Cisco ISE の機能をサポートするために必要なスイッチとワイヤレス LAN コントローラの設定

Cisco ISE がネットワーク スイッチと相互運用し、Cisco ISE の機能がネットワーク セグメント全体で正常に動作することを保証するには、Cisco ISE との通信に必要な NTP、RADIUS/AAA、802.1X、MAB などの設定を使用して、ネットワーク スイッチを設定する必要があります。

• MDM Interoperability のためのワイヤレス LAN コントローラでの ACL の設定 （12 ページ）

スイッチでの標準 Web 認証のサポートの有効化

認証時の URL リダイレクションのプロビジョニングなど、Cisco ISE 用の標準 Web 認証機能を有効にするには、次のコマンドをスイッチのコンフィギュレーションに含めます。

```
ip classless

ip route 0.0.0.0 0.0.0.0 10.1.2.3

ip http server
! Must enable HTTP/HTTPS for URL-redirection on port 80/443
ip http secure-server
```

代理 RADIUS トランザクション用のローカル ユーザ名とパスワードの定義

スイッチがこのネットワーク セグメントの RADIUS サーバであるかのように Cisco ISE ノードと通信するには、次のコマンドを入力します。

```
username test-radius password 0 abcde123
```

ログとアカウンティングのタイムスタンプの正確性を保証するための NTP サーバ設定

次のコマンドを入力して、**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [システム時刻（System Time）]** で Cisco ISE に設定したのと同じ NTP サーバを指定していることを確認してください。

```
ntp server <IP_address>|<domain_name>
```

AAA 機能を有効にするコマンド

802.1X および MAB 認証機能など、スイッチと Cisco ISE との間でさまざまな AAA 機能を有効にするには、次のコマンドを入力します。

```
aaa new-model
```

```
! Creates an 802.1X port-based authentication method list
aaa authentication dot1x default group radius
! Required for VLAN/ACL assignment
aaa authorization network default group radius
! Authentication & authorization for webauth transactions
aaa authorization auth-proxy default group radius
! Enables accounting for 802.1X and MAB authentications
aaa accounting dot1x default start-stop group radius
!
aaa session-id common
!
aaa accounting update periodic 5

! Update AAA accounting information periodically every 5 minutes

aaa accounting system default start-stop group radius
!
aaa server radius dynamic-author <cr>

client 10.0.56.17 server-key cisco
! Enables Cisco ISE to act as a AAA server when interacting with the client at IP address
 10.0.56.17
```

スイッチ上の RADIUS サーバの設定

Cisco ISE と相互運用し、RADIUS ソース サーバとして動作するようスイッチを設定するには、次のコマンドを入力します。

```
!
radius-server attribute 6 on-for-login-auth
! Include RADIUS attribute 8 in every Access-Request
radius-server attribute 8 include-in-access-req
! Include RADIUS attribute 25 in every Access-Request
radius-server attribute 25 access-request include
! Wait 3 x 30 seconds before marking RADIUS server as dead
```

```
radius-server dead-criteria time 30 tries 3


! Use RFC-standard ports (1812/1813)
radius-server host <Cisco_ISE_IP_address> auth-port 1812 acct-port 1813 test
 username test-radius key 0 <RADIUS-KEY>

!
radius-server vsa send accounting
!
radius-server vsa send authentication
!
! send RADIUS requests from the MANAGEMENT VLAN

ip radius source-interface <VLAN_number>
```

（注） 3回の再試行を含む30秒のデッド基準時間を設定し、Active Directoryを認証に使用するRADIUS要求に対して、より長い応答時間を提供することを推奨します。

RADIUS 許可変更（CoA）を有効にするコマンド

スイッチが RADIUS 許可変更動作を適切に処理し、Cisco ISE のポスチャ機能をサポートできるようにするための設定を指定するには、次のコマンドを入力します。

```
aaa server radius dynamic-author


client <ISE-IP> server-key 0 abcde123
```

