Cisco Intersight 仮想アプライアンスおよび Intersight Assist スタートアップ ガイド、1.0.9

最終更新：2024 年 8 月 28 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

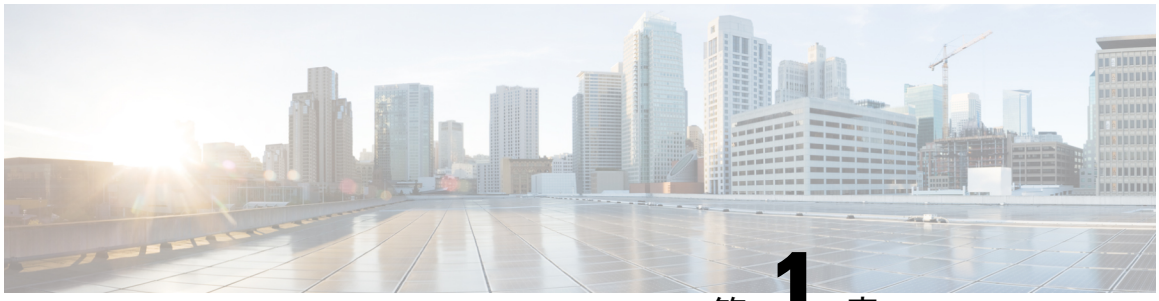
All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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)

© 2019–2021 Cisco Systems, Inc. All rights reserved.

目 次



第 1 章

このマニュアルについて

はじめに

Cisco Intersight は Intersight.com で Software as a Service（SaaS）か Cisco Intersight 仮想アプライアンスのいずれかとしてオンプレミスで実行することによってフレキシブルに展開できます。仮想アプライアンスは、Cisco Intersight のメリットを提供する一方で、データ局所性やセキュリティに関する追加の要件にも柔軟に対応することができます。インターネット接続型の Cisco Intersight 仮想アプライアンスソフトウェアはオンプレミスでの導入ですが、ユーザーは SaaS 機能を活用できます。プライベート仮想アプライアンスは、さらにセキュリティ上の制約がある組織で、オンプレミスに導入できます。

Cisco Intersight Assist は、エンドポイント デバイスを Cisco Intersight に追加するのに役立ちます。データセンターには、Cisco Intersight に直接接続しない複数のデバイスを含めることができます。Cisco Intersight でサポートされているが、直接接続しないデバイスには接続メカニズムが必要です。Cisco Intersight Assist は、その接続メカニズムを提供し、デバイスを Cisco Intersight に追加するのに役立ちます。

このガイドでは、Cisco Intersight 仮想アプライアンスと Cisco Intersight Assist を環境にインストールし、セットアップする方法の概要を示します。

新機能および変更された機能に関する情報

次の表に、このガイドに記載されている新機能および機能の重要な更新の概要を示します。

表 *1:* 新機能および機能変更

更新日時	機能/機能姓	説明	参照先
2023 年 12 月	バックアップの保持	バックアップ保持を有効にするために実行する手順に関する情報を含めるようにタスクを更新しました。	バックアップのスケジュール作成
	CIFS プロトコルのサポート	CIFS プロトコルのサポートに関する情報を含めるようにタスクを更新しました。	バックアップの作成
	バックアップの保持シナリオ	さまざまなバックアップ保持シナリオと予想される結果を説明する新しい表を追加しました。	バックアップの保持シナリオ
	ポート要件	Intersight 仮想アプライアンス通信の要件としてポート 9094 を含めるようにトピックを更新しました。	ポート要件
2023 年 10 月	既存のアプライアンス展開のリソース要件。	新しいタスクには、既存のアプライアンス展開のリソース要件と、VMware vSphere インストールのディスク サイズ要件に関する情報が含まれています。	既存の Intersight 仮想アプライアンスの VM 情報技術要件
	既存のシングル ノード アプライアンス展開をマルチノード クラスタ構成に拡張するための移行パス。	既存のシングルノードアプライアンス展開をマルチノードクラスタ構成に拡張する方法の手順を含む新しいタスク。	既存のシングルノード展開からマルチノードクラスタ構成への移行パス
	外部 Syslog の設定	タスクを更新して、最大 5 つの外部 syslog サーバーを構成できるようになったという情報を追加しました。	外部 Syslog の設定
	SSL 証明書	自己署名証明書への切り替えに関する情報を含めるためにタスクを更新しました。	証明書
	アプライアンス アラーム	アプライアンスアラームの表の情報を更新しました。	Intersight 仮想アプライアンスのモニタリング
	シングルサインオン	「IdP の要件」セクションを更新して、マルチノードクラスタ構成の情報を追加しました。	Intersight 仮想アプライアンスでのシングルサインオン

更新日時	機能/機能姓	説明	参照先
2023 年 7 月	Intersight 仮想アプライアンスからのテクニカルサポートバンドルの収集	Intersight 接続済み仮想アプライアンスのテクニカル サポート バンドルを収集するためのサポートが追加されました。	テクニカル サポート
	シリアル コンソールを使用した Cisco TAC サポートの構成	シリアル コンソールを使用して Cisco TAC サポートを構成するための新しいタスクが追加されました。	シリアル コンソールを使用した Cisco TAC Support の構成 （138 ページ）
	予約済み IP アドレスの範囲の要件	構成情報セクションを更新しました	予約済み IP アドレスの範囲の要件 （18 ページ）
2023 年 2 月	マルチノード クラスタ配置 **この機能は現在、技術プレビュー段階です。テクニカル プレビューでは、まだ開発中の機能のプレビューを提供します。テクニカル プレビュー機能は、実稼働環境での使用を想定していません。GUI および API インターフェイスを含むこれらの機能は、テクニカル プレビューと一般使用の間で変更される場合があります。** **テクニカル プレビューに関するフィードバックを提供するには、電子メールを intersight-preview-feedback@cisco.com に送信してください。**	Intersight 仮想アプライアンスのマルチノードクラスタを構成する方法に関する情報を提供する新しいタスクが追加されました。	Intersight 仮想アプライアンスのマルチノードクラスタの構成
		Intersight 仮想アプライアンスのためにマルチノードクラスタ内のノードを交換する方法に関する情報を提供する新しいタスクが追加されました。	Intersight 仮想アプライアンスのマルチノードクラスタのノードを交換 （54 ページ）

更新日時	機能/機能姓	説明	参照先
2023 年 1 月	予約済み IP アドレスの範囲の要件	予約済みIPアドレス範囲の要件に関する情報を含む新しいセクションを追加しました。	予約済み IP アドレスの範囲の要件 （18 ページ）
2022 年 11 月	外部 Syslog の設定	外部 Syslog の構成タスクを更新して、構成された外部 Syslog サーバーへのすべての Intersight アラームのエクスポートのサポートを含めました。	外部 Syslog の設定 （95 ページ）
	サポートされている構成の制限	大規模な展開に関する情報を含むように格納ファイルを更新しました。	Intersight 仮想アプライアンスでサポートされる構成の制限 （89 ページ）
2022 年 4 月	Intersight 仮想アプライアンスのモニタリング	「Intersight 仮想アプライアンス モニタリング」セクションに、接続型仮想アプライアンスによって UCS C シリーズ サーバー関連の障害が外部の Syslog サーバーに転送されないことを説明する注記を追加しました	Intersight 仮想アプライアンスのモニタリング （81 ページ）
	外部 Syslog の設定	外部 Syslog の設定タスクに、接続型仮想アプライアンスによって UCS C シリーズ サーバー関連の障害が外部 Syslog サーバーに転送されないことを説明した注記を追加しました。	外部 Syslog の設定 （95 ページ）
2022 年 1 月	ハイ アベイラビリティとディザスタ リカバリ	ベンダーが提供するソリューションを使用してハイ アベイラビリティを活用する方法に関する情報を追加しました。また、Intersight Virtual Appliance の既存のバックアップと復元機能や、その他のサードパーティ ソリューションを使用したディザスタリカバリーに関する情報も含まれています。	Cisco Intersight 仮想アプライアンスのハイアベイラビリティおよびディザスタリカバリ （56 ページ）
2021 年 12 月	『Intersight Assist Getting Started Guide』のコンテンツを『Intersight Virtual Appliance Getting Started Guide』とマージしました。	このガイドには、Intersight Virtual Appliance と Intersight Assist の両方のインストールとセットアップに関する情報が含まれています。	Cisco Intersight 仮想アプライアンスについて （11 ページ） Cisco Intersight Assist について （22 ページ）

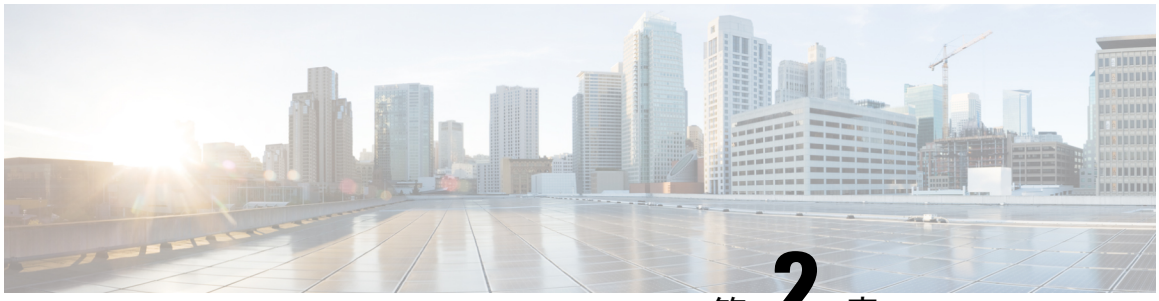
更新日時	機能/機能姓	説明	参照先
2021 年 11 月	アカウント設定の構成	「監査ログの保持期間」フィールドに関する情報を含めるために、「アカウント設定の構成」タスクを更新しました。	アカウント設定の構成
2021 年 10 月	Intersight 仮想アプライアンスのセットアップ	Intersight 接続型仮想アプライアンス、Intersight プライベート仮想アプライアンス、および Intersight Assist を設定するための新しいタスクが追加されました。	シングルノード Intersight 接続型仮想アプライアンスのセットアップ
	Intersight 仮想アプライアンスのリカバリ	Intersight 仮想アプライアンスをリカバリする方法に関する情報を提供する新しいタスクが追加されました。	Intersight 接続型仮想アプライアンスのリカバリ
	Intersight 仮想アプライアンス ソフトウェアの更新	Intersight 接続型仮想アプライアンスおよびIntersight プライベート仮想アプライアンスの更新方法に関する情報を提供するタスクを追加しました。	Intersight 接続型仮想アプライアンス ソフトウェアの更新
2021 年 7 月	Intersight 仮想アプライアンス設定の拡張	既存のTLSプロトコルに加えて、UDPおよびTCPプロトコルのサポートを含むように、外部syslogの設定タスクが更新されました。	外部 Syslog の設定 （95 ページ）
		ロール作成タスクが更新され、ロールごとの同時セッションの最大数の設定に関する情報が追加されました。	ロールの追加 （112 ページ）
2021 年 5 月	Intersight 仮想アプライアンス設定の拡張	Intersight 仮想アプライアンスのソフトウェアパッケージのダウンロード方法に関する情報を提供するタスクが更新されました。	Intersight 仮想アプライアンスのソフトウェアパッケージのダウンロード （60 ページ）
	NTP サーバーの設定	NTPサーバーの設定方法に関する情報を提供するタスクが更新されました。	NTP の設定 （94 ページ）

更新日時	機能/機能姓	説明	参照先
2021 年 2 月	Intersight 仮想アプライアンス設定の拡張	ローカルユーザーのパスワードポリシーの設定に関する情報を含む新しいタスクが追加されました。 ログイン画面の前に表示するバナーメッセージの設定に関する情報を含む新しいタスクが追加されました。	ローカルユーザー向けパスワードポリシーの設定 （106 ページ） ログイン画面の前に表示するバナーメッセージの設定 （93 ページ）
	KVMハイパーバイザへのアプライアンスのインストール	KVMハイパーバイザにCisco Intersight仮想アプライアンスをインストールする方法に関する情報を提供する新しいタスクが追加されました。	KVM ハイパーバイザでの Cisco Intersight 仮想アプライアンスおよび Intersight Assist のインストール （35 ページ）
2021 年 1 月	Intersight 仮想アプライアンス設定の拡張	Intersight Virtual ApplianceのIntersight Intelligenceの更新に関する情報を含む新しいタスクを追加しました。	Intersight Connected Virtual Appliance の Intersight Intelligence の更新 （89 ページ）
2020 年 10 月	Intersight 仮想アプライアンス設定の拡張	外部syslogの設定に関する情報を含む新しいタスクが追加されました。	外部 Syslog の設定 （95 ページ）
	エンドポイント向け IPv6 のサポート	このセクションを更新して、IPアドレスの設定に関する情報を追加しました。	Intersight 仮想アプライアンスおよび Intersight Assist のメンテナンス シェル （123 ページ）

更新日時	機能/機能姓	説明	参照先
2020 年 7 月	ライセンス要件	この項を更新して、Intersightプライベート仮想アプライアンスのライセンス要件を追加しました。	Intersight 仮想アプライアンスのライセンス要件 （12 ページ）
	テクニカル サポート	Intersight仮想アプライアンスからのテクニカルサポートバンドルの収集に関する情報を含む新しいセクションが追加されました。	テクニカル サポート （135 ページ）
	Microsoft Hyper-V サーバーにアプライアンスをインストール	Microsoft Hyper-V ServerにCisco Intersight仮想アプライアンスをインストールする方法に関する情報を提供する新しいタスクが追加されました。	Microsoft Hyper-V Server 上の Cisco Intersight 仮想アプライアンスおよび Intersight Assist のインストール （32 ページ）
	プライベート アプライアンス アカウントの作成	Intersightプライベート仮想アプライアンス導入用のソフトウェアパッケージをダウンロードするためのプライベートアプライアンスアカウントの作成に関する情報を提供する新しいタスクが追加されました。	ソフトウェアパッケージをダウンロードするためのアプライアンス アカウントの作成 （59 ページ）
	ソフトウェア パッケージのダウンロード	Intersightプライベート仮想アプライアンス導入のソフトウェアパッケージのダウンロードに関する情報を提供する新しいタスクが追加されました。	Intersight 仮想アプライアンスのソフトウェア パッケージのダウンロード （60 ページ）
	ソフトウェアパッケージのアップロード	Intersightプライベート仮想アプライアンス導入のソフトウェアパッケージのアップロードに関する情報を提供する新しいタスクが追加されました。	Intersight プライベート仮想アプライアンスのソフトウェアパッケージのダウンロード （61 ページ）

更新日時	機能/機能姓	説明	参照先
2020 年 3 月	設定の選択	既存の手順にステップが追加されました。	VMware vSphere 上の Cisco Intersight 仮想アプライアンスおよび Intersight Assist のインストール （27 ページ）
	Intersight 仮想アプライアンスでサポートされる構成の制限	新しく追加された **[最小（8 vCPU、16 Gi RAM）（Tiny (8 vCPU, 16 Gi RAM)）]** オプションは、Intersight Assist の展開にのみ適用されます。	Intersight 仮想アプライアンスでサポートされる構成の制限 （89 ページ）
2020 年 2 月	LDAP 設定	複数の LDAP ドメインのサポートが追加されました。 電子メールを必要としないLDAP/AD設定のサポートが追加されました。	LDAP の設定 （100 ページ）
	IP アドレスの変更	仮想アプライアンス VM の IP アドレスを変更する機能が追加されました。	Intersight 仮想アプライアンスおよび Intersight Assist のメンテナンスシェル （123 ページ）
2020 年 1 月	組織	組織には、アカウント内でマルチテナンシーをサポートし、システム定義の権限を持つユーザー定義ロールを作成する機能があります。	ロールの追加 （112 ページ）および組織の追加 （115 ページ）
	証明書	ユーザーが送信した証明書を許可し、自己署名証明書を作成できるようにします。	証明書 （102 ページ）
2019 年 12 月	Intersight 仮想アプライアンスでサポートされる構成の制限	Intersight 仮想アプライアンスは、2000 または 5000 サーバーをサポートするために、小規模または中規模の展開サイズで導入できます。	Intersight 仮想アプライアンスでサポートされる構成の制限 （89 ページ）
	アプライアンス VM のグレースフル リブート	Intersight 仮想アプライアンスは、Intersight アプライアンスの診断ツールから正常に再起動できます。	Intersight 仮想アプライアンスおよび Intersight Assist のメンテナンスシェル

更新日時	機能/機能姓	説明	参照先
2019 年 7 月	クラウド接続に基づくアラート	クラウド接続と中断された接続の影響についてユーザーに警告する拡張メッセージ。	Intersight 接続型仮想アプライアンスのネットワーク接続 （91 ページ）
	Intersight アプライアンス診断ツール	アプライアンスのインストール中の設定ミスやネットワークの問題のトラブルシューティングと対処に役立つコンソールベースの診断ツール。	トラブルシューティング
2019 年 6 月	DHCP のサポート	静的 IP アドレスを使用しないように、アプライアンスが同じネットワーク上で実行されている DHCP サーバーから IP アドレスを取得できるようにします。	Cisco Intersight 仮想アプライアンスのインストール
	バックアップのスケジュール作成	スケジュールに基づいてアプライアンス内のデータの完全な状態の定期バックアップをスケジュール設定し、バックアップされたデータをリモート サーバーに保存します。	バックアップのスケジュール作成 （86 ページ）



第 2 章

概要

Cisco Intersight 仮想アプライアンスの概要

Cisco Intersight 仮想アプライアンスについて

Cisco Intersight 仮想アプライアンスでは、展開が容易な VMware OVA、Microsoft Hyper-V Server VM および Linux の KVM ハイパーバイザで Intersight の管理機能が提供されます。Intersight 仮想アプライアンスは、インテリジェント レベルの管理を提供する Cisco Intersight の利点を享受でき、これにより、お客様は、データの局所性、セキュリティ、コンプライアンス要件に対する柔軟性を高めながら、前世代のツールよりも高度な方法で環境を分析、簡素化、自動化できます。

Intersight 仮想アプライアンスは、次のいずれかのモードで展開できます。

- Intersight 接続型仮想アプライアンス
- Intersight プライベート仮想アプライアンス

Intersight 接続型仮想アプライアンスでは、どのシステム情報がプレミス外に出るかを制御しながら、Intersight の管理機能を利用できます。Intersight 接続型仮想アプライアンスの展開では、自動更新および全機能の利用に必要なサービスへのアクセスのため、シスコおよび Intersight サービスに接続する必要があります。

Intersight プライベート仮想アプライアンスでは、システム情報がプレミス外に出ないよう制御しながら、Intersight の管理機能を利用できます。Intersight プライベート仮想アプライアンスの導入は、切断（エアギャップ）モードでデータセンターを運用する環境を対象としています。

Intersight Assist の概要については、「Cisco Intersight Assist について （22 ページ）」を参照してください。

シングルノード仮想マシンとして Intersight 仮想アプライアンスを短時間に既存の環境内に展開できます。

また、Intersight Virtual Appliance をマルチノード クラスターとして展開して、高可用性、安定性の向上、回復力の向上を実現することもできます。単一ノードアプライアンスの初期セットアップが完了したら、追加ノードを加えることができます。2 つの追加ノードを正常に追加したら、Intersight 仮想アプライアンスでマルチノード クラスタを作成できます。

このガイドでは、Intersight 仮想アプライアンスを環境にインストールし、セットアップする方法の概要を示します。

（注） Intersight 仮想アプライアンスは、トランスポート レイヤセキュリティを改善するため、HTTPS 通信に対して TLS 1.3 プロトコルをサポートします。

注目 Intersight Virtual Appliance をインストールしてセットアップする前に、新規の Intersight 仮想アプライアンスの VM 情報技術要件 セクションに記載されている情報を読むことを強くお勧めします。

Intersight の機能の最新の更新については、「Intersight アプライアンス ヘルプセンター」を参照してください。

Intersight 仮想アプライアンスのライセンス要件

Cisco Intersight 仮想アプライアンスはアプライアンスの機能を使用するために必要なサブスクリプションベースのライセンスを使用します。Intersight Essentials は **シスコ スマート ライセンス**によって提供されるサブスクリプション ライセンスです。Intersight Essentials を購入するには、シスコの営業担当者、チャネル パートナー、またはリセラーにお問い合わせください。これらのプラットフォームとは、正式な Cisco UCS Manager、Cisco IMC、Cisco HyperFlex ソフトウェアを含む Cisco Intersight デバイス コネクタのある Cisco UCS と Cisco HyperFlex システムです。

接続済み仮想アプライアンスを展開する場合は、Cisco Intersight 仮想アプライアンスの初期セットアップの一環としてライセンスを登録する必要があります。アプライアンスのインストールを完了したら、UI を起動し、インストール時に設定したパスワードでログインし、アプライアンスを Intersight に接続してライセンスを登録します。

初期セットアップ後に設定を編集する場合は、次の手順を実行します。

1. アプライアンス UI で、**[サービス セレクタ（Service Selector）]** ドロップダウン リストから **[システム（System）]** を選択し、**[設定（Settings）]** > **[ライセンス（Licensing）]** > **[ライセンスを登録（Register License）]**に移動します。

   [スマート ソフトウェア ライセンス製品の登録（Smart Software Licensing Product Registration）] ウィンドウが表示されます。

2. 製品インスタンス登録トークンがない場合は、**Cisco Smart Software Manager** の特定の仮想アカウントからトークンを生成します。

3. **Cisco Smart Software Manager** から取得した製品インスタンス登録トークンを入力し、**[登録（Register）]** をクリックします。Cisco Intersight のライセンス階層と登録に関するビデオを見るには、ここをクリックしてください。

プライベート仮想アプライアンスを展開する場合は、Cisco Intersight 仮想アプライアンスの初期セットアップの一環としてライセンスを予約する必要があります。初期設定の一部としてライセンスを予約する方法については、シングルノード Intersight プライベート仮想アプライアンスのセットアップ （44 ページ） を参照してください。

プライベート仮想アプライアンスの初期セットアップ後にライセンスを **更新** または **返却** する方法については、「Intersight プライベート仮想アプライアンスライセンスの更新」および「Intersight プライベート仮想アプライアンスライセンスの返却」を参照してください。

Cisco Intersight 仮想アプライアンスの Intersight 評価版ライセンスは、シスコの営業担当者、チャネル パートナー、またはリセラーから取得できます。Cisco スマート アカウントをすでに取得している場合、評価版ライセンスが Cisco スマート アカウントに追加されます。追加されたら、スマート アカウントに仮想アカウント用のトークンを生成して Cisco Intersight 仮想アプライアンス の登録に進むことができます。ライセンスのアクティブ化および管理の方法やスマート ライセンスの詳細については、「スマート ライセンスの管理」を参照してください。

Cisco Smart Software Manager の**予約ライセンス**機能の詳細については、『Smart Software Manager の概要』を参照してください。

システム要件

新規の Intersight 仮想アプライアンスの VM 情報技術要件

Cisco Intersight 仮想アプライアンスは、VMware ESXi 7.0 以降、Microsoft Hyper-V Server 2016 および 2019、Linux 上の KVM ハイパーバイザに導入できます。Intersight 仮想アプライアンスは、中規模または大規模の構成で展開できます。

Intersight 仮想アプライアンスのサイズ オプションとサポートされる最大設定制限の詳細については、Intersight 仮想アプライアンスでサポートされる構成の制限を参照してください。

表 *2*：新規の *Intersight* 仮想アプライアンス展開のリソース要件

Resource	**要件**	
	中規模	**大規模**
vCPU（AVX 必須）	24	48
RAM	64 GiB	96 GiB
ストレージディスク（Disk）	2 TiB*	2 TiB*

Resource	要件	
	中規模	大規模
サポートされるハイパーバイザ	VMware ESXi 7.0 以降と VMware vSphere Web クライアント 7.0 以降 Microsoft Hyper-V Server 2016 および 2019 Linux 上の KVM ハイパーバイザ	

*Cisco では、シック プロビジョニングを使用することを推奨しています。シン プロビジョニングを使用することが可能である一方、オーバープロビジョニングはストレージのキャパシティ不足を導き、サービスの低下や損失につながり、バックアップからの復元が必要になることがあります。

小規模構成は既存の展開で引き続きサポートされます。詳細については、「既存の Intersight 仮想アプライアンスの VM 情報技術要件 （16 ページ）」を参照してください。

注目

- VMware vSphere に Intersight 仮想アプライアンスをインストールしている間は、ディスクサイズのデフォルト設定を変更しないでください。ディスク サイズは、展開構成に基づいて計算されます。
- AVX 機能をサポートする CPU が必須です。VMware vSphere クラスタ向けに構成された vMotion との拡張された互換性（EVC）レベルの場合、EVC レベルが AVX 機能をサポートする CPU ファミリに設定されていることを確認してください。
- 割り当てられたリソースが中規模展開に必要なデフォルト値（vCPU の場合は 24、RAM の場合は 64 GiB）を下回る場合、展開に使用できるオプションは Assist のみになります。他のオプションはグレー表示されます。
- **メトリック収集**：
  - メトリック収集はオプトイン機能であり、現在は単一ノード展開でのみサポートされています。メトリック収集の構成方法については、「メトリック収集の構成」を参照してください。
  - メトリック収集が有効になっている場合、中規模構成では最大 500 台の IMM サーバを要求でき、大規模構成では最大 2000 台の IMM サーバを要求できます。ただし、中規模および大規模の構成でサポートされている制限まで、追加の UMM サーバを要求できます。
  - メトリックが収集されるアクティブ サーバの数が、アプライアンスのサイズがサポートできるしきい値（中規模または大規模）を超えると、Intersight 仮想アプライアンスはメトリック収集を自動的に無効にします。この予防措置は、パフォーマンスへの悪影響を防ぎ、手動による介入を必要とせずにシステムを円滑に運用できるようにするために行われます。メトリック収集を無効にすると、この機能のリソース要件が満たされた後に、手動で有効にする必要があります。
  - メトリック収集が有効になっている間に収集されたメトリックは、メトリック収集が後で一時停止された場合でも、引き続きアクセスできます。これにより、将来の分析と参照のために履歴データセットを継続的に使用できます。メトリック収集が無効になっている場合でも、メトリックのストレージおよび保持ポリシーの適用は継続されます。
  - メトリック収集に関する詳細は、「モニタリング概要」を参照してください。
- **マルチノード展開のための追加のネットワーク要件**
  - ディスクの書き込み速度は 150 Mbps を超える必要があります。
  - ノード間の遅延は 9 ミリ秒未満である必要があります。
  - ノードの 3 つのホスト名はすべて、同じ DNS サーバーのセットによって解決される必要があります。

既存の Intersight 仮想アプライアンスの VM 情報技術要件

Intersight は、CPU、RAM、およびディスクに必要な変更を評価して、クラウド サービスからの更新後に、再起動中の展開サイズを決定します。評価の結果として、次のいずれかの結果が発生します。

- 特定の展開サイズに必要な最小限のリソースが使用できない場合は、Intersight サービスがシャットダウンされ、アプライアンスの電源がオンのままになります。ただし、アプライアンスが機能しておらず、実行中のサービスが不安定になっている可能性があります。アプライアンス メンテナンス シェルの再起動中に、リソース ステータスに関するエラー メッセージが表示されます。エラーと必要な修正措置の詳細については、メンテナンス シェルにログインしてください。
- 展開サイズが既存の展開と同じ場合、VM は変更なしで再起動します。技術情報要件を決定した後で、より大きな展開サイズにアップグレードできます。

表 *3*: 既存の *Intersight* 仮想アプライアンス展開のリソース要件

Resource	要件		
	小規模	中規模	大規模
vCPU	16	24	48
RAM (GiB)	32	64	96
ストレージディスク（Disk）	620GiB 以上*	2TiB*	2TiB*
サポートされるハイパーバイザ	VMware ESXi 7.0 以降と VMware vSphere Web クライアント 7.0 以降 Microsoft Hyper-V Server 2016 および 2019 Linux 上の KVM ハイパーバイザ		

（注）
- *Cisco では、シック プロビジョニングを使用することを推奨しています。
- 並べ替えとフィルタ機能は、中規模および大規模の展開でのみサポートされます。
- 今後のメトリックの収集と可視化機能は、中規模および大規模の展開でのみサポートされます。必要なリソースが適切にプロビジョニングされていることを確認します。

サポートされているハードウェア システムとソフトウェア バージョンの詳細については、サポートされているハードウェア システムとソフトウェア バージョンを参照してください。

Intersight 仮想アプライアンス展開のリソースの管理

Intersight 仮想アプライアンス展開のリソースの管理

Intersight 仮想アプライアンスの展開サイズを表示し、次のように CPU、RAM、およびディスクサイズを変更できます。

1. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから **[システム（System）]** を選択します。
2. **[設定（Settings）]** > **[一般（General）]** >**[アプライアンス（Appliance）** に移動します。
3. サポートされているその他のスケーリング オプションを確認し、要件に合わせて適切な展開サイズを選択します。
4. サポートされている展開オプションの技術情報要件の詳細を確認した後、VM をシャットダウンし、必要に応じて CPU、RAM とディスク サイズを変更し、VM を再起動します。

（注）
- スナップショットがある場合は、ディスク サイズを変更できません。
- 仮想アプライアンスのサイズオプションを使用するには、Intersight Cloud サービスから最新のアップグレードを行う必要があります。

次の表に、Intersight 仮想アプライアンスのディスク サイズ要件に関する情報を示します。

表 *4 : Intersight* 仮想アプライアンス インストールのためのディスク サイズ要件

ディスク	すべての展開の最小ディスク サイズ要件	中規模および大規模の展開で推奨されるディスク サイズの要件
ディスク 1	ディスク サイズは変更しないでください。	ディスク サイズは変更しないでください。
Disk2	25 GiB	25 GiB
Disk3	150 GiB	150 GiB
Disk4	150 GiB	150 GiB
Disk5	100 GiB	190 GiB
Disk6	30 GiB	60 GiB
Disk7	60 GiB	360 GiB
Disk8	60 GiB	1190 GiB

（注） または、アプライアンスの最新のバックアップを使用して復元を実行することで、ディスク要件を満たすことができます。詳細については、「Intersight 接続型仮想アプライアンスのリカバリ」と「Intersight プライベート仮想アプライアンスのリカバリ」を参照してください。

IP アドレスとホスト名の要件

Intersight 仮想アプライアンスの IP アドレスおよびホスト名の要件

シングルノード Intersight 仮想アプライアンスをセットアップするには、IP アドレス 1 つと、その IP アドレスの DNS レコードが 2 つ必要です。DNS レコードは次の形式である必要があります。

- **myhost.mydomain.com**：この形式の DNS レコードを使用して GUI にアクセスします。これは、DNS で **A レコードと関連する PTR レコード**として定義する必要があります。PTR レコードは IP アドレスの逆引きルックアップに必要です。IP アドレスが複数のホスト名に解決される場合、最初に解決されたホスト名が使用されます。
- **dc-myhost.mydomain.com**：**dc-** をホスト名の先頭に追加する必要があります。この DNS レコードは、 **myhost.mydomain.com の CNAME** として定義する必要があります。アプライアンスがこの形式の DNS レコードを内部的に使用してターゲットの接続を管理します。

Intersight 仮想アプライアンスのマルチノードクラスタの設定は、3 つのホスト名、3 つの IP アドレスとそれぞれのホスト名に対して 1 つの DC-CNAME が必要です。フォーマットの例を次に示します：

- **myhost1.mydomain.com**
- **myhost2.mydomain.com**
- **myhost3.mydomain.com**
- **dc-myhost1.mydomain.com**
- **dc-myhost2.mydomain.com**
- **dc-myhost3.mydomain.com**

注目 前述のように、タイプ **A、CNAME、および PTR レコード**の適切なエントリが DNS にあることを確認します。

予約済み IP アドレスの範囲の要件

Intersight 仮想アプライアンスは、内部通信用に次の IP アドレス範囲を予約しています：

- **172.16.0.0/12 の範囲内の /20 サブネット**：このサブネットは、アプライアンスのインストール中に 1 回だけ設定できます。

- **192.168.20.21/32**：この IP アドレスはアプライアンスによって予約されており、構成できません。

ポート要件

Intersight 仮想アプライアンスのポート要件

次の表に、Intersight 仮想アプライアンス通信に必要があるポートのリストを示します。

ポート	プロトコル	アプライアンス構成モード	説明
443	TCP	シングルノードとマルチノード	このポートは次の通信に必要です。 • **Intersight 仮想アプライアンスとユーザーの Web ブラウザ間の通信。** • **Intersight 仮想アプライアンスとエンドポイントターゲット間の通信。** 接続の詳細については、「Intersight Connected Virtual Appliance のネットワーク接続要件」を参照してください。
53、67、68	UDP	シングルノードとマルチノード	これらのポートは、DNS および NTP トラフィックの送受信に使用されます。
2379、6443、2380、9092、9094、9100、1025	TCP	マルチノード	これらのポートは、Intersight 仮想アプライアンスのマルチノード構成で VM 間の通信に使用されます。
51820、51821	UDP	マルチノード	これらのポートは、Intersight 仮想アプライアンスのマルチノード構成で VM 間の VPN のセキュア化に使用されます。

Intersight Connected Virtual Appliance のネットワーク接続要件

（注） このセクションの情報は、Intersight 接続型仮想アプライアンスの展開にのみ適用されます。

- Cisco Intersight 仮想アプライアンス が次のサイトに直接か、またはプロキシを介して接続できることを確認します。プロキシの設定については、Intersight 接続型仮想アプライアンスのネットワーク接続 （91 ページ）を参照してください。次のすべての URL には HTTPS を使用してアクセスします。

- Cisco サービスにアクセスします (*. cisco.com)。

シスコサービス	説明	ターゲット デバイス
smartreceiver.cisco.com:443	Cisco Smart Licensing Manager にアクセスする場合	すべてのサーバに必要
swapi.cisco.com:443	Cisco Smart Licensing Manager にアクセスする場合	すべてのサーバに必要
tools.cisco.com:443	Cisco Smart Licensing Manager にアクセスする場合	すべてのサーバに必要
download-ssc.cisco.com*、dl.cisco.com、dl1.cisco.com、dl2.cisco.com	Cisco ソフトウェアのダウンロードサイトにアクセスする場合	次の場合に必要です。 • C シリーズ スタンドアロン サーバ • UCSM に管理された B シリーズおよび C シリーズ サーバー： • UCSM に管理されたファブリック インターコネクト • UCSM に管理されたファブリック インターコネクトが添付された Cisco UCS S3260 シャーシ
api.cisco.com:443		
cloudsso.cisco.com:443		

*Cisco Intersight を使用すると、新しいドメイン *download-ssc.cisco.com* を介してファームウェアのダウンロードを管理できます。この新しいドメインをファイアウォール ルールとネットワーク ルールに必ず追加してください。詳細については、Cisco ソフトウェア ダウンロードを参照します。

- Intersight クラウド サービスへのアクセス。

  Intersight 仮想アプライアンスは、次のいずれかの URL を解決することによって interswitch に接続します。

（注） 特定の URL の IP アドレスが変更される可能性があります。固定 IP を使用する URL のファイアウォール設定を指定する必要がある場合。次に、各リージョンに対応する静的IPアドレスを示します。

北米（us-east-1）リージョン

- svc-static1.intersight.com（**推奨**）。
- svc-static1.ucs-connect.com（**今後廃止予定**）
- これらの URL はどちらも次の IP アドレスに解決されます。
  - 3.208.204.228
  - 54.165.240.89
  - 3.92.151.78

