Cisco ACI のベストプラクティス

概要

2021 年 7 月

目次

概要

このペーパーでは、大多数（すべてではない場合）のユーザーが利用する必要がある Cisco ACI の構成オプションを示します。ユースケースに応じて使用する必要がある設定については、『Cisco ACI Design Guide』、その他のホワイトペーパー、または構成ガイドを参照してください。

ホワイトペーパー： https://www.cisco.com/c/ja_jp/solutions/data-center-virtualization/application-centric-infrastructure/white-paper-listing.html

構成ガイド： https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html

注：この製品のドキュメント セットは、偏向のない言語を使用するように配慮されています。このドキュメントセットでの偏向のない言語とは、年齢、障害、性別、人種的アイデンティティ、民族的アイデンティティ、性的指向、社会経済的地位、およびインターセクショナリティに基づく差別を意味しない言語として定義されています。製品ソフトウェアのユーザーインターフェイスにハードコードされている言語、RFP のドキュメントに基づいて使用されている言語、または参照されているサードパーティ製品で使用されている言語によりドキュメントに例外が存在する場合があります。

エンドポイント学習設定

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（Enforce Subnet Check）] は、各 VRF インスタンスのブリッジ ドメインで設定されたサブネットに基づいて、不要または意図しないエンドポイント学習（ローカルとリモートの両方）を防止します。これは、ローカル エンドポイントの学習のみを防止する、ブリッジ ドメインの **[IP 学習をサブネットに制限する（Limit IP Learning to Subnet）]**オプションの拡張バージョンです。

ベストプラクティスは、このオプションを有効にすることです。

場所

- 2.2(2q) : [ファブリック（Fabric）] > [アクセス ポリシー（Access Policies）] > [グローバルポリシー（Global Policies）] > [ファブリック全体の設定ポリシー（Fabric Wide Setting Policy）]
- 2.3(1) ～ 3.0(1)：サポート対象外
- 3.0(2)～最新 : [システム（System）] > [システム設定（System Settings）] > [ファブリック全体の設定（Fabric Wide Setting）]

オプション/注意事項

- これは、-EX、-FX、またはそれ以降のリーフノードでのみ機能します。古いリーフ ノード モデルを実行している場合は、すべてのブリッジ ドメインで **[IP 学習をサブネットに制限する（Limit IP Learning to Subnet）]** を使用します。
- 詳細については、『 Cisco ACI Endpoint Learning 』ドキュメントを参照してください。

エンドポイント IP のエージング

デフォルトでは、各エンドポイント（1 つの MAC アドレスと 1 つ以上の IP アドレス）には、エンドポイント保持タイマーと呼ばれるエージング タイマーが 1 つだけあります。**IP エージング** を使用すると、各 IP アドレスが独自のタイマーを維持できるため、個別にエージアウトするできます。この機能が有効になっていない場

合、MAC アドレスがファブリックで現用系ままである限り、学習されたすべての関連付けられた IP アドレスは、それらの IP アドレスがトラフィックの発信元でなくなった場合でも、その MAC アドレスに関連付けられたファブリックで学習されたままになります。

ベスト プラクティスは、このオプションを有効にすることです。

場所

- 2.1(1) – 2.3(1) : [ファブリック] > [アクセス ポリシー] > [グローバル ポリシー] > [IP エージング ポリシー]の [IP エージング] オプション。
- 3.0(1)ー最新 : [システム設定] > [エンドポイント制御] > [IP エージング]

オプション/注意事項

- 詳細については、「Cisco ACI エンドポイント学習」を参照してください。

ループ緩和の設定

MCP を有効にする（VLAN ごとに）

MisCabling Protocol（MCP）は、外部ソース（誤動作しているサーバー、STP を実行している外部ネットワーク機器など）からのループを検出し、ACI が自身のパケットを受信するインターフェイスを err-disable にします。

ベスト プラクティスは、ループを発生させる可能性のある外部レイヤ 2 ネットワークに接続されているリーフ ノード ポートで、このオプションを有効にすることです（「VLAN ごとの MCP PDU の有効化（Enable MCP PDU per VLAN）」を使用する場合もあります）。

