管理操作

サイトのステータスの表示

マルチサイト Orchestrator GUI の**ダッシュボード**ビューを使用して、各サイトのステータス、障害の数とタイプ、およびスキーマの健全性を表示できます。

[サイト ステータス (SITE STATUS)] パネルでは、ダッシュボードに次のフィールドが表示されます:

- **SITE NAME (サイト名)**
- **CRITICAL** Alarms (緊急アラーム)
- **MAJOR** Alarms (メジャー アラーム)
- **MINOR** Alarms (マイナー アラーム)
- **WARNING** Alarms (警告アラーム)

スキーマ ヘルスの表示

マルチサイト Orchestrator GUI ダッシュボードのスキーマ健全性機能を使用すれば、さまざまなサイトに関連付けられている個々のスキーマの健全性を表示できます。**[スキーマの詳細**

(Schema Details)] ウィンドウでは、各サイトに関連付けられているポリシー タイプを表示できます。

GUI の **[スキーマ ヘルス (SCHEMA HEALTH)]** チャートでは、以下のタスクを実行できます:

- マルチサイト ファブリック全体とすべてAPICの健全性スコアを集約して表示する
- **[スキーマの詳細 (Schema Details)]** ウィンドウで、集計されたエラー数と、スキーマごとのエラー タイプを表示する
- サイト間スキーマの健全性を表示する
- 複数のサイト ノードとそのコンポーネントの健全性を表示する
- 接続された APIC および ACI クラスタの健全性を表示する

GUI では、以下のいくつかのフォーマットで、スキーマの健全性を表示できます:

- 個々のセルにマウスを合わせます。**[スキーマ ヘルス (SCHEMA HEALTH)]** チャートの各セルは、スキーマの健全性を示しています。セルが緑色で表示されている場合、マウスをそのセルに合わせると、スキーマのアプリケーション健全性が表示されます。
- セルをクリックします。テーブルの個々のセルをクリックすると、テンプレートに関するスキーマの詳細と、各ポリシー タイプ (ANP、EPG、コントラクト、VRF、BD など) に関連付けられたエラーが表示されます。

  エラーと警告は各ポリシーの右側の列に表示されます。この機能は、詳細を収集し、健全性を低下させている問題についてより多くの情報を得るために使用されます。
- 健全性スコア スライダの表示。ページの上部にある健全性スコア スライダを使えば、健全性スコアの最小または最大に基づいてスキーマのフィルタリングを行えます。スライダによって範囲を調整すれば、健全性スコアの範囲に一致するスキーマを表示できます。たとえば、健全性スコアを調整して、0～30の範囲内の健全性スコアに一致するスキーマを表示することができます。
- 検索機能を使用する。スキーマの健全性ビューの検索機能では、検索エリアに入力されたキーワードに基づいてスキーマまたはポリシーを見つけることができます。検索領域にキーワードを入力すると、キーワードを含むスキーマだけが表示されます。結果は、スキーマ名、テンプレート名、またはそのスキーマ内で含まれているポリシーのいずれかの一部として一致するキーワードに基づいています。

個々のサイトの障害の表示

ここでは、マルチサイト GUI を使用して個々のサイトの障害を表示する方法について説明します。

ステップ 1 マルチサイト Orchestrator GUI にログインします。

ステップ 2 **Main Menu** で**Sites** をクリックします。

ステップ 3 **Sites list** ページで **CONFIGURE INFRA** をクリックします。

ステップ 4 **Fabric Connectivity Infra** ページの **Master List** で、適切なサイトをクリックします。たとえば、site1 をクリックします。

サイトの詳細と、関連付けられているポッドとスパインが GUI に表示されます。

パネルの上部には、障害の総数と障害のタイプが表示されます。たとえば、タイプとしては、Critical、Major、Minor、および Warning があります。それぞれの障害のタイプをクリックすると、障害の詳細と、個々のコードおよびその説明が表示されます。

DHCP リレー ポリシー

通常、DHCP サーバが EPG の下に配置されている場合、その EPG 内のすべてのエンドポイントがアクセス権を持ち、DHCP を介して IP アドレスを取得できます。ただし、多くの導入シナリオでは、DHCP サーバが必要なすべてのクライアントと同じ EPG、BD、または VRF に存在していない可能性があります。このような場合、1つの EPG 内のエンドポイントが別のサイトに配置された別の EPG/BD にあるサーバから、またはファブリックに外部に接続され、L3Out 接続を介して到達可能なサーバから IP アドレスを取得できるように、DHCP リレーを設定できます。

Orchestrator GUI で DHCP リレー ポリシーを作成してリレーを設定できます。また、DHCP オプション ポリシーを作成して、特定の設定の詳細を提供するためにリレーポリシーで使用できる追加オプションを設定することもできます。使用可能なすべての DHCP オプションについては、 RFC 2132 を参照してください。

DHCP リレーポリシーを作成する場合は、DHCP サーバが存在する EPG (たとえば、 `epg1`) または外部 EPG (たとえば、`ext epg1`) を指定します。DHCP ポリシーを作成した後、それをブリッジドメインに関連付けます。これにより、その EPG 内のエンドポイントが DHCP サーバに到達できるようになります。これにより、別の EPG (たとえば、`epg2`) に関連付けられます。最後に、リレー EPG (`epg1`または`epg1`) とアプリケーション EPG (`epg2`) 間の契約を作成し、通信を可能にします。作成した DHCP ポリシーは、ポリシーが関連付けられているブリッジ ドメインがサイトに展開されるときに、APIC にプッシュされます。

注意事項と制約事項

DHCP リレーポリシーは、次の警告でサポートされます。

- DHCP リレーポリシーは、Cisco APIC リリース 4.2(1) 以降を実行しているファブリックでサポートされています。
- DHCP サーバは、DHCP リレー エージェント情報オプション (オプション 82) をサポートしている必要があります。

  ACI ファブリックが DHCP リレーとして動作する場合、DHCP リレーエージェント情報オプションは、クライアントの代わりにプロキシする DHCP 要求に挿入されます。応答

（DHCP オファー）がオプション 82 なしで DHCP サーバから返された場合、その応答はファブリックによってサイレントにドロップされます。

- DHCP リレー ポリシーは、ユーザ テナントまたは共通テナントでのみサポートされます。DHCP ポリシーは、インフラまたは管理テナントではサポートされていません。

  ACI ファブリックで共有リソースとサービスを設定する場合は、共通テナントでこれらのリソースを作成することをお勧めします。これは、どのユーザ テナントでも使用できます。

- DHCP リレー サーバは、DHCP クライアントまたは共通テナントと同じユーザ テナントに存在する必要があります。

  サーバとクライアントは、異なるユーザ テナントに配置することはできません。

- DHCP リレー ポリシーは、プライマリ SVI インターフェイスにのみ設定できます。

  リレーポリシーを割り当てるブリッジドメインに複数のサブネットが含まれている場合、追加した最初のサブネットは SVI インターフェイスのプライマリ IP アドレスになりますが、追加のサブネットはセカンダリ IP アドレスとして設定されます。複数のサブネットを持つブリッジドメインを使用した設定のインポートなどの特定のシナリオでは、SVI のプライマリ アドレスがセカンダリ アドレスの1つに変更されることがあり、そのブリッジドメインの DHCP リレーが中断されることがあります。

  `Show ip interface vrf all`コマンドを使用して、SVI インターフェイスの IP アドレスの割り当てを確認できます。

- ブリッジドメインに割り当てた後に DHCP ポリシーを変更し、ブリッジ ドメインを 1 つ以上のサイトに展開した場合は、各サイトの APIC で DHCP ポリシーの変更を更新するために、ブリッジ ドメインを再展開する必要があります。

- L3Out 経由で到達可能な DHCP サーバとの VRF 間 DHCP リレーの場合、DHCP リレー パケットは、DHCP サーバに到達するためにサイト ローカル L3Out を使用する必要があります。異なるサイト (サイト間 L3Out) の L3Out を使用するパケットはサポートされていません。

- 次の DHCP リレー設定はサポートされていません。

  - L3Out の背後にある DHCP リレー クライアント。
  - APIC から既存の DHCP ポリシーをインポートしています。
  - グローバルファブリックアクセスポリシーでの DHCP リレーポリシーの設定はサポートされていません
  - 同じ DHCP リレーポリシー内の複数の DHCP サーバと EPG。

    同じ DHCP リレーポリシーで複数のプロバイダを設定する場合は、それぞれ異なる EPGs または外部 EPGs にする必要があります。

DHCP リレー ポリシーの作成

このセクションでは、DHCP リレー ポリシーの作成方法について説明します。

（注） DHCP ポリシーをブリッジ ドメインに割り当て、ブリッジ ドメインを1つ以上のサイトに展開した後で DHCP ポリシーに変更を加えた場合には、各サイトの APIC で更新する DHCP ポリシーの変更を行うために、ブリッジ ドメインを再展開する必要があります。

