

Cisco ACI の強化

概要

近年、サイバー攻撃はあらゆる規模や業界の組織にとってますます一般的な脅威となっています。ハッカーは、システムやネットワークの脆弱性を悪用する新しい戦術や技術を常に考案しているため、組織はインフラストラクチャの強化などのセキュリティ対策を優先することが不可欠です。

インフラストラクチャの強化には、攻撃対象領域を縮小し、組織のデジタルインフラストラクチャの基盤となるコンポーネントを強化するためのさまざまなセキュリティ対策の実装が含まれます。これには、強力なパスワードと多要素認証の実装、機密情報へのアクセスの制限、ファイアウォールと侵入検知システムのインストール、ソフトウェアとハードウェアのバージョンを最新のパッチとアップデートで最新の状態に保つことが含まれます。

インフラストラクチャの強化策を実装することで、組織はサイバー攻撃のリスクを大幅に軽減できます。システムとネットワークのセキュリティを強化することで、ハッカーが機密情報にアクセスしたり、データを盗んだり、運用に損害を与えたりすることをはるかに困難にすることができます。さらに、効果的なインフラストラクチャの強化は、組織が規制コンプライアンス要件を満たし、セキュリティへの取り組みを示すことで評判を保護するのに役立ちます。

Cisco では、製品開発プロセスのあらゆる側面でセキュリティを優先しています。Cisco は、すべての環境が独自のものであり、サイバー攻撃に対する最適な保護を確保するために特定のセキュリティ機能とメカニズムが必要であることを理解しています。

特に Cisco Application Centric Infrastructure (ACI) については、Cisco の主力製品であるデータセンター ソフトウェア定義型ネットワーク ソリューションは、業界標準と認定に準拠するように構築されています。Cisco ACI は、次のセキュリティ認定を取得しています。

- DoD UC APL ([Cisco ACI Certification Letter](#))
- 共通条件 ([Cisco ACI 証明書レポート](#))
- FIPS 140-2 ([Cisco ACI Compliance Letter](#))

さらに、Cisco ACI ソリューションは、[Verizon](#) によって証明されているように、顧客のカード所有者データ環境内で PCI コンプライアンス要件を満たしていることが証明されています。

Cisco ACI は最大限のセキュリティを念頭に置いて設計されていますが、各環境の特性に基づいてファブリックを適切に強化するために、使用可能な機能を有効にしてカスタマイズするには、いくつかの構成と調整が必要な場合があります。

このドキュメントの目的

このホワイトペーパーでは、Cisco ACI が最高のセキュリティ標準を満たし、攻撃に対する復元力があることを確認するための Cisco ACI の設定に関する推奨事項とガイダンスを提供します。

管理者がネットワーク インフラストラクチャを適切に強化するために焦点を当てる必要がある主な領域は、管理プレーン、コントロールプレーン、およびデータプレーンの 3 つです。3 つの領域はすべて、適切に強化されていないと侵害される可能性があるため等しく重要です。これらの領域への攻撃は、性質は異なりますが、同等の影響を与える可能性がある重大な損害を引き起こす可能性があります。

このホワイトペーパーでは、これら 3 つの領域の強化、Cisco ACI を強化するためにお客様が実行する必要がある推奨構成、および特定のシナリオで使用できる機能と使用する必要がある機能について、一般的な質問に回答します。

さらにこのホワイト ペーパーでは、安全な運用に最も関連する原則のいくつかと、システムを保護するためにエンジニアリングおよび製造の観点から Cisco ACI および Cisco Nexus 9000 で選択されたアーキテクチャの選択について説明します。

セキュアな運用の原則

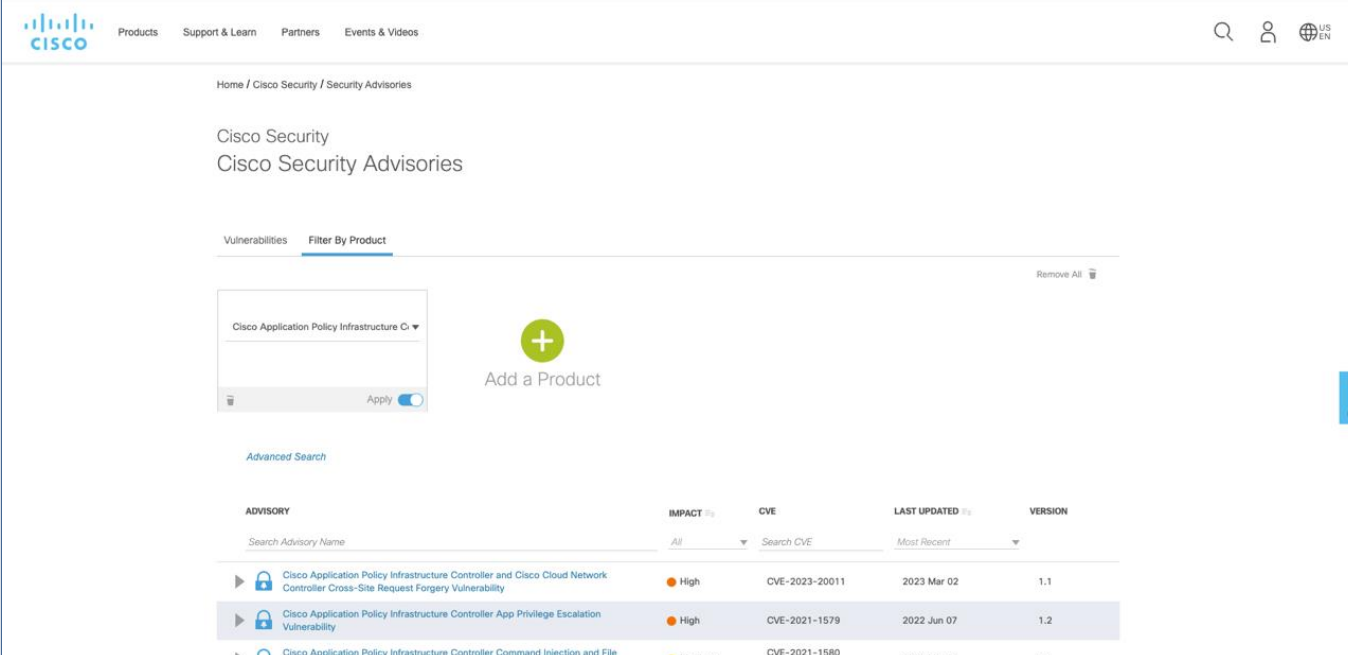
このドキュメントの大半は、Cisco ACI ファブリックの安全な構成について説明していますが、ネットワークを完全に保護するためには構成のみでは不十分です。基本となるデバイスの構成と同様に、ネットワークで 사용되는操作手順も、セキュリティにとって大きな役割を果たします。

このセクションでは、ネットワークを安全に維持し、攻撃対象領域と露出を最小限に抑えるのに役立つように、実装することを勧める運用上の推奨事項について説明します。このセクションでは、ネットワーク運用の重要な領域に焦点を当てており、包括的ではない場合があります。

Cisco セキュリティ アドバイザリおよびレスポンスの監視

Cisco Product Security Incident Response Team (PSIRT) は、Cisco 製品のセキュリティ関連問題に関して、Cisco PSIRT セキュリティ アドバイザリと呼ばれる通知を作成し、維持しています。

Cisco セキュリティ脆弱性ドキュメントは <http://www.cisco.com/go/psirt> で入手できます。



The screenshot shows the Cisco Security Advisories portal. At the top, there is a navigation bar with the Cisco logo and links for Products, Support & Learn, Partners, and Events & Videos. Below the navigation bar, the page title is "Cisco Security Advisories". There is a "Filter By Product" section with a dropdown menu currently set to "Cisco Application Policy Infrastructure". Below this, there is a table of advisories with columns for ADVISORY, IMPACT, CVE, LAST UPDATED, and VERSION. The table contains three rows of data.

ADVISORY	IMPACT	CVE	LAST UPDATED	VERSION
Cisco Application Policy Infrastructure Controller and Cisco Cloud Network Controller Cross-Site Request Forgery Vulnerability	High	CVE-2023-20011	2023 Mar 02	1.1
Cisco Application Policy Infrastructure Controller App Privilege Escalation Vulnerability	High	CVE-2021-1579	2022 Jun 07	1.2
Cisco Application Policy Infrastructure Controller Command Injection and File Upload Vulnerabilities	Medium	CVE-2021-1580 CVE-2021-1581	2022 Mar 08	1.1

図 1. Cisco セキュリティ アドバイザリ ポータル

Cisco は、毎年 2 回、グリニッジ標準時 (GMT) の 16:00 に定期的に Cisco セキュリティ アドバイザリのバンドルをリリースします。特定のリリース日とスケジュールは、Cisco 製品ごとに異なります。具体的には、Cisco ACI および NX-OS の場合、バンドルは 2 月と 8 月の第 4 水曜日の 16:00 GMT にリリースされます。

Cisco は、上記のスケジュール以外に個々のセキュリティ アドバイザリを公開する権利を留保します。

セキュアなネットワークを維持するために、リリース済みの Cisco セキュリティ アドバイザリおよびレスポンスに注意する必要があります。これを用意にするため、複数の方法で最新のセキュリティ脆弱性情報を Cisco から常時受信することができます。

Cisco.com

Cisco.com の [Cisco セキュリティ](#) ポータルは、Cisco のセキュリティ脆弱性関連ドキュメントと、関連する Cisco セキュリティ製品およびサービスを含む Cisco のセキュリティの情報を提供します。

電子メール

Cisco セキュリティ アドバイザリは、重大度が **Critical**、**High**、および **Medium** のセキュリティ脆弱性に関する情報を提供します。これらは、Cisco PSIRT [PGP 公開キー](#) でクリア署名され、サブスクライブ可能な外部の cust-security-announce@cisco.com メーリングリストに配布されます。

cust-security-announce メーリングリストに登録するには、cust-security-announce-join@cisco.com まで電子メールでお問い合わせください（メッセージの内容は問いません）。メールの受信確認、リストの説明、リストのポリシー ステートメントが記載されたメッセージが返信されます。

RSS フィード

Cisco のセキュリティ脆弱性情報は、Cisco.com の RSS フィードからも入手可能です。RSS フィードへの登録方法については、[シスコ セキュリティ RSS フィード ページ](#) [英語] を参照してください。

Cisco PSIRT openVuln API

Cisco PSIRT openVuln アプリケーションプログラミング インターフェイス (API) は、Cisco のセキュリティ脆弱性情報をマシンで処理可能な各種形式で配信する RESTful API です。この API へのアクセス方法と使用方法については、Cisco DevNet Web サイトの [PSIRT ページ](#) [英語] を参照してください。

マイ通知

[マイ通知 Web サイト](#)では、登録済みの Cisco.com ユーザーが、Cisco セキュリティ アドバイザリを含む重要な Cisco 製品およびテクノロジー情報を購読して受信できます。

シスコのセキュリティ脆弱性情報開示のポリシーおよび公表資料については、[セキュリティ脆弱性ポリシー](#)を参照してください。

Cisco Nexus Dashboard Insights

Cisco Nexus Dashboard Insights は、Insights、可視性、分析を提供することで、データセンター ネットワークの管理、運用、およびトラブルシューティングを支援する、Cisco の Day-2 運用ソリューションです。

Nexus Dashboard Insights が提供するさまざまなユース ケースと機能の中には、データセンター ファブリックに影響を与えるセキュリティ アドバイザリと Field Notice についてプロアクティブに通知する機能があります。

上記のオプションとは対照的に、Nexus Dashboard Insightsは、使用されているソフトウェア リリース、ハードウェア モデル、および機能に基づいて、環境に影響を与えるセキュリティ アドバイザリについてのみ通知します。システムに影響を与えるセキュリティ アドバイザリについては、推奨されるアクションの詳細な説明が記載されています。したがって、Nexus Dashboard Insights を使用すると、セキュリティ アドバイザリのモニタリングと対応が容易になります。

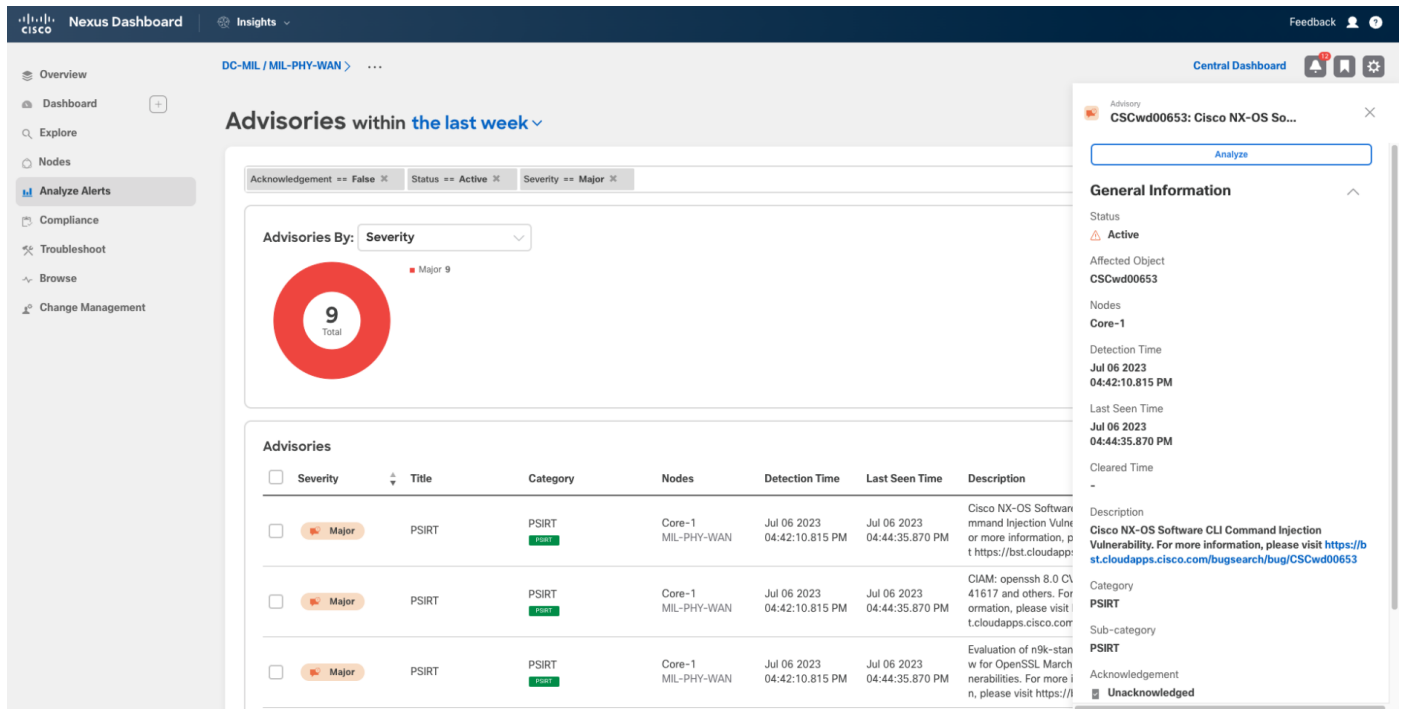


図 2. Cisco Nexus Dashboard Insights アドバイザリ

認証、認可、およびアカウントティングの使用

認証、認可、およびアカウントティング (AAA) は、システムおよびネットワーク内のリソースおよびサービスへのアクセスを制御するために使用されるよく知られたセキュリティフレームワークです。

認証は、リソースにアクセスしようとするユーザーまたはデバイスのアイデンティティを確認するプロセスを指します。これは通常、ユーザー名とパスワードを使用するか、多要素認証 (MFA) や生体認証などのより高度な方法を使用して行われます。

認可とは、ユーザーまたはデバイスが、ネットワーク内の特定のリソースにアクセスしたり、特定のアクションを実行したりするために必要な権限を持っているかどうかを判断するプロセスを指します。

アカウントティングは、アクセスするリソースや実行するアクションなど、ネットワーク内のユーザーとデバイスのアクティビティをログに記録するプロセスを指します。この情報は監査やその他の目的に使用できます。

これらの 3 つのコンポーネントが連携して包括的なセキュリティフレームワークを形成し、認可されたユーザーとデバイスだけがネットワークリソースにアクセスできるようにし、セキュリティと責任の目的でそれらのアクティビティを追跡できるようにします。

Cisco ACI は、ローカルユーザーとリモートユーザーの両方の AAA フレームワークをサポートします。

詳細については、[Cisco APIC セキュリティ構成ガイド](#)を参照してください。

最小権限の原則を適用する

最小権限の原則は、対象にジョブまたは機能を実行するために必要な最小レベルのアクセス権を付与する必要があることを示唆するセキュリティ概念です。つまり、対象には、特定のタスクを完了するために必要な権限と権限のみを付与する必要があり、それ以上は付与しないことを意味します。このコンテキストでは、対象は、ユーザー、自動化エンジン (Terraform や Ansible など)、プロセス、または別のシステムや製品のいずれかです。

最小権限の原則は、機密データやリソースの不正アクセスや偶発的な誤用のリスクを軽減するのに役立つため、重要です。必要なものだけにアクセスを制限することで、攻撃対象領域が縮小され、セキュリティ違反や脆弱性によって引き起こされる可能性のある損害が最小限に抑えられます。

Cisco ACI は、管理者がこの最小権限の原則を効果的に実装できるように、非常に強力なロールベース アクセス コントロール (RBAC) 機能セットを提供します。詳細については、『Cisco APIC 基本構成ガイド』の「[アクセス、認証、アカウンティング](#)」を参照してください。

ログ収集とモニタリングの一元化の使用

兆候削除技術 (IRT) は、セキュリティ インシデントまたは侵入の痕跡または兆候を削除して、さらなる検出や調査を防止するために使用されます。IRT には、ログ ファイルの削除または変更、システム設定または構成の変更、ネットワーク トラフィックの操作などのアクションを含めることができます。

セキュリティの観点から、ログはセキュリティ インシデントを検出および調査する際の証拠の重要なソースであるため、リモートで保存することを強くお勧めします。ログは、イベントの日時、ネットワーク トラフィックの送信元と宛先、システム上のユーザまたはプロセスによって実行されたアクションなどの貴重な情報を提供できます。

ログをリモートで保存することで、組織は、IRT や、ローカル システム上のログを変更または削除するその他の試みから保護されていることを確認できます。また、リモート ロギングを使用すると、ログを一元化された場所に安全に保存し、監視、分析、および関連付けをより簡単に行うことができます。

Cisco ACI は、イベントとログをリモート ロケーションにエクスポートするためのさまざまなメカニズムを提供します。これらのメカニズムには、以下が含まれます。

Syslog

Syslog は、ネットワーク デバイスおよびサーバーでシステム メッセージとイベントをロギングするために使用される標準プロトコルです。Cisco ACI は、UDP、TCL、または SSL を介した Syslog を使用したイベント、障害、および監査ログのエクスポートをサポートしています。

REST API サブスクリプション

Cisco APIC は、ユーザーがプログラムで Cisco ACI 管理対象オブジェクト (MO) に対して CRUD (作成、読み取り、更新、および削除) 操作を実行できるようにする強力な REST API インターフェイスを提供します。

API クエリが Cisco APIC で実行される場合、アクティブな API セッション中に発生するそのクエリの結果の将来の変更に対するサブスクリプションを作成するオプションがあります。ユーザまたはシステムにより開始されたアクションによって、MO が作成、変更、または削除されると、イベントが生成されます。これによりアクティブなサブスクライブ済みのクエリの結果が変わる場合、APIC はサブスクリプションを作成した API クライアントへのプッシュ通知を生成します。

このメカニズムを使用すると、APIC から定期的に情報をプルすることなく、イベントと変更について通知を受けることができます。詳細については、『Cisco APIC REST API 構成ガイド』を参照してください。

SNMP

Simple Network Management Protocol (SNMP) は、ルータ、スイッチ、サーバなどのデバイスのネットワーク管理とモニタリングに使用される標準プロトコルです。

SNMPは、ネットワーク管理者がルータ、スイッチ、サーバなど SNMP 対応デバイスからログおよびその他の管理情報を取得し、それらを集中ログ管理システムに送信して詳細な分析とモニタリングを行えるようにすることで、ログ収集に使用できます。SNMP 対応デバイスは、特定のイベントまたは条件が発生したときに、SNMP トラップと呼ばれる通知メッセージを集中型モニタリング システムに送信することもできます。

Cisco ACI は、SNMPv2c と SNMPv3 の両方をサポートします。SNMPv3 は認証と暗号化の両方を提供するため、セキュリティの観点から SNMPv3 を使用することを強く推奨します。Cisco ACI では、GET および TRAP 操作のみがサポートされています。

詳細については、『[Cisco APIC の障害、イベント、システム メッセージ管理ガイド](#)』を参照してください。

安全なプロトコルのみ使用

管理アクセスおよび運用の目的で使用されるプロトコルの多くは、適切に保護する必要がある機密性の高いネットワーク管理データを伝送します。したがって、これらの接続には可能な限りセキュアなプロトコルを使用する必要があります。表 1 に、セキュアなプロトコルとセキュアでないプロトコルの例を示します。

表 1 セキュアなプロトコルと非セキュアなプロトコル

セキュアなプロトコル	セキュアでないプロトコル
HTTPS	HTTP
SCP/SFTP	FTP
SNMPv3	SNMPv2
SSH	Telnet

これらの安全なプロトコル、および整合性、機密性、および信頼性を提供するその他の管理およびコントロールプレーンプロトコルは、暗号と暗号化アルゴリズムに依存します。これらのセキュリティ機能を提供するプロトコルを使用することに加えて、安全であると見なされ、既知の脆弱性がない暗号アルゴリズムと暗号を使用することも重要です。

したがって、より適切な代替手段がある限り、安全であると見なされなくなったアルゴリズムは避ける必要があります。これらの安全でないアルゴリズムと暗号の例は、MD5、SHA1、TLSv1.0/1.1 です。

Cisco ACI では、安全でないプロトコルがデフォルトで無効になっています。さらに、サポートされているか、デフォルトで有効になっている暗号アルゴリズムと暗号のリストは、新しいバージョンがリリースされるたびに確認されます。たとえば、TLSv1.0 と v1.1 は、Cisco APIC リリース 6.0 以降ではサポートされなくなり、TLSv1.2 がデフォルト オプションとして使用されます (TLSv1.3 もサポートされます)。詳細については、『[Cisco APIC セキュリティ構成ガイド](#)』の「[HTTPS アクセス](#)」のセクションを参照してください。

構成管理の実行

構成管理は、開発および運用ライフサイクル全体を通じて、システムまたはソフトウェアに加えられた変更を管理および制御するプロセスです。変更の提案、レビュー、承認、および展開の方法を決定します。

セキュリティと強化のコンテキスト内で、構成管理の最も関連する部分は、システムの復元が必要になった場合に備えて、構成のバックアップが定期的に収集され、安全にアーカイブされるようにすることです。エンジニアと管理者は、構成アーカイブを使用して、ネットワーク デバイスに加えられた変更をロールバックしたり、災害やインシデントの後にシステムを復元したりできます。

セキュリティに関しても、構成アーカイブを使用して、セキュリティの変更点やその時期を特定できます。この情報を監査ログ データと組み合わせて使用すると、ネットワーク デバイスのセキュリティ監査に役立ちます。

