初期設定の完了

初期設定ワークフロー

インストールしたすべての Cisco DNA Center アプライアンスの設定が完了したら、この章で説明するタスクを実行して、Cisco DNA Centerを実稼働に使用する準備をします。次の点に注意してください。

- この作業を完了するために必要なパラメータ情報については「必要な初期設定情報」を参照してください。
- 実稼働環境にハイアベイラビリティ（HA）を展開している場合、HA の動作を最適化するためにクラスタノード間でサービスを再配布する必要もあります（「サービスの再配布」を参照）。アプライアンスの SNMP 設定を行った後、この手順を完了します。

互換性のあるブラウザ

Cisco DNA Center の GUI は次の HTTPS 対応ブラウザと互換性があります。

- Google Chrome：バージョン 62.0 以降。
- Mozilla Firefox：バージョン 54.0 以降。

Cisco DNA Center へのログインに使用するクライアント システムは、64 ビット オペレーティング システムとブラウザを装備していることが推奨されます。

初回ログイン

Cisco DNA Center アプライアンスをインストールして設定した後、Web ベースの GUI にログインできます。Cisco DNA Center にアクセスする際には、互換性のある HTTPS 対応ブラウザを使用してください。

スーパーユーザ権限を持つ管理者（`admin` というユーザ名、スーパー管理者ロール（SUPER-ADMIN-ROLE）が割り当てられている）として初めてログインする場合、システムセキュリティを強化し、基本的なセットアップタスクを完了するのに役立つ、初回セットアップウィザードを完了するように求められます。ウィザードの各ステップを省略することは可能ですが、システムをできるだけ早く使用できるようにするため、指示どおりにすべてのステップを完了することをお勧めします。

また、新しいCisco DNA Centerユーザを作成する必要があります。毎日の操作で使用する追加のユーザアカウントを少なくとも 1 つ作成し、このユーザアカウントにネットワーク管理者ロール（NETWORK-ADMIN-ROLE）を割り当てることをお勧めします。

始める前に

Cisco DNA Center にログインして初回セットアップウィザードを完了するには、次の情報が必要です。

- 「Maglev ウィザードを使用したマスタノードの設定」または「ブラウザベースのウィザードを使用したマスタノードの設定」の手順に従って指定した「管理者」スーパーユーザのユーザ名とパスワード。
- [必要な初期設定情報（Required First-Time Setup Information）] に記載されている必要な情報。

ステップ 1 Cisco DNA Center アプライアンスのリブートが完了したら、ブラウザを起動します。

ステップ 2 **`HTTPS://`** と設定プロセスの最後に表示された Cisco DNA Center GUI の IP アドレスを使用して、Cisco DNA Center GUI にアクセスするホスト IP アドレスを入力します。

IP アドレスを入力すると、次のいずれかのメッセージが表示されます（使用しているブラウザによって異なります）。

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

ステップ 3 メッセージを無視して **[詳細設定（Advanced）]** をクリックします。

次のメッセージが表示されます。

- Google Chrome：

```
This server could not prove that it is GUI-IP-address; its security certificate is not trusted
 by your computer's
```

```
operating system. This may be caused by a misconfiguration or an attacker intercepting your
connection.
```

- Mozilla Firefox：

```
Someone could be trying to impersonate the site and you should not continue.

Websites prove their identity via certificates. Firefox does not trust GUI-IP-address because
 its certificate issuer is unknown,
the certificate is self-signed, or the server is not sending the correct intermediate
certificates.
```

こうしたメッセージが表示されるのは、コントローラが自己署名証明書を使用しているためです。Cisco DNA Center での証明書の使用方法については、『Cisco Digital Network Architecture Center 管理者ガイド』の「証明書と秘密キーのサポート」の項を参照してください。

