set aggressive-mode client-endpoint から show content-scan まで

show aaa servers

AAA サーバ MIB によって解釈される、すべてのパブリックおよびプライベート認証、許可、アカウンティング（AAA）RADIUS サーバとの間で送受信されるパケットのステータスと数を表示するには、ユーザ EXEC または特権 EXEC モードで **show aaa servers** コマンドを使用します。

show aaa servers [**private**| **public**]

構文の説明

private	（任意）プライベート AAA サーバのみを表示します。AAA サーバ MIB によっても表示されます。
public	（任意）パブリック AAA サーバのみを表示します。AAA サーバ MIB によっても表示されます。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更内容
12.2(6)T	このコマンドが導入されました。
12.3(7)T	このコマンドが、Cisco IOS Release 12.3(7)T に統合されました。
12.2(33)SRE	このコマンドが、Cisco IOS Release 12.2(33)SRE に統合されました。
15.1(1)S	このコマンドが変更されました。 CISCO-AAA-SERVER-MIB のプライベート RADIUS サーバのサポートが追加されました。
15.1(4)M	このコマンドが変更されました。 CISCO-AAA-SERVER-MIB のプライベート RADIUS サーバのサポートが追加されました。
15.2(4)S1	このコマンドが変更されました。 コマンド出力に、未処理の、およびスロットルされたトランザクション（アクセスとアカウンティング）を概算で表示するサポートが追加されました。

使用上のガイドライン

show aaa servers コマンドでは、RADIUS サーバのみがサポートされます。

コマンドは、すべての AAA トランザクション タイプ（認証、許可、アカウンティング）で送受信されたパケットに関する情報を表示します。

例

次に、**show aaa servers private** コマンドの出力例を示します。 表示の最初の 4 行のみがプライベート RADIUS サーバの状態に関係するため、表示のこの部分の出力フィールドを次の表で説明します。

```
Router# show aaa servers private

RADIUS: id 24, priority 1, host 172.31.164.120, auth-port 1645, acct-port 1646
     State: current UP, duration 375742s, previous duration 0s
     Dead: total time 0s, count 0
     Quarantined: No
     Authen: request 5, timeouts 1, failover 0, retransmission 1
             Response: accept 4, reject 0, challenge 0
             Response: unexpected 0, server error 0, incorrect 0, time 14ms
             Transaction: success 4, failure 0
             Throttled: transaction 0, timeout 0, failure 0
     Author: request 0, timeouts 0, failover 0, retransmission 0
             Response: accept 0, reject 0, challenge 0
             Response: unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction: success 0, failure 0
             Throttled: transaction 0, timeout 0, failure 0
     Account: request 5, timeouts 0, failover 0, retransmission 0
             Request: start 3, interim 0, stop 2
             Response: start 3, interim 0, stop 2
             Response: unexpected 0, server error 0, incorrect 0, time 12ms
             Transaction: success 5, failure 0
             Throttled: transaction 0, timeout 0, failure 0
     Elapsed time since counters last cleared: 4d8h22m
     Estimated Outstanding Access Transactions: 0
     Estimated Outstanding Accounting Transactions: 0
     Estimated Throttled Access Transactions: 0
     Estimated Throttled Accounting Transactions: 0
     Maximum Throttled Transactions: access 0, accounting 0
     Requests per minute past 24 hours:
             high - 8 hours, 22 minutes ago: 0
             low  - 8 hours, 22 minutes ago: 0
             average: 0
```

下の表で、この出力で表示される重要なフィールドについて説明しています。

表 *1*：*show aaa servers* のフィールドの説明

フィールド	説明
id	ルータに定義されているすべての AAA サーバの固有識別子。
priority	グループ内サーバの使用順序。
host	プライベート RADIUS サーバ ホストの IP アドレス。
auth-port	認証と許可要求に使用する AAA サーバの UDP 宛先ポート。 デフォルト値は 1645 です。

フィールド	説明
acct-port	アカウンティング要求に使用する AAA サーバの UDP 宛先ポート。 デフォルト値は 1646 です。
State	AAA サーバの現在の状態、同サーバがその状態を続けている時間（秒単位）、および同サーバが以前の状態を続けていた時間（秒単位）を示します。 次の状態が示されます。 • DEAD：サーバが現在ダウンしていること、およびフェールオーバーの際に同サーバがグループ内で最後に残ったサーバでなければ省略されることを示します。 • duration：サーバが現在の状態（UP または DEAD のいずれか）であると見なされる時間。 • previous duration：サーバが以前の状態にあったと見なされる時間。 • UP：サーバが現在稼働していると見なされ、そのサーバとの通信が試みられることを示します。
Dead	サーバが稼働していないとマークされた回数と、その状態にある時間を累積して秒単位で表します。