EMEA（eu-central–1）リージョン

- svc.eu-central-1-static1.Intersight.com
- これらの URL はどちらも次の IP アドレスに解決されます。
  - 99.84.238.166
  - 99.84.238.204
  - 99.84.238.94
  - 99.84.238.110

サポートされるブラウザ

Intersight 仮想アプライアンスでサポートされるブラウザ

Cisco Intersight は、以下のサポートされているブラウザのバージョン以降で動作します。

- Google Chrome 62.0.3202.94
- Firefox 57.0.1
- Safari 10.1.1
- Microsoft Edge (Chromium) Beta

ソフトウェアの互換性

Intersight 仮想アプライアンスのソフトウェア互換性

この項では、アプライアンスでサポートされている次のソフトウェアの最小バージョンの詳細を示します。

コンポーネント	サポートされている最小バージョン
Cisco UCS Manager	3.2(1)
Cisco HyperFlex Connect およびデータ プラットフォーム	2.6
Cisco IMC	3.1(3)（M5 サーバーの場合） 3.0(4)（M4 サーバーの場合） M4 サーバーと M5 サーバーの Cisco IMC ソフトウェアの要件の詳細については、ヘルプセンターの「サポートされるシステム」の項を参照してください。 サポートされるソフトウェアとデバイス コネクタの必要なバージョンの詳細なリストについては、『デバイス コネクタ要件』を参照してください。
Cisco UCS Director	6.7.2.0
Cisco Intersight 管理モード	4.1(2a)

Cisco Intersight Assist の概要

Cisco Intersight Assist について

Cisco Intersight Assist は、エンドポイント デバイスを Cisco Intersight に追加するのに役立ちます。データセンターには、Cisco Intersight に直接接続しない複数のデバイスを含めることができます。Cisco Intersight でサポートされているが、直接接続しないデバイスには接続メカニズムが必要です。Cisco Intersight Assist は、その接続メカニズムを提供し、デバイスを Cisco Intersight に追加するのに役立ちます。

Cisco Intersight Assist を使用すると、Intersight が、Intersight へのダイレクトパスを持っておらず、組み込みの Intersight デバイスコネクタを備えていないターゲットと通信できるようになります。これらには、ストレージデバイス、ハイパーバイザマネージャー、アプリケーション パフォーマンス管理製品などのターゲットが含まれます。Intersight Assist は、ターゲットのネイティブ API と通信し、Cisco Intersight との間の通信ブリッジとして機能します。Intersight Assist サービスは、Cisco Intersight SaaS とともに使用すると、スタンドアロン アプライアンス

として実行されます。接続型仮想アプライアンスとプライベート仮想アプライアンスの場合、サービスが併置されるため、個別の Assist アプライアンスは必要ありません。

アプライアンス UI > **ターゲット**に移動すると、Intersight Assist の詳細を表示できます。

セットアップウィザード中にインストーラから Cisco Intersight Assist をインストールすることを選択できます。ESXi サーバー、カーネルベースの仮想マシン (KVM)、HyperV ハイパーバイザにインストールできます。

（注） Intersight Assist の登録を解除することはできず、アプライアンスで別の Intersight Assist を要求することもできません。

Cisco Intersight に Intersight Assist を要求した後、[Intersight Assistによる要求（Claim Through Intersight Assist）] オプションを使用してエンドポイントデバイスを要求できます。詳細については、「ターゲットの要求」を参照してください

（注） Intersight 仮想アプライアンスは、トランスポートレイヤセキュリティを改善するため、HTTPS 通信に対して TLS 1.3 プロトコルをサポートします。

Cisco Intersight Assist は、IPv6 構成をサポートしていません。

Pure Storage デバイス、Hitachi Virtual Storage Platform デバイス、NetApp ストレージコントローラ、VMware vCenter などのデバイスを、Cisco Intersight Assist を使用して要求した後、Cisco Intersight に追加できるようになりました。

Intersight Assist のライセンス要件

ライセンスに関する詳細については、Cisco Intersight のライセンスを参照してください。

Intersight Assist のシステム要件

Intersight Assist の VM リソース要件

Cisco Intersight Assist は、カーネルベースの仮想マシン (KVM)、HyperV ハイパーバイザ、VMware ESXi 7.0 以降に、VMware vSphere Web Client 7.0 以降の Microsoft Hyper-V Server 2016 および 2019 とともに展開できます。ここでは、Cisco Intersight Assist をインストールして展開するためのシステム要件について説明します。Intersight Assist の展開には、小（Small）、中（Medium）と大（Large） のオプションがあります。

新規展開：Intersight 仮想アプライアンスは、小規模、中規模、または大規模の構成で展開できます。

既存の展開：既存の展開は、小規模、小規模、中規模、および大規模の構成でサポートされます。ただし、既存の小規模展開を小規模、中規模、または大規模構成に移行することを**お勧め**します。

（注）
- 小規模展開は、既存の Assist 展開でのみサポートされ、Intersight Orchestrator にのみ適用されます。

表 *5 : Intersight Assist* のリソース要件

Resource	要件			
	極小（既存の展開でのみサポート）	**小**	**中**	**大規模**
vCPU（AVX 必須）	8	16	24	48
RAM	16 GiB	32 GiB	64 GiB	96 GiB
Supported Features	ICO と IKS	ICO、IWO、IST、IKS	ICO、IWO、IST、IKS	ICO、IWO、IST、IKS
サポートされるハイパーバイザ	VMware ESXi 7.0 以降 VMware vSphere Web Client 7.0 以降 カーネルベース仮想マシン (KVM) Hyper-V ハイパーバイザ			

（注）
- AVX 機能をサポートする CPU が必須です。VMware vSphere クラスタ向けに構成された vMotion との拡張された互換性（EVC）レベルの場合、EVC レベルが AVX 機能をサポートする CPU ファミリに設定されていることを確認してください。

次の表では、Intersight Workload Optimizer に Cisco Intersight Assist を展開するためのシステム要件について説明します。

表 *6 : Intersight Workload Optimizer* の *Intersight Assist* リソース要件

リソース要件	システム要件		
	小	**中**	**大規模**
vCPU（AVX 必須）	16	24	48
RAM	32 GiB	64 GiB	96 GiB

リソース要件	システム要件		
ストレージ（ディスク）	500 GiB	500GiB/2TiB*	2 TiB*
設定の導入	最大 1000 の仮想マシン	最大 30000 の仮想マシン	最大 100,000 の仮想マシン

（注）
- *既存の展開は、500GiB のままにするか、2TiB にアップグレードすることで、**小規模**構成から**中規模**構成にアップグレードできます。
- ***中規模**および**大規模**構成の新しい展開は、2TiB のフルディスク サイズ構成でのみサポートされます。
- AVX 機能をサポートする CPU が必須です。VMware vSphere クラスタ向けに構成された vMotion との拡張された互換性（EVC）レベルの場合、EVC レベルが AVX 機能をサポートする CPU ファミリに設定されていることを確認してください。

以下のテーブルは、Intersight Service for HashiCorp Terraform Service（IST）の Cisco Intersight Assist のリソース要件をリストしています。

表 *7 : Intersight Service for HashiCorp Terraform Service (IST)* の *Intersight Assist* リソース要件

リソース	要件		
	小	中	大規模
vCPU（AVX 必須）	16	24	48
RAM	32 GiB	64 GiB	96 GiB
Terraform Agent の数	5	5	5

（注）
- AVX 機能をサポートする CPU が必須です。VMware vSphere クラスタ向けに構成された vMotion との拡張された互換性（EVC）レベルの場合、EVC レベルが AVX 機能をサポートする CPU ファミリに設定されていることを確認してください。

Intersight Assist のポート要件

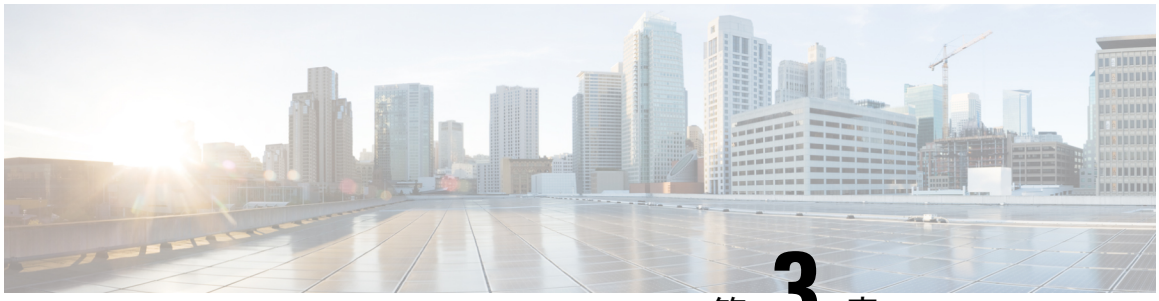
次の表に、Cisco Intersight Assist の通信のために開いておく必要があるポート番号を示します。

ポート	プロトコル	説明
443	TCP/UDP	次の通信に必要です。 • Cisco Intersight Assist とユーザーの Web ブラウザ間。 • Cisco Intersight Assist とエンドポイントデバイス間。

Intersight Assist でサポートされるブラウザ

Cisco Intersight Assist および Cisco Intersight は、以下のサポートされているブラウザのバージョン以降で動作します。

- Google Chrome 62.0.3202.94
- Firefox 57.0.1
- Safari 10.1.1
- Microsoft Edge (Chromium) Beta



第 3 章

インストール

VMware vSphere 上の Cisco Intersight 仮想アプライアンスおよび Intersight Assist のインストール

Cisco Intersight 仮想アプライアンスは、オープン仮想アプライアンス（OVA）ファイル形式、ZIP ファイル形式、または TAR ファイル形式で含まれている展開可能な仮想マシンとして配布されます。Cisco Intersight 仮想アプライアンスは VMware ハイアベイラビリティ (VMHA) をサポートしており、仮想アプライアンスの動作が中断しないことを保証します。VMHA の詳細については、vmware.com のマニュアルを参照してください。

注目 Intersight 仮想アプライアンスと Intersight Assist OVA は、VMware vCenter を使用して展開する必要があります。OVA を ESXi サーバーに直接展開することはできません。

デフォルトでは、VMware vCenter には、Intersight 仮想アプライアンス OVA ファイルの Cisco デジタル署名を検証する認証局（CA）が含まれていません。VMware vCenter GUI に、OVA の証明書が無効であり、信頼されていないことが示されます。可能ですが、**この警告を無視せず**にインストールを続行することをお勧めします。代わりに、次の表から、Intersight 仮想アプライアンス OVA ファイルのデジタル署名を検証する適切なルート CA をダウンロードしてインストールします。署名を検証することで、OVA が Cisco によって発行され、サードパーティによって変更されていないことが保証されます。

次の表に示すルート CA 証明書は、 Cisco の PKI ページで入手できます。

OVA バージョン	CA 発行者	CA シリアル番号	CA の有効期限

1.1.0-0]	TrustID EV コード署名 CA 4	40179e0104d0d1e884e3e897403	2030 年 3 月 18 日
1.0.9-630	TrustID EV コード署名 CA 4	40179e0104d0d1e884e3e897403	2030 年 3 月 18 日
1.0.9-588	DigiCert 信頼済み G4 コード署名 2021 CA1	8ad40b260d29e495acd9bd93acd9	2036 年 4 月 28 日
1.0.9-499	なし	なし	なし
1.0.9-342	DigiCert 信頼済み G4 コード署名 2021 CA1	8ad40b260d29e495acd9bd93acd9	2036 年 4 月 28 日

次のタスクの手順を使用して、VMware vSphere にアプライアンスをインストールして、展開します。**VMware vSphere にマルチノード Intersight 仮想アプライアンスをインストールして展開するには、次のタスクの手順を 3 回繰り返します。**

始める前に

シスコの担当者が提供した URL または、ローカル ハード ドライブ、ネットワーク共有ドライブまたは CD/DVD ドライブなど、セットアップからアクセス可能な場所から、Cisco Intersight 仮想アプライアンス パッケージをダウンロードしたことを確認します。

注目

- Intersight Virtual Appliance をインストールしてセットアップする前に、新規の Intersight 仮想アプライアンスの VM 情報技術要件 セクションに記載されている情報を読むことを強くお勧めします。
- シングルノード Intersight 仮想アプライアンスをセットアップするには、IP アドレス 1 つと、その IP アドレスの DNS レコードが 2 つ必要です。IP アドレスとホスト名の要件の詳細については、 IP アドレスとホスト名の要件を参照してください。
- Intersight 仮想アプライアンスのマルチノード クラスタの設定は、3 つのホスト名、3 つの IP アドレスとそれぞれのホスト名に対して 1 つの DC-CNAME が必要です。IP アドレスとホスト名の要件の詳細については、 IP アドレスとホスト名の要件を参照してください。
- Web ユーザ インターフェイスを介してアプライアンスにアクセスするには、HTTPS プロトコルと完全修飾ドメイン名のみを使用します。

ステップ 1 管理者クレデンシャルを使用して VMware vSphere Web クライアントにログインします。

ステップ 2 ホストを右クリックして **[OVF テンプレートの展開（Deploy OVF Template）]** を選択します。

ステップ 3 **[OVF テンプレートの展開 (Deploy OVF Template)]** ウィザードの **[テンプレートの選択 (\Select Template)]** ページで、送信元の場所を指定し、**[次へ (Next)]** をクリックします。URL を指定するか、またはローカル ハード ドライブ、ネットワーク共有、または DVD/CD ドライブからアクセス可能な場所を参照することができます。

ステップ 4 **[OVF テンプレートの詳細（OVF Template Details）]** ページで、OVF テンプレートの詳細を確認して [次へ（Next）] をクリックします。入力する必要はありません。

ステップ 5 **[名前とロケーションの選択 (Select a name and location)]** ページで、仮想アプライアンスの **[名前 (Name)]** と **[場所 (Location)]** を追加/編集し、**[次へ (Next)]** をクリックします。

ステップ 6 **[リソースの選択 (Select a resource)]** ページで、特定の**ホスト** (ESX station)、**クラスタ**、**リソース プール**、または,展開する**仮想アプライアンス**を選択して、**[次へ (Next)]** をクリックします。

各 VM は、vSphere HA または手動モードの vSphere DRS で構成されているクラスタの特定のホストに割り当てる必要があります。

ステップ 7 [詳細の確認（Review details）] ページで OVA テンプレートの詳細を確認し、[次へ（Next）] をクリックします。

ステップ 8 **[設定（Configuration）]** ページで [設定の導入（Custom）] を、選択して **[次へ（Next）]** をクリックします。

ステップ 9 **[ストレージの選択（Select storage）]** ページで、選択したホスト（ESX ステーション）内の VM ファイルに宛先ストレージ（ハード ドライブ）を選択し、**[次へ（Next）]** をクリックします。仮想マシンの仮想ディスクにディスク形式を選択します。

Cisco では、シック プロビジョニングを使用することを推奨しています。シン プロビジョニングを使用することが可能である一方、オーバープロビジョニングはストレージのキャパシティ不足を導き、サービスの低下や損失につながり、バックアップからの復元が必要になることがあります。

ステップ 10 **[ネットワークの選択 (Select networks)]** ページで、OVF テンプレートに指定されている各ネットワークに対して送信元ネットワークを選択し、それを宛先ネットワークにマップして **[次へ (Next)]** をクリックします。

ステップ 11 **[テンプレートのカスタマイズ (Customize Template)]** ページで、OVF テンプレートの展開プロパティをカスタマイズし、**[次へ (Next)]** をクリックします。

OVF プロパティ	**説明**
[DHCP を有効にする (シングルノード アプライアンスの場合のみ)（Enable DHCP (only for single-node appliance)）]	静的 IP アドレスを使用しないように、アプライアンスが同じネットワーク上で実行されている DHCP サーバーから IP アドレスを取得できるようにします。このオプションを選択すると、すべての静的パラメータが無視されます。DHCP の詳細については、この表の後の**[DHCP の有効化（Enabling DHCP）]** の項を参照してください。
[IP アドレス (IP Address)] *(DHCP* を有効にすると、入力した値は無視されます*)*	ノードの IPv4 アドレスを入力します。例：10.0.0.100
[ネット マスク (Net Mask)]*(DHCP* を有効にすると、入力した値は無視されます*)*	このフィールドには IPv4 ネットマスク 255.255.255.0 が事前に入力されています。
[デフォルト ゲートウェイ (Default Gateway)]*(DHCP* を有効にすると、入力した値は無視されます*)*	IPv4 のデフォルト ゲートウェイを入力します。例：10.0.1.254

OVF プロパティ	説明
[DNS ドメイン (DNS Domain)]*(DHCP を有効にすると、入力した値は無視されます)*	DNS 検索ドメインを入力します。
[DNS サーバ (DNS Servers)]*(DHCP を有効にすると、入力した値は無視されます)*	DNS サーバーのカンマ区切りの IPv4 アドレスのリストを入力します。最大 2 つの DNS サーバーがサポートされます。
[Admin Password]	admin パスワードを入力します。これは、アプライアンスへのログインに使用するパスワードと同じです。 **[パスワードの設定（Set Password）]**：Intersight にアプライアンスを登録する前に、管理者パスワードを作成する必要があります。パスワードには、0 ～ 9、A ～ Z、a ～ z と、コロン（:）およびスペースを除くすべての特殊文字を含めることができます。
[NTP Servers]	NTP サーバーのカンマ区切りの IPv4 アドレスのリストを入力します。NTP サーバーは最大 3 つまで追加できます。DHCP を使用して IP アドレスを取得する場合でも、この設定は必須です。
Disk Size	**[重要：（Attention:）]**ディスク サイズの値は、展開構成に基づいて計算されるため、変更しないでください。

注目　**アプライアンス登録時に設定したパスワードが脆弱である場合、Interswitch はパスワードをより強力なものに変更するように要求します。強力なパスワードに正常にリセットされると、アプライアンスに直接ログインします。ログ方法の詳細については、**Intersight 仮想アプライアンスにログイン （58 ページ） を参照してください。

DHCP のイネーブル化

Dynamic Host Configuration Protocol（DHCP）を使用すると、Cisco Intersight 仮想アプライアンス VM は、インストールされているネットワーク上で実行されている DHCP サーバーを介して、IP アドレスを取得できます。このオプションが有効になっている場合、Cisco Intersight 仮想アプライアンスはリース要件に従って、DHCP を介して IP アドレスの更新を処理するように設定されています。

注目　**DHCP は マルチノード Intersight 仮想アプライアンスではサポートされていません。**

シングルノード アプライアンスのため、DHCP の使用するために次の要件が満たされていることを確認します：

- DHCP を使用する場合は、アプライアンス VM に返された IP アドレスが、アプライアンスの設定に使用するのと**同じ FQDN** に対して解決されることを確認します。Cisco では、アプライアンス VM に対して同じ IP アドレスを返すように DHCP を設定し、IP アドレスを頻繁に変更しないことを推奨しています。

- アプライアンスは、DHCP リース情報から IP アドレス、ネットマスク、ゲートウェイ、および DNS サーバーのみを読み取ります。NTP 情報 (存在する場合) は、展開時に OVF パラメータに入力する必要があります。
- アプライアンス VM で使用されるすべての IP アドレスは、割り当てられた初期 IP アドレスと同じサブネット内にある必要があります。たとえば、別の DHCP サーバーを持つ vSwitch に接続して、VM に異なるサブネットからの IP を割り当てることはできません。

制限事項

- 強制リースの更新は、VM の設定に影響を与える可能性があり、アプライアンスを使用できなくなる可能性があります。

ステップ 12 **[準備完了 (Ready to Complete)]** ページで **[展開後に電源をオン (Power On After Deployment)]** を選択し、**[終了 (Finish)]** をクリックします。

アプライアンスの設定を完了する方法については、「シングルノード Intersight 接続型仮想アプライアンスのセットアップ」を参照してください。

トラブルシューティング ヒント：OVF パラメータを指定した後、電源をオンにしてから約 15 分後に <*https://fqdn-of-your-appliance*>にアクセスしたときに VM が応答しないことに気づいた場合は、Intersight アプライアンス メンテナンス シェルを使用して、ネットワーキングまたは設定不備の問題をトラブルシューティングすることができます。

トラブルシューティング ヒント: diag シェルに **192:** などのホスト名が表示される場合は、アプライアンスの展開中に、1 つ以上のネットワーク パラメーター（IP アドレス、ネットマスク、ゲートウェイ、ドメイン ネーム システム（DNS）サーバーなど）の入力が間違って入力しました。アプライアンス VM が、ネットワークへの接続と DNS ルックアップの実行を許可しないポートグループ/vswitch に接続されている可能性もあります。この問題が発生した場合は、OVA への入力と他のネットワーク パラメータを確認してください。誤った入力は、diag シェルを使用して修正できます。

診断ツールの目的は次のとおりです。

- インストールの前提条件に関する問題を検出して表示します。
- OVA の展開時に提供される入力の編集を有効にします。
- 設定を修正した後、または OVA の導入時に IP アドレス、サブネットマスク、デフォルトゲートウェイなどのネットワークインターフェイスのプロパティを設定した後、インストールを続行できるようにします。

詳細については、Intersight 仮想アプライアンスおよび Intersight Assist のメンテナンスシェル（123 ページ） を参照してください。

Intersight 仮想アプライアンス インストールおよびトラブルシューティングのデモンストレーションについては、『Cisco Intersight アプライアンスおよびデバッグ』をご確認ください。

Microsoft Hyper-V Server 上の Cisco Intersight 仮想アプライアンスおよび Intersight Assist のインストール

Cisco Intersight 仮想アプライアンスは、オープン仮想アプライアンス（OVA）ファイル形式、ZIP ファイル形式、または TAR ファイル形式で含まれている展開可能な仮想マシンとして配布されます。ZIP ファイル形式を使用して Microsoft Hyper-V サーバーにアプライアンスをインストールします。Microsoft Hyper-V サーバーの詳細については、Microsoft のマニュアルを参照してください。

（注） 次のタスクの中の手順を使用して、アプライアンスを Hyper-V Server Manager にインストールして展開します。

始める前に

シスコの担当者が提供した URL または、ローカル ハード ドライブ、ネットワーク共有ドライブまたは CD/DVD ドライブなど、セットアップからアクセス可能な場所から、Cisco Intersight 仮想アプライアンス パッケージをダウンロードしたことを確認します。

注目

- Intersight Virtual Appliance をインストールしてセットアップする前に、新規の Intersight 仮想アプライアンスの VM 情報技術要件 セクションに記載されている情報を読むことを強くお勧めします。
- シングルノード Intersight 仮想アプライアンスをセットアップするには、IP アドレス 1 つと、その IP アドレスの DNS レコードが 2 つ必要です。IP アドレスとホスト名の要件の詳細については、 IP アドレスとホスト名の要件を参照してください。
- **Intersight 仮想アプライアンスのマルチノードクラスタのセットアップは、Microsoft Hyper-V ではサポートされていません。**
- Web ユーザ インターフェイスを介してアプライアンスにアクセスするには、HTTPS プロトコルと完全修飾ドメイン名のみを使用します。

ステップ 1 管理者のクレデンシャルを使用して Hyper-V Server Manager にログインし、アプライアンスをインストールするサーバーを選択します。

ステップ 2 **[アクション（Actions）]** ペインで、**[仮想マシンのインポート（Import Virtual Machine）]** を選択し、**[次へ（Next）]** をクリックします。

a) `onprem_vms` など、抽出した仮想マシンを含むフォルダを選択し、**[次へ（Next）]** をクリックします。

b) インポートする仮想マシンを選択して、**[次へ >（Next >）]** をクリックします。

c) **[インポート タイプの選択（Choose Import Type）]** 画面で、**[仮想マシンのコピー（新しい固有 ID の作成）（Copy the virtual machine（create a new unique ID））]** オプションを選択し、**[次へ（Next）]** をクリックします。
d) **[宛先の選択（Choose Destination）]** 画面で選択を行い、**[次へ（Next）]** をクリックします。
e) **[ストレージ フォルダの選択（Choose Storage Folders）]** 画面で選択を行い、**[次へ（Next）]** をクリックします。
f) **[サマリ（Summary）]** 画面で選択内容を確認し、**[完了（Finish）]** をクリックします。

インポートが完了すると、インポートされた仮想マシンが Hyper-V Manager に表示されます。

ステップ 3 移行元の仮想マシン上で右クリックし、**[設定（Settings）]** を選択します。
a) **[ネットワーク アダプタ（Network Adapter）]** に移動し、ドロップダウン リストから仮想スイッチを選択します。
b) **[適用（Apply）]** をクリックします。

ステップ 4 **[アクション（Actions）]** ペインで、**[スタート（Start）]** を選択して仮想マシンの電源をオンにします。

ステップ 5 **[アクション（Actions）]** ペインで、**[接続（Connect）]** を選択して仮想マシンに接続します。

仮想マシン接続コンソールが表示されます。

ステップ 6 **仮想マシン接続**コンソールで、パスワード設定と IP プロパティをカスタマイズします。

プロパティ	説明
ユーザー管理者のパスワードを設定（Set password for user admin）	管理者ユーザーの新しいパスワードを設定します。 （注） アプライアンスへのログインに同じパスワードを使用するため、このパスワードを忘れないようにしてください。
IP 割り当てを選択（Choose IP Assignment）	スタティック IP 割り当ての場合は **S**、DHCP の場合は **D** を入力します。 IP あり当てに DHCP を選択することで、静的 IP アドレスを使用しないように、アプライアンスが同じネットワーク上で実行されている DHCP サーバーから IP アドレスを取得できるようにします。
IP アドレス（IP Address）	ノードの IP アドレスを入力します。例：10.0.0.100
サブネット マスク（Subnet Mask）	IP ネット マスクを入力します。255.255.255.0 などです。
デフォルト ゲートウェイ（Default Gateway）	IP のデフォルト ゲートウェイを入力します。例：10.0.1.254
DNS サーバ（DNS Servers）	DNS サーバーのカンマ区切りの IP アドレスのリストを入力します。最大 2 つの DNS サーバーがサポートされます。

プロパティ	説明
ドメイン（**DNS Domain**）	DNS 検索ドメインを入力します。
NTP サーバ （NTP Servers）	スタティック IP を設定するときに NTP 情報を入力します。 NTP サーバーのカンマ区切りの IP アドレスのリストを入力します。最大 3 台の NTP サーバーを追加できます。 IP 割り当てに選択した DHCP を設定した場合は、NTP 情報を提供できません。

注目　**アプライアンス登録時に設定したパスワードが脆弱である場合、Interswitch はパスワードをより強力なものに変更するように要求します。強力なパスワードに正常にリセットされると、アプライアンスに直接ログインします。ログ方法の詳細については、**Intersight 仮想アプライアンスにログイン（58 ページ） を参照してください。

DHCP のイネーブル化

Dynamic Host Configuration Protocol（DHCP）を使用すると、Cisco Intersight 仮想アプライアンス VM は、インストールされているネットワーク上で実行されている DHCP サーバーを介して、IP アドレスを取得できます。このオプションが有効になっている場合、Cisco Intersight 仮想アプライアンスはリース要件に従って、DHCP を介して IP アドレスの更新を処理するように設定されています。

注目　**シングルノードアプライアンスのため、DHCP の使用するために次の要件が満たされていることを確認します：**

- DHCP を使用する場合は、アプライアンス VM に返された IP アドレスが、アプライアンスの設定に使用するのと**同じ FQDN** に対して解決されることを確認します。Cisco では、アプライアンス VM に対して同じ IP アドレスを返すように DHCP を設定し、IP アドレスを頻繁に変更しないことを推奨しています。
- アプライアンスは、DHCP リース情報から IP アドレス、ネットマスク、ゲートウェイ、および DNS サーバーのみを読み取ります。静的IP を設定する場合は、Hyper-V Server の NTP 情報を仮想マシン接続コンソールに入力する必要があります。
- アプライアンス VM で使用されるすべての IP アドレスは、割り当てられた初期 IP アドレスと同じサブネット内にある必要があります。たとえば、別の DHCP サーバーを持つ vSwitch に接続して、VM に異なるサブネットからの IP を割り当てることはできません。

制限事項

- 強制リースの更新は、VM の設定に影響を与える可能性があり、アプライアンスを使用できなくなる可能性があります。

ステップ 7　*<https://fqdn-of-your-appliance>* に進み、アプライアンスのインストール後のセットアップを完了します。

アプライアンスの設定を完了する方法については、「シングルノード Intersight 接続型仮想アプライアンスのセットアップ」を参照してください。

トラブルシューティング ヒント：パスワードおよび IP プロパティ パラメータを指定した後、約 15 分後に <*https://fqdn-of-your-appliance*> にアクセスしたときに VM が応答しないことに気づいた場合は、Intersight アプライアンス メンテナンス シェルを使用して、ネットワーキングまたは設定ミスの問題をトラブルシューティングすることができます。

診断ツールの目的は次のとおりです。

- インストールの前提条件に関する問題を検出して表示します。
- OVA の展開時に提供される入力の編集を有効にします。
- 設定を修正した後、または OVA の導入時に IP アドレス、サブネットマスク、デフォルトゲートウェイなどのネットワークインターフェイスのプロパティを設定した後、インストールを続行できるようにします。

詳細については、Intersight 仮想アプライアンスおよび Intersight Assist のメンテナンスシェル（123 ページ） を参照してください。

Intersight 仮想アプライアンス インストールおよびトラブルシューティングのデモンストレーションについては、『Cisco Intersight アプライアンスおよびデバッグ』をご確認ください。

KVM ハイパーバイザでの Cisco Intersight 仮想アプライアンスおよび Intersight Assist のインストール

Cisco Intersight 仮想アプライアンスは、オープン仮想アプライアンス（OVA）ファイル形式、ZIP ファイル形式、または TAR ファイル形式で含まれている展開可能な仮想マシンとして配布されます。TAR ファイル形式を使用して KVM ハイパーバイザにアプライアンスをインストールします。次の手順は、Virtual Machine Manager（VMM）を使用して KVM ハイパーバイザにアプライアンスをインストールして展開する方法を示しています。

（注） ソフトウェア要件：

- KVM ハイパーバイザをサポートする Linux オペレーティング システム、または KVM ハイパーバイザで事前設定された Linux オペレーティング システム。CentOS 7.9 では、KVM ハイパーバイザの最小サポートバージョンは 1.5.3 です。
- VM へのネットワーク接続を提供する仮想ネットワークブリッジ。

（注） Virtual Machine Manager（VMM）を使用して KVM ハイパーバイザにアプライアンスをインストールして展開するために次のタスクの中の手順を使用します。

始める前に

シスコの担当者が提供した URL または、ローカル ハード ドライブ、ネットワーク共有ドライブまたは CD/DVD ドライブなど、セットアップからアクセス可能な場所から、Cisco Intersight 仮想アプライアンス パッケージをダウンロードしたことを確認します。

注目

- Intersight Virtual Appliance をインストールしてセットアップする前に、新規の Intersight 仮想アプライアンスの VM 情報技術要件 セクションに記載されている情報を読むことを強くお勧めします。
- シングルノード Intersight 仮想アプライアンスをセットアップするには、IP アドレス 1 つと、その IP アドレスの DNS レコードが 2 つ必要です。IP アドレスとホスト名の要件の詳細については、 IP アドレスとホスト名の要件を参照してください。
- **Intersight 仮想アプライアンスのマルチノードクラスタのセットアップは、KVM ハイパーバイザではサポートされていません。.**
- Web ユーザ インターフェイスを介してアプライアンスにアクセスするには、HTTPS プロトコルと完全修飾ドメイン名のみを使用します。

ステップ 1 Virtual Machine Manager（VMM）クライアントを起動します。

ステップ 2 新しい仮想マシンを KVM ハイパーバイザにインストールするには、メニュー バーで **[ファイル（File）]** > **[新規仮想マシン（New Virtual Machine）]** を選択します。

[新規 VM（New VM] ダイアログ ボックスが表示され、[新規 VM（New VM）] インストールのステップ 1/4 が表示されます。

ステップ 3 **[オペレーティング システムをインストールする方法を選択する（Choose how you want to install the operating system）]** で、**[既存のディスク イメージのインポート（Import existing disk image）]** を選択し、**[転送（Forward）]** をクリックします。

ステップ 2/4 が表示されます。

ステップ 4 **[既存のストレージ パスを指定する（Provide the existing storage path）]** で、**[参照（Browse）]** をクリックします。

ステップ 5 **[ストレージ ボリュームの選択（Choose storage volume）]** で、ディレクトリを参照して、システムで抽出した Intersight 仮想アプライアンス イメージ ファイルの最初のディスク（*intersight-appliance-1.0.9-180-1.qcow2* など）を選択します。

a) **[詳細（Advanced）] オプション**で、**[VirtIO]** を選択します。

（注） VirtIO は、KVM ハイパーバイザに Intersight 仮想アプライアンスと Intersight Assist をインストールする際にサポートされるストレージ用の唯一のディスク バスです。

ステップ 6 **[オペレーティング システム タイプおよびバージョンの選択（Choose an operating system type and version）]** で、[OS タイプ（OS type）] に **[Linux]**、[バージョン（Version）] に **[CentOS 7.0]** を選択し、**[転送（Forward）]** をクリックします。

ステップ 3/4 が表示されます。

ステップ 7 **[メモリと CPU 設定の選択（Choose Memory and CPU settings）]** で、次の手順を実行し、**[転送（Forward）]** をクリックします。

- [メモリ（RAM）（Memory（RAM））] に 32768 を選択または入力します。
- CPU を 16 に設定

ステップ 4/4 が表示されます。

アプライアンスの展開サイズの詳細については、Intersight 仮想アプライアンスでサポートされる構成の制限 （89 ページ） を参照してください。

ステップ 8 ダイアログ ボックスで、次のフィールドに値を入力します。

- **[インストールを開始する準備（Ready to start the installation）]** の **[名前（Name）]** フィールドに、Intersight Virtual Appliance ソフトウェアの名前を入力します。例：*intersight-appliance-1.0.9-180*
- **[インストール前に設定をカスタマイズする（Customize configuration before install）]** オプションが選択されていることを確認します。
- **[ネットワーク選択（Network selection）]** で、適切な仮想ネットワークブリッジを選択していることを確認します。

ステップ 9 **[終了（Finish）]** をクリックします。

これで、Intersight 仮想アプライアンス イメージの最初のディスクを追加するプロセスが完了しました。インストール プロセスを開始する前に、ディスク 2ー8 を 1 つずつ追加する必要があります。

ステップ 10 VMM コンソールで、次の設定を行います。

a) 左側のナビゲーション パネルの下部にある **[ハードウェアの追加（Add Hardware）]** をクリックします。
b) **[ストレージ（Storage）]** で、**[カスタム ストレージの選択または作成（Select or create custom storage）]** が選択されていることを確認します。
c) ディレクトリを参照して、システムで抽出した Intersight 仮想アプライアンス イメージ ファイルの 2 番目のディスク（*intersight-appliance-1.0.9-180-2.qcow2* など）を見つけて選択し、**[ボリュームの選択（Choose volume）]** をクリックします。
d) **[終了（Finish）]** をクリックします。

