実行します。

ステップ	アクション
ステップ 1	**ダウンロードした ISO ファイル**を USB に転送して、ブート可能な USB ドライブ

	を作成します（Linux の dd コマンドなどを使用）。
ステップ 2	サーバに**インストール用 USB** を挿入して、システムのインストールを開始します。 • 最初に USB から、次にハードディスクからブートする様に設定されたハードウェア BIOS • マスターブートレコードを使ってブートする様に設定されたハードウェア BIOS（レガシーBIOS モード）
ステップ 3	メディアの読み込みが完了するのを待ち、『SSM オンプレミス キックスタートガイド』を参照して、SSM オンプレミスのインストールを続行します。 **注：**インストール手順の中で使用する NIC をメモしていることを確認してください。

.iso ファイル（VMware ESXi）を使用して VM を手動で作成する

次の手順には、Cisco SSM オンプレミスの展開に関する一般的なガイドラインが記載されていますが、実行する必要がある正確な手順は、ご使用の VMware 環境と設定の特性によって異なる可能性があります。この手順と画面は、VMware ESXi 6.0 以降のバージョン に基づいています。VMware の導入に必要な具体的なインストール手順については、VMware のユーザガイドを参照してください。

VMware ESXi 6.0 以降のバージョンを使用して VM を作成するには、次の手順を実行します。

ステップ	アクション
ステップ 1	**ソフトウェアパッケージ**を VMware データストアにコピーします。
ステップ 2	V-sphere にログインして VMs and Templates をクリックします。
ステップ 3	右クリックでドロップダウンメニューから[新しいフォルダ（New Folder）] を選択して新しいフォルダーを作成します。
ステップ 4	フォルダー上で右クリックして、[新しい仮想マシンの作成（Create a New Virtual Machine）]オプションを選択して、[次へ（Next）]をクリックします。
ステップ 5	仮想マシンの名前を入力して[次へ（Next）]をクリックします。
ステップ 6	[ストレージ（Storage）]で、VM に使用する**データストア**を選択し、[次へ（Next）]をクリックします。
ステップ 7	仮想マシンバージョンで、仮想マシンバージョン 8 を選択して、[次へ（Next）]をクリックします。
ステップ 8	Compute resource を選択して、[次へ（Next）]をクリックします。
ステップ 9	Storage を選択して、[次へ（Next）]をクリックします。
ステップ 10	コンパチビリティを選択して、[次へ（Next）]をクリックします。
ステップ 11	**ESXi 6.0 or later** または **ESXi 6.5 or later** を選択します。
ステップ 12	ゲスト OS を選択して、[次へ（Next）]をクリックします。
ステップ 13	ゲスト OS の選択では、family として Linux を選択します。 ゲスト OS バージョンでは 64-bit version : CentOS 7(64 bit)か Other 2.6x Linux(64 bit) を選択します。
ステップ 14	[CPU（CPUs）]で、[4 コア（4 Cores）]の設定を選択します。実際の vCPU 設定は、規模の要件によって異なります。 **注**：選択した仮想ソケット数にかかわらず、ソケットあたりのコア数は常に 1 に

ステップ	アクション
	設定する必要があります。たとえば、4 つの vCPU 構成では 4 ソケット、ソケットあたり 1 コアとして設定する必要があります。
ステップ 15	ハードウェアのカスタマイズです。 a. CPUs : 2 b. ソケットあたりのコア数： 2 c. メモリ： 8 GB d. 新規ハードディスク：200 GB Thin Provision e. 新規ネットワーク：E1000 アダプター、電源 ON 時に接続 f. ネットワークデバイスの追加時は Add New Device と Network Adapter（上記 e で指定したのと同じ設定）を選択します。 g. 新規 CD/DVD ドライブ：[データストア ISO ファイル（Datastore ISO file）] と、**uploaded ios と connect at power on** を選択します。
ステップ 16	[次へ（Next）]をクリックします。
ステップ 17	設定を確認して Finish をクリックします。

Cisco Smart Software Manager オンプレミスの導入

NOTE: SSM オンプレミスを導入するのに必要な情報は開始前の準備 を参照してください。

メディアをブートした後、KickStart スクリーンで SSM On-Prem ライセンスサーバソフトウェアをインストールできるようになる前に初期設定値の入力が求められます。この時の入力を完了するために以下の情報が事前に必要です。

- 使用予定のサーバのホスト名
- セキュリティプロファイル(DISA STIG Profile を推奨)
- IP アドレス情報
- ネットマスクまたはサブネットに対応するプレフィクス
- ゲートウェイ IP アドレス
- DNS サーバ IP アドレス
- SSH シェルのパスワード: 大文字と小文字、数字、特殊文字を混合した 15 文字以上のパスワード(例えば CiscoAdmin!2345）

ISO image を以下の手順でインストールします。

ステップ	Action
ステップ 1	Cisco SSM On-Prem Quick Start Installation UI で以下の情報を入力してください。 • ホスト名のセットアップ • システム区分： Unclassified（デフォルト）, Confidential, Secret, Top Secret. 選択した区分はバナーとしてコンソールメッセージに表示されます。 • FIPS 140-2 Mode: Not changeable
ステップ 2	システムプロファイルを選択します。: (詳細はシステムプロファイルの選択 を参照) • Standard Profile • DISA STIG Profile を選択すると OS (CentOS 7.5.1804) は STIG Mode となります。
ステップ 3	**IPv4** または **IPv6** ネットワークの設定 • アドレス • ネットマスク / プレフィクス • ゲートウェイ
ステップ 4	**DNS 設定**
ステップ 5	Click **OK**.

ステップ	Action
ネットワークの設定が完了したら SSM On-Prem のインストールが可能になります。次のステップに進む。	
ステップ 6	**システムパスワードの設定**が表示されます。SHELL にアクセスするセキュアな **Linux SSH パスワード**を入力してください。 **注意:** これは UI admin のパスワードとは別のものです。回復不能のパスワードですので安全な場所に保管してください。
ステップ 7	**パスワード**を再入力します。
ステップ 8	Click **OK**. 初期セットアップは完了です。アプリケーションを起動する前に、インストールが終了するのをお待ちください。（約 10-15 分程度）

NOTE: SSM On-Prem システムが自動的にブートアップする様に、インストールの後サーバがリブートした後、ISO イメージをシステムから dismount することをお勧めします。

システムプロファイルの選択

SSM On-Prem には 2 つのプロファイルがあります。

- **Standard Profile**: On-Prem コンソールを使うために centos shell がデフォルトで提示されます。このプロファイルは国防以外の組織のための標準的なセキュリティを提供します。
  - セキュリティパッチを強化した SHA 256 signing key
  - LDAP Secure SSM On-Prem は TLS (Transport Layer Security) およびプレーンテキストによるログインをサポートします。LDAP はホスト、ポート、バインド DN の正しい設定を要求します。これらのパラメータが未入力であったり正しくない場合、エラーメッセージが表示されます。
  - その他に以下のセキュリティ機能が含まれます：
    - インストール中のシステムパスワードの変更が必須
    - アドミンパスワードをデフォルトに戻すことを許可しない
    - ユーザの追加・削除はイベントログに記録される
    - 10 分間ユーザがアイドル状態になると自動的にログアウトする

- **DISA STIG Profile**: ssh で shell を使用している場合、On-Prem コンソールではホワイトリストにあるコンソールコマンドだけが使用可能となるよう制限されるホワイトリストコンソールに置かれます。STIP コンプライアンスが必要な場合、このセキュリティプロファイルを選択します。国防総省のセキュリティシステムに必要な機能が有効化されます。更に、このプロファイルの選択により STIG (Security Technical Implementation Guide) コンプライアンスにも準拠します。STIG 機能とは：

- ブラウザの認証とそのフレームワークが有効な認証管理。この機能によりユーザアのローカルディレクトリを通じて自分の認証をインポートできます。
- パスワードの強度をセットしたり rest/recovery ワークフローを提供します。セキュリティウィジェット内に新しいタブが追加され、パスワードの有効期限や強度の設定が可能となります。
- ADFS: OAuth ADFS adds OAuth Active Directory Federation Services support for LDAP.
- Active directory (OAUTH2): Adds Active Directory Federation Services support in addition to Active Directory support to LDAP group import.