フィールド	説明
Authen	

フィールド	説明
	サーバと送受信した認証パケット、および成功または失敗した認証トランザクションに関する情報を提供します。 このフィールドでは、次の情報が報告されます。 • request：AAA サーバに送信された認証要求の数。 • timeouts：このサーバへの送信があった際に確認されたタイムアウト（応答なし）の数。 • Response：このサーバで確認された応答に関する統計情報。次のレポートが含まれます。 • unexpected：予期しない応答の数。 パケットのタイムアウト期間の期限を過ぎた後で受信された応答は、予期しないものと見なされます。 たとえば、サーバへのリンクが混雑している場合などに発生します。また、サーバが明確な理由なく応答を生成した場合も、予期しない応答が作成される場合があります。 • server error：サーバ エラーの数。 このカテゴリは、前のカテゴリのいずれにも当てはまらないエラー パケットの「キャッチオール」です。 • incorrect：不正な応答の数。 応答の形式が、プロトコルが予測するもの以外の不正な形式であれば、不正な応答と見なされます。 不正なサーバ キーがルータに設定されている場合に発生の可能性が高くなります。 • time：認証パケットに応答するために要した時間（ミリ秒単位）。 • Transaction：これらのフィールドは、サーバに関連する認証、許可、アカウンティング トランザクションに関する情報を提供します。 トランザクションは、AAA モジュール、または AAA クライアント (PPP

フィールド	説明
	など) によって AAA プロトコル (RADIUS またはTACACS+) に送信される認証情報、許可情報、またはアカウンティング情報の要求として定義されます。この場合、複数のパケット送信および再送信が行われる場合があります。 トランザクションでは、成功または失敗を確認するために 1 つのサーバグループ内の 1 つまたは複数のサーバへのパケット再送信が必要な場合があります。 成功または失敗は、RADIUS およびTACACS+プロトコルによって、次のように AAA に報告されます • success：トランザクションが成功すると増加します。 • failure：サーバグループの別のサーバへのパケット再送信が失敗または成功しなかった場合など、トランザクションが失敗すると増加します。 アクセス拒否など、アクセス要求に対する否定的な応答は、トランザクションの成功として見なされます。
Author	このカテゴリのフィールドは、Authen: フィールドと似ています。 ただし、作成者情報が RADIUS プロトコルの認証パケットで送信されるため、RADIUS を使用する場合これらのフィールドは増加しない点が大きく異なります。
Account	このカテゴリのフィールドは Authen: フィールドと似ていますが、アカウンティング トランザクションとパケットの統計情報を提供する点で異なります。
Elapsed time since counters last cleared	カウンタが最後にクリアされてから経過した日数、時間数、および分数を表示します。

（注） Intelligent Services Gateway（ISG）の場合、推定未完了アカウンティング トランザクションはゼロになるまでに時間がかかります。 これは、中間アカウンティング要求に常にチャーンがあるためです。

show aaa servers コマンド出力のフィールドは、Cisco AAA-SERVER-MIB の簡易ネットワーク管理プロトコル（SNMP）オブジェクトにマッピングされ、SNMP レポートで使用されます。 **show aaa servers** コマンドの出力例の最初の行（RADIUS: id 24, priority 1, host 172.31.164.120, auth-port 1645, acct-port 1646）は、次のように Cisco AAA-SERVER-MIB にマッピングされます。

- id は casIndex へマップ
- priority は casPriority へマップ
- host は casAddress へマップ
- auth-port は casAuthenPort へマップ
- acct-port maps は casAcctPort へマップ

Cisco AAA-SERVER-MIB マップにリストされている次のオブジェクトのセットを、**show aaa servers** コマンドで表示されるフィールドにマップすることは、より簡単です。たとえば、casAuthenRequests フィールドは、レポートの Authen: request 部分に対応し、casAuthenRequestTimeouts はレポートの Authen: timeouts 部分に対応します。以下も同様です。