（注） Cisco ISE では、RFC の CoA 用デフォルト ポート 3799 に対して、ポート 1700（Cisco IOS ソフトウェアのデフォルト）を使用します。既存の Cisco Secure ACS 5.x ユーザは、既存の ACS の実装の一部として CoA を使用している場合、すでにこれをポート 3799 に設定している可能性があります。

デバイス トラッキングと DHCP スヌーピングを有効にするコマンド

セキュリティに関連する Cisco ISE のオプション機能を提供できるようにするには、次のコマンドを入力することによって、デバイス トラッキングと DHCP スヌーピングを有効にし、スイッチ ポートのダイナミック ACL 内で IP 置換を実現します。

```
! Optional

ip dhcp snooping
```

```
! Required!
```

ip device tracking

RADIUS アカウンティングでは、DHCP スヌーピングが有効になっていても、DHCP 属性は IOS センサーによって Cisco ISE に送信されません。このような場合、DHCP スヌーピングを VLAN で有効にして DHCP をアクティブにする必要があります。

VLAN で DHCP スヌーピングを有効にするには、次のコマンドを使用します。

ip dhcp snooping

ip dhcp snooping vlan 1-100

（データおよび VLAN に使用する範囲を含める必要があります）

802.1X ポートベースの認証を有効にするコマンド

スイッチ ポートに対してグローバルに 802.1X 認証を有効にするには、次のコマンドを入力します。

dot1x system-auth-control

クリティカルな認証の EAP を有効にするコマンド

サプリカントによる LAN 経由での認証要求をサポートするには、次のコマンドを入力することによって、EAPをクリティカルな認証（アクセスできない認証バイパス）に対して有効にします。

dot1x critical eapol

リカバリ遅延を使用してAAA要求をスロットリングするコマンド

クリティカルな認証リカバリ イベントが発生した場合、次のコマンドを入力することによって、自動的に遅延（秒単位）を発生させるようスイッチを設定し、Cisco ISE がリカバリ後にサービスを再起動できるようにすることが可能です。

authentication critical recovery delay *1000*

適用状態に基づく VLAN の定義

ネットワーク内の既知の適用状態に基づいて VLAN 名、番号、および SVI を定義するには、次のコマンドを入力します。ネットワーク間のルーティングを有効にするには、それぞれの VLAN インターフェイスを作成します。これは特に、同じネットワーク セグメントを経由し

て渡される、複数のソースからのトラフィックを処理する場合に役立ちます。たとえば、PC とその PC がネットワークへの接続時に経由する IP 電話の両方からのトラフィックが考えられます。

```
vlan <VLAN_number>

name ACCESS!

vlan <VLAN_number>

name VOICE

!

interface <VLAN_number>

description ACCESS

ip address 10.1.2.3 255.255.255.0

ip helper-address <DHCP_Server_IP_address>

ip helper-address <Cisco_ISE_IP_address>

!

interface <VLAN_number>

description VOICE

ip address 10.2.3.4 255.255.255.0

ip helper-address <DHCP_Server_IP_address>
```

スイッチのローカル（デフォルト）ACL 定義

このような機能を古いバージョンのスイッチ（Cisco IOS ソフトウェア リリースのバージョンが 12.2(55)SE よりも前）で有効にし、Cisco ISE が認証と許可に必要なダイナミック ACL の更新を実行できるようにするには、次のコマンドを入力します。

```
ip access-list extended ACL-ALLOW

 permit ip any any

!
```

```
ip access-list extended ACL-DEFAULT
  remark DHCP
  permit udp any eq bootpc any eq bootps
  remark DNS
  permit udp any any eq domain
  remark Ping
  permit icmp any any
  remark Ping
  permit icmp any any
  remark PXE / TFTP
  permit udp any any eq tftp
  remark Allow HTTP/S to ISE and WebAuth portal
permit tcp any host <Cisco_ISE_IP_address> eq www

permit tcp any host <Cisco_ISE_IP_address> eq 443

permit tcp any host <Cisco_ISE_IP_address> eq 8443

permit tcp any host <Cisco_ISE_IP_address> eq 8905

permit udp any host <Cisco_ISE_IP_address> eq 8905

permit udp any host <Cisco_ISE_IP_address> eq 8906

permit tcp any host <Cisco_ISE_IP_address> eq 8080
```

```
permit udp any host <Cisco_ISE_IP_address> eq 9996


remark Drop all the rest
  deny ip any any log
!
! The ACL to allow URL-redirection for WebAuth
ip access-list extended ACL-WEBAUTH-REDIRECT
 permit tcp any any eq www
 permit tcp any any eq 443
```