SSM オンプレミスでのローカルアカウントの登録

SSM オンプレミスのセットアップが完了したら、SSM **オンプレミス管理ワークスペース**にログインし、最初のアカウントを登録します。

次の手順を実行して、SSM オンプレミスを Cisco スマートアカウントに登録し、スマートライセンス機能へのアクセスを有効にします。

次の URL を使用して、Cisco SSM オンプレミス**管理**ワークスペースを開きます。

https://< IP アドレス >:8443/admin/

ログイン画面が表示されたら、次のクレデンシャルを使用してログインします。

- 管理者ユーザ ID：**admin**
- 管理者の初期パスワード：**CiscoAdmin!2345**

管理者の**新しいパスワードを入力**するように求められます。入力後、その**新しいパスワード**を使用してログインするように求められます。

注： 10. セキュリティ上の理由により、新しい管理用ローカルアカウントを作成すると、すぐに**管理者パスワード**を変更するか、そのアカウントを無効にするように求められます。パスワードは大文字と小文字、数字、特殊文字を混合した 15 文字以上のパスワード(例えば MyOnpremPassword123!）でなければなりません。

共通名の設定

SSM オンプレミスの URL は、共通名（CN）に使用されます。共通名（CN）は管理ワークスペースの [セキュリティ（Security）] ウィジェットで設定し、SSM オンプレミスの完全修飾ドメイン名（FQDN）、ホスト名、または IP アドレスとして入力します。

注： 共通名は、Call Home 設定の一部として製品で使用されるものと**一致する必要があります。**

共通名を設定するには、次の手順を実行します。

ステップ	アクション
ステップ 1	**SSM オンプレミスの管理ワークスペース**（https://< IP アドレス >:8443/admin）に移動します。 **注**：この IP アドレスは、インストール時に使用される値です。さらに、HA クラ

ステップ	アクション
	スタの一部である場合は、仮想 IP アドレスを使用する必要があります。
ステップ 2	[セキュリティ（Security）] ウィジェットを開きます。
ステップ 3	[証明書（Certificates）] タブで、[ホストの共通名（Host Common Name）]（IP アドレス）を入力します。 **注**：この値は、製品の宛先 URL に使用する値と一致する必要があります。デュアルスタック（IPv4 と IPv6 の両方）を導入する場合、この値は IP アドレスではなく FQDN である必要があります。
ステップ 4	[保存（Save）] をクリックします

NTP サーバの設定

時刻設定は、手動または NTP との同期によって行えます。お使いの SSM オンプレミスシステムのタイムゾーンを UTC+0 に設定し、すべてのタイムスタンプを UTC 時間で表示することもできます。UTC+ 時差を設定すると、タイムスタンプはシステムの現地時間で表示されます。

注：

時刻の設定を変更すると、スケジュールされたすべてのバックグラウンドジョブも、時刻の変更を反映するように再スケジュールされます。

時刻を設定するには、次の手順を実行します。

ステップ	アクション
ステップ 1	**SSM オンプレミスの管理ワークスペース**（https://< IP アドレス >:8443/admin）に移動します。 **注**：この IP アドレスは、インストール時に使用される値です。HA クラスタの一部である場合は、仮想 IP アドレスを使用する必要があります。
ステップ 2	[設定（Settings）] ウィジェットを開き、[時刻設定（Time Settings）] タブを選択します。
ステップ 3	ドロップダウンメニューから [タイムゾーン（Time Zone）] を選択し、次の手順を実行します。

ステップ	アクション
	a. [手動で時刻を設定（Manually Set Time）] のトグルスイッチを [オン（On）] にスライドします。 b. [日付（Date）] を選択します（デフォルトは現在の日付）。 c. 時間、分、秒を設定します。

ステップ	アクション
ステップ 4	NTP サーバと同期する場合は、次の手順で [NTP サーバと同期（Synchronize With NTP Server）] を有効にします。 a. [NTP サーバと同期（Synchronize With NTP Server）] のトグルスイッチを右側にスライドします。 b. [サーバアドレス 1（Server Address 1）] に、**有効な IP アドレス**または完全修飾ドメイン名（FQDN）を入力します。 c. [ポート 1（Port 1）] に有効な**ポート**を入力します。 d. （オプション）2 つ目の NTP サーバがある場合は、[サーバアドレス 2（Server Address 2）] に、**IP アドレス**または **FQDN**、および**ポート**を入力します。 **注**：NTP サーバのアドレス設定を保存する際、SSM オンプレミスは、誤った IP アドレスがあるかどうかをチェックします。サーバ 1 のアドレスに接続できないことをシステムが検出すると、サーバはチェックを停止し、サーバ 1 のエラーを赤色で表示します。サーバ 1 のエラーが表示されている場合、SSM オンプレミスは、それが可能な場合でも、サーバ 2 に接続できるかどうかを確認**しません**。反対に、システムがサーバ 1 に接続できる場合は、SSM オンプレミスはサーバ 2 への接続を試み、接続できない場合はサーバ 2 のエラーを返します。
ステップ 5	1 台または両方のサーバに対して NTP/Chrony 認証を使用するには、次の手順を実行します。 a. セレクタを右にスライドさせて [サーバ 1 に対して NTP/Chrony 認証を使用する（Use NTP/Chrony Authentication for Server 1）] を有効にしてから、ドロップダウンリストから [NTP キータイプ（NTP Key Type）] を選択します。選択肢は、SHA1、SHA256、SHA384、SHA512 です。 **注**：セキュリティ上の理由から、SHA256、SHA384、SHA512 を選択することを強くお勧めします（SHA1 は安全であるとはみなされなくなりました）。 b. 一意の**キー ID** と**キー**を入力します（16 進数キーを使用する場合は、[16 進数（HEX）] のチェックボックスをオンにします）。 **注**：ツールチップには、SHA1、SHA256、SHA512 に使用できる 16 進数の値、および ASCII キーの範囲に関する情報が表示されます。 **注**：NTP/Chrony サーバが複数ある場合は、[サーバアドレス 2（Server Address 2）]、[ポート 2（Port 2）] を使用し、認証が使用されている場合は、2 つ目のアドレスの [キータイプ 2（Key Type 2）]、[キーID 2（Key ID 2）]、[キー2（Key 2）] を使用します。

ステップ	アクション
ステップ 6	[適用（Apply）] をクリックします。 **注**：時刻設定をリセットする必要がある場合は、[リセット（Reset）] をクリックします。 **注**：設定の保存時またはダイアログのロード時、[今すぐ時刻を同期（Synchronize Time Now）] が有効になります。ただし、NTP 設定パラメータの保存時に同期が行われるため、通常は不要です。さらに、他の NTP クライアントと同様に、SSM オンプレミスの NTP クライアントは、NTP サーバを自動的にポーリングしてサーバ時間を維持します。

新規ローカルアカウントのリクエスト

Smart Software Manager オンプレミスを使用するには、Cisco Smart Software Manager（https://software.cisco.com）に登録する必要があります。このプロセスを完了するために、次の要件を満たしていることを確認します。

