その他の ACI セキュリティ機能

この章は、次の項で構成されています。

その他のセキュリティ機能

現在 ACI でサポートされているその他のセキュリティ機能は次のリストのとおりです。それぞれの詳細については、他の構成ガイドで説明されています（https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html）。

- **コントラクト**の設定については、『*Cisco APIC Basic Configuration Guide, Release 3.x*（Cisco APIC 基本設定ガイド リリース 3.x）』および『*Operating Cisco Application Centric Infrastructure*（シスコ アプリケーション セントリック インフラストラクチャの運用）』を参照してください。
- **EPG 通信ルール**については、ナレッジベースの記事『*Use vzAny to Automatically Apply Communication Rules to all EPGs in a VRF*（vzAny を使用して通信ルールを VRF 内のすべての EPG に自動的に適用する ）』を参照してください。
- **インバンドおよびアウトオブバンドの管理アクセス**については、ナレッジベースの記事『*Cisco APIC and Static Management Access*（Cisco APIC と静的管理アクセス）』および『*Cisco APIC Layer 4 to Layer 7 Services Deployment Guide, Release 2.2(3)*（Cisco APIC レイヤ 4 ～ レイヤ 7 サービス導入ガイド、リリース 2.2(3)）』を参照してください。
- **EPG 内での分離適用**については、『*Cisco ACI Virtualization Guide, Release 3.0(1)*（Cisco ACI 仮想化ガイド、リリース 3.0 (1)）』を参照してください。
- **トラフィック ストーム制御**については、『*Cisco APIC Layer 2 Networking Configuration Guide*（Cisco APIC レイヤ 2 ネットワーキング設定ガイド）』を参照してください。

インフラ VLAN トラフィックの制限

ファブリック内のハイパーバイザー間の分離を強化するために、インフラ VLAN トラフィックをインフラ セキュリティ エントリ ポリシーで指定されたネットワーク パスのみに制限できます。この機能を有効にすると、各リーフ スイッチは、コンピューティング ノードからのインフラ VLAN トラフィックを制限して、VXLAN トラフィックのみを許可します。また、スイッチは、リーフ ノードへのトラフィックを制限して、OpFlex、DHCP/ARP/ICMP、および iVXLAN/VXLAN トラフィックのみを許可します。APIC 管理トラフィックは、インフラ VLAN のフロント パネル ポートで許可されます。

この機能は、デフォルトで無効にされています。この機能を有効にするには、次の手順を実行します。

手順

ステップ 1 メニュー バーで、**[システム（System）] > [システム設定（System Settings）]** を選択します。

ステップ 2 ナビゲーション ペインで **[ファブリック幅設定（Fabric-Wide Settings）]** をクリックします。

ステップ 3 [作業（Work）] ペインで、**[インフラ VLAN トラフィックの制限（Restrict Infra VLAN Traffic）]** のチェックボックスをオンにします。

ステップ 4 [Submit] をクリックします。

APIC で生成されたセッション ログ ファイルをオフにする

このセクションでは、APIC で生成されたログをオフにする方法について説明します。ファブリックに何らかの監視を設定している場合は、次のログ ファイルが表示されます。

```
Body of session record log example:
From-127.0.0.1-client-type-REST-Success
```

APIC で生成されたセッション ログ ファイルをオフにするには、次の手順を実行します。

手順

ステップ 1 メニュー バーで、**[ADMIN] > [AAA]** を選択します。

ステップ 2 **[AAA]** ペインで、**[セキュリティ（Security）]** をクリックします。

ステップ 3 **[ユーザー管理 – セキュリティ（User Management – Security）]** ペインで、デフォルトの **[管理設定（Management Settings）]** ペインが選択されていることを確認します。

ステップ 4 **[セッション レコードに更新を含める（Include Refresh in Session Records）]** フィールドで、チェック ボックスをオフにして、生成されたセッション ログ ファイルを無効にします。

ステップ 5 [送信（Submit）] をクリックします。

ステップ 6 **[変更の送信（Submit Changes）]** をクリックします。

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。