（注） WLC でこの設定を行うと、CPU 使用率が増加し、システムが不安定になるリスクが高まります。これは IOS の問題で、Cisco ISE は悪影響を受けません。

802.1X および MAB のスイッチ ポートを有効にする

802.1X および MAB のスイッチ ポートを有効にするには、以下の手順を実行します。

ステップ 1 すべてのアクセス スイッチ ポートのコンフィギュレーション モードを開始します。
interface range FastEthernet0/1-8

ステップ 2 次のように、（トランク モードではなく）アクセス モードのスイッチ ポートを有効にします。
switchport mode access

ステップ 3 静的にアクセス VLAN を設定します。アクセス VLAN のローカル プロビジョニングを提供するこの手順は、オープン モード認証に必要となります。
switchport access <*VLAN_number*>

ステップ 4 静的に音声 VLAN を設定します。
switchport voice <*VLAN_number*>

ステップ 5 オープン モード認証を有効にします。オープンモードを使用すると、認証が完了する前に、トラフィックをデータおよび音声 VLAN 上にブリッジングできます。実稼働環境では、ポートベースの ACL を使用して不正アクセスを防ぐことを強く推奨します。
! Enables pre-auth access before AAA response; subject to port ACL
authentication open

ステップ 6 ポートベースの ACL を適用して、認証されていないエンドポイントからアクセス VLAN 上にデフォルトでどのトラフィックをブリッジングするかを決定します。最初にすべてのアクセスを許可してからポ

リシーを適用する必要があるため、ACL-ALLOW を適用して、スイッチ ポートを通過するすべてのトラフィックを許可する必要があります。すでに現時点のすべてのトラフィックを許可するデフォルトの ISE 許可を作成しましたが、この理由は、完全な可視性を実現し、既存のエンドユーザ環境にはまだ影響を与えないようにするためです。

! An ACL must be configured to prepend dACLs from AAA server.

ip access-group ACL-ALLOW in

（注） DSBU スイッチ上に Cisco IOS Release 12.2(55)SE ソフトウェアを用意する前に、RADIUS AAA サーバからのダイナミック ACL を適用するためのポート ACL が必要です。デフォルトの ACL を用意できなかった場合、割り当てられた dACL はスイッチによって無視されます。Cisco IOS Release12.2(55)SE ソフトウェアでは、デフォルトの ACL が自動的に生成および適用されます。

（注） テストの現段階では、ポートベースの 802.1X 認証を有効にし、さらに既存のネットワークへの影響を避けるために、ACL-ALLOW を使用しています。今後のテストでは、実稼働環境に必要のないトラフィックをブロックする、異なる ACL-DEFAULT を適用する予定です。

ステップ 7 マルチ認証ホスト モードを有効にします。マルチ認証は、基本的には複数ドメイン認証（MDA）のスーパーセットです。MDA では、データ ドメイン内の単一のエンドポイントだけが許可されます。マルチ認証を設定すると、音声ドメイン内では認証された単一の電話が（MDA の場合と同じように）許可されますが、データ ドメイン内では認証できるデータ デバイスの数に制限がありません。

! Allow voice + multiple endpoints on same physical access port

authentication host-mode multi-auth

（注） IP 電話の背後で複数のデータ デバイス（仮想デバイスであるかハブに接続されている物理デバイスであるかにかかわらず）を使用すると、アクセス ポートの物理リンクステート認識度が低下する可能性があります。