- スマートアカウントへのアクセス。
- スマートアカウントにアクセスするための有効な CCO ユーザ ID とパスワード。
- スマートアカウントまたはバーチャルアカウントのいずれかが、Cisco スマートアカウントにアクセスできること。
- 適格な既存または新規の Cisco バーチャルアカウント。

これらの要件を満たしていれば、次のローカルアカウントの登録（要求）手順を実行することで、登録プロセスを進めることができます。

ステップ	アクション
ステップ 1	**SSM オンプレミスの管理ワークスペース**（https://< IP アドレス >:8443/admin）に移動します。 **注**：この IP アドレスは、インストール時に使用される値です。HA クラスタの一部である場合は、仮想 IP アドレスを使用する必要があります。
ステップ 2	[アカウント（Accounts）] ウィジェットを開きます。

ステップ	アクション
ステップ 3	[新規アカウント（New Account）] をクリックし、必要情報（ローカルアカウント**名**、Cisco **スマートアカウント**、Cisco **バーチャルアカウント**、通知用の**電子メールアドレス**）を入力します。必須フィールドには * というラベルが付いています。 **注：**Cisco **スマートアカウント**は、Cisco Smart Software Manager に存在する必要があります。Cisco **バーチャルアカウント**が Cisco Smart Software Manager に存在しない場合は、作成されます。各ローカルアカウントは、一意の Cisco バーチャルアカウントに関連付けられている必要があります。Cisco バーチャルアカウントには、製品またはその他のローカルアカウントが登録されていない場合があります。
ステップ 4	[送信（Submit）]をクリックします。
ステップ 5	その後、アカウントリクエストが [アカウント（Accounts）] ウィジェットの [アカウントリクエスト（Account Requests）] タブに表示されます。
ステップ 6	「新規ローカルアカウントの承認」セクションの手順に従って、ローカルアカウントを承認します。

新規ローカルアカウントの承認

新規ローカルアカウントが要求されると、管理ワークスペースの [アカウント（Account）] ウィジェットにある [アカウント要求（Account Requests）] タブにローカルアカウント要求が表示されます。そこでシステム管理者がローカルアカウントを承認し、Cisco スマートアカウントに登録するのを待ちます。登録手順の最後に、SSM オンプレミスをオンライン（ネットワークモード）とオフライン（手動モード）のどちらで使用するかを決定する必要があります。

ローカル アカウント リクエストの承認（ネットワーク モード）

[承認（Approve）] オプションで、[ネットワーク登録（Network Registration）] を選択します。この方法では、ローカルアカウントをネットワーク経由で Cisco Smart Software Manager に登録します。この方法は、登録リクエストを使用する場合にお勧めします。次の手順を実行して、ローカルアカウントを Cisco Smart Software Manager に登録します。

ステップ	アクション
ステップ 1	管理ワークスペースの [アカウント（Accounts）] ウィジェットにある [アカウントリクエスト（Account request）] タブで、承認をリクエストしているアカウントの [アクション（Actions）] ドロップダウンから [承認（Approve）] を選択します。
ステップ 2	[次へ（Next）] をクリックします。
ステップ 3	プロンプトが表示されたら、**CCO ID のクレデンシャル**を入力して、Cisco スマートアカウント/バーチャルアカウントによる Smart Software Manager へのアクセスを許可します。
ステップ 4	[送信（Submit）] をクリックします。
ステップ 5	アカウントの [登録（Registration）] ポップアップで、表示された情報を確認します。 **注**：Cisco スマートアカウント、または Cisco バーチャルアカウントが黒色のテキストで表示されている場合は、アカウントが存在し、使用できます。 Cisco スマートアカウント、または Cisco バーチャルアカウントが赤色のテキストで表示されている場合は、使用できません。新しい値をドロップダウンから選

ステップ	アクション
	択するか、手動で入力します。 Cisco バーチャルアカウントが青色のテキストで表示されている場合は、シスコに存在しないため、アカウントが作成されます。
ステップ 4	[送信（Submit）] をクリックします。 • SSM オンプレミスに登録の進捗状況が表示されます。 • 登録に成功すると、「アカウントが正常に作成されました（Account was created successfully）」というポップアップメッセージが画面に表示されます。
ステップ 5	[アカウント（Account）] タブでローカルアカウントが [アクティブ（Active）] と表示されていることを確認します。

ローカルアカウントの承認（手動モード）

また、ローカルアカウントを Cisco SSM（CSSM）に手動で登録することもできます。ローカルアカウントを手動で登録するには、[手動登録（Manual Registration）]を選択します。

注： 手動登録はサポートされていますが、登録ごとに特定の登録リクエスト/認証ファイルを追跡する必要があるため、お勧めしません。

次の手順を実行して、ローカルアカウントを手動で Cisco Smart Software Manager に登録します。

ステップ	アクション
ステップ 1	管理ワークスペースの [アカウント（Accounts）] ウィジェットにある [アカウントリクエスト（Account request）] タブで、承認をリクエストしているアカウントの [アクション（Actions）] ドロップダウンから [手動登録（Manual Registration）] をクリックします。
ステップ 2	[アカウント登録ファイルの生成（Generate Account Registration File）] をクリックし、ファイルを生成してローカル ファイル ディレクトリに保存します。ダイアログボックスの外側をクリックするか、Esc キーを押してダイアログを閉じます。 **注**：この手順の後、ブラウザで新しいタブを開き、**Smart Software Manager** にログインして登録ファイルを承認する必要があります。手順 3 ～ 11 に従ってログオンし、プロセスを続行してください。
ステップ 3	URL https://software.cisco.com/#SmartLicensing-On-Prem から **Smart Software Manager** を起動します。 **注**：このリンクを使用するには、スマートアカウントへのアクセスが必要です。
ステップ 4	ローカルアカウントの**ユーザ名**と**パスワード**を使用して、Smart Software Manager で**ローカルアカウント**にログインします。
ステップ 5	**Smart Software Manager** の画面で、[オンプレミスアカウント（On-Prem Accounts）] タブをクリックします。
ステップ 6	[オンプレミスアカウント（On-Prem Accounts）] タブで、[新規オンプレミス...

ステップ	アクション
	（New On-Prem...）]をクリックします。
ステップ 7	[新規オンプレミス（New On-Prem）]ダイアログボックスで、**オンプレミスの名前**を入力します。
ステップ 8	[ファイルの選択（Select File）]をクリックして、Cisco SSM オンプレミス セットアップ ツールで生成された**登録ファイル**を選択します。
ステップ 9	[バーチャルアカウント（Virtual Accounts）]フィールドで、新しいSSM オンプレミスインストールに追加する**Cisco バーチャルアカウント**を指定します。
ステップ 10	[連絡先の電子メールアドレス（Contact Email Address）]フィールドの横にあるテキストボックスに、電子メールアドレスを入力します。オンプレミスファイルが認証されると、電子メールで通知されます。
ステップ 11	[認証ファイルの生成（Generate Authorization File）]をクリックして続行します。リクエスト後 48 時間以内に認証ファイルが生成されること、およびそのファイルをダウンロードするための電子メール通知が届くことを示したメッセージが表示されます。 **注：**リクエスト後 48 時間以内に認証ファイルが生成されないか、または電子メールの通知が届かなかった場合は、シスコサポート（https://www.cisco.com/tac）にご連絡ください。
ステップ 12	電子メール通知を受け取ったら、**Cisco Smart Software Manager** にログインします。[サテライト（Satellites）]タブに移動します。
ステップ 13	オンプレミスの[アカウント（Accounts）]タブで、ローカルアカウントの**オンプレミステーブル**を検索し、作成した新しい**認証ファイル**を見つけます。[アラート（Alerts）]列に「認証ファイルの準備が整いました（Authorization File Ready）」というアラートメッセージが表示され、[アクション（Actions）]列には新しいオンプレミスインストール用の[認証ファイルのダウンロード（Download Authorization File）]リンクが表示されます。
ステップ 14	[認証ファイルのダウンロード（Download Authorization File）]リンクをクリッ

