認可変更のサポート

Identity-Based Networking Services は、セッションのクエリー、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 RADIUS Change of Authorization（CoA）コマンドをサポートします。 このモジュールでは、Identity-Based Networking Services 用にサポートされる CoA コマンドに関する情報を提供します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を確認し、各機能がサポートされているリリースのリストを確認するには、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

CoA のサポートに関する情報

RADIUS 認可変更のサポート

Cisco IOS ソフトウェアは、RFC 5176 で定義されている RADIUS CoA の拡張をサポートします。この拡張は、一般に、外部 AAA またはポリシー サーバからのセッションのダイナミックな再構成を可能にするプッシュモデルで使用されます。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]

要求は CoA クライアント（通常は AAA またはポリシー サーバ）から開始されて、リスナーとして動作するデバイスに転送されます。

次の表は、Identity-Based Networking Services でサポートされている RADIUS CoA コマンドとベンダー固有属性（VSA）を示します。 すべての CoA コマンドには、デバイスと CoA クライアント間のセッション ID が含まれている必要があります。

表 *1*：*Identity-Based Networking Services* でサポートされている *RADIUS CoA* コマンド

CoA コマンド	**シスコの VSA**
サービスのアクティブ化	Cisco:Avpair="subscriber:command=activate-service" Cisco:Avpair="subscriber:service-name=<*service-name*>" Cisco:Avpair="subscriber:precedence=<*precedence-number*>" Cisco:Avpair="subscriber:activation-mode=replace-all"
サービスの非アクティブ化	Cisco:Avpair="subscriber:command=deactivate-service" Cisco:Avpair="subscriber:service-name=<*service-name*>"
Bounce host port	Cisco:Avpair="subscriber:command=bounce-host-port"
Disable host port	Cisco:Avpair="subscriber:command=disable-host-port"
セッション クエリー	Cisco:Avpair="subscriber:command=session-query"
セッションの再認証	Cisco:Avpair="subscriber:command=reauthenticate" Cisco:Avpair="subscriber:reauthenticate-type=last" または Cisco:Avpair="subscriber:reauthenticate-type=rerun"
セッションの終了	これは、VSA を必要としない、標準の接続解除要求です。

セッションの識別

特定のセッションに対する接続解除およびCoA要求の場合、デバイスは次の1つまたは複数の属性に基づいてセッションを検出します。

- Acct-Session-Id（IETF 属性 #44）
- Audit-Session-Id VSA（シスコの VSA）
- Calling-Station-Id（ホスト MAC アドレスを含む IETF 属性 #31）
- 次のいずれかの IPv6 属性。
  - Framed-IPv6-Prefix（IETF 属性 #97）および Framed-Interface-Id（IETF 属性 #96）。ともに RFC 3162 に従った完全な IPv6 アドレスを作成する
  - Framed-IPv6-Address
- プレーン IP アドレス（IETF 属性 #8）

メッセージに複数のセッションID属性が含まれる場合は、すべての属性がセッションと一致する必要があります。一致しない場合、デバイスは、エラー コードが「Invalid Attribute Value」の Disconnect-NAK または CoA-NAK を返します。

特定の適用ポリシーを対象とする CoA 要求の場合、上記のセッション ID 属性のいずれかがメッセージに含まれていると、デバイスはエラー コードが「Invalid Attribute Value」のCoA-NAK を返します。

CoA サービスのアクティブ化コマンド

CoA サービスのアクティブ化コマンドを使用して、セッションでサービス テンプレートをアクティブ化することができます。 AAA サーバは次の VSA を使用して、標準の CoA 要求メッセージで要求を送信します。

Cisco:Avpair="subscriber:command=activate-service"

Cisco:Avpair="subscriber:service-name=<*service-name*>"

Cisco:Avpair="subscriber:precedence=<*precedence-number*>"

Cisco:Avpair="subscriber:activation-mode=replace-all"

このコマンドはセッション指向であるため、「セッションの識別, （3 ページ）」セクションに示されている 1 つ以上のセッション ID 属性とともに使用する必要があります。 デバイスがセッションを検出できない場合、デバイスは「Session Context Not Found」エラー コード属性を含む CoA-NAK メッセージを返します。 デバイスは、セッションを検出すると、ホスティング ポートに対するテンプレートのアクティブ化の操作を開始し、CoA-ACK が返されます。 テンプレートのアクティブ化が失敗すると、エラーコード属性が適切なメッセージに設定されたCoA-NAKメッセージが返されます。

デバイスが CoA-ACK をクライアントに返す前にデバイスに障害が発生した場合、クライアントから要求が再送信されると、新しいアクティブデバイス上でそのプロセスが繰り返されます。デバイスが CoA-ACK メッセージをクライアントに返した後でデバイスに障害が発生したが、操作が完了していない場合、その操作は新しいアクティブ デバイスで再開されます。