ステップ 4 メッセージを無視し、次のいずれかを実行します。

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

[ログイン（Login）]Cisco DNA Center ウィンドウが表示されます。

ステップ 5 **[ログイン（Login）]** ウィンドウで Cisco DNA Center の設定時に設定した管理ユーザ名（admin）とパスワードを入力し、**[ログイン（Log In）]** をクリックします。

[ログインのリセット（Reset Login）] ウィンドウが表示されます。

ステップ 6 古いパスワードを入力してから、スーパーユーザ権限を持つ管理者の新しいパスワードを入力して確認し、**[保存（Save）]** をクリックします。

[Cisco.com IDの入力（Enter Cisco.com ID）] ウィンドウが表示されます。

ステップ 7 Cisco.com ユーザのユーザ名とパスワードを入力してから **[次へ（Next）]** をクリックします。

cisco.com ユーザログインが既知のどの Cisco Smart Account ユーザログインとも一致しない場合は、**[Smart Account]** ウィンドウが表示されます。

ステップ 8 **[スマートアカウント（Smart Account）]** ウィンドウが表示された場合には、組織のスマートアカウントのユーザ名とパスワードを入力するか、対応するリンクをクリックして新しいスマートアカウントを開きます。完了したら **[次へ（Next）]** をクリックします。

[IPアドレスマネージャ（IP Address Manager）] ウィンドウが表示されます。

ステップ 9 組織が外部 IP アドレスマネージャ（IPAM）を使用している場合には、次の手順を実行してから **[次へ（Next）]** をクリックします。

- IPAM サーバの名前と URL を入力します。
- サーバへのアクセスに必要なユーザ名とパスワードを入力します。
- 使用中の IPAM プロバイダー（Infoblox など）を選択します。
- Cisco DNA Center で使用する利用可能な IP アドレスの特定のビューを IPAM サーバデータベースで選択します。

[プロキシサーバの入力（Enter Proxy Server）] ウィンドウが表示されます。

ステップ 10 組織が使用するプロキシサーバ情報を入力し、**[次へ（Next）]**をクリックします。

- プロキシサーバに対するログインが必要な場合には、サーバのユーザ名とパスワードを含めます。
- 続行する前にこの情報を検証する（推奨）場合には、**[設定の検証（Validate Settings）]** チェックボックスがオンになっていることを確認します。

ソフトウェアの **[EULA]** ウィンドウが表示されます。

ステップ 11 **[次へ（Next）]** をクリックして、ソフトウェアのエンドユーザライセンス契約書に同意します。

[準備完了（Ready to go!）] ウィンドウが表示されます。

ステップ 12 このウィンドウでいずれかのリンクをクリックするか、[システム360に移動（Go To System 360）] をクリックして [システム360（System 360）] ダッシュボードを表示することにより、Cisco DNA Center の使用を開始できます。

シスコでは、[ユーザ管理（User Management）] リンクをクリックして、[ユーザ管理（User Management）] ウィンドウを表示することを推奨しています。**[追加（Add）]** をクリックして、新しい Cisco DNA Center ユーザの追加を開始します。新しいユーザの名前とパスワードを入力し、ユーザのロールを選択したら、**[保存（Save）]** をクリックして新しいユーザを作成します。初期展開の新しいユーザすべてが追加されるまで、必要に応じてこの手順を繰り返します。ネットワーク管理者ロール（NETWORK-ADMIN-ROLE）を持つユーザを少なくとも 1 人作成してください。

次のタスク

残りの管理設定タスクを任意の順序で実行します。

- Cisco ISE との統合 Cisco DNA Center
- 認証サーバとポリシー サーバの設定
- SNMP プロパティの設定

Cisco ISE との統合 Cisco DNA Center

このリリースの Cisco DNA Center は、Cisco ISE と信頼された通信リンクを作成するメカニズムを備えており、Cisco DNA Center は安全な方法で Cisco ISE とデータを共有できます。Cisco ISE が Cisco DNA Center に登録されると、Cisco DNA Center が検出するすべてのデバイスが、関連する設定データやその他のデータとともに Cisco ISE にプッシュされます。ユーザは Cisco DNA Center を使用してデバイスを検出し、Cisco DNA Center と Cisco ISE の両方の機能を検出したデバイスに適用できます。この理由はこれらのデバイスが両方のアプリケーションに公開されるためです。 また Cisco DNA Center デバイスと Cisco ISE デバイスはすべてデバイス名で一意に識別されます。