ステップ	アクション
	クし、ハードドライブ上のローカルディレクトリに認証ファイルをダウンロードします。 **注**：この手順の後、**SSMオンプレミス**に戻り、認証済みファイルをアップロードします。セットアッププロセスを続行します。
ステップ 15	**Smart Software Manager** の [オンプレミスの登録（Register On-Prem）] ステップで、[参照（Browse）] をクリックし、認証済みの SSM オンプレミスファイルをダウンロードした場所に移動します。
ステップ 16	[アップロード（Upload）] をクリックして、認証済みの SSM オンプレミスファイルをアップロードします。
ステップ 17	[次へ（Next）] をクリックして [同期（Synchronization）] ウィジェットに進みます。オンプレミスとシスコライセンスサーバ間で定期的に同期を行ってライセンスを更新し、製品インスタンスを再認証する必要があります。

Smart Software Manager オンプレミスの同期

Smart Software Manager オンプレミスのローカルアカウントが登録および承認されたので、このアカウントを Cisco Smart Software Manager ライセンスサーバと同期する必要があります。

[同期（Synchronization）] ウィジェットに進み、同期を実行します。

注： オンプレミスと Cisco Smart Software Manager ライセンスサーバ間で定期的に同期を行ってライセンスを更新し、製品インスタンスを再認証する必要があります。

製品インスタンスの登録

製品インスタンスを SSM オンプレミスに登録します。『Cisco SSM オンプレミスユーザガイド』の「オンプレミスへの製品インスタンスの登録」、およびお使いの製品のマニュアルを参照してください。

- シスコ製品では、次の API エンドポイントを使用します。
  - HTTPS（443）：tools.cisco.com（登録/認証）
  - HTTP（80）： **www.cisco.com**
- Smart Software Manager オンプレミスでは、次の API エンドポイントを使用します。
  - ユーザインターフェイス：HTTPS（8443）のみ
  - 製品：HTTP（80）/HTTPS（443）
  - CSSM：HTTPS（443）
    - 同期：
      api.cisco.com （6.2 以前）
      swapi.cisco.com（6.3 以降）
    - アカウント登録：cloudsso.cisco.com
  - cloudsso.cisco.com

トラブルシューティング

次の 5 つのセクションでは、アカウント登録、製品登録、ネットワーク同期、手動同期に関する問題の対処方法について説明します。これらに関する問題が発生した場合は、以下のトピックを参照してください。

アカウント登録に関する問題

- ライセンスワークスペースで [スマートライセンス（Smart Licensing）] および [ローカルアカウントの管理（Manage Local Account）] オプションがグレー表示される
  - 新しいローカルアカウントをリクエストするか、既存のローカルアカウントへのアクセス権をリクエストする必要があります。
  - そのローカルアカウントを Cisco Smart Software Manager に登録します。
  - ログアウトしてからライセンスワークスペースに再度ログインすると、ローカルアカウントが右上に表示されます。
- ユーザを追加できない
  - 管理ワークスペースで適切な認証方式が設定されていることを確認します。
  - LDAP を使用している場合は、SSM オンプレミスのライセンスワークスペースにログインすると、[ユーザ追加（Add User）] 画面が表示されます。
- 製品を登録できない
  - トークンの有効期限が切れていないことを確認します。
  - 製品の URL で SSM オンプレミスの適切な共通名または IP アドレスが参照されていることを確認します（詳細については、「共通名の入力」を参照してください）。
- ユーザがライセンスワークスペースにログインすると、SSM オンプレミスのローカルアカウントが表示されない
  - ユーザにローカルアカウントのロール（アクセス権）が割り当てられていることを確認します。使用可能なロールは、ローカルアカウント管理者、ローカルアカウントユーザ、ローカル バーチャル アカウント管理者、ローカル バーチャル アカウント ユーザです。
- SSM オンプレミスで使用されるポートは何ですか。
  - ユーザインターフェイス：HTTPS（ポート 8443）
  - 製品登録：HTTPS（ポート 443）、HTTP（ポート 80）
  - Cisco Smart Software Manager：ファイアウォールでポート 443（HTTPS）が許可され、次のアドレスにアクセス可能であることを確認します。
  - cloudsso.cisco.com
    - 173.37.144.211
    - 72.163.4.74
  - api.cisco.com（6.2.0 より前）

- 173.37.145.221
- 72.163.8.72

- swapi.cisco.com（6.3 以降）
  - IPv4：146.112.59.25
  - IPv6：2a04:e4c7:fffe::4

製品登録に関する問題

製品登録プロセスで問題が発生した場合は、次の対処方法を試してください。

- SSM オンプレミスの設定が正しいことを確認します。
- 管理ワークスペースの [ネットワーク（Network）] ウィジェットが正しく設定されていることを確認します。
- オンプレミスの時刻が正しいことを確認します。
- クライアントの Call Home 設定で SSM オンプレミスを参照していることを確認します。
- Call Home 設定で使用される SSM オンプレミスからトークンが生成されていることを確認します。
- ファイアウォール設定で、SSM オンプレミスとの間で次のトラフィックを許可する必要があります。
  - 443（HTTPS を使用している場合）
  - 80（HTTP を使用している場合）
  - ユーザのブラウザから SSM オンプレミスの IP アドレスにアクセスする際は、ポート 8443 を使用

注： 厳格な SSL 証明書チェックをサポートする製品では、SSM オンプレミスのホスト名が、製品に設定されている宛先 http URL アドレスと一致する必要があります。

手動同期に関する問題

手動同期プロセスで問題が発生した場合は、次の対処方法を試してください。

- オンプレミスの時刻が正しいことを確認します。
- 関連付けられたバーチャルアカウントのライセンスを確認します。
- YAML（要求/応答）ファイルのアップロード/ダウンロードが正しい SSM オンプレミスアカウントから実施されていることを確認します。これを確認するには、同期する SSM オンプレミスの名前がファイル名に含まれていることを確認します。

注： 手動で標準同期を実行した後で、完全な手動同期を再度実行するように通知される場合があります。

ネットワーク同期に関する問題

ネットワーク同期プロセスで問題が発生した場合は、次の対処方法を試してください。

- SSM オンプレミスが cisco.com に到達できることを確認します。
- ファイアウォールでポート 443（HTTPS）が許可され、次のアドレスにアクセス可能であることを確認します。
  - cloudsso.cisco.com
    - 173.37.144.211
    - 72.163.4.74
  - api.cisco.com（6.2.0 より前）
    - 173.37.145.221
    - 72.163.8.72
  - swapi.cisco.com（6.3 以降）
    - IPv4：146.112.59.25
    - IPv6：2a04:e4c7:fffe::4
- 設定された DNS サーバに SSM オンプレミスから到達できることを確認します。
- SSM オンプレミスの時刻が正しいことを確認します。

IP アドレスの競合

IP アドレスの競合に関する問題が発生した場合は、次の対処方法を試してください。

- atlantis0 を管理 IP アドレスとして使用していることが原因で IP アドレスの競合が発生していないことを確認します（これが発生した場合は、シスコサポートに連絡してください）。

付録 1：SSM オンプレミスシステムのアップグレードの準備

注： アップグレードを実行する前に、データベースのバックアップを取得することをお勧めします（VM を使用している場合）。

注： アップグレードの実行後、ブラウザページに最新の変更が反映されない場合があります。ブラウザのページが最新の状態になるように、ブラウザのキャッシュをクリアしてください。.