始める前に

次のものが必要です。

- 使用している環境でセットアップして設定された DHCP サーバ。
- DHCP サーバがアプリケーション EPG の一部となる場合は、スキーマ管理 章での説明に従って、その EPG がマルチサイト Orchestrator ですでに作成されている必要があります。

  DHCP サーバがファブリックの外部にある場合は、スキーマ管理 章での説明に従って、DHCP サーバへのアクセスに使用される L3Out に関連付けられている外部 EPG がすでに作成されている必要があります。

ステップ 1 マルチサイト Orchestrator GUI にログインします。

ステップ 2 左のナビゲーションメニューから **[ポリシー (Policies)]** を選択します。

ステップ 3 メイン ペインの右上にある **[ポリシーの追加 (Add Policy)]** をクリックし、**DHCP** を選択します。

[DHCP の追加 (Add DHCP)] 設定画面が表示されます。

ステップ 4 **[名前 (Name)]** フィールドにポリシーの名前を入力します。

ステップ 5 **[テナントの選択 (Select Tenant)]** ドロップダウンから、DHCP サーバを含むテナントを選択します。

ステップ 6 (オプション) **[説明 (Description)]** フィールドに、このポリシーの説明を入力します。

ステップ 7 **[タイプ (Type)]** として `[リレー (Relay)]` を選択します。

ステップ 8 **[+プロバイダ]** をクリックします。

ステップ 9 プロバイダ タイプを選択します。

リレー ポリシーを追加する場合は、次の 2 つのタイプのいずれかを選択します。

- `[アプリケーション EPG (Application EPG)]`: エンドポイントとして追加する DHCP サーバを含む特定のアプリケーション EPG を指定します。
- `[L3 外部ネットワーク (L3 External Network)]`: DHCP サーバーへのアクセスに使用される L3Out に関連付けられた外部 EPG を指定します。

（注） Orchestrator で作成し、指定したテナントに割り当てられた EPG または外部 EPG は、サイトにまだ展開していない場合でも、選択することができます。展開されていない EPG を選択した場合でも、DHCP リレー設定を完了できます。ただし、リレーを使用できるようにするには、その前に EPG を展開する必要があります。

ステップ 10 ドロップダウン メニューから、EPG または外部 EPG を選択します。

ステップ 11 **[DHCP サーバ アドレス (DHCP Server Address)]** フィールドに、DHCP サーバの IP アドレスを入力します。

ステップ 12 [**保存 (Save)**] をクリックして、プロバイダを追加します。

ステップ 13 (オプション) 追加プロバイダがあれば、それを加えます。

追加する DHCP サーバごとに、ステップ 9 ~ 12 を繰り返します。

ステップ 14 **[保存 (Save)]** をクリックして DHCP リレー ポリシーを保存します。

DHCP オプションポリシーの作成

このセクションでは、DHCP オプション ポリシーの作成方法について説明します。DHCP オプションは、DHCP サーバとクライアントが交換するメッセージの末尾に追加され、DHCP サーバに追加の設定情報を提供するために使用されます。各 DHCP オプションには、オプション ポリシーを追加するときに指定する必要がある特定のコードがあります。DHCP オプションとコードの完全なリストの場合は、RFC 2132 を参照してください。

始める前に

次のものをあらかじめ設定しておく必要があります。

- 環境でセットアップして設定された DHCP サーバ。
- スキーマ管理 章の説明に従って、Multi-Site Orchestrator ですでに作成してある DHCP サーバを含む EPG。
- DHCP リレー ポリシーの作成 （5 ページ） の説明に従って作成された DHCP リレー ポリシー。

ステップ 1 マルチサイト Orchestrator GUI にログインします。

ステップ 2 左のナビゲーションメニューから **[ポリシー (Policies)]** を選択します。

ステップ 3 メイン ペインの右上にある **[ポリシーの追加 (Add Policy)]** をクリックし、**DHCP** を選択します。

[DHCP の追加 (Add DHCP)] 設定画面が表示されます。

ステップ 4 **[名前 (Name)]** フィールドにポリシーの名前を入力します。

これは、作成しているポリシーの名前であり、特定の DHCP オプションの名前ではありません。各ポリシーには、複数の DHCP オプションを含めることができます。

ステップ 5 **[テナントの選択 (Select Tenant)]** ドロップダウンから、DHCP サーバを含むテナントを選択します。

ステップ 6 (オプション) **[説明 (Description)]** フィールドに、このポリシーの説明を入力します。

ステップ 7 **[タイプ (Type)]** に対して `[オプション (Option)]` を選択します。

ステップ 8 **[+オプション (+Options)]** をクリックします。

ステップ 9 オプションの名前を指定します。

どうしても必要というわけではありませんが、 RFC 2132に記載されているオプションと同じ名前を使用することを推奨します。

たとえば、`[Name Server]`などです。

ステップ 10 オプションの ID を指定します。

RFC 2132に記載されているオプション コードを指定する必要があります。

たとえば、ネーム サーバ オプションの場合は `5` です。

ステップ 11 オプションのデータを指定します。

オプションで必要な場合は、値を入力します。

たとえば、ネーム サーバ オプションで、クライアントが使用可能なネーム サーバのリストです。

ステップ 12 オプションを保存するには、**[データ (Data)]** フィールドの横にあるチェックマークをクリックします。

ステップ 13 (オプション) その他のオプションを追加するには、この手順を繰り返します。

ステップ 14 **[保存 (Save)]** をクリックして DHCP オプション ポリシーを保存します。

DHCP ポリシーの割り当て

この項では、ブリッジ ドメインを作成する方法について説明します。

（注） ブリッジドメインに割り当てた後に DHCP ポリシーを変更し、ブリッジ ドメインを 1 つ以上のサイトに展開した場合は、各サイトの APIC で DHCP ポリシーの変更を更新するために、ブリッジ ドメインを再展開する必要があります。

始める前に

次のものがすでに設定されている必要があります。

- DHCP リレー ポリシーの作成 （5 ページ） の説明に従って、DHCP リレー ポリシー。
- (オプション) DHCP オプションポリシーの作成 （6 ページ） の説明に従って、DHCP オプション ポリシー。
- スキーマ管理 章の説明に従って、DHCP ポリシーに割り当てられたブリッジ ドメイン。

ステップ 1 マルチサイト Orchestrator GUI にログインします。

ステップ 2 左側のナビゲーション メニューで、**[スキーマ (schema)]** を選択します。

ステップ 3 ブリッジド メインが定義されているスキーマを選択します。

ステップ 4 **[[ブリッジ ドメイン (Bridge domain)]** エリアまで下にスクロールし、ブリッジド メインを選択します。

ステップ 5 右側のサイドバーで、下にスクロールして、 **[DHCP ポリシー (DHCP Policy)]** オプション チェックボックスをオンにします。

ステップ 6 **[DHCP リレーポリシー (DHCP Relay policy)]** ドロップダウンから、この BD に割り当てる DHCP ポリシーを選択します。

ステップ 7 (オプション)**[DHCP オプションポリシー (DHCP Option policy)]** ドロップダウンから、オプション ポリシーを選択します。

DHCP オプション ポリシーは、DHCP リレーに渡す追加のオプションを提供します。詳細については、DHCP オプションポリシーの作成 （6 ページ）を参照してください。

ステップ 8 リレー経由でDHCPサーバにアクセスする必要があるすべてのEPGにブリッジドメインを割り当てます。

DHCP リレー コントラクトの作成

DHCPパケットはコントラクトによってフィルタリングされませんが、多くの場合、VRF内およびVRF間でルーティング情報を伝搬するためにコントラクトが必要です。DHCPパケットがフィルタリングされない場合でも、クライアントEPGと、DHCPリレーポリシーでプロバイダとして設定されているEPGとの間では、コントラクトを設定することを推奨します。

このセクションでは、DHCP サーバーを含む EPG と、リレーを使用する必要のあるエンドポイントを含む EPG の間でコントラクトを作成する方法について説明します。DHCP ポリシーをすでに作成して、ブリッジ ドメインと、クライアントの EPG へのブリッジ ドメインに割り当てている場合でも、ルートのプログラミングを有効にするコントラクトを作成して割り当てる必要があります。

始める前に

次のものがすでに設定されている必要があります。

- DHCP リレー ポリシーの作成 （5 ページ） の説明に従って、DHCP リレー ポリシー。
- (オプション) DHCP オプションポリシーの作成 （6 ページ） の説明に従って、DHCP オプション ポリシー。
- DHCP ポリシーの割り当て （7 ページ） の説明に従って、DHCP ポリシーに割り当てられたブリッジ ドメイン。

