認可変更

認可変更（CoA）は、認証、認可、およびアカウンティング（AAA）セッションの属性を、認証された後に変更するためのメカニズムを提供します。

ID ベース ネットワーキング サービスは、セッションのクエリ、再認証、および終了、ポートバウンスとポートのシャットダウン、およびサービステンプレートのアクティブ化と非アクティブ化のための認可変更（CoA）コマンドをサポートします。

- 認可変更に関する情報 （1 ページ）
- 認可変更の制約事項 （3 ページ）
- 認可変更の設定方法 （4 ページ）
- 認可変更の設定例 （5 ページ）

認可変更に関する情報

認可変更と再認証の手順

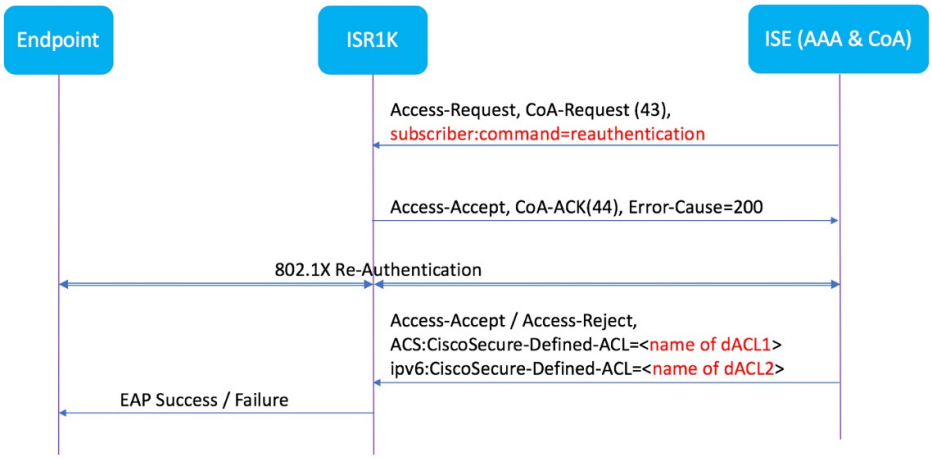
認可変更（CoA）は、認証、認可、およびアカウンティング（AAA）セッションの属性を、認証された後に変更するためのメカニズムを提供します。この手順の主なステップは次のとおりです。

- 認証
- ポスチャ アセスメント
- CoA の再認証
- ネットワーク アクセス認可

AAA でユーザー、またはユーザーグループのポリシーが変更された場合、管理者は、AAA サーバーから Cisco Identity Secure Engine（ISE）などの RADIUS CoA パケットを送信し、認証を再初期化して新しいポリシーを適用することができます。このセクションでは、使用可能な

プリミティブおよびそれらの CoA での使用方法を含む、RADIUS インターフェイスの概要について説明します。

RADIUS CoA は、AAA セッションの属性をセッション認証後に変更するためのメカニズムを提供します。RADIUS サーバーのユーザーまたはユーザーグループでポリシーが変更された場合、管理者は RADIUS サーバーから RADIUS CoA プロセスを開始して、新しいポリシーを再認証または再認可できます。



デフォルトでは、RADIUS インターフェイスがデバイスで有効になっています。ただし、次の属性については、一部の基本的な設定が必要になります。

- セキュリティとパスワード
- アカウンティング

ポスチャアセスメントが成功すると、最後のアセスメントから導出されたコンプライアンス状態に基づき、CoA 再認証コマンドによって特定のクライアントのデバイスに完全なネットワークアクセスがプッシュされます。ダウンロード可能な ACL を、対応するクライアントに対する特定のリソースへの Permit-ALL または制限付きアクセスを使用して適用するかどうかは任意です。セッションの特定、セッションの終了、ホストの再認証、ポートのシャットダウン、およびポートバウンスでは、セッションごとの CoA 要求がサポートされます。このモデルは、次のように、1 つの要求（CoA-Request）と 2 つの考えられる応答コードで構成されます。