Cisco ACI 構成のバックアップ

Cisco ACI を使用すると、管理者はオンデマンドおよび定期的なスナップショットを実行できます。これらのスナップショットは、ローカルまたはリモートの場所に保存できます。

障害が発生した場合に構成変更の損失を最小限に抑えるのに十分な頻度で、定期的なリモート バックアップを実行することを推奨します。Cisco ACI 構成のバックアップはサイズが数 KB を超えることはめったにない JSON ファイルであることを考えると、ほとんどの組織では 1 日に複数のバックアップを実行することは一般的に許容されます。バックアップは、定期的に自動的に実行するようにスケジュールすることもできます。

Cisco ACI の構成には、パスワードやシークレットなど、多くの機密情報が含まれています。したがって、バックアップ構成は適切に保護され、安全なリモートの場所に保存され、構成ファイルの機密情報が漏洩しないようにする必要があります。

Cisco APIC には、ユーザー指定の AES パスフレーズを使用して、AES を使用して設定こちらバックアップファイルに含まれる機密プロパティ（[こちら](#)を参照）を暗号化するオプションがあります。セキュリティの観点からだけでなく、ビジネス継続性の観点からも、このオプションを使用することを強くお勧めします。

AES 暗号化が有効になっていない場合、Cisco APIC はファイルをエクスポートする前に構成ファイルからすべての機密情報を削除します。したがって、構成のバックアップには、パスワード、キー、トークン、またはその他の機密属性は含まれません。このようなシナリオでは、バックアップを復元すると、一部の機能が正しく動作しません。たとえば、パスワードが設定されていないためにローカル ユーザーがログインできない、認証が使用されている場合に BGP ネイバーが起動しない、またはクレデンシャルが構成されていないために VM マネージャへの接続が失敗するなどです。

したがって、ファブリックの起動直後に AES パスフレーズを設定し、APIC の外部の安全な場所にパスフレーズを保存することをお勧めします。このパスフレーズは、災害が発生した場合にファブリックを復元するために必要な構成バックアップの暗号化を解除するため、管理者が提供する必要があります。

強力なパスワードと多要素認証 (MFA) を使用する

強力なパスワードと多要素認証 (MFA) は、機密データやシステムへの不正アクセス、およびサイバー攻撃からネットワークとシステムを保護するための重要なセキュリティ対策です。大文字と小文字、数字、特殊文字の組み合わせを含む強力なパスワードを使用すると、悪意のある攻撃者が高度なツールを使用している場合でも、パスワードのブルートフォース攻撃が非常に困難になります。MFA は、パスワードに加えて、フィンガープリントやセキュリティトークンなどの追加の形式の時間制限付き認証を提供するようにユーザーに要求することで、セキュリティのレイヤを追加します。これにより、ハッカーがフィッシングやその他の手段でユーザーのパスワードを取得した場合でも、ネットワークやシステムにアクセスする可能性が大幅に低下します。

さらに強力なパスワードと MFA で、パスワードとその MFA トークンまたはデバイスの両方を使用する必要があるため、個人がシステムまたはネットワーク デバイスにアクセスしたことを否定することがより困難になるため、アカウントビリティが向上します。Cisco ACI を使用すると、管理者はローカル ユーザーに強力なパスワードの使用を強制し、ユーザーごとに多要素認証をアクティブにすることができます。

管理プレーンのセキュリティ保護

管理プレーンの保護は、ネットワーク インフラストラクチャを強化する際に管理者が注力する必要がある主な領域の 1 つです。悪意のある攻撃者がファブリックの管理プレーンを侵害した場合、最終的にはインフラストラクチャで何らかのレベルの管理権限を取得し、可用性、機密性、または整合性に影響を与える可能性があります。

このセクションでは、Cisco ACI の管理プレーンを強化するために使用可能な機能と、この領域の推奨事項に焦点を当てます。

認証、許可、アカウントिंग (AAA)

管理プレーンの強化に関しては、認可された対象 (ユーザー) のみがシステムにアクセスできるようにすることが重要なことの 1 つです。さらに、これらの対象がシステムにアクセスする場合、最小権限の原則に従って、

リソースにアクセスして必要な操作のみを実行できる必要があります。最後に、管理者がフォレンジック分析のためにこれを参照できるように、ユーザーが実行したアクションをログに記録する必要があります。

これらは AAA フレームワークの一部であり、認証、認可、およびアカウントिंगの 3 つの領域があります。

リモート認証プロバイダを使用したユーザー認証

Cisco ACI は、ローカル ユーザーとリモート認証プロバイダの両方を使用したユーザー認証をサポートしています。ベストプラクティスとして、ユーザー認証に一元化された ID プラットフォームを使用することを推奨します。Cisco ACI は、リモート認証プロバイダを使用して、その集中型 ID プラットフォームに対してユーザーを認証できます。

Cisco APIC リリース 6.0 では、次のリモート認証プロバイダーがサポートされています。

- RADIUS
- TACACS+
- LDAP
- RSA SecurID
- SAML (Cisco APIC リリース 3.0 以降)
 - ADFS、Okta SSO、または PingFederate のいずれかを使用する
- Duo (Cisco APIC リリース 5.0(1) 以降)
 - Duo Proxy RADIUS サーバまたは Duo Proxy LDAP サーバの使用
- OAuth2.0 (Cisco APIC リリース 5.2(3) 以降)
 - 承認コード付与タイプの使用

通常の操作では、リモート認証プロバイダが推奨される唯一の認証方式である必要があります。ただし管理者は、リモート認証プロバイダが使用不可または到達不能になった場合でも、システムへのアクセスが引き続き可能であることを確認する必要があります。

AAA フォールバック

リモート認証プロバイダが到達不能になったときに Cisco ACI へのアクセスを許可するには、AAA フォールバックを構成し、リモート認証プロバイダが到達不能になった場合のみフォールバックが使用可能になるように構成する必要があります。Cisco APIC リリース 6.0 は、RADIUS、TACACS+、RSA、LDAP、および Duo によるフォールバックをサポートしています。

注： OAuth2 や SAML などの AAA フォールバックがサポートされていないリモート認証プロバイダは、常に使用不可として報告されます。したがって、フォールバックは常に可能です。

フォールバックはデフォルトでローカル認証を使用します。これを変更しないことをお勧めします。

リモート認証プロバイダが使用可能かどうかの確認は、次の 2 つの方法で実行できます。

ICMP ping チェック	デフォルトでは、ICMP エコーを使用してリモート認証プロバイダの可用性を確認します。ICMP エコー メッセージに対する応答が受信されない場合、フォールバック メカニズムがアクティブになります。ただし、このモニタリング メカニズムには注意点があります。リモート認証プロバイダがネットワークの観点から到達可能であるが、認証サービスが使用できない場合、ICMP エコー プロブは成功します
----------------	---

	が、ログインはできません。
サーバ モニタリング	<p>前述の警告を克服するために、AAA サーバ モニタリング機能が Cisco APIC リリース 3.1(1) で導入されました。サーバ モニタリングでは、管理者が定義したユーザーを使用して、リモート認証プロバイダに対して定期的な認証チェックを実行します。認証が成功すると、リモート認証プロバイダは正常であると見なされます。</p> <p>このメカニズムは、ネットワークの到達可能性を検証するだけでなく、スタック全体の可用性も検証し、その結果より正確であるため、このメカニズムをお勧めします。</p> <p>APIC リリース 6.0 の時点では、リーフおよびスパイン スイッチはサーバ モニタリングをサポートしていません。この制限は、ファブリックで実行されているバージョンに応じて異なる結果をもたらします。</p> <ul style="list-style-type: none"> ● Cisco APIC リリース 5.2(3e) より前では、サーバ モニタリングを使用する場合、リモート認証プロバイダが常に使用可能と見なされるため、フォールバック メカニズムを使用したスイッチへのアクセスはできません。このシナリオでは、バックアップ メカニズムとしてスイッチへのコンソール アクセスを使用することを強く推奨します。 ● Cisco APIC リリース 5.2(3e) 以降では、スイッチのフォールバックをサポートするために、サーバ モニタリングとともに ICMP ping チェックを使用できます。したがって、APIC はサーバ モニタリングを使用しますが、スイッチは ICMP ping チェックに依存します。このシナリオでも、バックアップ メカニズムとしてスイッチへのコンソール アクセスを使用することを推奨します。 <p>注： 次のように、リーフおよびスパイン スイッチでのサーバ モニタリング サポートを含めるために、追跡されている拡張機能がいくつかあります。 CSCvx74300 および CSCvy25958 です。</p>

フォールバックを使用したファブリックへのアクセス

リモート認証プロバイダが使用できない場合、フォールバックは自動的に有効になりません。ユーザーはフォールバックの使用を手動で選択する必要があります。ただし、フォールバックは、[ログイン ドメイン (Login Domain)] ドロップダウン GUI ランディングページでは使用できないオプションです。

フォールバックを使用して **Cisco APIC** にログインするには、次の構文を使用する必要があります。

- GUI の使用 : `apic:fallback\`
- CLI または REST API の使用 : `apic#fallback\`

注： CLI または REST API を介してシステムにアクセスするときに、デフォルトとは異なるログイン ドメインを使用する場合は、同じ構文を使用する必要があります。たとえば、`apic#myldap\ です。`

ローカル ユーザーを使用するユーザー認証

Cisco ACI は、ローカル ユーザーでも **AAA** フレームワークをサポートします。ただし、ローカル認証は、フォールバック アクセスやコンソール アクセスなど、いくつかの限定された使用例に限定する必要があります。したがってローカル ユーザーを使用する場合は、次の注意事項に従うことを推奨します。

- これらの特定の使用例では、個人用ローカルアカウントの数を減らして設定します。アカウントティングとアカウントの取り消しがより困難になるため、汎用アカウントの使用は避けてください。
- フォールバックチェックを構成して、リモート認証プロバイダが使用できない場合にのみローカル アカウントが使用されるようにします。
- 次のセクションで説明されている推奨事項を使用して、これらのローカル アカウントを次のように適切に強化します。パスワード強度チェック、パスワードの有効期限、および二要素認証。

ローカル管理者アカウント

一部の組織の強化のベストプラクティスでは、管理者アカウントを削除する必要があります。ただし、Cisco APIC では管理者アカウントを削除できません。管理者またはルートアカウントを削除できないシステムが多数あるため、これは驚くことではありません。

Cisco APIC の admin アカウントは root アカウントと同等ではないことに注意してください。管理者アカウントには、Cisco ACI ファブリック構成を管理するための完全な権限がありますが、Cisco ACI デバイスが実行に使用する基盤となるソフトウェア コンポーネントとファイル システムにはアクセスできません。

root アカウントへのアクセスは非常に制限されていますが、完全な権限を持つ root アカウントが引き続き存在します。絶対に必要な場合にのみ、特定の状況で Cisco テクニカル サポートは、Cisco テクニカル サポートがトラブルシューティングをサポートできるように、ルート アクセス用のローカル固有の期限付きパスワードを生成できます。この 1 回限りのパスワードは、アクセスする必要がある APIC からのトークンを使用して、Cisco テクニカル サポートによってのみ生成できます。つまり、ユーザーはどのような状況でも root としてログインできません。

ベスト プラクティスでは、管理者アカウントを通常の操作に使用しないでください。他のユーザーが実行できない最後の手段のアクセスと特定の操作にのみ使用する必要があります（これらの状況は非常に限られています）。

管理者アカウントの使用を防ぐために、組織が使用できるさまざまな戦略がありますが、これらはこのドキュメントの範囲外です。これらの戦略は、管理者パスワードを知っているユーザーが 1 人もいないようにしながら、管理者パスワードが必要な場合に短時間で取得できるようにすることを目的としています。

管理者アカウントとほぼ同じレベルの権限を持つ他のローカル ユーザーまたはリモート ユーザーがいる可能性があります。その場合でも、個々のアカウントを持つことで、適切なアカウントティングを確実に実行でき、必要ときにいつでもアクセスを取り消すことができます。

パスワード強度

このドキュメントで前述したように、パスワードが強力であることを確認することが推奨されるベストプラクティスです。Cisco ACI を使用すると、管理者は設定されたユーザー パスワードに特定の条件を適用し、パスワードが強力で安全であることを確認できます。

Cisco ACI では、パスワード強度チェックはデフォルトで有効になっています。システムの最初の起動時に、このチェックを無効にできます。[パスワード強度チェック (Password Strength Check)] を有効にしておくことを推奨します。

有効にすると、Cisco ACI はローカル ユーザーのパスワードが次の基準を満たしていることを確認します。

- 8 ~ 80 文字にする必要があります。
- 次の少なくとも 3 種類を含む。
 - 小文字
 - 大文字
 - 数字
 - 特殊文字
- 連続して 3 回以上繰り返される文字を含めないようにしてください。
- パスワードのディクショナリ チェックに合格します（英語ディレクトリ）。
- ユーザー名と同一、またはユーザー名を逆にしたものにならないでください。

- 空白にすることはできません。

パスワードの長さが必要な文字タイプは、パスワード強度プロファイルを使用してカスタマイズできます。たとえば、組織が 12 文字以上の 4 種類の文字すべてを含むパスワードを必要とする場合、次の図に示すようにパスワード強度プロファイルをカスタマイズすることで、これを適用できます。

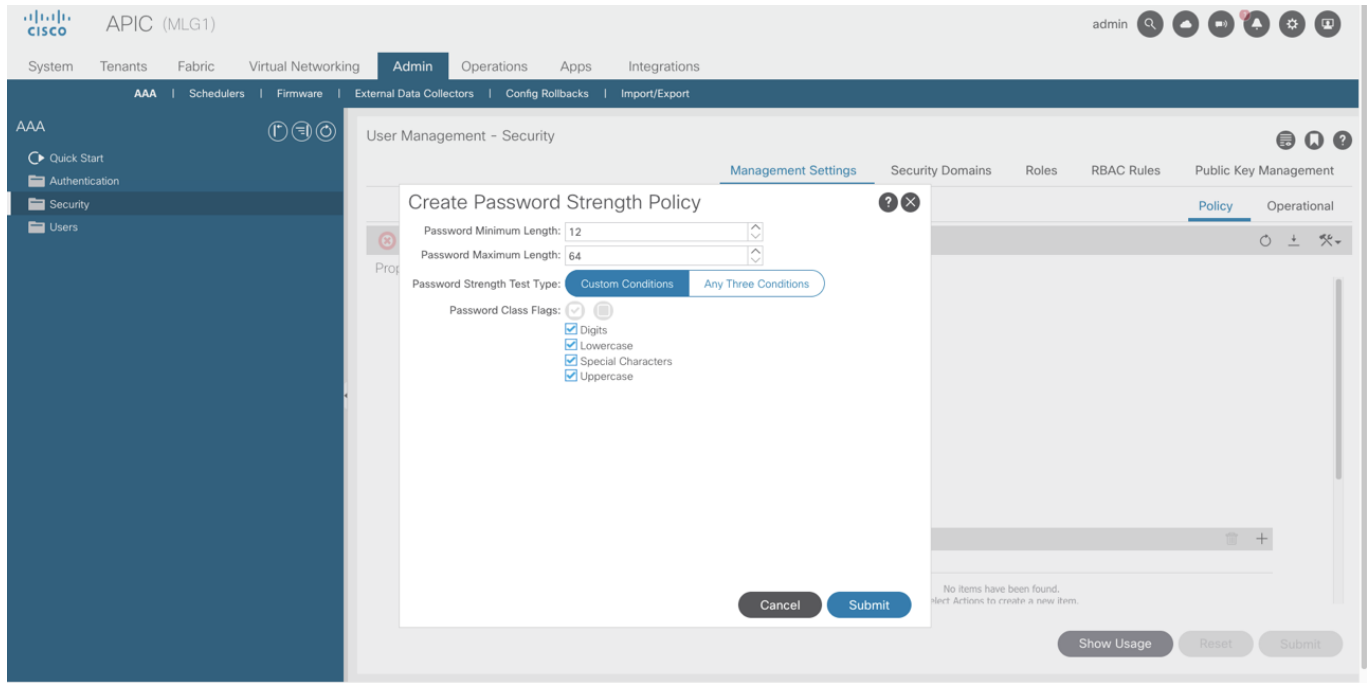


図 3. Cisco APIC 5.2 以前でのパスワード強度プロファイルのカスタマイズ

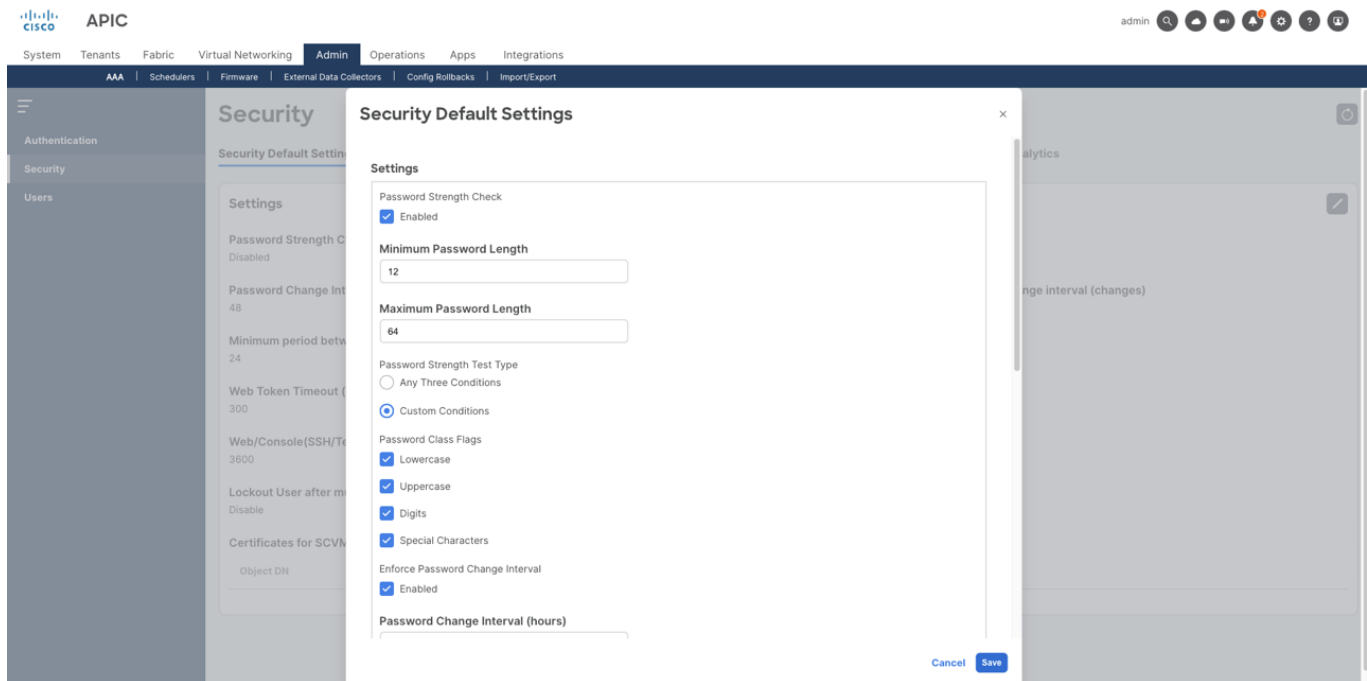


図 4. Cisco APIC 6.0 以降でのパスワード強度プロファイルのカスタマイズ

二要素認証機能 (2FA)

Cisco APIC リリース 3.0(1) では、ワンタイム パスワード (OTP) を使用した二要素認証のサポートが追加されました。二要素認証は、ユーザー単位で有効にできます。有効にすると、ユーザーが APIC に初めてログインしたときに、ユーザーの選択したデバイスを OTP キーの詳細で構成するように要求する画面が表示されます。

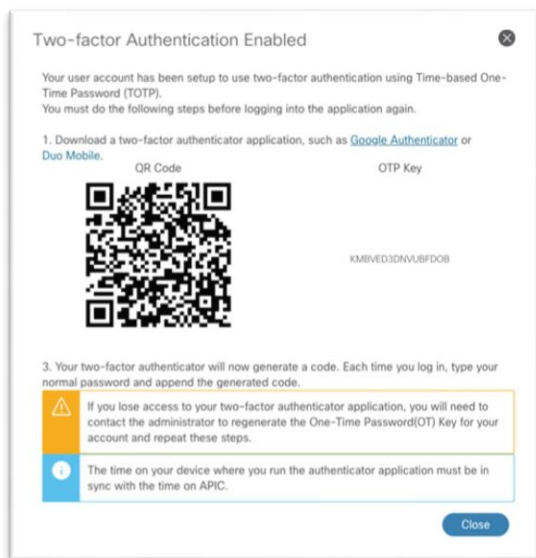


図 5. 2FA を有効にした後、ユーザーが初めてログインしたときに表示される画面

連続ログインの場合、ユーザーはパスワードに OTP コードを追加する必要があります。

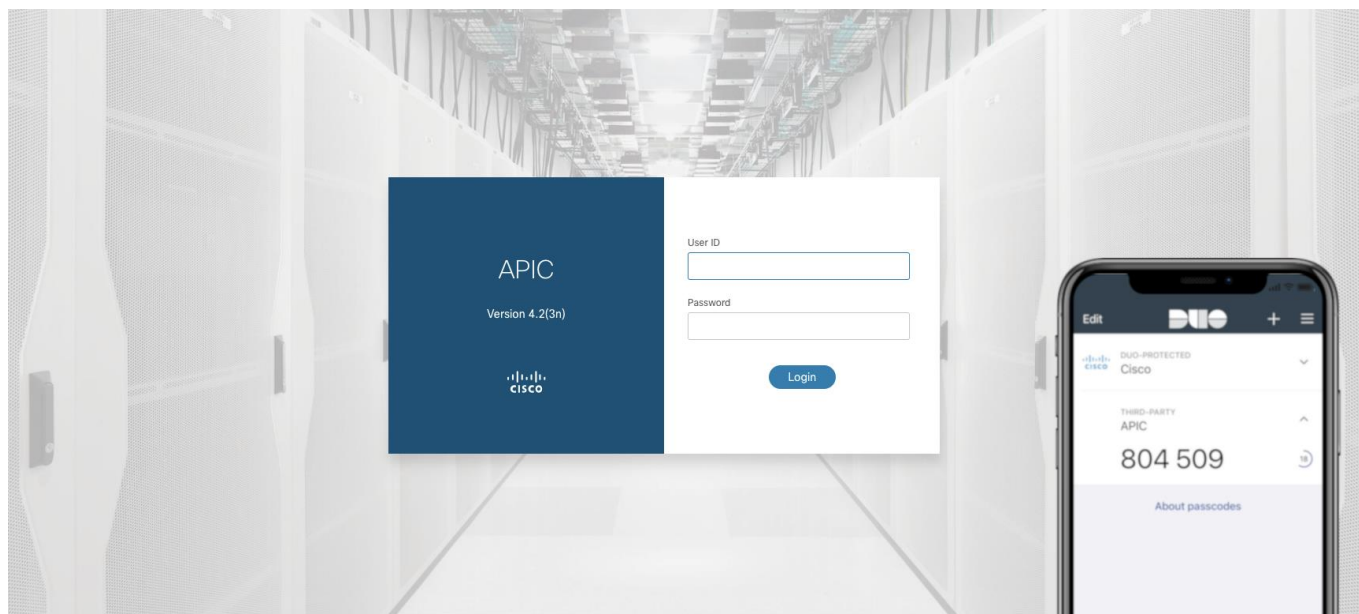


図 6. Duo Mobile で有効になっている二要素認証

ワンタイム パスワード (OTP) は 30 秒ごとに変更され、ユーザー デバイスが APIC と時刻同期されている必要があります。

すべてのローカル ユーザーに対して二要素認証を有効にすることをお勧めします。ただし、他の方法が失敗した場合に最後の手段のログイン情報で **Cisco ACI** ファブリックにアクセスできるように、管理者ユーザーに対して二要素認証を有効にしないことをお勧めします。