Cisco DNA Center デバイスは Cisco DNA Center サイト階層内の特定のサイトにプロビジョニングされて所属すると、即座に Cisco ISE にプッシュされます。Cisco DNA Center デバイスのアップデート（IP アドレス、SNMP または CLI のクレデンシャル、Cisco ISE 共有秘密情報など）はすべて、自動的に ISE 上の対応するデバイスインスタンスに使用されます。Cisco DNA Center デバイスが削除されるときは、Cisco ISE からも削除されます。Cisco DNA Center デバイスが Cisco ISE にプッシュされるのは、Cisco ISE が AAA サーバとして設定されている特定のサイトにそれらのデバイスが関連付けられている場合に限ることに注意してください。

始める前に

Cisco ISE を Cisco DNA Center と統合する前に、次の前提条件を満たしていることを確認します。

- ネットワークに 1 つ以上の Cisco ISE バージョン 2.3（以降）のホストを展開済みであること。Cisco ISE のインストールについては、Cisco Identity Services Engine のインストールガイド、アップグレードガイド（バージョン 2.3 以降用）を参照してください。
- スタンドアロン ISE 導入環境がある場合は、Cisco ISE ノード上で pxGrid サービスおよび ERS と統合し、これらを有効化する必要があります。
- 分散型 Cisco ISE 展開がある場合：
  - Cisco DNA Center を Cisco ISE 管理ノード、プライマリポリシー管理ノード（PAN）と統合し、ERS を有効にする必要があります。

    （注） PAN を介した ERS 使用がベストプラクティスです。ただしバックアップの場合は、PSN で発信をイネーブルにします。

  - 単一ノードの導入環境と同様に、分散型の導入環境内のいずれかの Cisco ISE ノード上で pxGrid サービスを有効化する必要があります。PAN 上で pxGrid サービスを有効化することを選択できますが、必須ではありません。分散型の導入環境では、他の任意の Cisco ISE ノード上で pxGrid を有効化できます。
- ポート 22、443、5222、8910、9060 で Cisco DNA Center と Cisco ISE の通信が有効になっています。
- pxGrid が有効化されている Cisco ISE ホストには、Cisco ISE eth0 インターフェイスの IP アドレス上の Cisco DNA Center から到達できる必要があります。
- Cisco ISE ノードは、アプライアンス NIC 経由でファブリック アンダーレイ ネットワークに到達できます。
- Cisco ISE ノードでは SSH が有効化されます。
- Cisco ISE 管理ノード証明書のサブジェクト名または SAN のいずれかに Cisco ISE の IP アドレスまたは FQDN が含まれます。

- Cisco DNA Center システム証明書の [サブジェクト代替名（SAN）（Subject Alternative Name（SAN））] フィールドに、Cisco DNA Center アプライアンスの IP アドレスと FQDN の両方がリストされている必要があります。

Cisco DNA Center に対応した Cisco ISE の設定の詳細については、『Cisco ISE Administrators Guide』の「*Cisco DNA Center* との統合」を参照してください。