ステップ 1 マルチサイト Orchestrator GUI にログインします。

ステップ 2 左側のナビゲーション メニューで、**[スキーマ (schema)]** を選択します。

ステップ 3 コントラクトを作成するスキーマを選択します。

ステップ 4 コントラクトを作成します。

DHCP パケットはコントラクトによってフィルタリングされないため、特定のフィルタは必要ありませんが、適切な BD とルートの展開を保証するために、有効なコントラクトを作成して割り当てる必要があります。

a) **[コントラクト (Contracts)]** エリアまで下方にスクロールし、+ をクリックして、コントラクトを作成します。
b) 右側のサイドバーで、コントラクトの**[表示名 (Display Name)]**を入力します。
c) **[範囲 (Scope)]** ドロップダウンから、適切な範囲を選択します。

DHCP サーバの EPG とアプリケーション EPG は同じテナント内にある必要があるため、次のいずれかを選択できます。

- `[vrf]`(両方の EPG が同じ VRF にある場合)
- `[テナント (tenant)]`(EPG が異なる VRF にある場合)

d) [**両方向に適用 (Apply Both Directions)**] ノブはオンのままにすることができます。

ステップ 5 DHCP リレー EPG にコントラクトを割り当てます。

a) EPG が配置されているテンプレートを参照します。
b) DHCP サーバが存在する EPG または外部 EPG を選択します。

これは、DHCP リレー ポリシーの作成時に選択したのと同じ EPG です。

c) 右側のサイドバーで、**[+コントラクト (+Contract)]** をクリックします。
d) 作成したコントラクトと、そのタイプのための*プロバイダ*を選択します。

ステップ 6 エンドポイントが DHCP リレー アクセスを必要とするアプリケーション EPG に、コントラクトを割り当てます。

a) アプリケーション EPG が配置されているテンプレートを参照します。
b) アプリケーション EPG を選択します。
c) 右側のサイドバーで、**[+コントラクト (+Contract)]** をクリックします。
d) 作成した契約と、そのタイプのための*コンシューマ*を選択します。

APIC での DHCP リレー ポリシーの確認

ここでは、Multi-Site Orchestrator を使用して作成および展開した DHCP リレーポリシーが各サイトの APIC に正しくプッシュされることを確認する方法について説明します。作成する DHCP ポリシーは、ポリシーが関連付けられているブリッジ ドメインがサイトに展開しているときに、APIC にプッシュされます。

ステップ 1 サイトの APIC GUI にログインします。

ステップ 2 上部のナビゲーションバーから、[**テナント(tenant)**] > **<テナント名>**を選択します。

DHCP ポリシーを展開したテナントを選択します。

ステップ 3 APIC で DHCP リレー ポリシーが設定されていることを確認します。

左側のツリー ビューで、**<テナント名>** > **ポリシー (Policies)** > **プロトコル (Protocol)** > **DHCP** > **リレー ポリシー(Relay policies)**に移動します。次に、設定した DHCP リレー ポリシーが作成されていることを確認します。

ステップ 4 DHCP オプション ポリシーが APIC で設定されていることを確認します。

DHCP オプション ポリシーを設定していない場合は、この手順をスキップできます。

左側のツリー ビューで、**<テナント名>** > **ポリシー (Policies)** > **プロトコル (Protocol)** > **DHCP** > **オプション ポリシー(Option Policies)**に移動します。次に、設定した DHCP オプション ポリシーが作成されていることを確認します。

ステップ 5 DHCP ポリシーがブリッジ ドメインに正しく関連付けられていることを確認します。

左側のツリー ビューで、**<テナント名>** > **ネットワーク** > **ブリッジ ドメイン** > **<ブリッジ ドメイン名>** > **DHCP リレー ラベル**に移動します。展開されたブリッジ ドメインにも DHCP ポリシーが関連付けられていることを確認します。

既存の DHCP ポリシーの編集または削除

このセクションでは、DHCP リレーまたはオプション ポリシーを編集または削除する方法について説明します。

（注）
- ブリッジ ドメインに割り当てた後に DHCP ポリシーを変更し、ブリッジ ドメインを 1 つ以上のサイトに展開した場合は、DHCP ポリシーの変更が各サイトの APIC で更新されるように再展開する必要があります。
- 1 つ以上のブリッジ ドメインに関連付けられているポリシーを削除することはできません。最初に、すべてのブリッジ ドメインからポリシーの割り当てを解除する必要があります。

ステップ 1 マルチサイト Orchestrator GUI にログインします。

ステップ 2 左のナビゲーションメニューから **[ポリシー (Policies)]** を選択します。

ステップ 3 DHCP ポリシーの横にある [アクション] メニューをクリックし、**[編集 (Edit)]** または **[削除 (Delete)]** を選択します。

システム ログ

マルチサイト Orchestrator システム ロギングは、最初に Orchestrator クラスタを展開したときに自動的に有効になり、環境内で発生したイベントと障害をキャプチャします。

マルチサイト Orchestrator ログを表示するには、メインのナビゲーション メニューから **[管理 (Admin)]** > **[監査ログ (Audit logs)]** を選択します。

[**監査ログ (Audit Logs)**] ページで、**[最新 (Most Recent)]** フィールドをクリックして、ログを表示する特定の期間を選択できます。たとえば、2017 年 11 月 14日から 2017 年 11 月 17日までの範囲を選択し、[**適用 (Apply)**] をクリックすると、この期間の監査ログの詳細が [**監査ログ (Audit Logs)**] ページに表示されます。

次の基準に従ってログの詳細のフィルタ処理を行うには、**[フィルタ (Filter)]** アイコンをクリックします。

- **ユーザ(User)**: ユーザ タイプに基づいて監査ログのフィルタ処理を行うには、このオプションを選択し、[**適用 (Apply)**] をクリックします。
- **タイプ (Type)**: ポリシー タイプに基づいて監査ログのフィルタ処理を行うには、このオプションを選択します。たとえばサイト、ユーザ、テンプレート、アプリケーションプロファイル、ブリッジドメイン、EPG、外部 EPG、フィルタ、VRF、BGP 設定、契約、OSPF ポリシー、ポッド、ノード、ポート、ドメイン、プロバイダは、RADIUS、TACACS+ をクリックして、[**適用 (Apply)**] をクリックします。
- **アクション(Action)**: アクションに基づいて監査ログをフィルタ処理するには、このオプションを選択します。使用可能なアクションとしては作成、更新、削除、追加、関連付け、関連付けの解除解除、展開、展開の解除、ダウンロード、アップロード、復元、ログイン、ログの失敗があります。アクションに従ってログの詳細をフィルタ処理するには、アクションを選択して **[適用 (Apply)]** をクリックします。

トラブルシューティング レポートとログの生成

このセクションでは、Cisco ACI マルチサイト Orchestrator により管理されているすべてのスキーマ、サイト、テナント、およびユーザのトラブルシューティング レポートとインフラストラクチャ ログ ファイルを生成します。

ステップ 1 マルチサイト Orchestrator GUI にログインします。

ステップ 2 右上隅で、**[オプション (Options)]** アイコンをクリックして、**[システム ログ(System Logs)]** をクリックします。

ステップ 3 ダウンロードするログを確認します。

[データベースのバックアップ (Database Backup)] をクリックして、Orchestrator データベースのバックアップをダウンロードします。

[サーバ ログ (Server Logs)] をチェックして、Orchestrator ログをダウンロードします。

ステップ 4 **[ダウンロード (DOWNLOAD)]** をクリックします。

選択した項目のアーカイブがシステムにダウンロードされます。このレポートには、次の情報が含まれています。

- JSON フォーマットでのすべてのスキーマ
- JSON フォーマットでのすべてのサイト定義
- JSON フォーマットでのすべてのテナント定義
- JSON フォーマットでのすべてのユーザ定義
- `infra_logs.txt` ファイル内のコンテナのすべてのログ

外部ログ アナライザへのログ ストリーミングを有効にする

Cisco ACI マルチサイト Orchestrator を使用すると、Orchestrator ログを外部のログ アナライザ ツールにリアルタイムで送信できます。生成されたイベントをストリーミングすることにより、追加のツールを使用して、遅延なしで重要なイベントをすばやく解析し、表示し、それらに対応できます。

ここでは、マルチサイト Orchestrator が外部アナライザ ツール (Splunk など) にログをストリーミングできるようにする方法について説明します。

始める前に

- ログ アナライザ サービス プロバイダをセットアップして構成します。

  外部ログ アナライザの設定方法の詳細については、マニュアルを参照してください。

  （注） Cisco ACI マルチサイト Orchestrator の本リリースでは、サービス プロバイダとして Splunk のみがサポートされています。

- サービス プロバイダの認証トークンを取得します。

  分裂サービスの認証トークンの取得については、Splunk のマニュアルで詳しく説明していますが、簡単に言うと、**[設定 (Settings)]** > **[データ入力 (Data Inputs)]** > **[HTTP イベント コレクタ (Data input HTTP Event Collector]**)を選択し、[**新規トークン (New token**)] をクリックして、認証トークンを取得できます。

ステップ 1 マルチサイト Orchestrator GUI にログインします。

ステップ 2 右上隅で、**[オプション (Options)]** アイコンをクリックして、**[システム ログ(System Logs)]** をクリックします。