ステップ	アクション
ステップ 1	**software.cisco.com/download/home** に移動します。
ステップ 2	[製品の選択（Select a Product）] フィールドに、「**Smart Software Manager サテライト（Smart Software Manager satellite）**」と入力します。
ステップ 3	[最新リリース（Latest Release）] の左側の列で、[8-202004] を選択します。
ステップ 4	**Smart Software Manager オンプレミスリリース 8 アップグレード**（ファイル名：SSM_On-Prem_8-202004_Upgrade.zip）を選択し、画面の右側にある [ダウンロード（Download）] アイコンをクリックします。
ステップ 5	ダウンロードが完了したら、zip ファイルが保存されているディレクトリに移動し、**ファイル**を右クリックして、[イメージの解凍（unzip image）] を選択します。

付録 2：バージョン 7 より前のシステムのアップグレード

バージョン 7 より前のリリースを実行している場合は、次の手順に従ってシステムに適切なアップグレードをダウンロードする必要があります。

注： アップグレードを実行する前に、データベースのバックアップまたはマシンのスナップショットを取得することをお勧めします（VM を使用している場合）。システムとしてのバックアップの詳細については、『Cisco Smart Software オンプレミスユーザガイド』の付録 1 を参照してください。

注： アップグレードの実行後、ブラウザページに最新の変更が反映されない場合があります。ブラウザのページが最新の状態になるように、ブラウザのキャッシュをクリアしてください。

ステップ	アクション
ステップ 1	「SSM オンプレミスシステムのアップグレードの準備」の手順を実行して、オンプレミスサーバのアップグレードに必要なファイルを取得します。
ステップ 2	「ssh」を使用して、管理者としてオンプレミスサーバに接続します。 **ssh admin@<your ip address>**
ステップ 3	CLI で次のコマンドを使用して、*.sh および *.sh.sha256 のファイルをオンプレミスサーバにコピーします。 **scp SSM_On-Prem_8-202004_Upgrade.sh admin@<your ip address>:SSM_On-Prem_8-202004_Upgrade.sh** **scp SSM_On-Prem_8-202004_Upgrade.sh admin@<your ip address>:SSM_On-Prem_8-202004_Upgrade.sh.sha256**
ステップ 4	リストコマンドを使用して、SCP が成功したことを確認します。 **ls**
ステップ 5	次のコマンドを入力して、アップグレードファイルのファイル権限を昇格させます。

ステップ	アクション
	sudo -s (to make yourself administrator) **chmod +x SSM_On-Prem_8-202004_Upgrade.sh** **chmod +x SSM_On-Prem_8-202004_Upgrade.sh.sha256**
ステップ 6	ステップ 5 でファイル権限を昇格した後、次のコマンドを入力してアップグレードプロセスを開始します。 **./SSM_On-Prem_8-202004_Upgrade sh** コマンドを起動すると、システムがアップグレード中であることを通知するメッセージプロンプトが表示されます。
ステップ 7	システムのアップグレードが完了したら（約 5 ～ 15 分）、プロセスが完了したことが通知されます。この時点で、システムは自動的にリブートします。

付録 3：バージョン 7 のシステムのアップグレード

注： アップグレードを実行する前に、データベースのバックアップを取得することをお勧めします。

オンプレミスコンソールからアップグレードをインストールする必要があります。

注： アップグレードの実行後、ブラウザページに最新の変更が反映されない場合があります。ブラウザのページが最新の状態になるように、ブラウザのキャッシュをクリアしてください。

バージョン 7 以降のシステムの場合は、次の手順を実行して、SSM オンプレミス ライセンス サーバに適切なアップグレードをダウンロードします。

ステップ	アクション
ステップ 1	「SSM オンプレミスシステムのアップグレードの準備」の手順を実行して、オンプレミスサーバのアップグレードに必要なファイルを取得します。
ステップ 2	Linux の「ssh」コマンドを使用して、オンプレミスサーバに管理者として接続します。 **ssh admin@<your ip address>**
ステップ 3	次のコマンドでオンプレミスコンソールを起動します。 **onprem-console**
ステップ 4	オンプレミスコンソールで、次の 2 つの例に示すように copy コマンドを使用します。 **注**：オンプレミスの copy コマンドを使用できるのは、自分がオンプレミスコンソールにいる場合のみです。ステップ 4 を参照してください。オンプレミスの copy コマンドは、リモートホスト**から**ローカルのオンプレミスマシン**に**フィールドをコピーします。 **copy <your username>@<your remote host>.com:/path/SSM_On-Prem_8-202004_Upgrade.sh patches:**

ステップ	アクション
	copy <your username>@<your remote host.com>:/path/SSM_On-Prem_8-202004_Upgrade.sh.sha256 patches: **注：<your username>@<your remote host.com>** は、オンプレミスのアップグレードファイルが存在するユーザ名とリモートホストアドレスを表し、**/path** はそれらのファイルへのパスを表します。
ステップ 5	copy コマンドの後に、次のアップグレードコマンドを使用します。 **upgrade patches:SSM_On-Prem-8_202004_Upgrade.sh** 対応する既存の署名ファイルが必要です。
ステップ 6	システムのアップグレードが完了したら（約 5 ～ 15 分）、プロセスが完了したことが通知されます。この時点で、システムは自動的にリブートします。 **注**：システムが自動的にリブートしない場合は、手動でリブートします。
ステップ 7	リブートが完了したら、**system の同期**を実行してください。

付録 4：システムの高可用性（HA）クラスタの管理

（SSM オンプレミスバージョン 7 リリース 201907 以降で導入）

SSM オンプレミスでは、Pacemaker と Corosync によって拡張高可用性がサポートされます。これらのアプリケーションは、インストールと設定を簡素化するために、ISO パッケージで提供されます。

高可用性（HA）クラスタの導入に必要な前提条件

- HA クラスタの各ノードのホスト名は、一意である必要があります（例：ホスト 1 とホスト 2）。ノードの名前が同じ場合、HA の導入は失敗します。マシンのホスト名を変更するには、オンプレミスコンソール の hostname コマンドを使用します。

⚠

注意： HA クラスタ内のホスト名が一致すると、導入が失敗し、ティアダウンおよび再導入が必要になります。

- 仮想 IP は、**未割り当て**（未使用）の **IP アドレス**である必要があります。これは、IP アドレスがクラスタ全体でフローティング IP アドレスとして使用されるためです。
- SSM オンプレミスは、各ノードで同じ SSM オンプレミスバージョンを共有する必要があります。異なるバージョンの SSM オンプレミスで HA クラスタを導入することはサポートされていません。
- 両ノードのインターフェイスがルーティング可能となるように、同じサブネット上にあり、各ノードからアクセス可能な IP アドレスを割り当てる必要があります。また、プロビジョニングを成功させるためにも、仮想 IP アドレスは未使用かつ、同じサブネット上に存在する必要があります。
- ネットワーク内のプライベート IP アドレスは未使用である必要があります。さらに、これらのアドレスはノード間の SSH トンネルにのみ使用されるため、ルーティング可能である必要はありません。
- スタンバイサーバは、**新しい**、**新規にインストールした** SSM オンプレミス（データのないもの）である必要があります。HA ソリューションが導入されると、アクティブサーバのデータがスタンバイサーバに複製されます。
- HA を導入する前に、両方のノードで NTP を設定する必要があります。

