RADIUS 認可変更

この章は、次の項で構成されています。

aaa server radius dynamic-author

ダイナミック認証ローカルサーバーコンフィギュレーションモードを開始し、認可変更（CoA）クライアントおよびパラメータを設定するには、aaa server radius dynamic-author グローバル コンフィギュレーション モード コマンドを使用します。

構文

aaa server radius dynamic-author

パラメータ

このコマンドには引数またはキーワードはありません。

コマンド モード

グローバル コンフィギュレーション モード

ユーザ ガイドライン

ダイナミック認証を使用すると、外部ポリシーサーバーは、PoD（パケットオブディスコネクト）またはCoA（認可変更）要求を介してデバイスに更新を動的に送信できます。このコマンドを設定すると、ダイナミック認証ローカル サーバー コンフィギュレーション モードが開始されます。このモードでは、ダイナミック RADIUS 関連のコマンド（client address や key など）を設定できます。

例

次に、ダイナミック認証ローカル サーバー コンフィギュレーション モード コンテキストを開始する例を示します。

```
Switch010203(config)# aaa server radius dynamic-author
Switch010203(config-locsvr-da-radius)#
```

attribute event-timestamp drop-packet

Event-Timestamp 属性を含まないパケットオブディスコネクト（POD）要求または認可変更（CoA）要求を破棄するようにデバイスを設定するには、ダイナミック認証ローカル サーバー コンフィギュレーション モードで attribute event-timestamp drop-packet コマンドを使用します。デフォルト設定に戻すには、このコマンドの no 形式を使用します。

構文

attribute event-timestamp drop-packet

no attribute event-timestamp drop-packet

パラメータ

このコマンドにはパラメータはありません。

デフォルト設定

デバイスは、event-timestamp 属性が含まれていない場合でも、PoD または CoA 要求を破棄しません。

コマンド モード

ダイナミック認証サーバ コンフィギュレーション（config-locsvr-da-radius）

使用上のガイドライン

Event-Timestamp（RADIUS 属性 55 - [RFC2869]）は、要求が最新であるかどうかを確認するためにスイッチによって使用されます。要求が最新でない場合は、通知なしで破棄されます（RFC 5176）。CoA クライアントがこの属性を送信することは必須ではありません。CoA セキュリティを強化するには、attribute event-timestamp drop-packet コマンドを使用して、Event-Timestamp RADIUS 属性を含まない PoD または CoA 要求を破棄します。

例

次に、Event-Timestamp RADIUS 属性を含まない PoD または CoA 要求を破棄するようにデバイスを設定する例を示します。

```
Switch010203(config)# aaa server radius dynamic-author
Switch010203(config-locsvr-da-radius)# attribute event-timestamp drop-packet
```

authentication command bounce-port ignore

RADIUS 認可変更（CoA）bounce port コマンドを無視するようにデバイスを設定するには、グローバル コンフィギュレーション モードで authentication command bounce-port ignore コマンドを使用します。デフォルトステータスに戻すには、このコマンドの no 形式を使用します。

構文

authentication command bounce-port ignore

no authentication command bounce-port ignore

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルト設定

デバイスは RADIUS CoA bounce port コマンドを受け入れます。

コマンド モード

グローバル コンフィギュレーション モード

ユーザ ガイドライン

これにより、このポートに接続されている 1 つまたは複数のホストから DHCP 再ネゴシエーションがトリガーされます。この状況は、VLAN の変更があり、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。authentication command bounce-port ignore コマンドは、RADIUS CoA bounce port コマンドを無視するようにデバイスを設定し、認証ポートに接続されているホストでリンクフラップが発生しないようにします。

例

次に、CoA bounce port コマンドを無視するようにデバイスを設定する例を示します。

```
Switch010203(config)# authentication command bounce-port ignore
```

authentication command disable-port ignore

RADIUS 認可変更（CoA）disable-port コマンドを無視するようにデバイスを設定するには、グローバル コンフィギュレーション モードで authentication command disable-port ignore コマンドを使用します。デフォルトステータスに戻すには、このコマンドの no 形式を使用します。