場所

- 1.1(1) – 3.1(2) : [ファブリック（Fabric）] > [アクセス ポリシー（Access Policies）] >> [ポリシー（Policies）] > [グローバル（Global）] > [MCP インスタンス ポリシー（MCP Instance Policy）] のデフォルト
- 3.2(1) – 最新： [ファブリック（Fabric）] > [アクセス ポリシー（Access Policies）] >> [ポリシー（Policies）] > [グローバル（Global）] > [MCP インスタンス ポリシー（MCP Instance Policy）] のデフォルト

オプション/注意事項

- 「VLAN ごとに MCP PDU を有効にする」オプション (2.0(2) 以降で使用可能) により、MCP は VLAN ごとにパケットを送信できるようになります。それ以外の場合、これらのパケットはタグなし VLAN でのみ送信され、ループはそれらの VLAN でのみ検出されます。VLAN ごとの MCP には、インターフェイスあたり 256 VLAN の拡張性制限があります。
- Cisco ACI には、リーフノードごとに 2,000 の論理的なポート（VLAN x ポート）の拡張性制限があります。
- システムの規模がこれらの制限を超える可能性がある場合は、特に VLAN ごとに MCP を有効にするときに注意してください。VLAN ごとの MCP PDU の処理は CPU に負荷がかかる可能性があるためです。

  各ファームウェアバージョンの最新の拡張性数値については、『Verified Scalability Guide』を参照してください。

EP ループ保護または不正エンドポイント制御

EP ループ保護 は、同じセットの 2 つのインターフェイスで学習されているエンドポイントを検出してループを検出します。ループが検出されると、Cisco ACI ファブリックは、エンドポイントが移動していたインターフェイスの 1 つをシャットダウンするか（***ポートの無効化***）、またはループがあるブリッジドメインのエンドポイント学習を無効にします（***[BD Learn の無効化]***）。どちらのアクションも有効になっていない場合、**EP ループ保護** はループイベントを内部プロセス（EPMC：エンドポイントマネージャクライアント）ログに記録しますが、アクションを実行したり、障害を発生させたりすることはありません。

不正エンドポイント制御 は、設定された間隔内に同じエンドポイントが異なるインターフェイスで複数回学習された場合に、エンドポイント（MAC/IP アドレス）を不正として識別します。誤動作している不正エンドポイントは、それ以上の移動を防ぐために最後に学習されたインターフェイスに固定され、設定されたホールド間隔の後に削除されます。これにより、Cisco ACI ファブリックは、新しいエンドポイントの場所に関してファブリック内のデバイスを常に更新する必要がなくなり、より安定した Cisco ACI 環境が可能になります。

また、両方のオプションで障害が発生します。構成されている場合は、syslog/SNMP トラップに送信できます。

ベスト プラクティスは、**[不正エンドポイントポイント制御（Rogue Endpoint Control）]** を **有効**にすることです。

ただし、（EP ループ保護）

- 1.1(1) ～ 2.3(1) : [ファブリック（Fabric）] > [アクセスポリシー（Access Policies）] > [グローバルポリシー（Global Policies）] > [EP ループ保護ポリシー（EP Loop Protection Policy）]
- 3.0(1) ～ 最新 : [システム（System）] > [システム設定（System 設定 ）] > [エンドポイント制御（Endpoint Controls）] > [EP ループ保護（Ep Loop Protection）]

ただし、（不正なエンドポイントの制御）

- 3.2(1) ～ 最新 : [システム（System）] > [システム設定（System 設定 ）] > [エンドポイント制御（Endpoint Controls）] > [不正 EP 制御（Rogue EP Control）]