CoA サービスの非アクティブ化コマンド

CoA サービスの非アクティブ化コマンドを使用して、セッションでサービス テンプレートを非アクティブ化することができます。 AAA サーバは次の VSA を使用して、標準の CoA 要求メッセージで要求を送信します。

Cisco:Avpair="subscriber:command=deactivate-service"

Cisco:Avpair="subscriber:service-name=<*service-name*>"

このコマンドはセッション指向であるため、「セッションの識別, （3 ページ）」セクションに示されている 1 つ以上のセッション ID 属性とともに使用する必要があります。 デバイスがセッションを検出できない場合、デバイスは「Session Context Not Found」エラー コード属性を含む CoA-NAK メッセージを返します。 デバイスは、セッションを検出すると、ホスティング ポートに対するテンプレートの非アクティブ化操作を開始し、CoA-ACK が返されます。 テンプレートの非アクティブ化が失敗すると、エラー コード属性が該当するメッセージに設定された CoA-NAK メッセージが返されます。

デバイスが CoA-ACK をクライアントに返す前にデバイスに障害が発生した場合、クライアントから要求が再送信されると、新しいアクティブデバイス上でそのプロセスが繰り返されます。デバイスが CoA-ACK メッセージをクライアントに返した後でデバイスに障害が発生したが、操作が完了していない場合、その操作は新しいアクティブ デバイスで再開されます。

CoA ホスト ポートのバウンス コマンド

CoA ホスト ポートのバウンス コマンドはセッションを終了し、ポート をバウンスします（リンク ダウン イベントに続いてリンク アップ イベントを開始します）。 AAA サーバは、次の VSA を含む標準の CoA 要求メッセージで要求を送信します。

Cisco:Avpair="subscriber:command=bounce-host-port"

このコマンドはセッション指向であるため、「セッションの識別, （3 ページ）」セクションに示されている 1 つ以上のセッション ID 属性とともに使用する必要があります。 セッションが見つからない場合、デバイスは「Session Context Not Found」エラー コード属性を使用して CoA-NAK メッセージを返します。 セッションが見つかった場合、デバイスはホスティング ポートを 10 秒間ディセーブルにし、再びイネーブルにして（ポート バウンス）、CoA-ACK を返します。

デバイスが CoA-ACK をクライアントに返す前にデバイスに障害が発生した場合、クライアントから要求が再送信されると、新しいアクティブデバイス上でそのプロセスが繰り返されます。デバイスが CoA-ACK メッセージをクライアントに返した後でデバイスに障害が発生したが、操作が完了していない場合、その操作は新しいアクティブ デバイスで再開されます。

CoA ポートのバウンス コマンドは、エンドポイントが承認の変更後に新しい IP アドレスを取得する必要があり、これが DHCP プロセスを再開するようエンドポイントに示す唯一の手段である

場合の最後の手段として役立ちます。 この状況は、VLAN が変更されており、この認証ポートに関する変化を検出するメカニズムがないデバイス（プリンタなど）がエンドポイントの場合に発生する可能性があります。このコマンドによって、認証ポートでリンク フラップが発生する場合があり、これにより、このポートに接続されている 1 つ以上のホストから DHCP 再ネゴシエーションがトリガされます。

CoA ホスト ポートのディセーブル化コマンド

CoA ホスト ポートのディセーブル化コマンドは、セッションをホスティングしている認証ポートを管理上の理由でシャット ダウンします。これにより、セッションは終了します。 AAA サーバは、次の VSA を含む標準の CoA 要求メッセージで要求を送信します。

Cisco:Avpair="subscriber:command=disable-host-port"

このコマンドはセッション指向であるため、「セッションの識別, （3 ページ）」セクションに示されている 1 つ以上のセッション ID 属性とともに使用する必要があります。 セッションを検出できない場合、デバイスは「Session Context Not Found」エラー コード属性を含む CoA-NAK メッセージを返します。 デバイスは、セッションを検出すると、ホスティング ポートを無効にし、CoA-ACK メッセージを返します。

デバイスが CoA-ACK をクライアントに返す前にデバイスに障害が発生した場合、クライアントから要求が再送信されると、新しいアクティブデバイス上でそのプロセスが繰り返されます。デバイスが CoA-ACK メッセージをクライアントに返した後でデバイスに障害が発生したが、操作が完了していない場合、その操作は新しいアクティブ デバイスで再開されます。

CoA セッション クエリー コマンド

CoA セッション クエリー コマンドは、加入者セッションに関するサービス情報を要求します。AAA サーバは次の VSA を含む標準の CoA 要求メッセージで要求を送信します。