構文

authentication command disable-port ignore

no authentication command bounce-port ignore

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルト設定

デバイスは、RADIUS CoA disable port コマンドを受け入れます。

コマンド モード

グローバル コンフィギュレーション モード

ユーザ ガイドライン

RADIUS CoA disable port コマンドを実行すると、セッションをホストしている認証ポートが管理的にシャットダウンされます。その結果、セッションは終了します。authentication command disable-port ignore コマンドを使用して、認証ポートおよびこの認証ポート上の他のホストが切断されないように、RADIUS CoA disable port コマンドを無視するようにデバイスを設定します。

例

例 1

次に、CoA disable port コマンドを無視するようにデバイスを設定する例を示します。

```
Switch010203(config)# authentication command disable-port ignore
```

クライアント

デバイスが認可変更（CoA）要求および切断要求を受け入れるRADIUSクライアントを指定するには、ダイナミック認証ローカル サーバー コンフィギュレーション モードで client コマンドを使用します。クライアントを削除するには、このコマンドの no 形式を使用します。

構文

client *ip-address***s** *[***server-key** *key-string*]

encrypted client *ip-address* **server-key** *encrypted-key-string*

no client *ip-address*

パラメータ

- *ip-address*：CoA クライアントのホスト IP アドレスを指定します。IP アドレスは、IPv4、IPv6、または IPv6z アドレスを使用できます。
- **server-key** *key-string*：（オプション）デバイスと CoA クライアント間で共有される RADIUS キーを設定します（範囲：0 ～ 128 文字）。空の文字列を指定するには、"" と入力します。
- **server-key** *encrypted-key-string*：key-string パラメータと同じですが、キーは暗号化された形式です。

デフォルト設定

CoA クライアントはデバイスで設定されていません。

コマンド モード

ダイナミック認証サーバ コンフィギュレーション（config-locsvr-da-radius）

使用上のガイドライン

外部ポリシーサーバー（このコマンドで設定）がデバイスに更新を動的に送信できるようにするには、client コマンドを使用します。この機能は CoA RADIUS 拡張により可能になりました。CoA によりピアツーピア機能が RADIUS に導入されました。この機能により、デバイスと外部ポリシーサーバーがそれぞれ CoA サーバーとクライアントとして動作できます。デバイスがサーバーとして機能する CoA クライアントを指定するには、client コマンドを使用します。

デバイスと指定した CoA クライアント間の RADIUS 通信用のキーを指定するには、オプションの server-key パラメータを使用します。このキーは、CoA クライアントが使用するキーと一致する必要があります。空の文字列を指定するには、"" と入力します。このパラメータを省略すると、グローバル CoA キー（server-key コマンド）が使用されます。グローバルキーが設定されていない場合、デバイスと CoA クライアント間の RADIUS 交換は失敗します。

ignore server-key コマンドが設定されている場合、キーの不一致がある場合やキーが設定されていない場合でも、デバイスと CoA クライアント間の RADIUS 交換は成功します。

例

例 1

次の例では、IP アドレス 1.1.1.1 の CoA クライアントがサーバーキー「key1」で追加されます。

```
Switch010203(config)# aaa server radius dynamic-author
Switch010203(config-locsvr-da-radius)# client 1.1.1.1 server-key key1
```

例 2

次の例では、クライアントサーバーキーを設定せずに、IP アドレス 2.2.2.2 の CoA クライアントを追加します。この場合、グローバルサーバーキー（設定されている場合）が使用されます。

```
Switch010203(config)# aaa server radius dynamic-author
Switch010203(config-locsvr-da-radius)# client 2.2.2.2
```

domain delimiter

受信した PoD および CoA 要求のユーザー名ドメインデリミタを設定するには、ダイナミック認証ローカル サーバー コンフィギュレーション モードで domain delimiter コマンドを使用します。デフォルトデリミタに戻るには、このコマンドの no 形式を使用します。

構文

domain delimiter *character*

no domain delimiter

パラメータ

- delimiter character：ドメインデリミタを指定します。次のオプションのいずれかを指定できます。@、/、$、%、\、#、または -

コマンド モード

ダイナミック認証サーバ コンフィギュレーション（config-locsvr-da-radius）

デフォルト設定

デフォルトのデリミタは @ 文字です。

使用上のガイドライン

domain delimiter コマンドを使用して、AAA または 802.1x ユーザーセッションの完全なユーザー名をストリッピングするときに使用するデリミタを設定し、パケットオブディスコネクト（POD）または認可変更（CoA）要求のパケットで指定されるユーザー名と比較します。完全なユーザー名のドメイン セクション ストリッピングの詳細については、domain delimiter コマンドを参照してください。