オプション/注意事項

- **不正エンドポイント制御（Rogue Endpoint Control）** が有効になっている場合、**EP ループ保護（EP Loop Protection）** は有効になりません。ループの影響を軽減するための各オプションの長所と短所を理解した後、いずれかを選択します。
- 詳細については、『Cisco ACI Design Guide』および『 Cisco ACI Endpoint Learning』を参照してください。
- 既存のファブリックで **不正エンドポイント制御**または **EP ループ保護** を有効にする場合は、ファブリックで現在発生しているループまたはフラップがないことを確認します。それ以外の場合は、エラー アクションがすぐに実行されます。

ブリッジ ドメイン設定

ユニキャスト ルーティング

ユニキャスト ルーティング により、ブリッジドメインはトラフィックをルートし、エンドポイント IP アドレスを学習できます。

ベスト プラクティスは、エンドポイントのデフォルト ゲートウェイがブリッジ ドメイン SVI でない場合は、このオプションを有効にしないことです。

場所

- [テナント（Tenant）] > [ネットワーキング（Networking）] > [ブリッジ ドメイン（Bridge Domains）] > [L3 構成（L3 Configurations）]

オプション/注意事項

- エンドポイントのデフォルト ゲートウェイがブリッジ ドメイン スイッチ仮想インターフェイス（SVI）ではない場合、ブリッジ ドメインはスイッチングのみを行います。この場合、 **ユニキャスト ルーティング** が有効になっており、IP アドレスがブリッジ ドメインで学習されている場合、この設定によりパケット転送の問題が発生する可能性があります。詳細については、 Cisco ACI エンドポイント学習のホワイトペーパー を参照してください。

L2 不明なユニキャスト

L2 不明ユニキャスト は、ブリッジ ドメイン が不明な MAC アドレス 宛てのパケットをフラッディングするか（***[フラッド （Flood）]***）、または COOP データベース ルックアップのためにスパインノードに送信するか（***[ハードウェア プロキシ（Hardware Proxy）]***）を決定します。

次のいずれかのシナリオでは、このオプションを ***[フラッド （Flood）]*** に設定するベスト プラクティスをお勧めします。

- ユニキャスト ルーティングは無効化されています。
- レイヤ 2 は、移行中など、Cisco 以外の ACI スイッチを使用して拡張されます。

場所

- [テナント（Tenant）] > [ネットワーキング（Networking）] > [ブリッジ ドメイン（Bridge Domains）] > [ポリシー（Policy）] > [全般（General）]

オプション/注意事項

- 上記の 2 つのシナリオの詳細については、 『Cisco ACI Design Guide』 を参照してください。

ARP フラッディング

ARP フラッディングは、ブリッジ ドメインが ARP 要求を常にフラッディングするか（[***Enabled***]）、または ARP ヘッダーでターゲット IP アドレスを検索してユニキャスト回送を実行するか（[***Disabled***]）を決定します。

ベストプラクティスは、クラスタ化されたサーバー、ファイアウォール、または負荷バランサがある場合にこのオプションを ***[有効（Enabled）]*** に設定して、GARP がフラッディングされるようにすることです。

場所

- [テナント（Tenant）] > [ネットワーキング（Networking）] > [ブリッジ ドメイン（Bridge Domains）] > [ポリシー（Policy）] > [全般（General）]

オプション/注意事項

- 詳細については、『Cisco ACI Design Guide』 を参照してください。

QoS の設定

DSCP 変換

DSCP 変換 は、Cisco ACI QoS クラスを VXLAN パケットの外部 IP アドレス ヘッダーの DSCP に変換して、トラフィックがポッドまたはサイトを通過するときにクラスが保持されるようにします。このオプションを使用しない場合、Cisco ACI QoS クラスは外部 Dot1Q ヘッダーを介して CoS として伝送され、IPN/ISN で変更または削除されるリスクが高くなります。

ベストプラクティスは、 **DSCP 変換** を有効にし、IPN/ISN で使用されていない DSCP クラスを Cisco ACI QoS クラスに割り当てることです。これにより、これらの DSCP 値が IPN/ISN によって上書きされなくなります。

場所

- [テナント（Tenant）] > [インフラ（infra）] > [プロトコル（Protocol）] > [L3 トラフィックの DSCP クラス CoS 変換ポリシー]