ステップ 8 次のように、さまざまな認証方式オプションを有効にします。

! Enable re-authentication

authentication periodic

! Enable re-authentication via RADIUS Session-Timeout

authentication timer reauthenticate server

authentication event fail action next-method

authentication event server dead action reinitialize *<VLAN_number>*

authentication event server alive action reinitialize

! IOS Flex-Auth authentication should do 802.1X then MAB

authentication order dot1x mab

authentication priority dot1x mab

ステップ 9 次のように、スイッチ ポートで 802.1X ポート制御を有効にします。

! Enables port-based authentication on the interface

authentication port-control auto

authentication violation restrict

ステップ 10 次のように、MAC 認証バイパス（MAB）を有効にします。

! Enable MAC Authentication Bypass (MAB)
mab

ステップ 11 次のように、スイッチ ポートで 802.1X を有効にします。
! Enables 802.1X authentication on the interface
dot1x pae authenticator

ステップ 12 次のように、再送信時間を 10 秒に設定します。
dot1x timeout tx-period *10*

（注） dot1x tx-period のタイムアウトは、10 秒に設定する必要があります。この値を変更する場合は、その影響を理解したうえで行ってください。

ステップ 13 次のように、PortFast 機能を有効にします。
spanning-tree portfast

EPM ロギングを有効にするコマンド

Cisco ISE の機能について発生する可能性があるトラブルシューティングや記録をサポートするには、次のように、スイッチに標準のロギング機能を設定します。

```
epm logging
```

SNMP トラップを有効にするコマンド

次のように、スイッチがこのネットワーク セグメント内の適切な VLAN を経由して、Cisco ISE から SNMP トラップ転送を受信できるようにします。

```
snmp-server community public RO


snmp-server trap-source <VLAN_number>
```

プロファイリング用の SNMP v3 クエリーを有効にするコマンド

SNMP v3 ポーリングが正常に発生し、Cisco ISE プロファイリング サービスがサポートされるように、スイッチを設定します。まず、**[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス（Network Devices）] > [追加（Add）]|[編集（Edit）] > [SNMP 設定（SNMP Settings）]** を選択して、Cisco ISE の SNMP 設定を設定します。

```
Snmp-server user <name> <group> v3 auth md5 <string> priv des <string>

snmp-server group  <group> v3 priv

snmp-server group <group> v3 priv context vlan-1
```

（注） **snmp-server group** *<group>* **v3 priv context** *vlan-1* コマンドは、コンテキストごとに設定する必要があります。**snmp show context** コマンドでは、すべてのコンテキスト情報がリストされます。

SNMP要求がタイムアウトになり、接続の問題が発生していない場合は、タイムアウト値を増加させることができます。

プロファイラによる収集を可能にするためのMAC通知トラップを有効にするコマンド

次のように、適切な MAC 通知トラップを送信するようスイッチを設定し、Cisco ISE のプロファイラ機能がネットワーク エンドポイントで情報を収集できるようにします。

```
mac address-table notification change

mac address-table notification mac-move

snmp trap mac-notification change added

snmp trap mac-notification change removed
```

スイッチ上での RADIUS Idle-timeout の設定

スイッチに RADIUS Idle-timeout を設定するには、次のコマンドを使用します。

```
Switch(config-if)# authentication timer inactivity
```

inactivity は、クライアントアクティビティが不正と見なされるまでの非アクティブ間隔を秒単位で表したものです。

Cisco ISE では、そのようなセッションの非アクティブ タイマーを適用する必要がある許可ポリシーに対して、**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[許可（Authorization）]** > **[許可プロファイル（Authorization Profiles）]** からこのオプションを有効にできます。

iOS サプリカント プロビジョニングのためのワイヤレス LAN コントローラ設定

シングル SSID の場合

同じワイヤレス アクセス ポイントで、Apple iOS ベースのデバイス（iPhone/iPad）が、ある SSID から別の SSID に切り替えることができるようにするには、「FAST SSID の変更」機能を有効にするようワイヤレス LAN コントローラ（WLC）を設定します。この機能によって、iOS ベースのデバイスがより迅速に SSID 間の切り替えを行うことができます。