例

例 1

次の例では、$ 文字がデリミタとして設定されています。

```
Switch010203(config)# aaa server radius dynamic-author
Switch010203(config-locsvr-da-radius)# domain delimiter $
```

domain stripping

受信した PoD および CoA 要求のユーザー名ドメインストリッピングの動作を有効にして定義するには、ダイナミック認証ローカル サーバー コンフィギュレーション モードで domain stripping コマンドを使用します。デフォルト設定に戻すには、このコマンドの no 形式を使用します。

構文

domain stripping [right-to-left]

no domain stripping

パラメータ

stripping：着信のユーザー名と、ドメインデリミタの左側にある名前を比較します。

stripping [right-to-left]（オプション）：右から左方向に見て最初のデリミタで文字列を終了します。

コマンド モード

ダイナミック認証サーバ コンフィギュレーション（config-locsvr-da-radius）

デフォルト設定

ストリッピングはデフォルトでは無効になっています。ストリッピングのデフォルト方向は左から右です。

使用上のガイドライン

domain stripping コマンドを使用すると、domain delimiter コマンドで設定されたデリミタに基づいたユーザー名ドメインストリッピングが有効になります。ドメインストリッピングで着信のユーザー名と、@ ドメインデリミタの左側にある名前を比較できます。

ドメインストリッピングを設定すると、@ ドメインデリミタ（またはコマンド domain delimiter を使用して設定された他のデリミタ）の前に存在するユーザー名のみを使用して切断メッセージを送信できます。これにより、スイッチは、このユーザー名を可能性のあるドメインを持つスイッチ上の任意のセッションユーザー名と比較し、照合します。たとえば、ドメインストリッピングが設定されていて、ユーザー名「test」を使用してパケットオブディスコネクト（POD）要求または認可変更（CoA）要求を送信すると、PoD/CoA メッセージとデバイスセッションユーザー名の比較が行われ、ユーザー名「test@example.com」または「test」が指定されたセッションがユーザー名「test」と一致します。

ドメインストリッピングが設定されていない場合（デフォルトの動作）、PoD および COA 要求で指定されたユーザー名は、デバイスのアクティブセッションに含まれる完全なユーザー名と比較されます。

right-to-left キーワードを使用すると、右から左方向に見て最初のデリミタでユーザー名文字列を終了するように指定します。

例

例 1：

次の例では、$ 文字がデリミタとして設定され、デリミタの左側でストリッピングが実行されます。この場合、セッションユーザー名が user1$my_users であると、PoD または CoA 要求で一致するユーザー名は「user1」です。

```
Switch010203(config)# aaa server radius dynamic-author
Switch010203(config-locsvr-da-radius)# domain delimiter $
Switch010203(config-locsvr-da-radius)# domain stripping
```

例 2：

次の例では、デフォルトのデリミタ @ を使用して、右から左方向に見て最初のデリミタの左でストリッピングが実行されます。ここでは、セッションユーザー名が user1@test.com@example.com の場合、PoD または CoA 要求で一致するユーザー名は「user1@test.com」です。

```
Switch010203(config)# aaa server radius dynamic-author
Switch010203(config-locsvr-da-radius)# domain stripping right-to-left
```

ignore server-key

CoA サーバーキーを無視するようにデバイスを設定するには、ダイナミック認証ローカル サーバー コンフィギュレーション モードで ignore server-key コマンドを使用します。デフォルト設定に戻すには、このコマンドの no 形式を使用します。

構文

ignore server-key

no ignore server-key

デフォルト設定

サーバーキーは無視されません。

コマンド モード

ダイナミック認証ローカル サーバー コンフィギュレーション（config-locsvr-da-radius）

使用上のガイドライン

PoD または CoA 要求で送信されたサーバーキーを無視するようにデバイスを設定するには、ignore server-key コマンドを使用します。サーバーキーが無視されると、CoA サーバーキーがデバイスで設定されていない場合（client または server-key コマンド）、またはデバイスで設定されたキーが PoD または CoA 要求で指定されたキーと一致しない場合でも、CoA クライアントとの RADIUS 交換は成功します。