ディスク 3 ーディスク 8 を追加するまで、この手順を繰り返します。8 つのディスクすべてが左側のナビゲーション パネルに表示されていることを確認します。

ステップ 11 **[インストールの開始（Begin Installation）]** をクリックします。

ステップ 12 VMM コンソールで、パスワード設定と IP プロパティをカスタマイズします。

プロパティ	説明
ユーザー管理者のパスワードを設定（Set password for user admin）	管理者ユーザーの新しいパスワードを設定します。 （注） アプライアンスへのログインに同じパスワードを使用するため、このパスワードを忘れないようにしてください。
IP 割り当てを選択（Choose IP Assignment）	スタティック IP 割り当ての場合は **S**、DHCP の場合は **D** を入力します。 IP あり当てに DHCP を選択することで、静的 IP アドレスを使用しないように、アプライアンスが同じネットワーク上で実行されている DHCP サーバーから IP アドレスを取得できるようにします。
IP アドレス（IP Address）	ノードの IPv4 アドレスを入力します。例：10.0.0.100 （注） アプライアンスを機能させるには、IPv4 アドレスを設定する必要があります。 IPv4 アドレスを使用したアプライアンスの初期インストールと展開の完了後に IPv6 アドレスを設定することをお勧めします。
サブネット マスク（Subnet Mask）	IP ネットマスクを入力します。255.255.255.0 などです。
デフォルト ゲートウェイ（Default Gateway）	IP のデフォルト ゲートウェイを入力します。例：10.0.1.254
DNS サーバ（DNS Servers）	DNS サーバーのカンマ区切りの IP アドレスのリストを入力します。最大 2 つの DNS サーバーがサポートされます。
ドメイン（DNS Domain）	DNS 検索ドメインを入力します。
NTP サーバ （NTP Servers）	スタティック IP を設定するときに NTP 情報を入力します。 NTP サーバーのカンマ区切りの IP アドレスのリストを入力します。最大 3 台の NTP サーバーを追加できます。 IP 割り当てに選択した DHCP を設定した場合は、NTP 情報を提供できません。

注目　**アプライアンス登録時に設定したパスワードが脆弱である場合、Interswitch はパスワードをより強力なものに変更するように要求します。強力なパスワードに正常にリセットされると、アプライアンスに直接ログインします。ログ方法の詳細については、**Intersight 仮想アプライアンスにログイン （58 ページ） を参照してください。

DHCP のイネーブル化

Dynamic Host Configuration Protocol（DHCP）を使用すると、Cisco Intersight 仮想アプライアンス VM は、インストールされているネットワーク上で実行されている DHCP サーバーを介して、IP アドレスを取得できます。このオプションが有効になっている場合、Cisco Intersight 仮想アプライアンスはリース要件に従って、DHCP を介して IP アドレスの更新を処理するように設定されています。

注目　**シングルノード アプライアンスのため、DHCP の使用するために次の要件が満たされていることを確認します：**

- DHCP を使用する場合は、アプライアンス VM に返された IP アドレスが、アプライアンスの設定に使用するのと**同じ FQDN** に対して解決されることを確認します。Cisco では、アプライアンス VM に対して同じ IP アドレスを返すように DHCP を設定し、IP アドレスを頻繁に変更しないことを推奨しています。
- アプライアンスは、DHCP リース情報から IP アドレス、ネットマスク、ゲートウェイ、および DNS サーバーのみを読み取ります。静的IP を設定する場合は、KVM ハイパーバイザの NTP 情報を VMM コンソールに入力する必要があります。
- アプライアンス VM で使用されるすべての IP アドレスは、割り当てられた初期 IP アドレスと同じサブネット内にある必要があります。たとえば、別の DHCP サーバーを持つ vSwitch に接続して、VM に異なるサブネットからの IP を割り当てることはできません。

制限事項

- 強制リースの更新は、VM の設定に影響を与える可能性があり、アプライアンスを使用できなくなる可能性があります。

ステップ 13　*<https://fqdn-of-your-appliance>* に進み、アプライアンスのインストール後のセットアップを完了します。

アプライアンスの設定を完了する方法については、「シングルノード Intersight 接続型仮想アプライアンスのセットアップ」を参照してください。

トラブルシューティング ヒント：パスワードおよび IP プロパティ パラメータを指定した後、約 15 分後に *<https://fqdn-of-your-appliance>* にアクセスしたときに VM が応答しないことに気づいた場合は、Intersight アプライアンス メンテナンス シェルを使用して、ネットワーキングまたは設定ミスの問題をトラブルシューティングすることができます。

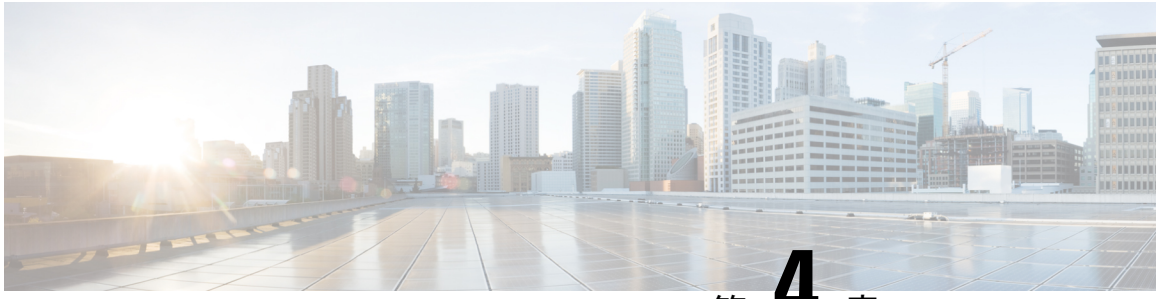
診断ツールの目的は次のとおりです。

- インストールの前提条件に関する問題を検出して表示します。
- アプライアンス イメージの展開時に提供される入力の編集を有効にします。

- 設定を修正した後、またはアプライアンス イメージの展開時に IP アドレス、サブネット マスク、デフォルト ゲートウェイなどのネットワーク インターフェイスのプロパティを設定した後、インストールを続行できるようにします。

詳細については、Intersight 仮想アプライアンスおよび Intersight Assist のメンテナンスシェル（123 ページ） を参照してください。

Intersight 仮想アプライアンス インストールおよびトラブルシューティングのデモンストレーションについては、『Cisco Intersight アプライアンスおよびデバッグ』をご確認ください。



第 4 章

セットアップ

シングルノード Intersight 接続型仮想アプライアンスのセットアップ

Cisco Intersight 仮想アプライアンスは、オープン仮想アプライアンス（OVA）ファイル形式、ZIP ファイル形式、または TAR ファイル形式で含まれている展開可能な仮想マシンとして配布されます。

始める前に:「VMware vSphere 上の Cisco Intersight 仮想アプライアンスおよび Intersight Assist のインストール （27 ページ）」の手順に従って、Intersight 仮想アプライアンスソフトウェアがインストールされていることを確認します。

Cisco Intersight 仮想アプライアンス ソフトウェアの展開が完了し、VM の電源がオンになったら、 <<https://your fqdn.com>> URLをクリックします。**[Intersight あぷらインす インストーラ**

（**Intersight Appliance Installer**）] 画面が表示され、新規インストール、バックアップからのアプライアンス ソフトウェアの回復、またはアプライアンスへのノードの追加のいずれかのセットアップを完了できます。

ウィザードで、ソフトウェアパッケージをダウンロードしてインストールする一連の手順を実行します。インストールの進行状況は確認できます。

次の手順を使用して、Intersight 接続型仮想アプライアンスのセットアップを完了します。

ステップ 1 **[Intersight アプライアンス インストーラ（Intersight Appliance Installer）]** 画面で **[Intersight 接続型仮想アプライアンス（Intersight Connected Virtual Appliance）]** を選択し、**[開始（Start）]** をクリックします。

ステップ 2 Cisco ID を使用して、[Intersight 仮想アプライアンスの接続（Intersight Virtual Appliance Connect ）] ページにログインします。シスコ ID をお持ちでない場合はこちらから作成してください。

1. **（オプション）[設定（Settings）]** をクリックして HTTPS プロキシ設定を有効にします。

   インターネットへ Cisco Intersight 仮想アプライアンスを接続するのに HTTP/S プロキシが必要な場合は、接続手順を実行する前にプロキシ設定を構成する必要があります。

   - **[設定（Settings）]** をクリックして **[HTTPS プロキシ（HTTPS Proxy）]** オプションを有効にします。
   - **プロキシ ホスト名**または **IP アドレス**と**プロキシ ポート**を追加します。

     プロキシ ポートは、1 ～ 65535 の範囲にする必要があります。アプライアンスの UI の **[システム（SystemI）]** > **[設定 (Settings)]** > **[ネットワーク (NETWORKING)]** > **[クラウド接続 (Cloud Connection)]** からプロキシの設定を編集することができます。

2. [接続 (Connect)] ページに表示されている**デバイス ID** と**要求コード**を使用して Intersight への接続を実行します。
3. **[接続 (Connection)]** のステータスに **[要求済み (Claimed)]** と表示されていることを確認します。

（注） 新しいブラウザ タブが表示され、Intersight でのデバイスの要求ステータスが示されます。Intersight アカウントを持っていない場合は、**[アカウント作成 (Account Creation)]** ウィンドウでアカウントを作成し、ターゲットを要求することができます。ターゲット接続に成功すると、成功メッセージが表示されます。**[閉じる（Close）]** タブをクリックしてタブを終了し、**Intersight 仮想アプライアンス**のセットアップ ウィザードに戻ります。ターゲット要求が失敗した場合は、Intersight へのログイン画面が表示され、ターゲットを要求するワークフローが再開されます。

ステップ 3 **Intersight アプライアンス インストーラ** のセットアップ ウィザードで、次の手順を実行します。

a) **[接続（Connect）]** : **[続行（Continue）]** をクリックして、**[ネットワーク要件の確認（Check Network Requirements）]** ステップに進みます。

b) **[ネットワーク要件の確認（Check Network Requirements）]** : 結果を表示し、**[次へ（Next）]** をクリックして、**[内部ネットワークの構成（Configure Internal Network）]** ステップに進みます。

ネットワーク要件のチェック中に、いずれかの DNS テストが失敗した場合は、設定を続行できないことに注意してください。

c) **[内部ネットワークの構成（Configure Internal Network）]**：必要に応じて、デフォルトの内部ネットワーク IP アドレスを変更し、**[次へ（Next）]** をクリックして、**[ソフトウェア バージョンの選択（Select Software Version）]** ステップに進みます。

注意：この IP アドレス範囲は、Intersight 仮想アプライアンス内の内部通信に使用されます。この範囲は、172.16.0.0/12 サブネット内に収まる必要がありますが、より小さな範囲になる可能性があります（最大 20 サブネット プレフィックス サイズ）。ほとんどの場合、デフォルト値を使用できます。デフォルト値を変更する理由としては、アプライアンスが同じサブネット内の他のデバイ スと直接通信する必要がある場合、NAT など IP 変換メカニズムを通さずに通信する必要がある場合が考えられます。

d) **[ソフトウェア バージョンの選択（Select Software Version）]**：アプライアンス ソフトウェアの最新バージョンをダウンロードするオプションがあります。または、インストーラのバージョンと同じか、インストーラのバージョンより大きい、サポートされている他のバージョンのソフトウェアをアップロードできます。

a) アプライアンス ソフトウェアの最新バージョンをダウンロードするには、**[最新バージョンのダウンロード（Download Latest Version）]** ボタンを選択し、**[完了（Finish）]** をクリックして、**[インストールの結果（Installation Result）]** 画面に進みます。

b) アプライアンス ソフトウェアのバージョンをアップロードするには、ソフトウェア パッケージの保存場所に応じて、**[ローカル マシン（Local Machine）]** または **[ネットワーク共有（Network Share）]** を選択します。

（注） Intersight Connected Virtual Appliance を手動で更新、インストール、または復元するには、アプライアンスアカウントにアクセスして、必要なソフトウェアパッケージをダウンロードする必要があります。詳細については、ソフトウェア パッケージをダウンロードするためのアプライアンス アカウントの作成 （59 ページ） および Intersight 仮想アプライアンスのソフトウェア パッケージのダウンロード （60 ページ） を参照してください。

- [ローカル マシン（Local Machine）] で、ソフトウェア イメージを保存した場所を参照し、**[完了（Finish）]** をクリックして、**[インストール結果（Installation Result）]** 画面に進みます。
- **[ネットワーク共有（Network Share）]** オプションの場合は、プロトコルを入力し、ファイルのコピー元であるリモート サーバーの詳細を入力して、**[完了（Finish）]** をクリックして、**[インストール結果（Installation Result）]** 画面に進みます。
  - **[プロトコル（Protocol）]**：ファイル転送に使用される通信プロトコル。SCP（Secure Copy Protocol）および SFTP（Secure File Transfer Protocol）がサポートされています。
  - **[サーバ IP/ホスト名（Server IP/Hostname）]**：ファイルのコピー元のホスト サーバー
  - **[ポート（Port）]**：使用する TCP ポート
  - **[場所（Location）]**：コピーするファイルが保存されているディレクトリ
  - **[ファイル名（Filename）]**：ネットワーク共有からコピーするファイルの名前
  - **[ユーザ名（Username）]**：ネットワーク共有で認証するためのユーザー名
  - **[パスワード（Password）]**：ネットワーク共有で認証するためのパスワード

c) **[インストール結果（Installation Result）]**：この画面でインストールの進行状況を確認できます。

ステップ 4 **[データ収集（Data Collection）]** を指定します。

Intersight がシスコに追加のシステム情報を送信できるようにする設定を指定します。このオプションは、デフォルトで有効です。Intersight でどんなデータが収集されるかの詳細については、Intersight 接続型仮想アプライアンスから収集されたデータ （119 ページ） を参照してください。

ステップ 5 **[ライセンスの登録（Register License）]** をクリックします。

Cisco Smart License Manager からライセンス登録トークンを取得し、トークンを適用して追加し、ライセンスをアクティブにします。ライセンスの登録プロセスは完了するまでに数分かかる場合があります。Intersight ライセンスの登録の詳細については、「Cisco Intersight ライセンスの階層と登録（Cisco Intersight Licensing Tiers and Registration）」を視聴してください。

[完了（Finish）] をクリックすると、Intersight 接続型仮想アプライアンス ダッシュボードが表示されます。

次のタスク

単一ノードの Intersight 仮想アプライアンスの初期セットアップが正常に完了したら、ノードを追加してマルチノード クラスタを作成できます。詳細については、Intersight 仮想アプライアンスのマルチノード クラスタの構成 （48 ページ） を参照してください。

シングルノード Intersight プライベート仮想アプライアンスのセットアップ

Cisco Intersight 仮想アプライアンスは、オープン仮想アプライアンス（OVA）ファイル形式、ZIP ファイル形式、または TAR ファイル形式で含まれている展開可能な仮想マシンとして配布されます。

始める前に:「VMware vSphere 上の Cisco Intersight 仮想アプライアンスおよび Intersight Assist のインストール （27 ページ）」の手順に従って、Intersight 仮想アプライアンスソフトウェアがインストールされていることを確認します。

Cisco Intersight 仮想アプライアンス ソフトウェアの展開が完了し、VM の電源がオンになったら、 <<https://your fqdn.com>> URLをクリックします。**[Intersight あぷらインす インストーラ（Intersight Appliance Installer）]** 画面が表示され、新規インストール、バックアップからのアプライアンス ソフトウェアの回復、またはアプライアンスへのノードの追加のいずれかのセットアップを完了できます。

ウィザードで、ソフトウェアパッケージをダウンロードしてインストールする一連の手順を実行します。インストールの進行状況は確認できます。

次の手順を使用して、Intersight プライベート仮想アプライアンスのセットアップを完了します。

ステップ 1 **[Intersight アプライアンスインストーラ（Intersight Appliance Installer）]** 画面で、**[Intersight プライベート仮想アプライアンス（Intersight Private Virtual Appliance）]** を選択し、**[開始（Start）]** をクリックして、単一ノードのプライベート仮想アプライアンスのセットアップを続行します。

[ソフトウェアのアップロード（Upload Software）] ページが表示されます。インストーラのバージョンと同じか、インストーラのバージョンより大きいソフトウェアのサポートされているバージョンをアップロードできます。

ステップ 2 **Intersight アプライアンス インストーラ** のセットアップ ウィザードで、次の手順を実行します。

a) **[ネットワーク要件の確認（Check Network Requirements）]**：結果を表示し、**[次へ（Next）]** をクリックして、**[内部ネットワークの構成（Configure Internal Network）]** ステップに進みます。

ネットワーク要件のチェック中に、いずれかの DNS テストが失敗した場合は、設定を続行できないことに注意してください。

b) **[内部ネットワークの設定（Configure Internal Network）]**：必要に応じて、デフォルトの内部ネットワーク IP アドレスを変更し、**[次へ（Next）]** をクリックして **[ソフトウェアのアップロード（Upload Software）]** ステップに進みます。

注意：この IP アドレス範囲は、Intersight 仮想アプライアンス内の内部通信に使用されます。この範囲は、172.16.0.0/12 サブネット内に収まる必要がありますが、より小さな範囲になる可能性があります（最大 20 サブネット プレフィックス サイズ）。ほとんどの場合、デフォルト値を使用できます。デフォルト値を変更する理由としては、アプライアンスが同じサブネット内の他のデバイ スと直接通信する必要がある場合、NAT など IP 変換メカニズムを通さずに通信する必要がある場合が考えられます。

c) **[ソフトウェアのアップロード（Upload Software）]**：インストーラのバージョンと同じか、インストーラのバージョンより大きいソフトウェアのサポートされているバージョンをアップロードできます。

ソフトウェア パッケージの保存場所に応じて、**[ローカル マシン（Local Machine）]** または **[ネットワーク共有（Network Share）]** を選択します。

（注） Intersight プライベート仮想アプライアンスの展開を完了するには、必要なソフトウェアパッケージをダウンロードできるようにアプライアンス アカウントにアクセスする必要があります。詳細については、ソフトウェア パッケージをダウンロードするためのアプライアンス アカウントの作成 （59 ページ） および Intersight 仮想アプライアンスのソフトウェアパッケージのダウンロード （60 ページ） を参照してください。

- [ローカル マシン（Local Machine）] で、ソフトウェア イメージを保存した場所を参照し、**[完了（Finish）]** をクリックして、**[インストール結果（Installation Result）]** 画面に進みます。
- **[ネットワーク共有（Network Share）]** オプションの場合は、プロトコルを入力し、ファイルのコピー元であるリモート サーバーの詳細を入力して、**[完了（Finish）]** をクリックして、**[インストール結果（Installation Result）]** 画面に進みます。
  - **[プロトコル（Protocol）]**：ファイル転送に使用される通信プロトコル。SCP（Secure Copy Protocol）および SFTP（Secure File Transfer Protocol）がサポートされています。
  - **[サーバ IP/ホスト名（Server IP/Hostname）]**：ファイルのコピー元のホスト サーバー

- **[ポート（Port）]**：使用する TCP ポート
- **[場所（Location）]**：コピーするファイルが保存されているディレクトリ
- **[ファイル名（Filename）]**：ネットワーク共有からコピーするファイルの名前
- **[ユーザ名（Username）]**：ネットワーク共有で認証するためのユーザー名
- **[パスワード（Password）]**：ネットワーク共有で認証するためのパスワード

d) **[インストール結果（Installation Result）]**：この画面でインストールの進行状況を確認できます。

ステップ 3 [Intersight仮想アプライアンスの接続（Intersight Virtual Appliance Connect）]ページにログインします。ユーザー名として **admin** を使用し、インストール プロセス中に設定したパスワードを入力します。

ステップ 4 **[ライセンス登録（Register License）]** プロセスを完了します。

1. このページで取得した予約要求コードを使用し、Cisco Smart Software Manager で予約承認コードを生成します。
2. **Cisco Smart Software Manager** で生成した予約承認コードをコピーし、[ライセンスの予約（Reserve License）] ページに貼り付けます。
3. **[インストール（Install）]** をクリックします。

   ライセンスの予約プロセスは完了するまでに数分かかる場合があります。Intersight ライセンス階層および登録に関する詳細は、『Cisco Intersight ライセンス階層および登録』をご覧ください。

[閉じる（Close）] をクリックすると、Cisco Intersight プライベート仮想アプライアンス ダッシュボードが表示されます。

次のタスク

単一ノードの Intersight 仮想アプライアンスの初期セットアップが正常に完了したら、ノードを追加してマルチノード クラスタを作成できます。詳細については、Intersight 仮想アプライアンスのマルチノード クラスタの構成 （48 ページ） を参照してください。

Intersight アプライアンス アシストのセットアップ

Cisco Intersight 仮想アプライアンスは、オープン仮想アプライアンス（OVA）ファイル形式、ZIP ファイル形式、または TAR ファイル形式で含まれている展開可能な仮想マシンとして配布されます。

始める前に:「VMware vSphere 上の Cisco Intersight 仮想アプライアンスおよび Intersight Assist のインストール （27 ページ）」の手順に従って、Intersight 仮想アプライアンスソフトウェアがインストールされていることを確認します。

Cisco Intersight 仮想アプライアンス ソフトウェアの展開が完了し、VM の電源がオンになったら、 <<https://your fqdn.com>> URLをクリックします。**[Intersight あぷらインす インストーラ**

（**Intersight Appliance Installer**）**]** 画面が表示され、新規インストール、バックアップからのアプライアンス ソフトウェアの回復、またはアプライアンスへのノードの追加のいずれかのセットアップを完了できます。

ウィザードで、ソフトウェアパッケージをダウンロードしてインストールする一連の手順を実行します。インストールの進行状況は確認できます。

次の手順を使用して Intersight Assist のセットアップを実行します。

ステップ 1 1.**[Intersight アプライアンス インストーラ（Intersight Appliance Installer）]** 画面で **[Intersight Assist]** を選択し、**[開始（Start）]** をクリックします。

ステップ 2 Cisco ID を使用して、[Intersight 仮想アプライアンスの接続（Intersight Virtual Appliance Connect ）] ページにログインします。シスコ ID をお持ちでない場合はこちらから作成してください。

1. （オプション）**[設定（Settings）]** をクリックして HTTPS プロキシ設定を有効にします。

   インターネットへ Cisco Intersight 仮想アプライアンスを接続するのに HTTP/S プロキシが必要な場合は、接続手順を実行する前にプロキシ設定を構成する必要があります。

   - **[設定（Settings）]** をクリックして **[HTTPS プロキシ（HTTPS Proxy）]** オプションを有効にします。
   - **プロキシ ホスト名**または **IP アドレス**と**プロキシ ポート**を追加します。

     プロキシ ポートは、1 ～ 65535 の範囲にする必要があります。アプライアンスの UI の **[システム（SystemI）]** > **[設定 (Settings)]** > **[ネットワーク (NETWORKING)]** > **[クラウド接続 (Cloud Connection)]** からプロキシの設定を編集することができます。

2. [接続 (Connect)] ページに表示されている**デバイス ID** と**要求コード**を使用して Intersight への接続を実行します。
3. **[接続 (Connection)]** のステータスに **[要求済み (Claimed)]** と表示されていることを確認します。

（注） 新しいブラウザタブが表示され、Intersight でのデバイスの要求ステータスが示されます。Intersight アカウントを持っていない場合は、**[アカウント作成 (Account Creation)]**ウィンドウでアカウントを作成し、ターゲットを要求することができます。ターゲット接続に成功すると、成功メッセージが表示されます。[閉じる（Close）] タブをクリックしてタブを終了し、Intersight 仮想アプライアンスのセットアップ ウィザードに戻ります。ターゲット要求が失敗した場合は、Intersight へのログイン画面が表示され、ターゲットを要求するワークフローが再開されます。

ステップ 3 **Intersight アプライアンス インストーラ** のセットアップ ウィザードで、次の手順を実行します。

a) **[接続（Connect）]** : **[続行（Continue）]** をクリックして、**[ネットワーク要件の確認（Check Network Requirements）]** ステップに進みます。

b) **[ネットワーク要件の確認（Check Network Requirements）]** : 結果を表示し、**[次へ（Next）]** をクリックして、**[内部ネットワークの構成（Configure Internal Network）]** ステップに進みます。

ネットワーク要件の確認中に DNS テストが失敗した場合は、構成を続行できないことに注意してください。

c) **[内部ネットワークの構成（Configure Internal Network）]**：必要に応じて、デフォルトの内部ネットワーク IP アドレスを変更し、**[次へ（Next）]** をクリックして **[インストール結果（Installations Results）]** 画面に進みます。

注意：この IP アドレス範囲は、Intersight 仮想アプライアンス内の内部通信に使用されます。この範囲は、172.16.0.0/12 サブネット内に収まる必要がありますが、より小さな範囲になる可能性があります（最大 20 サブネット プレフィックス サイズ）。ほとんどの場合、デフォルト値を使用できます。デフォルト値を変更する理由としては、アプライアンスが同じサブネット内の他のデバイ スと直接通信する必要がある場合、NAT など IP 変換メカニズムを通さずに通信する必要がある場合が考えられます。

d) **[インストール結果（Installation Result）]**：この画面でインストールの進行状況を確認できます。

Intersight 仮想アプライアンスのマルチノード クラスタの構成

インターサイト仮想アプライアンスのマルチノード クラスタにより、高可用性、安定性の向上、および回復力の向上が可能になります。VMware vSphere のシングルノード アプライアンスの初期セットアップが完了したら、追加ノードを加えることができます。2 つの追加ノードを正常に追加したら、Intersight 仮想アプライアンスでマルチノード クラスタを作成できます。

（注） マルチノード クラスタ構成は、VMware vSphere のインストールでのみサポートされることに注意してください。

重要 Intersight 仮想アプライアンスのマルチノード クラスタを設定すると、単一ノード インスタンスに戻すことはできません。

要件：

- 単一ノードアプライアンスの初期セットアップを完了した後に**のみ**、アプライアンスのマルチノードクラスタをセットアップできます。次のタスクの手順に従って、単一ノードの Intersight 仮想アプライアンス ソフトウェアがセットアップされていることを確認します。
  - シングルノード Intersight 接続型仮想アプライアンスのセットアップ
  - シングルノード Intersight プライベート仮想アプライアンスのセットアップ
- アプライアンスの初期設定が完了したら、いつでもマルチノード クラスタを設定できます。

- インターサイト仮想アプライアンスでマルチノードクラスタを作成するために追加のノードを追加できるようにするには、最初のノードが**操作可能**な状態になっている必要があります。

接続した仮想アプライアンスおよび プライベート仮想アプライアンスのマルチノード クラスタを設定するには、次の手順を実行します：

ステップ 1 VM を使用して <<https://myhost2.mydomain.com/ URL にアクセスします。

ステップ 2 **[Intersight アプライアンス インストーラー（Intersight Appliance Installer）]** 画面で、**[ノードをアプライアンスに追加（Add Node to Appliance）]** タブをクリックします。

ステップ 3 **[ノードをアプライアンスに追加（Add Node to Appliance）]** ページで次のフィールドの詳細を入力して**[終了（Finish）]**をクリックします。

- **[アプライアンス ホスト名/IP アドレス（ppliance Hostname/IP Address）]** — ノードが追加される既存のスタンドアローン アプライアンスのホスト名または IP アドレス。
- **[アプライアンス ユーザー名（Appliance Username）]** — 既存のスタンドアローン アプライアンスの管理ユーザー名。
- **[管理ユーザー パスワード（Admin User Password）]** — 既存のスタンドアローン アプライアンスの管理パスワード。

二つ目のノード（node2）が正常に追加されると、クラスタに参加する準備が整います。

この時点で、クラスタを作成できるように 3 番目のノード（node3）を追加できます。

ステップ 4 手順 1、2、および 3 の手順を繰り返して、node3 を追加します。

ステップ 5 node3 が正常に追加されたら、**[アプライアンス ポータルに移動（Go to Appliance Portal）]** をクリックしてアプライアンスに進みます。

ステップ 6 <<https:// myhost1.mydomain.com>> にログインします。

ステップ 7 **[サーバー セレクタ（Service Selector）]** ドロップダウン リストから **[システム（System）]** を選択し、**[設定（Settings）]** > **[一般（GENERAL）]** > **[アプライアンス（Appliance）]** に移動します。

node2 と node3 が**[参加準備完了（Ready to Join）]**状態であることを確認します。

ステップ 8 [クラスタの作成（Create Cluster）] をクリックします。

重要 クラスタを作成する操作は元に戻すことができません。

クラスタ作成ワークフローの実行中、アプライアンスはメンテナンス モードに切り替わることに注意してください。進行状況ページが読み込まれるまで 5 ～ 10 分かかります。その後、**[マルチノード クラスターの作成結果（Multi-Node Cluster Creation Results）]** ページでクラスター作成の進行状況を確認できます。また、ノード2とノード3でのクラスタ作成の進行状況を表示することもでき、すぐに利用できます。

セット アップが完了すると、ログイン画面が表示されます。

ステップ 9 **[インターサイト仮想アプライアンスの接続（Intersight Virtual Appliance Connect）]** ページにログインします。

ユーザー名として **admin** を使用し、初期の単一ノードアプライアンスセットアップ中に設定したパスワードを入力します。この時点で、node2 と node3 にもログインできます。

---

1 つのノードがダウンすると、マルチノード クラスタは完全に動作します。1 つのノードがダウンすると、アプライアンスは自動的に安定します。移行段階では、アプライアンスにアクセスできない場合があります。

2 つのノードがダウンすると、マルチノードクラスタはメンテナンスモードに移行します。この状態の間、システムは動作しません。

ノードが起動すると、マルチノードクラスタは自動的に **[動作可能（Operational）]** になります。

既存のシングルノード展開からマルチノードクラスタ構成への移行パス

既存の単一ノードの Intersight 仮想アプライアンス展開をマルチノード クラスタ構成に拡張するには、次の手順を実行します。

1. アプライアンスのバックアップを作成します。

   詳細については、「バックアップの作成」を参照してください。

2. Intersight 仮想アプライアンスを回復します。

   詳細については、「Intersight 接続型仮想アプライアンスのリカバリ 」と「Intersight プライベート仮想アプライアンスのリカバリ 」を参照してください。

既存の単一ノード展開用のマルチノードクラスタの構成が正常に完了したら、次のリンクの情報を使用して、マルチノード クラスタの追加構成を実行します。

- Intersight 仮想アプライアンスでのシングル サインオン
- 証明書

Intersight 接続型仮想アプライアンスのリカバリ

Cisco Intersight 仮想アプライアンスは、オープン仮想アプライアンス（OVA）ファイル形式、ZIP ファイル形式、または TAR ファイル形式で含まれている展開可能な仮想マシンとして配布されます。

接続型仮想アプライアンス構成を復元するには、初期セットアップ時にバックアップ ファイルからデータを復旧します。

始める前に:「VMware vSphere 上の Cisco Intersight 仮想アプライアンスおよび Intersight Assist のインストール （27 ページ）」の手順に従って、Intersight 仮想アプライアンスソフトウェアがインストールされていることを確認します。

Cisco Intersight 仮想アプライアンス ソフトウェアの展開が完了し、VM の電源がオンになったら、 <<https://your fqdn.com>> URLをクリックします。**[インストーラ オプション（Installer Options）]**画面が表示され、新規インストールのセットアップを完了したり、バックアップからアプライアンス ソフトウェアを回復したりできます。

ウィザードで、ソフトウェアパッケージをダウンロードしてインストールする一連の手順を実行します。リカバリの進行状況は確認できます。

次の手順を使用して、バックアップ ファイルから構成をリカバリします。

ステップ 1 **[インストーラ オプション（Installer Options）]** 画面で、**[バックアップからリカバリ（Recover from Backup）]** タブを選択し、**[スタート（Start）]** をクリックします。

ステップ 2 **[バックアップの選択（Select Backup）]** ページでプロトコルを選択し、バックアップ データをリカバリするリモート サーバーの詳細を入力します。

- **[プロトコル（Protocol）]** : バックアップ プロセスで使用される通信プロトコルのオプション。現時点で Intersight 仮想アプライアンスがバックアップでサポートしているプロトコルは SCP（Secure Copy Protocol）と SFTP（Secure File Transfer Protocol）です。
- **[サーバ IP/ホスト名（Server IP/Hostname）]** : バックアップ データのリカバリ元のホスト
- **[ポート（Port）]** : バックアップ サーバーの TCP ポート
- **[場所（Location）]** : バックアップ ファイルを保存するディレクトリ
- **[ファイル名（Filename）]** : 復元するバックアップ ファイルの名前
- **[ユーザ名（Username）]** : バックアップ サーバーでバックアップ クライアントを認証するためのユーザー名
- **[パスワード（Password）]** : バックアップ サーバーでバックアップ クライアントを認証するためのパスワード

ステップ 3 **[次へ（Next）]** をクリックします。

重要 **復元プロセスは一度開始すると変更できません。**

ステップ 4 ポップアップ上で **[続行（Continue）]** をクリックします。

ステップ 5 **[ソフトウェア バージョンの選択（Select Software Version）]** ページには、アプライアンス ソフトウェアの最新バージョンをダウンロードするオプションがあります。または、インストーラのバージョンと同じか、インストーラのバージョンより大きい、サポートされている他のバージョンのソフトウェアをアップロードできます。

a) アプライアンス ソフトウェアの最新バージョンをダウンロードするには、**[最新バージョンのダウンロード（Download Latest Version）]** ボタンを選択し、**[完了（Finish）]** をクリックします。

b) アプライアンス ソフトウェアのバージョンをアップロードするには、ソフトウェア パッケージの保存場所に応じて、**[ローカル マシン（Local Machine）]** または **[ネットワーク共有（Network Share）]** を選択します。

（注） Intersight 接続型仮想アプライアンスを手動で復元するには、アプライアンスアカウントにアクセスして、必要なソフトウェアパッケージをダウンロードする必要があります。詳細については、ソフトウェアパッケージをダウンロードするためのアプライアンスアカウントの作成（59 ページ） および Intersight 仮想アプライアンスのソフトウェアパッケージのダウンロード（60 ページ） を参照してください。

- [ローカル マシン（Local Machine）] で、ソフトウェア イメージを保存した場所を参照し、**[完了（Finish）]** をクリックします。
- **[ネットワーク共有（Network Share）]** オプションの場合は、プロトコルを入力し、ファイルのコピー元であるリモート サーバーの詳細を入力して、**[完了（Finish）]** をクリックします。
  - **[プロトコル（Protocol）]**：ファイル転送に使用される通信プロトコル。SCP（Secure Copy Protocol）および SFTP（Secure File Transfer Protocol）がサポートされています。
  - **[サーバ IP/ホスト名（Server IP/Hostname）]**：ファイルのコピー元のホスト サーバー
  - **[ポート（Port）]**：使用する TCP ポート
  - **[場所（Location）]**：コピーするファイルが保存されているディレクトリ
  - **[ファイル名（Filename）]**：ネットワーク共有からコピーするファイルの名前
  - **[ユーザ名（Username）]**：ネットワーク共有で認証するためのユーザー名
  - **[パスワード（Password）]**：ネットワーク共有で認証するためのパスワード

[リカバリ結果（Recovery Results）] ページでリカバリの進行状況を確認できます。リカバリ プロセスが完了すると、Cisco Intersight 接続型仮想アプライアンス ダッシュボードが表示されます。

次のタスク

マルチノードクラスタ展開のリカバリをするには：マルチノードクラスタ展開からバックアップからリカバリをする場合、まず node1 でリカバリしてから、Intersight 仮想アプライアンスのマルチノード クラスタの構成（48 ページ） の手順にしたがいマルチノードクラスタを作成するために 2 つの追加ノードを加えます。

Intersight プライベート仮想アプライアンスのリカバリ

Cisco Intersight 仮想アプライアンスは、オープン仮想アプライアンス（OVA）ファイル形式、ZIP ファイル形式、または TAR ファイル形式で含まれている展開可能な仮想マシンとして配布されます。

プライベート仮想アプライアンス構成を復元するには、初期セットアップ時にバックアップ ファイルからデータを復旧します。

始める前に:「VMware vSphere 上の Cisco Intersight 仮想アプライアンスおよび Intersight Assist のインストール （27 ページ）」の手順に従って、Intersight 仮想アプライアンスソフトウェアがインストールされていることを確認します。