デュアル SSID BYOD の場合

デュアル SSID BYOD をサポートするには、Fast SSID が有効になっている必要があります。ワイヤレス コントローラで Fast SSID Change が有効になっている場合、クライアントは SSID 間を高速で移動できます。高速 SSID が有効になっている場合、クライアント エントリがクリアされず、遅延は適用されません。Fast SSID の詳細と、Cisco WLC での Fast SSID の設定の詳細については、http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-3/config-guide/b_cg83/b_cg83_chapter_0100001.htmlを参照してください。

WLC の設定例

```
WLC (config)# FAST SSID change
```

一部の Apple iOS ベースのデバイスでは、ワイヤレス ネットワークに接続しようとすると、次のエラー メッセージが表示される場合があります。

```
ワイヤレスネットワークをスキャンできませんでした。（Could not scan for Wireless Networks.）
```

デバイス認証に影響しないため、このエラー メッセージは無視できます。

MDM Interoperability のためのワイヤレス LAN コントローラでの ACL の設定

未登録のデバイスおよび証明書プロビジョニングをリダイレクトするために許可ポリシーで使用する ACL をワイヤレス LAN コントローラで設定します。ACL は次の順序にする必要があります。

ステップ 1 サーバからクライアントへのすべての発信トラフィックを許可します。

ステップ 2 （任意）トラブルシューティングのためにクライアントからサーバへの ICMP 着信トラフィックを許可します。

ステップ 3 未登録および非準拠のデバイスが MDM エージェントをダウンロードし、コンプライアンス チェックに進むように MDM サーバへのアクセスを許可します。

ステップ 4 Web ポータルおよびサプリカント用 ISE、および証明書プロビジョニング フローに対するクライアントからサーバへのすべての着信トラフィックを許可します。

ステップ 5 名前解決のためにクライアントからサーバへの着信 DNS トラフィックを許可します。

ステップ 6 IP アドレスのためにクライアントからサーバへの着信 DHCP トラフィックを許可します。

ステップ 7 ISE へのリダイレクションのための、クライアントからサーバへの企業リソースに対するすべての着信トラフィックを（会社のポリシーに応じて）拒否します。

ステップ 8 （任意）残りのトラフィックを許可します。

例

次の例では、未登録のデバイスを BYOD フローにリダイレクトするための ACL を示しています。この例では、Cisco ISE IP アドレスは 10.35.50.165 で、社内ネットワークの IP アドレスは 192.168.0.0 および 172.16.0.0（リダイレクト用）で、MDM サーバ サブネットは 204.8.168.0 です。

図 *1*：登録されていないデバイスをリダイレクトするための *ACL*

General

Access List Name NSP-ACL

Deny Counters 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound	150720
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	ICMP	Any	Any	Any	Inbound	7227
3	Permit	0.0.0.0 / 0.0.0.0	204.8.168.0 / 255.255.255.0	Any	Any	Any	Any	Any	17626
4	Permit	0.0.0.0 / 0.0.0.0	10.35.50.165 / 255.255.255.255	Any	Any	Any	Any	Inbound	7505
5	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Inbound	2864
6	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DHCP Server	Any	Inbound	0
7	Deny	0.0.0.0 / 0.0.0.0	192.168.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	0
8	Deny	0.0.0.0 / 0.0.0.0	172.16.0.0 / 255.240.0.0	Any	Any	Any	Any	Inbound	4
9	Deny	0.0.0.0 / 0.0.0.0	10.0.0.0 / 255.0.0.0	Any	Any	Any	Any	Inbound	457
10	Deny	0.0.0.0 / 0.0.0.0	173.194.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	1256
11	Deny	0.0.0.0 / 0.0.0.0	171.68.0.0 / 255.252.0.0	Any	Any	Any	Any	Inbound	11310
12	Deny	0.0.0.0 / 0.0.0.0	171.71.181.0 / 255.255.255.0	Any	Any	Any	Any	Any	0
13	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	71819