ステップ 3 開いた **[システムログ (System Logs)]** ウィンドウで、**[外部ストリーミング (EXTERNAL STREAMING)]** ノブを有効にします。

ステップ 4 ストリーミングするログを選択します。

[すべてのログ (all logs)] または [監査ログのみ (audit log only)] のいずれかを選択できます。

ステップ 5 **[サービスの選択 (SELECT SERVICE)]** ドロップダウン メニューから、ログ アナライザ サービスを選択します。

このリリースの Cisco ACI マルチサイト Orchestrator では、サービス プロバイダとして Splunk のみがサポートされています。

ステップ 6 トラフィックの **[プロトコル(PROTOCOL)]** を選択します。

HTTP の場合には **[非セキュア (UNSECURE)]**、HTTPS の場合には **[セキュア (SECURE)]** を選択します。

ステップ 7 サービスの情報を入力します。

[ホスト (HOST)] フィールドに、ホストの IP アドレスを入力します。

[ポート (PORT)] フィールドに、ポート番号を入力します。

[トークン (TOKEN)] フィールドに、サービス プロバイダから取得した認証トークンを入力します。

ステップ 8 マルチサイト Orchestrator ノードごとに、ノードのルート パスワードを入力します。

（注） これは、Orchestrator GUI へのログインに使用するパスワードではなく、各 Orchestrator ノードのルート ユーザ パスワードです。

ステップ 9 **[OK]** をクリックして変更を保存します。

設定のバックアップと復元

Orchestrator の障害またはクラスタの再起動からのリカバリを容易にするために、マルチサイト Orchestrator 設定のバックアップを作成できます。Orchestrator の各アップグレードまたはダウングレードの前、および各設定の変更または展開後には、設定のバックアップを作成することを推奨します。また、Orchestrator ノードの VM の外部にある外部ストレージにバックアップをエクスポートすることをお勧めします。

（注） バックアップ アクションの復元は、マルチサイト Orchestrator でのデータベースを復元しますが、各サイトの APIC データベースには変更を加えません。したがって、Orchestrator データベースを復元した後で、Orchestrator と APIC サイト間のポリシーが食い違う可能性を避けるため、既存のスキーマを再展開する必要もあります。特定の設定が食い違うシナリオと、それぞれに関連するバックアップ復元手順の詳細については、次を参照してください。バックアップと復元に関するガイドライン （14 ページ）

バックアップと復元に関するガイドライン

設定のバックアップを保存および復元する際には、次のガイドラインが適用されます。

- バックアップを保存すると、設定は展開されたのと同じ状態で保存されます。バックアップを復元すると、展開されたすべてのポリシーが「展開済み」として表示されますが、展開されていないポリシーは「未展開」の状態のままになります。
- バックアップ アクションの復元は、マルチサイト Orchestrator でのデータベースを復元しますが、各サイトの APIC データベースに変更を加えません。そのため、以下で説明するように、以前の設定を復元して、Orchestrator と APIC サイトの間でポリシーが一致しない可能性を回避するために、特定の注意事項と手順を実行する必要があります。

バックアップ以降の設定変更がない場合

バックアップが作成されてから復元されるまでの間にポリシーの変更がない場合は、追加の考慮事項は必要ありません。バックアップの復元 （19 ページ） の説明に従って設定を復元するだけです。

バックアップ以降に作成、変更、または削除されたオブジェクトまたはポリシー

設定のバックアップが作成されてから復元された時間までの間に設定変更が行われた場合は、次の点を考慮してください。

- バックアップを復元しても、APIC サイトのオブジェクトやポリシーは変更されません。バックアップ以降に作成および展開された新しいオブジェクトまたはポリシーは、展開されたままになります。古い設定を回避するには、バックアップを復元した後に手動でこれらを削除する必要があります。

  または、すべてのポリシーを最初に展開解除することもできます。これにより、バックアップから設定が復元された後に、古いオブジェクトが残る可能性を回避されます。ただし、この操作により、これらのポリシーによって定義されたトラフィックまたはサービスの中断が発生します。

- 設定のバックアップを復元するために必要な手順については、バックアップの復元 （19 ページ） で説明しています。
- 復元した設定バックアップが APIC サイトに展開される前に保存された場合は、「未展開」状態で復元され、必要に応じて APIC サイトに展開できます。
- 設定がすでに展開されているときに復元した設定バックアップが保存された場合、APIC サイトにまだ存在していないポリシーがあっても、「展開済み」状態に復元されます。この場合、設定を各サイトに適切にプッシュするには、いくらかの設定変更をして、それを再展開して、Orchestrator の設定を APIC サイトと同期させる必要があります。

リモート バックアップ

Cisco ACI マルチサイト は、3 ノードのクラスタとして展開されます。クラスタを最初に展開すると、作成したバックアップは、 `/opt/cisco/msc/backups/`ディレクトリ内の各ノードのローカル ディスク上に配置されているデフォルトの場所に保存されます。

バックアップは任意の1つのノードで使用でき、Orchestrator GUI を使用して表示できますが、Orchestrator VM の外部にあるリモート ロケーションにすべてのバックアップをエクスポートすることを推奨します。すべての Orchestrator バックアップに対してリモート ロケーションを設定するには、次の 2 つの方法があります。

- リモート NFS 共有を設定し、各ノードのデフォルトのバックアップ ディレクトリにマウントします。その場合、バックアップファイルは、Orchestrator VM のローカル ドライブをバイパスするリモート NFS 共有に直接書き込まれます。

  このアプローチでは、Orchestrator GUI から作成されたすべての設定バックアップに 1 つのリモート ロケーションのみを使用できるため、柔軟性が低くなります。

- Orchestrator GUI を使用してリモート SCP または SFTP ロケーションを設定し、そこでバックアップ ファイルをエクスポートします。

  リモート NFS 共有アプローチとは異なり、Orchestrator GUI で 1 つ以上のリモート ロケーションを設定すると、複数の宛先を指定して、バックアップ ファイルを保存できる場所に柔軟性を高めることができます。

（注） 設定のバックアップを作成してリモートサーバにエクスポートすると、ファイルは最初に Orchestrators ローカル ドライブに作成され、その後リモートの場所にアップロードされ、最後にローカル ストレージから削除されます。ローカルバックアップのディスク領域の使用には制限があります。これに達すると、リモートバックアップの作成が妨げられる可能性があります。

バックアップのリモートロケーションの設定

ここでは、設定バックアップをエクスポートできるマルチサイト Orchestrator でリモート ロケーションを設定する方法について説明します。

ステップ 1 Cisco ACI マルチサイト Orchestrator にログインします。

ステップ 2 左側のナビゲーションウィンドウで、**[管理 (Admin)]** > **[リモートロケーション (Remote Locations)]** を選択します。

ステップ 3 メイン ウィンドウの右上隅で、[**リモート ロケーションの追加 (Add Remote Location)**] をクリックします。

[新規リモート ロケーションの追加 (Add New Remote Location)] 画面が表示されます。

ステップ 4 ロケーションの名前と説明 (任意) を入力します。

現在、設定バックアップのリモート エクスポートでは、次の2つのプロトコルがサポートされています。

- SCP
- SFTP

ステップ 5 リモート サーバのホスト名または IP アドレスを指定します。

[**プロトコル (Protocol)**] セクションに基づいて、指定するサーバでは SCP または SFTP 接続を許可する必要があります。

ステップ 6 バックアップを保存するリモート サーバ上のディレクトリへのフルパスを指定します。

パスはスラッシュ (/) 文字で始まる必要があり、ピリオド (.) またはバックスラッシュ (\) を含めることはできません。たとえば、 */backups/multisite*などです。

（注） ディレクトリはすでにリモート サーバに存在している必要があります。

ステップ 7 リモート サーバへの接続に使用するポートを指定します。

デフォルトでは、ポートは22に設定されています。

ステップ 8 リモート サーバに接続するときに使用する認証タイプを指定します。

次の 2 つの認証方式のいずれかを設定できます。

- パスワード: リモート サーバにログインするために使用するユーザ名とパスワードを指定します。
- SSH プライベート ファイル: リモートサーバへのログインに使用するユーザ名と SSH キー/パスフレーズのペアを指定します。

ステップ 9 [**保存 (Save)**] を使用して、リモート サーバを追加します。

既存のバックアップをリモート ロケーションへ移動する

このセクションでは、マルチサイト Orchestrator GUI で作成した既存の設定バックアップを、ノードのローカル ドライブからリモート ロケーションに移動する方法について説明します。

始める前に

次の設定が済んでいる必要があります。

- バックアップの作成 （18 ページ） の説明に従って、設定のバックアップを作成されていること。
- バックアップのリモートロケーションの設定 （15 ページ） の説明に従って、バックアップをエクスポートするためのリモート ロケーションが追加されていること。