- casAuthenRequests
- casAuthenRequestTimeouts
- casAuthenUnexpectedResponses
- casAuthenServerErrorResponses
- casAuthenIncorrectResponses
- casAuthenResponseTime
- casAuthenTransactionSuccesses
- casAuthenTransactionFailures
- casAuthorRequests
- casAuthorRequestTimeouts
- casAuthorUnexpectedResponses
- casAuthorServerErrorResponses
- casAuthorIncorrectResponses
- casAuthorResponseTime
- casAuthorTransactionSuccesses
- casAuthorTransactionFailures
- casAcctRequests

- casAcctRequestTimeouts
- casAcctUnexpectedResponses
- casAcctServerErrorResponses
- casAcctIncorrectResponses
- casAcctResponseTime
- casAcctTransactionSuccesses
- casAcctTransactionFailures
- casState
- casCurrentStateDuration
- casPreviousStateDuration
- casTotalDeadTime
- casDeadCount

選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を検索およびダウンロードするには、http://www.cisco.com/go/mibs にある MIB Locator を使用してください。

関連コマンド

コマンド	説明
radius-server dead-criteria	一方または両方の基準値（RADIUS サーバを停止状態としてマーキングするために使用）を、指定の定数値に強制的に設定します。
server-private	特定のプライベート RADIUS サーバを定義済みのサーバ グループに関連付けます。

show access-lists

現在のアクセス リストの内容を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show access-lists** コマンドを使用します。

show access-lists [*access-list-number*| *access-list-name*]

構文の説明

access-list-number	（任意）表示するアクセス リストの数です。デフォルトでは、システムによりすべてのアクセス リストが表示されます。
access-list-name	（任意）表示する IP アクセス リストの名前です。

コマンド デフォルト

システムは、すべてのアクセス リストを表示します。

コマンド モード

ユーザ EXEC 特権 EXEC

コマンド履歴

リリース	変更内容
10.0	このコマンドが導入されました。
12.0(6)S	出力でコンパイルされた ACL を識別できるように変更されました。
12.1(1)E	このコマンドが Cisco 7200 シリーズに実装されました。
12.1(5)T	コマンド出力でコンパイルされた ACL を識別できるように変更されました。
12.1(4)E	このコマンドが Cisco 7100 シリーズに実装されました。
12.2(2)T	コマンド出力に IPv6 アクセス リストの情報が表示されるように変更されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。

リリース	変更内容
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の12.2SXリリースにおけるサポートは、フィーチャ セット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。

使用上のガイドライン

show access-lists コマンドは、ルータで動作している現在の ACL を表示するために使用します。高速化された ACL として動作している各アクセス リストには、Compiled 表示を使用してフラグが付けられます。

この表示には、ACL 内の各エントリと一致したパケットの数も示されるため、ユーザは、許可または拒否された特定のパケットをモニタすることができます。 また、このコマンドは、アクセス リストがコンパイルされたアクセス リストとして実行されているかどうかも示します。

例

次は、アクセス リスト 101 が指定されている場合の、**show access-lists** コマンドの出力例を示します。

```
Router# show access-lists 101
Extended IP access list 101
    permit tcp host 198.92.32.130 any established (4304 matches) check=5
    permit udp host 198.92.32.130 any eq domain (129 matches)
    permit icmp host 198.92.32.130 any
    permit tcp host 198.92.32.130 host 171.69.2.141 gt 1023
    permit tcp host 198.92.32.130 host 171.69.2.135 eq smtp (2 matches)
    permit tcp host 198.92.32.130 host 198.92.30.32 eq smtp
    permit tcp host 198.92.32.130 host 171.69.108.33 eq smtp
    permit udp host 198.92.32.130 host 171.68.225.190 eq syslog
    permit udp host 198.92.32.130 host 171.68.225.126 eq syslog
    deny   ip 150.136.0.0 0.0.255.255 224.0.0.0 15.255.255.255
    deny   ip 171.68.0.0 0.1.255.255 224.0.0.0 15.255.255.255 (2 matches) check=1
    deny   ip 172.24.24.0 0.0.1.255 224.0.0.0 15.255.255.255
    deny   ip 192.82.152.0 0.0.0.255 224.0.0.0 15.255.255.255
    deny   ip 192.122.173.0 0.0.0.255 224.0.0.0 15.255.255.255
    deny   ip 192.122.174.0 0.0.0.255 224.0.0.0 15.255.255.255
    deny   ip 192.135.239.0 0.0.0.255 224.0.0.0 15.255.255.255
    deny   ip 192.135.240.0 0.0.7.255 224.0.0.0 15.255.255.255
    deny   ip 192.135.248.0 0.0.3.255 224.0.0.0 15.255.255.255
```