ユーザーのロックアウト

Cisco APIC リリース **4.2(4)** 以降、管理者は指定された回数のログイン試行の失敗後にユーザーがログインできないようにブロックできます。管理者は、特定の期間にユーザーをロックアウトするために必要なログイン試行の失敗回数と、ロックアウト期間を指定できます。

ユーザー ロックアウト機能は、ローカル ユーザーとリモート ユーザーの両方でサポートされます。リモート ユーザーの場合、次の注意事項があります。

- リモート ユーザーがロックアウトされると、リモート認証プロバイダに対してロックアウトされます。
- リモート認証プロバイダが到達不能またはダウンしていることによるログインの失敗は考慮されません。
- 不正な **SSH** キーまたは無効な証明書によるログインの失敗は考慮されません。

ユーザーがロックアウト状態の場合、コントローラやスイッチを含むファブリックの一部であるすべてのノードでロックアウトが適用されます。ユーザー ロックアウト機能を有効にすることをお勧めします。

ユーザー認可

ユーザー認証を使用すると、管理者は各ユーザーに、ジョブに必要なアクションを実行するために必要な権限のレベルを付与できます。これにより、最小権限の原則が実装されます。

Cisco ACI は、次の 3 つの主要な要素に基づいてロールベース アクセス コントロール (**RBAC**) モデルを使用します。

- セキュリティ ドメイン
- ロール
- 権限

Cisco ACI オブジェクトモデルの各オブジェクト クラスには、その特定のクラスからオブジェクトを読み書きする権限を有効にする権限のリストがあります。これらの権限は、オブジェクト モデル構成にリストされません。次の図に、クラス **fvBD** (ブリッジ ドメイン) の例を示します。

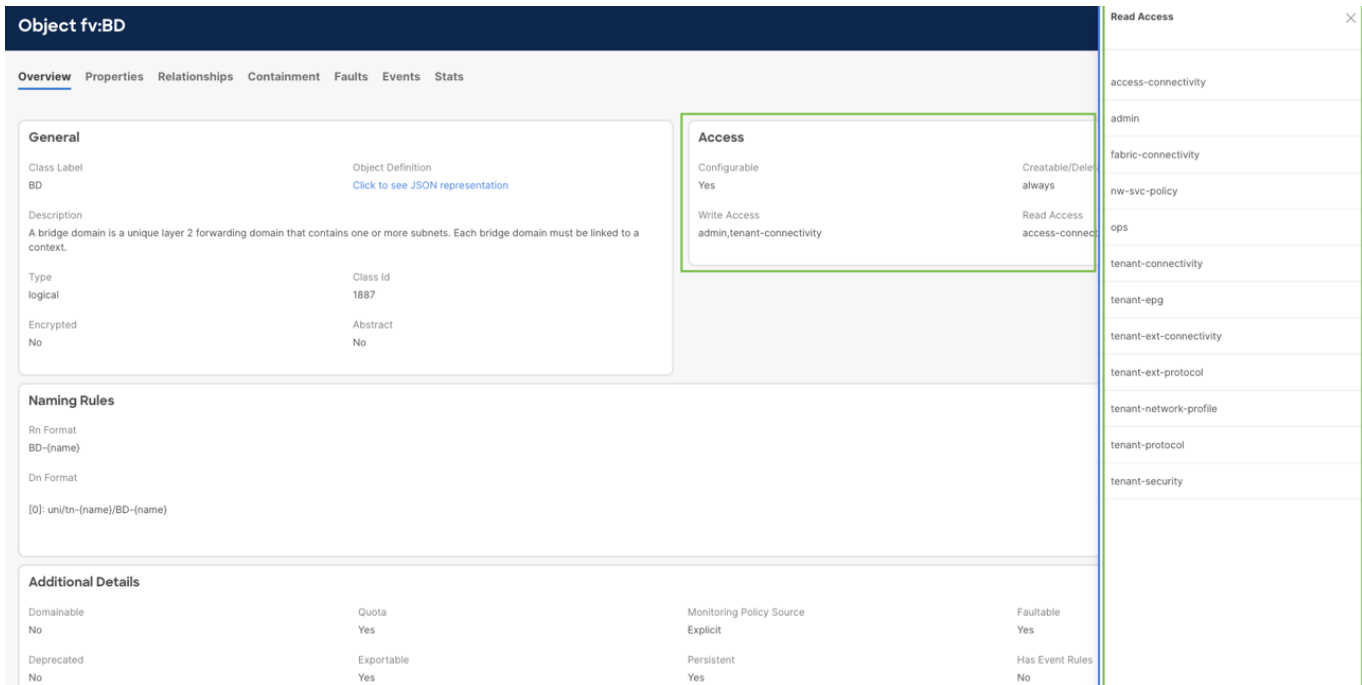


図 7. モデルのドキュメントに記載されているアクセス権限

1 つ以上の権限を 1 つのロールにグループ化し、そのロールをユーザーに関連付けて、そのユーザーが特定のクラス セットを管理できるようにすることができます。マルチテナント機能とよりきめ細かい RBAC 制御を提供するために、Cisco ACI はセキュリティドメインの概念を導入しました。セキュリティドメインは、テナントやスイッチのセットなど、管理情報ツリー (MIT) のセクションを表します。

特定のオブジェクト セットへのユーザー アクセス権を提供するには、ユーザーが 1 つ以上のセキュリティドメインに関連付けられている必要があります。ユーザーが関連付けられているセキュリティドメインごとに、管理者はそのセキュリティドメイン内のユーザーのロールを定義できます。

たとえば、ユーザーはセキュリティドメイン **Tenant-A** のロール **tenant-admin** を持ち、同時にテナント **common** を含むセキュリティドメイン **common** のロール **read-all** を持つことができます。

セキュリティドメイン、ロール、および権限のこれらの概念を組み合わせることで、管理者はきめ細かい権限を構成し、最小権限の原則を効果的に実装できます。

Cisco ACI は、すぐに使用できる一連の権限とロールを提供します。ただし、管理者は、既存の権限とカスタムロールがニーズに合わない場合に備えて、カスタム権限とカスタムロールを定義することもできます。詳細については、[Cisco APIC セキュリティ構成ガイド](#)を参照してください。

リモート認証プロバイダを使用したユーザー認証

リモート認証を使用する場合、管理者は 2 つの方法で各ユーザーに必要な権限を構成できます。

Cisco AV ペアの使用

管理者は、Cisco AV ペアを使用して、ユーザーに構成された RBAC ロールと権限を Cisco APIC に指定できます。Cisco AV ペアの使用は、LDAP、SAML、および OAuth2.0 ではオプションですが、RSA SecurID、RADIUS、および TACACS+ で使用できる唯一のオプションです。

外部認証サーバで Cisco AV ペアを設定するには、管理者が既存のユーザーレコードに Cisco AV ペアを追加します。Cisco AV ペアの形式は、使用されているプロバイダに関係なく同じです。

```
shell:domains =
domainA/writeRole1|writeRole2|writeRole3/readRole1|readRole2,
domainB/writeRole1|writeRole2|writeRole3/readRole1|readRole2(16003)
```

上記のように、お客様が権限を持つドメインごとに、AV ペアは書き込みロールと読み取り専用ロールを指定します。

属性/値 (AV) ペア文字列のカッコ内の数字は、APIC バッシュ シェルのユーザーの UNIX ユーザー ID として使用されます。Linux シェル用の APIC 上のユーザー ID は、ローカル ユーザー向けの APIC 内で生成されます。リモート ユーザーの場合、Linux シェルのユーザー ID を Cisco AV ペアで指定できます (上記の例では 16003)。有効な範囲は 16000 ~ 23999 です (含まれていません)。この範囲外のユーザー ID を関連付けようとすると、ユーザー認証時にエラーが発生します。

UNIX ユーザー ID が Cisco AV ペアで指定されていない場合、APIC は一意の UNIX ユーザー ID を内部的に割り当てます。ユーザー ID を指定する必要があるかどうかに関するベスト プラクティスはありません。手動で指定する場合は、ユーザー ID がユーザーに一意に割り当てられ、重複しないようにします。

Linux ユーザー ID がバッシュ セッション中に使用され、標準の Linux 権限が適用されます。また、ユーザーが作成するすべての管理対象オブジェクトは、そのユーザーの Linux ユーザー ID によって作成されたとマークされます。

前の例を続けると、ユーザーがセキュリティ ドメイン Tenant-A のロール tenant-admin を持ち、同時にセキュリティ ドメイン common のロール read-all を持っている場合、そのユーザーに対応する Cisco AV ペアは次のようになります。

```
shell:domains = Tenant-A/tenant-admin/,common//read-all
```

グループ マッピングの使用

Cisco AV ペアに加えて、LDAP、SAML、および OAuth2.0 プロバイダは、ユーザー権限を割り当てるためのグループ マッピングもサポートしています。グループ マッピングを使用すると、LDAP *memberOf* などの特定の属性で、エンコードされたリモート認証プロバイダから受信した、ユーザーが属するグループに基づいてユーザー権限が割り当てられます。SAML および OAuth2.0 で使用される属性をカスタマイズできます。LDAP の場合、使用される属性は *memberOf* です。

管理者は、リモート認証プロバイダから受信できるすべてのグループに対して、ユーザー グループ マップルールを使用して、対応するユーザー権限を付与するように構成できます。

次の図は、Okta 認証プロバイダを使用した SAML ログインドメインでのグループ マッピングの構成を示しています。

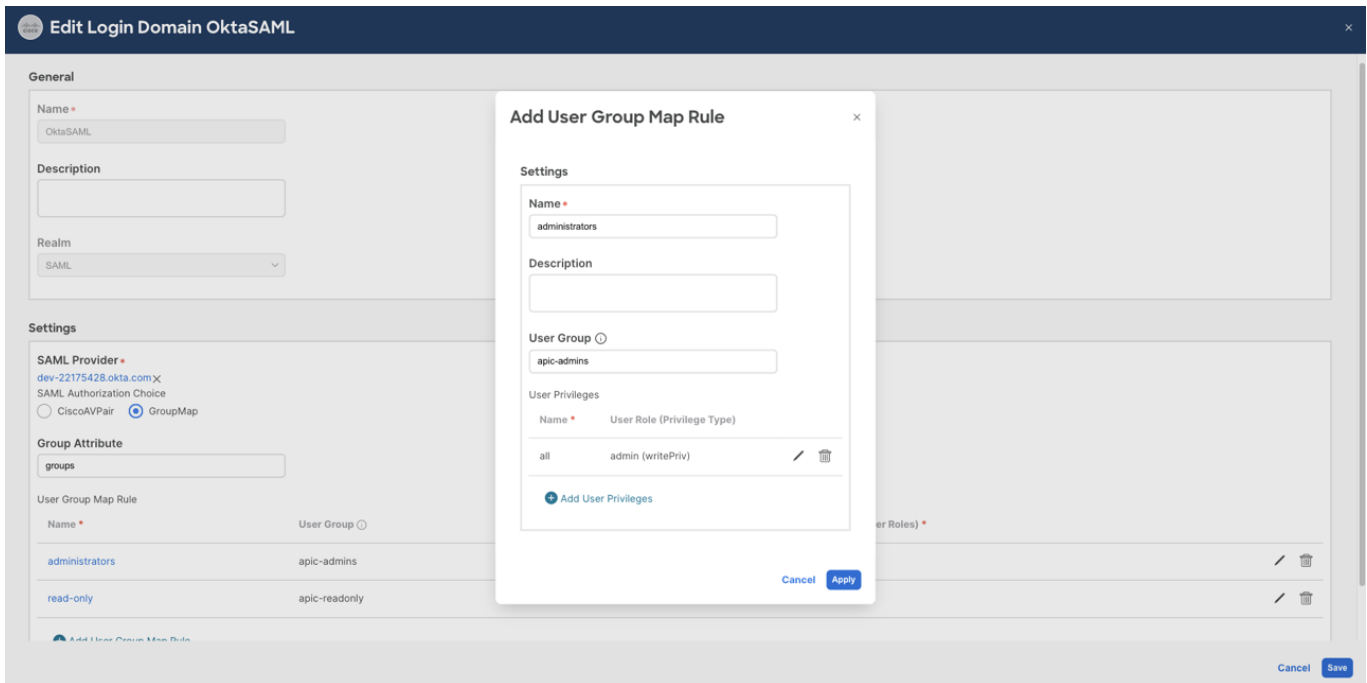


図 8. SAML プロバイダ グループ マップの構成

使用されているリモート認証プロバイダに応じて、一方または両方のメカニズムを使用できます。次の表に、Cisco APIC リリース 6.0 の時点でサポートされている組み合わせの概要を示します。

表 2 リモート認証プロバイダからユーザー権限を受け取るためにサポートされるメカニズム

プロバイダー	Cisco AVペア	グループ マッピング (Group Mapping)
RADIUS	サポート対象	非対応
TACACS+	サポート対象	非対応
LDAP	サポート対象	サポート対象
SAML	サポート対象	サポート対象
RSA SecurID	サポート対象	非対応
OAuth 2.0	サポート対象	サポート対象

アカウントिंगおよび監査ログ

Cisco ACI は、Cisco APIC で構成可能なオブジェクトに対して行われたすべての変更を記録します。これには、変更がいつ行われたか、どのようなアクションが実行されたか（作成、更新、または削除）、アクションを実行したユーザー、およびセッションが確立されたソース IP アドレスに関する情報が含まれます。この情報は APIC に保存され、複数のメカニズムを使用して監査目的でアクセスおよびエクスポートできます。

Cisco APIC GUI を使用した監査ログの参照

Cisco APIC グラフィカル ユーザー インターフェイスから監査ログを参照するには、**[履歴 (History)] > [監査ログ (Audit Logs)]** タブに移動します。このタブは、GUI のほぼすべてのセクションで使用できます。テナ

ントなどの特定のセクションの下の監査ログに移動すると、その特定のオブジェクトとその下のすべての子の監査ログが表示されます。

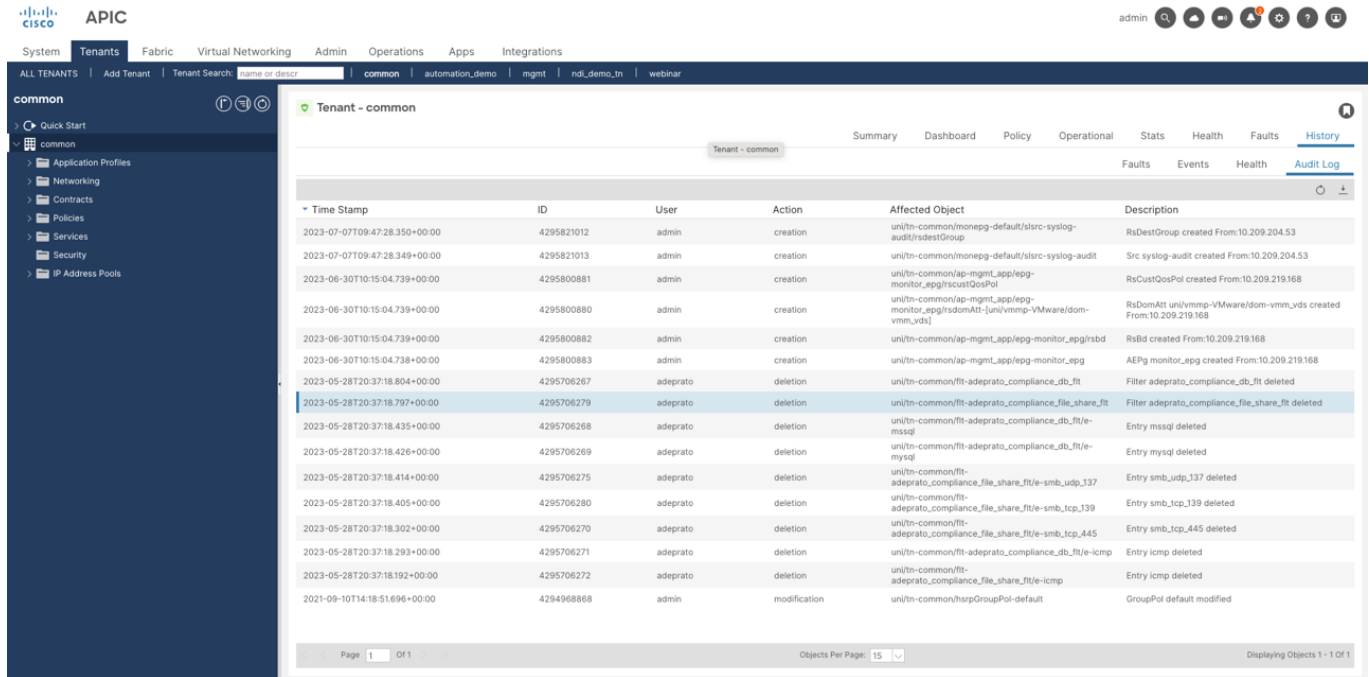


図 9. 特定のテナントの下に表示される監査ログ

ファブリック全体のすべての監査ログとセッションログのグローバルビューは、[システム (System)] > [履歴 (History)] で確認できます。

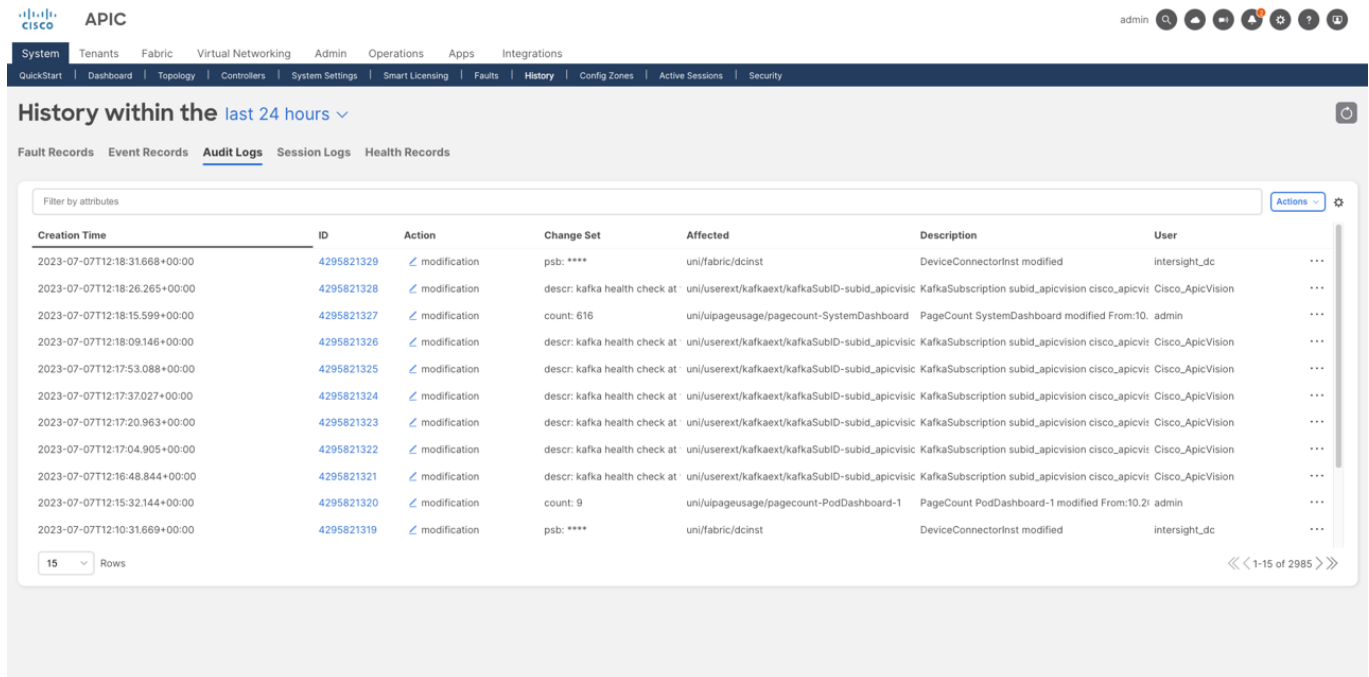


図 10. Cisco ACI ファブリック全体の監査ログ

Cisco APIC CLI を使用した監査ログの参照

コマンド「show audits」を使用して、Cisco APIC コマンドライン インターフェイス (CLI) から監査ログを参照することもできます。このコマンドを使用すると、管理者は、ユーザー、時間、アクションなどの複数のパラメータに基づいて監査ログをフィルタリングできます。

```
apic1-mdrl# show audits ?
<CR>
action Object action indicator
detail Detailed audit-log information
end-time Logs created in time interval
id Log ID
last-days Logs created in time interval
last-hours Logs created in time interval
last-minutes Logs created in time interval
start-time Logs created in time interval
tenant Show Tenants Information
user Name of user
```

以前のコマンドの出力例：

```
apic1-mdrl# show audits user admin last-minutes 30
Creation Time : 2023-07-07T09:47:40.568+00:00
ID : 4295821016
User : admin
Action : deletion
Affected Object : uni/tn-test-audit/rsTenantMonPol
Description : RsTenantMonPol deleted From:10.209.204.53
```

```
Creation Time : 2023-07-07T09:47:40.568+00:00
ID : 4295821017
User : admin
Action : deletion
Affected Object : uni/tn-test-audit/eptags
Description : EpTags deleted From:10.209.204.53
```

```
Creation Time : 2023-07-07T09:47:40.568+00:00
ID : 4295821015
User : admin
Action : deletion
Affected Object : uni/tn-test-audit/svcCont
Description : SvcCont deleted From:10.209.204.53
```

```
Creation Time : 2023-07-07T09:47:40.567+00:00
```

```
ID : 4295821018
User : admin
Action : deletion
Affected Object : uni/tn-test-audit
Description : Tenant test-audit deleted From:10.209.204.53
--More--
```

Cisco APIC REST API を使用した監査ログの参照

Cisco ACI は、障害およびイベントと同じメカニズムで処理される 2 つの管理対象オブジェクト

(*aaaSessionLR* および *aaaModLR*) を使用してアカウントिंगを処理します。*aaaSessionLR* 管理対象オブジェクトは、Cisco APIC およびスイッチのユーザー アカウント ログイン、ログアウトセッション、およびトークンの更新を追跡します。*aaaModLR* 管理対象オブジェクトは、ユーザーがオブジェクトに対して行う変更、およびいつ変更が発生したかを追跡します。*aaaSessionLR* と *aaaModLR* の両方のイベント ログが、Cisco APIC データベースに保存されます。データがプリセットされているストレージ割り当てサイズを超えると、FIFO メカニズムを使用してレコードが上書きされます。