Cisco Intersight 仮想アプライアンス ソフトウェアの展開が完了し、VM の電源がオンになったら、 <<https://your fqdn.com>> URLをクリックします。**[インストーラ オプション（Installer Options）]**画面が表示され、新規インストールのセットアップを完了したり、バックアップからアプライアンス ソフトウェアを回復したりできます。

ウィザードで、ソフトウェアパッケージをダウンロードしてインストールする一連の手順を実行します。リカバリの進行状況は確認できます。

次の手順を使用して、バックアップ ファイルから構成をリカバリします。

ステップ 1 **[インストーラ オプション（Installer Options）]** 画面で、**[バックアップからリカバリ（Recover from Backup）]** タブを選択し、**[スタート（Start）]** をクリックします。

ステップ 2 **[バックアップの選択（Select Backup）]** ページでプロトコルを選択し、バックアップ データをリカバリするリモート サーバーの詳細を入力します。

- **[プロトコル（Protocol）]**：バックアップ プロセスで使用される通信プロトコルのオプション。現時点で Intersight 仮想アプライアンスがバックアップでサポートしているプロトコルは SCP（Secure Copy Protocol）と SFTP（Secure File Transfer Protocol）です。
- **[サーバ IP/ホスト名（Server IP/Hostname）]**：バックアップ データのリカバリ元のホスト
- **[ポート（Port）]**：バックアップ サーバーの TCP ポート
- **[場所（Location）]**：バックアップ ファイルを保存するディレクトリ
- **[ファイル名（Filename）]**：復元するバックアップ ファイルの名前
- **[ユーザ名（Username）]**：バックアップ サーバーでバックアップ クライアントを認証するためのユーザー名
- **[パスワード（Password）]**：バックアップ サーバーでバックアップ クライアントを認証するためのパスワード

ステップ 3 **[次へ（Next）]** をクリックします。

重要　復元プロセスは一度開始すると変更できません。

ステップ 4 ポップアップ上で **[続行（Continue）]** をクリックします。

ステップ 5 **[ソフトウェア バージョンの選択（Select Software Version）]** ページでは、インストーラのバージョンと同じか、インストーラのバージョンより大きい、サポートされている他のバージョンのソフトウェアをアップロードできます。

（注） Intersight プライベート仮想アプライアンスを手動で復元するには、必要なソフトウェアパッケージをダウンロードできるようにアプライアンスアカウントにアクセスする必要があります。詳細については、ソフトウェア パッケージをダウンロードするためのアプライアンス アカウントの作成（59 ページ） および Intersight 仮想アプライアンスのソフトウェアパッケージのダウンロード（60 ページ） を参照してください。

- [ローカル マシン（Local Machine）] で、ソフトウェア イメージを保存した場所を参照し、**[完了（Finish）]** をクリックします。
- **[ネットワーク共有（Network Share）]** オプションの場合は、プロトコルを入力し、ファイルのコピー元であるリモート サーバーの詳細を入力して、**[完了（Finish）]** をクリックします。
  - **[プロトコル（Protocol）]**：ファイル転送に使用される通信プロトコル。SCP（Secure Copy Protocol）および SFTP（Secure File Transfer Protocol）がサポートされています。
  - **[サーバ IP/ホスト名（Server IP/Hostname）]**：ファイルのコピー元のホスト サーバー
  - **[ポート（Port）]**：使用する TCP ポート
  - **[場所（Location）]**：コピーするファイルが保存されているディレクトリ
  - **[ファイル名（Filename）]**：ネットワーク共有からコピーするファイルの名前
  - **[ユーザ名（Username）]**：ネットワーク共有で認証するためのユーザー名
  - **[パスワード（Password）]**：ネットワーク共有で認証するためのパスワード

[リカバリ結果（Recovery Results）] ページでリカバリの進行状況を確認できます。リカバリ プロセスが完了すると、Cisco Intersight プライベート仮想アプライアンス ダッシュボードが表示されます。

次のタスク

マルチノード クラスタ 展開のリカバリをするには： マルチノード クラスタ展開からバックアップからリカバリをする場合、まず node1 でリカバリしてから、Intersight 仮想アプライアンスのマルチノード クラスタの構成（48 ページ） の手順にしたがいマルチノードクラスタを作成するために 2 つの追加ノードを加えます。

Intersight 仮想アプライアンスのマルチノードクラスタのノードを交換

次のいずれかの理由により、マルチノードクラスタ内のノードを置き換えることができます。

- マルチノード クラスタ内のノードに **障害**が発生した場合。
- 既存のマルチノード クラスタ内 **のノードの IP アドレスを変更する場合** 。

既存のクラスタ内のノードを交換するには、次の手順を実行します。

ステップ 1 VMware vSphere、Microsoft Hyper-V サーバ、KVM ハイパーバイザのインストールから、不具合のあるノードまたはまたは IPv4 アドレスを変更するノードをパワーオフして削除します。

ステップ 2 マルチノード クラスタで別の運用ノードにログインします。

ステップ 3 **[サーバー セレクタ（Service Selector）]** ドロップダウン リストから **[システム（System）]** を選択し、**[設定（Settings）]** > **[一般（GENERAL）]** > **[アプライアンス（Appliance）]** に移動します。

ステップ 4 **[ノード（Node）]** の下のテーブルで、次の手順を実行します。

1. **[障害（Impaired）]**または**[不明（Unknown）]**ステータスを表示するノードの行で、**[省略記号（ellipses）]**をクリックします。
2. **[ノードの置換（Replace Node）]** をクリックします。

このノードのステータスは、**[アウト オブ サービス（Out of Service）]**として表示されます。

ステップ 5 同じ IPv4 アドレスまたは新しい IPv4 アドレスを使用して、置き換えられるノードと同じ DNS ドメイン値を使用して、新しい OVA を展開します。

（注） IPv4 アドレスを変更する場合は、新しい IPv4 アドレスで DNS ドメイン値を更新します。

アプライアンスのインストールと展開の詳細については、VMware vSphere 上の Cisco Intersight 仮想アプライアンスおよび Intersight Assist のインストールの章を参照してください。

ステップ 6 <https://*fqdn-of-your-appliance*.com> URL を使用して VM にアクセスします。

ステップ 7 [インストーラー オプション] 画面で、[ノードをアプライアンスに追加] タブをクリックします。

ステップ 8 **[ノードをアプライアンスに追加（Add Node to Appliance）]** ページで次のフィールドの詳細を入力して **[終了（Finish）]**をクリックします。

- **[アプライアンス ホスト名/IP アドレス（Appliance Hostname/IP Address）]**：ノードが追加される既存のアプライアンス VM のホスト名または IP アドレスが追加されます。
- **[アプライアンス ユーザー名（Appliance Username）]**：既存のアプライアンス VM の管理ユーザー名。
- **[管理ユーザー パスワード（Admin User Password）]**：既存のアプライアンス VM の管理パスワード。

ノードが正常に追加されると、クラスタに参加する準備が整います。

ステップ 9 運用ノードの 1 つにログインします。

ステップ 10 運用ノードの **[アプライアンス ポータルに移動（Go to Appliance Portal）]** をクリックし、アプライアンスに進みます。

ステップ 11 **[設定（Settings）]** アイコン > **[設定（Settings）]** > **[一般（General）]** > **[アプライアンス（Appliance）]** に移動します。

ステップ 12 クラスタに参加する準備ができているノードの行で、次の手順を実行します。

1. 省略記号をクリックします。
2. **[クラスタに参加（Join Cluster）]** をクリックします。
3. ポップアップ画面で、**[参加（Join）]** をクリックします。

ワークフローの進行状況をモニタリングできます。ワークフローが正常に実行されると、置き換えられたノードは完全に動作可能になります。

Cisco Intersight 仮想アプライアンスのハイアベイラビリティおよびディザスタリカバリ

Cisco Intersight 仮想アプライアンスは、ハイアベイラビリティ（HA）およびディザスタリカバリ（DR）の移行アーキテクチャをサポートします。

Intersight 仮想アプライアンスを正常に移行するには、次の要件を満たす必要があります。

- Intersight 仮想アプライアンスに完全修飾ドメイン名（FQDN）があります。Intersight 仮想アプライアンスを移行するには、アプライアンスの FQDN（ホスト名）を同じままにする必要があります。
- Intersight 仮想アプライアンスとその管理対象エンドポイント間のネットワーク接続を維持する必要があります。

Intersight 仮想アプライアンスのハイアベイラビリティ

ベンダーが提供するソリューションを活用して、Intersight 仮想アプライアンスでハイアベイラビリティ（HA）機能を提供できます。

VMware vSphere に展開された Intersight 仮想アプライアンス — Intersight 仮想アプライアンスは VMware ハイアベイラビリティ (VMHA) をサポートしており、仮想アプライアンスの動作が中断しないことを保証します。VMware HA の詳細については、VMware の Web サイトで関連するドキュメントを参照してください。

Microsoft Hyper-V Server に展開された Intersight 仮想アプライアンス — Intersight 仮想アプライアンスは Microsoft Hyper-V ハイアベイラビリティ (VMHA) をサポートしており、仮想アプライアンスの動作が中断しないことを保証します。Microsoft Hyper-V は、ホストサーバーで実行されているワークロードを保護するためのフェイルオーバー クラスタリング ハイアベイラビリティ ソリューションを提供し、それによってアプライアンスを保護します。フェールオーバー クラスタリング機能により、ユーザーはサービスの中断を最小限に抑えることができます。Microsoft Hyper-V HA の詳細については、Microsoft のウェブサイトの関連ドキュメントを参照してください。

KVM ハイパーバイザに展開された Intersight 仮想アプライアンス — KVM は、複数のオペレーティング システム（OS）ベンダーによってサポートされています。最も一般的な OS ベンダー

は、Red-Hat Virtualization と Ubuntu です。ハイアベイラビリティの特定のソリューションについては、OS ベンダーが提供するドキュメントを参照してください。

Intersight 仮想アプライアンスのディザスタリカバリ

ディザスタリカバリには、Intersight 仮想アプライアンスまたはその他のサードパーティ ソリューションの既存のバックアップと復元機能を使用できます。

Intersight 仮想アプライアンスでのバックアップと復元

シスコでは、Intersight 仮想アプライアンスの定期的なバックアップを取ることを強くお勧めしています。

Intersight 仮想アプライアンスのバックアップについては、「データのバックアップ」を参照してください。

Intersight 接続型仮想アプライアンスの復元については、「Intersight 接続型仮想アプライアンスのリカバリ」を参照してください。

Intersight プライベート仮想アプライアンスの復元については、「Intersight プライベート仮想アプライアンスのリカバリ」を参照してください。

サードパーティのディザスタリカバリ ソリューション

仮想マシンのディザスタリカバリ構成では、ベンダーが提供するソリューションを使用してディザスタリカバリ機能を強化できます。構成の詳細については、ベンダー固有の構成マニュアルを参照してください。

VMware のディザスタリカバリ ソリューション

- **VMware スナップショット** — Intersight 仮想アプライアンスのバックアップおよび復元機能に加えて、VMware では、仮想マシンの状態とデータを保持するための VM スナップショットも使用できます。状態の保持には VM の電源状態が含まれ、データの保持には、ディスク、メモリなどデバイスの仮想ネットワーク インターフェイス カードを含むすべてのファイルが含まれます。VM スナップショットを作成する前に、アプライアンス（VM）の電源をオフにすることを強くお勧めします。VM スナップショットの詳細については、VMware の Web サイトで関連ドキュメントを参照してください。
- **VMware vSphere 上に展開された Intersight 仮想アプライアンス** — VMware には、ディザスタリカバリのためのソリューションがいくつかあります。
  - VMware-SRM（VMware Site Recovery Manager）
  - VMware-VRS（VMware vSphere Replication）

Microsoft Hyper-V のディザスタリカバリ ソリューション

Microsoft Hyper-V には、効率的な VM ディザスタリカバリを提供する一連の組み込み機能が含まれています。Hyper-V 仮想マシンのディザスタリカバリは、VM をバックアップまたはレプリケートすることによって実行できます。どちらのオプションにも、ディザスタリカバリ計画を作成する際に考慮すべき特定の側面があります。詳細については、Microsoft の Web サイトの関連ドキュメントを参照してください。

KVM ハイパーバイザのディザスタリカバリ ソリューション

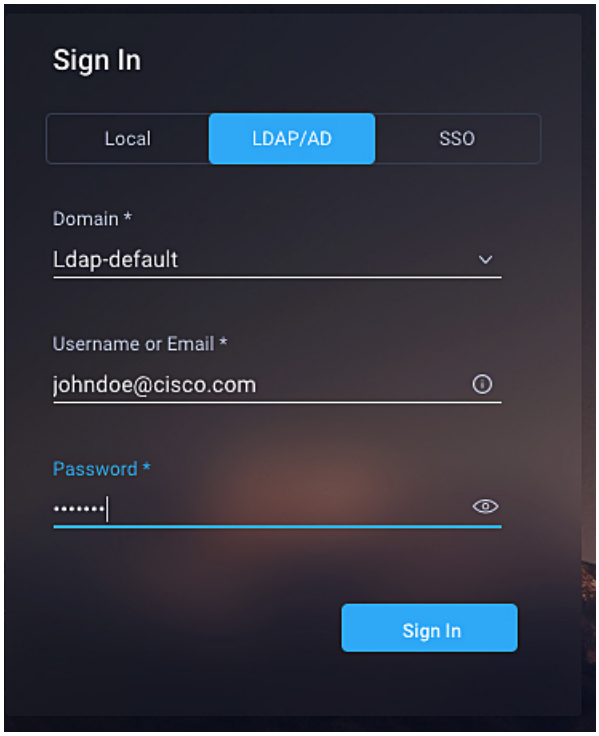
KVM は、複数のオペレーティングシステム（OS）ベンダーによってサポートされています。最も一般的な OS ベンダーは、Red Hat Virtualization と Ubuntu です。KVM 上に展開された Intersight 仮想アプライアンスのディザスタリカバリ専用ソリューションについては、OS ベンダーが提供するドキュメントを参照してください。

その他の承認されたサードパーティ製ディザスタリカバリ ソリューションについては、サードパーティのインストールマニュアルを参照してください。

Intersight 仮想アプライアンスにログイン

Intersight 仮想アプライアンスにログイン

Intersight 仮想アプライアンスをインストールした後、次に説明するいずれかの方法でユーザーとしてアプライアンスにログインできます。[LDAP/AD] タブと [SSO] タブは、アカウントの LDAP 設定または SSO を設定した後に表示されます。



- **[ローカル ユーザ (Local User)]**: ユーザー名として **admin** を使用し、アプライアンスの登録時に設定したものと同じパスワードを使用します。登録時に設定したパスワードが脆弱である場合、Interswitch はパスワードをより強力なものに変更するように要求します。強力なパスワードに正常にリセットされると、アプライアンスに直接ログインします。Intersight は、ローカル ユーザー（admin）を 1 つだけサポートします。

- **[LDAP/AD]**: 設定した LDAP ドメインを選択し、**ユーザー名**または**電子メール**と、LDAP サーバーで設定したパスワードを入力します。ログインに使用するユーザー名は、LDAP サーバーでユーザに対して設定した **sAMAccountName** と同じである必要があります。詳細については、「LDAP 設定」、「ユーザーの追加」および「グループの追加」を参照してください。
- **[SSO]**: ID プロバイダーで SSO を設定するために使用した電子メール ID を入力します。シングル サインオン (SSO) 認証では複数のアプリケーションへのログインに 1 つのクレデンシャル セットを使用できます。SSO の詳細については、「SSO のセットアップ」を参照してください。

[ローカル ユーザのみの場合（For Local User Only）]：ユーザー名またはパスワードが正しくないためにローカル ユーザー ログインが失敗した場合、失敗したログイン情報の詳細が監査ログに記録されます。アプライアンスに正常にログインすると、監査ログにある失敗したログインの詳細を表示できます。

ソフトウェア パッケージをダウンロードするためのアプライアンス アカウントの作成

Intersight プライベート仮想アプライアンスの展開を完了する、または Intersight 接続型仮想アプライアンスを手動で更新するには、Intersight 仮想アプライアンス、HyperFlex、UCS Director、および HCI ソフトウェア パッケージをダウンロードできるように、アプライアンス アカウントにアクセスする必要があります。

（注） アプライアンス アカウントの更新を定期的に確認し、Intersight 仮想アプライアンス ソフトウェアの最新バージョンを使用することを強くお勧めします。Intersight 仮想アプライアンス ソフトウェアは、新機能と拡張機能を含むように継続的に改善されているためです。また、製品の「N-3」ソフトウェア バージョンのみがサポートされ、「N」がアプライアンス ソフトウェアの最新バージョンであることに注意することも重要です。

インストール用に手動でアップロードするソフトウェアのバージョンが、常に実行中のバージョンよりも高いことを確認します。

このタスクの手順を使用して、アプライアンスアカウントを作成します。

ステップ 1 Cisco ID を使用して https://www.intersight.com/pvapp にログインしてください。シスコ ID をお持ちでない場合はこちらから作成してください。

注：プライベート仮想アプライアンスアカウントを作成する場合にのみ、https://www.intersight.com/pvapp にログインする必要があります。アプライアンス アカウントを作成したら、Intersight にログインすることでアカウントにアクセスできます。

ステップ 2 ライセンス条項に同意し、**[次へ（Next）]** をクリックします。

ステップ 3 **[アプライアンス アカウントの作成（Appliance Account Creation）]** 画面でアプライアンス アカウントの名前を入力します。

ステップ 4 **[作成（Create）]** をクリックします。

アプライアンスアカウントが正常に作成されたら、Intersight にログインしてアカウントにアクセスし、必要な Intersight プライベート仮想アプライアンス、HyperFlex、、または Cisco UCS Director ソフトウェアパッケージをダウンロードできます。

Cisco UCS サーバーファームウェアおよび Cisco UCS サーバー設定ユーティリティをダウンロードするには、Cisco Software Central にアクセスします。

（注） アカウント管理者は、作成されたアプライアンス アカウントにユーザーとグループがアクセスできるようにします。ユーザーとグループを追加する方法の詳細については、「ユーザーの追加 （109 ページ）」と「グループの追加 （111 ページ）」を参照してください。

（注） Intersight 仮想アプライアンスのソフトウェア更新を最新の状態に保つように電子メール通知を構成できます。詳細については、「Intersight 仮想アプライアンスでのソフトウェア更新の電子メール通知の構成」を参照してください。

Intersight 仮想アプライアンスのソフトウェアパッケージのダウンロード

このタスクの手順を使用して、Intersight 仮想アプライアンス、UCS ファームウェア、Hyperflex、UCS Director、HCI ソフトウェア パッケージをダウンロードします。

（注） Cisco UCS サーバーファームウェアおよび Cisco UCS サーバー設定ユーティリティをダウンロードするには、Cisco Software Central にアクセスします。

始める前に

アプライアンスアカウントが作成されていることを確認します。アプライアンスアカウントを作成していない場合は、ソフトウェア パッケージをダウンロードするためのアプライアンス アカウントの作成 （59 ページ） を参照してください。

ステップ 1 Cisco ID を使用して Intersight にログインします。シスコ ID をお持ちでない場合はこちらから作成してください。

ステップ 2 アプライアンス アカウントにアクセスするために作成したアカウントを選択します。

[ソフトウェアのダウンロード（Software Download）] ページが表示されます。

ステップ 3 **[ソフトウェア カタログ（Catalog）]** をクリックします。

このページに表示されるタブから必要なソフトウェア パッケージをダウンロードできます。**[+]** をクリックしてカスタムタブを作成することもできます。

[ダウンロード（My Download）] タブには、すべてのダウンロードに関する情報と、ダウンロード可能なソフトウェアの最新バージョンが表示されます。さらに、アプライアンスの **[監査ログ（Audit Logs）]** ですべてのダウンロードのログを見つけることができます。

アプライアンスへのソフトウェアのアップロードに進むことができます。詳細については、「Intersight プライベート仮想アプライアンスのソフトウェア パッケージのダウンロード （61 ページ）」を参照してください。

ソフトウェアパッケージをアップロードした後、要求されたターゲットにそれらをインストールできます。Cisco UCS Director ターゲットのコネクタパックをアップグレードするには、「UCS Director インスタンスでのコネクタパックのアップグレード」を参照してください。

（注） ESXi ソフトウェアパッケージも、Hyperflex ソフトウェアパッケージの一部としてダウンロードされます。したがって、ESXi ソフトウェアパッケージを個別にダウンロードする必要はありません。

Intersight プライベート仮想アプライアンスのソフトウェア パッケージのダウンロード

Intersight プライベート仮装アプライアンスは、切断（エアギャップ）モードでデータセンターを運用する環境を対象としています。したがって、ソフトウェアパッケージは Cisco Software Central サイトから、または Intersight のアプライアンスアカウントにアクセスしてダウンロードし、アプライアンスにアップロードする必要があります。

プライベート仮想アプライアンスのソフトウェアパッケージをアップロードするには、次の手順を使用します。

始める前に

必要なソフトウェアパッケージが次のようにダウンロードされていることを確認します。

- Cisco UCS サーバーファームウェアおよび Cisco UCS サーバー設定ユーティリティをダウンロードするには、Cisco Software Central にアクセスします。
- Cisco HyperFlex、Cisco UCS Director、またはIntersight Private Virtual Appliance ソフトウェアパッケージをダウンロードするには、アプライアンスアカウントにアクセスする必要があります。詳細については、ソフトウェアパッケージをダウンロードするためのアプライアンス アカウントの作成 （59 ページ）およびIntersight 仮想アプライアンスのソフトウェアパッケージのダウンロード （60 ページ）を参照してください。

ステップ 1 左のナビゲーション パネルから、**[ソフトウェア リポジトリ（Software Repository）]** > **[ソフトウェア（Software）]**.をクリックします。

ステップ 2 **[ソフトウェアをアップロード（Upload Software）]** をクリックします。

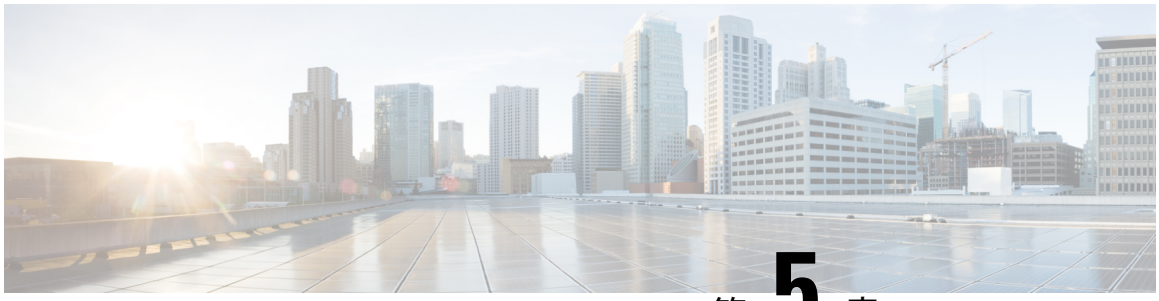
[ソフトウェアをアップロード（Upload Software）] ページが表示されます。

a) ソフトウェア パッケージの保存場所に応じて、**[ローカル マシン（Local Machine）]** または **[ネットワーク共有（Network Share）]** を選択し、**[次へ（Next）]** をクリックします。

b) **[ネットワーク共有（Network Share）]** オプションの場合は、プロトコルを入力し、ファイルのコピー元であるリモートサーバーの詳細を入力します。

- **[プロトコル（Protocol）]**：ファイル転送に使用される通信プロトコル。SCP（Secure Copy Protocol）および SFTP（Secure File Transfer Protocol）がサポートされています。
- **[サーバ IP/ホスト名（Server IP/Hostname）]**：ファイルのコピー元のネットワーク共有サーバー
- **[ポート（Port）]**：使用する TCP ポート
- **[場所（Location）]**：コピーするファイルが保存されているディレクトリ
- **[ファイル名（Filename）]**：ネットワーク共有からコピーするファイルの名前
- **[ユーザ名（Username）]**ネットワーク共有で認証するためのユーザー名
- **[パスワード（Password）]**：ネットワーク共有で認証するためのパスワード

[要求（Requests）] アイコンをクリックすると、アップロードの進行状況を追跡できます。アップロードプロセスが正常に完了すると、アップロードしたソフトウェアが [ソフトウェア リポジトリ（Software Repository）] ページに表示されます。



第 5 章

ソフトウェア アップデート

Intersight 仮想アプライアンス 1.1.0-0 のアップグレード動作：CentOS 7 から AlmaLinux 9 への移行の影響

Intersight 仮想アプライアンスリリースバージョン 1.1.0-0 以降、基盤となるオペレーティングシステムは AlmaLinux 9 です。

（注） アップグレード プロセスを開始する前に、アプライアンス VM のスナップショットとアプライアンスのバックアップを作成することを強くお勧めします。

次の情報は、この移行の主要な側面を示しています。

- Intersight 仮想アプライアンス リリース バージョン 1.1.0-0 以降、すべての新しいアプライアンスと Assist のインストールは、AlmaLinux 9 に基づいています。
- バージョン 1.1.0-0 以降にアップグレードするバージョン 1.0.9-631 以降の既存の Appliance and Assist インストールは、AlmaLinux 9 にインプレース アップグレードされます。
- バージョン 1.0.9-615 以前からバージョン 1.1.0-0 に直接アップグレードすると失敗します。したがって、バージョン 1.0.9-615 以前からバージョン 1.1.0-0 にアップグレードする場合は、次の手順を実行します。
  - アプライアンスがディスク要件を満たしていることを確認します。詳細については、「新規の Intersight 仮想アプライアンスの VM 情報技術要件」を参照してください。

- バージョン 1.1.0-0 にアップグレードする前に、次のいずれかのバージョンにアップグレードします。
  - 1.0.9-631
  - 1.0.9-655
  - 1.0.9-675
  - 1.0.9-677

- 既存のアプライアンスまたは Assist をバージョン 1.1.0-0 にアップグレードする場合、次の動作が想定されます。
  - アップグレードが完了するまでに少なくとも 4 時間かかり、複数回再起動します。
  - アプライアンス Web UI、REST API、および CLI インターフェイスは使用できない場合があります。VM コンソールでアップグレードの進捗をモニタ出来ます。
  - VM が損傷し、アップグレードプロセスが中断する可能性があるため、アップグレード プロセス中にアプライアンスまたはアシスト VM を手動で再起動し**ない**ことを **強く推奨**します。

- リリース バージョン 1.1.0-0 のインストールとアップグレードのバンドル サイズは、AlmaLinux への切り替えにより、以前のリリースのバンドル サイズよりも大きくなります。

Intersight 接続型仮想アプライアンス ソフトウェアの更新

Intersight Connected Virtual Appliance では、更新サービスによって新しいバージョンが使用可能になったときに自動的にソフトウェアを更新するか、実行中のバージョンよりも上位の使用可能なバージョンに手動で更新することができます。

接続型仮想アプライアンスが**自動**モード（デフォルト モード）で更新するように設定されている場合、クラウドからソフトウェアを直接取得して、サービス パッケージ、カーネルを含む OS パッケージ、およびその他のセキュリティ修正を更新します。設定中に行われた選択に基づいて、インストールは猶予期間に従って行われるか、カスタムインストールスケジュールに従って行われます。自動モードでは、新しい更新が 90 日以上利用可能にならない場合は、Intersight 仮想アプライアンスが intersight に接続されていることを確認します。

（注）
- アプライアンス ソフトウェアの更新には**自動**モードを使用することをお勧めします。
- ソフトウェアのアップグレードはノード レベルではなくクラスタ レベルで行われるため、マルチノード アプライアンスでのソフトウェア アップグレードとシングル ノード アプライアンスでのソフトウェア アップグレードに違いはありません。

手動モードで更新するようにアプライアンスが設定されている場合、ソフトウェアイメージを保存した場所に応じて、ローカル マシンまたはネットワーク共有サーバーからソフトウェアイメージをアップロードできます。ソフトウェアイメージがアップロードされたら、更新をすぐにインストールするか、またはインストールの日時をスケジュールするかを選択できます。接続型仮想アプライアンスを手動で更新するには、アプライアンスポータルから必要なソフトウェアパッケージをダウンロードする必要があることに注意してください。詳細については、ソフトウェア パッケージをダウンロードするためのアプライアンス アカウントの作成 （59 ページ）およびIntersight 仮想アプライアンスのソフトウェアパッケージのダウンロード （60 ページ）を参照してください。

（注） アプライアンスアカウントの更新を定期的に確認し、Intersight 仮想アプライアンス ソフトウェアの最新バージョンを使用することを強くお勧めします。Intersight 仮想アプライアンス ソフトウェアは、新機能と拡張機能を含むように継続的に改善されているためです。また、製品の「N-3」ソフトウェア バージョンのみがサポートされ、「N」がアプライアンス ソフトウェアの最新バージョンであることに注意することも重要です。

インストール用に手動でアップロードするソフトウェアのバージョンが、常に実行中のバージョンよりも高いことを確認します。

次の手順を使用して、**接続済み仮想アプライアンス**のソフトウェア更新を設定します。

開始する前に：Intersight Connected Virtual Appliance が Intersight に接続されていることを確認します。

ステップ 1 アカウント管理者ロールを持つユーザーとして Intersight 仮想アプライアンスにログインします。

ステップ 2 **[サーバー セレクタ（Service Selector）]** ドロップダウン リストから **[システム（System）]** を選択し、**[設定（Settings）]** > **[一般（GENERAL）]** > **[ソフトウェア（Software）]** に移動します。 インストールされているソフトウェアに関する次の詳細が表示されます。

自動設定モードでは、次の詳細が表示されます。

- **稼働中のバージョン**：現在のソフトウェア バージョン番号
- **更新モード**：自動
- **[インストールスケジュール（Installation Schedule）]**：更新がスケジュールされている日時が表示されます。

手動設定モードでは、次の詳細が表示されます。

- **稼働中のバージョン**：現在のソフトウェア バージョン番号
- **更新モード**：手動

両方のモードで、**保留中の更新**に関する次の詳細が表示される場合があります。

- **バージョン**：更新がスケジュールされているソフトウェア バージョンを示します。

- **更新の影響タイプ**：これは、**破壊的**、**破壊的な再起動**、または**なし**の可能性があります。この影響は、インフラストラクチャのアップグレードまたは他のサービスのアップグレードによって中断される可能性があります。中断のない更新によって、**更新の影響期間**に指定された期間に Intersight が使用できなくなる場合があります。アプライアンスの中断的な再起動は、カーネルの更新とサービスの再起動が原因で発生する可能性があります。更新の計画と管理を改善するために、猶予期間が提供されます。中断を伴う再起動がある場合、UI には適切なメッセージが表示されます。

  注目　アプライアンスの更新が完了するまでに約 90 分かかる場合があります。

  この間、一部の機能は一時的に使用できなくなります。

  更新をトリガーする前にバックアップを実行し、アプライアンスを再起動しないことをお勧めします。再起動する必要がある場合、Intersight アプライアンスは自動的に動作します。

- **[インストール日時（Installation Date / Time）]**：更新がスケジュールされている日時が表示されます。鉛筆アイコンをクリックして、インストール日時を編集できます。
- **リリース ノート**：保留中のソフトウェア アップデートのリリース ノートへのリンク

[ソフトウェア（Software）] ページには、**[更新履歴（Update History）]** の下にアプライアンス ソフトウェア アップデートのテーブル ビューも表示されます。次の表に、インストールの日付、アプライアンス ソフトウェアのバージョン、ソフトウェア バージョンの説明、および更新のインストールのステータスを示します。このテーブル ビューから、特定のバージョンのソフトウェアと、インストールされた日付、およびインストールのステータスを検索できます。

ステップ 3　ソフトウェアアップデートを設定するには、**[設定の更新（Update Settings）]** をクリックします。

ステップ 4　**[設定の更新（Update Settings）]** ページで、自動モードまたは手動モードのいずれかを選択して、設定の更新モードを選択します。

自動モードの場合：

1. 更新の**自動**モードを選択します。
2. インストール スケジュールに **[システム デフォルト（System Default）]** と **[カスタム（Custom）]** を選択します。**[システム デフォルト（System Default）]** を選択すると、Intersight は猶予期間に従って更新をインストールします。**[カスタム（Custom）]** を選択すると、更新の繰り返しとインストール時間を定義できます。選択したインストール スケジュールに基づいて、更新が利用可能になると、アプライアンスが自動的に更新されます。
3. **ブラックアウトの日付**を有効にし、更新ブラックアウトの**ブラックアウトの開始日**と**ブラックアウトの終了日**を指定し、**[保存 (Save)]** をクリックします。**ブラックアウト期間は、システムによるアプライアンスの自動更新が禁止されています。**

   注目　アプライアンスが過去 90 日間に更新されていない場合、ブラックアウト期間を定義することはできません。ブラックアウト期間は、90 日を超えることはできません。

4. Intersightインテリジェンスを更新する戦略を選択します。詳細については、Intersight Connected Virtual Appliance の Intersight Intelligence の更新　（89 ページ）を参照してください。
5. **[保存（Save）]** をクリックします。

自動モードの場合：

1. **手動**モードの更新を選択します。

   Intersightインテリジェンスを更新する戦略を選択します。詳細については、Intersight Connected Virtual Appliance の Intersight Intelligence の更新 （89 ページ）を参照してください。

2. [保存（Save）] をクリックします。

3. アプライアンス UI から、**[設定（Settings）]** アイコン > **[設定 (Settings)]** > **[一般（General）]** > **[ソフトウェア (Software)]** に移動し、**[インストールの更新（Install Updates）]** をクリックします。

   [ソフトウェアをアップロード（Upload Software）] ページが表示されます。

4. ソフトウェア イメージの保存場所に応じて、[ローカル マシン（Local Machine）] または [ネットワーク共有（Network Share）] を選択します。

   1. **[ローカル マシン（Local Machine）]** オプションで、ソフトウェアをアップロードする場所を参照し、**[次へ（Next）]** をクリックします。

   2. **[ネットワーク共有（Network Share）]** オプションの場合は、プロトコルを入力し、ファイルのコピー元であるリモート サーバーの詳細を入力して、**[次へ（Next）]** をクリックします。

      - **[プロトコル（Protocol）]**：ファイル転送に使用される通信プロトコル。SCP（Secure Copy Protocol）および SFTP（Secure File Transfer Protocol）がサポートされています。
      - **[サーバ IP/ホスト名（Server IP/Hostname）]**：ファイルのコピー元のネットワーク共有サーバー
      - **[ポート（Port）]**：使用する TCP ポート
      - **[場所（Location）]**：コピーするファイルが保存されているディレクトリ
      - **[ファイル名（Filename）]**：ネットワーク共有からコピーするファイルの名前
      - **[ユーザ名（Username）]**：ネットワーク共有で認証するためのユーザー名
      - **[パスワード（Password）]**：ネットワーク共有で認証するためのパスワード

   3. すぐにインストールするか、または後で日時にインストールをスケジュールするかを選択します。

   4. **[適用（Apply）]** をクリックします。

1. **[要求（Requests）]** アイコンをクリックすると、アップロードの進行状況を追跡できます。

   アップロードが完了すると、**[ソフトウェア（Software）]** ページに**保留中の更新**の詳細が表示されます。**[保留中の更新の詳細（Pending Update Details）]** セクションでは、更新をキャンセルしたり、すぐに更新したり、インストール日時を編集したりできます。