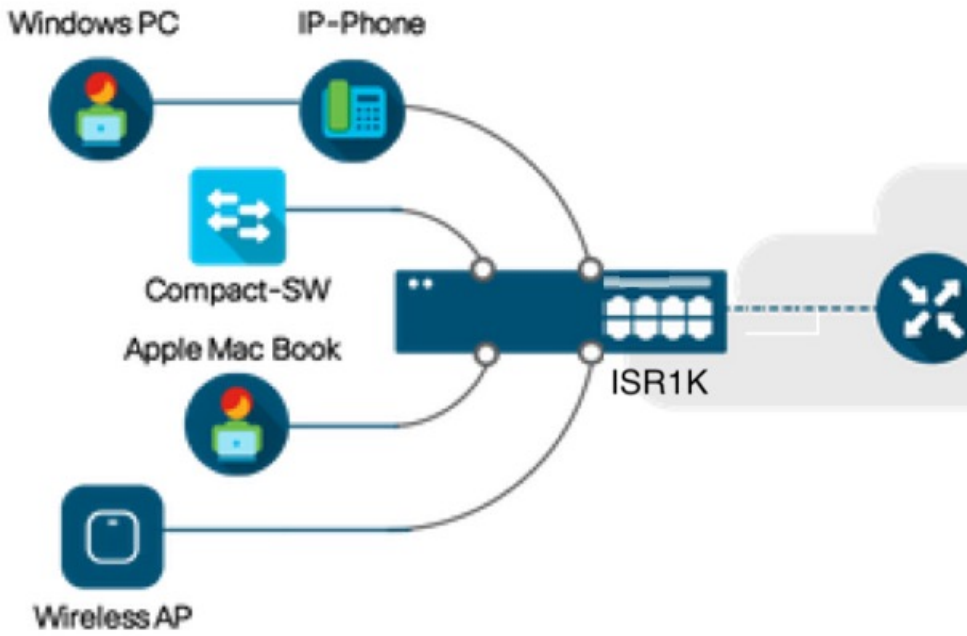
- CoA acknowledgement（ACK）[CoA-ACK]
- CoA nonacknowledgement（NAK）[CoA-NAK]

認可変更

認可変更（CoA）は、ポスチャアセスメントの結果に基づいて、エンドポイントのネットワークアクセスに対する再認証または再認可を開始するためのソリューションの重要な部分です。この機能は、Cisco AnyConnect バージョン 4.8 および Cisco ISE バージョン 2.6 と統合されています。

次のネットワークトポロジは、キャンパスまたはデータセンターに展開されたISEや他のネットワークサービスによるセキュアアクセスに使用される、ネットワーク内のブランチルータとしての一般的な Cisco 1000 シリーズ サービス統合型ルータを示しています。

図 *1 : ISE* や他のネットワークサービスによるセキュアアクセスに使用されるネットワーク内の *Cisco ISR1000*



CoAは、ポスチャアセスメントの結果に基づいて、エンドポイントのネットワークアクセスに対する再認証または再認可を開始するためのソリューションの重要な部分です。ダウンロード可能な ACL がソリューション全体のターゲット/目的です。この ACL により、クライアントごとにカスタマイズされたセキュリティポリシーが実現します。

認可変更の制約事項

- DACL およびリダイレクト ACL をサポートする TCAM があるのは 8 ポート SKU のみです。
- xACL は正確な値にのみ一致します（>、<、>=、<= はサポートされていません）。
- スイッチ ASIC TCAM が保持できるのは合計 255 エントリ（IPv4 ACL エントリ）までです。
- IPv4 オプションヘッダーはサポートされておらず、ACL パケットインスペクションでの IP フラグメントもサポートされていません。
- IPv6 はこの機能ではサポートされていません。
- ポート ACL はこの機能ではサポートされていません。

