CHAPTER 6

セキュリティに関する問題のトラブルシューティング

Cisco Nexus 5000 シリーズ NX-OS は、意図的な攻撃または意図しない深刻な間違いに起因する性能低下や障害、データの損失や損傷からネットワークを保護するセキュリティを提供します。

この章では、Cisco Nexus 5000 シリーズ スイッチでセキュリティに関連して発生する問題を特定し、解決する方法について説明します。

この章で説明する内容は、次のとおりです。

ロール

ユーザがログインするとロールの割り当てに失敗する

RBAC の観点から見たとき、ユーザがログインするとロールの割り当てに失敗します。

考えられる原因

TACAC+ サーバまたは RADIUS サーバで AV-Pair が適切に設定されていません。

解決方法

次の手順を実行して、ロールの割り当てを完了します。

ステップ 1 TACACS+ サーバ（ACS サーバなど）の設定を確認します。

- 次のメニュー パスを使用して、該当の設定にアクセスします。

  [Interface Configuration] > [TACACS+ (Cisco IOS)]

  - シェル（exec）の [User] ボックスを確認します。
  - Advanced TACACS+ Features を確認します。

  選択したサービスごとに、カスタマイズした TACACS 属性を詳細な設定オプションに入力するウィンドウを表示します。
- 次のメニュー パスを使用して該当の設定にアクセスし、シェル属性にストリングを追加します。

  [User Setup] >[Add/Edit "admin"] > [TACACS+ Settings]

  - シェル属性とカスタム属性のボックスを確認します。

- テキストボックスに次のストリングを追加します。

  cisco-av-pair=shell:roles="network-admin"

ステップ 2　RADIUS サーバ（ACS サーバなど）の設定を確認します。

- 次のメニュー パスを使用して該当の設定にアクセスします。

  [Network Configuration] > [AAA] > [AAA Servers] > [svi,20.1.1.2,CiscoSecure ACS]

  [Network Configuration] > [AAA] > [AAA Client] > [20.1.1.1 20.1.1.1 RADIUS (Cisco IOS/PIX 6.0)] > [SharedSecret=test1234, Authenticate Using=RADIUS (Cisco IOS/PIX 6.0)]

  [Interface Configuration] > [RADIUS (Cisco IOS/PIX 6.0)]

  - cisco-av-pair の [User] を確認します。
- 次のメニュー パスを使用して該当の設定にアクセスし、RADIUS 属性にストリングを追加します。

  [User Setup] > [Add/Edit <username>] > [Cisco IOS/PIX 6.x RADIUS Attributes]

  - 属性のボックスを確認します。
  - 次のストリングを入力します。

    shell:roles="network-admin"

ステップ 3　ユーザ アカウントで指定されている RADIUS サーバ（RADIUSD サーバなど）の設定を確認します。

- 次のパスを使用してユーザ アカウントの定義にアクセスします。

  .../etc/raddb
- ユーザ アカウントの定義に次の内容があることを確認します。

  cisco-avpair= "shell: roles = network-admin"

ステップ 4　このユーザで再度ログインします。

ステップ 5　「show user-account」コマンドを使用して、ロールの割り当てを確認します。

ロールの許可 / 拒否のアクションを指定するルールが正しく機能しない

ユーザ定義のロールをユーザ アカウントに割り当てると、そのロールのルール ポリシーが機能していないように見えます。たとえば、ロール設定のルールで、すべてのインターフェイス コンフィギュレーション コマンドを拒否するように設定したとします。それでも、ユーザはインターフェイスのコマンドを引き続き設定できます。

考えられる原因

ロールでのルール設定の順序が正しくありません。

（注）　RBAC パーサは、ルール番号が大きいルールから順番にアクセスします。

解決方法

正しく機能していないルールを特定し、そのルールよりも前の順番にあるルールの中に、このルールと矛盾するものやこのルールを無効にするものがないか確認します。

たとえば、正しく機能しないルールのルール ID が 10 である場合は、ルール ID が 11 以上のルールをすべて調べ、ルール 10 と矛盾するものがないか確認します。この例として、ルール 15 によってルール 10 が無効になっていることがわかったとします。この矛盾を解決するには、ルール 15 を修正するか、ルール 10 のルール ID を 16 以上の値に変更する必要があります。