   （注） 手動モードでは、保留中の更新をキャンセルした場合、更新を開始できるようにアプライアンスソフトウェアを再度アップロードする必要があります。

（注） 更新が失敗し、更新が回復可能な場合、**更新履歴**にはインストールが**[失敗（Failed）]**と表示され、既存の**[保留中の更新の詳細（Pending Update Details）]**はそのまま残ります。アップグレードプロセスを再試行できます。ソフトウェア更新エラーと考えられる解決策の詳細については、「Intersight 仮想アプライアンス ソフトウェア アップデートの不具合問題のトラブルシューティング」を参照してください。

更新が失敗し、更新が回復不能である場合、**更新履歴**にはインストールが**[失敗（Failed）]**と表示され、既存の**保留中の更新の詳細**は表示されません。ただし、既存のすべての機能と機能は、以前と同様に動作し続けます。ソフトウェア更新エラーと考えられる解決策の詳細については、「Intersight 仮想アプライアンス ソフトウェア アップデートの不具合問題のトラブルシューティング」を参照してください。

更新後、同じブラウザを使用してアプライアンスにログインすると、エラーコード *SEC_ERROR_REUSED_ISSUER_AND_SERIAL* が表示されることがあります。この問題を解決するには、アプライアンスへのログインに使用しているのと同じブラウザからサーバーのシステム生成証明書を削除する必要があります。たとえば、システムで生成されたサーバーの証明書をGoogle Chromeから削除するには、**[設定（Settings）]** > **[プライバシーとセキュリティ（Privacy and security）]** > **[証明書の管理（Manage certificate）]**に移動します。削除するシステム生成の証明書を選択し、**[削除（Remove）]**をクリックして、**[閉じる（Close）]**をクリックします。ブラウザを閉じ、新しいブラウザからアプリケーションにログインします。PFC の詳細については、証明書 （102 ページ） を参照してください。

Intersight プライベート仮想アプライアンス ソフトウェアの更新

Intersight プライベート仮想アプライアンスでは、実行中のバージョンよりも新しいバージョンにソフトウェアを手動で更新できます。ソフトウェアイメージを保存した場所に応じて、ローカル マシンまたはネットワーク共有サーバーからソフトウェア イメージをアップロードできます。ソフトウェアイメージがアップロードされたら、更新をすぐにインストールするか、またはインストールの日時をスケジュールするかを選択できます。

プライベート仮想アプライアンスを手動で更新するために必要なソフトウェア パッケージをアプライアンス ポータルからダウンロードできます。詳細については、ソフトウェア パッケージをダウンロードするためのアプライアンス アカウントの作成 （59 ページ）およびIntersight 仮想アプライアンスのソフトウェアパッケージのダウンロード （60 ページ）を参照してください。

（注）
- ソフトウェアのアップグレードはノード レベルではなくクラスタ レベルで行われるため、マルチノード アプライアンスでのソフトウェア アップグレードとシングル ノード アプライアンスでのソフトウェア アップグレードに違いはありません。

開始する前に：Intersightプライベート仮想アプライアンスをアップグレードするために必要なソフトウェア パッケージがアプライアンス アカウントからダウンロードされていることを確認します。プライベートアプライアンスアカウントの作成方法の詳細については、ソフトウェア パッケージをダウンロードするためのアプライアンス アカウントの作成 （59 ページ） を参照してください。

プライベート仮想アプライアンスのソフトウェアアップデートを設定するには、次の手順を使用します。

ステップ 1 アカウント管理者ロールを持つユーザーとして Intersight 仮想アプライアンスにログインします。

ステップ 2 **[サーバー セレクタ（Service Selector）]** ドロップダウン リストから **[システム（System）]** を選択し、**[設定（Settings）]** > **[一般（GENERAL）]** > **[ソフトウェア（Software）]** に移動します。 インストールされているソフトウェアに関する次の詳細が表示されます。

自動設定モードでは、次の詳細が表示されます。

- **稼働中のバージョン**：現在のソフトウェア バージョン番号
- **更新モード**：自動

保留中の更新に関する次の詳細が表示されます。

- **バージョン**：更新がスケジュールされているソフトウェア バージョンを示します。
- **更新の影響タイプ**：これは、**破壊的**、**破壊的な再起動**、または**なし**の可能性があります。この影響は、インフラストラクチャのアップグレードまたは他のサービスのアップグレードによって中断される可能性があります。中断のない更新によって、**更新の影響期間**に指定された期間に Intersight が使用できなくなる場合があります。アプライアンスの中断的な再起動は、カーネルの更新とサービスの再起動が原因で発生する可能性があります。更新の計画と管理を改善するために、猶予期間が提供されます。中断を伴う再起動がある場合、UI には適切なメッセージが表示されます。

  注目　アプライアンスの更新が完了するまでに約 90 分かかる場合があります。

  この間、一部の機能は一時的に使用できなくなります。

  更新をトリガーする前にバックアップを実行し、アプライアンスを再起動しないことをお勧めします。再起動する必要がある場合、Intersight アプライアンスは自動的に動作します。

- **[インストール日時（Installation Date / Time）]**：更新がスケジュールされている日時が表示されます。鉛筆アイコンをクリックして、インストール日時を編集できます。
- **リリース ノート**：保留中のソフトウェア アップデートのリリース ノートへのリンク

[ソフトウェア（Software）] ページには、**[更新履歴（Update History）]** の下にアプライアンス ソフトウェア アップデートのテーブル ビューも表示されます。次の表に、インストールの日付、アプライアンス ソフトウェアのバージョン、ソフトウェア バージョンの説明、および更新のインストールのステータスを示します。このテーブル ビューから、特定のバージョンのソフトウェアと、インストールされた日付、およびインストールのステータスを検索できます。

ステップ 3 **[更新のインストール（Install Update）]** をクリックします。

[ソフトウェアをアップロード（Upload Software）] ページが表示されます。

ステップ 4 **[設定の更新（Update Settings）]** ページで、自動モードまたは手動モードのいずれかを選択して、設定の更新モードを選択します。

自動モードの場合：

1. ソフトウェア イメージの保存場所に応じて、**[ローカル マシン（Local Machine）]** または **[ネットワーク共有（Network Share）]** を選択します。
    1. **[ローカル マシン（Local Machine）]** で、ソフトウェア イメージを保存した場所を参照し、**[次へ（Next）]** をクリックします。
    2. **[ネットワーク共有（Network Share）]** オプションの場合は、プロトコルを入力し、ファイルのコピー元であるリモートサーバーの詳細を入力します。
        - **[プロトコル（Protocol）]**：ファイル転送に使用される通信プロトコル。SCP（Secure Copy Protocol）および SFTP（Secure File Transfer Protocol）がサポートされています。
        - **[サーバ IP/ホスト名（Server IP/Hostname）]**：ファイルのコピー元のネットワーク共有サーバー
        - **[ポート（Port）]**：使用する TCP ポート
        - **[場所（Location）]**：コピーするファイルが保存されているディレクトリ
        - **[ファイル名（Filename）]**：ネットワーク共有からコピーするファイルの名前
        - **[ユーザ名（Username）]**：ネットワーク共有で認証するためのユーザー名
        - **[パスワード（Password）]**：ネットワーク共有で認証するためのパスワード
    3. すぐにインストールするか、または後で日時にインストールをスケジュールするかを選択します。
    4. **[適用（Apply）]** をクリックします。

[要求（Requests）] アイコンをクリックすると、アップロードの進行状況を追跡できます。

アップロードが完了すると、**[ソフトウェア（Software）]** ページに**保留中の更新**の詳細が表示されます。**[保留中の更新の詳細（Pending Update Details）]** セクションでは、更新をキャンセルしたり、すぐに更新したり、インストール日時を編集したりできます。

（注） 保留中の更新をキャンセルした場合は、更新を開始できるようにアプライアンス ソフトウェアを再度アップロードする必要があります。

（注） 更新が失敗し、更新が回復可能な場合、**更新履歴**にはインストールが**[失敗（Failed）]**と表示され、既存の**[保留中の更新の詳細（Pending Update Details）]**はそのまま残ります。アップグレードプロセスを再試行できます。ソフトウェア更新エラーと考えられる解決策の詳細については、「Intersight 仮想アプライアンス ソフトウェア アップデートの不具合問題のトラブルシューティング」を参照してください。

更新が失敗し、更新が回復不能である場合、**更新履歴**にはインストールが**[失敗（Failed）]**と表示され、既存の**保留中の更新の詳細**は表示されません。ただし、既存のすべての機能と機能は、以前と同様に動作し続けます。ソフトウェア更新エラーと考えられる解決策の詳細については、「Intersight 仮想アプライアンス ソフトウェア アップデートの不具合問題のトラブルシューティング」を参照してください。

更新後、同じブラウザを使用してアプライアンスにログインすると、エラーコード *SEC_ERROR_REUSED_ISSUER_AND_SERIAL* が表示されることがあります。この問題を解決するには、アプライアンスへのログインに使用しているのと同じブラウザからサーバーのシステム生成証明書を削除する必要があります。たとえば、システムで生成されたサーバーの証明書をGoogle Chromeから削除するには、**[設定（Settings）]** > **[プライバシーとセキュリティ（Privacy and security）]** > **[証明書の管理（Manage certificate）]**に移動します。削除するシステム生成の証明書を選択し、**[削除（Remove）]**をクリックして、**[閉じる（Close）]**をクリックします。ブラウザを閉じ、新しいブラウザからアプリケーションにログインします。PFC の詳細については、証明書 （102 ページ） を参照してください。

Intersight Assist ソフトウェアの更新

Cisco Intersight Assist ソフトウェアは、アップグレードサービスによって新しいバージョンが使用可能になると、Intersight クラウドから自動的にアップグレードされます。90 日以上使用可能な新しいアップグレードがない場合は、Intersight Assist が intersight に接続されていることを確認します。Intersight Assist は、クラウドから直接自動的にアップグレードして、サービスパッケージ、カーネルなどのセキュリティ修正を含む OS パッケージを更新できます。アプライアンス UI には、アップグレードの影響やサービスの中断など、アップグレードに関するガイダンスが記載されています。毎週のメンテナンスウィンドウ中に更新が利用可能になったら、更新が自動的に実行されるようにスケジュールできます。

ソフトウェア アップグレード スケジュールを設定するには、次の手順を実行します。

始める前に

Cisco Intersight Assist が Intersight に接続されていることを確認します。

ステップ 1 アカウント管理者ロールを持つユーザーとして Intersight Assist にログインします。

ステップ 2 **[サーバー セレクタ（Service Selector）]** ドロップダウン リストから **[システム（System）]** を選択し、**[設定（Settings）]** > **[一般（GENERAL）]** > **[ソフトウェア（Software）]** に移動します。 インストールされているソフトウェアに関する次の詳細が表示されます。

[新規バージョン (New Version)] セクション:

- **[バージョン (Version)]**：使用可能なソフトウェア バージョン番号。
- **アップグレードの影響タイプ**：これは、**破壊的**、**破壊的な再起動**、または**なし**の可能性があります。この影響は、インフラストラクチャのアップグレードまたは他のサービスのアップグレードによって中断される可能性があります。中断のない更新によって、**アップグレードの影響期間**に指定された期間に Intersight が使用できなくなる場合があります。アプライアンスの中断を伴う再起動は、オペレーティング システムまたはその他のコンポーネントの変更による更新が原因で発生する可能性があります。アップグレードの計画と管理を改善するために、猶予期間が提供されます。中断を伴う再起動がある場合、UI には適切なメッセージが表示されます。

  注目　Assist のアップグレードが完了するまでに最大で 90 分かかる場合があります。

  この間、一部の機能は一時的に使用できなくなります。

  アップグレードをトリガーする前にバックアップを実行し、アプライアンスを再起動しないことをお勧めします。アプライアンスのアップグレード中は、アプライアンスを手動で再起動しないでください。再起動する必要がある場合、Intersight Assist は自動的に再起動します。

- **[インストールをオンにするようにスケジュール (Install To Install On)]**：：新しいバージョンがインストールされる予定の日付と時刻。アップグレードがトリガーされると、経過表示バーに更新のステータスが表示されます。
- **[機能 (features)]** セクション：新しいソフトウェア バージョンの一部である機能、拡張、および不具合の修正を一覧表示します。

アップグレード スケジュールの設定に応じて、スケジュールされたインストール時間の自動アップグレードを待機するか、**[今すぐインストール (Install Now)]** をクリックして新しいバージョンをすぐにインストールします。

（注） 新しいソフトウェアバージョンには、7 日以内にアップグレードする必要があります。アップグレードしない場合、Intersight Assist が自動的にアップグレードサービスを完了します。

現在インストールされているソフトウェアに関する次の詳細が表示されます。

- **[バージョン (Version)]**：現在インストールされているアプライアンス ソフトウェアのバージョン。
- **[スケジュール (Schedule)]**：次のアップグレード ステータスのいずれかが表示されます。
  - [自動 (automatic)]：自動更新を選択し、スケジューラが設定されていない場合
  - 特定の更新時間がスケジュールされている場合は、日付と時刻
  - [**スケジュール**（**Schedule**）] フィールドの鉛筆アイコンをクリックして、次の詳細を指定します。
    1. 更新戦略を選択して、アプライアンスを更新します。**[自動 (Automatic)]** または **[毎週のメンテナンス (Weekly Maintenance)]** を選択します。**[自動 (Automatic)]** オプションを選択すると、更新が利用可能になったときにアプライアンスが自動的に更新されます。アップグレードサービスがこの間隔内で保留中の更新を検出し、猶予期間が有効期限切れになった場合、アップグレードが自動的にトリガーされます。**[設定 (Settings)]** > **[ソフトウェア (Software)]** からアップグレードの詳細を表示できます。

2. [**Weekly Maintenance Window**] オプションを選択した場合は、次の**週の曜日と時刻**を選択して、アップグレードプロセスを開始します。スケジュールは、設定された曜日のその時刻からその日の終了時点までの間隔です。アップグレードは、スケジュールで選択されている特定の時刻と曜日に基づいてトリガーされます。毎週のメンテナンス オプションは、更新が利用可能な場合にのみアップグレードされます。

3. Intersightインテリジェンスを更新する戦略を選択します。[**Intersight Intelligence をすぐに更新（Update Intersight Intelligence Immediately）**] オプションはデフォルトで有効になっています。これにより、アプライアンスソフトウェアのアップグレードスケジュールに関係なく、ハードウェア互換性リスト（HCL）などのIntersightインテリジェンスが利用可能になり次第、すぐに更新できます。詳細については、「Intersight Connected Virtual Appliance の Intersight Intelligence の更新 （89 ページ）」を参照してください。

- **[更新履歴 (Update History)]**：アプライアンスのソフトウェア更新のテーブル ビュー。次の表に、**インストールの日付**、アプライアンス ソフトウェアの**バージョン**、ソフトウェア バージョンの**説明**、および更新のインストールの**ステータス**を示します。このテーブル ビューから、特定のバージョンのソフトウェアと、インストールされた日付、およびインストールのステータスを検索できます。

（注） アップグレードが失敗し、アップグレードが回復可能な場合、[**今すぐインストール（Install Now）**] ボタンは有効のままです。アップグレードプロセスを再試行できます。ソフトウェア更新エラーと考えられる解決策の詳細については、「Intersight 仮想アプライアンス ソフトウェア アップデートの不具合問題のトラブルシューティング」を参照してください。

アップグレードが失敗し、アップグレードが回復不可能な場合、[**今すぐインストール（Install Now）**] ボタンは無効になります。ただし、既存のすべての機能と機能は、以前と同様に動作し続けます。ソフトウェア更新エラーと考えられる解決策の詳細については、「Intersight 仮想アプライアンス ソフトウェア アップデートの不具合問題のトラブルシューティング」を参照してください。

アップグレード後、同じブラウザを使用してアプライアンスにログインすると、エラーコード *SEC_ERROR_REUSED_ISSUER_AND_SERIAL* が表示されることがあります。この問題を解決するには、アプライアンスへのログインに使用しているのと同じブラウザからサーバーのシステム生成証明書を削除する必要があります。たとえば、システムで生成されたサーバーの証明書をGoogle Chromeから削除するには、**[設定（Settings）]** > **[プライバシーとセキュリティ（Privacy and security）]** > **[証明書の管理（Manage certificate）]** に移動します。削除するシステム生成の証明書を選択し、**[削除（Remove）]** をクリックして、**[閉じる（Close）]** をクリックします。ブラウザを閉じ、新しいブラウザからアプリケーションにログインします。PFC の詳細については、証明書 （102 ページ） を参照してください。

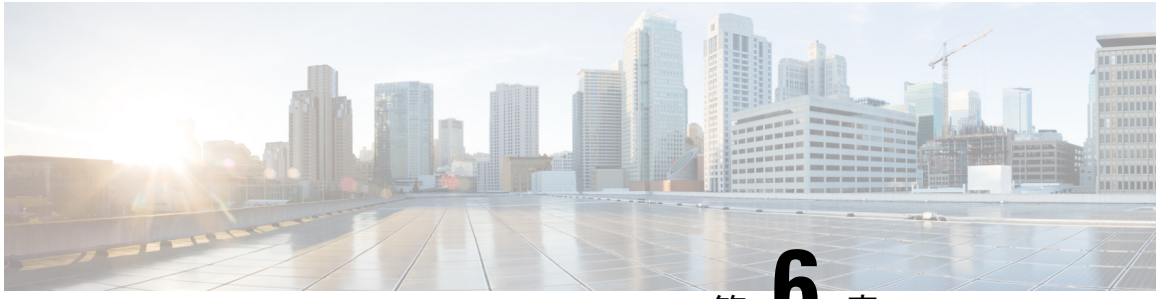
Intersight 仮想アプライアンス ソフトウェア アップデートの不具合問題のトラブルシューティング

次の表に、アプライアンスの更新中に発生する可能性のあるエラー メッセージの一部と、それぞれの考えられる解決策を示します。時間が経っても問題が解消しない場合は、Cisco TACにお問い合わせください。

表 *8*: アプライアンス ソフトウェア アップデートの失敗に関する問題

エラー メッセージ	考えられる解決策
ディスク サイズが最小要件を満たしていません。	アプライアンスのハードウェア ディスク領域が、アップグレードを正常に実行するのに十分ではありません。「新規の Intersight 仮想アプライアンスの VM 情報技術要件」セクションの情報を参照し、要件を満たすようにハードウェアを更新します。
アプライアンスは現在、バージョン *CURRENTVERSION*で実行されています。バージョン *PENDINGVERSION* にアップグレードする前に、バージョン *INTERMEDIATEVERSION*に手動でアップグレードする必要があります。 （注） *CURRENTVERSION*、*INTERMEDIATEVERSION*、および *PENDINGVERSION* は変数であり、ここではプレースホルダテキストとして機能します。表示されたエラー メッセージに示されているバージョンに従います。	お使いのアプライアンス バージョンは、保留中のアップグレード バージョンへの直接アップグレードをサポートしていません。保留中のバージョンにアップグレードする前に、エラー メッセージにリストされている中間バージョンへの手動アップグレードをトリガします。
アプライアンスには、AVX 命令セットをサポートする CPU が必要です。	アプライアンスに使用されている CPU は AVX をサポートしていません。ハードウェアをアップグレードし、AVX をサポートする CPU を使用します。

エラー メッセージ	考えられる解決策
AlmaLinux を実行しているアプライアンスにアップグレードするには、アプライアンスバージョン *INTERMEDIATEVERSION* 以降のバージョンからアップグレードする必要があります。 （注） *INTERMEDIATEVERSION* は変数であり、ここでプレースホルダテキストとして機能します。表示されたエラーメッセージに示されているバージョンに従います。	お使いのアプライアンス バージョンは、保留中のアップグレード バージョンへの直接アップグレードをサポートしていません。保留中のバージョンにアップグレードする前に、エラー メッセージにリストされている中間バージョンへの手動アップグレードをトリガします。
アプライアンスのストレージ デバイスは、VirtIOドライバのみを使用する必要があります。	KVM でアプライアンスを実行している場合は、ストレージに VirtIO ドライバのみを使用していることを確認します。



第 6 章

ダッシュボードの設定

Intersight 仮想アプライアンス設定

Intersight 仮想アプライアンス**[設定（Settings）]**ページでは、アプライアンス ステータスの監視、データのバックアップと復元、アプライアンス ソフトウェアのアップグレード、ネットワーク設定の構成、ユーザーとグループの追加などを行うことができます。

設定オプション	説明
[一般 (GENERAL)] > **[アカウントの詳細 (Account Details)]**	アカウント名、アカウントID、アクセス リンク、ライセンス タイプ、デフォルトのアイドル タイムアウト、ユーザーあたりの同時セッションの最大数、デフォルトのセッション タイムアウトなどのアカウントの詳細を表示します。 デフォルトのアイドルタイムアウト、デフォルトのセッションタイムアウト、およびユーザーあたりの同時セッションの最大数などのアカウント設定も設定できます。詳細については、アカウント設定の構成 （92 ページ）を参照してください。
[一般 (GENERAL)] > **[アクセスの詳細 (Access Details)]**	名前、アカウント名、電子メールID、ロール、アイドルタイムアウト、セッションタイムアウト、ユーザーあたりの最大同時セッション数、ログイン時間、ロールの簡単な説明、ユーザーとその権限のテーブルビューなど、ユーザーの詳細を表示します。このページの下部ペインに表示されます。
[一般 (GENERAL)] > **[アプライアンス (Appliance)]**	アプライアンス接続のステータスを表示し、アプライアンスの健全性、ホスト名、バージョン番号、展開サイズ、データ収集ポリシーを表示します。接続されたノードのリストには、接続されたノードの IP アドレス、ステータス、ゲートウェイ、およびネットマスクが表示されます。接続されたノード上のアラームを表示することもできます。

設定オプション	説明
[一般（GENERAL）] > [バックアップ（Backup）]	アプライアンスのバックアップを完全な状態で作成し、リモート サーバー上にイメージを保存します。このページからバックアップをスケジュールすることもできます。詳細な手順については、「バックアップの作成」と「バックアップのスケジュール作成」を参照してください。 アプライアンス構成は、Intersight 接続型仮想アプライアンスのリカバリ （50 ページ） と Intersight プライベート仮想アプライアンスのリカバリ （52 ページ）の手順を使用してバックアップ ファイルからリカバリできます。
[一般（GENERAL）] > [バナー メッセージ（Banner Message）]	バナーメッセージの設定の詳細を表示します。有効にすると、設定されたバナー メッセージがユーザーログイン画面の前に表示されます。詳細については、ログイン画面の前に表示するバナーメッセージの設定 （93 ページ） を参照してください。
[一般（GENERAL）] > [ソフトウェア（Software）]	アプライアンスの現在のソフトウェアバージョンの詳細を表示します。これには、バージョン番号、インストールされたコンポーネント、インストールに関するメッセージ、およびインストールされたソフトウェアのフィンガープリントも含まれます。 Intersight 仮想アプライアンス ソフトウェアの更新の詳細については、「Intersight 接続型仮想アプライアンス ソフトウェアの更新」を参照してください。
[一般（General）] > [デバイス コネクタ（Device Connector）]	（注） この設定は、接続型仮想アプライアンスの展開にのみ適用されます。 Intersight へのアプライアンス接続のステータス、アクセスモード、デバイスID、および要求コードを表示します。[デバイス コネクタ (Device Connector)] ウィンドウの **[設定 (Settings)]** メニューから **HTTPS プロキシ**を追加できます。詳細については、Intersight 接続型仮想アプライアンスのネットワーク接続 （91 ページ） を参照してください。

設定オプション	説明
[ネットワーク（NETWORKING）] > [DNS]	DNS 設定構成し、IPv4 DNS サーバー アドレスと DNS サーバーの代替 IPv4 アドレスを追加します。詳細については、DNS の設定 （93 ページ） を参照してください。
[ネットワー キング（NETWORKING）] > [NTP]	NTP サーバーを設定し、既存の NTP サーバー設定を編集します。詳細については、NTP の設定 （94 ページ） を参照してください。
[ネットワーキング（NETWORKING）] > [外部 Syslog（External Syslog）]	外部 syslog サーバーへの監査ログとアラーム情報の送信の有効化と無効化を含む、外部 syslog 設定を設定します。詳細については、外部 Syslog の設定 （95 ページ） を参照してください。
[認証（AUTHENTICATION）] > [LDAP/AD]	LDAP サーバー、DNS パラメータ、構築メソッド、検索パラメータ、グループ認証の設定を作成し、構成します。詳細については、LDAP の設定 （100 ページ） を参照してください。
[認証（AUTHENTICATION）] > [シングル サインオン（Single Sign-On）]	シングルサインオン（SSO）認証をセットアップします。SSO では、1 つのクレデンシャル セットを使用して複数のアプリケーションにログインできます。SSO 認証では、Cisco ID の代わりに企業のクレデンシャルを使用して Intersight にログインできます。Intersight でのシングル サインオンの詳細については、Intersight 仮想アプライアンスでのシングル サインオン （101 ページ） を参照してください。
[認証 (AUTHENTICATION)] > [証明書 (Certificates)]	信頼できる証明書を追加して LDAP または HTTPS サーバーとの TLS 通信を確認します。証明書署名要求または自己署名証明書を生成できます。詳細については、証明書 （102 ページ） を参照してください。
[認証（AUTHENTICATION）] > [ローカル ユーザー（Local Users）]	現在のパスワード ポリシー設定の詳細を表示するか、新しいパスワード ポリシーを設定します。詳細については、ローカル ユーザー向けパスワード ポリシーの設定 （106 ページ） を参照してください。

設定オプション	説明
[アクセスおよび権限 (ACCESS & PERMISSIONS)] > [ユーザー（Users)]	ユーザを表示または新規ユーザーを追加し、電子メールを使用した Intersight へのアクセスを許可し、ID プロバイダーと権限の設定を指定します。詳細については、ユーザーの追加（109 ページ） を参照してください。
[アクセスおよび権限（ACCESS & PERMISSIONS）] > [グループ（Groups）]	ユーザー **グループ**を表示するか、またはシングル サインオンまたは LDAP ベースの認証の新しいグループを追加します。詳細については、グループの追加 （111 ページ） を参照してください。
[アクセスおよび権限 (ACCESS & PERMISSIONS)] > [ロール (Roles)]	既存のロールを表示するか、またはカスタム ロールを作成して権限を割り当てます。詳細については、「ロールの追加」を参照してください。
[アクセスおよび権限 (ACCESS & PERMISSIONS)] > [組織 (Organizations)]	組織のリストを表示するか、または新しい組織を作成して、論理リソースと物理リソースへのアクセスを管理します。詳細については、「組織の追加」を参照してください
[API] > [API キー（API Keys）]	アカウント内の既存の API キーのリストを表示するか、または新しい API キーを生成します。詳細については、「API キー」を参照してください。
OAuth2 トークン	OAuth2 トークンのリストと、アプリケーションと関連付けられたデバイスの詳細を表示します。

Intersight 仮想アプライアンスのモニタリング

Intersight 仮想アプライアンスには、アプライアンスの概要と健全性ステータスが示され、事前に定義した制限値を超過するか、またはしきい値が発生した場合はアラームが表示されます。

[アプライアンス（Appliance）]：の下の次の詳細を表示するには、アプライアンス UI で、**[サービス セレクタ（Service Selector）]** ドロップダウン リストから **[システム（System）]** を選択し、**[設定（Settings）] > [一般 （General）] > [アプライアンス（Appliance）]**に移動します。

- **[健全性 (Health)]**：アプライアンスの全体的なステータス
- **[ホスト名（Hostname）]**：FQDN またはホスト名

- **[バージョン（Version）]**：インストールされているアプライアンス ソフトウェアのバージョン
- **[展開サイズ（Deployment Size）]**：アプライアンスの展開サイズ。展開サイジングについては、以下を参照してください。 Intersight 仮想アプライアンスでサポートされる構成の制限 （89 ページ）
- **[ノード（Node）]**：Cisco Intersight 仮想アプライアンスのアプライアンス ノードのリストのテーブル ビュー。IP アドレス、運用ステータス、ゲートウェイ、またはネットワーク別に特定のノードを検索できます。仮想アプライアンスのアプライアンスノードのリスト右側のペインでアラームを表示し、それらのアラームを重大度でフィルタリングすることができます。

Intersight 仮想アプライアンスは特定のクリティカルなパラメータを監視して、事前に定義した制限値を超過するか、またはしきい値が発生した場合にアラームを発生させます。現時点では、アプライアンスはシステム レベルとノード -レベルのアラームを報告します。次の表に、アラームのレベルとそれらの説明を示します。

表 *9 : Intersight* 仮想アプライアンスのアラーム

レベル	コンポーネント	説明	コメント
システム	ノード	ノードがダウンしています	ノードごとに 1 つのアラーム
システム	ノード	ノードはサービスを展開する準備が整っていません	ノードごとに 1 つのアラーム
ノード	CPU 使用率	CPU使用率がしきい値を超過しています	ノードごとに 1 つのアラーム。しきい値：75%
ノード	メモリ使用率	メモリ使用率がしきい値を超過しています	ノードごとに 1 つのアラーム。しきい値：75%
ノード	ファイル システムのディスク使用率	ファイル システムのディスク使用率がしきい値を超過しています	ファイルシステムごとに 1 つのアラーム。しきい値：75%
システム	実行中のサービスインスタンスの数	実行中のサービスインスタンスの数は予想を下回っています	任意のサービスダウンに対して 1 つのアラーム
システム	準備が整っているサービスインスタンスの数	準備が整っているサービスインスタンスの数が予想を下回っています	任意のサービスダウンに対して 1 つのアラーム

レベル	コンポーネント	説明	コメント
システム	Web 証明書	警告: Web 証明書が 120 日以内に期限切れになります 重大: Web 証明書が 90 日以内に期限切れになります	アプライアンスごとに 1 つのアラーム
システム	デバイス証明書	警告: デバイス証明書が 120 日以内に期限切れになります 重大: デバイス証明書が 90 日以内に期限切れになります	アプライアンスごとに 1 つのアラーム
システム	[Appliance Backup]	警告：過去 1 週間以内に Intersight アプライアンスのバックアップが作成されていません。新しいバックアップをスケジュールするか、作成してください。	アプライアンスごとに 1 つのアラーム
システム	[Appliance Backup]	[重大（Critical）]：最新の Intersight アプライアンスのバックアップに失敗しました。別のバックアップをスケジュールするか、作成してください。	アプライアンスごとに 1 つのアラーム

レベル	コンポーネント	説明	コメント
システム	クラウド接続	警告：Intersight クラウドへの接続が 30 日以上ダウンしています 重大：Intersight クラウドへの接続が 60 日以上ダウンしている 非常に重大：Intersight クラウドへの接続が90日以上ダウンしています。接続が復元されるまで、新しいデバイスの要求は許可されません。	アプライアンスごとに 1 つのアラーム
ノード	ネットワーク リンク接続	警告: クラスタノード間の遅延が 10 ミリ秒を超えています	リンクごと、ノードごとに 1 つのアラーム

（注） 電源やファンの障害などの Cisco UCS C シリーズ サーバー関連の障害は、Intersight 仮想アプライアンスによって外部の syslog サーバに転送されません。UCS C シリーズのイベントと障害の転送を処理するには、UCS C シリーズ CIMC 側で外部 syslog サーバーを設定してください。

データのバックアップ

Cisco Intersight 仮想アプライアンスの定期的なバックアップは不可欠です。定期的にバックアップをしないと、構成の設定を再構築したり、プロファイルやポリシーを再作成するための自動的な手段はありません。データが損失または破損した場合に、スケジュールされたバックアップを使用して一日 1 回定期バックアップを実行するか、オンデマンドでバックアップを作成できます。Cisco Intersight 仮想アプライアンスを使用すると、アプライアンス内のデータの完全な状態のバックアップを取得し、リモートサーバーに保存できます。サイト全体の障害やその他のディザスタ リカバリの状況が発生した場合、復元機能により、バックアップしたシステム データからシステムを完全な状態で復元できます。

データをバックアップするには、次のオプションを使用できます。

- **[バックアップの作成 (Create Backup)]**: オンデマンドで Cisco Intersight 仮想アプライアンス データの完全な状態バックアップを作成し、バックアップしたデータをリモート サーバーに保存します。

- **[バックアップのスケジュール (Schedule Backup)]**: スケジュールに基づいてアプライアンス内のデータの完全な状態の定期バックアップをスケジュールし、バックアップされたデータをリモート サーバーに保存します。

（注） マルチノード アプライアンスで実行されているバックアップと単一ノード アプライアンスで実行されているバックアップに違いはありません。バックアップは、ノード レベルではなく、クラスタ レベルで実行されます。バックアップは1つのノードから発生しますが、バックアップの発生元のノードに制限はありません。

バックアップの作成

Intersight仮想アプライアンスの定期的なバックアップを完全な状態で作成し、バックアップしたファイルをリモートサーバーに保存することができます。バックアップを作成するには、次の手順を実行します。

ステップ 1 アカウント管理者ロールを持つユーザーとして Intersight 仮想アプライアンスにログインします。

ステップ 2 **[サーバー セレクタ（Service Selector）]** ドロップダウン リストから **[システム（System）]** を選択し、**[設定（Settings）]** > **[一般（GENERAL）]** > **[バックアップ（Backup）]** に移動します。

ステップ 3 **[バックアップの作成（Create Backup）]**をクリックします。

[バックアップ（Backup）] ウィンドウが表示されます。

ステップ 4 次の詳細を入力します。

- **[プロトコル（Protocol）]**：バックアップ プロセスで使用される通信プロトコルのオプション。現時点で Intersight 仮想アプライアンスがバックアップでサポートしているプロトコルは、CIFS（Common Internet File System）、SCP（Secure Copy Protocol）と SFTP（Secure File Transfer Protocol）です。バックアップ データを保存するリモート サーバーの詳細を入力します。
- **[リモート ホスト (Remote Host)]**：バックアップ ファイルを保存するためのリモート ホスト
- **[リモート ポート（Remote Port）]**：バックアップ サーバーのリモート TCP ポート（SCP と SFTP のみに適用可能）。
- **[リモート パス（Remote Path）]**：バックアップ ファイルを保存するディレクトリ。

  （注） CIFS 共有名には英数字のみを含める必要があり、*^(\w+)(/\w+)*/?$*などの正規表現に準拠している必要があります。スペースを含めることはできません。また、CIFS 共有の下のフォルダを指定する場合は、スラッシュ（/）を区切り文字として使用する必要があります。たとえば、*backupshare/Intersight/Daily* や *backupshare/Monthly*などです。

- **[ファイル名 (Filename)]**：復元するバックアップ ファイルの名前
- **[ユーザー名 (Username)]**：バックアップ サーバーでバックアップ クライアントを認証するためのユーザー名

- **[パスワード (Password)]**：バックアップ サーバーでバックアップ クライアントを認証するためのパスワード
- **[パスワードの確認 (Password Confirmation)]**：パスワードを再入力します

ステップ 5 **[バックアップの開始（Start Backup）]** をクリックします。

バックアップのスケジュール作成

バックアップのスケジュールを使用すると、アプライアンス間で定期的にデータをバックアップするようにスケジュールすることができます。アプライアンスでは、アプライアンス上でバックアップの 3 つのコピーをローカルに保存できます。

ステップ 1 アカウント管理者ロールを持つユーザーとして Intersight 仮想アプライアンスにログインします。

ステップ 2 **[サーバー セレクタ（Service Selector）]** ドロップダウン リストから **[システム（System）]** を選択し、**[設定（Settings）]** > **[一般（GENERAL）]** > **[バックアップ（Backup）]** に移動します。

ステップ 3 **[バックアップのスケジュール (Schedule backup)]** ウィンドウで、**[バックアップ スケジュールの使用 (Use backup Schedule)]** を有効にします。