オプション/注意事項

- **DSCP 変換** と **CoS の保持** は同時に使用できません。
- **CoS の保持** は、入力リーフノードからの元の CoS とともに Cisco ACI QoS クラスも DSCP に変換します。ただし、 **Preserve CoS** は設定不可能な内部 DSCP マッピングを使用します。つまり、ユーザは、信頼する DSCP 値を選択し、IPN/ISN で変更しないで ください。一方、**DSCP 変換**を使用すると、 元の CoS を変更できないというトレードオフを伴い、選択した DSCP 値を Cisco ACI QoS クラスにマップします。
- Cisco ACI ファブリックが Cisco ACI マルチポッドと Cisco ACI マルチサイトのいずれも使用していない場合は、**[CoS の保持（Preserve CoS）]** を使用できます。

その他の設定

ファブリック ポート トラッキング

ファブリック ポート トラッキングは、特定のリーフ ノード上の稼働中のファブリック ポート（アップリンク）の数を監視し、設定されたしきい値以下に減少すると、リーフ ノードのダウンリンク ポートがダウンし、外部デバイスが他の正常なリーフ ノードに切り替えることができるようになります。

ベスト プラクティスは、しきい値としてゼロの現用系ファブリック ポートでこのオプションを有効にすることです。

場所

- 1.2(2) ～ 3.2(1) : [ファブリック（Fabric）] > [アクセスポリシー（Access Policies）] > [ポリシー（Policies）] > [グローバル（Global）] > [ポートトラッキング（Port Tracking）]
- 3.2(2) : 最新 : [システム（System）] > [システム設定（System Settings ）] > [ポートトラッキング（Port Tracking）]

オプション/注意事項

- Cisco 以外のすべての ACI デバイスが、vPC などの適切なフェールオーバーメカニズムを使用して冗長性を確保するために 2 つ以上のリーフ ノードに接続されている場合は、しきい値として 0 より大きい値を設定できます。
- すべての APIC が冗長性のために推奨されるように 2 つのリーフ ノードに接続されている場合（「APIC 接続」を参照）、***[APIC ポートを含める（Include APIC ports）]*** オプションを有効にすることができます

グローバル AES 暗号化

AES 暗号化 を使用すると、Cisco APIC はパスワードを暗号化し、構成のエクスポート（バックアップ）に含めることができます。このような構成バックアップをインポートする場合は、 **AES 暗号化**を有効にするために使用したものと同じパスフレーズを指定する必要があります。このオプションを構成しないと、設定のバックアップにはパスワードがなく、VMM ドメインなどのパスワードを必要とする構成は、インポート後に機能しなくなります。

ベスト プラクティスは、このオプションを有効にすることです。

場所

- 4.0(1) より前：[管理（Admin）] > [AAA] > [構成エクスポート（とインポート）のための AES 暗号化パスフレーズおよびキー（AES Encryption Passphrase and Keys for Config Export (and Import)）]
- 4.0(1) から：[システム（System）] > [システム設定（System 設定 ）] > [グローバル AES パスフレーズ暗号化設定（Global AES Passphrase Encryption 設定 ）]

オプション/注意事項

- パスフレーズを忘れた場合は、新しいパスフレーズで **AES 暗号化** を再構成し、構成を再度エクスポートします。

VLAN Pool

VLAN プール は、各 VLAN に割り当てられる VXLAN 識別子 （VNID）を決定します。たとえば、VLAN プール A と VLAN プール B の VLAN 10 には、異なる VNID が割り当てられます。AEP は、Cisco ACI スイッチ上のインターフェイスのグループを表します。Cisco APIC は、VLAN プールと AEP を関連付ける物理ドメインなどのドメインに基づいて、どのインターフェイス上のどの VLAN にどの VLAN プールを使用するかを決定します。

ベスト プラクティスは、VLAN 範囲の重複を避けるために、最小数の VLAN プールを構成することです。

場所

- （[ファブリック（Fabric）] > [アクセス ポリシー（Access Policies）] > [プール（Pools）] > [VLAN プール（Vlan Pools）]）