デフォルトの動作では、サーバーキーは無視されません。つまり、キーの不一致が発生した場合、または CoA クライアントにキーが設定されていない場合、PoD または CoA 要求は破棄されます。

例

例 1：

次に、サーバーキーを無視するようにデバイスを設定する例を示します。

```
Switch010203(config)# aaa server radius dynamic-author
Switch010203(config-locsvr-da-radius)# ignore server-key
```

port

デバイスが設定されている CoA クライアントからの認可変更（CoA）要求およびパケットオブディスコネクト（PoD）要求をリッスンするポートを指定するには、ダイナミック認証ローカル サーバー コンフィギュレーション モードで port コマンドを使用します。デフォルト設定に戻すには、このコマンドの no 形式を使用します。

構文

port udp-port

no port

パラメータ

- *udp-port*：認証要求用の UDP ポート番号を指定します。（範囲：0 ～ 59,999）

デフォルト設定

デバイスは、UDP ポート 1700 で CoA および PoD 要求をリッスンします。

コマンド モード

ダイナミック認証サーバ コンフィギュレーション（config-locsvr-da-radius）

使用上のガイドライン

デバイスが CoA クライアントからの要求をリッスンするポートを指定するには、port コマンドを使用します。この設定は、すべての CoA クライアントからの RADIUS PoD または CoA 要求に適用されます。ポート番号が 0 に設定されている場合、CoA クライアントが設定されていても、PoD および CoA 要求はドロップされます。

例

例 1：

次の例では、デバイスが RADIUS PoD および CoA 要求をリッスンするポートとしてポート 1648 が指定されます。

```
Switch010203(config)# aaa server radius dynamic-author
Switch010203(config-locsvr-da-radius)# port 1648
```

server-key

デバイスと CoA の間で共有されるデフォルトの RADIUS キーを設定するには、ダイナミック認証ローカル サーバー コンフィギュレーション モードで server-key コマンドを使用します。設定を削除するには、このコマンドの no 形式を使用します。

構文

server-key *key-string*

encrypted server-key *encrypted-key-string*

no server key

パラメータ

- *key-string*：デバイスと CoA クライアントのサーバー間のすべての RADIUS 通信に認証および暗号キーを指定します（範囲：0 ～ 128 文字）。PoD または CoA 要求で指定されるキーは、このキーと一致する必要があります。空の文字列を指定するには、"" と入力します。
- *encrypted-key-string*：key-string パラメータと同じですが、キーは暗号化された形式です。

デフォルト設定

デフォルトサーバーキーは設定されていません。

コマンド モード

ダイナミック認証サーバ コンフィギュレーション（config-locsvr-da-radius）

使用上のガイドライン

デバイスと CoA クライアント間の通信で使用するデフォルトの RADIUS キーを定義するには、server-key コマンドを使用します。このキーは、特定のクライアントキー（client コマンド）で設定されていないクライアントによって使用されます。

このキーは、CoA クライアントが使用するキーと一致する必要があります。空の文字列を指定するには、"" と入力します。

ignore server-key コマンドが設定されている場合、キーの不一致がある場合やキーが設定されていない場合でも、デバイスと CoA クライアント間の RADIUS 交換は成功します。

例

例 1：

次の例では、デフォルトのサーバーキー「key123」が設定されます。

```
Switch010203(config)# aaa server radius dynamic-author
Switch010203(config-locsvr-da-radius)# server-key key123
```

show aaa clients

AAA（CoA）クライアントの統計情報を表示するには、show aaa clients 特権 EXEC モードコマンドを使用します。

- ip-address（オプション）：特定の CoA クライアントホストの統計情報を表示します。IP アドレスは、IPv4、IPv6、または IPv6z アドレスを使用できます。