このオプションを無効にする場合は、**[バックアップ スケジュールの使用 (Use Backup schedule)]** オプションを有効にしてバックアップをスケジュールする必要があります。

ステップ 4 **バックアップスケジュール**の作成を完了するには、次の詳細を入力します。

- **バックアップ スケジュール**
  - **[曜日 (day Of week)]**: データ バックアップをスケジュールする曜日を指定します。
  - **[時刻 (time Of day)]**: データ バックアップのスケジュールを設定する時刻を指定します。時刻はセッションのブラウザの時間に従い、その日の現地時刻が表示されます。
- **Backup Destination**
  - **[プロトコル（Protocol）]**：バックアップ プロセスで使用される通信プロトコル（CIFS/SCP/STFP）。
  - **[リモート ポート（Remote Port）]**：バックアップ サーバーのリモート TCP ポート（SCP と SFTP のみに適用可能）。
- **[リモート ホスト (Remote Host)]**：バックアップ ファイルを保存するためのリモート ホスト
- **[リモート パス (Remote Path)]**：バックアップ ファイルを保存するディレクトリ

（注） CIFS 共有名には英数字のみを含める必要があり、*^(\w+)(/\w+)*/?$*などの正規表現に準拠している必要があります。スペースを含めることはできません。また、CIFS 共有の下のフォルダを指定する場合は、スラッシュ（/）を区切り文字として使用する必要があります。たとえば、*backupshare/Intersight/Daily* や *backupshare/Monthly*などです。

- **[ファイル名 (Filename)]**：復元するバックアップ ファイルの名前
- **[ユーザー名 (Username)]**：バックアップ サーバーでバックアップ クライアントを認証するためのユーザー名
- **[パスワード (Password)]**：バックアップ サーバーでバックアップ クライアントを認証するためのパスワード
- [パスワードの確認（Password Confirmation）]：パスワードを再入力します
- **バックアップ保持（Backup Retention）**：保持するバックアップの数。

  [バックアップの保持を有効にする（**Enable Backups Retention**）] をクリックして、リモート サーバーに保持するバックアップの数を入力します。デフォルトは 15 です。1ー100 の数値を入力できます。

  （注） SCP プロトコルの使用中にバックアップ保持制限が適切に機能するには、リモート ホストでも SFTP プロトコルが有効になっていることを確認します。

  さまざまなバックアップ保持シナリオの詳細については、「バックアップ保持シナリオ」を参照してください。

ステップ 5 **[バックアップのスケジュール（Schedule Backup）]** をクリックしてプロセスを完了します。

バックアップの保持シナリオ

次の表に、さまざまなバックアップ保持シナリオと予想される結果を示します。

表 *10*：バックアップの保持シナリオ

バックアップの保持シナリオ	達成する
バックアップ保持を有効にし、バックアップの蓄積を許可してから、バックアップ保持を無効にします。	保持ポリシーに基づいて作成されたバックアップは削除されません。
バックアップ保持を有効にし、バックアップの蓄積を許可してから、バックアップ保持を無効にします。ここで、バックアップ保持を再度有効にします。	保持が最初に有効になっているときに作成されたバックアップは影響を受けません。保持が再度有効になった後に作成されたバックアップのみが保持ポリシーの一部になります。
保持ポリシーでファイルパスまたはホスト名を変更します。	変更前に作成されたバックアップは影響を受けません。ポリシーの変更後に作成されたバックアップのみが、最新の保持ポリシーの一部になります。
バックアップの数を増やす	バックアップは、バックアップの最大数に達するまで保持ポリシーの一部として蓄積され続け、最も古いバックアップが削除されます。

バックアップの保持シナリオ	達成する
バックアップの最大数を X から Y に減らします。	元の保持ポリシーの古いバックアップは、ポリシーの一部ではなくなります。これは、保持ポリシーが番号 Y の最新のバックアップにのみ実装されることを意味します。それ以前のバックアップはそのまま残ります。 例：保持カウントが 5 で、保持カウントを 3 に減らしたとします。この場合、元の保持ポリシーの最も古い 2 つのバックアップは影響を受けません。保持ポリシーは、3つのバックアップでのみ有効になります。

メトリック収集の設定

Intersight 仮想アプライアンス内のメトリック収集は、デフォルトで無効になっています。Intersight仮想アプライアンスをインストールまたはアップグレードした後、メトリック収集を開始するには、**[メトリック（Metrics ）]** ページの Intersight 仮想アプライアンスでメトリック収集を有効にする必要があります。

さらに、**[メトリック（Metrics）]** ページには、Intersight 仮想アプライアンスのしきい値制限とともにアクティブなサーバー数が表示されます。

（注） メトリック収集は、個々のデバイスではなく、Intersight仮想アプライアンス全体に対して有効または無効にできます。

メトリック収集を有効または無効にするには、次の手順を実行します。

1. アカウント管理者ロールを持つユーザーとして **Intersight 仮想アプライアンス**にログインします。
2. **[サーバー セレクタ（Service Selector）]** ドロップダウン リストから **[システム（System）]** を選択し、**[設定（Settings）] > [一般（GENERAL）] > [メトリックス（Metrics）]** に移動します。
3. [構成（Configure）] をクリックします。
4. **[メトリックの有効化（Enable Metrics）]** スライダを使用して、メトリック収集を有効または無効にします。

（注）
- メトリック収集を有効にすると、エンドポイントからのメトリック収集が即時にトリガーされます。
- メトリック収集を無効にすると、設定の変更が完了し、メトリックの収集が停止するまでに最大 1 時間の遅延が発生する可能性があります。

5. [設定（Configure）] をクリックします。

Intersight Connected Virtual Appliance の Intersight Intelligence の更新

Intersight Connected Virtual Applianceでは、アプライアンスソフトウェアのアップグレードスケジュールに関係なく、ハードウェア互換性リスト（HCL）などのIntersightインテリジェンスが利用可能になり次第、それを更新できます。HCLの更新には、サーバーモデル、プロセッサ、ファームウェア、アダプタ、オペレーティングシステム、およびドライバの互換性検証結果とコンプライアンスステータスが含まれます。HCL の詳細については、ハードウェア互換性リスト(HCL)への準拠を参照してください。

Intersightインテリジェンスを更新するには、次の手順を使用します。

ステップ 1 アカウント管理者ロールを持つユーザーとして Intersight 仮想アプライアンスにログインします。

ステップ 2 **[サーバー セレクタ（Service Selector）]** ドロップダウン リストから **[システム（System）]** を選択し、**[設定（Settings）]** > **[一般（GENERAL）]** > **[ソフトウェア（Software）]** に移動します。

ステップ 3 **[スケジュール（Schedule）]** フィールドの鉛筆アイコンをクリックします。

[更新スケジュールの設定（Set Update Schedule）] ウィンドウが表示されます。

ステップ 4 **[Intersight インテリジェンスの即時更新（Update Intersight Intelligence Immediately）]** を選択し、**[保存（Save）]** をクリックします。

Intersight 仮想アプライアンスでサポートされる構成の制限

Cisco Intersight 仮想アプライアンスは、環境のスケーリング要件をサポートするために、複数の展開サイズで使用できます。次のようにアプライアンスを展開できます。

新規展開：Intersight 仮想アプライアンスは、中規模または大規模の構成で展開できます。サイズを選択する前に、リソース要件を評価し、Intersight アプライアンス メンテナンス シェルで

適切なオプションを選択して、展開する必要があるサイズを選択します。選択したサイズは、アプライアンス VM の再起動時に展開されます。情報技術要件の詳細については、新規の Intersight 仮想アプライアンスの VM 情報技術要件を参照してください。

次の表は、サポートされている構成の制限をリストします：

表 *11* : 新しい *Intersight* 仮想アプライアンスでサポートされる構成の制限

品目	設定の制限値		
	Small（既存の展開でのみサポート）	**中規模**	**大規模**
サーバー数	2000	5000	8,000
Intersight 管理モード（IMM）ドメイン（FI）の数	4	最大 32	64
Intersight 管理モード（IMM）サーバーの数	170（小規模な展開ではメトリック収集はサポートされません）	500（メトリック収集が有効な場合）	2000（メトリック収集が有効な場合）
		5000（メトリック収集が無効な場合）	8000（メトリック収集が無効な場合）
UCSM 管理モード（UMM）ドメインの数	30	500	800
UCSM 管理モード（UMM）サーバーの数	330	最大 5000	8,000
スタンドアロンのラック サーバーの数	1500	5000	8,000
パラレル HyperFlex インストールの数	2	5	5
サポートされている同時動作の数	50	100	100
同時ユーザーセッション（GUI および API）の数	32	32	32

Intersight 接続型仮想アプライアンスのネットワーク接続

Cisco Intersight 接続型仮想アプライアンスは、組み込みデバイスコネクタを介して Cisco Intersight に接続します。デバイスコネクタは、接続されているターゲットに対して、セキュアなインターネット接続を使用して情報を送信し、Cisco Intersight から制御命令を受信できる安全な方法を提供します。クラウドへの接続に関する次の詳細を表示するとともに、**[デバイス コネクタ（Device Connector）]** ページから設定を構成できます。

1. アプライアンス UI で、**[サービス セレクタ（Service Selector）]** ドロップダウン リストから **[システム（System）]** を選択し、**[設定（Settings）]** > **[一般 （General）]** > **[デバイス コネクタ（Device Connector）]**に移動します。**[デバイス コネクタ（Device Connector）]** ウィンドウが表示されます。

   デバイス ID、要求コード、アクセス モード、デバイス コネクタ ステータスなどの詳細を表示できます。デバイス コネクタ、ステータス、およびエラー条件の設定の詳細については、**リソース**の「**デバイス コネクタの設定**」を参照してください。

2. **[設定（Settings）]** をクリックし、次の設定を行います。

   - **[一般（General）]**：**デバイス コネクタ**を有効にして、アプライアンスを要求し、Cisco Intersight の機能を活用し、アクセスモードを選択できるようにします。デバイス コネクタのオプションが無効になっている場合は、Cisco Intersight への通信は許可されません。**[保存（Save）]** をクリックします。
   - **プロキシ設定**
     - **[プロキシの有効化（Enable Proxy）]** を有効にします。**プロキシ ホスト名**または **IP アドレス**と**プロキシ ポート**を追加します。プロキシ ポートは、1 ～ 65535 の範囲にする必要があります。
     - **認証**を有効にし、認証されたプロキシのユーザー名とパスワードを追加します。プロキシ設定は復元後に自動的にリセットされるため、手動でアプライアンスプロキシをリセットする必要があります。

       [**保存（Save）]** をクリックします。
   - **Certificate Manager**：プロキシ証明書をインポートします。

Intersight への接続に基づくアラート

Intersight クラウドへの接続が中断され、90 日以内に接続が復元されない場合、ターゲットの要求機能は失われます。接続された TAC、ファームウェア アップグレード、HyperFlex クラスタの展開、および Intersight クラウドへの接続を必要とするユーザー フィードバックを含むアプライアンスの機能も、接続が復元されるまで影響を受ける可能性があります。接続を再確立すると、ターゲットの要求操作を再開し、その他のすべての機能を以前と同様に使用できます。

Intersightは、中断された接続の影響について警告するために、次のアラームと警告を発生させます。

- **[警告 (Warning)]**: 操作ステータスについて警告するためのアプライアンス UI が表示されます。これは、接続が失われてから 30-60 日の間に表示されます。この間、アプライアンスの通常の動作が中断されることはなく、ターゲットの要求と管理を続行できます。
- **[障害 (Fault)]**: 60-90 日と、接続の中断後 90 日の間にエラーが表示されます。90 日で接続が失われるまで、アプライアンスでのターゲットの要求と管理を続行できます。90 日後に接続が復元されない場合、ターゲットの要求はブロックされます。ターゲットを要求し、通常の操作を再開するには、接続を復元する必要があります。

アカウント設定の構成

このタスクでは、Intersight仮想アプライアンスでのアカウント設定の詳細について説明します。

ステップ 1 アカウント管理者ロールを持つユーザーとして Intersight 仮想アプライアンスにログインします。

ステップ 2 **[サービス セレクタ（Service Selector）]** ドロップダウン リストから **[システム（System）]** を選択し、**[設定（Settings）]** > **[一般（GENERAL）]** > **[アカウントの詳細（Account Details）]**に移動します。

既存のアカウント設定の詳細を表示できます。

ステップ 3 **[構成（Configure）]** をクリックします。

[アカウント設定の構成（Configure Account Settings）] ウィンドウが表示されます。

ステップ 4 必要に応じて、次のフィールドを更新します。

- **アカウント名**：アカウントの名前。
- **デフォルトのアイドルタイムアウト（秒）**：Webセッションのアイドルタイムアウト間隔（秒）を指定します。システムのデフォルト値は 18,000 秒（5 時間）です。
- **デフォルトのセッション タイムアウト（秒）**：セッションの有効期限を秒単位で指定します。システムのデフォルトは57,600（16時間）です。
- **ユーザあたりの最大同時セッション数（セッション）**：ユーザー1人あたりに許可される最大同時セッション数を指定します。システムのデフォルトおよび同時セッションの最大数は32です。
- **監査ログの保持期間(月)**：監査ログの保持期間を指定します。システムのデフォルトは48か月です。許可される範囲は 6 か月から 48 か月です。監査ログの削除タスクは、毎日午前 6:00 UTC に実行されるように設定されており、このフィールドで設定された保持期間を満たすすべての監査ログは、この時点で自動的に削除が開始されます。削除すると、監査ログを取得できなくなります。

ステップ 5 [保存（Save）] をクリックします。

ログイン画面の前に表示するバナーメッセージの設定

このタスクでは、Intersight仮想アプライアンスでバナーメッセージを設定する方法について説明します。有効にすると、設定されたバナーメッセージがユーザーログイン画面の前に表示されます。

ステップ 1 アカウント管理者ロールを持つユーザーとして Intersight 仮想アプライアンスにログインします。

ステップ 2 **[サーバー セレクタ（Service Selector）]** ドロップダウン リストから **[システム（System）]** を選択し、**[設定（Settings）]** > **[一般（GENERAL）][バナー メッセージ（Banner Message）]**に移動します。

ステップ 3 **[設定（Configure）]** をクリックします。

[バナー メッセージの設定（Configure Banner Message）]ウィンドウが表示されます。

ステップ 4 次のフィールドを更新します。

- **[ログイン前にバナー メッセージを表示する（Show banner message before login）]**—このオプションを有効にします。
- **[バナー タイトル（Banner Title）]** : バナー メッセージのタイトルを入力します。タイトルの長さは 128 文字を超えることはできません。
- **[バナー内容（Banner Content）]** : バナー メッセージの内容を入力します。このフィールドの内容は 2000 文字未満にする必要があります。

ステップ 5 **[保存（Save）]** をクリックします。

設定されたバナー メッセージの内容がタイトルとともに **[バナー メッセージ（Banner Message）]** プレビュー ウィンドウに表示されます。

DNS の設定

この手順では、Virtual Appliance 仮想アプライアンスで DNS 設定を構成/**編集**する手順を示します。

ステップ 1 アカウント管理者ロールを持つユーザーとして Cisco Intersight 仮想アプライアンスにログインします。

ステップ 2 **[サービス セレクタ（Service Selector）]** ドロップダウン リストから **[システム（System）]** を選択し、**[設定（Settings）]** > **[ネットワーキング（NETWORKING）]** > **DNS** に移動します。

既存の DNS 設定の表示の詳細。

ステップ 3 **[DNS の編集（Edit DNS）]** をクリックします。**[DNS の構成（Configure DNS）]** ウィンドウが表示されます。

ステップ 4 次のプロパティを更新します。

- **[優先 IPV4 DNS サーバ（Preferred IPv4 DNS Server）]**：プライマリ DNS サーバーの IP アドレスを入力します。
- **[代替 IPV4 DNS サーバ（Alternate IPv4 DNS Server）]**：セカンダリ DNS サーバーの IP アドレスを入力します。

ステップ 5 [保存（Save）] をクリックします。

NTP の設定

Cisco Intersight 仮想アプライアンスで少なくとも 1 つの Network Time Protocol（NTP）を設定して、アプライアンスの時刻を NTP サーバーと同期させる必要があります。NTP サーバーの認証スキーマは、非認証または認証のいずれかになります。アプライアンスの初期設定時に最大 4 台の未認証 NTP サーバーと 4 台の認証済み NTP サーバーを追加し、必要に応じて後で編集できます。

NTP サーバーを設定するには、次のタスクの情報を使用します。

ステップ 1 アカウント管理者ロールを持つユーザーとして Cisco Intersight 仮想アプライアンスにログインします。

ステップ 2 **[サービス セレクタ（Service Selector）]** ドロップダウン リストから **[システム（System）]** を選択し、**[設定（Settings）]** > **[ネットワーキング（NETWORKING）]** > **NTP** に移動します。

既存の NTP 設定の詳細が表示されます。

ステップ 3 **[設定（Configure）]** をクリックします。

[NTP の設定（Configure NTP）] ウィンドウが表示されます。

ステップ 4 **[NTP サーバの追加（Add NTP Servers）]** をクリックして NTP サーバーを追加します。

a) **[+]** をクリックします。

b) **[サーバ名（Server Name）]** にサーバーのホスト名またはIPアドレスを入力し、**[保存（Save）]** をクリックして、NTP サーバーを未認証のものとして保存します。

c) NTP サーバーを認証済みサーバーとして追加するには、**[NTP認証の有効化（Enable NTP Authentication）]** ボタンを有効にします。

次の情報を入力します。

- **サーバ名**：サーバー ホスト名または IP アドレス
- **対称キー タイプ**：このサーバーに使用する対称キーのタイプ
- **対称キー ID**：NTP メッセージの認証に使用される暗号キーを識別する正の整数
- **対称キー値**：対称キーの値

d) **[保存（Save）]** をクリックします。

既存の NTP サーバー設定を編集するには、設定済みの NTP サーバーのいずれかで **[+]** をクリックし、必要に応じて編集を行い、編集した設定を保存します。

外部 Syslog の設定

Intersight 仮想アプライアンスは、外部の syslog サーバーを構成する機能を提供します。Intersight 仮想アプライアンスで外部 Syslog を有効にすると、外部 Syslog の構成時に提供された詳細に基づいて、次のタイプのログとアラームをエクスポートできます。

- **[ウェブ サーバー ログ（Web Server Logs）]** — ユーザーセッションアクティビティに関連するすべてのトランザクションの Web サーバー アクセス ログ。
- **[監査ログ（Audit Logs）]** — Intersight 仮想アプライアンスの監査ログ画面に表示される、ログイン、ログアウト、作成、変更、削除などのイベントの監査ログ。
- **[アラーム（Alarms）]** — 管理対象の障害（障害）またはしきい値を超えたときにアラートを提供するアプライアンス アラームを含むすべての Intersight アラーム。Intersight のアラームの詳細については、[アラーム（Alarms）] を参照してください。Intersight 仮想アプライアンスののアラームの詳細については、Intersight 仮想アプライアンスのモニタリングにある *Intersight* 仮想アプライアンスのアラームの表を参照してください。

注目

- Intersight 仮想アプライアンスでは、TLS、UDP、および TCP のプロトコルを使用して、外部syslog サーバーへのセキュア通信を提供できます。ただし、実稼働環境では TLS**のみ**を使用することを強くお勧めします。
- 電源やファンの障害などの UCS C シリーズ サーバー関連の障害は、Intersight 仮想アプライアンスによって外部の syslog サーバーに転送されません。UCS C シリーズのイベントと障害の転送を処理するには、UCS C シリーズ CIMC 側で外部 syslog サーバーを設定してください。

Intersight 仮想アプライアンスで外部 syslog を構成するには、次の手順を実行します。

始める前に

ウェブ サーバー ログ、監査ログと Intersight 仮想アプライアンス内のアラームを送信する外部 syslog サーバーの証明書が追加されていることを確認します。この証明書を使用して、外部の syslog サーバーとの TLS 通信を確認します。証明書の追加方法については、証明書 （102 ページ） を参照してください。

- 外部 syslog サーバーの設定時に **[ホスト名/ IP アドレス（Hostname / IP Address）]** フィールドで FQDN を使用する場合は、共通syslog の適切な FQDN エントリまたはサブジェクト

代替名の DNS エントリを使用して外部syslog サーバーの証明書を設定します。外部syslog の設定時に、**[ホスト名/ IP アドレス（Hostname / IP Address）]** フィールドにこの情報を入力します。

- 外部syslog サーバーの設定時に **[ホスト名/ IP アドレス（Hostname / IP Address）]** フィールドに IPv4 または IPv6 アドレスを使用する場合は、共通名に IP アドレスを使用して外部 syslog サーバーの証明書を設定します。外部syslog の設定時に、**[ホスト名/ IP アドレス（Hostname / IP Address）]** フィールドにこの情報を入力します。

ステップ 1 アカウント管理者ロールを持つユーザーとして Intersight 仮想アプライアンスにログインします。

ステップ 2 **[サービス セレクタ（Service Selector）]** ドロップダウン リストから **[システム（System）]** を選択し、**[設定（Settings）]** > **[ネットワーキング（NETWORKING）]** > **[外部 Syslog（External Syslog）]** に移動します。

既存の外部syslog設定の詳細を表示できます。

ステップ 3 **[外部 Syslog サーバーの追加（Add External Syslog Server）]** をクリックします。

[外部 Syslog の構成（Configure External Syslog）] ウィンドウが表示されます。

ステップ 4 必要に応じて、次のフィールドを更新します。

- **[外部 Syslog を有効にする（Enable External Syslog）]**—有効にすると、Web サーバー アクセス ログ、監査ログ、およびアラームが、**[ホスト名/IP アドレス（Hostname/IP Address）]**、**[ポート（Port）]**、**[プロトコル（Protocol）]**、および **[レポートするアラームの最小重大度（Minimum Severity of Alarms to Report）]**のフィールドで提供される構成の詳細に従って、構成された外部 Syslog サーバーに送信されます。**[レポートアラームの最小重大度（Minimum Severity of Alarms to Report）]**のフィールドは、**[アラーム（Alarms）]**にのみ適用されることに注意してください。
- **[Web サーバアクセスログ（Web Server Access Logs）]**—有効にすると、ユーザー セッション アクティビティに関連するすべてのトランザクションの Web サーバー アクセス ログをエクスポートできます。

  （注） このオプションを有効にしないことを強くお勧めします。ログファイルがすぐに過密になるためです。このオプションは主に、Web サーバーのアクセス ログをエクスポートする機能を必要とするお客様が使用できます。

- **[監査ログ（Audit Logs）]**—有効にすると、監査ログ画面に表示されるログイン、ログアウト、作成、変更、削除などのイベントの監査ログが、構成された外部 syslog サーバーに送信されます。
- **[アラーム（Alarms）]**—有効にすると、管理対象ターゲットの障害（障害）またはしきい値を超えたときにアラートを提供するアプライアンス アラームを含む Intersight アラームが、構成された外部 syslog サーバーに送信されます。
- **ホスト名/ IP アドレス**：FQDN、IPv4 アドレス、または IPv6 アドレスを入力します。この情報は、外部syslog サーバーの証明書で指定した詳細と一致する必要があります。
- **Port**：外部 syslog サーバーに使用するポート

- **プロトコル**：ドロップダウンリストからプロトコルを選択します。実稼働環境ではTLS **のみ**を使用することを強く推奨します。
- **[レポートするアラームの最小重大度（アラームのみに適用）（Minimum Severity of Alarms to Report (Applicable for Alarms Only)）]**— 報告されるアラームの最小重大度として、警告、情報、または重大のいずれかを選択します。選択した重大度以上のアラームがエンドポイントでクリアされると、その通知も外部 syslog サーバーにエクスポートされます。

ステップ 5 **[追加（Add）]** をクリックします。

E メール通知の SMTP 設定

ネットワークシステムとソフトウェアは、重要なイベントまたは傾向が検出されたことを示すアラームを頻繁に作成します。E メール通知は、最近のアラームを自動的にポーリングし、重大度を決定し、作成したルールに基づいて、重要なアラームをユーザーの E メール アドレスに送信します。

Intersight 仮想アプライアンスで E メール通知を構成するには、次の 2 つのタスクを実行します。

- Simple Mail Transfer Protocol（SMTP）設定の構成
- 通知ルールの作成

SMTP 設定の構成

SMTP 設定を構成するには、次の手順を行います。

1. アカウント管理者ロールを持つユーザーとしてIntersight仮想アプライアンスにログインします。
2. **[サービス セレクタ（Service Selector）]** ドロップダウンリストから **[システム（System）]** を選択し、**[設定（Settings）]** > **[ネットワーキング（NETWORKING）]** > **SMTP** に移動します。

   既存の SMTP 設定の詳細を表示できます。ここで初めて E メール通知用に SMTP を構成する場合、フィールドにはデフォルト値が表示されるか、値が表示されません。
3. [構成（Configure）] をクリックします。
4. SMTP トグルボタンをオンにし、E メール通知を設定します。
5. [SMTP サーバーアドレス（SMTP Server Address）] フィールドに、E メール通知を送信するドメイン内のサーバーの IP アドレスまたはドメイン名を入力します。
6. [SMTP ポート（SMTP Port）] リストで、E メール通知の転送を実行するサーバーのポート番号を入力または選択します。

ポート 25 は、標準の SMTP リレーポートです。ポート 465 または 587 は、セキュリティで保護されたメール ルーティング ポートです。ポート選択の値の範囲は 1 ～ 65535 で、デフォルトは 25 です。

7. [SMTP 送信者名（SMTP Sender Name）] フィールドに、E メール通知を送信するユーザーの E メールアドレスを入力します。

8. （オプション）TLS トグルボタンをオンにします。

   TLS は、SMTP E メール サーバーの認証局（CA）を検証することによってセキュリティを提供する認証形式です。TLS セキュリティを適用するには、TLS リージョンのリストから適用する CA を選択します。

9. （オプション）SMTP サーバーで認証が必要な場合は、認証トグルボタンをオンにし、SMTP サーバーへの認証に使用するユーザー名とパスワードを指定します。

10. [構成（Configure）] をクリックします。

次に、通知ルールを作成する手順を完了します。

通知ルールの作成

通知は、受信アラームに対して設定したルールに基づいています。

E メール通知設定を構成するには、次の手順を実行します。

1. アプライアンス UI で、**[サービス セレクタ（Service Selector）]** ドロップダウン リストから **[システム（System）]** を選択し、**[設定（Settings）]** > **[一般 （General）]** > **[通知（Notifications）]**に移動します。

   既存のルールが入力された通知ルール リストを表示できます。

   各ルールは、通知の発生条件（アラーム列）と通知先（メール列）の両方として使用されます。このセッションで [SMTP の設定（Configure SMTP）] 画面の [SMTP 送信者名（SMTP Sender Name）] で設定された E メール アドレスの通知ルールを初めて作成する場合、既存のルールはリストに表示されません。リストには、次の列が表示されます。

   - **名前（Name）**—ルールの名前。
   - **有効（Enabled）**—ルールの管理状態。**[はい（Yes）]** 設定は、ルールがアクティブであることを示し、ルール条件が満たされたときに E メール通知tが生成されます。**[いいえ（No）]** 設定は、ルールが非アクティブであることを示し、E メール通知は生成されません。
   - **E メール（Email）**—通知の送信先となる E メールアドレス。
   - **アラーム（Alarms）**— 通知を生成するために必要なイベントの重大度。
   - **最終更新日時（Last Updated）**— 作成または編集セッションのいずれかで、通知が最後に構成された日時。タイムスタンプの形式は < 日>:< 時>:<分> です。

2. 画面右上の **[ルールの追加（Add Rule）]** ボタンをクリックします。

   [ルールの追加（Add Rule）] 画面が表示されます。

3. ルールを構成するには、[**ルールを有効にする（Enable Rule**）] トグルボタンを有効にする必要があります。
4. [名前（Name）] フィールドに、ルールの名前にする文字列を最大 32 文字で入力します。
5. [E メール（Email）] フィールドに、生成された E メール通知の送信先となる E メールアドレスを入力します。**(+)** アイコンをクリックして、他の宛先の追加の E メールアドレスを入力します。

（注） E メール通知用に最大 3 つの E メール送信先を作成できます。

6. [重大度（Severity）] リージョンで、通知メールを送信するために到達するアラームの緊急度レベルを選択します。

   アラームの緊急度レベルは、Critical（最も緊急）、Warning（2 番目に緊急度が低い）、および Info（緊急度なし）です。1 つまたは複数の緊急度レベルを選択できます。複数の重大度を設定した場合、緊急度が最も低いレベルに到達すると E メール通知の送信がトリガーされます。
7. [**追加（Add**）] をクリックします。

   次の警告メッセージが表示されます。

   ```
   警告! 電子メール通知には機密データが含まれている場合があります。E メールアドレスが正しく入力されており、データの受信が承認されていることを確認してください。
   ```

8. **[続行（Continue**）**]**をクリックします。

   [通知（Notifications）] 画面に戻り、リストに新しいルールが表示されます。

制限事項

E メール通知を構成する場合は、次の制限に注意してください。

- ルールごとに最大 3 つの E メールを設定できます。
- アカウントごとに最大 5 つのルールを設定できます。
- イベントは、10 秒のスライディング タイムウィンドウで収集されます。Intersight は、まず 10 秒間待機して、アラームをポーリングします。この最初の期間に 1 つまたは複数のアラームが検出された場合、Intersight はアラームを検出するためにさらに 10 秒間待機します。この期間中にアラームが検出されると、アラームが検出されなくなるまで追加の期間が発生します。アラームが検出されないままさらに 10 秒が経過すると、検出されたアラームがアラームグループにバンドルされ、アラームを含むEメールが指定されたアドレスに送信されます。
- E メール アドレスは最大 100 のアラームに関連付けることができ、送信される E メールの数はアラームグループの大きさによって異なります。アラームグループに 100 を超えるア

ラームが含まれている場合は、追加の E メールが送信されます。一部のイベントでは、1,000 のアラームが生成される場合があります。その場合、10 通のメールが送信されます。

LDAP の設定

Intersight 仮想アプライアンスは、LDAP/AD ベースのリモート認証をサポートしています。LDAP を使用したユーザー ログインを認証するようにアプライアンスを構成できます。複数の LDAP ドメインを設定し、ログイン用のドメインを選択できます。

LDAP ユーザーは、電子メール ID またはユーザー名を使用して Intersight 仮想アプライアンスにログインし、LDAP ユーザーが設定されている対応するドメインを選択できます。各 Intersight アカウントには最大 6 個の LDAP ドメインを追加できます。**[設定 (Settings)] アイコン** > **[設定 (Settings)]** > **[ネットワーク (NETWORKING)]** > **[LDAP/AD]** テーブル ビューに設定された LDAP ドメインのリストを表示できます。仮想アプライアンスを LDAP/AD サービスと統合する方法については、このビデオをご覧ください。

Intersight 仮想アプライアンスで LDAP 認証を設定するには、次の手順を実行します：

ステップ 1 アカウント管理者ロールを持つユーザーとして Intersight 仮想アプライアンスにログインします。

ステップ 2 **[サービス セレクタ（Service Selector）]** ドロップダウン リストから **[システム（System）]** を選択し、**[設定（Settings）]** > **[ネットワーキング（NETWORKING）]** > **LDAP/AD** に移動します。

[LDAP の構成（Configure LDAP）] ウィンドウが表示されます。

ステップ 3 **[LDAP の構成（Configure LDAP）]** ページで、次に示すフィールドに対応する詳細を追加し、**[保存（Save）]** をクリックします。

- **[名前 (name)]**: ： 設定する LDAP ドメインを簡単に識別するための名前を入力します。
- **[ベース DN（Base DN）]**：サーバーのベース識別名（DN）を入力します。たとえば、DC=Intersight、DC=com などです。
- **[バインド DN（Bind DN）]**：LDAP サーバーに対する認証に使用する DN とユーザーのパスワードを入力します。
- **[グループ属性（Group Attribute）]**：LDAP エントリが属するグループメンバー属性を入力します。Cisco Intersight 仮想アプライアンスは、このグループ属性を使用して、Intersight ロールをユーザーにマッピングまたは割り当てます。デフォルト値は **member** です。これは、[LDAP の編集（Edit LDAP）] で編集できます。
- **[パスワード（Password）]**：ユーザーの DN パスワードを入力します。
- **[ネストされたグループ検索（Nested Group Search）]**：有効にすると、拡張検索は、祖先のチェーン全体をルートまで実行し、各グループとサブグループが属するすべてのグループとサブグループを再帰的に返します。

- **[暗号化の有効化（Enable Encryption）]**：LDAP サーバー上の通信を保護する暗号化を有効にする必要があります。暗号化を有効にすると、信頼できるルート証明書を追加する必要があります。SSL 証明書の手動による追加の詳細については、「証明書の追加」を参照してください。
  - 将来のリリースでは、Intersight 仮想アプライアンスは、SHA-1 ハッシュ関数で署名された証明書のサポートを段階的に廃止します。SHA-256、SHA-384、SHA-512 など、SHA-1 よりも強力なハッシュ関数を使用する署名アルゴリズムを使用するように証明書をアップグレードすることを強くお勧めします。
  - 共通名の使用が廃止されたため、LDAP サーバー用に作成された証明書にはサブジェクト代替名（SAN）が含まれている必要があります。SAN のない証明書は検証に失敗し、接続の問題が発生します。

- **サーバ**：LDAP サーバーの IP アドレスまたはホスト名を追加します。Cisco Intersight 仮想アプライアンスは、1 つの LDAP プロバイダーとポートのみをサポートします。

  注目
  - LDAPS は、ポート 636 およびポート 3269 でサポートされています。他のすべてのポートは、TLS で LDAP をサポートしています。
  - **Intersight 仮想アプライアンスは、電子メール識別子またはユーザー名を使用して LDAP ユーザーにログイン**します。電子メール ID を使用してアプライアンスにログインする場合は、LDAP サーバーでメール属性を設定します。ユーザー名を使用する場合は、LDAP サーバーでそのユーザーに設定されている **sAMAccountName** を使用します。
  - **LDAP を設定するために必要な詳細を追加した後、ユーザーまたはグループを追加して LDAP ユーザーに適切なロールを割り当てる前に、 Deployappliance Eldap ワークフローが完了するのを待ちます。要求内のワークフローのステータスを確認できます。詳細については、「ユーザーの追加」または「**グループの追加**」を参照してください。**
  - **Intersight API を使用してアプライアンスの LDAP ログインを設定する場合は、LDAP ポリシーが appliance.management:true にタグ付けされていることを確認します。これは、[設定 (Settings)] で LDAP を設定するユーザーに対して自動的に実行されます。**

  LDAP を設定するために必要な詳細を追加した後、LDAP ユーザーとしてログインする前に、**Deployappliance Eldap** ワークフローが完了するのを待ちます。**要求**内のワークフローのステータスを確認できます。

- **[ポート (Port)]**：LDAP サーバー ポートを追加します。

Intersight 仮想アプライアンスでのシングル サインオン

シングル サインオン（SSO）認証では複数のアプリケーションへのログインに 1 つのクレデンシャル セットを使用できます。SSO 認証では企業のクレデンシャルを使用して Intersight にログインできます。Intersight は SAML 2.0 を介して SSO をサポートし、サービス プロバイダー（SP）として機能して、SSO 認証のために ID プロバイダー（IdP）と統合できます。

アプライアンスを介して SSO をセットアップするには、管理者ロールを持つユーザーとして Cisco Intersight 仮想アプライアンスにログインし、SP メタデータをダウンロードし、ID プロバイダー（IdP）を Intersight 仮想アプライアンスに登録する必要があります。