ステップ 1 Cisco ACI マルチサイト Orchestrator にログインします。

ステップ 2 左側のナビゲーションウィンドウで、**[管理 (Admin)]** > **[バックアップ (Backups)]** を選択します。

ステップ 3 エクスポートするバックアップを見つけて、その横にあるアクション(⋮)アイコンをクリックし、**[リモート ロケーションへ移動 (Move to remote location)]** をクリックします。

[バックアップをリモート ロケーションに移動 (Move Backup To Remote Location)] ウィンドウが開きます。

ステップ 4 **[リモート ロケーション (Remote location)]** ドロップダウンメニューから、リモート ロケーションを選択します。

ステップ 5 (オプション) リモート ロケーションのパスを更新します。

リモート バックアップのロケーションを作成するときに設定したリモート サーバ上のターゲット ディレクトリが、**[リモート パス (Remote Path)]** フィールドに表示されます。

パスにはサブディレクトリを追加することができます。ただし、ディレクトリはデフォルトの設定済みパスの下にある必要があり、すでにリモート サーバで作成されている必要があります。

Adding an NFS Share to Store Backups

ここでは、設定のバックアップを保存するために、マルチサイト Orchestrator VM に NFS 共有を追加する方法について説明します。

（注） 設定のバックアップには単一のリモート NFS 共有を設定できますが、Orchestrator GUI で使用可能なリモートバックアップロケーション機能を使用することをお勧めします。代わりに、バックアップのリモートロケーションの設定 （15 ページ） で説明します。

ステップ 1 ルートユーザとして、マルチサイト Orchestrator ノードの VM に直接ログインします。

ステップ 2 NFS 共有をマウントします。

次のコマンドは、共有 NFS ディレクトリをデフォルトの Orchestrator バックアップ フォルダにマウントします。これにより、将来のすべてのバックアップは、Orchestrator VM 外の外部ストレージに自動的に保存されます。

（注） 保存するデフォルト ディレクトリに既存のバックアップがある場合は、NFS 共有をマウントする前に、それらを手動で別の場所に移動する必要があります。共有がマウントされると、マウント ディレクトリ内の既存のファイルは表示されなくなります。

```
# mount <nfs-server-ip>:/<nfs-share-path> /opt/cisco/msc/backups/
```

ステップ 3 各 Orchestrator VM でステップ 1 ~ 2 を繰り返します。

各 Orchestrator ノードは独自のバックアップ ファイルを作成して保存できるため、すべてのノードに同じ NFS 共有をマウントする必要があります。

ステップ 4 Docker バックアップ サービスを更新します。

新しくマウントされたファイル システムを Orchestrator サービスで使用可能にするには、次の Docker 更新コマンドを実行する必要があります。ただし、コマンドによってクラスタ全体のサービスが更新されるため、各ノードに共有をマウントした後にこの操作を実行する必要があるのは1回だけです。

```
# docker service update msc_backupservice --force
```

次のタスク

いずれかの時点でNFS共有を削除して、各VMにローカルにバックアップを保存する場合は、各ノードのディレクトリをアンマウントして、`docker service update msc_backupservice--force` コマンドを再度実行します。

バックアップの作成

このセクションでは、 マルチサイト Orchestrator 設定の新しいバックアップを作成する方法について説明します。

始める前に

リモート ロケーションを使用してバックアップを作成する場合は、最初に バックアップのリモートロケーションの設定 （15 ページ） の説明に従ってリモート ロケーションを追加する必要があります。

ステップ 1 Cisco ACI マルチサイト Orchestrator にログインします。

ステップ 2 左側のナビゲーションウィンドウで、**[管理 (Admin)]** > **[バックアップ (Backups)]** を選択します。

ステップ 3 メイン ウィンドウ ペインで、**[新規バックアップ (New Backup)]** をクリックします。

[新規バックアップ (New Backup)] ウィンドウが開きます。

ステップ 4 **[名前 (Name)]** フィールドに、バックアップ ファイルの名前を入力します。

名前には、最大10文字の英数字を使用できますが、スペースまたはアンダースコア (_) は使用できません。

ステップ 5 (オプション) **[注 (Notes)]** フィールドに、バックアップについての追加情報を入力します。

ステップ 6 **[バックアップの場所 (Bacjup Location)]**を選択します。

バックアップファイルは、Orchestrator ノードにローカルに保存するか、またはリモート ロケーションにエクスポートすることができます。

バックアップ ファイルをローカルに保存する場合は、**[ローカル (Local)]** を選択します。

それ以外で、バックアップ ファイルをリモートの場所に保存するには、**[リモート (Remote)]** を選択して次の情報を入力します。

- **[リモート ロケーション (Remote location)]** ドロップダウンメニューから、リモート ロケーションを選択します。

- **[リモートパス (Remote Path)]** では、デフォルトのターゲットディレクトリのままにするか、またはパスにサブディレクトリを追加することができます。ただし、ディレクトリはデフォルトの設定済みパスの下にある必要があり、すでにリモート サーバで作成されている必要があります。

ステップ 7 **[保存（Save）]** をクリックして、バックアップを作成します。

バックアップの復元

このセクションでは、マルチサイト Orchestrator 設定を前の状態に復元する方法について説明します。

始める前に

バックアップ アクションの復元は、マルチサイト Orchestrator でのデータベースを復元しますが、各サイトの APIC データベースには変更を加えません。したがって、Orchestrator データベースを復元した後で、Orchestrator と APIC サイト間のポリシーが食い違う可能性を避けるため、既存のスキーマを再展開する必要もあります。

特定の構成の不一致とそれぞれに関連する望ましい復元手順の詳細は、バックアップと復元に関するガイドライン （14 ページ）を参照してください。

ステップ 1 マルチサイト Orchestrator GUI にログインします。

ステップ 2 必要に応じて、既存のポリシーの展開を解除します。

バックアップが作成されたときから現在の設定までに、設定に新しいオブジェクトまたはポリシーが追加されている場合は、この手順を実行することをお勧めします。追加情報については、バックアップと復元に関するガイドライン （14 ページ） を参照してください。

ステップ 3 左側のナビゲーション メニューで、**[管理 (Admin)]** > **[バックアップ (Backups)]** を選択します。

ステップ 4 メイン ウィンドウで、復元するバックアップの隣のアクション ( ) アイコンをクリックし、**[このバックアップにロールバック (Rollback to this backup)]** を選択します。

選択したバックアップのバージョンが、実行中のマルチサイトのバージョンと異なる場合、ロールバックが原因で、バックアップされたバージョンには存在しない機能が削除される可能性があります。

ステップ 5 **[はい (Yes)]** をクリックして、選択したバックアップを復元することを確認します。

[はい (Yes)] をクリックすると、システムは現在のセッションを終了して、ユーザはログアウトされます。

ステップ 6 必要に応じて、設定を再展開します。

復元された設定を APIC サイトと同期するには、この手順を実行することをお勧めします。追加のコンテキストは、バックアップと復元に関するガイドライン （14 ページ） にあります。

バックアップのダウンロード

ここでは、 マルチサイト Orchestrator からバックアップをダウンロードする方法について説明します。

始める前に

ステップ 1 マルチサイト Orchestrator GUI にログインします。

ステップ 2 左のナビゲーション メニューから**[管理者(Admin)]** > **[バックアップ(Backups)]**を選択します。

ステップ 3 メイン ウィンドウで、ダウンロードするバックアップの隣のアクション ( ) アイコンをクリックし、[**ダウンロード (Download)**] を選択します。

これにより `msc-backups-<タイムスタンプ>.tar.gz` 形式でシステムにバックアップ ファイルがをダウンロードされます。その後、ファイルを抽出してその内容を表示することができます。

バックアップのインポート

ここでは、マルチサイト Orchestrator に既存のバックアップをインポートする方法について説明します。

始める前に

ステップ 1 マルチサイト Orchestrator GUI にログインします。

ステップ 2 左のナビゲーション メニューから**[管理者(Admin)]** > **[バックアップ(Backups)]**を選択します。

ステップ 3 メインウィンドウで、[**インポート (Import)**] をクリックします。

ステップ 4 [**ファイルからインポート (import from file)**] ウィンドウが開いたら、[**ファイルの選択 (Select file)**] をクリックして、インポートするバックアップファイルを選択します。

バックアップをインポートすると、[**バックアップ (backups)**] ページに表示されるバックアップのリストにそのバックアップが追加されます。

カスタム SSL 証明書

Cisco ACI マルチサイト Orchestrator OVA は、Orchestrator のインストール中に各ノードの `/data/msc/secrets` ディレクトリに保存された事故署名付きの SSL 証明書を含みます。デフォルトで、Orchestrator GUI は HTTPS 接続に対してこの証明書を使用します。

Orchestratorノード サーバーに直接ログインして、そのウェブ サーバー (`nginx`) 構成を変更することでこれらの証明書をあらかじめ更新できましたが、Cisco ACI マルチサイト Orchestrator リ

