



Application Visibility and Control (アプリケーションの可視化と制御)

- [Application Visibility and Control について \(1 ページ\)](#)
- [フロー モニターの作成 \(3 ページ\)](#)
- [フロー モニターの設定 \(GUI\) \(4 ページ\)](#)
- [フロー エクスポートの作成 \(5 ページ\)](#)
- [フロー エクスポートの確認 \(6 ページ\)](#)
- [AVC の WLAN の設定 \(7 ページ\)](#)
- [ポリシー タグの設定 \(7 ページ\)](#)
- [WLAN インターフェイスへのポリシー プロファイルのアタッチ \(GUI\) \(8 ページ\)](#)
- [WLAN インターフェイスへのポリシー プロファイルのアタッチ \(CLI\) \(8 ページ\)](#)
- [AP へのポリシー プロファイルのアタッチ \(10 ページ\)](#)
- [AVC の設定の確認 \(10 ページ\)](#)
- [AVC ベースの選択的リアンカー \(11 ページ\)](#)
- [AVC ベースの選択的リアンカーの制限事項 \(11 ページ\)](#)
- [フロー エクスポートの設定 \(12 ページ\)](#)
- [フロー モニターの設定 \(12 ページ\)](#)
- [AVC リアンカー プロファイルの設定 \(13 ページ\)](#)
- [ワイヤレス WLAN プロファイル ポリシーの設定 \(14 ページ\)](#)
- [AVC リアンカーの確認 \(15 ページ\)](#)

Application Visibility and Control について

Application Visibility and Control (AVC) は、トラフィック情報を提供できる Flexible NetFlow (FNF) パッケージ全体のサブセットです。AVC 機能では、アクセスポイント (AP) または組み込みワイヤレスコントローラで実行される NBAR のメリットをもたらす分散型アプローチが利用されており、ディープパケットインスペクション (DPI) を実行してその結果を FNF メッセージで報告することを目的としています。

AVCにより、リアルタイム分析を実施し、ネットワークの輻輳、コストのかかるネットワークリンクの使用、およびインフラストラクチャの更新を削減するためのポリシーを作成できます。トラフィックフローがNBAR2エンジンを使用して分析および認識され、認識されたプロトコルまたはアプリケーションと一緒に、特定のフローがマークされます。このフロー単位の情報を、FNFによるアプリケーションの可視化に使用できます。アプリケーションの可視化が確立されると、ユーザーはクライアントのポリシングメカニズムを使用してコントロールルールを定義できます。

AVCルールを使用すると、WLAN上でjoinしているすべてのクライアントに対して、特定アプリケーションの帯域幅を制限できます。これらの帯域幅コントラクトは、アプリケーション単位のレート制限より優先されるクライアント単位のダウンストリームレート制限と共存します。

FNFはワイヤレスでサポートされる機能であり、フレックスモードの組み込みワイヤレスコントローラでNetFlowが有効になっている必要があります。

AVCソリューションの動作は、ワイヤレスの展開に基づいて変わります。ここでは、すべてのシナリオにおける共通点と相違点について説明します。

フレックスモード

- NBARはAPで有効になっています。
- AVCは、FNF設定をAPにプッシュします。
- AVC-FNFで、ローミングのコンテキスト転送をサポートします。
- NetFlowエクスポートをサポートします。

Application Visibility and Control の前提条件

- アクセスポイントは、AVC対応である必要があります
- AVC (QoS) の制御部分を機能させるには、FNF付きのアプリケーションの可視化機能を設定する必要があります。

Application Visibility and Control の制限

- レイヤ2ローミングは、組み込みワイヤレスコントローラでサポートされていません。
- マルチキャストトラフィックはサポートされていません。
- AVCは次のアクセスポイントでのみサポートされます。
 - Cisco Aironet 1800 シリーズ アクセスポイント
 - Cisco Aironet 2700 シリーズ アクセスポイント
 - Cisco Aironet 2800 シリーズ アクセスポイント

- Cisco Aironet 3700 シリーズ アクセス ポイント
 - Cisco Aironet 3800 シリーズ アクセス ポイント
 - Cisco Aironet 4800 シリーズ アクセス ポイント
-
- AVC は、Cisco Aironet 702W、702I (128 M メモリ)、および 1530 シリーズ アクセス ポイントではサポートされません。
 - App の可視性と認識されているアプリケーションのみ、QoS 制御の適用に使用できます。
 - データリンクは AVC の NetFlow フィールドではサポートされません。
 - AVC 非対応ポリシープロファイルと AVC 対応ポリシープロファイルの両方に同じ WLAN プロファイルをマッピングすることはできません。
 - NBAR 対応 QoS ポリシー設定は有線物理ポートでポリシープロファイルで設定された、クライアントレベルおよび BSSID レベルの VLAN、ポートチャネル、および他の論理インターフェイスなどの仮想インターフェイスではサポートされていません。