監査ログはクラスタ全体に複製されません。APIC が失われた場合、またはそのハード ドライブが損傷した場合、一部の監査ログが永久に失われる可能性があります。これが、監査ログを外部の場所にエクスポートすることを推奨する理由の 1 つです (ただし、唯一でも最も重要でもありません)。

aaaModLR および *aaaSessionLR* 管理対象オブジェクトは、REST API を使用してクラス (最も一般的) または識別名 (DN) で照会できます。管理者は REST API フィルタを使用して、レポート、監査、またはトラブルシューティングの目的で監査ログのサブセットを取得できます。

Callhome/Syslog/TACACS を使用した監査ログのエクスポート

Cisco ACI には、さまざまなプロトコルとメカニズムを使用してモニタリング情報をストリーミングするオプションがあります。特に監査ログとセッション ログについては、Cisco ACI は次のメカニズムをサポートしています。

- Callhome (および Smart Callhome)
- Syslog (UDP、TCP、または SSL 経由)
- TACACS+

注: TACACS+ 外部ロギングのサポートは、Cisco ACI リリース 6.0(2) で導入されました。詳細については、[こちら](#)を参照してください。

これらのメカニズムを使用した監査ログとセッション ログのエクスポートの構成は、Cisco ACI の標準モニタリング構成に従います。つまり、モニタリング ポリシーを使用します。

モニタリング ポリシーは、ACI ファブリックのさまざまなコンポーネントのモニタリング方法をカスタマイズするために使用されます。これには、特定のオブジェクトの障害ライフサイクル、各ファシリティの **syslog** メッセージをトリガーする重大度、生成される **syslog** および **SNMP** トラップのリモート宛先が含まれますが、これらに限定されません。

モニタリング ポリシーは、複数のオブジェクトにアタッチできますが、すべてのオブジェクトにアタッチすることはできません。モニタリング ポリシーをオブジェクトで明示的に構成できるが、構成されていない場合は、親のモニタリング ポリシーが継承されます。一方、関連付けられたモニタリング ポリシーを持つ可能性がないオブジェクトは、常に親からそのポリシーを継承します。

管理者は、特定のポリシーを作成して特定のオブジェクト（テナントなど）に適用するか、デフォルトで APIC で使用可能なデフォルト ポリシーをカスタマイズできます。どちらの方法が優先されるかに関係なく、モニタリング ポリシーには 3 つの異なる範囲があることに注意することが重要です。

- アクセス範囲
 - たとえば、アクセス ポリシー、アクセス ポート、または VM コントローラに適用されます。
 - **[ファブリック (Fabric)]**、**[アクセス ポリシー (Access Policies)]**、**[ポリシー (Policies)]**、**[モニタリング (Monitoring)]** の下にあります。
- ファブリック範囲
 - ファブリック ポリシー、ファブリック ポート、カード、シャーシ、ファン、およびその他のインフラストラクチャ要素に適用されます。
 - **[ファブリック (Fabric)]**、**[ファブリック ポリシー (Fabric Policies)]**、**[ポリシー (Policies)]**、**[モニタリング (Monitoring)]** の下にあります。
- テナントの範囲
 - テナント ポリシーとテナントに関連付けられた要素に適用されます
 - **[テナント (Tenants)]**、**[テナント XYZ (Tenant XYZ)]**、**[ポリシー (Policies)]**、**[モニタリング (Monitoring)]** にあります。

モニタリング ポリシーは、モニタリングするオブジェクトに応じて、適切な範囲で作成する必要があります。

同様に、これらの各範囲で使用可能なさまざまなデフォルトのモニタリング ポリシーがあります。これらのポリシーのいずれかで監査ログのエクスポートを構成すると、指定された範囲内のオブジェクトにのみ適用されません。

- ファブリック共通ポリシー
 - アクセスおよびファブリックスコープのすべてのオブジェクトにデフォルトで適用されます
 - **[ファブリック (Fabric)]**、**[ファブリック ポリシー (Fabric Policies)]**、**[ポリシー (Policies)]**、**[モニタリング (Monitoring)]** の下にあります。
- ファブリック デフォルト ポリシー
 - ファブリック範囲内のすべてのオブジェクトにデフォルトで適用されます
 - **[ファブリック (Fabric)]**、**[ファブリック ポリシー (Fabric Policies)]**、**[ポリシー (Policies)]**、**[モニタリング (Monitoring)]** の下にあります
- アクセス デフォルト ポリシー
 - アクセス範囲内のすべてのオブジェクトにデフォルトで適用されます
 - **[ファブリック (Fabric)]**、**[アクセスポリシー (Access Policies)]**、**[ポリシー (Policies)]**、**[モニタリング (Monitoring)]** の下にあります
- テナントのデフォルト ポリシー
 - デフォルトでは、任意の テナント範囲のすべてのオブジェクトに適用されます
 - **[テナント (Tenants)]**、**[テナント共通 (Tenant Common)]**、**[ポリシー (Policies)]**、**[モニタリング (Monitoring)]** の下にあります。

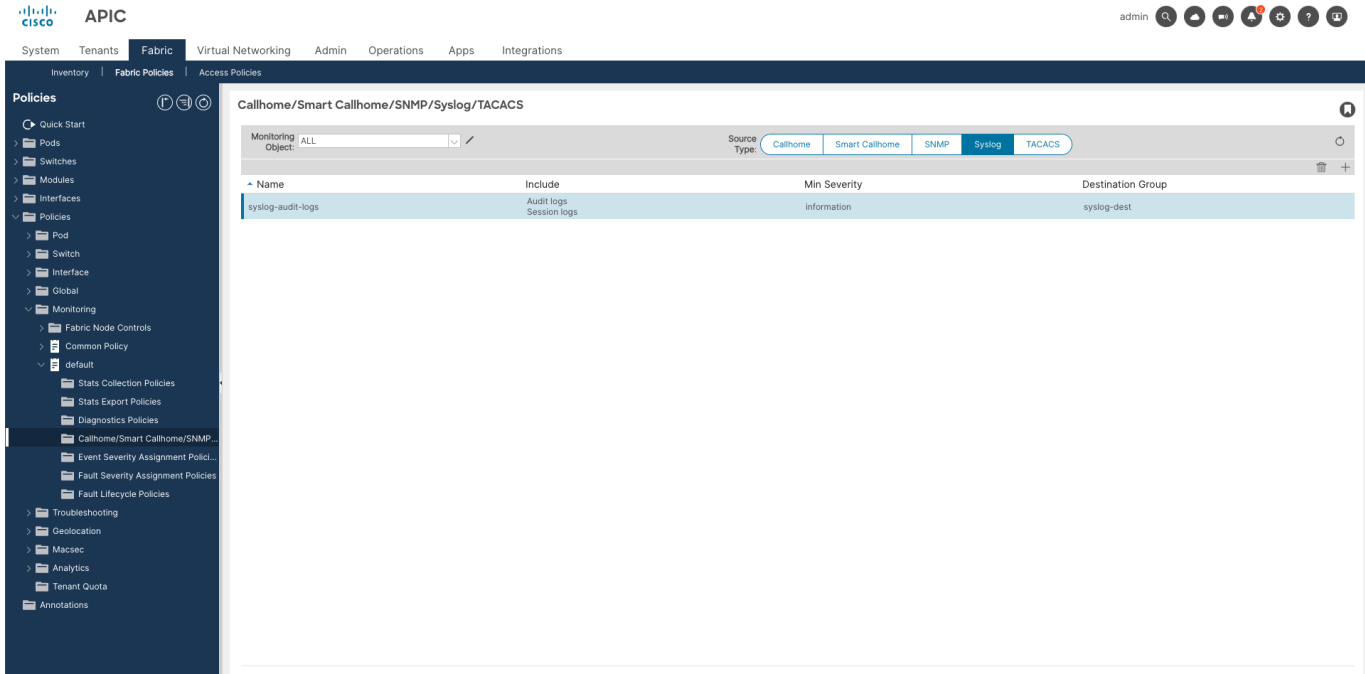


図 11. Syslog エクスポートのデフォルトのファブリック モニタリング ポリシー構成

注： Cisco ACI は、デフォルトでは、これらのメカニズムを介して監査ログまたはセッション ログをエクスポートしません。したがって、管理者は監査ログとセッション ログのエクスポートを開始するために、少なくともこれらのデフォルトのモニタリング ポリシーを変更する必要があります。

コンソールアクセス

コンソール ポートは、ローカルおよびリモート操作のためにデバイスへの最後の手段としてのアクセスを提供します。何らかの問題でデバイスの起動や管理アクセスの有効化ができない場合、デバイスに接続してトラブルシューティングを実行する唯一の代替手段はコンソールポートです。コンソールはラストリゾート アクセスであるため、デフォルトでローカル認証を使用するようにこのインターフェイスを構成することを推奨します。これにより、リモート認証サーバに到達できない場合でも、コンソールを使用したログインが常に可能になります。

コンソール アクセスに使用するローカル アカウントは、強力なパスワードと二要素認証を使用して適切に強化する必要があります。さらに、コンソール サーバを使用してコンソール インターフェイスへのリモート アクセスを提供する場合は、ベンダーのベスト プラクティスに従って、それらのコンソール サーバも強化する必要があります。

簡易ネットワーク管理プロトコル (SNMP) のセキュア化

Simple Network Management Protocol (SNMP) は、ネットワーク デバイスをモニタするために世界中の組織で広く使用されています。REST API、gRPC NMI、およびその他の方法を使用したモニタリングに傾向が移行しているにもかかわらず、まだ広く使用されています。したがって、Cisco ACI は、ポーリング (GET) と通知 (TRAP) の両方で SNMPv2c と SNMPv3 の両方をサポートします。Cisco ACI では、SET 操作を使用した SNMP を使用した変更のプッシュはサポートされていないことに注意してください。これにより、SNMP を有効にすると攻撃対象領域が大幅に減少します。デフォルトでは、SNMPv2c と SNMPv3 の両方が無効になっています。使用する前に明示的に構成する必要があります。

使用するバージョンに関して、SNMPv2c には、プロトコルの望ましくない重要なセキュリティ制限があります。たとえば、コミュニティはクリア テキストで送信されるため、傍受されて公開される可能性があります。

SNMPv3 は認証と暗号化の両方をサポートしているため、非常に安全な代替手段です。このため、可能な限り SNMPv3 を使用することを強く推奨します。

SNMPv2c は、互換性の制限を克服する場合にのみ使用してください。外部の制限のために SNMPv2c を使用する必要がある場合は、露出を制限し、攻撃対象領域を可能な限り減らすために従うべき推奨事項がいくつかあります。

- 強力なコミュニティ文字列を使用し、強力なパスワードの推奨事項に従う
- コミュニティ文字列を定期的にローテーションする
- SNMP クライアント グループ ポリシーを使用して、SNMP アクセスを特定の IP アドレス セットに制限する
- 管理コントラクトを使用して、SNMP プロトコルを使用して Cisco ACI 管理インターフェイスにアクセスできるユーザーを制限する

使用していないサービスおよびプロトコルの無効化

未使用の安全でないプロトコルを無効にすることは、IT インフラストラクチャを強化するための一般的なベストプラクティスです。従来、初期設定を容易にするために、一部のネットワーキング プラットフォームでは有効になっていることが多い一連のプロトコルがありますが、これらは安全でないだけでなく、通常は使用されません。したがって、管理者は、これらのデバイスを強化するための最初のアクションの 1 つとして、これらのプロトコルを無効にします。

Cisco ACI では、これは過去のもので、デフォルトでは、Cisco ACI は 2 つのポートのみを公開します。

- APIC とスイッチの両方での GUI アクセスおよび REST API アクセス用の HTTPS (TCP 443)
- APIC とスイッチの両方での CLI アクセス用の SSH (TCP 22)

他のポートには外部からアクセスできません。

デフォルト (外部) で使用されるプロトコルに関しても、リストは小さくなります。ファブリック内で排他的に使用されるプロトコルを除き、Cisco ACI がデフォルトで使用するプロトコルは次のとおりです。

- LLDP (Link Layer Discovery Protocol) は、ゼロタッチ ファブリック プロビジョニングをサポートするために使用されるため、デフォルトで有効になっています。

LLDP はループ防止にも使用されるため、信頼できるインターフェイスでは LLDP を有効にしておくことを推奨します。また、VMM 統合などの他の機能にも使用できます。信頼できないネットワークへのインターフェイスでは、LLDP を無効にすることをお勧めします。

Cisco ACI は、デフォルトでは不要なサービスを実行せず、デフォルトでアクティブなリモート管理サービスまたはプロトコルを制限するように設計されています。したがって、管理者の観点から、それらを無効にするために必要なアクションはありません。SNMP などの他のプロトコルが必要な場合は、管理者が明示的に構成する必要があります。

安全でないプロトコルと暗号の無効化

前述のように、安全な操作の原則の 1 つは、安全でないプロトコルを無効にして、代わりに安全な代替プロトコル (存在する場合) を使用することです。Cisco ACI の観点から、この推奨事項は次のことを意味します。

- HTTPS のみを使用し、HTTP は無効のままにします。

Cisco ACI では、HTTP がデフォルトで無効になっています。管理者は HTTP を有効にできますが、これを有効にすることは推奨されません。

- SSH のみを使用し、Telnet は無効のままにします。

Cisco ACI では、デフォルトで Telnet が無効になっています。APIC リリース 6.0(2) 以降、Telnet はサポートされなくなりました。以前のリリースでは、管理者は Telnet を有効にできましたが、これを有効にすることは推奨されません。

- ファイル転送およびエクスポートには、SCP、SFTP、または HTTPS を使用します。

ソフトウェア イメージのダウンロード、構成のバックアップ、テクニカル サポートのエクスポートなどを含むファイル転送に、FTP などの安全でないプロトコルを使用しないでください。代わりに、常に安全な代替手段を使用してください。

さらに、管理者は使用されているプロトコルだけでなく、使用されている暗号スイートにも注意を払う必要があります。次の内容が含まれています。

- TLS1.0 や TLS1.1 などの廃止または非推奨の TLS バージョンを無効にし、リリースで使用可能な最も強力な TLS バージョンのみを使用します。
- 組織が安全でないと見なした暗号または暗号化アルゴリズムを無効にします。たとえば、CBC 暗号は一般に安全であると考えられていますが、パディング オラクルおよびビースト攻撃に対して脆弱であることが知られているため、一部の組織では暗号を無効にして GCM 暗号のみを使用する場合があります。Cisco ACI では、管理者は、[ファブリック (Fabric)]、[ファブリック ポリシー (Fabric Policies)]、[ポッドポリシー (Pod Policies)]、[管理アクセス (Management Access)] で、使用する暗号とアルゴリズムを構成できます。

デフォルトでアクティブなプロトコル、暗号、およびアルゴリズムは、使用中の APIC リリースによって異なる場合があります。すべてのリリースで、Cisco は現在の最新技術に基づいて、この領域に必要な変更があるかどうかを確認します。たとえば、APIC リリース 6.0 では、TLS1.1 の互換性が削除され、TLS1.3 のサポートが導入されました。

コントラクトを使用した管理アクセスの制限

コントラクトは、データ プレーンでセグメンテーションを実装するための Cisco ACI のよく知られた機能です。ただし、コントラクトは、APIC とスイッチの両方の Cisco ACI デバイスへの管理アクセスを保護するためにも使用できます（使用する必要があります）。

Cisco ACI コントラクトは、アウトオブバンドとインバンドの両方を含む、Cisco ACI の管理インターフェイスに到達できるトラフィック フローを制限するために、専用管理テナントで構成できます。アウトオブバンド管理ポートは、ノード自体の背面にある専用の物理インターフェイスです。インバンド管理インターフェイスは、ACI ノードを相互接続するファブリック リンクと、APIC クラスタ メンバーに接続する前面パネルインターフェイスを使用します。コントラクトを使用してコンソール ポートを保護することはできません。

管理者はきめ細かい管理契約を使用して、使用するポートだけでなく、それらのポートのファブリックに到達できる送信元も制限することを強く推奨します。

コントラクトは、通常のテナントとまったく同じ方法で構成されますが、適用される場所と内部での実装方法がいくつか異なります。このセクションでは、これらのコントラクトを構成および適用する方法に関する推奨事項について説明します。

管理コントラクトの適用方法

管理コントラクトの準備ができたなら、コンシューマとプロバイダを設定して、コントラクトをファブリックに適用する必要があります。

アウトオブバンド管理コントラクトは、アウトオブバンド EPG と呼ばれるノード管理 EPG によって提供されます。この EPG は、APIC とスイッチを含むすべてのファブリックノードのアウトオブバンド管理インターフェイスを表します。

アウトオブバンド管理コントラクトは、[外部管理ネットワーク インスタンス プロファイル (External Management Network Instance Profiles)] と呼ばれるオブジェクトによって使用されます。

注： アウトオブバンド契約は、一方向にのみ適用できます。これは、着信トラフィックのみを制限できることを意味します。

インバンド管理コントラクトは、インバンド EPG と呼ばれるノード管理 EPG によって提供または使用できます。この EPG は、APIC とスイッチを含むすべてのファブリックノードのインバンド管理インターフェイスを表します。

インバンド管理コントラクトは、構成に応じて、管理テナント内の EPG または外部 EPG によって使用または提供されます。最も一般的な設定は、*inb VRF* インスタンスを使用して、*mgmt* テナントで *L3Out* を構成することです。この *L3Out* は、組織の管理ネットワークとの間の外部接続を提供します。この場合、インバンド管理コントラクトは、この *L3Out* で構成された外部 EPG によって消費または提供されます。

または、管理者は、管理テナントの下のファブリックに管理ステーションを直接接続することもできます。その場合、コントラクトはコンシューマにすることも、管理テナントのアプリケーション EPG によって提供することもできます。

注： ファブリックに直接接続されている管理ステーションは、ファブリック内の潜在的な問題の影響を受ける可能性があります。したがって、インシデントが発生した場合にファブリックのトラブルシューティングに必要なシステムまたはサービスを接続することはお勧めしません。

推奨される管理コントラクトの構成

Cisco では、管理者が必要なプロトコルのみを許可し、これらの接続の送信元であると予想される送信元からのみ許可するように、きめ細かい管理コントラクトを構成することを推奨しています。

次の図は、適切な管理コントラクト構成の例を示しています。

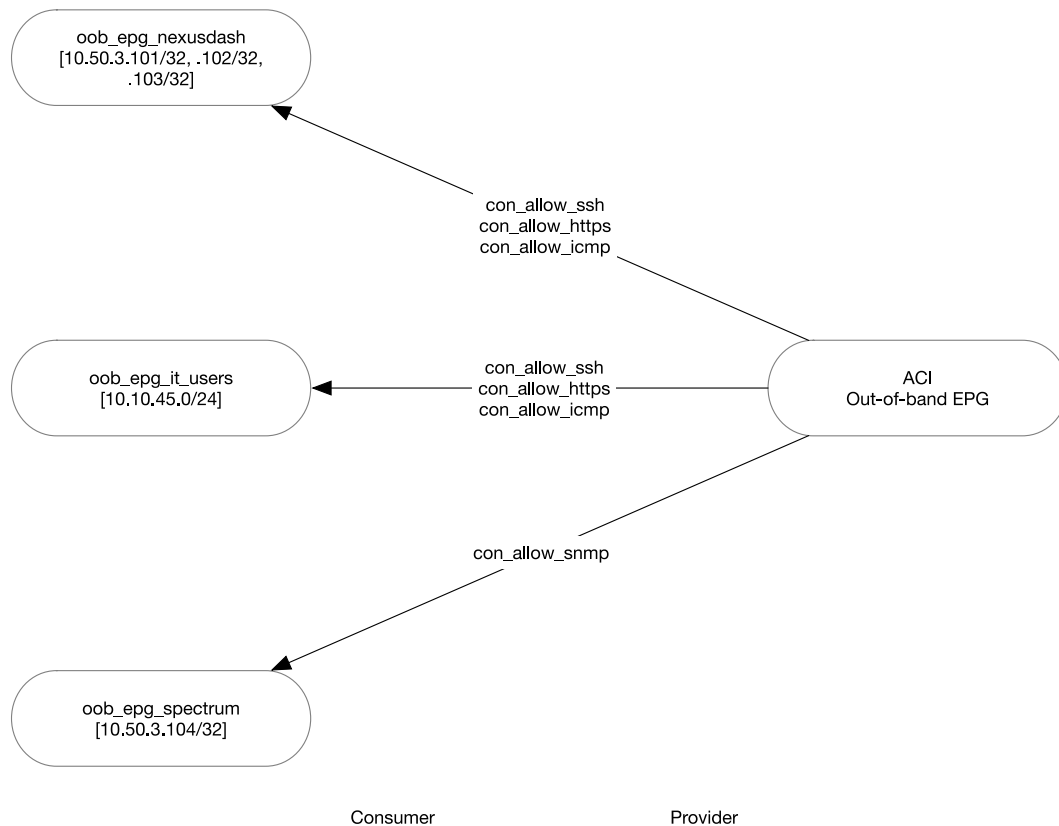


図 12. アウトオブバンド コントラクトの例

上記の例では、管理目的でファブリック アウトオブバンド管理インターフェイスに到達する必要があるさまざまなソースを表す 3 つの外部管理ネットワーク インスタンス プロファイルが作成されています。

これらの発信元ごとに、必要なコントラクトが関連付けられています。この例では、プロトコルごとに個別のコントラクトを使用していますが、これはオプションであり、設計上の選択にすぎません。重要な点は、各送信元に必要なプロトコルまたはポートのみが許可されていることです。

同様の構成がインバンドにも必要です。ただし、重要な違いがあります。アウトオブバンド コントラクトはインバウンド方向でのみ実装され、ステートフルです。これは、**iptables** を使用して内部で実装されるためです。対照的に、インバンド管理コントラクトは、**ACI** ゾーン分割ルール（通常のコントラクトと同じ）を使用して実装されます。つまり、両方向に適用され、ステートレスです。したがって、発信トラフィックも明示的に許可する必要があります。許可しない場合はドロップされます。