ロールのインターフェイスまたは VLAN のポリシーが正しく機能していないように見える

ユーザ定義のロールをユーザ アカウントに割り当てて、特定のインターフェイスへのアクセスが拒否されるようにそのロールのインターフェイスまたは VLAN のポリシーを設定しても、そのユーザ アカウントで「show」コマンドを使用すると、アクセスが拒否されるはずのインターフェイスまたは VLAN の設定、ステータス、指定内容、または統計を引き続き表示できます。

考えられる原因

そのインターフェイスまたは VLAN のロールのポリシーを、ユーザが「show interface brief」や「show vlan」などの CLI コマンドを使用して確認しています。

解決方法

RBAC は、コマンドを表示するときのフィルタ処理には対応していません。インターフェイスや VLAN のロールのポリシーは、コンフィギュレーション コマンドまたは操作コマンドのみに適用されます。

考えられる原因

ユーザがロールに適切に割り当てられていません。

解決方法

- 「show user-account」コマンドを使用して、そのユーザへのロール割り当てを確認します。
- 「show role name <name>」コマンドを使用してロール定義を確認します。

1 人のユーザに複数のロールを割り当てると、正しく機能していないように見える

1 つのユーザ アカウントを複数のロールに割り当てて、あるコマンドへのアクセスが拒否されるようにそのいずれかのロールで設定していても、ユーザはそのコマンドにアクセスできます。その結果、複数のロールではコマンド パーサが機能していないように見えます。

考えられる原因

1 つのユーザ アカウントに割り当てた複数のロールは順番に解析されるとユーザが想定している可能性があります。

解決方法

NXOS の設計上、複数のロールは、結合して許可する機能で解析されます。たとえば、各コマンドはすべてのロールで検証され、比較されます。

いずれかのロールで許可されているコマンドをユーザが使用すれば、CLI で操作を継続できます。

たとえば、「interface eth1/1」コマンドがロールで許可されていれば、ユーザは CLI からインターフェイス eth1/1 のコンフィギュレーション モードに入ることができます。

各ロールは、それぞれのポリシー（インターフェイス、VLAN、VSAN など）を他のロールに関係なく適用します。この例のように、あるロールで eth1/1 を拒否するインターフェイス ポリシーを設定していると、そのロールではこのコマンドは拒否されますが、別のインターフェイス ポリシーを持つロールが他に存在し、そこでは同じインターフェイスが許可されていることが考えられます。

ロール設定の変更が適用されない

ユーザ アカウントをロールに割り当てた後、そのユーザが Nexus 5000 にログインしていると、そのロール設定のどのような変更もそのユーザにすぐには適用されません。

考えられる原因

ロール A に割り当てたユーザ アカウントにユーザがログインしているときに管理者がロール A を変更していますが、その管理者はロール A に対する変更がログイン中のユーザにただちに適用されると想定しています。しかし、そのユーザはロールに適切に割り当てられていません。

解決方法

NXOS では、ロール設定の変更がリアルタイムではアクティブになりません。つまり、ユーザが次にログインしたときに、新しいロールに対する設定の変更が初めて有効になります。

機能グループの削除が CLI で拒否される

管理者が「no role feature-group name <group-name>」コマンドを使用して機能グループを削除しようとすると CLI で拒否されます。

考えられる原因

その機能グループが使用中であることが CLI エラーで示されています。つまり、この機能グループを指定しているロール設定が存在します。

解決方法

このエラーを解決するには、次の手順を実行します。

- 「show role | egrep Role:|feature-group」コマンドを使用して、このロールにどの機能グループが関連付けられているか、またどのロールの下にどの機能グループが存在しているかを表示します。
- ロール コンフィギュレーション モードで「no rule」コマンドを使用して、該当の関連付けを解除します。続いて機能グループを削除します。

AAA

TACACS+ 認証や RADIUS 認証でユーザがログインできない

サーバグループを Nexus 5000 向けに適切に設定し、TACACS+ サーバまたは RADIUS サーバでサーバグループに「aaa authentication login default」設定を割り当てると、Telnet/SSH ログインで次のエラーが発生してユーザを認証できません。