HA クラスタの導入

（SSM オンプレミス 8 リリース 202004 用に更新）

HA の導入は、オンプレミスの CLI コンソールで特定のコマンドを使用してのみ実施できます。ヘルプコマンドの詳細については、『Cisco SSM オンプレミス コンソール ガイド』を参照してください。インストールと設定を簡素化するカスタム インストール スクリプトが提供されています。このスクリプトはオンプレミスコンソールにあり、**<ha_deploy>** コマンドを使用して起動します。

注： オンプレミスコンソールおよびヘルプコマンドの使用方法については、『Cisco Smart Software オンプレミス コンソール リファレンス ガイド』を参照してください。

注： インストール時に STIG モードを選択した場合、SSM オンプレミスサーバに SSH で接続すると、オンプレミスコンソールに自動的に配置されます。標準モードを選択した場合は、SSM オンプレミスサーバに SSH で接続し、bash プロンプトで **<onprem-console>** コマンドを実行すると、コンソールを開くことができます。

HA クラスタの導入を容易にするために、導入プロセスを 3 つの主要なステップ（後述）に分け、ステップごとに導入の特定のフェーズに焦点を当てています。

注： 導入手順では、「アクティブサーバ」と「スタンバイサーバ」という用語を使用します。ティアダウンシーケンスでは、「プライマリノード」と「セカンダリノード」という用語を使用します。次に、サーバ/ノードの用語の対応関係を示します。

アクティブサーバ = プライマリノード

スタンバイサーバ = セカンダリノード

ステップ 1：プライマリノードのキーの生成に焦点を当てます。これらのキーは、プライマリノードとセカンダリノード間のセキュアな通信チャネルを確立する、ユーザとセットアップの SSH キーです。

ステップ 2：スタンバイサーバの導入に焦点を当てます。

ステップ 3：アクティブサーバの導入に焦点を当てます。

1 つ目のステップ：ユーザと SSH キーの生成

ステップ 1 では、プライマリノードとセカンダリノード（アクティブサーバとスタンバイサーバ）間のセキュアな通信チャネルを確立するための、ユーザと SSH キーを生成します。

注： 導入が成功した後にスナップショットを取得し、各ノード（IP アドレス）間を移動できるようにすることをお勧めします。

ステップ	アクション
ステップ 1	**プライマリ**ノードに SSH で接続し、管理者としてコンソールに入ります。 **注**：DISA STIG モードでは、デフォルトでオンプレミスコンソールに配置されます。 DISA STIG モードでない場合は、次のコマンドを入力してオンプレミスコンソールを開きます。 **onprem-console** **Enter** を押します。 コンソールが開きます。

ステップ	アクション

ステップ 2	sshtunnel のセットアップを開始するには、次のコマンドを入力します。
	ha_generatekeys
	Enter を押します。
	次に、続行するために**管理者パスワードの入力を求めるプロンプト**が表示されます。
	注：このパスワードを入力すると、ha_generatekeys などの ha_ コマンドを実行するための適切な権限が付与されます。
	注：!@#$%^&*()-=[];:",.<>?| などの特殊文字を使用できます。
	HA クラスタ（sshtunnel）パスワードではスペースを使用**できません**。
	管理者パスワードを入力します。
	Enter を押します。
	ha_generatekeys コマンドと予想される出力を次に示します。
	`>>ha_generatekeys`
	`==========`
	`This step will generate a user and setup SSH keys to be used to establish a secure channel of communication between the two nodes.`
	`This is step 1 of 3 for deploying a HA cluster.`
	`The password chosen here is temporary and used only during the HA setup process. Remember this password, as you will be asked for this same password several times during the setup of the HA cluster.`
	`==========`
	`Choose an HA cluster password: <HA Cluster Password>`
	注：**HA クラスタパスワード**は、ユーザ **sshtunnel** のパスワードと同義です。この用語は、次の行に示すように、同じ意味で使用されます。
	`Changing password for user sshtunnel.`
	`passwd: all authentication tokens updated successfully.`
	`Generating SSH keys...`
	`Operating in CiscoSSL FIPS mode`
	`SSH keys generated successfully.`

ステップ 3	キー生成コマンドが完了したら、**onprem シェルを終了**し、SSH セッションも終了します。 **注**：認証トークンが更新され、SSH キーが生成されます。

ステップ	アクション
	これで、導入プロセスの 2 つ目のステップである、スタンバイサーバのプロビジョニングの準備が整いました。

2 つ目のステップ：スタンバイサーバ（セカンダリノード）のプロビジョニング

導入プロセスの次の部分では、スタンバイサーバ（セカンダリノード）をプロビジョニングします。

次のアクションを実行して、スタンバイサーバをプロビジョニングします。

ステップ	アクション
ステップ 1	**スタンバイ**ノードに SSH で接続し、管理者としてコンソールに入ります。 **注**：DISA Stig モードでは、デフォルトでオンプレミスコンソールに配置されます。 DISA Stig モードでない場合は、次のコマンドを入力してオンプレミスコンソールを開きます。 **onprem-console** **Enter** を押します。 コンソールが開きます。
ステップ 2	スタンバイノードでプロビジョニングプロセスを開始するには、次のコマンドを入力します。 **ha_provision_standby** と入力し、**Enter** を押します。
ステップ 3	**管理者パスワード**の入力を求められます。
ステップ 4	ここで、現在 HA 導入の 2 つ目の主要ステップにいることが通知され、1 つ目のステップで SSH キー（ha_generatekeys）を生成済みであることを確認するよう求められます。 次に、**アクティブノードの IP アドレス**、**アクティブノードのプライベート IP アドレス**、**スタンバイノードの IP アドレス**、**スタンバイノードのプライベート IP アドレス**を入力するように求められます。次の順序で IP アドレスを入力します（以下の通知を参照）。 a. アクティブノードの IP アドレスに **<IP アドレス>** を入力します。

ステップ	アクション

	b. アクティブノードのプライベート IP アドレスに**<プライベート IP アドレス>**を入力します。
	c. スタンバイノードの IP アドレスに **<IP アドレス>** を入力します。
	d. スタンバイノードのプライベート IP アドレスに **<プライベート IP アドレス>** を入力します。
	e. HA クラスタのパスワードには、**HA パスワード（sshtunnel のユーザパスワード）**を入力します。
	注：HA の IP アドレスを更新する場合は、アクティブノードとスタンバイノードの両方の IP アドレスを入力する必要があります。各ノードの IP アドレスは、自動的には複製**されません**。手動で各ノードの IP アドレスを更新する必要があります。
	注：HA に使用するすべての IP アドレスは、同じ IP バージョンである必要があります。IPv4 と IPv6 アドレスの組み合わせは許可されていません。
	ha_provision_standby コマンドと予想される出力を次に示します。
	`>> ha_provision_standby`
	`[sudo] password for admin: <admin password>`
	`Last login: Thu Mar 26 19:28:43 UTC 2020 on pts/0`
	`==========`
	`Provision SSM On-Prem server as a standby node`
	`==========`
	`This procedure will convert a stand-alone SSM On-Prem server to act as the standby node in an HA environment. Proceeding will first destroy the current database in order to begin replication from the active node.`
	`IMPORTANT: This is step 2 of 3 for deploying HA. Please ensure that you have generated SSH keys on the primary node before running this step!`
	`ALL DATABASE DATA WILL BE WIPED ON THIS NODE UNTIL REPLICATION BEGINS!`
	`==========`
	`Enter IP address of the active node: <active node physical IP>`
	`Enter the private IP address of the active node: <private address used for the ssh tunnel only!>`
	`Enter IP address of the standby node: <standby node physical IP>`
	`Enter the private IP address of the standby node: <private address used for the ssh tunnel only!>`