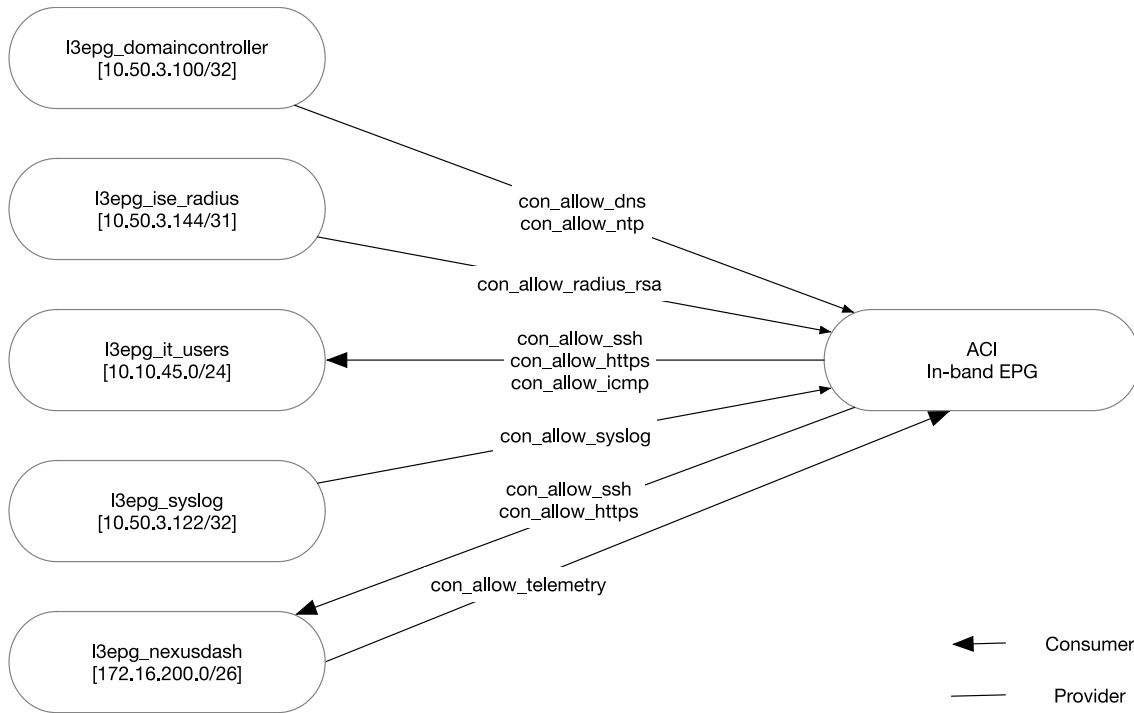


図 13. インバンド コントラクトの例

管理契約の内部

管理コントラクトの構成は、管理者が通常の Cisco ACI コントラクトに慣れている構成とあまり変わりませんが、これらの管理コントラクトの実装は、特にアウトオブバンド コントラクトの場合は大きく異なります。

APIC とスイッチの両方のアウトオブバンドコントラクトは、**iptables**を使用して実装されます。アウトオブバンド コントラクトがレンダリングされると、**iptables** ルールに変換され、ファブリック ノードで構成されます。スイッチまたは APIC を見ると、特定の構成はわずかに異なりますが、一般的な考え方は同じです。

注： APIC での **iptables** の確認は、通常の管理者ユーザーを使用して実行できます。ただし、スイッチで **iptables** を確認するには、ルート アクセスが必要です。

したがって、例として、APIC の **iptables** を見てみましょう。わかりやすくするために、出力がクリーンアップされていることに注意してください。

```

apic1-mdri1# acidiag run iptables-list
Chain INPUT (policy DROP 0 packets, 0 bytes)
target                prot opt in      out      source           destination
apic-default-drop    all  --  *        *        0.0.0.0/0       0.0.0.0/0
apic-scheduler-input all  --  *        *        0.0.0.0/0       0.0.0.0/0
apic-default-allow   all  --  *        *        0.0.0.0/0       0.0.0.0/0
apic-default         all  --  *        *        0.0.0.0/0       0.0.0.0/0
apic-default-ifm     all  --  *        *        10.50.3.111     0.0.0.0/0

Chain FORWARD (policy DROP 0 packets, 0 bytes)
target                prot opt in      out      source           destination
CNI-FORWARD          all  --  *        *        0.0.0.0/0       0.0.0.0/0
ACCEPT               47  --  *        *        0.0.0.0/0       0.0.0.0/0
ACCEPT               all  --  !xcbr0 !bond0.3914 0.0.0.0/0       0.0.0.0/0
ACCEPT               all  --  !bond0.3914 !xcbr0 0.0.0.0/0       0.0.0.0/0
ACCEPT               all  --  docker0 !bond0.3914 0.0.0.0/0       0.0.0.0/0
ACCEPT               all  --  !bond0.3914 docker0 0.0.0.0/0       0.0.0.0/0          ctstate RELATED,ESTABLISHED

Chain OUTPUT (policy ACCEPT 8681 packets, 2504K bytes)
target                prot opt in      out      source           destination
DROP                  icmp --  *        *        0.0.0.0/0       0.0.0.0/0          icmp type 14
apic-scheduler-output all  --  *        *        0.0.0.0/0       0.0.0.0/0

Chain CNI-ADMIN (1 references)
target                prot opt in      out      source           destination

Chain CNI-FORWARD (1 references)
target                prot opt in      out      source           destination
CNI-ADMIN             all  --  *        *        0.0.0.0/0       0.0.0.0/0          /* CNI firewall plugin admin overrides */
ACCEPT               all  --  *        *        0.0.0.0/0       172.17.13.11      ctstate RELATED,ESTABLISHED
ACCEPT               all  --  *        *        172.17.13.11    0.0.0.0/0

Chain apic-default (1 references)
target                prot opt in      out      source           destination
ACCEPT               icmp --  *        *        0.0.0.0/0       0.0.0.0/0          icmp type 255 limit: avg 100/sec burst 10
DROP                 icmp --  *        *        0.0.0.0/0       0.0.0.0/0          icmp type 255
ACCEPT               tcp  --  *        *        0.0.0.0/0       0.0.0.0/0          ctstate NEW tcp dpt:22 limit: avg 2/sec burst 4
REJECT               tcp  --  *        *        0.0.0.0/0       0.0.0.0/0          ctstate NEW tcp dpt:22 reject-with tcp-reset
ACCEPT               tcp  --  *        *        0.0.0.0/0       0.0.0.0/0          ctstate NEW tcp dpt:80
ACCEPT               tcp  --  *        *        0.0.0.0/0       0.0.0.0/0          ctstate NEW tcp dpt:443
ACCEPT               tcp  --  *        *        0.0.0.0/0       0.0.0.0/0          ctstate NEW tcp dpt:4200

Chain apic-default-allow (1 references)
target                prot opt in      out      source           destination
ACCEPT               tcp  --  *        *        0.0.0.0/0       0.0.0.0/0          ctstate RELATED,ESTABLISHED
ACCEPT               udp  --  *        *        0.0.0.0/0       0.0.0.0/0          ctstate RELATED,ESTABLISHED
apic-docker-allow    all  --  !oobmgmt *        *        0.0.0.0/0       0.0.0.0/0
ACCEPT               all  --  !o        *        *        0.0.0.0/0       0.0.0.0/0

Chain apic-default-drop (1 references)
target                prot opt in      out      source           destination
DROP                 tcp  --  *        *        0.0.0.0/0       0.0.0.0/0          tcp flags:0x03/0x03
DROP                 tcp  --  *        *        0.0.0.0/0       0.0.0.0/0          tcp flags:0x06/0x06
DROP                 all  --  oobmgmt *        *        169.254.0.0/16   0.0.0.0/0
DROP                 all  --  docker0 *        *        169.254.0.0/16   0.0.0.0/0
DROP                 all  --  !lo    *        *        127.0.0.0/8      0.0.0.0/0
DROP                 icmp --  *        *        0.0.0.0/0       0.0.0.0/0          icmp type 13
DROP                 tcp  --  oobmgmt *        *        0.0.0.0/0       0.0.0.0/0          tcp dpt:7777
DROP                 tcp  --  oobmgmt *        *        0.0.0.0/0       0.0.0.0/0          tcp dpt:7766
DROP                 tcp  --  oobmgmt *        *        0.0.0.0/0       0.0.0.0/0          tcp dpt:7581
DROP                 tcp  --  oobmgmt *        *        0.0.0.0/0       0.0.0.0/0          tcp dpt:7630
DROP                 tcp  --  docker0 *        *        0.0.0.0/0       0.0.0.0/0          tcp dpt:7777
DROP                 tcp  --  docker0 *        *        0.0.0.0/0       0.0.0.0/0          tcp dpt:7766
DROP                 tcp  --  docker0 *        *        0.0.0.0/0       0.0.0.0/0          tcp dpt:7581
DROP                 tcp  --  docker0 *        *        0.0.0.0/0       0.0.0.0/0          tcp dpt:7630

Chain apic-default-ifm (1 references)
target                prot opt in      out      source           destination
ACCEPT               tcp  --  *        *        0.0.0.0/0       0.0.0.0/0          ctstate NEW tcp dpt:12055
--more--

Chain apic-docker-allow (1 references)
target                prot opt in      out      source           destination
ACCEPT               all  --  !docker0 *        *        0.0.0.0/0       0.0.0.0/0
ACCEPT               all  --  docker0 *        *        172.17.0.0/16    0.0.0.0/0

Chain apic-scheduler-input (1 references)
target                prot opt in      out      source           destination

```

図 14. oobmgmt コントラクトが構成される前の iptables の出力

iptables 出力の上部に、デフォルトの iptables チェーン（入力、出力、および転送）があります。入力と転送の両方のデフォルトアクションは **DROP** です。出力の場合、デフォルトのアクションは **ACCEPT** です。前述したように、アウトバウンド接続はデフォルトで許可されています。これは、確立された接続を許可する別のルールと組み合わせると、アウトオブバンドインターフェイスを介したファブリック開始型の接続を明示的に許可する必要がなくなります。

これらのチェーンは、同様のルールをグループ化し、iptables 管理を簡素化する他のカスタム チェーンを参照します。

- チェーン「**CNI_ADMIN**」および「**CNI_FORWARD**」には、Cisco CNI 通信に必要なルールが含まれています。Cisco Container Network Interface (CNI) は、Cisco ACI 機能をコンテナランタイム環境に拡張するために Cisco が開発したプラグインであり、Cisco ACI と Kubernetes の統合の主要コンポーネントです。
- チェーン「**apic-default**」には、ICMP、HTTPS (443)、SSH (22)、および有効になっている場合は HTTP (80) と Web SSH (4200) を使用したインバウンド接続を許可するデフォルト ルールが含まれています。これらのポートが iptables で許可されている場合でも、Web を介した HTTP または SSH アクセスが明示的に有効になっていない限り、これらのポートでリッスンするサービスがないため、ポートが開いていることにはなりません。詳細については、「[Cisco ACI デバイスの公開ポート](#)」セクションを参照してください。
- チェーン「**apic-default-allow**」には、確立されたセッションと関連するセッション (TCP と UDP の両方)、および oobmgmt とは異なるインターフェイスからの内部トラフィックを許可するための一連の定義済みルールが含まれています。
- チェーン「**apic-default-drop**」には、どのような状況でも外部から到達可能であってはならないいくつかのブロックされたポート、いくつかの特定の TCP フラグを持つトラフィックなど、トラフィックをドロップする一連のルールが含まれています。このルールは、チェーン入力の下での最上位にあります。これは、カスタマー構成がこれらのルールをオーバーライドできないことを意味します。
- チェーン「**apic-default-ifm**」には、APIC IP アドレスから発信され、APIC で実行されている他のサービス宛ての IFM (ファブリック間メッセージング) トラフィックを許可する一連のルールが含まれています。
- チェーン「**apic-docker-allow**」には、APIC Docker 環境で実行されているアプリケーションに属するトラフィックの一連のルールが含まれています。

アウトオブバンド管理コントラクトが適用されると、iptables ルールがそれに応じて変更され、管理者の意図が実装されます。次の例は、サブネット 10.0.0.0/8 からの HTTPS、SSH、および ICMP を許可するコントラクトを適用した後の iptables の表示方法を示しています。変更されたチェーンのみが表示されます。

```

apic1-mdri# acidiag run iptables-list
Chain INPUT (policy DROP 0 packets, 0 bytes)
target                prot opt in      out      source        destination
apic-default-drop     all  --  *        *        0.0.0.0/0     0.0.0.0/0
apic-scheduler-input  all  --  *        *        0.0.0.0/0     0.0.0.0/0
apic-default-allow    all  --  *        *        0.0.0.0/0     0.0.0.0/0
apic-default          all  --  *        *        10.50.3.0/24   0.0.0.0/0
fp-5                  all  --  *        *        0.0.0.0/0     0.0.0.0/0
fp-9                  all  --  *        *        0.0.0.0/0     0.0.0.0/0
fp-19                 all  --  *        *        0.0.0.0/0     0.0.0.0/0
apic-default-ifm      all  --  *        *        10.50.3.111   0.0.0.0/0

--LINES REMOVED--

Chain fp-19 (1 references)
target                prot opt in      out      source        destination        tcp dpt:22
ACCEPT               tcp  --  *        *        10.0.0.0/8     0.0.0.0/0          tcp dpt:4200
ACCEPT               tcp  --  *        *        10.0.0.0/8     0.0.0.0/0

Chain fp-5 (1 references)
target                prot opt in      out      source        destination
ACCEPT               icmp --  *        *        10.0.0.0/8     0.0.0.0/0

Chain fp-9 (1 references)
target                prot opt in      out      source        destination        tcp dpt:443
ACCEPT               tcp  --  *        *        10.0.0.0/8     0.0.0.0/0

```

図 15. oobmgmt コントラクトが構成された後の iptables の出力

コントラクトが適用されると、iptables で次の変更が行われます。

- コントラクトに関連付けられたフィルタごとに 1 つの新しい iptables チェーンが追加されます。チェーン名は、リーフ スイッチでレンダリングされるときに、フィルタに関連付けられたフィルタ ID に実際にマッピングされます。
- チェーン「fp-xx」は、「apic-default」チェーンが参照された直後に INPUT チェーンから参照されます。
- チェーン INPUT のチェーン「apic-default」参照は、送信元 IP アドレスフィルタを適用することによって変更されます。コントラクトが適用されると、デフォルトで開いているポートは、ローカル サブネットからのみアクセス可能になります。コントラクトで特に許可されていない限り、ローカル サブネットを超えた場所からの接続はブロックされます。

注： アウトオブバンド コントラクトが追加されるとすぐに、HTTPS および SSH を使用したアクセスは、直接接続されたアウトオブバンド管理サブネットに制限されます。アウトオブバンドコントラクトで SSH と HTTPS が明示的に許可されていることを確認します。

注： アウトオブバンド契約には、宛先ポートのみが指定されているフィルタを含める必要があります。Cisco APIC リリース 6.0 では、送信元ポートが指定されている場合、宛先ポートとして iptables にレンダリングされるため、管理者の意図とは一致しません。

インバンド管理コントラクトは、iptables を使用して実装されるのではなく、Cisco ACI の他のコントラクトと同じ方法で、スイッチの TCAM でプログラムされた通常のゾーン分割ルールを使用して実装されます。次の例は、インバンド管理コントラクトが適用される場合にゾーン分割ルールがどのようにプログラムされるかを示しています。

```
S1-LEAF1101# show zoning-rule scope 2326528
```

Rule ID	SrcEPG	DstEPG	FilterID	Dir	operSt	Scope	Name	Action	Prio
4124	0	0	implicit	uni-dir	enabled	2326528		deny, log	any_any
4125	0	0	implarp	uni-dir	enabled	2326528		permit	any_any_f
4126	0	15	implicit	uni-dir	enabled	2326528		deny, log	any_vrf_a
4184	0	16386	implicit	uni-dir	enabled	2326528		permit	src_dst
4160	16388	16387	9	bi-dir	enabled	2326528	mgmt:inb_con	permit	fully_o
4243	16387	16388	10	uni-dir-ignore	enabled	2326528	mgmt:inb_con	permit	fully_o
4253	16387	16388	5	uni-dir-ignore	enabled	2326528	mgmt:inb_con	permit	fully_o
4141	16388	16387	5	bi-dir	enabled	2326528	mgmt:inb_con	permit	fully_o
4216	16388	16387	19	bi-dir	enabled	2326528	mgmt:inb_con	permit	fully_o
4260	16387	16388	20	uni-dir-ignore	enabled	2326528	mgmt:inb_con	permit	fully_o

図 16. インバンド管理コントラクトが構成された後のゾーン分割ルール

ルール 4160、4141、および 4216 は、pcTag 16388 が属する送信元 EPG が、インバンド EPG に属する pcTag 16387 を持つ L3Out および宛先 EPG の下の外部 EPG に属している場合、それぞれ HTTPS、ICMP、および SSH を使用したインバンド管理インターフェイスへのインバウンド接続を許可します。

ルール 4243、4253、および 4260 は、以前のルールのリターン トラフィックを許可します。これらのルールは、コントラクト 対象 レベルの下にある [リバース フィルタ ポート (Reverse Filter Ports)] フラグをオンにすることで自動的に作成されます。

注： デフォルトでは、インバンド管理インターフェイスを通過するトラフィックは許可されません。

REST API の強化

Cisco ACI ソリューションの価値提案の 1 つは、ソリューションが提供する強力な REST API です。

この REST API は、システム全体の可用性と応答性を損なう可能性のある潜在的な攻撃や誤用から保護する必要があるもう 1 つの管理インターフェイスです。このセクションでは、REST API を使用した認証方式と、使用可能な DoS 保護メカニズムの 2 つの異なるトピックについて説明します。

REST API を使用した認証

Cisco ACI は、REST API を介して使用できる 2 つの認証メカニズムを提供します。ユーザー名とパスワードを使用した認証と、X.509 証明書を使用した署名ベースの認証です。

ユーザー名とパスワードによる認証

ユーザー名とパスワードを使用する REST API 認証では、特定の URI への POST 要求を使用してログイン プロセスを開始します。ユーザー名とパスワードは、POST 要求で XML または JSON ペイロードとして Cisco APIC に渡されます。したがって、HTTP トランザクションは SSL (HTTPS) を使用して保護することが重要です。

POST 操作への応答には、**Set-Cookie** ヘッダーと応答の属性の両方として認証トークンが含まれます。このトークンの有効期間は制限されており、その後、対象はトークンを更新する必要があります。

REST API の後続の操作では、このトークン値を **APIC-cookie** という名前の **cookie** としてその後の要求の認証に使用できます。

ユーザー名とパスワードの認証は広く使用されており、有効な証明書で HTTPS と組み合わせて使用すれば十分に安全ですが、一部のシナリオではいくつかの課題が発生する可能性があります。この認証方式が提示する一般的なチャレンジは、スクリプトまたは自動化エンジンがすべての API 要求のトークンを更新するときに、ログイン API エンドポイントで要求スロットリングが発生することです。この動作により、APIC は最終的に API 要求を拒否し、エラー コードを返します。

次の方法では、この課題を解決しながら、追加のセキュリティ レベルを提供します。

署名ベースのトランザクションによる認証

署名ベースのトランザクションを使用した REST API 認証では、トランザクションごとに計算される署名が使用されます。その署名の計算には秘密キーが使用され、そのキーは安全な場所に保管して秘密にしておく必要があります。Cisco APIC がトークン以外の署名が付いた要求を受信すると、APIC は X.509 証明書を活用して署名を確認します。

署名ベースの認証では、APIC に対するすべてのトランザクションに新しく計算された署名が必要です。これは、ユーザがトランザクションごとに手動で行うタスクではありません。理想的には、この機能は APIC と通信するスクリプトまたはアプリケーションで使用する必要があります。

注： Cisco ACI Terraform プロバイダと Ansible コレクションは、署名ベースの認証をサポートしていません。

この方法では、攻撃者がユーザ クレデンシャルを偽装またはなりすますためには RSA/DSA キーを解読する必要があります。そのため、最も安全です。この方法では、使用するローカル ユーザーの X.509 証明書を構成する必要はありません。

注： X.509 証明書は、ローカル ユーザーに対してのみ構成できます。リモートユーザーは、署名ベースの認証ではサポートされていません。

署名ベースの認証では、ユーザー名やパスワードなどのペイロード内の機密値は公開されませんが、リプレイ攻撃などの他のタイプの攻撃を防ぐために、HTTPS を使用することをお勧めします。

REST API サービス妨害からの保護

Cisco ACI REST API は、Cisco ACI のバックエンドへの単一のインターフェイスです。GUI や CLI などの他のインターフェイスは、実際には内部で REST API を使用しています。したがって、信頼できるクライアントが REST API を使用できることを確認することが重要です。

攻撃者または不正なスクリプトが REST API に複数の要求を高速で送信している場合、これらの要求は、Cisco APIC インターフェイスを含む同じ API を使用する他の正規のアプリケーションと競合する可能性があります。Cisco ACI は、REST API に対する DoS 攻撃に対して 2 つの異なる保護を提供します。

AAA ログインの HTTP/HTTPS スロットリング

Cisco ACI Web サーバ (NGINX) は、ログインに使用されるエンドポイント、つまり `aaaLogin` および `aaaRefresh` に送信される要求をスロットリングするように、デフォルトで事前構成されています。NGINX では、これらのエンドポイントへのリクエストのレートを 1 秒あたり最大 2 リクエスト、最大バースト 4 に制限するように、2 段階のレート リミッタが構成されています。

このレート制限はユーザーが構成できますが、ほとんどのシナリオではこれらの値を変更する必要はありません。これが必要な場合は、『[Cisco APIC REST API 構成ガイド](#)』を参照してください。

HTTP/HTTPS グローバルスロットリング

Cisco APIC リリース 4.2(3) 以降、Cisco ACI は、任意の API エンドポイントに適用可能なグローバル レート制限の構成をサポートします。このグローバル レート リミッタはデフォルトで無効になっており、**[ファブリック (Fabric)]**、**[ファブリック ポリシー (Fabric Policies)]**、**[ポッドポリシー (Pod Policies)]**、**[管理アクセス (Management Access)]**にある管理アクセス ポリシーを使用して有効にできます。

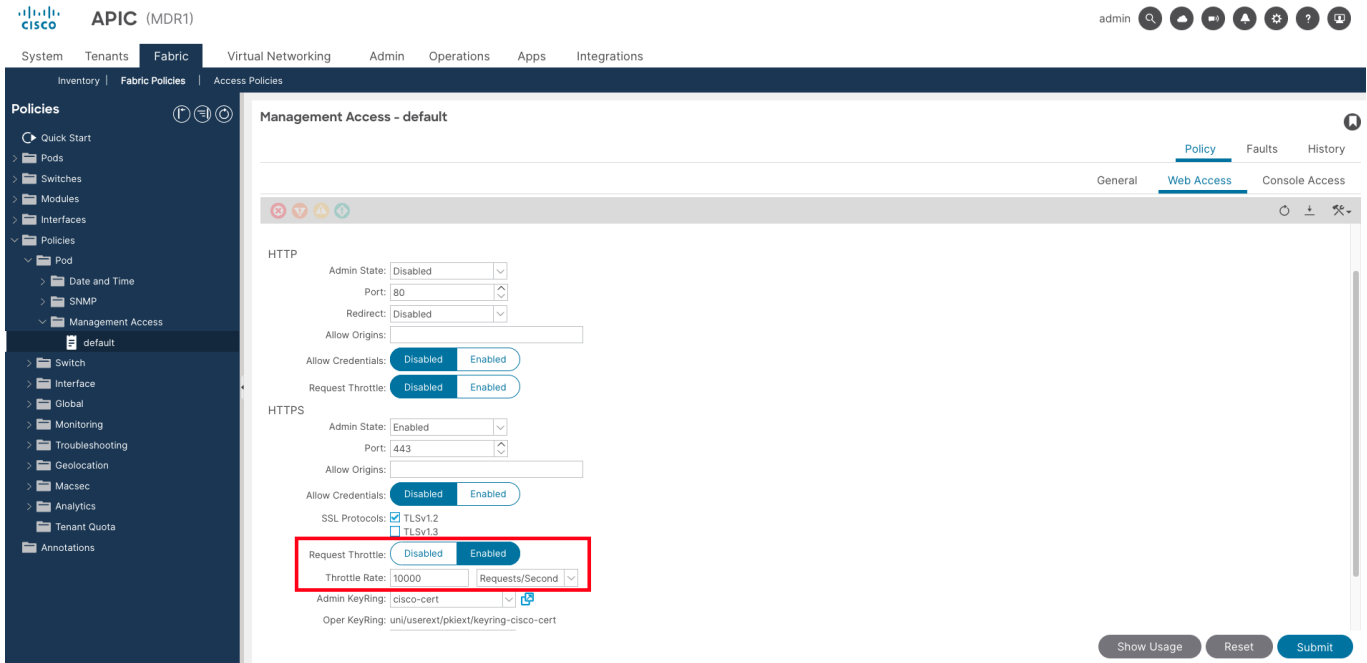


図 17. HTTP/HTTPS グローバルスロットリング構成

HTTPS グローバル要求スロットリングを有効にすることは、DoS 攻撃やスクリプトの誤動作から REST API を保護するための良い方法です。

この値は、Cisco ACI REST API を使用する自動化ツールとリモート システムのニーズと動作に大きく依存するため、すべての環境で機能するスロットルレートの推奨値はありません。