リース 2.1(1) 以降、GUIを使用して、Orchestrator の GUI 接続に使用されるカスタム証明書を簡単に追加または更新できます。

カスタム証明書を追加するときに、次の 2 つのオプションの 1 つを使用できます。

- **自己署名付き証明書** は、Orchestrator の GUI により使用される独自のパブリックとプライベート キーを作成する機能を付与します。
- **CA 発行証明書**は、既存の認証局 (CA) とそのキーにより提供された証明書を使用できます。

GUIでパブリック/プライベートキーの組み合わせを含む複数のCAとキーリングを追加できますが、一度にアクティブにできるのは1つのキーリングのみで、Orchestrator GUIとブラウザー間の通信を保護するために使用できます。

カスタム認証局の追加

HTTPS トラフィックの暗号化のために Orchestrator によって提供されるパブリック キーを検証するために使用されるカスタム認証局 (CA) を追加できます。

このセクションでは、マルチサイト Orchestrator GUI でカスタム CA を追加し、設定する方法について説明します。キーリングとキーの設定については、次のセクションで説明します。

ステップ 1 マルチサイト Orchestrator GUI にログインします。

ステップ 2 左のナビゲーション メニューから **[管理者(Admin)]** > **[セキュリティ(Security)]** を選択します。

ステップ 3 メイン ウィンドウで、**[認証局 (Certificate Authority)]** タブを選択し、**[認証局の追加 (Add Certificate Authority)]** をクリックします。

ステップ 4 開いた **[認証局の追加 (Add Certificate Authority]** ウィンドウで、CA の詳細を指定します。

[名前 (Name)]フィールドに、認証局の名前を入力します。

[説明 (Description)] フィールドに、説明を入力します。

[証明書チェーン(Certificate Chain)] フィールドに、CA の証明書チェーンを入力します。中間証明書とルート証明書の両方を含める必要があります。中間証明書を最初に入力し、その後にルート証明書を入力する必要があります。

ステップ 5 **[保存 (Save)]** をクリックして、変更内容を保存します。

カスタム キーリングの追加

Orchestrator GUI の HTTPS トラフィックの暗号化に使用される公開キーと秘密暗号キーを含むカスタムキーリングを追加できます。

ここでは、カスタム キーリングを追加する方法について説明します。このキーリングで公開キーの確認に使用できる認証局 (CA) を追加する手順については、前のセクションを参照してください。

ステップ 1 マルチサイト Orchestrator GUI にログインします。

ステップ 2 左のナビゲーション メニューから **[管理者(Admin)]** > **[セキュリティ(Security)]** を選択します。

ステップ 3 メインウィンドウで、 **[キーリング (Key Rings)]** タブを選択し、**[キーリングの追加 (ADD KEY RING)]** をクリックします。

ステップ 4 **[キーリングの作成 (Create Key Ring)]** ウィンドウが開くので、キーリングの詳細を入力します。

[認証局の選択 (SELECT CERTIFICATE AUTHORITY)]ドロップダウンメニューから、キーリングを含む認証局を選択します。

[名前 (Name)]フィールドに、キーリングの名前を入力します。

[キーリングの説明 (KEY RING DESCRIPTION)] フィールドに、キーリングの説明を入力します。

[公開キー (PUBLIC KEY)] フィールドに、リングの公開キーを入力します。

[**秘密キー (PRIVATE KEY)]** フィールドに、リングの秘密キーを入力します。

ステップ 5 **[保存 (Save)]** をクリックして、変更内容を保存します。

カスタムキーリングのアクティブ化

前のセクションで説明したようにキーリングを追加した後、デフォルトのキーリングとしてアクティブ化する必要があります。

ステップ 1 マルチサイト Orchestrator GUI にログインします。

ステップ 2 左のナビゲーション メニューから **[管理者(Admin)]** > **[セキュリティ(Security)]** を選択します。

ステップ 3 メインウィンドウで、**[キーリング (Key Rings)]** タブを選択します。

ステップ 4 メインウィンドウで、アクティブにするキーリングの横にある **[...]** アイコンをクリックし、**[キーリングをアクティブにする (Make Keyring Active)]** を選択します。

ステップ 5 キーリングをアクティブにするには、**[アクティベート(ACTIVATE)]** をクリックします。

キーをアクティブにすると、 マルチサイト Orchestrator GUI からログアウトされます。ログインページがロードされると、新しい証明書とキーが使用されます。

カスタム証明書のトラブルシューティング

ここでは、マルチサイト Orchestrator でカスタム SSL 証明書を使用する場合の一般的な問題を解決する方法について説明します。

Orchestrator GUI をロードできません

カスタム証明書をインストールしてアクティブ化した後に Orchestrator GUI ページをロードできない場合は、各 Orchestrator ノードに証明書が正しくコピーされていない可能性があります。この問題を解決するには、デフォルトの証明書を回復してから、新しい証明書のインストール手順を再度繰り返します。

デフォルトの Orchestrator 証明書を回復するには、次のようにします。

1. 各 Orchestrator ノードに直接ログインします。
2. 証明書ディレクトリに移動します。

```
# cd /data/msc/secrets
```

3. msc.key ファイルと msc.cert ファイルを、それぞれ msc.key_backup ファイルと msc.cert_backup ファイルに置き換えます。

```
# cp msc.key_backup msc.key
# cp msc.cert_backup msc.cert
```

4. Orchestrator GUI サービスを再起動します。

```
# docker service update msc_ui --force
```

5. 前のセクションで説明したように、新しい証明書を再インストールしてアクティブにします。

クラスタへの新しい Orchestrator ノードの追加

マルチサイト Orchestrator クラスタに新しいノードを追加する場合は、次のようにします。

1. Orchestrator GUI にログインします。
2. 前のセクションで説明したように、使用しているキーを再度アクティブにします。

外部認証

RADIUS、TACACS+、LDAP サーバを使用して、外部ユーザ認証と認可を設定できます。

マルチサイト Orchestrator 管理者は、次のことができます。

- 1 つ以上の外部認証プロバイダを追加します。

  冗長性のために、少なくとも 2 つの認証プロバイダを設定することをお勧めします。

- ログイン ドメインを作成し、プロバイダに関連付けます。

  デフォルト ドメインは、ローカル認証のためのローカル ドメインです。

- ユーザをドメインに割り当てます。

ドメインを作成した後、ドメインの編集、非アクティブ化または削除を行えます。ローカル ドメインを削除することはできませんが、非アクティブにすることはできます。

監査ログは、外部認証と承認をサポートします。

外部認証サーバの設定に関するガイドライン

マルチサイトOrchestrator ユーザ認証用の外部認証サーバを設定する場合は、次のようにします。

- リモート認証サーバーのユーザごとに設定を行う必要があります。
- 各ユーザに対して、そのユーザに割り当てられた使用権限(ロール)を指定して、カスタム属性値 (AV) ペアを追加する必要があります。ロールについては、ユーザ、ロール、および権限に記載されています。

  ロールを指定する場合は、次の形式を使用します。

  `cisco-av-pair=shell:msc-roles=role1,role2`

  次に例を示します。

  `cisco-av-pair=shell:msc-roles=siteManager,schemaManager.`

- リリース 2.1 (2) 以降では、各ユーザ ロールを読み取り専用モードで割り当てることができます。読み取り専用権限が付与されている場合、ユーザは以前と同様に、そのロールで使用可能な任意のファブリック オブジェクトを表示できますが、それらのオブジェクトに変更を加えることはできません。

  AV ペアの文字列形式は、特定のユーザに読み取り専用または読み取り専用のロールを設定する場合に異なります。次の例では、読み取り/書き込みロールはスラッシュ (/) 文字を使用して読み取り専用ロールから分離されていますが、個々のロールはパイプ (|) 文字で区切られています。

  `cisco-av-pair=shell:msc-roles=writeRole1|writeRole2/readRole1|readRole2`

  次の例は、スキーマ マネージャとユーザ マネージャのロールをユーザに割り当てる方法を示していますが、サイト マネージャのユーザに表示されるオブジェクトを表示することもできます。

  `shell:msc-roles=schemaManager|userManager/siteManager`

  ユーザの読み取り専用権限または読み取り/書き込み権限のみを設定する場合は、スラッシュ (/) 文字を含める必要があります。次の例は、Site Manager ロールで使用可能なオブジェクトへの読み取り/書き込みアクセスまたは読み取り専用アクセスを設定する方法を示しています。

  - 読み取り専用: `shell:msc-roles=/sitemanager`
  - 読み取り/書き込み: `shell:msc-roles=sitemanager/`

（注） 古い(カンマ区切り) 書式または新しい(パイプとスラッシュ) 書式のどちらでもサポートされていますが、単一のユーザを設定するときにそれらを混在させることはできません。混在または不適切に書式設定された AV 文字列は解析されず、ユーザ ロールは設定されていません。