オプション/注意事項

- 同じ AEP に関連付けられた VLAN 識別子範囲が重複している複数の VLAN プールがある場合、VNID の割り当てが不確定になり、エンドポイント学習、STP BPDU フラッディングなどにさまざまな問題が発生する可能性があります。

- 最終的に、ポートごとの VLAN など、異なる VLAN プールを必要とする機能が必要ない場合は、ファブリック全体に対して 1 つまたは 2 つの VLAN プールで十分です。
- [システム（System）] > [システム設定（System Settings）] > [ファブリック全体の設定（Fabric Wide Setting）]（3.2(6) リリース以降で利用可能）の下にある **EPG VLAN 検証の強制**を検討してください。これにより、重複する VLAN プールを含む 2 つのドメインが同じ EPG に関連付けられるのを防ぎます。VNID 割り当てロジックに精通していて、重複する VLAN プールを意図的に使用する必要がある場合は、この検証は必要ありません。そうではない場合は、このオプションを有効にすることをお勧めします。

ISIS 再配布メトリック

Cisco ACI マルチポッド展開では、 **ISIS 再配布メトリック** は、スパインノードがルーティングプロトコル（OSPF など）から ISIS にこれらのルートを再配布する場合の Cisco ACI インフラ TEP ルートのメトリックセットです。これらの再配布された ISIS ルートは、同じポッド内のリーフ ノードにアドバタイズされるため、スパイン ノードを介して他のポッドに到達できます。

ベストプラクティスは、このメトリックを、デフォルトの 63 ではなく、62 以下に設定することです。

場所

- 5.0(1) 以前：[ファブリック（Fabric）] > [ファブリック ポリシー（Fabric Policies）] > [ポリシー（Policy）] > [ポッド（Pod）] > [ISIS ポリシー デフォルト（ISIS Policy Default）] > [再配布ルートの ISIS メトリック（ISIS metric for redistributed routes）]
- 5.0(1) 以降：[システム（System）] > [システム設定（System 設定）] > [ISIS ポリシー（ISIS Policy）] > [再配布されたルートの ISIS メトリック（ISIS metric for redistributed routes）]

オプション/注意事項

- スパイン ノードが再起動するか、新たにファブリックに参加すると、スパイン ノードが安定して Cisco APIC からのポリシーのダウンロードが完了するまで、ノードはより高いメトリックで ISIS 再配布ルートをアドバタイズするしようとします。これは「過負荷モード」と呼ばれます。 **ISIS 再配布メトリック** が最大値であるデフォルト値の 63 のままである場合、過負荷と非過負荷のメトリックが同じであるため、過負荷機能は無効になります。これにより、Cisco ACI マルチポッド セットアップでスパイン ノードが再起動した後、コンバージェンス時間が長くなる可能性があります。値を小さくすることで、リーフ ノードは他の安定したスパイン ノードを優先して他のポッドに到達できます。
- **ISIS 再配布メトリック** 値の設定は中断されません。

COOP グループ

COOP グループ を ***厳格（Strict）*** に設定すると、Cisco ACI スイッチノードはすべての COOP 通信に MD5 認証を使用して、Cisco ACI スイッチ ノードが同じファブリック内のスイッチ間でのみ COOP データベース情報を交換できるようになります。

ベスト プラクティスは、このオプションを ***厳格（Strict）*** に設定することです。

場所

- [システム（System）] > [システム設定（System Settings ）] > [COOP グループ（COOP Group）]