ステップ 1 次のように Cisco ISE の pxGrid サービスと ERS を有効化します。

a) Cisco ISE のプライマリ管理ノードにログインします。

b) **[管理（Administration）]** > **[システム（System）]** > **[展開（Deployment）]** を選択します。

[展開設定（Deployment Configuration）] ウィンドウが開きます。

c) pxGrid サービスを有効化する Cisco ISE ノードのホスト名をクリックします。

分散型展開の場合、これは展開環境内の任意の Cisco ISE ノードです。

[ノードの編集（Edit Node）] ウィンドウが開き、**[General Settings（一般設定）]** タブがデフォルトで選択されています。

d) **[pxGrid]** チェックボックスがオンになっていることを確認してから、**[保存（Save）]** をクリックします。

e) **[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** の順に選択します。

f) 左側のナビゲーションウィンドウで **[ERS 設定（ERS Settings）]** をクリックして、**[ERS 設定（ERS Settings）]** ウィンドウを開きます。

g) **[読み取り/書き込み用にERSを有効化（Enable ERS for Read/Write）]** オプションボタンをクリックし、通知プロンプトで **[OK]** をクリックします。

h) **[保存（Save）]** をクリックします。

ステップ 2 次のように Cisco ISE ノードを AAA サーバとして Cisco DNA Center に追加します。

a) Cisco DNA Center GUI にログインします。

b) **メニュー**アイコン（☰）をクリックし、**[システム（System）]** > **[システム360（System 360）]** を選択します

c) [Identity Services Engine（ISE）] ペインで、**[設定（Configure）]** リンクをクリックします。

d) **[認証サーバとポリシーサーバ（Authentication And Policy Servers）]** ウィンドウで [] をクリックします。

e) **[AAA/ISEサーバの追加（Add AAA/ISE server）]** スライドインペインで、次のタスクを実行します。

- **[サーバIPアドレス（Server IP address）]** フィールドに、Cisco ISE 管理 IP アドレスを入力します。
- ネットワークデバイスと Cisco ISE の通信を保護するために使用する **[共有秘密（Shared Secret）]** を入力します。
- **[Cisco ISEサーバ（Cisco ISE Server）]** スライダをクリックして、すべての Cisco ISE 関連フィールドが表示されていることを確認します。

- 該当する Cisco ISE 管理者の CLI クレデンシャルを **[ユーザ名（Username）]** と **[パスワード（Password）]** フィールドに入力します。
- Cisco ISE ノードの **FQDN** を入力します。
- **[サブスクライバ名（Subscriber Name）]** を入力します（例：cdnacenter）。
- （任意）Cisco ISEへの接続に使用される Group14-SHA1 **SSH キー**を入力します
- （任意）**仮想 IP アドレス（Virtual IP Address）**：Cisco ISE ポリシーサービスノードが背後に配置されているロードバランサの仮想 IP アドレス。異なるロードバランサの背後に複数のポリシーサービス ノード ファームがある場合は、最大 6 つの仮想 IP アドレスを入力できます。

f) **[保存（Save）]** をクリックし、サーバのステータスが **[アクティブ（Active）]** になるまで待ちます。

ステップ 3 次のように Cisco ISE が Cisco DNA Centerに接続され、接続にサブスクライバがあることを確認します。

a) Cisco DNA Center を統合した Cisco ISE ノードにログインします。
b) **[管理（Administration）]** > **[pxGrid サービス（pxGrid Services）]** を選択します。

現在のステータスが **[オフライン（Offline）]** のpxGrid サービスサブスクライバが、ユーザの入力した名前（cdnacenter など）で表示されます。デフォルトでは、サブスクライバのステータスは**オフライン**のままであることに注意してください。

ステップ 4 Cisco DNA Center が Cisco ISE に接続していること、Cisco ISE SGT グループとデバイスが Cisco DNA Center にプッシュされることを次の手順で確認します。

a) Cisco DNA Center GUI にログインします。
b) **メニュー**アイコン（☰）をクリックし、**[システム（System）]** > **[システム360（System 360）]** を選択します。
c) [Identity Services Engine（ISE）] ペインで、**[Update（更新）]** リンクをクリックします。
d) **[認証サーバとポリシーサーバ（Authentication And Policy Servers）]** ウィンドウで、Cisco ISEAAA サーバのステータスがまだ **[アクティブ（Active）]** であることを確認します。
e) **メニュー**アイコン（☰）をクリックし、**[ポリシー（Policy）]** >**[グループベースアクセスコントロール（Group Based Access Control）]** を選択します。