- 読み取り専用ユーザ ロールを設定してから、マルチサイト Orchestrator を以前のバージョンにダウングレードした場合、読み取り専用権限はサポートされません。これらのロールは、すべてのユーザから削除されます。これは、読み取り専用ロール**のみ**を持つすべてのユーザにロールが割り当てられず、削除されることも意味します。パワーユーザまたはユーザ マネージャは、ユーザを再度作成し、新しい読み取り/書き込みロールを割り当てる必要があります。
- LDAP 設定のベストプラクティスは、属性文字列として**`CiscoAVPair`**を使用することです。何らかの理由で、オブジェクト ID `1.3.6.1.4.1.9.22.1`を使用できない場合は、追加のオブジェクト ID `1.3.6.1.4.1.9.2742` を使用できません。*`1-5`*は、LDAP サーバでも使用できます。

RADIUS または TACACS+ を認証プロバイダとして追加する

このセクションでは、Cisco ACI マルチサイト Orchestrator ユーザを認証するための外部認証サーバとして 1 つ以上の RADIUS または TACACS+ サーバーを追加する方法を説明します。

ステップ 1 ローカル ドメインを使用して、Cisco ACI マルチサイト Orchestrator に `admin` ユーザとしてログインします。

ステップ 2 左側のナビゲーション ペインから **[管理 (Admin)]** > **[プロバイダ (Provider)]** を選択します。

ステップ 3 メインウィンドウで、**[プロバイダの追加 (Add Provider)]**をクリックします。

ステップ 4 外部認証サーバのホスト名または IP アドレスを入力します。

ステップ 5 (オプション) 追加するプロバイダの説明を入力します。

ステップ 6 追加するプロバイダ タイプとして、**[RADIUS]** または **[TACACS +]** を選択します。

ステップ 7 **[キー (KEY)]** フィールドにキーを入力し、**[キーの確認 (CONFIRM KEY)]** フィールドでそれを確認します。

ステップ 8 (オプション)。追加設定を行います。

a) **[Additional Settings (追加設定)]**] を展開して、詳細設定を行います。

b) 認証サーバに接続するために使用されるポートを指定します。

デフォルトのポートは、 **RADIUS** の場合は `1812`、 **TACACS +** の場合は `49` です。

c) 使用するプロトコルを指定します。

[PAP] プロトコルと **[CHAP]** プロトコルのいずれかを選択します。

d) 認証サーバに接続する際のタイムアウトと試行回数を指定します。

LDAP を認証プロバイダとして追加する

このセクションでは、Cisco ACI マルチサイト Orchestrator ユーザを認証するための外部認証サーバとして 1 つ以上の LDAP サーバーを追加する方法を説明します。

ステップ 1 ローカル ドメインを使用して、Cisco ACI マルチサイト Orchestrator に `admin` ユーザとしてログインします。

ステップ 2 左側のナビゲーション ペインから **[管理 (Admin)]** > **[プロバイダ (Provider)]** を選択します。

ステップ 3 メインウィンドウで、**[プロバイダの追加 (Add Provider)]**をクリックします。

ステップ 4 外部認証サーバのホスト名または IP アドレスを入力します。

ステップ 5 (オプション) 追加するプロバイダの説明を入力します。

ステップ 6 追加する追加するプロバイダのタイプとして、**[LDAP]** を選択します。

ステップ 7 LDAP サーバの **[ベース DN (Base DN)]**、**[バインド DN (Bind DN)]**、および **[キー (Key)]** 値を入力します。

ベース DN とバインド DN は、LDAP サーバがどのように設定されているかに応じて決まります。ベース DN とバインド DN 値は、LDAP サーバで作成されたユーザの識別名から取得できます。

ベース DN は、サーバがユーザを検索するポイントです。たとえば、 `DC = mso, DC = local`のようになります。

バインド DN は、サーバに対する認証に使用されるクレデンシャルです。たとえば、 `CN = admin, CN = Users, DC = mso, DC = local`のようになります。

バインド DN には、次のフィールドに入力できるキーを付属させます。

ステップ 8 (オプション) LDAP 通信で SSL を有効にします。

a) **[有効（Enabled）]** チェックボックスをオンにします。

b) 使用する証明書を選択します。

c) 検証レベルを選択します。

[許可 (Permissive):] 任意の認証局 (CA) によって署名された証明書を受け入れ、暗号化に使用します。

[制限あり (Restrictive):] 使用する前に証明書チェーン全体を確認します。

ステップ 9 (オプション)。追加設定を行います。

a) **[追加設定 (Settings)]** をクリックして展開します。

b) LDAP サーバに接続するポートを指定します。

LDAP のデフォルトのポートは `389` です。

c) 認証サーバに接続する際のタイムアウトと試行回数を指定します。

d) 使用するフィルタを指定します。

フィルタ値はLDAPサーバの設定によって異なります。デフォルトのLDAPフィルタは(cn = username)です。ただし、Microsoft LDAP サーバを使用している場合は、代わりにフィルタを(sAMAccountName = {username})に設定します。

e) 認証タイプを指定します。

認証タイプは次のとおりです。

- **[Cisco AVPair]**: 属性値 (AV) ペアを使用して、個々のユーザのロールに基づいて認可を設定します。この方法を使用する場合は、**[属性 (Attribute)]** フィールドを [Ciscoavpair] に設定します。

  また、次の形式でAVペア文字列を使用して、LDAPサーバで各ユーザを個別に設定する必要があります。

  - リリース 2.1(2) 以降:

    ```
    cisco-av-pair=shell:msc-roles=writeRole1|writeRole2/readRole1|readRole2
    ```

  - リリース 2.1(1) 以前:

    ```
    cisco-av-pair=shell:msc-roles=role1,role2
    ```

  詳細については、外部認証サーバの設定に関するガイドライン （24 ページ）を参照してください。

- **[LDAP グループマップルール (LDAP Group Map Rules)]**: LDAP サーバ グループを使用して、ユーザのグループ メンバシップに基づいて許可を設定します。この方法を使用する場合は、**[属性 (Attribute)]** フィールドを [memberOf] に設定し、 **[+LDAP グループ マップ ルール (+ LDAP group Map Rules)]** をクリックしてグループ メンバシップを指定します。

  [新しいグループ マップ ルール (New Group Map Rule)]で、グループ DN と (たとえば、CN=group1,OU=msc-ou,DC=msc,DC=local)、そのグループに割り当てられるユーザ ロールを指定します。同じグループ マップ ルールに複数のロールを追加できます。各ユーザロールの詳細な説明については、ユーザ、ロール、および権限を参照してください。

ログイン ドメインの作成

ログイン ドメインは、ユーザの認証ドメインを定義します。ログイン ドメインは、ローカル、RADIUS、TACACS+、または LDAP 認証メカニズムを設定できます。

GUI を使用して Cisco ACI マルチサイト Orchestrator にログインする場合には、ユーザが選択できるよう、ログイン画面にドメインのドロップダウン リストが表示されます。ドメインを指定しなかった場合は、ローカル ドメインがユーザ名の検索のために使用されます。

REST API を使用して Cisco ACI マルチサイト Orchestrator にログインする場合には、POST メッセージのログイン情報とともにログイン ドメインが指定されます。たとえば、次のようになります。

```
{
    "username":"bob",
    "password":"We1come2msc!",
```

```
    "domainId":"59d5b5978d0000d000909f65"
}
```

Cisco ACI マルチサイト Orchestrator GUI でログイン ドメインを作成するには、次の手順に従います。

始める前に

RADIUS または TACACS+ を認証プロバイダとして追加する （25 ページ） または LDAP を認証プロバイダとして追加する （26 ページ） で説明されているように、1 つ以上の認証プロバイダを追加しておく必要があります。

ステップ 1 Cisco ACI マルチサイト Orchestrator にログインします。

ステップ 2 左側のナビゲーション ペインから **[管理 (Admin)]** > **[ログイン ドメイン(Login Domains)]** を選択します。

ステップ 3 メインウィンドウで、[**ログインドメインの追加 (ADD LOGIN DOMAIN)**] をクリックします。

ステップ 4 ドメイン名を入力します。

ステップ 5 （オプション）ドメインの説明を入力します。

ステップ 6 認証プロバイダを指定するために、 **[レルム (REALM)]** のタイプを選択します。

ログイン ドメインを作成する前に、外部認証プロバイダを追加しておく必要があります。

ステップ 7 ログイン ドメインを 1 つ以上のプロバイダに割り当てます。

ドメインに割り当てる 1 つ以上のプロバイダ名の横のチェックボックスをオンにします。

次のタスク

ドメインを作成した後、ログイン ドメインの編集、削除、または非アクティブ化 （28 ページ） で説明されているように、ドメインの編集、非アクティブ化または削除を行えます。

ログイン ドメインの編集、削除、または非アクティブ化

1つ以上のログインドメインを作成した後、このセクションで説明されている手順を使用して、それらを編集、削除、または非アクティブ化することができます。ローカル ドメインを削除することはできませんが、非アクティブにすることはできます。