このレート制限の可能な値を評価する場合は、次の点を考慮してください。

- レート制限の 2 倍の最大バーストが自動的に構成されます。
- レート制限は、クライアント IP アドレスごとに個別に適用されます。したがって、1 つのクライアントが許容レートを超過してスロットリングされている場合、これは異なる IP アドレスを持つ他のクライアントには影響しません。
- APIC 自体 (GUI/CLI) からの要求は、レート制限の対象ではありません。

USB ポートの無効化

Cisco ACI コードを実行している Cisco Nexus 9000 スイッチでは、USB ポートがデフォルトで有効になっています。USB ポートが有効になっている場合、スイッチは最初に USB ドライブから起動しようとします。これは、悪意のある攻撃者がデバイスの電源を再投入して、悪意のあるコードを含む USB イメージからスイッチを起動しようとする可能性があるため、悪意のある攻撃者がスイッチに物理的にアクセスした場合、セキュリティリスクになる可能性があります。

ほとんどの組織が物理アクセス セキュリティ ガイドラインを実施していることを考慮すると、これは一般的なシナリオではありませんが、Cisco ACI リリース 5.2(3) では、特定のスイッチ ポリシーを使用して USB ポートを無効にするオプションが導入されました。

デバイスへの物理アクセスが厳密に制御されていない環境、またはこの追加の保護レイヤが必要な環境では、USB ポートを無効にすることをお勧めします。

USB ポートを無効にする方法の詳細については、[こちら](#)を参照してください。

ログインバナーの表示

一部の司法管轄地域では、システムの使用が許可されていないことが通知されていない限り、悪意のあるユーザーが起訴や法的な監視を行うことはできません。この通知を提供する 1 つの方法は、ユーザーがシステムにアクセスしようとしたときに表示されるバナー メッセージにこの情報を配置することです。

法的通知要件は複雑で、司法管轄地域や状況によっても異なるため、この問題はお客様の担当弁護士と相談する必要があります。これらのバナーに通常表示される情報には、次のようなものがあります。

- 特別に承認された人のみがシステムへのログインやシステムの使用を許可されていることを伝える通知と、だれが使用を承認できるのかを示す情報。
- システムの不正な使用は違法であり、民事罰および刑事罰が課される場合があることを伝える通知。
- システムのあらゆる使用が、これ以上の警告なしに記録または監視され、その結果得られたログが裁判所での証拠として使用される場合があることを伝える通知。
- 地域法によって規定されている特定の通知

セキュリティ（法務以外）の観点から、ログイン時のバナーには、ルータの名前、モデル、ソフトウェア、所有権についての具体的な情報は含めないでください。これらの情報は悪意のあるユーザーに利用される可能性があります。次の図に、CLI および GUI バナーの GUI 構成を示します。

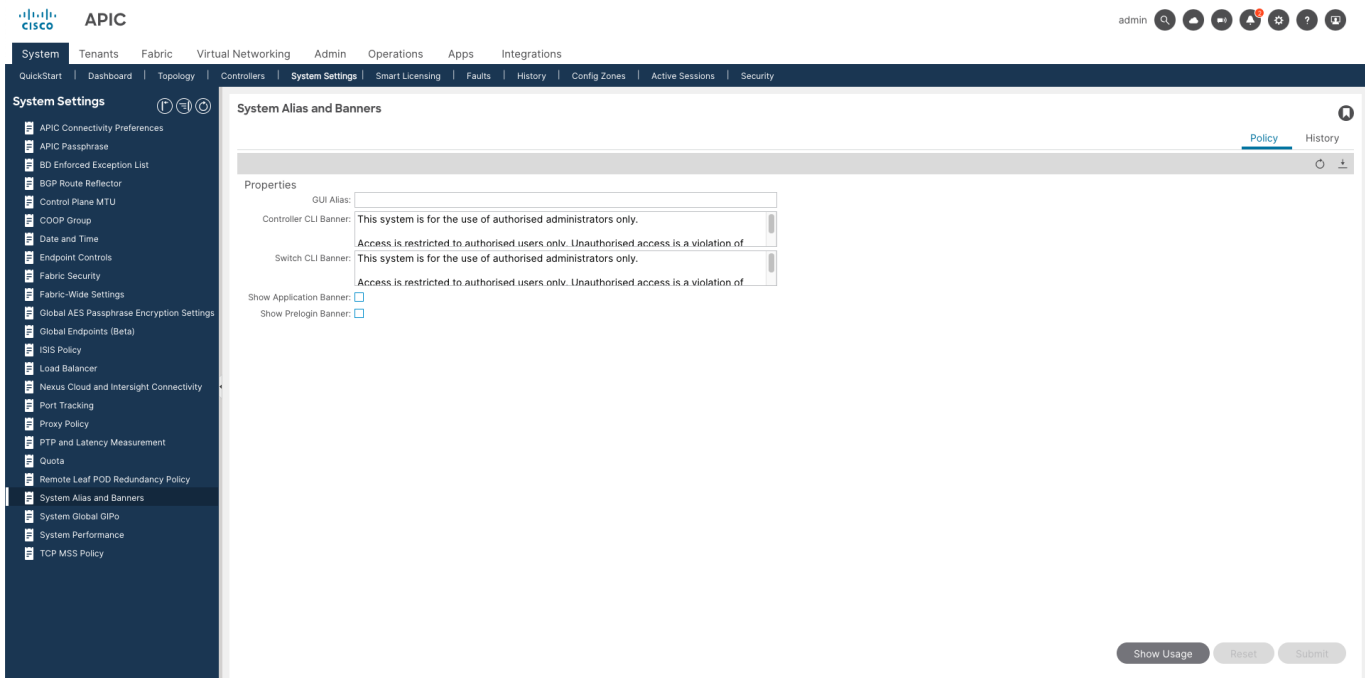


図 18. ログインバナーの構成

CIMC の強化

Cisco CIMC は、Cisco APIC が実行するサーバなど、Cisco UCS C シリーズ サーバの組み込みサーバ管理を提供するベースボード管理コントローラです。他の管理インターフェイスと同様に、CIMC インターフェイスも強化する必要があります。

このセクションでは、この管理インターフェイスを強化するために CIMC で使用する必要がある機能の概要を示します。推奨事項は、CIMC GUI のどこにあるかに基づいてグループ化されます。

- ユーザ管理

- 強力なパスワードの適用とパスワードの自動有効期限を有効にします。
- 可能な場合は、LDAP リモート認証を使用します。
- または、TACACS+ は CIMC 4.1(3b) 以降でサポートされます。
- 他のリモート認証オプションはサポートされていません。
- ネットワーク セキュリティ
 - ログイン試行が数回失敗した後に IP アドレスをブロックするには、**[IP ブロッキング (IP Blocking)]** を有効にします。
 - 制限された IP アドレスのセットからの CIMC アクセスのみを許可するには、**[IP フィルタリング (IP Filtering)]** を有効にします。
- 通信サービス
 - NTP
 - NTP を設定します。
 - NTP 認証はサポートされていません。
 - HTTP/HTTPS
 - HTTPS を適用するには、HTTP から HTTPS へのリダイレクションを有効にします。
 - 自己署名証明書を信頼できる CA 署名付き証明書に置き換えます。
 - SSH/TELNET
 - Telnet はサポートされていません。
 - SSH アクセスを有効にします。
 - SNMP
 - 可能な限り SNMPv3 を使用します。
 - または、読み取り専用 SNMPv2 アクセスを持つことができる IP アドレスを制限します。
- セキュリティ管理
 - 自己署名証明書を、信頼できる CA によって署名された証明書に置き換えます。
 - 必要に応じて、FIPS および CC モードを有効にします。FIPS および CC モードの詳細については、「[FIPS モード](#)」を参照してください。
- その他
 - リモート ロギングを有効にして、ログが外部 syslog サーバに転送されるようにします。これは、**[シャーシ (Chassis)]**、**[障害とログ (Faults and Logs)]**、**[ロギング制御 (Logging Controls)]** の順に選択します。
 - Cisco APIC の場合と同じ推奨事項に従って、ログイン バナーを構成します。これは、**[管理 (Admin)] > [ユーティリティ (Utilities)] > [Cisco IMC バナーの追加/更新 (Add/Update Cisco IMC Banner)]** から実行できます。

注： Cisco IMC は、脆弱性を持つ可能性のあるもう 1 つの管理ソフトウェアです。したがって、CIMC に関連する PSIRT セキュリティ アドバイザリをモニタし、必要に応じてアップグレードします。CIMC をアップグレードする場合は、すべてのサーバファームウェア コンポーネントもアップグレードすることを強く推奨します。CIMC を含むこれらすべてのコンポーネントは、UCS Host Upgrade Utility (HUU) を使用して 1 つのプロセスでアップグレードできます。これには、サーバ BIOS、VIC ファームウェア、RAID コントローラ、およびディスクが含まれます。

注： ESXi で vAPIC を使用している場合は、『VMware セキュリティ強化ガイド』を参照してください。

FIPS モード (FIPS Mode)

連邦情報処理標準 (FIPS) 発行 140-2、暗号化モジュールのセキュリティ要件では、暗号化モジュールの米国政府要件が詳述されています。

FIPS は特定の暗号アルゴリズムがセキュアであることを条件とするほか、ある暗号モジュールが FIPS 準拠であると称する場合は、どのアルゴリズムを使用すべきかも指定しています。

Cisco ACI の FIPS モード

Cisco ACI を使用すると、管理者は FIPS モードを有効にできます。FIPS モードが有効になっている場合、Cisco ACI は使用されている基盤となる暗号ライブラリを変更し、FIPS 140-2 承認の暗号化モジュールである FIPS オブジェクトモジュール バージョン 7.2a (証明書 #4036) の使用を開始します。

注： FIPS モードを有効にするには、システム全体を再起動する必要があります。

FIPS モードを有効にすると、[コンプライアンス レター](#)に記載されているように、Cisco ACI は FIPS 140-2 に準拠します。

この FIPS 準拠の暗号化モジュールは、Cisco ACI ソフトウェアで内部的に確立された暗号化 SSL セッションだけでなく、暗号化アルゴリズムを使用するノースバウンドプロトコルにも使用されます。

FIPS オブジェクトモジュールは、次のプロトコルでサポートされています。

- TLS v1.2 および v1.3
- SSHv2
- SNMPv3

したがって FIPS モードを有効にする前に、上記のプロトコルのサポートされていないバージョンを無効にすることを強くお勧めします。これは、この強化ガイドで提供されている推奨事項に沿っています。

FIPS の注意事項と制限事項の詳細については、『[Cisco APIC セキュリティ構成ガイド](#)』を参照してください。

FIPS モードをイネーブルにするには、次の手順を実行します。

ステップ 1. 『セキュリティ構成ガイド』に記載されている FIPS モードを有効にするためのすべての前提条件と注意事項が満たされていることを確認します。

ステップ 2. Cisco APIC で FIPS モードを有効にします。この設定は、**[システム設定 (System Settings)]** > **[ファブリック セキュリティ (Fabric Security)]** にあります。

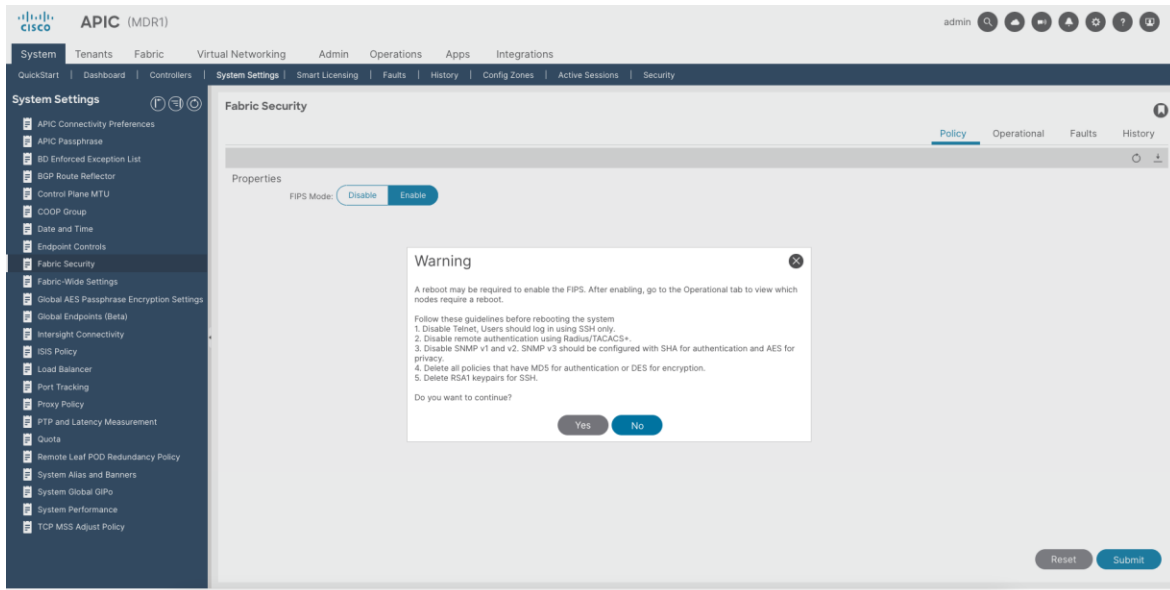


図 19. Cisco APIC で FIPS モードを有効にする

ステップ 3. FIPS モードを有効にするには、すべてのノードを再起動します。動作ステータスには、リポートが保留中のノードが表示されます。

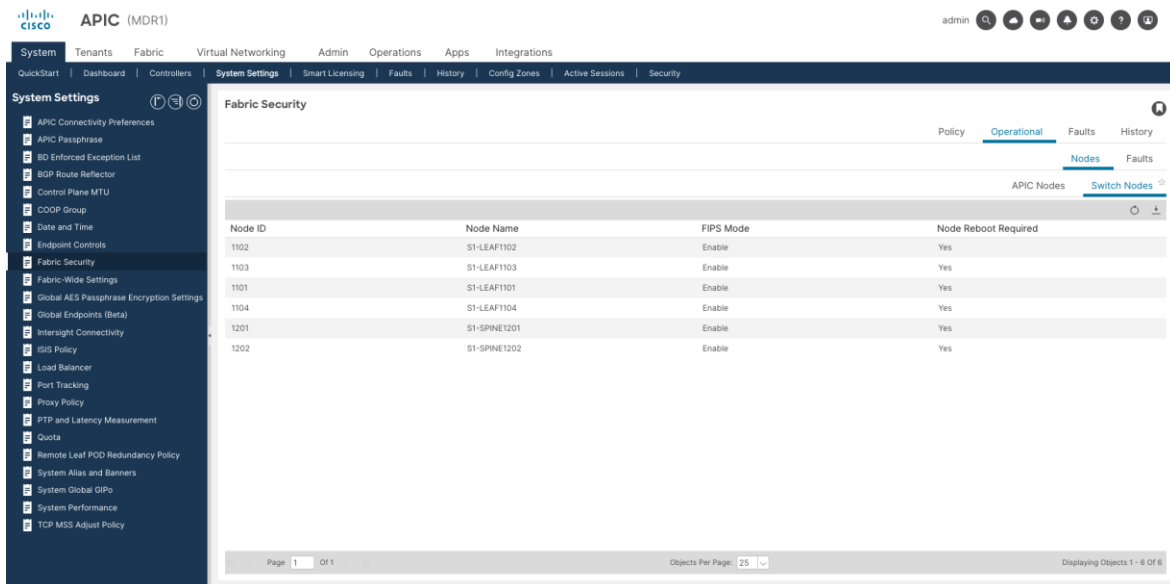


図 20. FIPS モードの動作ステータス、ノードの再起動が必要

APIC で次の CLI コマンドを使用して、FIPS モードの動作ステータスを確認することもできます。

```
apic1-mdr1# show fips status
```

```
ノード ID ノード名 Fips 状態の再起動が必要です
```

```
-----
1 apic1-mdr1 enable no
1101 S1-LEAF1101 enable yes
1102 S1-LEAF1102 enable yes
1103 S1-LEAF1103 enable yes
```

```
1104 S1-LEAF1104 enable yes
1201 S1-SPINE1201 enable yes
1202 S1-SPINE1202 enable yes
```

上記の例では、**APIC** はすでにリロードされていますが、**FIPS** モードを有効にするにはスイッチノードをリロードする必要があります。

一般的なガイダンスとして、**FIPS** モードは、組織が **FIPS** 標準に準拠する必要がある場合にのみ有効にする必要があります。

FIPS Mode in Cisco Integrated Management Controller (CIMC) の FIPS モード

Cisco Integrated Management Controller (CIMC) も、リリース 3.1(3) 以降で **FIPS** に準拠しています。このリリースでは、組織で **FIPS** コンプライアンスが必要な場合に有効にできる **FIPS** モードが提供されます。具体的な手順については、『[Cisco IMC 構成ガイド](#)』を参照してください。

コントロールプレーンのセキュリティ保護

データ センター ファブリックが受ける可能性のあるコントロールプレーンに対する攻撃には、サービス妨害攻撃やコントロールプレーン プロトコル ポイズニング攻撃など、いくつかのタイプがあります。コントロールプレーンを適切に強化して、ファブリックの可用性を保護することが重要です。このセクションでは、最適な保護を実現するために使用可能な機能と推奨される構成を示します。

コントロールプレーン ポリシング (CoPP)

コントロールプレーン ポリシング (CoPP) は、Cisco ACI スイッチのコントロールプレーンの主要な保護メカニズムの 1 つです。コントロールプレーン ポリシングを使用すると、ユーザはレート制限を構成して、スイッチの CPU へのコントロールプレーン パケットのトラフィック フローを管理し、偵察やサービス妨害 (DoS) 攻撃から保護できます。

CoPP は、コントロールプレーン パケットの宛先 (またはパント) であるスイッチ CPU インターフェイス宛でのトラフィックを検査し、トラフィック ポリサーを適用します。CPU に向かうトラフィックの例としては、IGP プロトコルまたは BGP セッションによって発信されたトラフィック、期限切れの TTL などの IP 例外、ARP パケットなどがあります。

スイッチによって転送されるファブリック エンドポイント間のトラフィックは、CoPP によって検査されません。宛先がスイッチ自体であるパケットだけが検査されます。

CoPP はデフォルトで有効になっており、Cisco のエンジニアリング チームによって策定およびテストされ、ほとんどのファブリック展開で十分であることが証明されている Cisco 計算値で事前構成されています。ただし、追加の調整が必要なシナリオもあります。

したがって、推奨されるアプローチは次のとおりです。

1. 最初は、デフォルト ポリシーを使用します。
2. CoPP ドロップをモニタします。
3. ドロップが絶えず増加する場合にのみ、CoPP しきい値を変更します。

CoPP ドロップのモニタ方法

CoPP の統計情報とドロップをモニタするには、CLI コマンドや Cisco APIC GUI 統計情報など、複数の方法があります。さまざまなメカニズムの中で、最も正確な結果を提供するメカニズムは、スイッチで次の CLI コマンドを実行することです。

```
Leaf-101# vsh_lc -c 'show system internal aclqos brcm copp entries unit 0'
```

INGRESS ENTRIES

Ingress = Drops in Bytes

Green = Allowed
Red = Dropped

Byte Policer

Protocol	CPUQ	PolID (Sw/HW)	Prio	Rate (Bps)	Burst (Bytes)	GreenBytes	RedBytes
QINQ	50	2 /1	361	4096000	4096000	0	0
HSRP	38	3 /2	216	4096000	2048000	0	0
LLDP	14	4 /3	356	4096000	4096000	900808361	0
LACP	12	5 /4	347	4096000	4096000	85456256	0
CDP	15	6 /5	338	4096000	4096000	127017604	0
DHCP	25	8 /7	327	5570560	1392640	1656	0

[...]

EGRESS ENTRIES

Egress = Drops in Packets

This is the value configured
in CoPP policy

Packet Policer: Avg pkt size: 3000

Protocol	Type	CPUQ	PolID (Sw/Hw)	Rate (pps)	Burst (pkts)	GreenPkts	RedPkts
glean	Dyn	20	21 /21	100	100	153135	0
coop	Dyn	23	22 /22	5000	5000	475080	0

[...]

OHD	Static	16	4 /4	2000	2000	46619374	2313868
-----	--------	----	------	------	------	----------	---------

[...]