AVC が有効になっている場合、AVC プロファイルは、デフォルトの DSCP ルールを含む最大 23 個のルールのみをサポートします。ルールが 23 個を超えている場合、AVC ポリシーは AP までプッシュされません。

AVC の設定の概要

AVC を設定するには、次の手順に従います。

1. **record wireless avc basic** コマンドを使用してフロー モニターを作成します。
2. ワイヤレス ポリシー プロファイルを作成します。
3. フロー モニターをワイヤレス ポリシー プロファイルに適用します。
4. ワイヤレス ポリシー タグを作成します。
5. WLAN をポリシー プロファイルにマッピングします。
6. ポリシー タグを AP に接続します。

フロー モニターの作成

NetFlow の設定には、フロー レコード、フロー モニター、およびフロー エクスポートが必要です。この設定は、AVC 全体の設定における最初のステップとして行ってください。



- (注) Flex モードでは、**cache timeout active** および **cache timeout inactive** コマンドのデフォルト値は AVC に最適ではありません。フロー モニターでは、両方の値を 60 に設定することを推奨します。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	flow monitor monitor-name 例： Device(config)# flow monitor fm_avc	フロー モニターを作成します。
ステップ 3	record wireless avc basic 例： Device(config-flow-monitor)# record wireless avc basic	基本のワイヤレス AVC フローテンプレートを指定します。 (注) record wireless avc basic コマンドは record wireless avc ipv4 basic コマンドと同じです。ただし、Flex または ファブリックモードでは record wireless avc ipv4 basic コマンドはサポートされていません。このようなシナリオでは record wireless avc basic コマンドを使用します。

フローモニターの設定 (GUI)

始める前に

フローモニターからデータをエクスポートするには、フローエクスポートを作成しておく必要があります。

手順

ステップ 1 [Configuration] > [Services] > [Application Visibility] の順に選択し、[Flow Monitor] タブに移動します。

ステップ 2 [Monitor] エリアで、[Add] をクリックしてフローモニターを追加します。

ステップ 3 [Flow Monitor] ウィンドウで、フローモニターと説明を追加します。

ステップ 4 ドロップダウンリストからフローエクスポートを選択して、フローモニターからコレクタにデータをエクスポートします。

(注) Wireless NetFlow データをエクスポートするには、以下のテンプレートを使用します。

- ETA (暗号化トラフィック分析)
- ワイヤレス AVC の基本
- ワイヤレス AVC の基本 IPv6

ステップ 5 [Apply to Device] をクリックして、設定を保存します。

フロー エクスポートの作成

フロー エクスポートを作成すると、フローのエクスポート パラメータを定義できます。これは、フローのエクスポート パラメータを設定するためのオプションの手順です。



(注) AVC 統計情報が組み込みワイヤレスコントローラに表示されるようにするには、次のコマンドを使用してローカルのフローエクスポートを設定する必要があります。

- **flow exporter my_local**
- **destination local wlc**

また、フローモニターでは、統計情報を組み込みワイヤレスコントローラに表示するためにこのローカルのエクスポートを使用する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	flow exporter flow-export-name 例： Device(config)# flow exporter export-test	フロー モニターを作成します。

	コマンドまたはアクション	目的
ステップ 2	description string 例： Device(config-flow-exporter) # description IPv4flow	最大 63 文字で、フローレコードの説明を示します。
ステップ 3	例： Device(config-flow-exporter) # destination local wlc	エクスポートがデータを送信する宛先のローカル WLC を指定します。
ステップ 4	show flow exporter 例： Device # show flow exporter	(任意) 設定を確認します。

フローエクスポートの確認

フローエクスポートの説明を確認するには、次のコマンドを使用します。

たとえば、**my-flow-exporter** という名前のフローエクスポートに関するフローエクスポートの説明を確認するには、次の例を参照してください。

```
Device# show flow exporter
Flow Exporter my-flow-exporter:
  Description:           User defined
  Export protocol:       NetFlow Version 9
  Transport Configuration:
    Destination type:    Local (1)
    Destination IP address: 0.0.0.0
    Source IP address:   10.0.0.1
    Transport Protocol:  UDP
    Destination Port:    9XXX
    Source Port:         5XXXX
    DSCP:                0x0
    TTL:                 255
    Output Features:     Not Used
```