ステップ	アクション
	Enter HA cluster password: **<HA Cluster Password used in ha_generate>** HA Secondary Node Setup Confirmation Active (other node): <active node physical IP> Private Active : <active node private address used for the ssh tunnel only!> Standby (this node): <standby node physical IP> Private Standby : <standby node private address used for the ssh tunnel only!> HA Cluster Password : <**HA Cluster Password used in ha_generate**> !!! DO NOT ABORT THIS PROCESS AFTER PROCEEDING !!! You will be prompted another time for the HA Cluster Password (user sshtunnel password). Please enter the HA Cluster password that you set previously in the initial HA setup. Proceed with the above configuration? Enter 'yes' to continue: **<yes>** Provisioning machine as a secondary node for HA cluster... Establishing SSH tunnel for both nodes... Operating in CiscoSSL FIPS mode Changing password for HA Cluster (user sshtunnel). passwd: <HA Cluster Password used in ha_generate> all authentication tokens updated successfully. Operating in CiscoSSL FIPS mode sshtunnel@<standbyIP>'s password:

ステップ	アクション
	Operating in CiscoSSL FIPS mode Last login: Thu Mar 26 19:31:46 UTC 2020 on pts/0 Verifying SSH access to 10.122.81.20 ... Operating in CiscoSSL FIPS mode Last login: Thu Mar 26 19:31:50 UTC 2020 on pts/0 OK Created symlink from /etc/systemd/system/multi-user.target.wants/tunha.service to /etc/systemd/system/tunha.service. Stopping services... Removed symlink /etc/systemd/system/multi-user.target.wants/satellite.service. Starting cluster... Created symlink from /etc/systemd/system/multi-user.target.wants/pcsd.service to /usr/lib/systemd/system/pcsd.service. Changing password for user hacluster. passwd: all authentication tokens updated successfully. Last login: Thu Mar 26 19:28:44 UTC 2020 on pts/0 Setting up for data replication... (active node: 10.122.81.20) 5d91258862f94a54e1836dc5db7c0c9499d863433d71701e2cf80aef3cbd97e9 Standby provisioning is complete! You may now proceed with HA deployment from the active node.
ステップ 5	プロビジョニングが完了すると、2 つ目のメインステップが終了します。

3 つ目のステップ：アクティブサーバ（プライマリノード）の導入

アクティブサーバ（プライマリノード）を導入するには、次の手順を実行します。

ステップ	アクション
ステップ 1	**プライマリ**ノードに SSH で接続し、管理者としてコンソールに入ります。

ステップ	アクション
	注：DISA Stig モードでは、デフォルトでオンプレミスコンソールに配置されます。 DISA Stig モードでない場合は、次のコマンドを入力してオンプレミスコンソールを開きます。 **onprem-console** **Enter** を押します。 コンソールが開きます。
ステップ 2	プライマリノードでプロビジョニングプロセスを開始するには、次のコマンドを入力します。 **ha_deploy** と入力して **Enter** を押します。
ステップ 3	**管理者パスワード**の入力を求められます。
ステップ 4	次に、以下の順序で次の情報を入力するように求められます。 a. アクティブノードの IP アドレスに **< IP アドレス >** を入力します。 b. アクティブノードのプライベート IP アドレスに**< プライベート IP アドレス >** を入力します。 c. スタンバイノードの IP アドレスに **< IP アドレス >** を入力します。 d. スタンバイノードのプライベート IP アドレスに **< プライベート IP アドレス >** を入力します。 e. HA クラスタのパスワードには、**HA のパスワード**（sshtunnel のパスワード）を入力します。 **注**：HA の IP アドレスを更新する場合は、アクティブノードとスタンバイノードの両方の IP アドレスを入力する必要があります。各ノードの IP アドレスは、自動的には複製**されません**。手動で各ノードの IP アドレスを更新する必要があります。 **注**：HA に使用するすべての IP アドレスは、同じ IP バージョンである必要があります。IPv4 と IPv6 アドレスの組み合わせは許可されません。 もう 1 つの確認メッセージが表示されます。 **yes** と入力し、**Enter** を押します。 **Enter** を押すと、導入プロセスが開始されます。 導入プロセスが完了するまで待ちます。 **注**：すべてのサービスが実行中になるように、**1 分**以上待ってから IP にアクセスします。

ステップ	アクション
	プロビジョニングプロセスの最後に、コマンドラインに仮想 IP アドレスが表示されます。 HA の導入プロセスが完了し、HA クラスタを使用できるようになりました。 ha_deploy コマンドと予想される出力を次に示します。 >> ha_deploy [sudo] password for admin: **<admin password>** ========== Deploy SSM On-Prem two-node HA cluster ========== IMPORTANT: This is step 3 of 3 for deploying a HA cluster. Be sure that you have first provisioned the standby node before running this step. ========== Enter IP address of the active node: **<active node physical IP>** Enter the private IP address of the active node: **<private address used for the ssh tunnel only!>** Enter IP address of the standby node: **<standby node physical IP>** Enter the private IP address of the standby node: **<private address used for the ssh tunnel only!>** Enter virtual IP address: **<Virtual IP Address>** Enter HA cluster password: **<HA Cluster Password used in ha_generate> (sshtunnel password)** Verifying SSH access to <Standby Node> ... Operating in CiscoSSL FIPS mode OK High Availability Setup Confirmation Active (other node): <active node physical IP> Private Active : <active node private address used for the ssh tunnel only!> Standby (this node): <standby node physical IP> Private Standby : <standby node private address used for the

ステップ	アクション
	ssh tunnel only!> Virtual IP : <Virtual IP Address> HA Password : <HA Cluster Password used in ha_generate> !!! DO NOT ABORT THIS PROCESS AFTER PROCEEDING !!! NOTICE: It is strongly recommended that you perform a backup of your database before proceeding. Please see the documentation for details. Proceed with the above configuration? Enter 'yes' to continue: **<yes>** Deploying HA cluster... Removing password for HA Cluster (user sshtunnel). passwd: Success Operating in CiscoSSL FIPS mode Operating in CiscoSSL FIPS mode Last login: Thu Mar 26 19:32:08 UTC 2020 on pts/0 Running sshtunnel post-install... Removing password for HA Cluster (user sshtunnel). passwd: Success Starting secure tunnel... Created symlink from /etc/systemd/system/multi-user.target.wants/tunha.service to /etc/systemd/system/tunha.service. Created symlink from /etc/systemd/system/multi-user.target.wants/sshtunha.service to /etc/systemd/system/sshtunha.service. Stopping services... Removed symlink /etc/systemd/system/multi-user.target.wants/satellite.service.