IdP の要件

Intersight に追加する IdP は SAML 2.0 とサービス プロバイダーが開始した SSO をサポートしている必要があります。最も一般的に使用されている IdP でこのステップを実行する手順は異なっています。

（注） Intersight 仮想アプライアンスのマルチノード クラスター セットアップがある場合、またはシングルノード構成からマルチノードクラスタ 構成に拡張する場合、Okta などの一部の IdP では 3 つの SSO を手動で構成する必要がありますが、ADFS などの他の IdP では、xml ファイルを直接インポートできます。SSO 構成が手動の IdP の場合、アプライアンスの SSO 画面からダウンロードしたメタデータ ファイルで指定された 3 つの異なる SSO URL を構成する必要があります。3 つの URL を構成したら、3 つのノードのいずれかから SSO ログインを続行できます。

アプライアンスでのマルチノード クラスタ セットアップの追加要件：

- SLO（シングル ログアウト）は、アプライアンスのマルチノード セットアップでサポートされていますが、SLO エンドポイントは 1 つだけです。SLO URL で指定されたノードが停止している場合、SLO は機能しません。この場合、Intersight からのみログアウトされます。
- IDP によって開始される SSO は、エンティティ ノードに対してのみ機能します。

Intersight での SSO のセットアップと ID プロバイダーの追加の詳細については、「Intersight でのシングル サインオン」を参照してください。Intersight シングル サインオンを有効にし、Intersight を使用して外部 ID プロバイダー（IdP）でカスタム SAML 2.0 アプリケーションをセットアップする方法を示したビデオを視聴するには、こちらをクリックしてください。

証明書

外部ターゲット（LDAP サーバーなど）にセキュア認証を提供するには、ターゲットの ID を確認する信頼できるソースからサードパーティ証明書を追加するか、ブラウザを介してアプライアンスのセキュアな **HTTPS** アクセス用の CA 署名付き証明書または自己署名証明書を追加できます。

- 将来のリリースでは、Intersight 仮想アプライアンスは、SHA-1 ハッシュ関数で署名された証明書のサポートを段階的に廃止します。SHA-256、SHA-384、SHA-512 など、SHA-1 よりも強力なハッシュ関数を使用する署名アルゴリズムを使用するように証明書をアップグレードすることを強くお勧めします。

- 共通名の使用が廃止されたため、LDAP サーバー用に作成された証明書にはサブジェクト代替名（SAN）が含まれている必要があります。SAN のない証明書は検証に失敗し、接続の問題が発生します。

信頼できる証明書

外部ターゲットへの接続時にセキュアな認証を提供するために、信頼できるソースからのサードパーティ証明書、またはターゲットの ID を確認する自己署名証明書を追加できます。サードパーティ証明書は、発行元トラストポイント（ルート認証局（CA）、中間 CA、またはルート CA につながるトラスト チェーンの一部となるトラスト アンカーのいずれか）によって署名されます。

信頼できる証明書テーブル ビューには、**[設定 (Settings)]** > **[設定 (Setting)]** > **[認証 (AUTHENTICATION)]** > **[信頼できる証明書 (Trusted Certificates)]** からアクセスでき、Intersight に追加された証明書のリストが表示されます。

証明書の追加

次のタスクでは、Intersight 仮想アプライアンスで信頼できる証明書を追加する方法について詳しく説明します。

1. アカウント管理者ロールを持つユーザーとして Intersight 仮想アプライアンスにログインします。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから **[システム（System）]** を選択し、**[設定（Settings）]** > **[認証（AUTHENTICATION）]** > **[証明書（Certificates）]** > **[信頼済み（Trusted）]** に移動します。

   信頼できる証明書に関する次の詳細がテーブル ビューに表示されます。

   - **[名前（Name）]**：CA 証明書の共通名
   - **[発行者（Issued By）]**：証明書発行認証局
   - **[使用（Usage）]**：証明書を使用しているターゲットの数を表示します。
   - **[有効期限（Expires）]**：証明書の有効期限。

3. [証明書の **追加（Add Certificate）]** をクリックして、信頼できる証明書を追加します。
4. **[参照（Browse）]** をクリックして、システムに保存されている証明書を選択し、**[保存（Save）]** をクリックします。証明書が正常にインポートされると、**[信頼できる証明書（Trusted Certificates）]** テーブル ビューに表示されます。

重要 インポートする信頼できる証明書は base64 で暗号化された X.509(PEM) 形式である必要があります。

SSL 証明書の追加

ブラウザを介してアプライアンスのセキュアな **HTTPS** アクセスを有効にするには、証明書署名要求を生成し、証明書を生成するか、自己署名証明書に切り替えることができます。これらのタスクにアクセスするには、**[システム（System）]** > **[設定（Settings ）]** > **[認証（ AUTHENTICATION ）]** > **[証明書（ Certificate ）]** > **[SSL（ SSL ）]**に移動します。

（注） シングルノード展開からマルチノード クラスタ構成に移行する際に、シングルノード展開で SSL 証明書がすでに生成されている場合は、マルチノードクラスタ構成への移行が完了し、クラスタが **正常な** 状態になると、を削除してから、SSL 証明書を削除して再生成します。

証明書署名要求（CSR）を作成するには：

1. アプライアンス UI で、**[サービス セレクタ（Service Selector）]** ドロップダウン リストから**[システム（System）]** を選択し、**[設定（Settings）]** > **[認証（AUTHENTICATION）]** > **[証明書（Certificates）]** > **SSL**に移動します。

   現在の証明書に次の詳細が表示されます。

   - **[名前（Name）]**：CA 証明書の共通名。
   - **[追加者 (Added By)]**：アカウントに証明書を追加したユーザー
   - **[発行者 (Issued By)]**：証明書発行認証局
   - **[有効期限 (Expires):**：証明書の有効期限。

   [すべて表示 (View All)] をクリックして、**[証明書の表示 (View Certificate)]** ウィンドウを表示します。上記の詳細に加えて、フィンガープリント、国、地域、組織、組織単位、および発行者名、組織、共通名、および署名アルゴリズムの詳細情報を表示することもできます。

2. **[アクション (Action)]** ドロップダウン メニューから、**[CSR の作成 (Create CSR)]** を選択します。

   [証明書署名要求の作成 (Create Certificate Signing Request)] ウィザードが表示されます。次のように必要な詳細情報を入力します。

   - [組織 (Organization)]：企業の正式名称
   - [組織単位 (organization Unit)]：証明書を処理する組織の下位。たとえば、HR などです。
   - [地域 (Locality)]：組織が所在する都市/町
   - [状態 (State)]：組織が配置されている状態
   - [国 (Country)]：組織の所在地の国を表す 2 文字の ISO コードです。国コードの完全なリストについては、「ISO 3166」を参照してください。

- [電子メール アドレス (Email Address)]：組織に連絡するために使用される電子メール アドレス
- [係数（Modulus）]：CSR の署名に使用される RSA 秘密キーの係数

3. **[CSR の作成（Create CSR）]** をクリックします。

[CSR の作成 (Create CSR)] をクリックすると、新しい証明書署名要求 (CSR) が生成されます。次のいずれかのオプションを選択できます。

- **[CSR のダウンロード（Download CSR）]**：CSR をローカルでダウンロードして保存し、**認証局**（CA）から信頼できる証明書を取得できるようにします。

（注） 証明書発行要求プロセスでは、情報カテゴリの別名（SAN）フィールドでアプライアンスの FQDN のみを使用します。認証局から Intersight アプライアンスおよび Intersight Assist の信頼できる証明書を取得するときは、SAN フィールドにホスト名または IP アドレスを入力しないでください。

- **[CSR の削除（Delete CSR）]**：信頼できる証明書を生成する際に使用しない場合は、CSR を削除します。
- **[証明書の適用 (Apply Certificate)]**：CA が証明書を発行した後、**[適用 (Apply)]** をクリックして、**[証明書の適用 (Apply Certificate)]** ウィンドウの **[証明書 (Certificate)]** フィールドに証明書の内容を貼り付けます。**[アップロード (Upload)]** オプション ボタンをクリックして、証明書をアップロードすることもできます。**[適用 (Apply)]** をクリックしてプロセスを完了します。CA によって発行された証明書は、*.csr*、*.pem*、または *.crt* 形式にすることができます。

自己署名証明書に切り替える方法：

1. アプライアンス UI で、**[サービス セレクタ（Service Selector）]** ドロップダウン リストから**[システム（System）]** を選択し、**[設定（Settings）]** > **[認証（AUTHENTICATION）]** > **[証明書（Certificates）]** > **SSL**に移動します。
2. **[アクション (Action)]** ドロップダウン メニューから、**[自己署名への切り替え (Switch to Self-Signed)]** を選択します。

   自己署名証明書への切り替えには数分かかることを警告するポップアップウィンドウが表示されます。
3. 先に進むには **[適用（Apply）]** をクリックします

- Cisco では、CA 署名付き証明書を使用してアプライアンスにアクセスすることを推奨しています。自己署名証明書が使用されている場合、最新のブラウザはアプライアンスへのアクセスを無効にする可能性があります。Intersight 仮想アプライアンスは、Cisco が提供し

た自己署名証明書の有効期限が切れた場合に、自己署名証明書に切り替えて証明書の有効期間を延長するオプションを提供します。

- 自己署名証明書に切り替えるように選択すると、現在のSSL証明書が新たに生成された自己署名証明書に置き換えられます。新しい証明書が適用されているかどうかを確認するには、ブラウザのアドレス(ロケーション)バーのURLの前にある[ロック(Lock)]または[警告(Warning)]アイコンをクリックします。更新後、アプライアンスに再度ログインせずに、**[設定(Setting)]** > **[証明書(Certificates)]** ページに直接移動します。

ローカル ユーザー向けパスワード ポリシーの設定

このタスクでは、Intersight仮想アプライアンスでローカルユーザーのパスワードポリシーを設定する方法について説明します。

ステップ 1 アカウント管理者ロールを持つユーザーとして Intersight 仮想アプライアンスにログインします。

ステップ 2 **[サービス セレクタ（Service Selector）]** ドロップダウン リストから **[システム（System）]** を選択し、**[設定（Settings）]** > **[認証（AUTHENTICATION）]** > **[ローカル ユーザー（Local Users）]**に移動します。

既存のパスワードポリシーの詳細を表示できます。

ステップ 3 **[構成（Configure）]** をクリックします。

[ローカル ユーザーの設定（Configure Local Users）] ウィンドウが表示されます。

ステップ 4 必要に応じて、次のパスワードポリシーオプションを更新して、パスワードポリシーを設定します。

パスワード ポリシー オプション	許容範囲/デフォルト値
パスワードの最小長	8ー127文字 デフォルトでは 8 です。
必要な大文字の最小数	1 ～ 64 文字 デフォルトでは 1 です。
必要な小文字の最小数	1 ～ 64 文字 デフォルトでは 1 です。
必要な数字の最小数	1 ～ 64 文字 デフォルトでは 1 です。
特殊文字の最小数	0 ～ 64 文字 デフォルトでは 0 です。 （注） 特殊文字には、句読点と記号が含まれます。

パスワード ポリシー オプション	許容範囲/デフォルト値
許可されない以前のパスワードの数	0 ～ 10 デフォルトでは 0 です。
以前のパスワードとは異なる最小文字数	0 ～ 15 デフォルトでは 0 です。 （注） 以前のパスワードとの差異は、指定されたパスワード内の同じ文字位置に基づいてチェックされます。
パスワード変更を許可されるまでの最小日数	0 ー 7 日 デフォルトでは 0 です。 （注） このパスワードポリシーオプションに値0を指定した場合、ユーザーはパスワード変更の間隔が制限されません。
不正なログイン試行の時間（秒）	300 ～ 3600 秒（5 ～ 60 分） デフォルト値は1 ,800 秒（30分）です。 不正なログイン試行が連続した場合、期間が追跡されます。この期間中に設定された最大不正ログイン試行回数を超えると、ユーザーはロックアウトされます。 ロックアウト機能の詳細については、「ローカル ユーザーアカウントのロックアウト」を参照してください。
不正ログインの最大許容試行回数	3～10 デフォルトは 5 です。 設定された時間内に許可された不正ログインの最大連続試行回数を超えると、ユーザーはロックアウトされます。
管理者ユーザーのロックアウトの有効化	デフォルトは false です。 ローカルの「admin」ユーザーに対してユーザー ロックアウト機能を有効にする必要があるかどうかを決定します。このオプションは、他のローカル ユーザーに対して常に有効になります。

パスワード ポリシー オプション	許容範囲/デフォルト値
	ロックアウト機能の詳細については、「ローカル ユーザー アカウントのロックアウト」を参照してください。
ロックアウト期間（秒）	60 ～ 3600 秒（1 ～ 60 分） デフォルトは 900秒（15分）です ローカル ユーザー アカウントがロックされたままになる期間（秒単位）。アカウントは、設定されたロックアウト時間が経過した後にのみ自動的にロック解除されます。

ステップ 5 **[保存（Save）]** をクリックします。

パスワード ポリシーの変更は、次回のパスワード変更時に確認できます。

ローカル ユーザー アカウントのロックアウト

ローカルユーザーについて、設定された時間内に連続する不正ログイン試行が追跡され、この期間中に設定された不正ログイン試行回数を超えると、アカウントがロックアウトされます。ローカル ユーザー アカウントがロックされると、[ローカル ユーザー（Local User）] テーブルのユーザーの横に警告アイコンが表示されます。設定されたロックアウト期間が経過すると、アカウントは自動的にロック解除されます。アカウント管理者またはユーザー アクセス管理者は、設定されたロックアウト期間中にパスワードをリセットすることで、アカウントのロックを解除できます。

（注） ロックアウト機能：

- ローカル ユーザーにのみ適用され、リモート ユーザーには適用されません。
- 設定が有効になっている場合にのみ、ローカルの「admin」ユーザーに適用されます。

ローカル ユーザーのパスワードのリセット

アカウント管理者は、ローカル ユーザーのパスワードをリセットできます。ユーザー アクセス管理者は、アカウント管理者のロールを持つユーザーを除き、ローカルユーザーのパスワードをリセットすることもできます。

ローカル ユーザーのパスワードをリセットするには、次の手順を実行します。

1. アカウント管理者ロールを持つユーザーとしてIntersight仮想アプライアンスにログインします。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから **[システム（System）]** を選択し、**[設定（Settings）]** > **[アクセスと権限（ACCESS & PERMISSIONS）]** > **[ユーザー（Users）]** に移動します。
3. パスワードをリセットするローカル ユーザーを選択します。
4. 鉛筆アイコンをクリックし、パスワードを変更します。
5. **[保存（Save）]** をクリックします。

注目 アカウント管理者がローカルの「admin」ユーザーのパスワードをリセットすると、GUI パスワードのみが変更されます。ローカルの「admin」ユーザーの SSH パスワードは変更されません。ローカルの「admin」ユーザーは、新しくリセットされたパスワードを使用してアプライアンスにログインする必要があります。ローカルの「admin」ユーザーがログインすると、ローカルの「admin」ユーザーにパスワードの変更を要求するプロンプトが表示され、GUI と SSH の両方のパスワードがリセットされます。

ユーザーの追加

Intersight 仮想アプライアンスでは、ユーザーへのグループ ロールの割り当てをオーバーライドできます。アカウントに追加されたユーザーのリストは**[ユーザ（User）]**ページに表示できます。このリストには、ユーザーの**[名前（Name）]**、**[ID プロバイダー（Identity Provider）]**、**[電子メール（Email）]**、**[ロール（Role）]**、および**[最終ログイン時刻（Last Login Time）]**が表示されます。リモートユーザーとローカルユーザーを追加できます。最大 100 のローカル ユーザーを追加できることに注意してください。

- リモートユーザー：IDP 経由で認証（LDAP および SSO）
- ローカルユーザ：Intersight 仮想アプライアンス経由で認証

注目 ユーザーを作成したり、ユーザー ロールを割り当てるには、アカウント管理者またはユーザー アクセス管理者である必要があります。

Intersight 仮想アプライアンスでユーザーを追加するには、次の手順を実行します。

ステップ 1 アカウント管理者ロールを持つユーザーとして Cisco Intersight 仮想アプライアンスにログインします。

ステップ 2 **[サービス セレクタ（Service Selector）]** ドロップダウン リストから **[システム（System）]** を選択し、**[設定（Settings）]** > **[アクセスと権限（ACCESS & PERMISSIONS）]** > **[ユーザー（Users）]** に移動します。

ステップ 3 **[ユーザーの追加（Add User）]** ウィンドウで、次の詳細情報を追加します。

リモート ユーザーまたはローカル ユーザーを追加するオプションがあります。最大 100 のローカル ユーザーを追加できることに注意してください。

リモート ユーザーを追加するには、次の詳細を入力します。

- **[ID プロバイダー（Identity ）]**：このアカウントに追加する ID プロバイダーを選択します。Intersight 検証済みの ID プロバイダーのいずれかを選択できます。詳細については、**<Your FQDN>/help** の「サポートされるシステム ページの「検証済みの *ID* プロバイダー」を参照してください。

  LDAP ユーザーを追加する場合は、適切な ID プロバイダ (IDP) の下にそれらを追加する必要があります。IDP の名前は、LDAP 設定で設定した LDAP ドメイン名と同じになります。

- **[ユーザー ID (User ID)]**：ID プロバイダへのアカウントの登録に使用した有効な電子メール ID を入力します。**ユーザー名は、LDAP サーバーで構成されている sAMAccountName と同じである必要があります。**電子メールを使用してログインする場合は、電子メール ID が LDAP サーバーのメール属性で設定されているものと同じであることを確認してください。

- **ロール（Role）**：リモート ユーザー アカウントに 1 つのロールを割り当てることができます。詳細については、「ロールと権限」の項を参照してください。

ローカル ユーザーを追加するには、次の詳細を入力します。

- **名（First Name）**：ローカル ユーザーの名を入力します。
- **姓（Last Name）**：ローカル ユーザーの姓を入力します。
- **ユーザーID（User ID）**：ローカル ユーザーがアプライアンスにログインするために使用する電子メール ID またはユーザー名を入力します。
- **パスワード（Password）**：ローカル ユーザー パスワード ポリシーに従って有効なパスワードを入力します。
- **ロール（Role）**：ローカル ユーザー アカウントに複数のロールを割り当てることができます。詳細については、「ロールと権限」の項を参照してください。

ステップ 4 **[保存（Save）]** をクリックして新しいユーザーをアカウントに追加します。

注目 新しいローカル ユーザーを追加するときに入力したユーザー ID とパスワードは、新しいローカル ユーザーに直接伝える必要があります。これは、現在 Intersight 仮想アプライアンスには、新しいローカル ユーザーにログイン情報を自動的に通知するメカニズムがないためです。新しいローカル ユーザーがこれらのログイン情報を使用してログインすると、新しいローカル ユーザーにパスワードの変更を要求するプロンプトが表示されます。

ローカル ユーザーは、画面の右上にある **[プロファイル（Profile）] メニュー** に移動し、**[パスワードの変更（Change Password）]** をクリックすることで、いつでもパスワードを変更できます。

グループの追加

グループは、特定のロール、権利、および権限を持つユーザーのコレクションを表します。複数のユーザー グループを作成して共通のロールと権限を一連のユーザーに割り当てることができます。**[グループ（Group）]** ページに、アカウントに追加したグループのリストを表示できます。このリストには、**[名前（Name）]**、**[ID プロバイダー（Identity Provider）]**、**[ロール（Role）]**、および **[ID プロバイダーのグループ名（Group Name in Identity Provider）]** が表示されます。グループを追加するには、次の手順を実行します。

ステップ 1 アカウント管理者ロールを持つユーザーとして Intersight 仮想アプライアンスにログインします。

ステップ 2 **[サービス セレクタ（Service Selector）]** ドロップダウン リストから **[システム（System）]** を選択し、**[設定（Settings）]** > **[アクセスと権限（ACCESS & PERMISSIONS）]** > **[グループ（Groups）]** に移動します。

ステップ 3 右上の**[グループの追加（Add Group）]** ボタンをクリックします。**[グループの追加（Add Group）]** ウィンドウが表示されます。

ステップ 4 **[グループの追加（Add Group）]** ウィンドウで、次の詳細情報を追加します。

- **[ID プロバイダー（Identity ）]**：このアカウントに追加する ID プロバイダーを選択します。Intersight 検証済みの ID プロバイダーのいずれかを選択できます。詳細については、**<Your FQDN>/help** の「サポートされるシステム ページの「検証済みの *ID* プロバイダー」を参照してください。LDAP クレデンシャルを使用してログインするグループに適切な LDAP ドメインを選択する必要があります。
- **[名前（Name）]**：Intersight でグループを識別するために名前を入力します。
- **[ID プロバイダーでのグループ名（Group Name in Identity Provider）]**：ID プロバイダー内に追加されているユーザー グループ名を入力します。グループ名はLDAP識別名（DN）形式である必要があります。例：

  ```
  cn=Finance,cn=Users,dc=example,dc=com
  ```

- **[ロール (Role)]**: 次のシステム定義のロールのいずれかをユーザー グループに割り当て、ユーザー定義のロールを割り当てることができます。
  - **[アカウント管理者 (Account Administrator)]**：このロールでは、グループのメンバーはデターゲットを要求し、Element Manager をクロス起動し、プロファイルとポリシーを作成して、技術サポート バンドルを収集し、要求したデバイスまたはアカウントの設定に変更を加えることができます。
  - **[読み取り専用 (Read-Only)]** ：このロールでは、グループのメンバーはアカウント内の要求済みターゲットの詳細とステータスを表示できます。ただし、要求済みターゲットやアカウントの設定を変更することはできません。
  - **[デバイス技術者 (Device Technician)]**：このロールでは、グループのメンバーは Intersight でターゲットを要求し、要求したターゲットのリストを [ターゲット (Targets)] テーブル ビューに表示できます。
  - **[デバイス管理者 (Device Administrator)]**：このロールでは、グループのメンバーは Intersight でターゲットを要求し、要求したターゲットのリストを表示し、ターゲットを削除(要求解除)できます。

- **[サーバ管理者 (Server Administrator)]**：このロールでは、グループのメンバーはファームウェアのアップグレード、技術サポート バンドルの収集、サーバー タグの設定、サーバー プロファイルまたはポリシーの作成、編集、および展開、サーバー詳細の表示など、すべてのサーバー アクションを実行できます。
- **[HyperFlex クラスタ管理者 (HyperFlex Cluster Administrator)]**：このロールでは、グループのメンバーは HyperFlex クラスタ プロファイルの作成、クラスタのアップグレード、クラスタ タグの設定、クラスタ ダッシュボードと概要の表示、技術サポートバンドルの収集、アラームの監視、**HX Connect** の起動と管理を行えます。
- **[ユーザ アクセス管理者（User Access Administrator）]**：このロールでは、グループのメンバーはアカウントの詳細の表示、およびユーザーの追加、グループの追加、IDプロバイダーとシングルサインオンのセットアップ、アカウントに関連する API キーの生成など、ユーザー アクセス関連のアクションを実行できます。

注目 グループを作成したり、ユーザー ロールを割り当てるには、アカウント管理者またはユーザー アクセス管理者である必要があります。

ステップ 5 [保存（Save）] をクリックして新しいグループをアカウントに追加します。

ロールの追加

ユーザー定義のロールの作成

Intersight 内のシステム定義のロールに加えて、ユーザー定義のロールを作成できます。**[ロール (Roles)]** ページに、アカウントに追加したグループのリストを表示できます。このリストには、ロールの**名前**、**タイプ**、**使用状況**、**範囲**、および**説明**が表示されます。ユーザー定義のロールを作成するには、次の手順を実行します。

注目 **アカウント管理者権限またはユーザーアクセス管理者権限を持つユーザのみが、ユーザー定義のロールを作成できます。**

1. Cisco Intersight にログインします。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから **[システム（System）]** を選択し、**[設定（Settings）]** > **[アクセスと権限（ACCESS & PERMISSIONS）]** > **[ロール（Roles）]** に移動します。
3. **[ロール (Roles)]** で、**[ロールの作成 (Create Role)]** をクリックします。
4. **名前**を入力して、Intersight でロールを識別し、ロールの使用状況に関する**説明**を入力します。

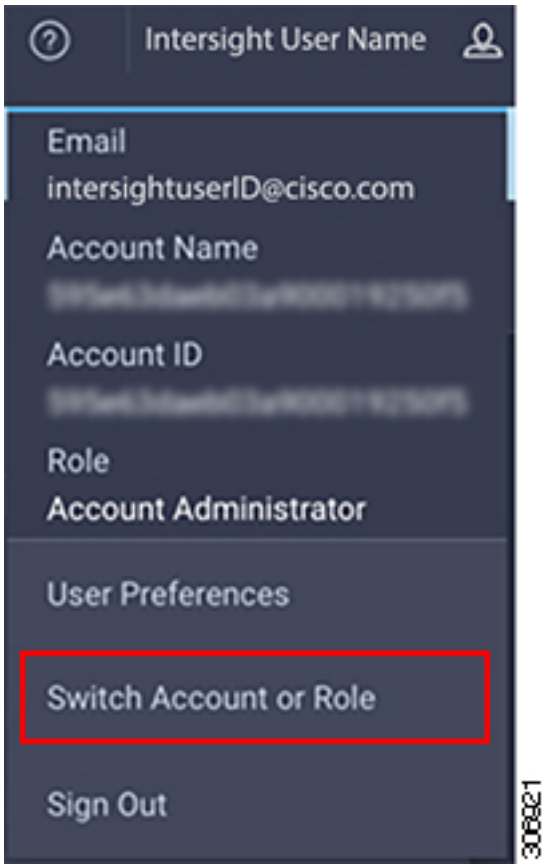
[セッション タイムアウト（Session Timeout）]、[アイドル タイムアウト（Idle Timeout）]、および [同時セッション（Concurrent Sessions）] のデフォルトのアカウント レベル設定を保持することも、これらの設定をカスタマイズすることもできます。

5. **[セッションとアイドルのタイムアウト設定（Session & Idle Timeout settings）]** では、次のいずれかを選択できます。
   - **[アカウント デフォルト設定の使用（Use Account Default Settings）]**：このオプションはデフォルトで有効になっています。セッション タイムアウト値は、アカウント レベルの設定から継承できます。これらの値は、ロールの作成時にデフォルト設定として使用されます。アカウント レベルの [セッション タイムアウト]と [アイドル タイムアウト] の詳細を確認するには、**[設定（Settings）]** アイコン > **[設定（Settings）]** > **[一般（General）]** > **[アカウントの詳細（Account Details）]** に移動します。
   - **[アカウントのデフォルト設定を使用しない（Disable Use Account Default Settings）]**：このオプションを無効にすると、ロールレベルで次のフィールドの値を設定できます。
     - **のセッション タイムアウト（秒）**：セッションの有効期限を秒単位で指定します。最小値は300秒で、最大値は31536000秒(1年)です。システムのデフォルト値は57600秒です。
     - **のアイドル タイムアウト（秒）**：Webセッションの間隔（秒）を指定します。この期間内にセッションが更新されない場合、セッションはアイドルとしてマークされ、削除されます。最小値は300秒、最大値は18000秒(5時間)です。システムデフォルト値は1800秒です。
     - **[最大同時セッション数（Maximum Number of Concurrent Sessions (Sessions)）]** は、アカウント内または権限内で許可されている同時セッション数です。最小セッション数は1、最大セッション数は128です。デフォルト値は 128 です。

6. **[次へ（Next）]** をクリックします。
7. アカウントのリソースへのユーザーアクセスを委任する**範囲**を選択します。ユーザーがアカウント全体にアクセスできるようにするか、または選択した組織へのアクセスを制限するかを選択できます。
   - **[すべて (Al)]**: ユーザーはすべてのアカウントリソースにアクセスできます。ユーザーにロールを割り当てる権限を追加します。選択した権限がアカウント全体に適用されます。
   - **[組織 (Organization)]**: ユーザーは指定された組織にのみアクセスできます。ドロップダウン リストから 1 つ以上の**組織**を選択し、ユーザーにロールを割り当てる**権限を追加**します。権限の詳細については、「**ロール**」の項を参照してください。
8. **[作成 (Create)]** をクリックして、新しいユーザー定義ロールをアカウントに追加します。

アカウントまたはロールの切り替え

アプリケーションからログアウトすることなく、Cisco Intersight でアカウントまたはロールを切り替えることができます。複数のアカウントまたはロールにログインしている場合は、Intersight ダッシュボードの **[プロファイル（Profile）]** メニューに **[アカウントまたはロールの切り替え（Switch Account or Role）]** を行うオプションが表示されます。



（注）

- [アカウントまたはロールの切り替え（Switch Account or Role）] オプションは、単一のアカウントへのアクセスが承認されており、そのアカウントに1つのロールのみがマップされている場合は使用できません。
- アカウントURLを使用してIntersightにログインする場合は、**[アカウントとロールの切り替え（Switch Account and Role）]** オプションによって同じアカウント内のロール間でのみ切り替えられるようになります。
- スイッチングの時点で、認証後にIDプロバイダー（IdP）によって返された属性に基づいてアカウントが再評価されます。アカウントに追加されたユーザーも、IDプロバイダーによってそれらのロールが再認証されます。したがって、アカウントを切り替える前にIntersightがアカウントまたはロールに変更があることを検出した場合は、**[アカウントとロールの選択（Select Account and Role）]** リストにその変更が表示されます。
- Intersight仮想アプライアンスの場合は、LDAPを設定するか、またはSSOを使用してログインして、[アカウントの切り替え(Switch Account)] または [ロール(Role)] オプションを表示する必要があります。

アカウントを切り替えるには次のステップを実行します。

1. **[プロファイル（Profile）]**>**[アカウントまたはロールの切り替え（Switch Account or Role）]** に移動します。**[アカウントとロールの選択 (Select Account and Role)]** ウィンドウが開きます。
2. **[アカウントとロールの選択（Select Account and Role）]**ウィンドウで、切り替え先のアカウント（またはロール）を選択します。新しいアカウントにログインされます。
3. ロールを変更するには、**[設定（Settings）]**>**[アクセスと権限（ACCESS & PERMISSIONS）]** > **[ユーザ（Users）]**に移動し、ロールを変更するユーザーを選択して **[編集（Edit）]**アイコンをクリックします。
4. **[ユーザーの編集（Edit User）]** ウィンドウでロールを選択し、**[保存（Save）]** をクリックします。

組織の追加

組織の作成

[組織 (Organizations)] ページでは、アカウントに追加された組織のリストを表示できます。このリストには、**名前**、**メンバーシップ**、**使用状況**、および**説明**が表示されます。組織を追加するには、次の手順を使用します。

注目 管理者特権を持つユーザーだけがユーザー アカウントを作成、削除、または変更できます。ユーザ アクセス管理者権限を持つユーザーは組織を作成することはできませんが、ユーザー アカウントでそれらを表示し、組織をロールに割り当てることができます。

1. Cisco Intersight にログインします。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから **[システム（System）]** を選択し、**[設定（Settings）]** > **[アクセスと権限（ACCESS & PERMISSIONS）]** > **[組織（Organizations）]** に移動します。
3. **組織**から、**[組織の作成 (Create Organization)]** をクリックします。
4. Intersight で組織を識別するための**名前**を入力し、組織の使用状況に関する**説明**を入力します。
5. **[メンバーシップ (Memberships)]** では、すべてのリソースへのアクセスを割り当てるか、またはリソースの選択的グループへのアクセスを制限するかを選択できます。メンバーシップ タイプに次のいずれかのオプションを選択できます。
   - **[カスタム (Custom)]**: アカウントで使用可能なターゲットのリストから、組織に一連の物理リソースを割り当てるために必要なターゲットを選択します。

重要 カスタム組織内に作成されたプロファイルとポリシーは、同じ組織内のターゲットにのみ適用されます。

   - **[すべて (All)]**: アカウントで使用可能なすべてのターゲットがこの組織に含まれます。
6. **[作成 (Create)]** をクリックして、新しい組織をアカウントに追加します。

組織の詳細と、アカウントでマルチテナントをサポートするためにそれらを活用する方法については、[ヘルプ センター（Help Center）]の [リソース（Resources）] の下にあるロールベースのアクセス コントロールを参照するか、 <*https://your fqdn.com*>/help を参照してください。

API キーの生成と管理

API キーを使用して、Cisco Intersight にアプリケーションを登録します。

ステップ 1 アカウント管理者ロールを持つユーザーとして Cisco Intersight 仮想アプライアンスにログインします。

ステップ 2 **[サービス セレクタ（Service Selector）]** ドロップダウン リストから **[システム（System）]** を選択し、**[設定（Settings）]** > **[API]** > **[API キー（API Keys）]**に移動します。

ステップ 3 [新しい API キーの生成（Generate）] 画面で、API キーの目的を入力して [生成（Generate）] をクリックします。API キー ID と RSA 秘密キーが表示されます。

ステップ 4 秘密キーの情報を *.pem* ファイルに保存します。

（注） スクリプトからアクセス可能な場所に保存してください。

OAuth2トークン

アプリケーションで使用される OAuth2 トークンのリストを表示して、[API] の [OAuth2] セクションで Intersight や対応するターゲットの詳細にアクセスできます。

ステップ 1 アカウント管理者ロールを持つユーザーとして Cisco Intersight 仮想アプライアンスにログインします。

ステップ 2 **[サービス セレクタ（Service Selector）]** ドロップダウン リストから **[システム（System）]** を選択し、**[設定（Settings）]** > **[API]** > **[OAuth2 トークン（OAuth2 Tokens）]** に移動します。

トークンを使用するアプリケーション名、デバイス モデル、ログインと有効期限、クライアント IP アドレス、ユーザー ロール、および電子メール ID を使用する OAuth2 トークンのテーブル ビューが表示されます。

デバイス コネクタの要件

組み込みデバイス コネクタを介してデバイスを Cisco Intersight 仮想アプライアンス で要求できます。ターゲットを要求する前に、デバイスコネクタの要件が満たされていることを確認します。次の表に、Intersight 仮想アプライアンスのソフトウェア互換性とサポートされているデバイス コネクタを示します。

表 *12*：デバイス コネクタの要件

コンポーネント	接続型仮想アプライアンスの最小ソフトウェア バージョン	プライベート仮想アプライアンスの最小ソフトウェア バージョン	サポートされているデバイスコネクタのバージョン	サポートされているデバイスコネクタを含む最小サポートバージョン
Cisco UCS Manager	3.2(1)	4.0(2a)	1.0.9-2290	4.0(2a)
Cisco IMC ソフトウェア	M5 サーバーの場合：3.1(3a) M4 サーバーの場合：3.0(4)	4.0(2d)	1.0.9-335	4.0(2d)

コンポーネント	接続型仮想アプライアンスの最小ソフトウェア バージョン	プライベート仮想アプライアンスの最小ソフトウェア バージョン	サポートされているデバイスコネクタのバージョン	サポートされているデバイスコネクタを含む最小サポートバージョン
HyperFlex Connect およびデータ プラットフォーム	2.6	3.5(2a)	1.0.9-1335	3.5(2a)
Cisco UCS Director	6.7.2.0	6.7.2.0	1.0.9: 911	6.7.2.0