- SISF は、none-secure device-tracking（セキュリティレベル「glean」のトラッキングポリシー）のみをサポートしています。
- マルチ認証 VLAN は、Cisco 1000 シリーズ サービス統合型ルータではサポートされていません。
- トラッキングが「enable tracking」に置き換えられることはありません。
- クライアント インターフェイスで操作を複数回繰り返したことに伴い、その都度 VLAN が変更されることはありません。

認可変更の設定方法

Essential dot1x | SANet の設定

```
aaa new-model
aaa authentication dot1x default group coa-ise
aaa authorization network default group coa-ise
dot1x system-auth-control
aaa group server radius coa-ise
 server name coa
radius server coa
 address ipv4 10.10.1.10 auth-port 1812 acct-port 1813
 key cisco123
policy-map type control subscriber simple_coa
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x
interface gigabitethernet0/0/1
 switchport access vlan 22
 switchport mode access
 access-session closed
 access-session port-control auto
 dot1x pae authenticator
service-policy type control subscriber simple_coa
```

認可変更の設定

```
aaa server radius dynamic-author
 client
 server-key ******
 auth-type any
 ignore server-key
ip access-list extended redirect_acl
 20 deny udp any eq bootps any
 25 deny udp any eq domain any
 30 deny udp any any eq bootpc
 40 deny udp any eq bootpc any
 50 deny ip any host %{ise.ip}
 60 permit tcp any any eq www
 70 permit tcp any any eq 443
device-tracking tracking
```

```
device-tracking policy tracking_test
 security-level glean
 no protocol ndp
 no protocol dhcp6
 tracking enable
interface 0/0/1
 device-tracking attach-policy tracking_test
```

認可変更の設定例

例：RADIUS サーバーが稼働中かどうかの確認

```
Device# show aaa servers
RADIUS: id 1, priority 1, host 10.75.28.231, auth-port 1812, acct-port 1813, hostname
host
     State: current UP, duration 188755s, previous duration 0s
     Dead: total time 0s, count 0
     Platform State from SMD: current UP, duration 188755s, previous duration 0s
```

例：デバイス トラッキング ポリシー

```
Device# show aaa group radius coa3 **** port 1813 new-code
User successfully authenticated
USER ATTRIBUTES
username             0   "coa3"
```

パラメータが有効になっているかどうかを確認する例：

```
Device# show device-tracking policies
Target               Type  Policy               Feature        Target range
Gi0/1/1              PORT  tracking_test        Device-tracking vlan all
Gi0/1/2              PORT  tracking_test        Device-tracking vlan all
Gi0/1/3              PORT  tracking_test        Device-tracking vlan all
Gi0/1/4              PORT  tracking_test        Device-tracking vlan all
```

SISF テーブルを確認する例：

```
Device# show device-tracking database
Binding Table has 1 entries, 1 dynamic (limit 100000)
0001:MAC and LLA match     0002:Orig trunk            0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access   0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated    0100:Statically assigned
Network Address        Link Address       Interface  vlan  prlvl    age    state
Time left
ARP 10.11.22.20       0050.5683.3f97      Gi0/1/4     22    0005    11s   REACHABLE
  295 s
```

アクセスセッションが認証され、自動化されているかどうかを確認する例：

```
Device# show access-session interface gigabitEthernet 0/1/7 detail
            Interface:  GigabitEthernet0/1/7
```

```
            IIF-ID:  0x0DB9315A
       MAC Address:  b496.913d.4f9b
      IPv6 Address:  Unknown
      IPv4 Address:  10.10.22.27
         User-Name:  coa2
            Status:  Authorized
            Domain:  DATA
    Oper host mode:  multi-auth
  Oper control dir:  both
   Session timeout:  N/A
 Common Session ID:  611C4B0A00000053F483D7B0
   Acct Session ID:  Unknown
            Handle:  0x21000049
    Current Policy:  POLICY_COA
Server Policies:  Filter-ID: Filter_ID_COA2
Method status list:  Method           State
                     dot1x           Authc Success
```

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。