ステップ	アクション
	Created symlink from /etc/systemd/system/multi-user.target.wants/pcsd.service to /usr/lib/systemd/system/pcsd.service. Changing password for user hacluster. passwd: all authentication tokens updated successfully. Last login: Thu Mar 26 19:35:50 UTC 2020 on pts/1 Authenticating cluster user... secondary-node: Authorized primary-node: Authorized Setting up cluster... 2287b3ebcc5fa498d3d9aeb3ada3f36a3328a3ea58dbdd933ee7b6c16789fe6a Destroying cluster on nodes: primary-node, secondary-node... secondary-node: Stopping Cluster (pacemaker)... primary-node: Stopping Cluster (pacemaker)... primary-node: Successfully destroyed cluster secondary-node: Successfully destroyed cluster Sending 'pacemaker_remote authkey' to 'primary-node', 'secondary-node' primary-node: successful distribution of the file 'pacemaker_remote authkey' secondary-node: successful distribution of the file 'pacemaker_remote authkey' Sending cluster config files to the nodes... primary-node: Succeeded secondary-node: Succeeded Starting cluster on nodes: primary-node, secondary-node... primary-node: Starting Cluster (corosync)... secondary-node: Starting Cluster (corosync)... secondary-node: Starting Cluster (pacemaker)... primary-node: Starting Cluster (pacemaker)... Synchronizing pcsd certificates on nodes primary-node, secondary-node... secondary-node: Success

ステップ	アクション
	primary-node: Success Restarting pcsd on the nodes in order to reload the certificates... secondary-node: Success primary-node: Success Waiting for node(s) to start... primary-node: Started secondary-node: Started Configuring cluster... Adding redis backend (kind: Mandatory) (Options: first-action=start then-action=start) Adding postgres_clone_data backend (kind: Mandatory) (Options: first-action=start then-action=start) Adding gobackend central_logger (kind: Mandatory) (Options: first-action=start then-action=start) Adding backend central_logger (kind: Mandatory) (Options: first-action=start then-action=start) Adding central_logger frontend (kind: Mandatory) (Options: first-action=start then-action=start) Adding frontend recovermaster (kind: Mandatory) (Options: first-action=start then-action=start) Adding frontend promotetomaster (kind: Mandatory) (Options: first-action=start then-action=start) Adding promotetomaster virtual_ip (kind: Mandatory) (Options: first-action=start then-action=start) Warning: Defaults do not apply to resources which override them with their own defined values primary-node: Cluster Enabled secondary-node: Cluster Enabled DB replication to secondary node complete. HA cluster deployment complete! You may now access SSM On-Prem using the virtual IP at https:// **<Virutal IP>** 以上で導入が完了しました。

注意： SSM オンプレミスにアクセスする際は、常に仮想 IP アドレスを使用してください。ホスト OS から直接アクセスする場合を除き、サービス IP アドレスを使用してサーバにアクセスしないでください。

HA 構成により、すべてのデータがアクティブサテライトとスタンバイサテライトの間で自動的に複製されます。アクティブサテライトとの接続が失われた場合は自動フェールオーバーが行われ、スタンバイサテライトが応答を開始することで、無停止でのリカバリと継続的な運用が可能になります。

接続の問題やその他の予期しない問題によって HA のセットアップが失敗（ログから確認）した場合は、「高可用性クラスタのダウングレード高可用性クラスタのダウングレード」セクションで説明した手順を実行した後、HA クラスタのインストールを再試行することをお勧めします。ダウングレードすると、SSM のオンプレミスがスタンドアロンモードに戻ります。

オンプレミスコンソールで、次のコマンドを使用して HA クラスタにアクセスします。

```
ha_status
```

注： 高可用性クラスタには、オンプレミスコンソールからアクセスします。

ha_status とその他のコマンドは、オンプレミスコンソールで使用します。ヘルプコマンドの詳細については、付録 1 の「コンソールのヘルプコマンド」を参照してください。

有効にすると、アクティブ SSM オンプレミスでスタンバイサテライトにデータを複製するプロセスが自動的に開始されます。初期データのレプリケーションがノード全体で完了するまで、スタンバイ SSM オンプレミスは使用できません。

高可用性クラスタの強制フェールオーバー

注： **プライマリ（アクティブ）**から**スタンバイ**へのスイッチオーバーは、最大で 2 分かかります。

スイッチオーバーが発生すると、スタンバイはアクティブオンプレミスに昇格され、パフォーマンスの低下した SSM オンプレミスはクラスタへの再参加時にスタンバイに降格されます。

高可用性クラスタのダウングレード

Cisco Smart Manager オンプレミスのクラスタは、単一ノードのスタンドアロンに直接ダウングレードできます。

オンプレミスコンソールを使用して **プライマリ/アクティブ** SSM オンプレミスに接続し、<ha_teardown> コマンドを使用します。

SSM オンプレミスの動作の確認後、セカンダリ/スタンバイサーバは破棄され、再利用できなくなります。これで、クラスタではなくスタンドアロンシステムになります。

注： オンプレミスコンソールおよびヘルプコマンドの使用方法については、『Cisco Smart Software オンプレミス コンソール リファレンス ガイド』を参照してください。

付録 5：高可用性（HA）クラスタのアップグレード

高可用性（HA）クラスタのアップグレード

注意： 高可用性（HA）クラスタをアップグレードする場合は、次の条件が満たされていることを確認してください。

- アップグレードを実行する前に、データベースのバックアップを取得することをお勧めします。

HA クラスタへのアップグレードをインストールするには、次の手順を実行します。

ステップ	アクション
ステップ 1	teardown コマンドを使用して、既存のクラスタを 2 台のスタンドアロンマシンに戻します。各マシンタイプに対して、次のコマンドを実行します。 `ha_teardown`
ステップ 2	各マシンがスタンドアロンの状態に戻ったら、「SSM オンプレミスシステムのアップグレードの準備」および「SSM オンプレミス 7 のアップグレード」の手順に従います。
ステップ 3	各マシンがアップグレードされたら、「HA クラスタの導入」の手順に従います。

これで HA クラスタのアップグレードプロセスが完了し、システムが完全に稼働するようになりました。

付録 6：IPv4 のプロビジョニング

オンプレミスコンソールを使用して、IPv4 ルーティングをカスタマイズできます。既存の IPv4 ルートをカスタマイズするには、次の手順を実行します。

ステップ	アクション
ステップ 1	CLI からサーバの IP アドレスに**管理者として ssh で接続**し、次のコマンドを入力してコンソールを開きます。 **`onprem-console`** **ヒント**：コマンド入力にはタブ補完を使用できます。
ステップ 2	コンソールで、「**?**」と入力してヘルプメニューを開きます。
ステップ 3	ヘルプメニューで、次のヘルプコマンドを入力します。 **ha_network_manager** NetworkManager TUI が開きます。
ステップ 4	[接続の編集（Edit a connection）] を選択します。 **Enter** を押して、[イーサネット（Ethernet）] 画面を開きます。 **ヒント**：**Tab** を使用して画面内を移動し、**Enter** を押してコマンドを開きます。
ステップ 5	[イーサネット（Ethernet）] 画面で、編集する**イーサネット接続**を選択します。
ステップ 6	Tab で [編集（Edit）] を選択し、**Enter** を押します。[接続の編集（Edit Connection）] 画面が開きます。
ステップ 7	Tab で [ルーティング<編集...>（Routing <Edit...>）] を選択し、**Enter** を押します。
ステップ 8	この画面から、接続の編集、追加、または削除を行うことができます。 接続を追加するには、Tab で [追加（Add）] を選択して **Enter** を押します。別の接続回線が開きます。 イーサネット接続を追加または編集する場合は、次のフィールドを設定する必要があります。 • 宛先/プレフィックス • ネクストホップ

ステップ	アクション
	• メトリック

ステップ	アクション
ステップ 9	イーサネット接続の追加または編集が完了したら、Tab で [OK] を選択して **Enter** を押します。システムによって変更が保存され、[接続の編集（Edit Connection）] 画面に戻ります。 **注**：[キャンセル（Cancel）] を選択して、[接続の編集（Edit Connection）] 画面に戻ることもできます。
ステップ 10	接続を適切にカスタマイズしたら、Tab で [OK] を選択して **Enter** を押し、[イーサネット（Ethernet）] 画面に戻ります。
ステップ 11	NetworkManager TUI 画面に戻るには、Tab で [戻る（Back）] を選択して **Enter** を押します。
ステップ 12	Network_Manager アプリケーションを終了するには、Tab で [終了（Quit）] を選択して **Enter** を押します。オンプレミスコンソールに戻ります。