デバイス コネクタのアップグレード

エンドポイント上のデバイス コネクタのバージョンに互換性がない場合は、次の方法でアップグレードできます。

- サポートされているデバイス コネクタが搭載されているバージョンにファームウェアの完全アップグレードを実行します。このプロセスには、構成設定の更新が含まれていることがあります。
- デバイス コネクタを手動でアップグレードします。このオプションは、Cisco UCS Manager のみでサポートされています。詳細については、「デバイス コネクタの手動アップグレード（Cisco UCS ファブリック インターコネクトにのみ適用）」を参照してください。
- Cisco Intersight 仮想アプライアンス クラウドからのデバイス コネクタのアップグレードをサポートしています。ターゲットの要求プロセスで、エンドポイントのデバイスコネクタのバージョンに互換性がないことが検出されると、Intersight Cloud からのデバイスコネクタのアップグレードがトリガーされます。このアップグレードを容易にするには、ポート 80 をアプライアンスとエンドポイントターゲット間で開く必要があります。ポート 80 で実行されている HTTPS プロキシは、ファイアウォールの設定でポート 80 を介して通信できる必要があります。

  Intersight クラウドからのデバイス コネクタのアップグレードはオプションです。クラウドからのアップグレード時に、アプライアンスからの一部のターゲット データ（サーバー インベントリ）が施設から離れます。このオプションを選択すると、次のデータが施設から離れます。

  - エンドポイント ターゲット タイプ：Cisco UCS ファブリック インターコネクト、Integrated Management Controller、Cisco HyperFlex System、Cisco UCS Director
  - エンドポイントのファームウェア バージョン
  - エンドポイント ターゲットのシリアル番号
  - エンドポイントターゲットの IP アドレス
  - エンドポイントターゲットのホスト名
  - エンドポイント デバイス コネクタのバージョンと公開キー

注目 ターゲットコネクタがアプライアンスをサポートしていない古いバージョンであり、初期セットアップ時にデータ収集オプションを無効にした場合は、デバイスの要求が失敗することがあります。1 回限りのアップグレードが機能するように施設から離れる必要があるエンドポイントの詳細によってこの障害が引き起こされます。ターゲットの要求が失敗しないようにするには、[データ収集の有効化（Enable Data Collection）] オプションを一時的に選択するか、または前述の他の方法でデバイス コネクタをアップグレードします。

デバイス コネクタの手動アップグレード（Cisco UCS ファブリック インターコネクトにのみ適用）

ターゲットコネクタの自動アップグレードの一環としてデバイスデータを共有しない場合は、Cisco UCS ファブリック インターコネクトのデバイス コネクタを手動でアップグレードすることができます。デバイス コネクタをアップグレードするには、次の手順を実行します。

```
Log in to your UCS Fabric Interconnect as an admin user and run the following command:
UCS-A# connect local-mgmt
UCS-A(local-mgmt)# copy scp://username@10.100.100.100/filepath/filename.bin workspace:/
UCS-A(local-mgmt)# update-device-connector workspace:/filename.bin
Update Started
Updating Device Connector on local Fabric interconnect
Successfully updated device connector on local Fabric interconnect
UCS-A(local-mgmt)#
```

Intersight 接続型仮想アプライアンスから収集されたデータ

Cisco Intersight 接続型仮想アプライアンスは接続モードで動作し、ホストされている Intersight サービスへの接続が必要です。Intersight にアプライアンスを登録し、UCS または HyperFlex のインフラストラクチャを管理する必要があります。

追加情報の収集を許可するオプションを有効にすると、**収集された最小データ**の表に一覧表示されているものを超えて、Intersight は管理対象システムに関するその他の詳細情報を収集することができます。アプライアンス UI の [**セキュリティおよびプライバシー（Security & Privacy）**] にある [**データ収集（データ収集）**] オプションのいずれかが有効になっている場合、シスコは、診断および予防的なトラブルシューティングの目的で、より多くのデータを収集する権利を保有します。

次の表に、Intersight で収集されるデータの詳細を示します。

表 *13 :* 収集された最小データ

コンポーネント	収集したデータの詳細
Intersight 仮想アプライアンスから	• アプライアンス ID（シリアル番号） • アプライアンスの IP アドレス • アプライアンスのホスト名 • アプライアンス上のデバイス コネクタのバージョンと公開キー
アプライアンス ソフトウェアの自動アップグレード	ソフトウェア コンポーネントまたはアプライアンス上で実行しているサービスのバージョン
アプライアンスの健全性	• CPU 使用率 • メモリ使用率 • ディスク使用量 • サービスの統計情報
ライセンス	サーバー カウント
エンドポイントターゲットに関する情報	• シリアル番号と PID（接続されている TAC に対応するため） • UCS ドメイン ID • プラットフォームタイプ

表 *14*：ワンタイム デバイス コネクタのアップグレード中に収集されたデータ

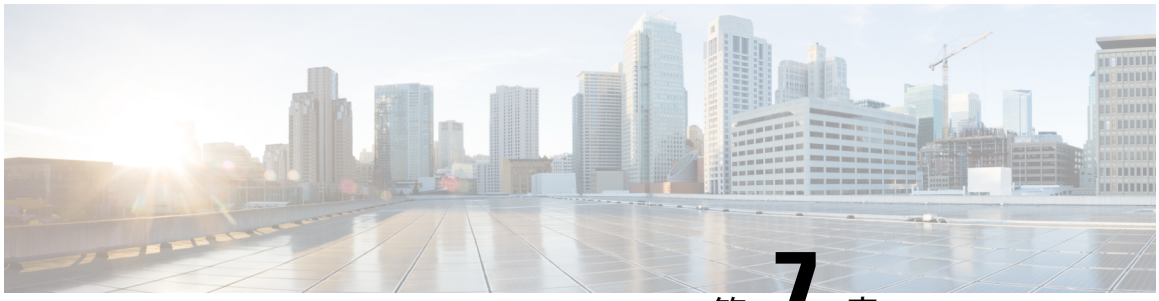
コンポーネント	収集したデータの詳細
エンドポイント ターゲットから（1 回限りのデバイス コネクタのアップグレードを使用する場合のみ）	• エンドポイント ターゲット タイプ：Cisco UCS ファブリック インターコネクト、Integrated Management Controller、Cisco HyperFlex System • エンドポイントのファームウェア バージョン • エンドポイント ターゲットのシリアル番号 • エンドポイントターゲットの IP アドレス • エンドポイントターゲットのホスト名 • エンドポイント デバイス コネクタのバージョンと公開キー

プロアクティブ サポートの詳細については、「Intersight を介して有効化されるプロアクティブ サポート」を参照してください。

プロアクティブサポートワークフロー、サポートの対象となる障害、詳細オプションの設定、プロアクティブ RMA のオプトアウトの詳細については、「Proactive RMA for Intersight Connected Devices」を参照してください。

テクニカル サポートの診断ファイル収集

Cisco TAC でケースをオープンすると、Intersight はテクニカル サポートの診断ファイルを収集して、オープン サポート ケースを支援します。収集されたデータには、ハードウェア テレメトリ、システム設定、および TAC ケースのアクティブなトラブルシューティングに役立つその他の詳細情報が含まれることがあります。指定したデータ収集オプションに関係なく、テクニカル サポートの収集が実行されます。ただし、この情報は任意で収集されるわけではありませんが、システムに対してケースをオープンする場合に限り、システム サポートの支援が必要になります。



第 7 章

診断

Intersight 仮想アプライアンスおよび Intersight Assist のメンテナンスシェル

Cisco Intersight 仮想アプライアンスは、インストールをモニタし、アプライアンスを正常にインストールするための修復手順を提供する診断ユーティリティを提供します。このコンソールベースのユーティリティは、アプライアンスのインストール中の設定ミスやネットワークの問題のトラブルシューティングと対処で役立ちます。メンテナンス シェルの目的は次のとおりです。

- インストールの前提条件に関する問題を検出して表示します。
- アプライアンスの展開時に提供される入力の編集を有効にします。
- アプライアンスの展開時に設定を修正した後、または入力を変更した後、インストールの続行をサポートします。

VM の電源がオンになった後、<*https://fqdn-of-your-appliance*>にアクセスして、インストールのステータスを確認します。電源がオンになってから約 15 分後に VM が応答しないことに気づいた場合は、Intersight 仮想アプライアンス メンテナンス シェルを使用して、ネットワーキングまたは設定ミスの問題をトラブルシューティングしてください。ログインプロンプトが表示されたら、診断アカウントの準備ができています。トラブルシューティングを行うには、次の手順を実行します。

1. 次の 3 つのオプションのいずれかを使用して、Intersight 仮想アプライアンス メンテナンス シェルを起動します。
   - ハイパーバイザでコンソール ウィンドウを開きます。
     1. VMWare vCenter または Microsoft Hyper-V Manager から、仮想マシンに移動し、コンソール ウィンドウを開きます。

2. ユーザー名に **admin** を使用して管理ユーザーとしてログインし、アプライアンス展開時に使用した管理者パスワードを入力します。

- SSH セッションを開始します。
  1. Intersight 仮想アプライアンスの IP アドレスに SSH 接続します。
  2. ユーザー名に **admin** を使用して管理ユーザーとしてログインし、アプライアンス展開時に使用した管理者パスワードを入力します。

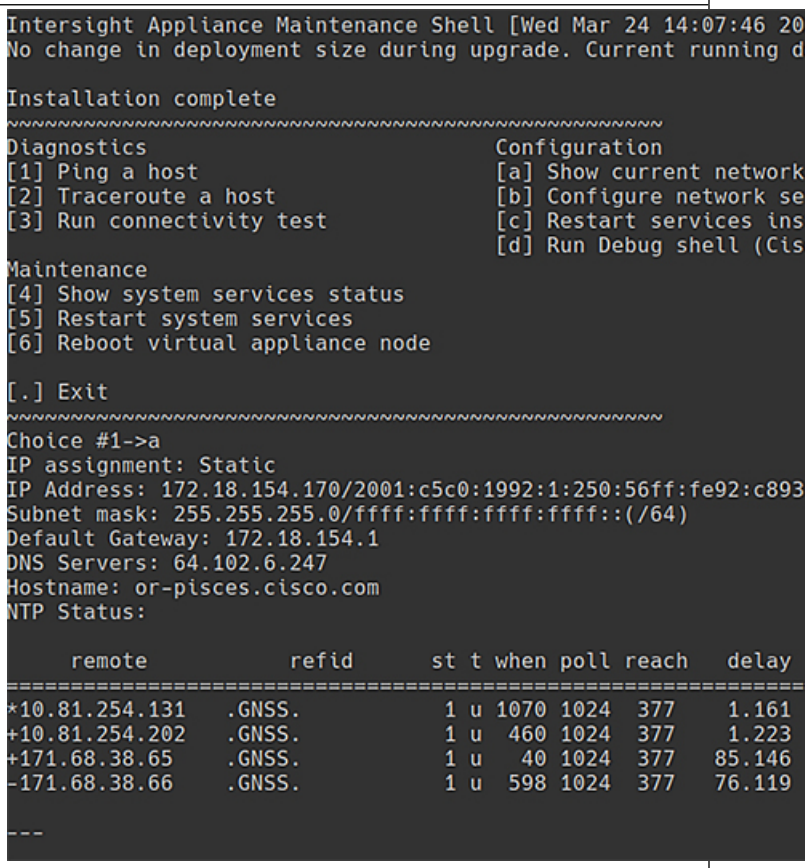
- シリアル コンソールへの Telnet セッションを開きます。
  1. Intersight 仮想アプライアンスへの SSH セッションを開くことができない場合は、「シリアル コンソールを使用した Cisco TAC Support の構成」で説明されている情報を使用して、Intersight 仮想アプライアンス VM にシリアルコンソールを追加します。
  2. シリアル コンソールのセットアップで指定された PORT_NUMBER の vCenter ホスト IP に Telnet 接続します。
  3. ユーザー名に **admin** を使用して管理ユーザーとしてログインし、アプライアンス展開時に使用した管理者パスワードを入力します。

2. コマンドの詳細とコマンドの結果については、次の表に示すオプションのいずれかを選択してください。

Intersight アプライアンス メンテナンス シェルのオプション	**説明**
診断オプション	• **[1] [ホストに ping を送信する (ping a host)]**：このオプションを使用すると、ホストにpingを送信して、すべてのプロパティと要件が正しく入力された後でもインストールが失敗した理由を確認できます。 • **[2] [ホストをトレースルート (Traceroute a host)]**: このオプションは、ホストが通過したすべてのIPアドレスを表示します。 • **[3] [接続テストの実行 (Run connectivity test)]**: このオプションは、接続テストを実行し、ホストからDNSサーバーへのパスにあるすべてのホストにpingを実行します。このツールは、IPアドレスが有効かどうかを確認するためのいくつかのテストを実行し、重複したIPをチェックして、複数のインスタンスで使用されているかどうかを確認します。[接続テストの実行 (Run connectivity test)] オプションが DNS サーバーに到達し、接続の問題を解決します。

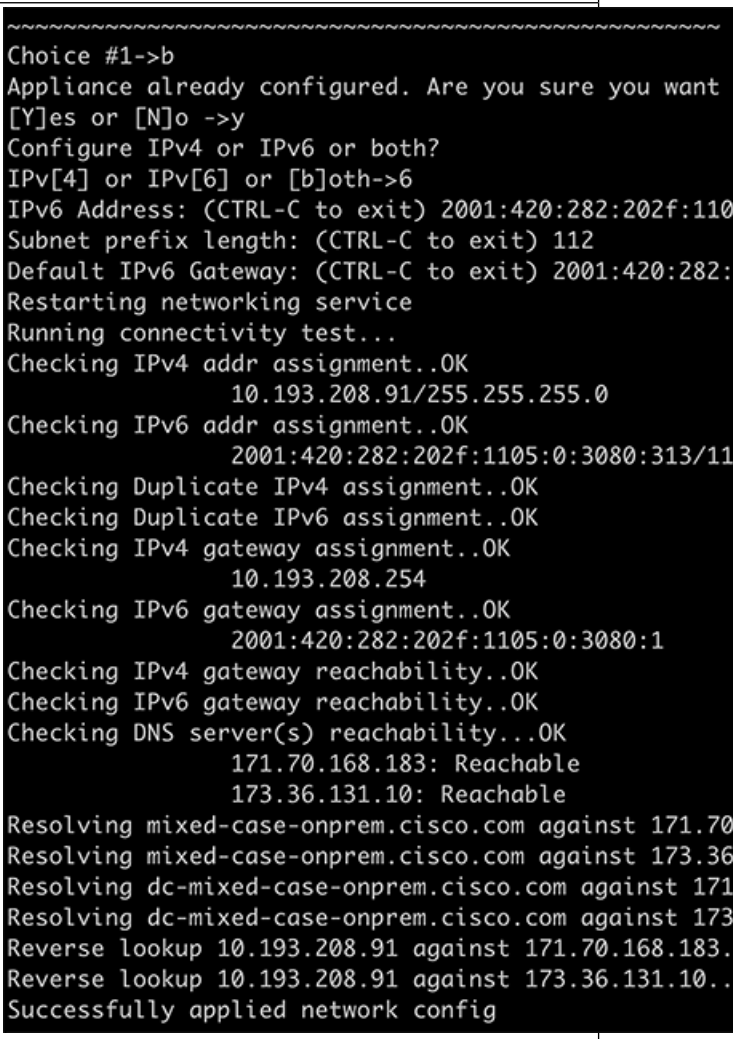
Intersight アプライアンス メンテナンス シェルのオプション	説明
設定オプション	

Intersight アプライアンス メンテナンス シェルのオプション	説明
	• **[a] [現在のネットワーク設定の表示 (Show current network configuration)]**：このオプションは、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 サーバー、ホスト名、および DNS 接続ステータス（NTP Servers、、NTP サーバーなどの既存の設定を表示し、すべての設定が正しく入力されていることを確認するために役立ちます。接続のステータスを確認するには、接続テスト (**オプション 3**) を実行します。

Intersight アプライアンス メンテナンス シェルのオプション	説明
	

Intersight アプライアンス メンテナンス シェルのオプション	説明
	• **[b] [ネットワーク インターフェイス プロパティの設定 (set network interface properties)]**：このオプションは、設定したネットワークインターフェイスのプロパティを表示します。**[Enter]** をクリックすると、既存のプロパティを保持したり、異なる入力セットを指定したりできます。このオプションは、次のプロパティを使用して問題 (存在する場合) を検出します。 • **[IP アドレスが無効または重複 (An invalid or duplicate IP address)]**：正しいクレデンシャルを使用してホスト名を設定している場合でも、IPアドレスが間違っている可能性があります。 • **[無効なサブネットマスク (Invalid subnet mask)]**: 無効なサブネットマスクでは自身のネットワーク内を移動することができますが、外部トラフィックに影響を与える可能性があります。 • **[不正または無効なデフォルト ゲートウェイ (Incorrect or invalid Default Gateway)]**： DNS サーバーがネットワークの外部にある場合、無効なデフォルト ゲートウェイは外部ホストへの接続に影響します。 **[IP アドレスの変更 (Changing IP Address)]**：このオプションを使用すると、**管理**ユーザー (ユーザー名 **admin**) によって次の変更が可能になります。 • 同じネットワーク上に新しいIPアドレスを割り当て、アプライアンス VM を別のネットワークに接続し、そのネットワーク上にIPを割り当てます。 • 別の vCenter または Hyper-V Manager 展開に移行した後、アプライアンス VM の IP アドレスを変更します。 **注目** 変更が開始される前に DNS サーバー レコード (A、CNAME、および PTR) が更新され、新しい IP アドレスが以前と同じ FQDN に対して解決されることを確認する必要があります。 IPv4アドレスのみを変更するか、IPv6アドレスを変更するか、または両方を同時に変更するかを選択できます。 IPv6アドレスは、アプライアンスが完全に

Intersight アプライアンス メンテナンス シェルのオプション	説明
	インストールされた後にのみ設定できます。IPv6アドレスを変更した後は、アプライアンスのサービスでダウンタイムは発生しません。アプライアンスVM自体は、最初に導入されたときにアプライアンスのIPv4アドレスに割り当てられたDNS名で引き続き管理されます。IPv6アドレスを設定すると、IPv6エンドポイントのターゲット要求のみが有効になります。 IP の変更には最大 15 分かかる場合があります。この間、アプライアンス VM を再起動しないことを推奨します。約 15 分待機した後、UI からアプライアンスに再度ログインします。 

Intersight アプライアンス メンテナンス シェルのオプション	説明
	 • **マルチノードのみの場合**：マルチノードクラスタ内のノードの IPv4 アドレスを変更する方法の詳細については、「マルチノードクラスタ内のノードの IPv4 アドレスを変更する」を参照してください。

Intersight アプライアンス メンテナンス シェルのオプション	説明
	• **[c] インストール サービスの再起動** このオプションは、すでに動作していると想定されていたネットワークの設定を修正する場合に役立ちます。たとえば、次のものがあります。 • 選択した IP の PTR レコードが欠落しています (静的 IP 割り当て)。 • VM が誤った portgroup/vSwitch に接続されています。 • DHCP 経由で IP 割り当てを選択した場合、DHCP サーバーが動作しません。 • インストールの進行状況を確認するには、URL <*fqdn-of-your-appliance-vm*> にアクセスします。 • **[d] 実行デバッグ (認証が必要) (Run Debug (requires authentication))]**：**このユーティリティは、Cisco TAC がインストールの問題をトラブルシューティングする場合にのみ使用します。** • **[e] ログインバナーの設定**：このオプションを使用すると、新しいバナーメッセージを設定したり、ログイン画面の前に表示される既存のバナーメッセージを編集したりできます。

Intersight アプライアンス メンテナンス シェルのオプション	説明
メンテナンンス オプション	このオプションを使用すると、アプライアンス VM をグレースフル リブートし、アプライアンス サービスを再起動することができます。**このサブメニューのオプションはデバッグとリカバリを目的としており、Cisco TAC の指示に従って使用する必要があります。**このオプションには**管理者**ユーザーとしてアクセスできます。 **[4] [システム サービス ステータスの表示 (Show system service status)]**: このオプションは、実行中/保留中のサービスの概要を提供し、エラーを報告します。このオプションを使用すると、システムが応答しない場合やサービスの中断が発生した場合にはいつでも、アプライアンスのステータスをモニタできます。 **[5] [システム サービスの再起動 (Restart system services)]**：このオプションでアプライアンスのトラブルシューティングを行い、実行中のサービスを再起動することができます。 **[6] [仮想アプライアンス ノードの再起動 (Reboot virtual appliance node)]**：このオプションは、サービスを停止し、アプライアンスを再起動し、アプライアンスが再起動したときにサービスを復元します。

Intersight 仮想アプライアンス インストールおよびトラブルシューティングのデモンストレーションについては、『Cisco Intersight アプライアンスおよびデバッグ』をご確認ください。

仮想アプライアンスのサイズ オプションのモニタリング

Intersight アプライアンス メンテナンス シェルは、展開サイズの決定と後続のアクションに関するステータスの更新を表示します。コンソールで展開のステータスをモニタし、必要に応じて修正措置を取ることができます。次の表に示すメッセージは、展開のシナリオと特定のリソース要件について説明しています。

初期メッセージ	最終メッセージ
<サイズ>の展開サイズをインストールします。 このメッセージは、必要なリソースが十分であり、目的のサイズが展開されている場合に表示されます。 （注） リソース要件を評価した後、小規模、中規模、大規模または中程度のオプションで展開することを選択できます。	**<サイズ>の展開サイズをインストールしました。**

初期メッセージ	最終メッセージ
<サイズ>の展開サイズをインストールします (リソース提供後)。 このメッセージは、既存の展開が現在の展開サイズに対してリソースを使用している場合、および必要なリソースが追加された後に VM を再起動した場合に表示されます。この展開はどちらのサイズでもかまいません。	**<サイズ>の展開サイズをインストールしました (リソース提供後)。**
<サイズ>の展開サイズをインストールしました。 このメッセージは、既存のリソースと必要なリソースが類似しており、アップグレードが不要な場合に表示されます。	**再起動中に展開サイズの変更はありません。現在実行中の展開サイズは小さくなります。**
展開サイズを中規模から小規模にダウングレードします。 このメッセージは、中規模の展開のサイズが小規模にダウングレードされた場合に展開されます。	**ダウングレードされた展開サイズ (中から小)。**
展開サイズのアップグレード (小から中)。 このメッセージは、展開サイズが小規模から中規模にアップグレードされた場合に表示されます。	**展開サイズが小規模から中規模にアップグレードされました。**

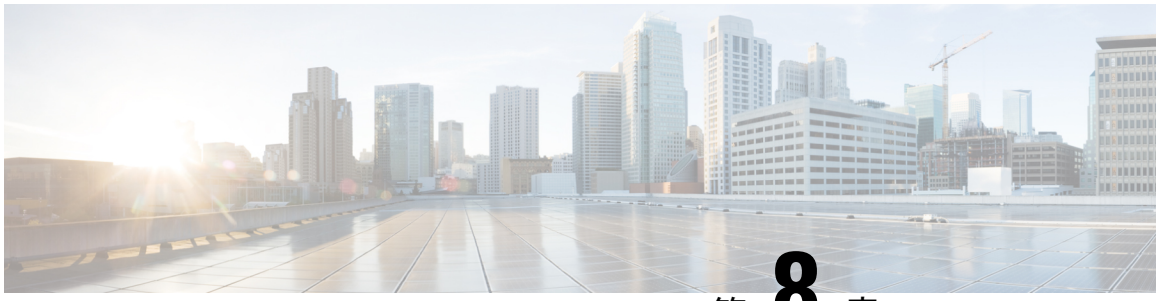
コンソール メッセージ

Intersight 仮想アプライアンスおよび Intersight Assist のインストール中または通常の操作中に、コンソールに次のようなメッセージが表示されることがあります。メッセージの正確な内容は、状況によって異なります。

```
kernel:NMI watchdog: BUG: soft lockup - CPU#0 が 36 秒間スタックします。
[watchdog/0:11]
```

これらのメッセージは、ハイパーバイザが VM の「スナップショット」を作成している場合や、ハイパーバイザホストのリソースが制約されている場合など、Intersight 仮想アプライアンスまたは Intersight Assist がハイパーバイザによって部分的または完全に一時停止されている場合に表示されます。Intersight 仮想アプライアンスと Intersight Assist は、これらのメッセージが存在する場合でも正常に動作し続けます。

このようなメッセージが特に短期間に多数発生する場合は、ハイパーバイザ環境を調査して根本原因を特定することを強くお勧めします。



第 8 章

テクニカルサポートおよびフィードバック

テクニカル サポート

Cisco Technical Assistance Center（TAC）が提供するテクニカル サポートは Essentials のライセンスに含まれています。Cisco Intersight 仮想アプライアンスのインストール、セットアップ、または操作に関する問題については、Cisco TAC でケースをオープンし、サポートを受けてください。

シスコ テクニカル サポートの Web サイトでは、シスコの製品およびテクノロジーに関する技術上の問題のトラブルシューティングや解決に役立つオンライン ドキュメントやツールを提供しています。

http://www.cisco.com/techsupport

TAC Support Case Manager オンライン ツールを利用することで、最も素早く S3 および S4 のサポート ケースを開くことができます（S3 および S4 のサポート ケースは、最小限のネットワーク障害の問題と製品情報要求から構成されます）。状況を説明すると、TAC Support Case Manager が推奨する解決方法を自動的に提供します。推奨リソースを使用しても問題を解決できなかった場合、TAC Support Case Manager はそのサポート ケースを Cisco TAC のエンジニアに割り当てます。以下の場所から、TAC Support Case Manager にアクセスできます。

https://mycase.cloudapps.cisco.com/case

S1 または S2 のサポート ケースに関して、またはインターネット アクセスがない場合は、電話で Cisco TAC にご連絡ください（S1 または S2 のサポート ケースはサービスの低下や停止など、製品ネットワークの問題で構成されます）。S1 および S2 のサポート ケースには Cisco TAC のエンジニアがすぐに割り当てられて、事業運営を円滑に続行できるようにします。

電話でサポート ケースを開く場合は、次のいずれかの電話番号をご利用ください。

· アジア太平洋地域：+61 2 8446 7411

· オーストラリア：1 800 805 227

· EMEA：+32 2 704 5555

· 米国：1 800 553 2447

エンタープライズ製品とサービス プロバイダー製品の Cisco TAC のな連絡先の詳細なリストについては、http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html を参照してください。

Cisco Small Business Support Center（SBSC）の連絡先の詳細なリストについては、http://www.cisco.com/c/en/us/support/web/tsd-cisco-small-business-support-center-contacts.html を参照してください。

Intersight 仮想アプライアンスから直接 TAC ケースを開く

セットアップが完了してターゲットを要求した後、**[サーバの詳細 (Server Details)]** ページから Cisco Support Case Manager を起動することによって、Cisco Intersight 仮想アプライアンスから Cisco TAC Service Request (SR) を直接作成できます。ケースをオープンする前に、次の要件を満たしていることを確認してください。

- ハードウェアに有効なサービス契約（権限付与）が存在している。
- Cisco ID がサービス契約に関連付けられている。

（注） Cisco Technical Assistance Center（TAC）にアクセスしてサービスリクエストを作成できるように、ブラウザをインターネットに接続する必要があります。

Cisco Intersight 仮想アプライアンスから Cisco TAC ケースを直接開くには、次の手順を実行します。

1. アプライアンス UI で、**サーバー** テーブル ビューからサーバーを選択します。
2. または、選択したサーバーの省略記号（**...**）ボタンをクリックし、**[TAC ケースを開く (Open TAC Case)]** を選択することもできます。

   選択したサーバーまたはファブリック インターコネクトの名前とシリアル番号が含まれた **[TAC ケースを開く(Open a TAC Case)]** ウィンドウが表示されます。
3. **[続行（Continue）]** をクリックして Cisco Support Case Manager を起動します。
4. Cisco Support Case Manager の UI から、自動的に挿入されたケースの詳細を確認し、TAC ケースの説明とタイトルを追加し、**[送信（Submit）]** をクリックします。

Intersight 仮想アプライアンスからのテクニカルサポートバンドルの収集

アプライアンスのセットアップを完了し、ターゲットを要求した後、アプライアンスに要求された Intersight 仮想アプライアンスとターゲットの技術サポート バンドルを収集し、それを Cisco TAC サービスリクエスト（SR）に添付できます。Cisco UCS ファブリック インターコネクトおよび接続された UCS B、C、S シリーズ サーバー、Cisco UCS C シリーズ スタンドアロ

ン サーバー、Cisco HyperFlex クラスタ、および Cisco UCS Director から技術サポートバンドルを収集できます。

アプライアンスに要求されたターゲットのテクニカル サポート バンドルを収集しするには、次の手順を行います。

1. 次のいずれかのロールを持つユーザーとして、アプライアンスにログインします。
   - アカウント管理者
   - サーバー管理者
   - Hyperflex 管理者
2. アプライアンス ダッシュボードから、技術サポート バンドルを収集するターゲットに移動します。
   - **[サーバ（Servers）]**、**[ファブリック インターコネクト（Fabric Interconnects）]**、および **[UCS Director]** の場合、選択する省略記号（**...**）ボタンをクリックし、**[技術サポート バンドルの収集（Collect Tech Support Bundle）]** を選択します。
   - **Hyperflex クラスタ**の場合、クラスタとクラスタに対応するノードを選択した後、選択する省略記号（**...**）ボタンをクリックし、**[技術サポート バンドルの収集（Collect Tech Support Bundle）]** を選択します。

（注） Cisco Technical Assistance Center（TAC）でサービスリクエストを作成する際に、クラスタ内のすべてのノードに技術サポートバンドルを提供する必要がある場合があります。

3. 生成が完了したら、**[サービス セレクタ]** ドロップダウン リストから **[システム]** を選択し、**[管理（Administration）]** > **[技術サポート バンドル（Tech Support Bundles）]** に移動し、ターゲットの技術サポート バンドルをダウンロードします。

アプライアンスの技術サポート バンドルを収集するには、次の手順を実行します。

1. 次のいずれかのロールを持つユーザーとして、アプライアンスにログインします。
   - アカウント管理者
   - サーバー管理者
   - Hyperflex 管理者
2. **[サーバー セレクタ（Service Selector）]** ドロップダウン リストから **[システム（System）]** を選択し、**[管理（Admin）]** > **[技術サポート バンドル（Tech Support Bundles）]**に移動します。
3. [技術サポート バンドル（Tech Support Bundle）] ページの **[アプライアンス技術サポート バンドルの収集（Collect Appliance Tech Support Bundle）]** をクリックします。

生成が完了したら、アプライアンスの技術サポート バンドルをダウンロードできます。

これで、Cisco Support Case Manager に進み、サービスリクエストを作成できます。

シリアル コンソールを使用した Cisco TAC Support の構成

Intersight 仮想アプライアンスがネットワーク上の SSH 経由で到達不能になり、Cisco TAC サポートが必要な場合、VMWare リモートコンソール（VMRC）を介してアプライアンスで Cisco TAC サポートモードを有効にすることはできません。したがって、アプライアンス仮想マシンにシリアルポートデバイスを追加する必要があります。このシリアル ポートを使用すると、Cisco TAC は、お客様の支援を受けて Intersight 仮想アプライアンスに接続し、Cisco TAC サポート モードを開始できます。

（注） シリアル コンソールのサポートは、Intersight 仮想アプライアンス バージョン 1.0.9-589 以降でのみ使用できます。

アプライアンス仮想マシンにシリアル ポート デバイスを追加するには、次の手順を実行します。

1. Intersight 仮想アプライアンス仮想マシンが実行されている VMWare vSphere ホストで、次の手順を実行します。
   1. **[構成（Configuration）]** タブを選択します。
   2. **[システム（System）]** グループで、**[ファイアウォール（Firewall）]** を選択します。
   3. **[編集（Edit）]** ボタンをクリックして、ファイアウォール ルールを編集します。
   4. *VM serial port connected over network* という名前のルールが有効になっていることを確認します。
      - ステップ 3.c（ポート URI）でこのポート範囲を入力する必要があるため、このルールで許可される TCP ポートの範囲（23 および 1024 ～ 65535 など）に注意してください。
      - 必要に応じて、ファイアウォール ルールで指定された送信元 IP アドレスのみを許可します。
   5. このルールを保存します。
2. Intersight 仮想アプライアンス仮想マシンの電源を切ります。
3. Intersight 仮想アプライアンス仮想マシンの vSphere 設定を編集します。
   1. **[デバイスの追加（Add Device）]** を選択します。
   2. **[その他のデバイス（Other Devices）]** で、**[シリアル ポート（Serial Port）]** を選択します。

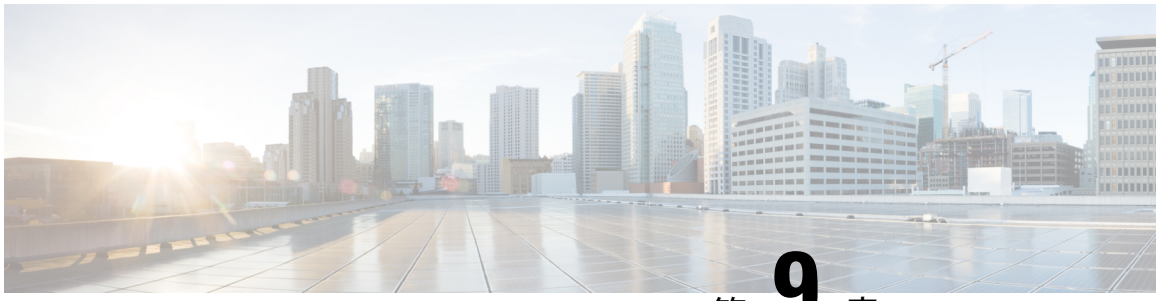
3. 新しいシリアル ポートで次の設定を選択します。
    1. 新しいシリアル ポート： ネットワークの使用
    2. [ステータス（Status）]：*[*パワーオン時に接続（*Connect at Power On*）*]* チェックボックスをオンにします。
    3. 方向：サーバー
    4. ポート URI： *telnet://:PORT_NUMBER*。PORT_NUMBER は、ステップ 1 で有効にしたファイアウォール ルールで許可された範囲内にある vCenter ホスト上の使用可能なポートを表す整数です（例：12345）。
    5. この新しいデバイスを保存します。
4. Intersight 仮想アプライアンス仮想マシンの電源を切ります。

これで、指定したポート（例：12345）で vCenter ホストの IP アドレスに Telnet 接続し、Intersight 仮想アプライアンスのログイン プロンプトに接続できるようになります。Cisco TAC は、画面共有セッションを介してこの接続を使用して、アプライアンスで Cisco TAC サポートモードを有効にして、その機能を回復できます。

フィードバックの送信

（注） この機能は、Intersight 接続型仮想アプライアンスの展開にのみ適用されます。

アプライアンス UI からの Cisco Intersight 仮想アプライアンスでのエクスペリエンスのフィードバックを共有できます。アプライアンス ダッシュボードの **[ヘルプ（Help）]** ドロップダウン リスト（疑問符のマーク）をクリックし、**[フィードバックを送信（Send Us Feedback）]**を選択します。エクスペリエンスの評価または問題の報告を行ったり、機能の向上に関するコメントを残すことができます。



第 9 章

関連資料

関連ドキュメントへのリンク

• Cisco Intersight は、複数のデータ センターにまたがって Cisco UCS と Cisco HyperFlex システムを管理するクラウド ベースの RESTful API を提供します。Intersight API の詳細については、「API のドキュメント」を参照してください。

• Intersight での障害とアラームの詳細については、次を参照してください。

  • UCS の障害とエラー メッセージ

  • HyperFlex HX データ プラットフォームのイベント

管理インターフェイスでの Intersight の管理の有効化に関する詳細については、次の中から該当するガイドを参照してください。

• Cisco UCS Manager アドミニストレーション ガイド

• 『Cisco UCS C-Series Integrated Management Controller GUI Configuration Guide』

• 『Cisco HyperFlex Systems Installation Guide for Cisco Intersight』

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。