単一 の ホストおよびマルチドメイン シナリオのための設定 IBNS 2.0

目次

概要

この資料に単一 の ホストおよびマルチドメイン シナリオのための Identity Based Networking Services 2.0 （ IBNS ）を設定する方法を記述されています。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ローカル エリア ネットワーク（ EAPoL ）上の Extensible Authentication Protocol
- RADIUS プロトコル
- Cisco Identity Services Engine バージョン 2.0

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco 識別 サービス エンジン バージョン 2.0 パッチ 2
- Windows 7 OS のエンドポイント
- IOS 15.2(4)E1 の Ciscoスイッチ 3750X
- 03.02.03.SE の Ciscoスイッチ 3850
- Cisco IP Phone 9971

このドキュメントの情報は、特定のラボ環境に置かれたデバイスに基づいて作成されました。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

設定

設定理論

IBNS 2.0 を有効に するために、Ciscoスイッチの特権 モードのコマンドを実行する必要があります:

```
#authentication display new-style
```

示されているようにコマンドで IBNS 2.0 のためのスイッチポートを設定して下さい:

```
 access-session host-mode {single-host | multi-domain | multi-auth}
 access-session port-control auto
 dot1x pae authenticator
{mab} service-policy type control subscriber TEST
```

これらのコマンドはインターフェイスの dot1x 認証およびオプションで MAC 認証 バイパス（MAB）を有効に します。 新しい構文に続くとき、アクセス セッションから開始するコマンドを使用します。 それらのコマンドの目的は古い 構文を使用するコマンドのためと同じです（**認証**キーワードから開始する）。 インターフェイスのために使用する必要がある **policy-map を**規定するために**サービス ポリシーを**適用して下さい。

上記される **policy-map は**認証の間にスイッチ（オーセンティケータ）の動作を定義します。 たとえば、起こるはずであるものが認証失敗の場合には規定できます。 各**イベント**の場合それの下で設定される **class-map** で一致するイベントの種類に基づいて複数のアクションを設定できます。 一例として、示されているようにリストの見てみて下さい（**policy-map TEST4**）。 このポリシーが適用するインターフェイスに接続される dot1x エンドポイントが失敗した場合、**DOT1X_FAILED** で定義される操作は実行されます。 **MAB_FAILED** および **DOT1X_FAILED** のようなクラスのための同じ動作を規定 することを望んだ場合デフォルト クラスを- **class-map 常に**使用できます。

```
policy-map type control subscriber TEST4
(...)
 event authentication-failure match-first
  10 class DOT1X_FAILED do-until-failure
   10 terminate dot1x
(...)
  40 class always do-until-failure
   10 terminate mab
   20 terminate dot1x
   30 authentication-restart 60
(...)
```

IBNS 2.0 に使用する **Policy-map は**型**制御サブスクライバが**常になければなりません。

利用可能 な イベントのリストをこのように表示できます:

```
Switch(config-event-control-policymap)#event ?
  aaa-available                aaa-available event
  absolute-timeout             absolute timeout event
  agent-found                  agent found event
  authentication-failure       authentication failure event
  authentication-success       authentication success event
```

```
  authorization-failure         authorization failure event
  inactivity-timeout            inactivity timeout event
  session-started               session started event
  tag-added                     tag to apply event
  tag-removed                   tag to remove event
  template-activated            template activated event
  template-activation-failed    template activation failed event
  template-deactivated          template deactivated event
  template-deactivation-failed  template deactivation failed event
  timer-expiry                  timer-expiry event
  violation                     session violation event
```

イベント構成でクラスがどのように評価する必要があるか定義する可能性があります:

```
Switch(config-event-control-policymap)#event authentication-failure ?
  match-all    Evaluate all the classes
  match-first  Evaluate the first class
```

クラスが一致すれば操作がどのように実行する必要があるかここに規定 するが**クラスマップ**のための同じようなオプションを定義できます:

```
Switch(config-class-control-policymap)#10 class always ?
  do-all            Execute all the actions
  do-until-failure  Execute actions until one of them fails
  do-until-success  Execute actions until one of them is successful
```

dot1x の新式の設定の最後の一部 (オプションの) は **class-map** です。それはまた**制御サブスクライバ**を入力する必要があり、特定の動作かトラフィックを一致する使用します。 **class-map** のための設定必要条件は評価を調節します。 またはどの条件でも一致しなければならないか、または条件のどれも一致しなければならないか、ことをすべての条件が一致する必要がないこと規定できます。

```
Switch(config)#class-map type control subscriber ?
  match-all   TRUE if everything matches in the class-map
  match-any   TRUE if anything matches in the class-map
  match-none  TRUE if nothing matches in the class-map
```