「%TACACS-3-TACACS_ERROR_MESSAGE: All servers failed to respond」

考えられる原因

サーバにアクセスするための正しい VRF で AAA グループが設定されていません。

解決方法

次の手順を実行してログインをイネーブルにします。

- 「show running-config aaa」コマンドと「show aaa authentication」コマンドを使用して、どの AAA グループが認証に使用されているかを確認します。

- TACACS+ では、「show tacacs-server groups」コマンドと「show running-config tacacs+」コマンドを使用して、その AAA グループと VRF との関連付けを確認します。
- RADIUS+ では、「show radius-server groups」コマンドと「show running-config radius」コマンドを使用して、その AAA グループと VRF との関連付けを確認します。
- VRF の関連付けを修正し、「test aaa group <name> <username> <password>」コマンドを使用して VRF 設定をテストします。
- 「test aaa」コマンドを実行すると「user has failed authentication」というエラーが返る場合、サーバはアクセス可能ですが、このユーザアカウントのクレデンシャルが正しくありません。サーバ上のユーザ設定が正しいかどうかを確認します。

考えられる原因

ネットワーク上で AAA サーバがアクセス不能になっています。

解決方法

VRF の関連付けとユーザ アカウントのクレデンシャルを修正しても問題が解決しない場合は、次の手順を実行します。

- 「test aaa」コマンドを実行すると「error authenticating to server」というエラーが返る場合は、設定上でサーバへのルートが欠落している可能性があります。AAA サーバをデフォルトの VRF に関連付けている場合は、「ping <server>」コマンドを使用します。AAA サーバを VRF 管理に関連付けている場合は、「ping <server> vrf management」コマンドを使用します。
- メッセージ「No route to host」が表示される場合は、サーバへのスタティック ルートが適切に設定されていません。該当の VRF コンテキストで IP ルートを設定し直します。
- 再度、「ping <server>」コマンドを入力します。このコマンドを正常に実行できた場合は、「test aaa group <name> <username> <password>」コマンドを使用します。
- 「ping <server>」コマンドを正常に実行できない場合は、ネットワークの接続を確認します。たとえば、「show ip arp [vrf management]」コマンドでネクストホップ ルータの ARP エントリが表示されるかどうか、Nexus 5000 の ARP エントリがネクストホップ ルータの ARP テーブルに存在するかどうかなどを確認します。

Wireshark でパケットの内容をデコードできない

AAA パケットはネットワークからキャプチャできますが、そのパケットの内容を Wireshark でデコードできません。

考えられる原因

ホスト キーがイネーブルとなっているときは、AAA パケットが暗号化されています。

解決方法

次の手順を実行してパケットの内容をデコードします。

- 「no tacacs-server」コマンドを使用して TACACS サーバの設定を削除します。
- どのキーも指定せずに TACACS サーバを再設定します。
- ACS の [Network Configuration] ページで、ホスト キーを削除して、Nexus 5000 向けに AAA クライアントを再設定します。
- もう一度傍受を実行します。キャプチャしたパケットは暗号化されていないので、Wireshark でデータの内容を正しくデコードできます。

- パケットをキャプチャした後、セキュリティを損なわないように、管理者がホスト キーの設定を元に戻す必要があります。

ユーザがログインするとロールの割り当てに失敗する

ユーザがログインすると、ロールの割り当てに失敗します（Nexus 5000 自身の AAA から見た場合）。

考えられる原因

ACS または TACACS+/RADIUS のシスコ属性値（av）ペアが正しく設定されていると仮定すると、ユーザログインに対する内部またはローカルの VRF 割り当てが正しく機能していないことが問題であると考えられます。

解決方法

ロールの割り当てに対して次の手順を実行します。

- 「show running-config aaa」コマンドと「show aaa authentication」コマンドを使用して、どの AAA グループが認証に使用されているかを確認します。
- TACACS+ では、「show tacacs-server groups」コマンドと「show running-config tacacs+」コマンドを使用して、その AAA グループと VRF との関連付けを確認します。
- RADIUS+ では、「show radius-server groups」コマンドと「show running-config radius」コマンドを使用して、その AAA グループと VRF との関連付けを確認します。
- 上記のコマンドで関連付けが正しいことがわかった場合は、「debug tacacs+ all」コマンドを使用してトレースをイネーブルにします。
- このユーザでもう一度ログインし、デバッグ トレースを収集します。
- このトレースには、詳しい調査に使用できる情報が記録されています（以下の例を参照）。