デフォルト設定

デフォルトでは、すべての CoA ホストの統計情報が表示されます。

コマンド モード

特権 EXEC モード

例

```
Switch010203# show aaa clients

Dynamic Author Client 1.1.1.1
CoA: requests: 0, transactions: 0
retransmissions: 0, active transactions: 0
Ack responses: 0, Nak reponses: 0
invalid requests: 0, errors: 0
PoD: requests: 0, transactions: 0
retransmissions: 0, active transactions: 0
Ack responses: 0, Nak reponses: 0
invalid requests: 0, errors: 0
Average Ack response time: 0 msec

Dynamic Author Client 2.2.2.2
CoA: requests: 0, transactions: 0
retransmissions: 0, active transactions: 0
Ack responses: 0, Nak reponses: 0
invalid requests: 0, errors: 0
PoD: requests: 0, transactions: 0
retransmissions: 0, active transactions: 0
Ack responses: 0, Nak reponses: 0
invalid requests: 0, errors: 0
Average Ack response time: 0 msec

Details of counters displayed:
1. Requests – Counts the Requests received from CoA clients
2. transactions – Counts CoA completed transactions. A Completed transaction occurs once
 the Switch send an ACK or NAK in response to a Request from a CoA client.
3. Retransmissions – Counts received retransmitted CoA Requests. A retransmitted CoA
Requests is a Request in which the Request identifier is identical to the identifier of
 a previous Request.
4. active transactions – Transactions that are currently active. An active transaction
is a transaction in which a Request from a COA Client has been received but an ACK or
NAK response has not been sent yet. Once an ACK or NAK is sent this counter is decremented.
5. Ack responses - Counts the number of Ack responses sent by the switch.
6. Nak responses - Counts the number of Nak responses sent by the switch
7. invalid requests – Counts invalid requests received by the switch. An invalid request
 is one of the following
    a) A Request in which the secret in the Request does not match the Secret configured
 on the device,
```

```
    b) A Request with no session identifier
    c) A Request with an unsupported attribute
    d) A Request in which a supported attribute is empty
    e) A Request which is discarded because the event-timestamp is not current, or if
event-timestamp is mandatory and received request does not include this attribute
    f) A Request with a not current or missing Event-Timestamp attribute
    g) A request received with “disable port” or “bounce port” command that are dropped
 due to user configuration.
8. errors – Counts errors. an error can be an internal error in which a request cannot
be processed due to resource issue, or if a secret has not been configured for the CoA
client
9. Average Ack response time – in milliseconds
```

show aaa server radius dynamic-author

CoA 設定を表示するには、show aaa server radius dynamic-author 特権 EXEC モードコマンドを使用します。

構文

show aaa server radius dynamic-author *[ip-address]*

パラメータ

ip-address：表示する CoA クライアントホストの IP アドレスを指定します。IP アドレスは、IPv4、IPv6、または IPv6z アドレスを使用できます。

コマンド モード

特権 EXEC モード

デフォルト設定

デフォルトでは、コマンドは設定されているすべての CoA クライアントの情報を表示します。

例

例 1

```
Switch010203# show aaa server radius dynamic-author
CoA UDP port: 1700
Default Server-Key MD5: 9aa6e5f2256c17d2d430b100032b997c
Ignore Server-Key: disabled
Domain delimiter: @
Domain stripping: disabled
“disable port” command: process
“bounce port” command: process
Event-Timestamp attribute drop packet: disabled
```

CoA Client Address	Server-Key's MD5
1.1.1.1	02cea75e335fcb814cd81932f1c15dc2
1111::1100	デフォルト

例 2

```
Switch010203# show aaa server radius dynamic-author
CoA UDP port: 1968
Default Server-Key MD5: Not configured
Ignore Server-Key: enabled Domain delimiter: $
Domain stripping: enabled (left to right) “disable port” command: ignore
“bounce port” command: process
Event-Timestamp attribute drop packet: enabled
```

CoA Client Address	Server-Key's MD5
1.1.1.1	02cea75e335fcb814cd81932f1c15dc2
1111::1100	デフォルト

例 3

```
Switch010203# show aaa server radius dynamic-author 1.1.1.1
CoA UDP port: 1977
Default Key MD5: Not configured
Ignore Server-Key: enabled Domain delimiter: $
Domain stripping: enabled (left to right)
“disable port” command: process
“bounce port” command: ignore
Event-Timestamp attribute drop packet: disabled
```

CoA Client Address	Server-Key's MD5
1.1.1.1	02cea75e335fcb814cd81932f1c15dc2

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。