アクセス リスト カウンタは、アクセス リストの各行により、何個のパケットが許可されたかをカウントします。 この数字は一致した数として表示されます。 Check は、1 つのパケットがアクセス リストと比較され、一致しなかった回数を意味します。

次に、Turbo Access Control List（ACL）機能が次のアクセス リストすべてで設定されているときの show access-lists コマンドの出力例を示します。

（注） show access-lists コマンドによって表示される許可および拒否の情報は、access-list コマンドを使用して入力した順序と同じではない可能性があります。

```
Router# show access-lists
```

```
Standard IP access list 1 (Compiled)
    deny   any
Standard IP access list 2 (Compiled)
    deny   192.168.0.0, wildcard bits 0.0.0.255
    permit any
Standard IP access list 3 (Compiled)
    deny   0.0.0.0
    deny   192.168.0.1, wildcard bits 0.0.0.255
    permit any
Standard IP access list 4 (Compiled)
    permit 0.0.0.0
    permit 192.168.0.2, wildcard bits 0.0.0.255
```

次に、ネットワークで IPv6 が設定されている場合に、IPv6 アクセス リストの情報を表示する、**show access-lists** コマンドの出力例を示します。

```
Router# show access-lists
IPv6 access list list2
     deny ipv6 FEC0:0:0:2::/64 any sequence 10
     permit ipv6 any any sequence 20
```

関連コマンド

コマンド	説明
access-list（IP 拡張）	拡張 IP アクセス リストを定義します。
access-list（IP 標準）	標準 IP アクセス リストを定義します。
clear access-list counters	アクセス リストのカウンタをクリアします。
clear access-template	ダイナミック アクセス リストから一時アクセス リストのエントリを手動でクリアします。
ip access-list	IP アクセス リストを名前で定義します。
show ip access-lists	現在のすべての IP アクセス リストの内容を表示します。
show ipv6 access-list	現在のすべての IPv6 アクセス リストの内容を表示します。

show authentication interface

特定のインターフェイスの認証マネージャに関する情報を表示するには、特権 EXEC モードで **show authentication interface** コマンドを使用します。

show authentication interface *type number*

構文の説明

type	インターフェイス タイプ。 詳細については、疑問符（?）オンライン ヘルプ機能を使用します。
number	インターフェイス番号を指定します。 ネットワーキングデバイスに対する番号付け構文の詳細については、疑問符（?）のオンライン ヘルプ機能を使用してください。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
12.2(33)SXI	このコマンドが導入されました。
15.2(2)T	このコマンドが、Cisco IOS Release 15.2(2)T に統合されました。

使用上のガイドライン

show authentication interface コマンドを使用して、特定のインターフェイスの認証マネージャに関する情報を表示します。

例

次に、**show authentication interface** コマンドの出力例を示します。

```
Switch# show authentication interface g1/0/23
Client list:
  MAC Address     Domain   Status         Handle      Interface
  000e.84af.59bd  DATA     Authz Success  0xE0000000  GigabitEthernet1/0/23
Available methods list:
  Handle  Priority  Name
  3        0        dot1x
Runnable methods list:
```

```
  Handle  Priority  Name
  3        0        dot1x
```

下の表で、この出力で表示される重要なフィールドについて説明しています。 その他のフィールドは説明がなくても理解できます。

表 *2*：*show authentication interface* のフィールドの説明

フィールド	説明
MAC Address	クライアントの MAC アドレス。
Domain	クライアントのドメイン（DATA または VOICE）。
Status	認証セッションのステータス。 次の値が可能です。 • Authc Failed：このセッションで認証方式が実行され、認証は失敗しました。 • Authc Success：このセッションで認証方式が実行され、認証は成功しました。 • Authz Failed：機能が失敗し、セッションが終了しました。 • Authz Success：すべての機能がセッションに適用され、セッションがアクティブです。 • Idle：このセッションは初期化されていますが、認証方式が実行されませんでした。これは中間の状態です。 • No methods：このセッションの結果を出した認証方式はありません。 • Running：このセッションの認証方式が実行中です。
Interface	認証インターフェイスのタイプと番号。
Available methods list	インターフェイスで使用できる認証方式のサマリー情報。
Runnable methods list	インターフェイスで実行できる認証方式のサマリー情報。