これは dot1x 認証失敗と一致するために使用される **class-map** の例です:

```
class-map type control subscriber match-all DOT1X_FAILED
 match method dot1x
 match result-type method dot1x authoritative
```

いくつかのシナリオに関しては、大抵サービス テンプレートが使用中のとき、許可 (CoA) の変更のための設定を追加する必要があります:

```
aaa server radius dynamic-author
 client 10.48.17.232 server-key cisco
```

単一 の ホストのためのシナリオ

ネットワーク図

設定

IOS 15.2(4)E1 の Catalyst 3750X でテストされる単一 の ホスト シナリオに必要な 802.1X 基本的な設定。 Windows ネイティブ サプリカントおよび Cisco AnyConnect とテストされるシナリオ
。

```
aaa new-model
!
aaa group server radius tests
 server name RAD-1
!
aaa authentication dot1x default group tests
aaa authorization network default group tests
!
dot1x system-auth-control
!
policy-map type control subscriber TEST
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x priority 10
!
interface GigabitEthernet1/0/21
 switchport access vlan 613
 switchport mode access
 access-session host-mode single-host
 access-session port-control auto
 dot1x pae authenticator
 service-policy type control subscriber TEST
!
radius server RAD-1
 address ipv4 10.48.17.232 auth-port 1812 acct-port 1813
 key cisco
```

マルチドメインのためのシナリオ

ネットワーク図

設定

マルチドメイン シナリオは IP Phone （ 9971 ） Cisoc IP Phone のための PoE （ Power over Ethernet ）必要条件による IOS 03.02.03.SE の Catalyst 3850 でテストされました。

```
aaa new-model
!
aaa group server radius tests
 server name RAD-1
!
aaa authentication dot1x default group tests
aaa authorization network default group tests
!
aaa server radius dynamic-author
 client 10.48.17.232 server-key cisco
!
dot1x system-auth-control
!
```

```
class-map type control subscriber match-all DOT1X
 match method dot1x
!
class-map type control subscriber match-all DOT1X_FAILED
 match method dot1x
 match result-type method dot1x authoritative
!
class-map type control subscriber match-all DOT1X_NO_RESP
 match method dot1x
 match result-type method dot1x agent-not-found
!
class-map type control subscriber match-all MAB
 match method mab
!
class-map type control subscriber match-all MAB_FAILED
 match method mab
 match result-type method mab authoritative
!
policy-map type control subscriber TEST4
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x priority 10
   20 authenticate using mab priority 20
 event authentication-failure match-first
  10 class DOT1X_FAILED do-until-failure
   10 terminate dot1x
  20 class MAB_FAILED do-until-failure
   10 terminate mab
   20 authenticate using dot1x priority 10
  30 class DOT1X_NO_RESP do-until-failure
   10 terminate dot1x
   20 authentication-restart 60
  40 class always do-until-failure
   10 terminate mab
   20 terminate dot1x
   30 authentication-restart 60
 event agent-found match-all
  10 class always do-until-failure
   10 terminate mab
   20 authenticate using dot1x priority 10
 event authentication-success match-all
  10 class always do-until-failure
   10 activate service-template DEFAULT_LINKSEC_POLICY_SHOULD_SECURE
!
interface GigabitEthernet1/0/1
 switchport access vlan 613
 switchport mode access
 switchport voice vlan 612
 access-session host-mode multi-domain
 access-session port-control auto
 mab
 dot1x pae authenticator
 spanning-tree portfast
 service-policy type control subscriber TEST4
!
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server vsa send cisco-nas-port
!
radius server RAD-1
 address ipv4 10.48.17.232 auth-port 1812 acct-port 1813
 key cisco
```

確認

このセクションでは、設定が正常に機能していることを確認します。

確認するために、すべてのスイッチポートからのセッションをリストするのにこれらのコマンドを使用して下さい:

```
show access-session
```

また単一スイッチポートからのセッションについての詳細な情報を表示できます:

```
show access-session interface [Gi 1/0/1] {detail}
```

トラブルシューティング

このセクションでは、設定のトラブルシューティングに役立つ情報を提供します。

802.1X 関連 問題を解決するために、デバッグしますオールドスタイル 802.1X 構文のためのと同じ方法を有効に なることができます:

```
debug mab all
debug dot1x all
debug pre all*
```

* optionaly デバッグのために前にイベントだけ使用しおよび/または IBNS 2.0 関連情報に出力を制限するために支配できます。