オプション/注意事項

- MD5 トークンは、Cisco APIC によって 1 時間ごとに自動的に更新され、Cisco APIC によって管理されるスイッチに送信されます。

HTTPS リクエスト スロットル

管理アクセス ポリシーの [HTTPS]セクションで、[スロットル要求（Request Throttle）] パラメータを使用すると、Cisco APIC は、 HTTP GET を使用して情報をクエリし、 HTTP POST を使用して構成を変更するユーザー ソフトウェアやスクリプトなどの外部 API クライアントからの HTTPS API 要求をスロットリングできます。過剰な量の API 要求は、他のコンピュータと同様に、Cisco APIC ノードに悪影響を与える可能性があります。その結果、 API 要求だけでなく、バックエンドで API を使用する APIC GUI アクセスも遅くなったり、応答しなくなったりする可能性があります。このオプションを有効にすると、外部クライアントが Cisco APIC ノードで過剰なコンピューティング リソースを使用するのを防ぐことができます。

ベスト プラクティスは、1 秒あたり 30 リクエストでこのオプションを有効にすることです。

場所

- 6.0(2) 以前 : [ファブリック（Fabric）] > [ファブリック ポリシー（Fabric Policies）] > [ポリシー（Policies）] > [ポッド（Pod）] > [管理アクセス（Management Access）] > [デフォルト（Default）] > [ポリシー（Policies）]
- 6.0(2) 以降 : [ファブリック（Fabric）] > [ファブリック ポリシー（Fabric Policies）] > [ポリシー（Policies）] > [ポッド（Pod）] > [管理アクセス（Management Access）] > [デフォルト（Default）] > [ポリシー（Policy）] > [Web アクセス（Web Access）]

オプション/注意事項

- HTTPS リクエストスロットルの詳細については、「Cisco ACI Support for NGINX Rate Limit」を参照してください。
- 各 API リクエストに使用される時間とリソースは、その格納ファイルによって異なります。たとえば、クラスクエリは識別名（DN）クエリよりも多くのリソースを必要とします。これは、クラスクエリが同じクラスを持つオブジェクトのすべてのインスタンスを返すのに対し、DN クエリは特定の DN を持つオブジェクトの 1 つのインスタンスを返すためです。API リクエストのクエリ フィルタは、操作のコストを変更するもう 1 つの要因です。

トポロジ

APIC 接続

APIC には、 ACI リーフ ノードに接続する 2 つの物理インターフェイスがあります。APIC は、これらのインターフェイスを使用して、同じ ACI ファブリック内のすべての ACI スイッチノードおよび他の APIC と通信し、管理します。これらのインターフェイスは、各 APIC で現用系/スタンバイとして機能します。

ベスト プラクティスは、アップグレード中など、リーフ ノードの 1 つがダウンした場合でも各 APIC がファブリックに到達できるように、各 APIC に 2 つの異なるリーフ ノードを接続することです。可能な場合は、APIC クラスタのすべての APIC をリーフ ノードの異なるセットに分散します。

オプション/注意事項

- APIC 接続と APIC クラスタ設計の詳細については、 『Cisco ACI Design Guide』を参照してください。

- 各 APIC のインターフェイスを異なるスイッチに接続するという同じ原則は、APIC が IPN を介してリモートで ACI ファブリックに接続されている場合にも適用されます。このオプションの詳細については、「APIC クラスタ接続のレイヤ 3 ネットワークへの展開」を参照してください。

スイッチの接続

ACI スイッチ は、常にスパインリーフ トポロジにあります。 この基本的なトポロジは固定されていますが、リーフノードの 2 番目の階層/レイヤを使用できるマルチティアや、一部のリーフノードが IPN を介してリモートに接続されているリモートリーフなどの高度な機能で拡張できます。

ベストプラクティスは、スパイン ノードとリーフ ノード間をフルメッシュ ケーブルで接続することです。

オプション/注意事項

- 詳細については、『Cisco ACI Design Guide』 を参照してください。

Printed in USA

米国本社
Cisco Systems, Inc.
サンノゼ（カリフォルニア州）

アジア太平洋本社
Cisco Systems (USA) Pte. Ltd.
Singapore

ヨーロッパ本社
Cisco Systems International BV Amsterdam
アムステルダム（オランダ）

シスコは世界各国 200 箇所にオフィスを開設しています。住所、電話番号、ファックス番号はシスコの Web サイト https://www.cisco.com/go/offices を掲載されています。