ISE SGT グループは **[スケーラブルグループ]** 表に表示されます。

グループベースのアクセスコントロール：ポリシーデータの移行と同期

Cisco DNA Center 1.3.1.0 の使用を開始するとき

Cisco DNA Center の以前のリリースでは、グループベースのアクセス コントロール ポリシー機能でポリシーのアクセス契約とポリシーを Cisco DNA Center ローカルに保存していました。Cisco DNA Centerでは同じデータを Cisco ISE にも反映します。Cisco ISEではネットワークにランタイムポリシーサービスも提供します。その一環でグループベースのアクセスコントロール

ポリシーのファイルがネットワークデバイスにダウンロードされます。通常、Cisco DNA Center のポリシー情報は Cisco ISE のポリシー情報と一致します。ただし、データが同期されていない可能性があり、その場合はデータが一致していない可能性があります。このため、新規であれアップグレードであれ Cisco DNA Center1.3.1.0 をインストールした後は、グループベースのアクセスコントロール機能を使用する前に、次の手順が必要になります。

- Cisco ISE と Cisco DNA Center を統合する（未統合の場合）
- Cisco ISE をアップグレードする（必須バージョンさえない場合）。Cisco ISE の必須バージョンについては「Cisco DNA Centerリリースノート」を参照してください。
- ポリシーの移行と同期の実行

「移行と同期」とは何ですか。

Cisco DNA Center は統合された Cisco ISE に含まれるグループベースのアクセス コントロール ポリシー データをすべて読み取り、そのデータを Cisco DNA Center のポリシーデータと比較します。以前のバージョンからアップグレードした場合は、既存のポリシーデータが保持されます。Cisco DNA Center のグループベースのアクセス コントロール ポリシーを管理するには、先にポリシーを同期しておく必要があります。

移行と同期はどのように機能しますか。

通常、Cisco ISEと Cisco DNA Center のポリシーデータは一貫しているため、データの処理や変換は特に必要ありません。ささいな不一致や不整合がある場合、移行中に一部のデータのみが変換されることがあります。競合がある場合は、ネットワーク内でポリシーの挙動が変わらないように Cisco ISE のデータが優先されます。次のリストは、移行中に実行されるアクションを示しています。

- スケーラブルグループ（Scalable Groups）：スケーラブルグループタグ（SGT）（数値）は、スケーラブルグループを一意に特定します。Cisco ISEセキュリティグループが Cisco DNA Center のスケーラブルグループと比較されます。
  - 名前と SGT の値が同じであれば、何も変更されません。Cisco DNA Center の情報は Cisco ISE と一貫性があり、変更する必要はありません。
  - Cisco ISE セキュリティグループの SGT 値が Cisco DNA Center に存在しない場合は、Cisco DNA Centerに新しいスケーラブルグループが作成されます。新しいスケーラブルグループには「Default_VN」のデフォルトの関連付けが施されます。
  - Cisco ISE セキュリティグループの SGT 値が Cisco DNA Center に存在しているが、名前が一致しない場合は、Cisco ISEセキュリティグループの名前が Cisco DNA Center のスケーラブルグループの名前に置き換えられます。
  - Cisco ISE セキュリティグループの名前が同じであるが、SGT 値が異なる場合は、Cisco ISEからセキュリティグループが移行されます。この処理では名前とタグの値は保持されますが、Cisco DNA Centerスケーラブルグループの名前は変更されます。「_DNA」というサフィックスが追加されます。