Cisco:Avpair="subscriber:command=session-query"

このコマンドはセッション指向であるため、「セッションの識別, （3 ページ）」セクションに示されている 1 つ以上のセッション ID 属性とともに使用する必要があります。 デバイスがセッションを検出できない場合、デバイスは「Session Context Not Found」エラー コード属性を含む CoA-NAK メッセージを返します。 デバイスは、セッションを検出すると、セッションに対してセッション クエリー操作を実行し、CoA-ACK メッセージを返します。

デバイスが CoA-ACK をクライアントに返す前にデバイスに障害が発生した場合、クライアントから要求が再送信されると、新しいアクティブデバイス上でそのプロセスが繰り返されます。デバイスが CoA-ACK メッセージをクライアントに返した後でデバイスに障害が発生したが、操作が完了していない場合、その操作は新しいアクティブ デバイスで再開されます。

CoA セッションの再認証コマンド

セッションの認証を開始するために、AAA サーバは次の VSA を含む標準の CoA 要求メッセージを送信します。

Cisco:Avpair="subscriber:command=reauthenticate"

Cisco:Avpair="subscriber:reauthenticate-type=<last | rerun>"

「reauthenticate-type」は、CoA 再認証要求が、該当のセッションで最後に成功した認証方式を使用するか、認証プロセス全体を再実行するかどうかを指定します。

次のルールが適用されます。

- 「subscriber:command=reauthenticate」は、再認証をトリガーするために必要です。
- 「subscriber:reauthenticate-type」が指定されていない場合、デフォルトの動作は該当のセッションで最後に成功した認証方式の再実行です。この方式での再認証が成功すると、すべての古い承認データが、再認証された承認データで置き換えられます。
- 「subscriber:reauthenticate-type」が有効なのは、「subscriber:command=reauthenticate」とともに使用されている場合のみです。別の CoA コマンドに含まれている場合、この VSA は暗黙的に無視されます。

デバイスが CoA-ACK をクライアントに返す前にデバイスに障害が発生した場合、クライアントから要求が再送信されると、新しいアクティブデバイス上でそのプロセスが繰り返されます。デバイスが CoA-ACK メッセージをクライアントに返した後でデバイスに障害が発生したが、操作が完了していない場合、その操作は新しいアクティブ デバイスで再開されます。

CoA セッションの終了コマンド

CoA 接続解除要求コマンドは、ホスト ポートをディセーブルにせずにセッションを終了します。このコマンドによって、指定したホストのオーセンティケータ ステートマシンが再初期化されますが、ホストのネットワークへのアクセスは制限されません。セッションが見つからない場合、デバイスは「Session Context Not Found」エラー コード属性を使用して Disconnect-NAK メッセージを返します。セッションが見つかった場合、デバイスはセッションを終了します。セッションが完全に削除されると、デバイスは Disconnect-ACK を返します。

デバイスが CoA-ACK をクライアントに返す前にデバイスに障害が発生した場合、クライアントから要求が再送信されると、新しいアクティブ デバイス上でそのプロセスが繰り返されます。

ホストのネットワークへのアクセスを制限するには、
Cisco:Avpair="subscriber:command=disable-host-port" VSA を含む CoA 要求を使用します。このコマンドは、ホストがネットワーク上で問題を起こしていることを把握し、ホストのネットワーク アクセスを即座にブロックする必要がある場合に便利です。ポートのネットワーク アクセスを復元する場合は、非 RADIUS メカニズムを使用して再びイネーブルにします。

その他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
Identity-Based Networking Services コマンド	『Cisco IOS Identity-Based Networking Services Command Reference』
アドレス解決プロトコル（ARP）コマンド	『Cisco IOS IP Addressing Services Command Reference』
ARP 設定作業	『*IP Addressing - ARP Configuration Guide*』
認証、許可、およびアカウンティング（AAA）の設定作業	『*Authentication Authorization and Accounting Configuration Guide*』
AAA コマンド	『*Cisco IOS Security Command Reference*』

標準および RFC

標準/RFC	Title
RFC 5176	『*Dynamic Authorization Extensions to RADIUS*』

テクニカル サポート

説明	Link
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

CoA サポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。 その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *2* : *CoA* サポートの機能情報

機能名	リリース	機能情報
『Change of Authorization』	Cisco IOS XE Release 3.2SE	次を開始する CoA 要求がサポートされています。 • セッションでのサービス テンプレートのアクティブ化および非アクティブ化 • ポート バウンス • ポートのシャットダウン • セッションのクエリー • セッション再認証 • セッションの終了 これらの VSA は、AAA サーバからの標準 CoA 要求メッセージで送信されます。