Ignore these drops

図 21. CoPP ドロップを確認するための推奨コマンド

コマンド出力には、入力用と出力用の 2 つのセクションがあり、構造は類似しています。

- **[プロトコル (Protocol)]** は、トラフィックが分類されるプロトコルまたはクラスを示します。
- **レート (bps または pps)** は、ポリサーで構成されたレートを示します。
- **GreenPackets** または **GreenBytes** は、ポリサーによって受け入れられたパケットまたはバイトを示します。
- **RedPackets** または **RedBytes** は、ポリサーによって廃棄されたパケットを示します。これは、モニタする必要がある値です。

注： OHD と呼ばれるクラスがあり、ほとんどのファブリックでドロップが発生する可能性があります。このクラスのドロップは、ドロップされているコントロールプレーン パケットを表していないため、無視できません。

いずれかのクラス (OHD 以外) でドロップが発生し、時間の経過とともにドロップが増加している場合は、対処が必要です。ドロップがあるが、一定の方法で増加しない場合は、トラフィックのピークによって生成された可能性があるため、ドロップは予期され、望ましいドロップです (コントロールプレーンが飽和しないように保護する必要があります)。

この CLI コマンドを使用した大規模なファブリックのモニタリングは、特に自動化を設定する場合は、推奨される方法ではない可能性があります。したがって、REST API を使用してファブリック全体をモニタし、問題が発生した場合にのみこのコマンドを使用してさらに詳しく調べることができます。

CoPP しきい値の変更方法

前述のように、CoPP 統計情報をモニタリングして望ましくないドロップを特定する場合は、CoPP しきい値をカスタマイズする必要があります。この場合、Cisco ACI には CoPP の動作を調整するためのいくつかの構成オプションが用意されています。

たとえば、特定のクラス（またはプロトコル）ごとに CoPP しきい値を変更できます。スイッチごと、さらにはインターフェイスごとに異なるしきい値を適用できます。さらにCisco ACI では、CPU に送信されるコントロールプレーンパケットをフィルタリングするインフラストラクチャ ACL として機能する CoPP プレフィルタを構成できます。

これらの構成オプションについては、『Cisco APIC セキュリティ構成ガイド』の「[コントロールプレーントラフィック](#)」セクションを参照してください。

ICMP リダイレクトおよび到達不能

ICMP メッセージは、DoS 攻撃を実行するために不注意または悪意を持って使用される可能性のある攻撃ベクトルです。同じインターフェイスでパケットを送受信する際に、ルータでは ICMP リダイレクトメッセージが生成される場合があります。この場合、ルータはパケットを転送し、元のパケットの送信者には ICMP リダイレクトメッセージを送信します。この動作により、送信者はそのルータをバイパスして、後続パケットを宛先（または宛先により近いルータ）に直接転送できます。

悪意のあるユーザーは、ルーターに連続してパケットを送信し、これにより強制的にルーターを ICMP リダイレクトメッセージに対応させて、CPU とルーターのパフォーマンスに悪影響を及ぼすことによって、ICMP リダイレクトメッセージを送信するルーターの機能を悪用する可能性があります。

パケットがネットワークでフィルタリングされるたびに、ICMP 到達不能メッセージがトラフィックフローの送信元に送り返される可能性があります。

同様に、悪意のあるユーザーは、フラッドされたデバイスから到達できない宛先アドレスを含む多数のパケットでターゲット デバイスをフラッドすることで、これを悪用できます。これにより、CPU 使用率が増加し、デバイスのパフォーマンスに影響を与える可能性があります。

一般的な強化のベストプラクティスは、ネットワーク デバイスが ICMP リダイレクトメッセージや到達不能メッセージを送信しないようにするか、これらのメッセージをレート制限して悪影響を防ぐことです。ただし、Cisco ACI では、ICMP リダイレクトおよび ICMP 到達不能メッセージはデフォルトで無効になっており、有効にできないため、この強化構成は必要ありません。

コントロールプレーンプロトコル認証

両方のプロトコルがサポートし、すべてのピアがサポートしている限り、コントロールプレーンプロトコルで認証を使用することを強く推奨します。これは、ポイズニング攻撃、中間者攻撃、およびその他の攻撃からコントロールプレーンを保護するのに役立ちます。

Cisco ACI は、NTP、BFD、OSPF、BGP、EIGRP などのほとんどのコントロールプレーンプロトコルと、内部で使用される他のプロトコル（Coop など）の認証をサポートしています。

Council of Oracle Protocol (COOP) での認証

Council of Oracle Protocol (COOP) は、スパインスイッチプロキシにエンドポイントマッピング情報（場所と ID）を通信するために使用されます。COOP を使用したスパインスイッチ（Oracle と呼ばれる）に対してリーフスイッチ転送エンドポイントアドレス情報。スパインノードで実行している COOP によって、すべ

てのスパイン ノードが一貫性のあるエンドポイント アドレスとロケーション情報のコピーを維持することができ、さらに、ロケーション マッピング データベースに対するエンドポイント ID の分散レポジトリを維持することができます。

COOP メッセージは、Zero Message Queue (ZMQ) と呼ばれるプロトコルを使用して、インフラストラクチャ VLAN を介してリーフ スイッチとスパイン スイッチの間で交換されます。したがって、通常の状態では、ファブリックの一部であるデバイスのみがインフラストラクチャ VLAN にアクセスでき、ZMQ メッセージを送受信できます。

COOP には、MD5 認証を利用して、悪意のあるトラフィック注入から COOP メッセージを保護するオプションがあります。Cisco ACI は、2 つの ZMQ 認証モードをサポートします (Strict および Compatible)。厳密モードにおいて、COOP では MD5 認証 ZMQ 接続のみ許可します。Compatible モードでは、COOP では MD5 認証接続と非認証 ZMQ 接続の両方を許可します。

デフォルトでは、Cisco ACI は互換モードを使用します。セキュアで強化されたファブリックの場合、特にインフラストラクチャ VLAN をファブリックの外部に拡張する必要がある場合、つまり、[インフラストラクチャ VLAN の有効化 (Enable Infrastructure VLAN)] が任意の Attachable Access Entity Profile (AAEP) でアクティブな場合は、Strict モードをお勧めします。

注： ACI ファブリックのアップグレード中は、スイッチがアップグレードされるまで、COOP は compatible モードに戻ります。この保護は、アップグレード プロセス中に早期に strict モードを有効にすることでトリガされる可能性がある、予期しない COOP 接続の拒否を防ぎます。ユーザーの観点から必要なアクションはありません。これはアップグレード手順の一部として自動的に処理されます。

インフラ VLAN トラフィックの制限

Cisco ACI CNI を使用したコンテナ ソリューションとの統合など一部の特定の VMM 機能を使用する場合は、インフラストラクチャ VLAN をファブリックの外部に拡張し、外部サーバまたはハイパーバイザまで拡張する必要があります。

このような状況では、ハイパーバイザ間の分離レベルを上げ、インフラストラクチャ VLAN 経由で許可される通信を制限することをお勧めします。これを行うには、ファブリック レベルで [インフラ VLAN トラフィックの制限 (Restrict Infra VLAN Traffic)] オプションを有効にします。

このオプションを有効にすると、各リーフ スイッチはインフラ VLAN 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特定の宛先に許可し、予期しない他のトラフィックをブロックします。Cisco 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。

ファブリック ノード間認証セキュリティ レベル

Cisco ACI ファブリックが起動すると、ファブリックを形成するさまざまなノードが相互に認証し、それら間に信頼関係を構築し、TLS を使用して情報を交換するセキュアなチャンネルを形成します。ファブリック管理者は、このノード間認証を 2 つの異なるセキュリティレベルで実行するように構成できます。

デフォルトでは、ファブリック ノード間認証セキュリティ レベルは permissive に設定されています。permissive モードの場合：

- SSL 証明書は検証されません。
- シリアル番号検証は適用されません。
- コントローラは、ファブリックに参加するために自動的に承認されます。
- ファブリックに参加するには、スイッチを手動で承認する必要があります。

許可モードを使用するファブリックは、1 つ以上のスイッチが無効な証明書を所持していても、正常に動作します。通常の場合では、正規のスイッチは製造プロセスの一部としてプログラムされているため、無効な証明書を持つことはできません。証明書が検証されない場合でも、ノード間の通信は TLS を使用して暗号化されます。

Cisco APIC が **permissive** モードを使用してファブリックに参加すると、初期パラメータが一致している限り、クラスタの一部として自動的に追加されます。シリアル番号や証明書の検証はなく、ユーザーの承認も必要ありません。

ファブリック管理者は、ファブリックノード間認証セキュリティレベルを **strict** に設定できます。**strict** モードは、デフォルトの **permissive** 動作の上に追加のセキュリティメカニズムを追加します。厳密モード：

- SSL 証明書が検証されます。
- シリアル番号検証が適用されます。
- ファブリックに参加するには、コントローラおよびスイッチを手動で承認する必要があります。

strict モードでは、ノードがファブリックに参加できるようになる前に SSL 証明書が検証されます。さらにシリアル番号は、デバイスのシリアル番号を工場出荷時の SSL 証明書の一部として含まれているシリアル番号と比較することによっても検証されます。両方の条件が満たされたノードのみがファブリックに参加できます。

permissive モードと比較した 2 番目の違いは、コントローラがファブリックに参加する方法にあります。厳密モードを有効にすると、管理者は新しい APIC ノードを手動で承認してから、クラスタへの参加を受け入れる必要があります。一方、APIC が接続されているリーフスイッチは、ポートをアウトオブサービス状態に設定して、この APIC がファブリック内の他のものと通信しないようにします。

すべてのカスタマーファブリックで **strict** モードを使用することをお勧めします。これにより、不正なデバイスがファブリックとインフラ VLAN にアクセスし、ファブリックに参加しようとした場合に、特別なレベルの保護が保証されます。

すべてのノードに有効な SSL 証明書がある限り、**permissive** モードから **strict** モードに移行しても影響はありません。したがって、すでに実稼働しているファブリックでこの構成を変更する前に、ファブリック管理者はすべての証明書が有効で、期限切れになっていないことを確認する必要があります。これらの証明書は、**[ファブリック (Fabric)]**、**[インベントリ (Inventory)]**、**[ファブリックメンバーシップ (Fabric Membership)]**、**[登録済みノード (Registered Nodes)]** で確認できます。このチェックを実行した後、管理者はモードを厳密に変更できます。

The screenshot shows the Cisco APIC (MDR1) interface. The main content area displays the configuration for a client named "Client - FDO24090XZM". The "General" tab is selected, showing the following information:

- Properties:** Supported Model: Yes, RL TEP Pool: 0, Rack Name: n9000-16.0(3d), Version: n9000-16.0(3d)
- LLDP Neighbors:** A table with columns: Node ID, Name, Version, Interfaces.
- Certificate:** Subject: /serialNumber=PID-N9K-C9332C SNFDO24090XZM/CN=N9K-C9332C, Valid from: 2020-02-29T18:44:50.000+01:00, Valid to: 2029-05-14T21:25:42.000+01:00

Node ID	Name	Version	Interfaces
1101	S1-LEAF1101	n9000-16.0(3d)	eth1/54
1102	S1-LEAF1102	n9000-16.0(3d)	eth1/54
1103	S1-LEAF1103	n9000-16.0(3d)	eth1/54
1104	S1-LEAF1104	n9000-16.0(3d)	eth1/54

On the right side of the interface, there is a table for "managed Fabric Nodes" with columns "Maintenance Mode" and "Status".

Maintenance Mode	Status
No	Active
No	Active
No	Active
No	Active
No	Active
No	Active

図 22. ファブリック ノード証明書の詳細

ファブリック ノード間認証セキュリティ レベルは、APIC GUI の [システム (System)] > [コントローラ (Controllers)] > [コントローラ (Controllers)] > <apic_name>[ノード別に確認可能なクラスター (Cluster as Seen by Node)] で確認できます。

データ プレーンのセキュリティ保護

Cisco ACI のデータ プレーンは、ファブリック内の異なるエンドポイント間、またはこれらのエンドポイントと外部のルーテッド ドメインおよびスイッチド ドメイン間で送信されるすべての顧客データを伝送します。したがって、データ プレーンを保護することは、整合性、機密性、または可用性の観点から、データが侵害されるのを防ぐために重要です。

この領域は、特にファブリックに接続できるエンドポイントの性質が異なることや、Cisco ACI が使用可能なさまざまな環境とユース ケースにより、その機能が自分のユースケースに適切かどうかを判断するための柔軟性をCisco がファブリック管理者に対して提供しています。

データ プレーン全般の強化

すべてのデータ センター ネットワークで推奨される一般的なベストプラクティスがいくつかあります。これらの一部は、デフォルトで Cisco ACI ですでに適用されているため、管理者によるアクションは必要ありません。

IP送信元ルーティング

IP ソース ルーティングは、Loose Source and Record Route (LSRR) または Strict Source and Record Route (SSRR) オプションを使用して、IP データグラムのソースがパケットが通るネットワーク パスを指定できるようにします。ネットワークのセキュリティ制御に関するトラフィックをルーティングしようとする場合にもこの機能を使用できます。

Cisco ACI では、IP ソース ルーティングはデフォルトで無効になっており、有効にすることはできません。したがって、Cisco ACI は IP ソース ルーティング情報を受け入れず、ファブリックはスイッチのルーティング テーブルに従ってパケットをルーティングします。したがって、特に対処の必要はありません。

IPダイレクトブロードキャスト

IP ダイレクトブロードキャストによって、IP ブロードキャスト パケットをリモート IP サブネットに送信できるようになります。パケットがリモート ネットワークに到達すると、フォワーディング IP デバイスによってパケットはレイヤ 2 ブロードキャストとしてサブネット上の全ステーションに送信されます。このダイレクトブロードキャスト機能は、SMURF 攻撃などいくつかの攻撃で増幅やリフレクションの手段として利用されてきました。

Cisco ACI では、IP ダイレクトブロードキャストはデフォルトで無効になっており、有効にすることはできません。Cisco ACI スイッチは、IP ダイレクトブロードキャスト パケットをドロップします。したがって、特に対処の必要はありません。

ストーム制御

トラフィック ストームは、パケットが LAN でフラッディングする場合に発生するもので、過剰なトラフィックを生成し、ネットワークのパフォーマンスを低下させます。これは通常、ネットワークの構成ミスまたはハードウェア障害の結果として誤って発生しますが、ネットワークの可用性に影響を与える悪意のある攻撃の一部である可能性もあります。

管理者がトラフィック ストーム制御ポリシーを使用すると、物理インターフェイス上におけるブロードキャスト、未知のマルチキャスト、または未知のユニキャストのトラフィック ストームによって、レイヤ 2 ポート経由の通信が妨害されるのを防ぐことができます。

ストーム制御のレートを最初に定義する場合は、同様の環境ですでに使用されている値、選択したインターフェイスのピーク ブロードキャスト トラフィック レベル、またはしきい値の基準として使用した以前のブロードキャスト最大レベルのいずれかに基づいてレートを決定することを推奨します。

観測データの抑制しきい値と、追加のキャパシティを加えたものに基づきます。たとえば、インターフェイスで許容されるピーク ブロードキャスト トラフィックが 1% の場合、1.5% のしきい値が適切です。ポート速度が速いほど、必要な追加容量は少なくなります。

ストーム制御を適用した後、ストーム制御による不要なドロップがないかインターフェイスをモニタし、そのような場合はレートを上げます。

ストーム制御に関する Cisco ACI のデフォルト構成では、ストーム制御を 100% のレートで有効にすることで、ストーム制御を効果的に無効にします。すべてのお客様がストーム制御を有効にし、上記の一般的な注意事項に基づいて値を設定することをお勧めします。

Cisco ACI は、フラッドイングを減らすためにストーム制御以外のメカニズムを提供します。これらのメカニズムは、ハードウェア プロキシなどのブリッジ ドメインごとに有効にできます。これにより、不明なユニキャストがブリッジ ドメイン全体にフラッドイングされるのを防ぐことができます。

IP フラグメント

従来のネットワークで、フラグメント化された IP パケットのフィルタリングは、セキュリティ デバイスにとって課題となることがあります。フラグメント処理はわかりにくいいため、IP フラグメントが誤って ACL によって許可されることがあります。したがってフラグメンテーションは、侵入検知システムによる検出を回避する試みでしばしば使用されます。

さらに、IP フラグメントは、ティアドロップ攻撃など、データグラム フラグメンテーション メカニズムを利用する他のタイプの悪意のある攻撃でよく使用されます。これらの理由から、ネットワークに適用される ACL の最上位でフィルタリングすることを推奨します。

繰り返しますが、Cisco ACI はこの領域ですぐに使用できるより高いレベルのセキュリティを提供します。Cisco ACI は、デフォルトでゼロトラストセキュリティ モデルを実装しています。つまり、明示的に許可されていないトラフィックはすべてドロップされます。パケットが許可されるかドロップされるかを判断するために、IP/TCP ヘッダー（レイヤ 3 およびレイヤ 4）からの情報が使用されます。

IP フラグメントが Cisco ACI で受信されると、リーフ スイッチには 適切なフィルタを適用するために必要な情報を決定する方法がありません。したがって、ACI はデフォルトで IP フラグメントを廃棄します。IP フラグメントを許可する必要がある場合は、後続のフラグメントに一致するフィルタ エントリを使用して明示的に許可する必要がありました（最初のフラグメントにはパケット ヘッダーがあるため、通常どおり処理されます）。

要約すると、管理者の観点からみると、IP フラグメントをフィルタリングするためのアクションは必要ありません。一方、アプリケーションまたは通信で IP フラグメントを許可する必要がある場合は、それらを明示的に許可する必要があります。

Mis-Cabling Protocol (MCP) を使用したループからの保護

従来のネットワークとは異なり、Cisco ACI ファブリックはスパンニングツリープロトコル (STP) には参加せず、ブリッジ ドメイン データ ユニット (BPDU) を生成しません。BPDU は、同じエンドポイント グループお

よび VLAN にマッピングされたポート間で、ファブリックを介して透過的に転送されます。そのため、Cisco ACI は、外部デバイスのループ防止機能にある程度依存します。

2 つのリーフポートを誤ってケーブル接続した場合などは、ファブリック内の LLDP を使用して直接処理されま
す。ただし、別レベルでの保護が必要な場合もあります。そのような場合は、Mis-Cabling Protocol (MCP)
を有効にすることが役立ちます。

MCP は、STP または LLDP で検出できないファブリック内のループから保護するように設計された軽量プロト
コルです。MCP は、タイムスタンプが付けられ、ファブリックで構成された MCP キーによって一意に識別さ
れる小さなレイヤ 2 パケットを使用します。MCP パケットは、MCP が有効になっているすべての運用中（稼
働中）のポートから送信され、MCP パケットが戻るのをファブリックが確認した場合、ファブリックはループ
があることを認識し、そのイベントに基づいてアクションを起こします。

ループが検出されると、MCP は障害、イベント、および syslog メッセージを生成して状況を通知します。さ
らに、そうするように構成されている場合、MCP もポートを err-disable にします。Cisco ACI は、errdisable
リカバリ ポリシーを構成し、errdisabled ステータスから自動的に回復するように構成できます。

MCP は、グローバルに、およびインターフェイスごとに有効にできます。デフォルトでは、グローバルに無効
にされ、各ポートで有効になっています。MCP が機能するには、インターフェイス単位の構成に関係なく、グ
ローバルに有効にする必要があります。

デフォルトでは、MCP PDU はネイティブ VLAN 経由でのみ送信されます。VLAN ごとの MCP を有効にする
と、MCP はサポートされている最大数（リリースに応じて 256 または 2000。特定のバージョンの MCP の
ACI スケーラビリティ ガイドを参照）まで、ポートでアクティブな各 VLAN で MCP PDU を送信します。
VLAN 単位の MCP を使用すると、MCP は非ネイティブ VLAN のループを検出できます。ただし、アクション
はポート全体に適用されることに注意してください。

強化の観点から、Cisco では、外部デバイスに面するすべてのポートで MCP を有効にし、実際に付加価値が高
いインターフェイスでのみ VLAN 単位 MCP を有効にすることを推奨します（すべてのポートで VLAN 単位
MCP を有効にすることは、ファブリック）。

MCP の使用に関する推奨事項の詳細については、『Cisco ACI 設計ガイド』の「[Miscabling Protocol \(MCP\)](#)」セクションを参照してください。

アンチスプーフィング メカニズム

IP および MAC アドレス スプーフィングは、攻撃者がネットワーク パケット内の送信元 IP または MAC アド
レスを変更して、別のネットワーク エンティティから送信されたかのように見せる手法です。スプーフィング
は、セキュリティ制御のバイパスや正当なエンティティの偽装など、さまざまな悪意のある目的に使用される可
能性があります。

Cisco ACI には、アドレス スプーフィングのリスクを軽減するための機能がいくつか用意されています。以下
で説明する機能は、このセクションで説明されている場合でも、スプーフィング以外の他のタイプの攻撃に対し
て効果的です。

サブネットチェックの適用 (Enforce Subnet Check)

サブネットチェックの適用機能は、VRF レベルでサブネット チェックを適用し、IP アドレスがサブネット外で
はないエンドポイントのみを Cisco ACI が学習するようにします。サブネット チェック範囲が VRF レベルだ
としても、この機能はファブリック全体での設定ポリシーの下ではグローバルにのみ有効または無効にでき
、ファブリック内のすべての VRF インスタンスに適用されます。

[サブネットチェックの適用 (Enforce Subnet Check)] は、エンドポイントがローカル エンドポイント（入力リーフで受信したトラフィック）であるか、リモート エンドポイント（別のリーフから受信したトラフィック）であるかによって動作が異なります。

入力リーフ（ローカル エンドポイント学習）では、Cisco ACI は、受信パケットの送信元 IP アドレスが入力ブリッジドメインサブネットの 1 つに属している場合にのみ、IP アドレスと MAC アドレスを新しいローカルエンドポイントとして学習します。

出力リーフ（リモート エンドポイント学習）では、Cisco ACI は、受信パケットの送信元 IP アドレスが出力リーフの同じ VRF インスタンス内のブリッジドメインサブネットに属している場合にのみ、IP アドレスをリモートエンドポイントとして学習します。

この動作により、エンドポイントが VRF インスタンスのブリッジドメインのいずれにも属していない予期しない送信元 IP アドレス（L3Out 接続の背後に存在する IP アドレスなど）を持つパケットを送信する、IP アドレススプーフィングシナリオを防止します。

[サブネットチェックの適用 (Enforce Subnet Check)] を有効にすることをお勧めします。

注： [サブネットチェックの適用 (Enforce Subnet Check)] を有効にすると、すべてのリモートエントリが削除されます。これによりリモートエントリの学習が短時間停止されます（30 秒）。スパインプロキシのエントリは削除されないため、構成変更中でもトラフィック転送は継続されます。[サブネットチェックの適用 (Enforce Subnet Check)] を有効にしても、中断は予想されません。ただし VRF インスタンスに属さないサブネットからのトラフィックをネットワークが処理している場合に機能を有効にすると、これらのトラフィックフローが中断されます。

ポートセキュリティ

Cisco ACI のポートセキュリティは、ポートごとに MAC アドレスの数を制限することによって、不明な MAC アドレスでフラグディングしないようにファブリックを保護します。ポートセキュリティは、アクセスインターフェイスで MAC アドレススプーフィングを移行するために使用できます。

この機能を使用すると、管理者は特定のインターフェイス（アクセス、ポートチャネル、または VPC）で学習できる MAC エンドポイントの最大数を指定できます。MAC アドレスの数がその特定のポートで設定された最大値を超えると、MAC ラーニングは無効になり、MAC アドレスは CAM テーブルに追加されません。Mac ラーニングは、設定されているタイムアウト値の後に再度有効になります。

データセンター固有のリスク評価に基づいて、この機能の必要性を慎重に評価することをお勧めします。管理者は、DC 環境（特に仮想化されている場合）はダイナミックであるため、ポートの背後にある MAC アドレスの数は時間の経過とともに大きく変動する可能性があることを考慮する必要があります。したがって、通常、エンドポイントの最大数を予測することはできません。

その他の注意事項と考慮事項については、『Cisco APIC セキュリティ構成ガイド』の「[ポートセキュリティ](#)」セクションを参照してください。

IEEE 802.1X

802.1X は、ポートベースのネットワーク アクセス コントロールを提供するネットワーク認証プロトコルです。これは IEEE 802.1X 標準の一部であり、通常はイーサネット経由でネットワークに接続しようとするデバイスの認証および許可のメカニズムを定義します。

802.1X は、ポートに接続されたエンドユーザーまたはデバイスに基づいてネットワーク接続を許可または拒否する機能を提供します。802.1X 対応ポートは、それに接続するユーザーまたはデバイスの ID に基づいて、ダイナミックに有効または無効にすることができます。

802.1x は、キャンパス ネットワークのアクセス レイヤでセキュリティ ルールを適用する上で重要な役割を果たしますが、通常は DC 環境では使用されません。DC は通常物理的に安全で制御されていると見なされるため、サーバは通常データ センター スイッチに対して自身を認証する必要はありません。

