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 （16 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 と Intersight プライベート仮想アプライアンスのリカバリ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 （17 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 （14 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 （17 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 （18 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 （19 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 （24 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 （25 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 （26 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 （30 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（33 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 （35 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 （13 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 *1 : 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
Node	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 *2:* 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を中規模または大規模構成で展開し、それぞれ 5000 台または 8000 台のサーバーをサポートできます。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、[Intersight 仮想アプライアンスの情報技術要件（Resource Requirements for Intersight Virtual Appliance）]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：

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	5000	8,000
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 （26 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、[システム設定（ System > 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。

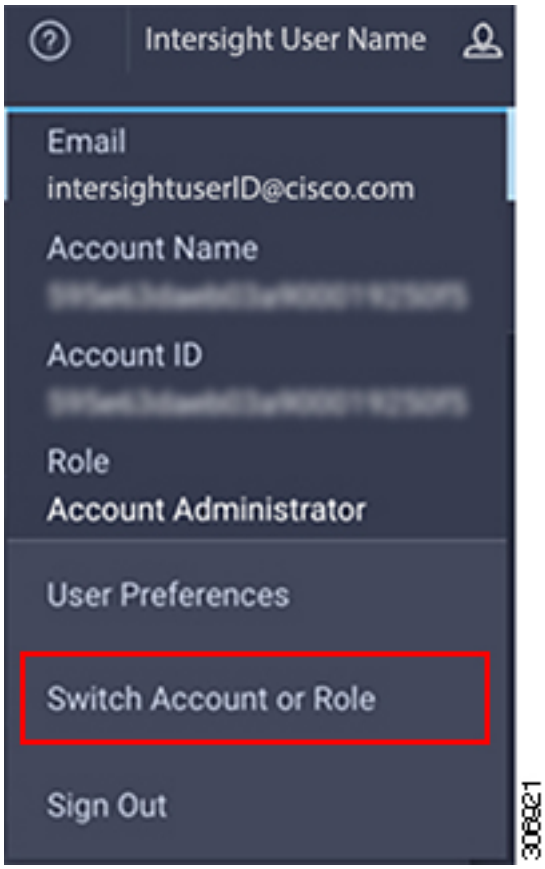
1. Cisco Intersight にログインします。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから **[システム（System）]** を選択し、**[設定（Settings）]** > **[アクセスと権限（ACCESS & PERMISSIONS）]** > **[ロール（Roles）]** に移動します。
3. **[ロール (Roles)]** で、**[ロールの作成 (Create Role)]** をクリックします。
4. **名前**を入力して、Intersight でロールを識別し、ロールの使用状況に関する**説明**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 (All)]**: 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 *3*: 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 *4:* 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 *5:* 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。

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。