契約

ポリシーの参照する Cisco ISE の SGACL はすべて、Cisco DNA Centerの契約と比較されます。

- SGACLと契約の名前と内容が同一の場合、それ以上のアクションは必要ありません。Cisco DNA Center の情報はCisco ISE と一貫性があり、変更する必要はありません。
    - SGACL と契約の名前が同一で、内容が異なっている場合は、Cisco ISEから SGACL の内容が移行されます。Cisco DNA Centerの以前のコントラクトコンテンツは破棄されます。

SGACL が Cisco DNA Center に存在しない場合、その名前で新しい契約が作成され、Cisco ISE からSGACL の内容が移行されます。

（注） Cisco ISE SGACL の内容に沿って新しいアクセス契約を作成する場合は、Cisco DNA Centerがテキストコマンドラインが解析され、これらの SGACL コマンドが可能な限りアクセス契約モデルとしてレンダリングされます。各 ACE 行は、「高度な」アプリケーション回線としてレンダリングされます。Cisco ISE SGACL に正常に解析できないテキストが含まれている場合、SGACL テキストの内容はモデル化された形式に変換されません。これは raw コマンドラインテキストとして保存されます。この SGACL 契約文は編集できますが、移行中、テキストの内容の解析または構文チェックは実行されません。

ポリシー

ポリシーは、送信元グループと宛先グループのペアで一意に識別されます。すべてのCisco ISE TrustSec イーグレス ポリシー マトリックス ポリシーが、Cisco DNA Centerのポリシーと比較されます。

- 送信元グループと宛先グループのポリシーで Cisco ISE の同じ SGACL または契約名を参照している場合、変更は行われません。
- 送信元グループと宛先グループのポリシーで Cisco ISE の別の SGACL または契約名を参照している場合、ポリシーではCisco ISE の契約名が参照されます。この結果、Cisco DNA Centerで以前の契約参照が上書きされます。
- Cisco ISE のデフォルトポリシーがチェックされ、Cisco DNA Centerに移行されます。

（注） Cisco DNA Center はアクセスポリシー内のいずれか 1 つの契約をサポートします。Cisco ISE にはアクセスポリシーで複数の SGACL を使用するオプションがありますが、ISE ではこのオプションがデフォルトでは無効であり、広く一般的には使用されていません。以前のリリースの Cisco DNA Center を使用してグループベースのアクセス コントロール ポリシーを管理していた既存の SDA のお客様は、このオプションを使用しないでください。

Cisco ISE で複数の Sgacl を許可するオプションを有効にしてポリシー作成時に使用した場合、これらのポリシーはこのリリースでは Cisco DNA Center に移行できません。移行できない [複数のSGACL（multiple SGACL）] オプションを利用する特定のポリシー機能は次のとおりです。

- ポリシー内で複数の SGACL
- ポリシーレベルの catch-all ルールは [許可（Permit）] または [拒否（Deny）] に設定されています現在の移行では [なし（None）] の値のみCisco DNA Centerサポートされています。
- 顧客が作成した SGACL を使用するよう設定されたデフォルトポリシー。ただし現在、Cisco DNA Centerへの移行では、[IPを許可（Permit IP）]、[Permit_IP_Log]、[IPを拒否（Deny IP）]、[Deny_IP_Log] の標準値のみサポートされています。