(注) 宛先のないフローエクスポートは、UNKNOWN タイプとしてマークされます。エクスポートが UNKNOWN としてマークされる 2 つの方法は次のとおりです。

1. 宛先を指定しないで CLI コマンドを使用してフローエクスポートを設定する場合。
2. EWC は、最大 1 つの外部フローエクスポートと 1 つの内部フローエクスポートをサポートします。タイプごとに複数のフローエクスポートを設定しようとすると、宛先が拒否され、フローエクスポートは UNKNOWN と見なされます。

AVC の WLAN の設定

AVC の WLAN を設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	wlan wlan-avc 1 ssid-avc 例： Device(config)# wlan wlan1 1 ssid1	WLAN を設定します。
ステップ 2	shutdown 例： Device(config-wlan)# shutdown	WLAN をシャットダウンします。
ステップ 3	no security wpa akm dot1x 例： Device(config-wlan)# no security wpa akm dot1x	dot1x に対するセキュリティの AKM をディセーブルにします。
ステップ 4	no security wpa wpa2 ciphers aes 例： Device(config-wlan)# no security wpa wpa2 ciphers aes	AES の WPA2 暗号化を無効にします。

ポリシー タグの設定

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	wireless tag policy policy-tag-name 例： Device(config-policy-tag)# wireless tag policy rr-xyz-policy-tag	ポリシー タグを設定し、ポリシー タグ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	end 例： Device(config-policy-tag)# end	設定を保存し、コンフィギュレーションモードを終了して、特権 EXEC モードに戻ります。

WLAN インターフェイスへのポリシー プロファイルのタッチ (GUI)

手順

-
- ステップ 1 [Configuration] > [Tags & Profiles] > [Tags] > > を選択します。
 - ステップ 2 [Manage Tags] ページで、[Policy] タブをクリックします。
 - ステップ 3 [Add] をクリックして、[Add Policy Tag] ウィンドウを表示します。
 - ステップ 4 ポリシー タグの名前と説明を入力します。
 - ステップ 5 [Add] をクリックして、WLAN とポリシーをマッピングします。
 - ステップ 6 適切なポリシープロファイルを使用してマッピングする WLAN プロファイルを選択し、チェックアイコンをクリックします。
 - ステップ 7 [Save & Apply to Device] をクリックします。
-

WLAN インターフェイスへのポリシー プロファイルのタッチ (CLI)

始める前に

- 異なるポリシー タグ間で同じ WLAN に異なる AVC ポリシー プロファイルを適用しないでください。

次に、正しくない設定例を示します。

```
wireless profile policy avc_pol1
  ipv4 flow monitor fm-avc1 input
  ipv4 flow monitor fm-avc1 output
  no shutdown
wireless profile policy avc_pol2
  ipv4 flow monitor fm-avc2 input
  ipv4 flow monitor fm-avc2 output
  no shutdown
wireless tag policy avc-tag1
wlan wlan1 policy avc_pol1
```

```
wireless tag policy avc-tag2
wlan wlan1 policy avc_pol2
```

この例は前述の制限に反しています。つまり、WLAN *wlan1* を2つのポリシー プロファイル (*avc_pol1* と *avc_pol2*) にマッピングしています。したがって、WLAN *wlan1* をすべての場所で *avc_pol1* または *avc_pol2* にマッピングする必要があるため、この設定は正しくありません。

- 同じ WLAN でのポリシー プロファイルの競合はサポートされていません。たとえば、ポリシー プロファイルを (AVC の有無にかかわらず) 異なるポリシー タグ内の同じ WLAN に適用する場合などです。

次に、正しくない設定例を示します。

```
wireless profile policy avc_pol1
no shutdown
wireless profile policy avc_pol2
ipv4 flow monitor fm-avc2 input
ipv4 flow monitor fm-avc2 output
no shutdown
wireless tag policy avc-tag1
wlan wlan1 policy avc_pol1
wireless tag policy avc-tag2
wlan wlan1 policy avc_pol2
```

この例では、AVC の有無にかかわらずポリシー プロファイルを異なるタグ内の同じ WLAN に適用しています。

手順

	コマンドまたはアクション	目的
ステップ 1	wireless tag policy avc-tag 例 : Device(config)# wireless tag policy avc-tag	ポリシー タグを作成します。
ステップ 2	wlan wlan-avc policy avc-policy 例 : Device(config-policy-tag)# wlan wlan_avc policy avc_pol	WLAN プロファイルにポリシー プロファイルをアタッチします。

次のタスク

- 設定が完了したら、WLAN で **no shutdown** コマンドを実行します。
- WLAN がすでに **no shutdown** モードになっている場合は、**shutdown** コマンドを実行し、その後に **no shutdown** コマンドを実行します。