関連コマンド

コマンド	説明
show authentication registrations	認証マネージャに登録されている認証方式に関する情報を表示します。
show authentication sessions	現在の認証マネージャ セッションに関する情報を表示します。

show authentication registrations

認証マネージャに登録されている認証方式に関する情報を表示するには、特権 EXEC モードで **show authentication registrations** コマンドを使用します。

show authentication registrations

構文の説明

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

特権 EXEC（#）

コマンド履歴

リリース	変更内容
12.2(33)SXI	このコマンドが導入されました。
15.2(2)T	このコマンドが、Cisco IOS Release 15.2(2)T に統合されました。

使用上のガイドライン

show authentication re gistrations コマンドを使用して、認証マネージャに登録されているすべての方式に関する情報を表示します。

例

次に、show authentication registrations コマンドの出力例を示します。

```
Switch# show authentication registrations
Auth Methods registered with the Auth Manager:
   Handle   Priority   Name
     3         0       dot1x
     2         1       mab
     1         2       webauth
```

下の表で、この出力で表示される重要なフィールドについて説明しています。

表 *3* : *show authentication registrations* のフィールドの説明

フィールド	説明
Priority	方式のプライオリティ。 **authentication priority** コマンドを使用して認証方式のプライオリティが設定されていない場合、デフォルトのプライオリティが表示されます。最高から最低までのデフォルトは dot1x、mab、および webauth です。
Name	認証方式の名前。 値は、dot1x、mab、および webauth です。

関連コマンド

コマンド	説明
show authentication interface	特定のインターフェイスの認証マネージャに関する情報を表示します。
show authentication sessions	現在の認証マネージャ セッションに関する情報を表示します。

show authentication sessions

現在の認証マネージャ セッションに関する情報を表示するには、特権 EXEC モードで **show authentication sessions** コマンドを使用します。

（注） Cisco IOS Release 12.2(33)SXI から、**show dot1x** コマンドは **show authentication sessions** コマンドで補完されます。 **show dot1x** コマンドは 802.1X 認証方式の使用に固有の出力を表示するために予約されています。 **show authentication sessions** コマンドは、すべての認証方式と許可機能の情報を表示します。

Cisco IOS XE Release 3SE and Later Releases

show authentication sessions [**[database]**| [**handle** *handle-number*| **interface** *type number*| **mac** *mac-address*| **method** *method-name* [**interface** *type number*]| **session-id** *session-id*]] **[details]**

All Other Releases

show authentication sessions [**handle** *handle-number*| **interface** *type number*| **mac** *mac-address*| **method** *method-name* **interface** *type number*| **session-id** *session-id*]

構文の説明

database	（任意）セッション データベースに保存されたセッション データを表示します。 このキーワードを使用することで、内部にキャッシュされた VLAN ID などの情報を表示できます。 セッションデータベースに格納されているデータが内部にキャッシュされたデータと一致しない場合は、警告メッセージが表示されます。
handle *handle-id*	（任意）認証マネージャ情報を表示する特定のハンドルを指定します。
interface *type number*	（任意）認証マネージャ情報を表示する特定のインターフェイスのタイプおよび番号を指定します。 インターフェイスに対する有効なキーワードおよび引数を表示するには、疑問符（?）によるオンライン ヘルプ機能を使用します。
mac *mac-address*	（任意）情報を表示する特定の MAC アドレスを指定します。

method *method-name*	（任意）認証マネージャ情報を表示する特定の認証方式を指定します。 有効な方式は次のいずれかです。 • **dot1x**：IEEE 802.1X 認証方式。 • **mab**：MAC 認証バイパス（MAB）方式。 • **webauth**：Web 認証方式。 方式を指定する場合は、インターフェイスも指定できます。
session-id *session-id*	（任意）認証マネージャ情報を表示する特定のセッションを指定します。
details	（任意）セッションに関する 1 行のサマリーを表示する代わりに、各セッションの詳細情報を表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
12.2(33)SXH	このコマンドがサポートされるようになりました。
12.2(33)SXI	このコマンドは、**handle** *handle* キーワードおよび引数を追加して出力に情報を追加するために変更されました。
15.2(2)T	このコマンドが、Cisco IOS Release 15.2(2)T に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが変更されました。 **database** キーワードと **details** キーワードが追加されました。

使用上のガイドライン

show authentication sessions コマンドを使用して、現在の認証マネージャ セッションすべてに関する情報を表示します。 特定の認証マネージャ セッションに関する情報を表示するには、1 つ以上のキーワードを使用します。