始める前に

ログイン ドメインの作成 （27 ページ） の説明に従って、1 つ以上のログインドメインを作成しておく必要があります。

ステップ 1 Cisco ACI マルチサイト Orchestrator にログインします。

ステップ 2 左側のナビゲーション ペインから **[管理 (Admin)]** > **[ログイン ドメイン(Login Domains)]** を選択します。

ステップ 3 編集するログイン ドメインの横にある **...** メニューをクリックします。

ドメイン情報を**編集**し、使用できないようにドメインを**非アクティブ化**するか、**デフォルトとして設定**して、GUI を使用してログインするときに自動的に選択されるように選択できます。

リモート ユーザのログイン

外部認証が Cisco ACI マルチサイト で有効になっている場合には、以下の方法で マルチサイト Orchestrator にログインできます。

ステップ 1 ブラウザを使用して、 マルチサイト URL に移動します。

ステップ 2 ドロップダウン リストから、自分が割り当てられているドメインを選択します。

ステップ 3 ユーザ名とパスワードを入力します。

ステップ 4 **[送信 (Submit)]**をクリックします。
許可を受けており、認証が成功すれば、マルチサイト Orchestrator GUI が表示され、割り当てられているロールに従って権限が与えられます。パスワードは、初回ログオン時に変更する必要があります。

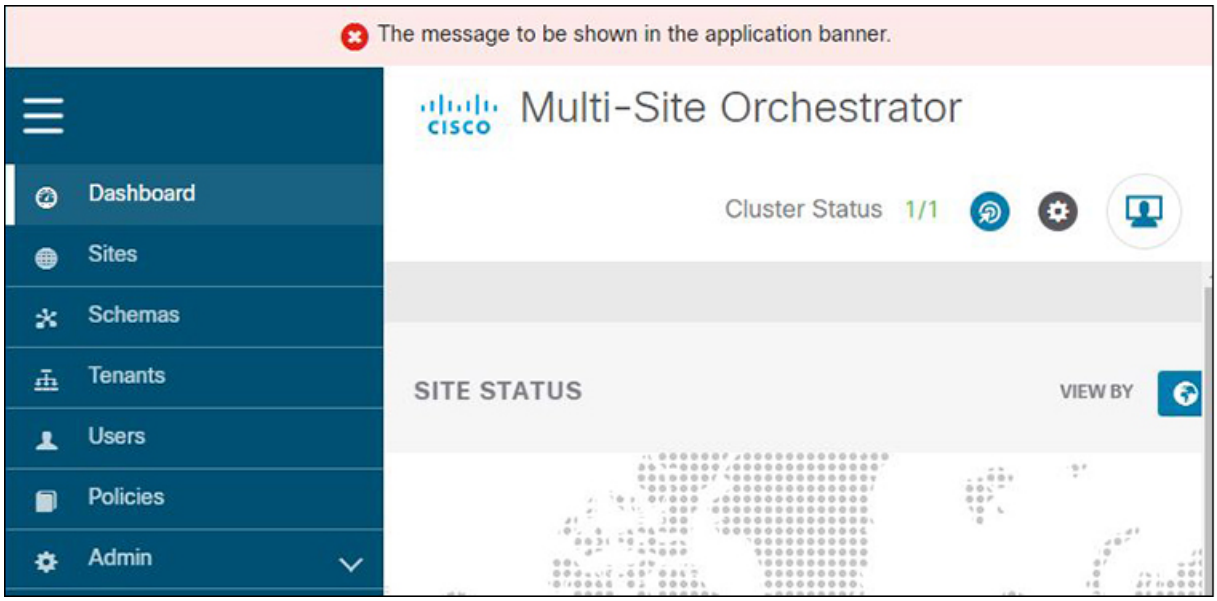
システム設定

次のセクションで説明するように、Multi-Site Orchestrator に対して設定できる、 **管理** > **システム設定**で使用可能なグローバルシステム設定が多数あります。

システム エイリアスとバナー

このセクションでは、マルチサイト Orchestrator のエイリアスを設定する方法と、次の図に示すように、GUI 全体で画面の上部に表示されるカスタムのバナーを有効にする方法について説明します。

図 *1:* システム バナーの表示



ステップ 1 Orchestrator にログインします。

ステップ 2 左側のナビゲーション ペインから**[管理 (Admin)]** > **[システム設定 (System Configuration)]** を選択します。.

ステップ 3 **[編集 (Edit)]** のアイコンをクリックします。これは**[システム エイリアスとバナー System Alias & Banners)]** 領域の右にあります。

[システム エイリアスとバナー System & Banners)] の設定ウィンドウが表示されます。

ステップ 4 **[エイリアス (Alias)]** フィールドで、システムのエイリアスを指定します。

ステップ 5 GUI バナーを有効にするかどうかを選択します。

ステップ 6 バナーを有効にする場合には、バナーに表示されるメッセージを指定する必要があります。

ステップ 7 バナーを有効にする場合には、バナーの重大度を意味する色を選択する必要があります。

ステップ 8 **[保存（Save）]** をクリックして、変更内容を保存します。

ログイン試行回数とロックアウト時間

Orchestratorがログイン試行を連続して失敗したことが検出されると、そのユーザは、不正アクセスを防ぐために、システムからロックアウトされます。ログイン試行が失敗した場合の処理方法は設定できます。たとえば、何回失敗するとロックアウトされるか、およびロックアウトの長さなどがあります。

（注） この機能は、リリース 2.2(1) 以降を最初にインストールしたとき、アップグレードしたときにデフォルトで有効になります。

ステップ 1 Orchestrator にログインします。

ステップ 2 左側のナビゲーション ペインから**[管理 (Admin)]** > **[システム設定 (System Configuration)]** を選択します。.

ステップ 3 **[試行の失敗&ロックアウト時間 (Fail Attempts & Lockout Time)]**エリアの右側にある **[編集 (Edit)]** アイコンをクリックします。

これにより、**[試行の失敗&ロックアウト時間 (Fail Attempts & Lockout Time)]** 設定ウィンドウが表示されます。

ステップ 4 **[試行の失敗の設定 (Fail Attempts Settings)]** ドロップダウンから、ユーザが何回試行に失敗するとロックアウトされるかを選択します。

ステップ 5 **[ロックアウト時間 (分) (Lockout Time (Minutes)]** ドロップダウンから、ロックアウトの長さを選択します。

これは、トリガーされた後の、基本的なロックアウト期間を指定します。このタイマーは、さらにログイン試行が連続して失敗するたびに、3 ずつ延長されます。

ステップ 6 **[保存（Save）]** をクリックして、変更内容を保存します。

プロキシ サーバ

オンプレミスとクラウド サイトの組み合わせや、社内ネットワーク内で実行されている Orchestrator などの特定の導入シナリオでは、Orchestrator はプロキシを介してインターネットおよびクラウドサイトにアクセスする必要があります。プロキシは、このセクションで説明されている方法で設定して有効にすることができます。

プロキシ サーバが有効になっている場合でも、Orchestrator は、プロキシをバイパスして直接通信する、IP アドレスとホスト名の「プロキシなし」リストを維持します。このリストは、ユーザ指定のホストまたはドメインと、現在 Orchestrator に追加されているすべてのオンプレミス APIC サイトの組み合わせです。新しいサイトを Orchestrator に追加するなど、新しいアドレスでリストが更新されるたびに、プロキシサービスは再起動されます。すべてのオンプレミスサイトの完全なリストを事前に指定しておけば、サービスの再起動を最小限に抑えることができます。たとえば、プロキシ設定の構成時に、ドメイン全体を「プロキシなし」リストに追加します。

ステップ 1 Orchestrator にログインします。

ステップ 2 左側のナビゲーション ペインから**[管理 (Admin)]** > **[システム設定 (System Configuration)]** を選択します。.

ステップ 3 **[プロキシ サーバ (Proxy Server)]** エリアの右側の **[編集 (Edit)]** アイコンをクリックします。

これにより、**[プロキシ設定 (Proxy Settings)]** ウィンドウが開きます。

ステップ 4 **[有効化 (Enable)]** を選択して、プロキシを有効にします。

ステップ 5 **[プロキシ サーバ (Proxy Server)]** フィールドで、プロキシ サーバの IP アドレスまたはホスト名を指定します。

ステップ 6 **[プロキシ サーバ ポート (Proxy Server Port)]** フィールドで、プロキシ サーバに接続するために使用するポート番号を指定します。

ステップ 7 **[プロキシなしリスト (No Proxy List)]** フィールドで、プロキシをバイパスするホストとドメインのコンマ区切りのリストを指定します。

リストを指定するときには、IP アドレスまたはホスト名を指定します。または、ワイルドカード (*) 文字を使用して、ドメイン全体を指定することもできます。IP アドレスにワイルドカードを使用することはできません。

たとえば、`203.0.113.1, apic1.example.com, *.example.local` のようにします。

ステップ 8 **[保存 (Save)]**をクリックして、変更内容を保存します。

プロキシを設定して有効にすると、Orchestrator アプリケーションが再起動します。