AP へのポリシー プロファイルのアタッチ

手順

	コマンドまたはアクション	目的
ステップ 1	ap ap-ether-mac 例： Device(config)# ap 34a8.2ec7.4cf0	AP コンフィギュレーションモードを開始します。
ステップ 2	policy-tag policy-tag 例： Device(config)# policy-tag avc-tag	アクセス ポイントにアタッチするポリシー タグを指定します。

AVC の設定の確認

手順

	コマンドまたはアクション	目的
ステップ 1	show avc wlan wlan-name top num-of-applications applications {aggregate downstream upstream} 例： Device# show avc wlan wlan_avc top 2 applications aggregate	これらのアプリケーションを使用している上位のアプリケーションとユーザーに関する情報を表示します。 (注) ワイヤレス クライアントが WLAN に関連付けられていて、トラフィックが生成されていることを確認し、その後 90 秒間待ってからコマンドを実行してください (統計情報を確実に参照できるようにするため)。
ステップ 2	show avc client mac top num-of-applications applications {aggregate downstream upstream}	上位の数のアプリケーションに関する情報を表示します。

	コマンドまたはアクション	目的
	例 : <pre>Device# show avc client 9.3.4 top 3 applications aggregate</pre>	(注) ワイヤレスクライアントが WLAN に関連付けられていて、トラフィックが生成されていることを確認し、その後 90 秒間待ってからコマンドを実行してください (統計情報を確実に参照できるようにするため)。
ステップ 3	show avc wlan wlan-name application app-name top num-of-clients aggregate 例 : <pre>Device# show avc wlan wlan_avc application app top 4 aggregate</pre>	これらのアプリケーションを使用している上位のアプリケーションとユーザーに関する情報を表示します。
ステップ 4	show ap summary 例 : <pre>Device# show ap summary</pre>	組み込みワイヤレスコントローラに接続しているすべてのアクセスポイントのサマリーを表示します。
ステップ 5	show ap tag summary 例 : <pre>Device# show ap tag summary</pre>	ポリシー タグを持つすべてのアクセスポイントのサマリーを表示します。

AVC ベースの選択的リアンカー

AVC ベースの選択的リアンカー機能は、クライアントが一方の組み込みワイヤレスコントローラから他方のコントローラにローミングするときにクライアントをリアンカーすることを目的としています。クライアントをリアンカーすることで、Cisco WLC の新しいクライアントで使用可能な IP アドレスが枯渇するのを防ぎます。クライアントをリアンカーするか保留するかを決めるために、AVC プロファイルベースの統計情報が使用されます。この機能は、AVC ルールで定義されている音声またはビデオアプリケーションをクライアントが積極的に実行している場合に便利です。

リアンカーのプロセスでは、アンカーされたクライアントの認証解除も伴います。クライアントは、WLC 間をローミングしている時に、AVC ルールにリストされているアプリケーションのトラフィックを送信していない場合に、認証解除されます。

AVC ベースの選択的リアンカーの制限事項

- この機能はローカルモードでのみサポートされています。FlexConnect モードおよびフレックモードはサポートされていません。

- この機能は、ゲスト トンネリングおよびエクスポート アンカーのシナリオではサポートされていません。
- 古い IP アドレスは、IP アドレスのリース期間が終了するまで、リアンカー後も解放されません。

フロー エクスポートの設定

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	flow exporter name 例： Device(config)# flow exporter avc-reanchor	フロー エクスポートを作成し、フロー エクスポート コンフィギュレーション モードを開始します。 (注) このコマンドを使用して既存のフロー エクスポートを変更することもできます。
ステップ 3	destination local wlc 例： Device(config-flow-exporter)# destination local wlc	エクスポートをローカルとして設定します。

フロー モニターの設定

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	flow monitor monitor-name 例： Device(config)# flow monitor fm_avc	フロー モニターを作成し、Flexible NetFlow フロー モニター コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
		(注) このコマンドを使用して既存のフロー モニターを変更することもできます。
ステップ 3	exporter <i>exporter-name</i> 例 : Device(config-flow-monitor)# exporter avc-reanchor	フロー エクスポートの名前を指定します。
ステップ 4	record wireless avc basic 例 : Device(config-flow-monitor)# record wireless avc basic	キャッシュの定義に使用するフロー レコードを指定します。
ステップ 5	cache timeout active value 例 : Device(config-flow-monitor)# cache timeout active 60	アクティブ フロー タイムアウトを秒単位で設定します。
ステップ 6	cache timeout inactive value 例 : Device(config-flow-monitor)# cache timeout inactive 60	非アクティブ フロー タイムアウトを秒単位で設定します。