例

次に、スイッチ上のすべての認証セッションを表示する例を示します。

```
Device# show authentication sessions

Interface  MAC Address     Method   Domain   Status         Session ID
Gi1/48     0015.63b0.f676  dot1x    DATA     Authz Success  0A3462B1000000102983C05C
Gi1/5      000f.23c4.a401  mab      DATA     Authz Success  0A3462B10000000D24F80B58
Gi1/5      0014.bf5d.d26d  dot1x    DATA     Authz Success  0A3462B10000000E29811B94
```

次に、インターフェイス上のすべての認証セッションを表示する例を示します。

```
Device# show authentication sessions interface gigabitethernet2/47

Interface:  GigabitEthernet2/47
          MAC Address:  Unknown
           IP Address:  Unknown
               Status:  Authz Success
               Domain:  DATA
       Oper host mode:  multi-host
     Oper control dir:  both
        Authorized By:  Guest Vlan
          Vlan Policy:  20
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A3462C8000000000002763C
      Acct Session ID:  0x00000002
               Handle:  0x25000000
Runnable methods list:
       Method   State
       mab      Failed over
       dot1x    Failed over
----------------------------------------
            Interface:  GigabitEthernet2/47
          MAC Address:  0005.5e7c.da05
           IP Address:  Unknown
            User-Name:  00055e7cda05
               Status:  Authz Success
               Domain:  VOICE
       Oper host mode:  multi-domain
     Oper control dir:  both
        Authorized By:  Authentication Server
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A3462C8000000010002A238
      Acct Session ID:  0x00000003
               Handle:  0x91000001
Runnable methods list:
       Method   State
       mab      Authc Success
       dot1x    Not run
```

次に、指定したセッション ID の認証セッションを表示する例を示します。

```
Device# show authentication sessions session-id 0B0101C70000004F2ED55218

            Interface:  GigabitEthernet9/2
          MAC Address:  0000.0000.0011
           IP Address:  20.0.0.7
             Username:  johndoe
               Status:  Authz Success
               Domain:  DATA
       Oper host mode:  multi-host
     Oper control dir:  both
        Authorized By:  Critical Auth
          Vlan policy:  N/A
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0B0101C70000004F2ED55218
```

```
      Acct Session ID:  0x00000003
               Handle:  0x91000001
Runnable methods list:
       Method   State
       mab      Authc Success
       dot1x    Not run
```

次に、指定した認証方式によって許可されたすべてのクライアントを表示する例を示します。

```
Device# show authentication sessions method mab

No Auth Manager contexts match supplied criteria

Device# show authentication sessions method dot1x

Interface  MAC Address     Domain   Status         Session ID
Gi9/2      0000.0000.0011  DATA     Authz Success  0B0101C70000004F2ED55218
```

下の表で、この出力で表示される重要なフィールドについて説明します。

表 *4*：*show authentication sessions* のフィールドの説明

フィールド	説明
Interface	認証インターフェイスのタイプと番号。
MAC Address	クライアントの MAC アドレス。
Domain	ドメインの名前（DATA または VOICE）。
Status	認証セッションのステータス。 次の値が可能です。 • Authc Failed：このセッションで認証方式が実行され、認証は失敗しました。 • Authc Success：このセッションで認証方式が実行され、認証は成功しました。 • Authz Failed：機能が失敗し、セッションが終了しました。 • Authz Success：すべての機能がセッションに適用され、セッションがアクティブです。 • Idle：このセッションは初期化されていますが、認証方式が実行されませんでした。これは中間の状態です。 • No methods：このセッションの結果を出した認証方式はありません。 • Running：このセッションの認証方式が実行中です。

フィールド	説明
Handle	コンテキストのハンドル。
State	レポートされた認証セッションの動作状態。 次の値が可能です。 • Not run：このセッションの方式が実行されませんでした。 • Running：このセッションの方式が実行中です。 • Failed over：この方式が失敗し、次の方式で結果を提供すると想定されています。 • Success：この方式は、セッションの成功した認証結果を提供しました。 • Authc Failed：この方式は、セッションの失敗した認証結果を提供しました。

関連コマンド

コマンド	説明
show access-sessions	セッション対応ネットワーキングセッションに関する情報を表示します。
show authentication registrations	認証マネージャに登録されている認証方式に関する情報を表示します。
show authentication statistics	認証マネージャセッションの統計情報を表示します。
show dot1x	802.1X 認証方式の使用に固有のアイデンティティ プロファイルの詳細を表示します。