ポリシー移行と同期の操作中に先行する SGACL が何か検出された場合は、通知が生成されます。続行するには、次のオプションの中から選択する必要があります。

- **Cisco DNA Center でのグループ ベース アクセス コントロール ポリシーを管理**：このオプションが選択されている場合は、Cisco DNA Centerでグループベースのアクセス コントロール ポリシーの管理がすべて実行されます。Cisco ISE セキュリティグループ、SGCAL、イーグレスポリシーを管理する Cisco ISE のユーザインターフェイス画面は、読み取り専用モードで使用できます。（Cisco ISEで複数の SGACL を使用しているために）ポリシーの移行中に問題が生じた場合、これらのポリシーには Cisco DNA Center で選択した契約が含まれなくなります。このポリシーではデフォルトポリシーが使用され、移行が完了したら、そのポリシーに対応する契約を新しく選択できます。デフォルトポリシーの移行中に問題が発生した場合は、デフォルトポリシーが [許可（Permit）] に設定されます。
- **Cisco ISE でのグループ ベース アクセス コントロール ポリシーを管理（Manage Group-Based Access Control Policy）**：このオプションが選択されている場合は、Cisco DNA Centerグループベースのアクセス コントロール ポリシーの管理がすべて非アクティブになります。Cisco ISE は変更されず、ネットワーク内のポリシーの適用には影響しません。グループベースのアクセス コントロール ポリシーは、TrustSec ワークセンターの Cisco ISE で管理されます。
- **Cisco DNA Center と Cisco ISE の両方でグループベースのアクセス コントロール ポリシーを管理するには** このオプションは Cisco ISE で加えられたポリシー変更が Cisco DNA Center と同期されないため、一般的な使用には推奨されません。2 つのシステムを常に同期しておくことはできません。このオプションは短期または暫定オプションとして意図されており、Cisco ISEで [複数のSGACLを許可（Allow Multiple SQUADl] オプションを有効にした場合にのみ考慮する必要があります。Cisco ISE の更新でより多くの時間と一段と優れた柔軟性が必要になった場合に使用できます。

認証サーバとポリシー サーバの設定

Cisco DNA Center は AAA サーバをユーザ認証に使用し、Cisco ISE をユーザ認証とアクセス制御の両方に使用します。この手順を使って Cisco ISE を含む AAA サーバを設定します。

始める前に

- Cisco ISE を使用してポリシーと AAA 機能の両方を実行する場合、Cisco DNA Center と Cisco ISE が「Cisco ISE との統合 Cisco DNA Centerの統合」の説明に従って統合されたことを確認します。
- 他の製品（Cisco ISE 以外）で AAA 機能を使用している場合、以下に注意してください。
  - AAA サーバで Cisco DNA Center を登録します。これには、AAA サーバと Cisco DNA Center の共有秘密を定義することが含まれます。
  - AAA サーバで Cisco DNA Center の属性名を定義します。
  - Cisco DNA Center マルチホストクラスタの設定の場合は、AAA サーバのマルチホストクラスタに、すべての個別のホスト IP アドレスと仮想 IP アドレスを定義します。

ステップ 1 Cisco DNA Center のホームページで、⚙ > **[System Settings]** > **[Settings]** > **[Authentication and Policy Servers]** の順に選択します。

ステップ 2 ⊕ Add をクリックします。

ステップ 3 次の情報を入力して、プライマリ AAA サーバを設定します。

- **サーバの IP アドレス（Server IP Address）**：AAA サーバの IP アドレス。
- **共有秘密（Shared Secret）**：デバイス認証キー。共有秘密情報の長さは、最大 128 文字です。

ステップ 4 AAA サーバ（Cisco ISE 以外）を設定するには、**[Cisco ISE サーバ（Cisco ISE Server）]** ボタンを **[オフ（Off）]** 位置のままにして、次の手順に進みます。

Cisco ISE サーバを設定するには、**[Cisco ISE サーバ（Cisco ISE server）]** ボタンをクリックして **[オン（On）]** の位置に合わせ、次のフィールドに情報を入力します。

- **ユーザ名（Username）**：Cisco ISE CLI へのログインに使用する名前です。

  （注） このユーザにはスーパーユーザの管理権限が必要です。

- **パスワード（Password）**：Cisco ISE CLI ユーザ名のパスワード。
- **FQDN** - Cisco ISE サーバの FQDN。

  （注）
  - Cisco ISE（**[管理（Administration）]** > **[展開（Deployment）]** > **[展開ノード（Deployment Nodes）]** > **[リスト（List）]**）で定義されている FQDN をコピーして、このフィールドに直接貼り付けすることをお勧めます。
  - 入力した FQDN は、Cisco ISE証明書で定義されている FQDN、共通名（CN）または Subject Alternative Name（SAN）と一致する必要があります。