  例：

  ```
  tacacs: process_aaa_tplus_request: Group t1 found. corresponding vrf is management
  ```

- 「no debug tacacs+ all」コマンドを使用して、TACACS+ でのデバッグ トレースをオフにします。

TACACS+ アカウンティングを有効にすると、ACS サーバ上にコマンド アカウンティングのログが存在しない

TACACS+ アカウンティングを有効にすると、ACS サーバ上にコマンド アカウンティングのログが見つかりません。

考えられる原因

ACS サーバの設定が間違っているか、不完全です。

解決方法

次の手順を実行します。

- ネットワーク設定の ACS の GUI で、任意のクライアントの AAA クライアント設定に移動します。[Log Update/Watchdog Packets from this AAA Client] チェックボックスをオンにします。[Submit + Apply] ボタンをクリックします。

- 次のメニュー パスで CMD アカウンティングを確認します。

  [Reports and Activity] > [TACACS+ Administration]

  「Tacacs+Administration <active|DATE>.csv」ファイルを開き、各行の「cmd」とタイムスタンプを確認します。

RADIUS で PAP 認証が機能しない

TACACS+ では PAP 認証が機能しますが、RADIUS では機能しません。

考えられる原因

NXOS では、リリース 4.2（1）より TACACS+ でのみ ASCII（PAP）認証をサポートするようになりました。

解決方法

NXOS では、ASCII 認証は PAP 認証と同等です。デフォルトでは、TACACS+ と RADIUS はいずれも CHAP を使用します。「aaa authentication login ascii-authentication」コマンドを使用すると、PAP 認証に切り替えることができます。

ユーザが RADIUS と同時に TACACS+ も設定しようとすると、次の例にあるような Syslog メッセージがログインの際に表示されます。

例：

```
2010 May 19 16:12:19 mars %$ VDC-1 %$ %RADIUS-2-RADIUS_NO_AUTHEN_INFO: ASCII
authentication not supported
2010 May 19 16:12:19 mars %$ VDC-1 %$ %AUTHPRIV-3-SYSTEM_MSG: pam_aaa:Authentication
failed for user oregon-regress from 10.193.128.5 - login[5698]
```

認証のフォールバック メカニズムが動作していないように見える

NXOS が認証でサポートしているフォールバック メカニズムでは、どの AAA リモート RADIUS サーバにも、またどの AAA リモート TACACS+ サーバにもアクセスできない場合は、ログインの際にローカルで SSH/Telnet ユーザを認証しようとします。しかし、Nexus 5000 へのログインがローカル認証でも失敗します。

考えられる原因

ユーザがログインで使用しているユーザ アカウントが、ローカルのユーザ データベースに存在していません。

解決方法

次の手順を実行して、認証のフォールバック メカニズムを確認します。

- 基本的な手順として、設定で「aaa authentication login error-enable」を指定する必要があります。これを設定で指定すると、フォールバック メカニズムが正しく機能しているかどうかをログイン セッションで確認できます。「Remote AAA servers unreachable; local authentication done」や「Remote AAA servers unreachable; local authentication failed」というメッセージが表示される場合は、フォールバック メカニズムが正しく機能しています。
- AAA サーバにアクセスできない場合は、ローカル認証のためのユーザ クレデンシャルがローカルのユーザ データベースに存在するかどうかを確認します。「show user-account」コマンドを使用してクレデンシャルを表示します。

（注）「show user-account」コマンドでは、REMOTE 認証によってどのユーザ アカウントが作成されているかを確認できます。REMOTE 認証で作成したユーザ アカウントはローカル（フォールバック）ログインで使用できません。

- リモート AAA サーバにアクセスできるようになるまで、「username <username> password <password> role <role name>」コマンドを使用してローカルのユーザ アカウントを作成します。