ただし、802.1x を活用してデータ センター内のアクセス制御を強化できるユース ケースがいくつかあります。たとえば、DC 内の適切なリソースへの VM ユーザー アクセスを提供するために 802.1x を使用できる VDI 環境などです。

Cisco ACI は 802.1X をサポートしているため、管理者はこの機能が特定のユース ケースに必要であると考えられる場合に設定できます。Cisco ACI での 802.1X 設定の詳細については、『Cisco APIC セキュリティ構成ガイド』の「[802.1X](#)」セクションを参照してください。

ファーストホップ セキュリティ

初期ホップ セキュリティ (FHS) は、スプーフィングや中間者攻撃など、さまざまなネットワーク攻撃から保護することを目的とした一連のセキュリティ機能を指します。ネットワークの初期ホップ ルータやスイッチに実装されるこれらの機能は、ロールの強制、バインディングの強制、DoS 攻撃の緩和を実行するなどして、ARP、DHCP、ND などの特定のプロトコルの全体的なセキュリティを向上させます。

Cisco ACI で、FHS 機能はテナント ブリッジ ドメイン (BD) ごとに有効になっています。Cisco ACI でサポートされている機能は次のとおりです。

- IP インスペクション : ARP、ND、および DHCP インスペクションを含む
- ソース ガード : IPv4 および IPv6 ソースガードを含む
- ルータ アドバタイズメント (RA) ガード

さらに、信頼制御ポリシーを EPG ごとに構成して、DHCP、ARP、または ND インスペクションの観点から特定のエンドポイントを信頼できるものとして設定できます。

これらの機能は、データ センター環境のセキュリティを強化するのに役立ちますが、偶発的な問題 (意図しない IP アドレスのスプーフィングなど) からの保護にも役立ちますが、これらの機能は規模に影響を与えるため、すべてのデータ センター展開にこれらの機能を推奨することはできません。

データ センターは通常、エンドポイントが信頼され、新しいエンドポイントの接続または起動が許可された管理者のみに制限されている環境です。ただしこれは標準ですが、複数の攻撃者にアクセス権が付与される共有 DC 施設や、多くの個人がほとんど制御されずにリソースをスピンアップできるような、軽く制御されたセルフ サービス アクセスのある環境など、そうでない場合もあります。

このようなシナリオでは、ファーストホップ セキュリティ (FHS) 機能の使用が推奨されます。これらのシナリオでも、FHS は、これが必要なブリッジ ドメインでのみ有効にする必要があります。

FHS の注意事項と考慮事項の詳細については、『Cisco APIC セキュリティ構成ガイド』の「[ファーストホップ セキュリティ](#)」セクションを参照してください。スケーラビリティのガイダンスについては、お使いのリソースの「[検証されたスケーラビリティ ガイド](#)」を参照してください。

MACsec

MACsec は、IEEE 802.1AE 規格ベースのレイヤ 2 ホップバイホップ暗号化であり、これにより、メディア アクセス非依存プロトコルに対してデータの機密性と完全性を確保できます。

Cisco ACI は、ファブリック ポート、つまりリーフ スイッチとスパイン スイッチ間のインターフェイス (Fabric MACsec)、および外部デバイスへのアクセス ポート (Access MACsec) で MACsec をサポートします。

可能な限り、Cisco ACI マルチポッドなどの分散アーキテクチャで MACsec を使用することをお勧めします。このようなシナリオでは、特に組織の完全な制御下でないリンクをトラフィックが通過する場合に、相互接続ネットワーク（この場合はポッド間ネットワーク（IPN））を通過するトラフィックを保護します。

MACsec はホップバイホップ暗号化を提供するため、MACsec を使用して IPN トラフィックを保護するには、パス内のすべてのデバイスが MACsec（または別の代替暗号化メカニズム）を実装する必要があります。

MACsec は、Cisco ACI で *Must Secure* モードと *Should Secure* モードの 2 つの異なるモードをサポートします。

Must Secure モードはリンクで暗号化されたトラフィックのみを許可し、*Should Secure* モードはリンク上でクリアおよび暗号化されたトラフィックの両方を許可します。*Must Secure* モードで MACsec を展開する前に、キーチェーンは影響を受けるリンクで展開する必要がありますまたはリンクがダウンします。この問題に対処するには、*Should Secure* モードで MACsec を展開し、すべてのリンクが起動した後にセキュリティ モードを *Must Secure* に変更することを推奨します。

Cisco ACI での MACsec に関するその他の考慮事項（*Must Secure* モードに関する追加の考慮事項を含む）については、『Cisco APIC レイヤ 2 ネットワーキング構成ガイド』の「[MACsec](#)」セクションを参照してください。

Cisco ACI セキュリティ ポリシー（別名コントラクト）

このセクションで説明する強化機能とセキュリティ機能に加えて、Cisco ACI はお客様がゼロトラスト ネットワーク セキュリティ アーキテクチャを実装できるようにする許可リスト ポリシー モデルを提供します。Cisco ACI を使用すると、2 つの特定のエンドポイントグループ（EPG）間の通信はデフォルトで拒否されるため、必要な通信を明示的に許可する必要があります。

ポリシーは、2 つの EPG 間のトラフィックを許可、拒否、ログ、またはリダイレクトするコントラクトとして表されます。固有の EPG に属する 2 つのエンドポイントが同じ物理スイッチまたは仮想スイッチのインターフェイスに接続されている場合でも、これらの EPG 間の通信を許可する明示的な許可/リダイレクト ポリシーがコントラクト上にある場合を除き、これらのエンドポイント間に接続はありません。

Cisco ACI は、EPG 間のトラフィックを制限するさまざまなユース ケースに対応する多数の機能を提供し、セグメンテーションとマイクロセグメンテーションの過程で組織をサポートします。これには、次のような機能が含まれます。

- Inter-VRF および Intra-VRF コントラクト
- ポリシーベースのリダイレクションとレイヤ 4 からレイヤ 7 へのサービス挿入
- EPG 内分離および EPG 内コントラクト
- vzAny コントラクト
- エンドポイントセキュリティ グループ（ESG）

Cisco ACI コントラクトとセグメンテーション機能を使用して、データセンター内で East-West トラフィック フローおよび North-South トラフィック フローのセグメンテーションを提供し、前者の場合は他のセキュリティ デバイスやソリューションと組み合わせて、*defense-in-depth* 戦略を実施することをお勧めします。

これらの各機能については、このホワイト ペーパーの範囲外です。これらのすべての機能については、Cisco ACI のドキュメントを参照してください。このトピックに関する参考資料は次のとおりです。

- [Cisco ACI 設計ガイド](#)
- [Cisco ACI コントラクト ガイド ホワイト ペーパー](#)

- [Cisco ACI Policy-Based Redirect Service Graph Design White Paper](#)
- [Cisco ACI エンドポイントセキュリティグループ \(ESG\) 設計ガイド](#)

工場出荷時のセキュリティ強化とシステム整合性

このホワイトペーパーの前のセクションでは、Cisco ACI ソリューションを強化し、攻撃対象領域を減らしてソリューション全体の安全性を高めるために推奨される構成について説明しました。ただし、Cisco ACI には Cisco ACI を本質的に安全にすることを目的とした、製品のアーキテクチャに組み込まれた追加のセキュリティレイヤがいくつかあります。このセクションでは、これらのソリューションの一部について説明します。

デバイス認証とファブリック内メッセージング暗号化

Cisco ACI ファブリックの起動中、または新しいデバイスがファブリックに追加されるたびに、認証プロセスがトリガされ、製造時に一意でデジタル署名された X.509 証明書を使用して、すべてのノードが Cisco APIC によって認証されます。

これらの証明書は、APIC 側のトラステッドプラットフォーム モジュール (TPM)、および Cisco Nexus 9000 スイッチのトラステッドアンカー モジュール (TAM) と呼ばれるセキュアなハードウェア暗号化モジュールに安全に保存されます。

証明書は、ファブリックで構成されたファブリック ノード間認証セキュリティ レベルに従って検証されます (このドキュメントの「ファブリックノード間認証セキュリティ レベル」のセクションを参照)。

検証が完了すると、Cisco ACI ファブリックはそれらの X.509 証明書を使用して、TLS1.2 を使用してファブリック内でセキュアな通信を確立します。したがって、構成、モニタリング、および操作に使用されるファブリック内のすべてのメッセージングが暗号化されます。

トラストアンカーモジュール (TPM)

TPM チップは、暗号化操作を実行するように設計されたセキュアな暗号化モジュールです。TPM には、改ざん防止のための複数のセキュリティ メカニズムが含まれています。TPM は、サーバの認証に使用されるアーティファクトを安全に保存し、ブート プロセス中にプラットフォームの整合性を確保します。アーティファクトとは、パスワード、証明書や暗号化キーなどを指します。

Cisco APIC は TPM を使用して、APIC サーバを一意に識別し、特定のシリアル番号を持つ正当な Cisco APIC サーバであることを証明するために使用される証明書を安全に保存します。Cisco APIC は、サーバでの実行が許可されているデジタル署名されたソフトウェア イメージを検証するために必要な暗号化キーを保存するためにも TPM を使用します。

トラストアンカーモジュール (TAM)

TPM と同様に、トラステッドアンカー モジュール (TAM) は、Cisco Nexus 9000 スイッチ (および Cisco のポートフォリオ内の他のデバイス) にインストールされた改ざん耐性のある Cisco Trust Anchor チップであり、Cisco Secure Boot プロセスの基本的な部分である偽造防止対策を実装するために使用されます。

Cisco Nexus 9000 スイッチは、TAM を使用して X.509 証明書をハードウェアに安全に保存します。これには、証明書だけでなく、関連するキー ペアと証明書チェーン全体も含まれます。このすべての情報は、クロード、セキュリティ保護、および監査済みの製造プロセス中に TAM にプログラムされます。このプログラミングは強力なサプライ チェーン セキュリティを提供します。これは、ルータやスイッチなどの組み込みシステムにとって重要です。

シスコのセキュアブート

シスコのセキュアブートは、シスコ製ハードウェア プラットフォーム上で実行される最初のコードが真正であり、改ざんされていないことを確認します。このプロセスには、2つの個別の部分が含まれます。

一方で、整合性と信頼性が保証されるように、Cisco のソフトウェア イメージに署名する必要があります。すべての Cisco ACI ソフトウェア イメージは、RSA-2048 秘密キーを使用してデジタル署名されます。

一方、Cisco のハードウェア プラットフォームは、インストールする前にイメージが有効であり、変更されおらず、本物であることを確認できる必要があります。Cisco ACI プラットフォームのこのソフトウェア認証はハードウェアに固定されているため、最も堅牢なセキュリティが提供されます。

イメージが Cisco ACI ファブリックデバイスにロードされると、ハードウェア ルートの Cisco Secure Boot を使用し、APIC またはスイッチ イメージの検証にそれぞれ TPM または TAM 暗号化モジュールを利用して、署名されたイメージの信頼性を常に検証する必要があります。この検証が正常に完了した場合にのみ、イメージのロードと起動を完了できます。デジタル署名チェックが何らかの失敗をした場合、Cisco ACI デバイスはそのソフトウェアを起動させず、悪意のあるコードがデバイスに実行されないように確認します。

Web アプリケーションセキュリティ

Cisco APIC Web インターフェイスは、おそらく Cisco ACI と対話するために最も広く使用されているインターフェイスであり、強力な REST API がそれに続きます。製品の安全性を高めるという Cisco の取り組みに沿って、Cisco ACI は最新の Web セキュリティ メカニズムを実装して、一般的な Web 攻撃を防止または軽減します。

これらのセキュリティ メカニズムには、次のようなものがあります。

- クロスサイト スクリプティング (XSS) 保護 (ユーザー入力の検証と反射型 XSS 攻撃に対する保護を含む)。
- HTTP Strict Transport Security (HTST) を使用して、main-in-the-middle 攻撃を防止し、SSL の使用を強制します。HSTS は、Strict-Transport-Security という名前の応答ヘッダー フィールドを使用して、HTTPS のみを使用してサイトにアクセスする必要があること、および HTTP を使用してアクセスしようとするると自動的に HTTPS に変換する必要があることをブラウザに通知します。
- OS フィンガープリントの防止と、HTTP サーバ ヘッダーで潜在的な攻撃者に提供される情報の削減。Cisco ACI では、使用されている Web サーバに関する情報は含まれません。

Cisco ACI デバイスの公開ポート

多くの場合、特定の攻撃にさらされる可能性を評価したり、攻撃対象領域を把握したりするために、特定のシステムで開いているポートを特定する必要があります。分析の実行方法によっては、実際に存在するポートよりも多くのポートが公開されているという印象を与える可能性があるため、混乱を招く可能性があります。

ホスト ファイアウォール、iptables、およびサービス対象のポートで許可されているポートを明確に区別することが重要です。

管理者が APIC で実行されているプロセスと、それらがリッスンしているポートを確認すると、複数のプロセスとポートが開かれていることがわかります。ただし、これらのポートが外部に公開されていることを意味するのではなく、iptables が機能する場所です。

逆のことも起こり得ます。管理者が APIC レベルで iptables エントリをチェックすると、開きたくないいくつかのポート (HTTP/80 など) があることに気づき、iptables で許可されていると表示されます。問題は、ポートが実際にサービスを提供されているかどうかです。

ポートがサービスされているということは、あるサービスやアプリケーションがその特定のポートをアクティブにリッスンし、受信接続を受け入れ、そのポートが外部からアクセス可能であることを意味します。nmap の用語では、フィルタ処理されたポートまたは閉じられたポートとは対照的に、これはオープンポートです。

実際、これらの検証では、Cisco ACI で公開されているポートの完全なビューを提供することはできません。より良いアプローチは、nmap などのツールを使用してファブリックに対してポート スキャンを実行し、外部からアクセス可能で受信接続をアクティブにリッスンしているポートを証明することです。

デフォルト構成の Cisco ACI ファブリック、つまり追加の管理プロトコルが構成されておらず、管理コントラクトが適用されていない場合、これは nmap を使用した完全なポートスキャンの結果です。

```
[root@utils-01-mdr1 ~]# nmap -Pn -n -p0- -v -A -T4 apic1-mdr1.cisco.com
Starting Nmap 6.40 ( http://nmap.org ) at 2023-07-11 16:16 WEST
NSE: Loaded 110 scripts for scanning.
NSE: Script Pre-scanning.
Initiating ARP Ping Scan at 16:16
Scanning apic1-mdr1.cisco.com (10.50.3.111) [1 port]
Completed ARP Ping Scan at 16:16, 0.20s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 16:16
Scanning apic1-mdr1.cisco.com (10.50.3.111) [65536 ports]
Discovered open port 22/tcp on 10.50.3.111
Discovered open port 443/tcp on 10.50.3.111
SYN Stealth Scan Timing: About 4.14% done; ETC: 16:28 (0:11:58 remaining)
--LINES REMOVED--
Completed SYN Stealth Scan at 16:26, 618.63s elapsed (65536 total ports)
Initiating Service scan at 16:26
Scanning 2 services on apic1-mdr1.cisco.com (10.50.3.111)
Completed Service scan at 16:26, 18.04s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against apic1-mdr1.cisco.com (10.50.3.111)
Retrying OS detection (try #2) against apic1-mdr1.cisco.com (10.50.3.111)
NSE: Script scanning 10.50.3.111.
Initiating NSE at 16:26
Completed NSE at 16:26, 0.10s elapsed
Nmap scan report for apic1-mdr1.cisco.com (10.50.3.111)
Host is up (0.00025s latency).
Not shown: 65532 filtered ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.2 (protocol 2.0)
80/tcp closed http
443/tcp open ssl/https?
|_http-favicon: Unknown favicon MD5: D05D9B3C0EB82AB07AD1496EE983996C
|_http-methods: No Allow or Public header in OPTIONS response (status code 405)
|_http-title: APIC
|_ssl-cert: Subject: commonName=apic1-mdr1.cisco.com/organizationName=Cisco Systems
Inc./stateOrProvinceName=California/countryName=US
| Issuer: commonName=HydrantID Server CA 01/organizationName=IdenTrust/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
```

```
| Not valid before: 2023-01-11T09:22:00+00:00
| Not valid after: 2024-01-11T09:21:00+00:00
| MD5: ddae b5ff 4f52 2d4d 0af5 8988 eb48 e279
|_SHA-1: 7615 e12e ea42 874e eff1 cb6c c131 3f8b af3f 7c09
```

4200/tcp closed vrml-multi-use

データが返されましたが、1 個のサービスが認識されませんでした。サービス/バージョンがわかっている場合は、次のフィンガープリントを <http://www.insecure.org/cgi-bin/servicefp-submit.cgi> で送信してください。

```
SF-Port443-TCP:V=6.40%T=SSL%I=7%D=7/11%Time=64AD74B6%P=x86_64-redhat-linux
SF:-gnu%r(GetRequest,FDE,"HTTP/1\1\20200\200K\r\nServer:\20Cisco\20AP
SF:IC\r\nDate:\20Tue,\2011\20Jul\202023\2015:27:13\20GMT\r\nContent-
SF:Type:\20text/html;\20charset=utf-8\r\nContent-Length:\203251\r\nConn
SF:ection:\20close\r\nVary:\20Accept-Encoding\r\nLast-Modified:\20Mon,\
SF:x2013\20Mar\202023\2022:10:33\20GMT\r\nVary:\20Accept-Encoding\r\n
SF:ETag:\20"640f9f59-cb3"\r\nExpires:\20Thu,\2001\20Jan\201970\200
SF:0:00:01\20GMT\r\nCache-Control:\20no-cache\r\nAccess-Control-Allow-He
SF:aders:\20Origin,\20X-Requested-With,\20Content-Type,\20Accept,\20D
SF:evCookie,\20APIC-challenge,\20Request-Tag\r\nAccess-Control-Allow-Met
SF:hods:\20POST,GET,OPTIONS,DELETE\r\nX-Frame-Options:\20SAMEORIGIN\r\nS
SF:trict-Transport-Security:\20max-age=31536000;\20includeSubDomains\r\n
SF:Client-Cert-Enabled:\20false\r\nX-Content-Type-Options:\20nosniff\r\n
SF:X-XSS-Protection:\201;\20mode=block\r\nAccess-Control-Allow-Origin:\x
SF:20http://127\0\0\1:8000\r\nAccess-Control-Allow-Credentials:\20fals
SF:e\r\nAccept-Ranges:\20bytes\r\n\r\n<html>\n<head><!--\20production-->
SF:0-->\n<title>APIC</title>\n<meta\20content="text/html"\>\n<meta\20ch
SF:a")%r(HTTPOptions,310,"HTTP/1\1\20405\20Not\20Allowed\r\nServer:\x2
SF:0Cisco\20APIC\r\nDate:\20Tue,\2011\20Jul\202023\2015:27:18\20GMT
SF:\r\nContent-Type:\20text/html;\20charset=utf-8\r\nContent-Length:\20
SF:331\r\nConnection:\20close\r\nETag:\20"640f9f59-14b"\r\nAccess-Cont
SF:rol-Allow-Headers:\20Origin,\20X-Requested-With,\20Content-Type,\20
SF:Accept,\20DevCookie,\20APIC-challenge,\20Request-Tag\r\nAccess-Contr
SF:ol-Allow-Methods:\20POST,GET,OPTIONS,DELETE\r\nAccess-Control-Allow-Or
SF:igin:\20http://127\0\0\1:8000\r\nAccess-Control-Allow-Credentials:\
SF:x20false\r\n\r\n<!DOCTYPE\20html\20PUBLIC\20"-//W3C//DTD\20XHTML\20
SF:201\0\20Transitional//EN"\20"http://www.w3.org/TR/xhtml1/DTD/xht
SF:ml1-transitional.dtd">\n<html\20xmlns="http://www.w3.org/1999/xht
SF:ml">\n<head>\n<meta\20http-equiv="Content-Type"\20content="text/h
SF:tml;\20charset=UTF-8"\20/>\n<title>Untitled\20Document</title>\n</h>
SF:ead>\n\n<body>\n405\20Method\20Not\20Allowed\n</body>\n</html>\n");
MAC Address: 10:F9:20:BE:B1:7E (Unknown)
```

Aggressive OS guesses: Netgear DG834G WAP or Western Digital WD TV media player (94%), OpenWrt Kamikaze 7.09 (Linux 2.6.22) (93%), Asus RT-N10 router or AXIS 211A Network Camera (Linux 2.6) (92%), AXIS 211A Network Camera (Linux 2.6.20) (92%), OpenWrt (Linux 2.4.32)

```
(92%), OpenWrt White Russian 0.9 (Linux 2.4.30) (92%), Linux 2.6.24 (92%), Linux 2.6.18 - 2.6.24 (92%), Linux 2.6.16 (92%), OpenWrt 0.9 - 7.09 (Linux 2.4.30 - 2.4.34) (92%)
```

```
No exact OS matches for host (test conditions non-ideal).
```

```
Network Distance: 1 hop
```

```
IP ID Sequence Generation: All zeros
```

```
TRACEROUTE
```

```
HOP RTT ADDRESS
```

```
1 0.25 ms 10.50.3.111
```

```
NSE: Script Post-scanning.
```

```
Read data files from: /usr/bin/./share/nmap
```

```
OS and Service detection performed. Please report any incorrect results at  
http://nmap.org/submit/ .
```

```
Nmap done: 1 IP address (1 host up) scanned in 641.47 seconds
```

```
Raw packets sent: 197149 (8.679MB) | Rcvd: 529 (22.502KB)
```

上記の出力によると、**iptables** で許可されている 4 つのポート (**22**、**80**、**443**、および **4200**) があり、そのうちポート **22** と **443** のみがアクティブにサービスされていることがわかります。デフォルトでは、ポート **80** および **4200** でリッスンするサービスはありません。

リーフ スイッチまたはスパイン スイッチに対して同じテストを実行しても、同様の結果が得られます。デフォルトでは、ポート **22** と **443** のみがオープンまたはサービスされます。

まとめ

結論として、サイバー攻撃がますます頻繁かつ巧妙になっている世界では、インフラストラクチャの強化がこれまで以上に重要になっています。デジタル インフラストラクチャを強化するためのさまざまなセキュリティ対策を実装することで、組織はリスクを軽減し、重要な資産と情報を保護し、永続的な脅威に直面しても運用を維持できます。

Cisco ACI は、攻撃対象領域を減らし、堅牢で安全なデータセンター ネットワーク インフラストラクチャを組織に提供するために、複数のセキュリティメカニズムを実装しています。デフォルトのこのレベルのセキュリティと、このドキュメントで説明されている推奨事項により、**Cisco ACI** はより厳しいセキュリティ要件を満たす堅牢なインフラストラクチャになります。

米国本社
Cisco Systems, Inc.
カリフォルニア州サンノゼ

アジア太平洋本社
Cisco Systems (USA), Pte. Ltd.
シンガポール

ヨーロッパ本社
Cisco Systems International BV
Amsterdam, The Netherlands

2023 年 11 月発行

© 2023 Cisco and/or its affiliates. All rights reserved.

Cisco および Cisco ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の国における商標または登録商標です。シスコの商標の一覧については、www.cisco.com/go/brand をご覧ください。記載されているサードパーティの商標は、それぞれの所有者に帰属します。「パートナー」または「partner」という言葉が使用されていても、シスコと他社の間にパートナーシップ関係が存在することを意味するものではありません。1175152207 10/23



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。