  FQDN は次の形式で、ホスト名とドメイン名の 2 つのパートで構成されています。

  hostname.domainname.com。

たとえば Cisco ISE サーバの FQDN は、ise.cisco.com である可能性があります。

- **サブスクライバ名（Subscriber Name）**：Cisco ISE pxGrid サービスに登録するとき pxGrid クライアントを識別する一意のテキスト文字列（acme など）。ユーザ名は Cisco DNA Center を Cisco ISE に統合中に使用されます。
- （任意）**SSH キー**：Cisco ISEへの接続に使用される Diffie-Hellman-Group14-SHA1 SSH キー。
- （任意）**仮想IPアドレス**：Cisco ISE ポリシーサービスノードが背後に配置されているロードバランサの仮想 IP アドレス。異なるロードバランサの背後に複数のポリシー サービス ノード ファームがある場合は、最大 6 つの仮想 IP アドレスを入力できます。

（注） 設定された ISE サーバのステータスがパスワードの変更により [失敗（FAILED）] になっている場合は、**[再試行（Retry）]** をクリックし、パスワードを更新して ISE 接続を再同期します。

ステップ 5 [詳細設定の表示（View Advanced Settings）] をクリックして、設定を構成します。

（注） 必要な設定は、サーバのプロトコル設定によって異なります。

- **プロトコル（Protocol）**：**[RADIUS]** はデフォルトで設定されていますが、代わりに **[TACACS]** を選択するか、両方のプロトコルを選択することもできます。

  注目 Cisco ISE サーバに **[TACAS]** を選択しない場合、Cisco ISE ノードの設定には使用できません。

- **認証ポート（Authentication Port）**：**RADIUS** が AAA サーバに認証メッセージを中継するために使用されるポート。デフォルト値は UDP ポート 1812 です。
- **アカウンティングポート（Accounting Port）**：**RADIUS** が AAA サーバに重要なイベントを中継するために使用するポート。これらのイベントの情報は、セキュリティおよび請求目的で使用されます。デフォルトの UDP ポートは 1813 です。
- **ポート（Port）**：**TACACS** が AAA サーバとの通信に使用するポート。デフォルト ポートは 49 です。
- **再試行（Retries）**：接続の試行が中止される前に、Cisco DNA Centerが AAA サーバへの接続を試みた回数。デフォルトの試行回数は 3 回です。
- **タイムアウト（Timeout）**：接続の試行が中止される前に、デバイスが AAA サーバの応答を待機する時間。デフォルトのタイムアウトは 4 秒です。

ステップ 6 [適用（Apply）] をクリックします。

ステップ 7 セカンダリサーバを追加するには、ステップ 2 ～ 6 を繰り返します。

SNMP プロパティの設定

SNMP の再試行とタイムアウトの値を設定できます。

始める前に

SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。詳細については、*Cisco Digital Network Architecture Center* 管理者ガイドを参照してください。

ステップ 1 Cisco DNA Center のホームページで ⚙ をクリックし、**[システムの設定（System Settings）]** > **[設定（Settings）]** > **[SNMP プロパティ（SNMP Properties）]** の順に選択します。

ステップ 2 次のフィールドを設定します。

- **再試行回数（Retries）**：許容されるデバイス接続の最大試行回数。有効な値は 1 ～ 3 です。デフォルトは 3 です。
- **タイムアウト（秒数）（Timeout（in Seconds））**：タイムアウトになるまでにデバイスとの接続の確立を試みる際に、Cisco DNA Center が待機する秒数。有効な値は 5 秒間隔で 1 ～ 300 秒の範囲内です。デフォルトは 5 秒です。

ステップ 3 [適用（Apply）] をクリックします。

（注） デフォルト設定に戻すには、**[デフォルトに戻す（Revert to Defaults）]** をクリックします。