AVC リアンカー プロファイルの設定

始める前に

- AVC-Reanchor-Class クラス マップを使用していることを確認します。それ以外のクラス マップ名はすべて、選択的リアンカーでは無視されます。
- システムの起動中に、AVC-Reanchor-Class クラス マップが存在するかどうかチェックされます。見つからなかった場合は、デフォルトのプロトコル (jabber-video、wifi-calling など) が作成されます。AVC-Reanchor-Class クラス マップが見つかった場合、設定の変更は行われず、スタートアップコンフィギュレーションに保存されているプロトコルの更新はリブート後も維持されます。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 :	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	Device# configure terminal	
ステップ 2	class-map cmap-name 例 : Device(config)# class-map AVC-Reanchor-Class	クラス マップを設定します。
ステップ 3	match any 例 : Device(config-cmap)# match any	デバイスを通過するいずれかのプロトコルと照合するようにデバイスに指示します。
ステップ 4	match protocol jabber-audio 例 : Device(config-cmap)# match protocol jabber-audio	アプリケーション名との一致を指定します。 必要に応じて、後でクラスマップ設定を編集し、jabber-video や wifi-calling などのプロトコルを追加または削除することができます。

ワイヤレス WLAN プロファイル ポリシーの設定

WLAN プロファイル ポリシーを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	wireless profile policy policy-name 例 : Device(config)# wireless profile policy default-policy-profile	WLAN ポリシー プロファイルを設定し、ワイヤレス ポリシー コンフィギュレーション モードを開始します。
ステップ 3	shutdown 例 : Device(config-wireless-policy)# shutdown	ポリシープロファイルを無効にします。
ステップ 4	central switching 例 : Device(config-wireless-policy)# central switching	中央スイッチングを有効にします。

	コマンドまたはアクション	目的
ステップ 5	ipv4 flow monitor <i>monitor-name</i> input 例 : Device(config-wireless-policy)# ipv4 flow monitor fm_avc input	IPv4 入力フローモニターの名前を指定 します。
ステップ 6	ipv4 flow monitor <i>monitor-name</i> output 例 : Device(config-wireless-policy)# ipv4 flow monitor fm_avc output	IPv4 出力フローモニターの名前を指定 します。
ステップ 7	reanchor class <i>class-name</i> 例 : Device(config-wireless-policy)# reanchor class AVC-Reanchor-Class	選択的リアンカー機能のプロトコルを使 用してクラス マップを設定します。
ステップ 8	no shutdown 例 : Device(config-wireless-policy)# no shutdown	ポリシープロファイルを有効にします。

AVC リアンカーの確認

AVC リアンカーの設定を確認するには、次のコマンドを使用します。

```
Device# show wireless profile policy detailed avc_reanchor_policy
```

```
Policy Profile Name      : avc_reanchor_policy
Description              :
Status                  : ENABLED
VLAN                    : 1
Wireless management interface VLAN      : 34
!
.
.
.
AVC VISIBILITY          : Enabled
Flow Monitor IPv4
  Flow Monitor Ingress Name : fm_avc
  Flow Monitor Egress Name  : fm_avc
Flow Monitor IPv6
  Flow Monitor Ingress Name : Not Configured
  Flow Monitor Egress Name  : Not Configured
NBAR Protocol Discovery : Disabled
Reanchoring             : Enabled
Classmap name for Reanchoring
  Reanchoring Classmap Name : AVC-Reanchor-Class
!
.
.
.
```

```
-----
Device# show platform software trace counter tag wstatsd chassis active R0 avc-stats
debug
```

```
Counter Name Thread ID Counter Value
-----
```

```
Reanch_deassociated_clients 28340 1
Reanch_tracked_clients 28340 4
Reanch_deleted_clients 28340 3
```

```
Device# show platform software trace counter tag wncd chassis active R0 avc-afc debug
```

```
Counter Name Thread ID Counter Value
-----
```

```
Reanch_co_ignored_clients 30063 1
Reanch_co_anchored_clients 30063 5
Reanch_co_deauthed_clients 30063 4
```

```
Device# show platform software wlavc status wncd
```

```
Event history of WNCDB:
```

```
AVC key: [1,wlan_avc,N/A,Reanc,default-policy-tag]
Current state : READY
Wlan-id : 1
Wlan-name : wlan_avc
Feature type : Reanchoring
Flow-mon-name : N/A
Policy-tag : default-policy-tag
Switching Mode : CENTRAL
```

```
Timestamp FSM State Event RC Ctx
-----
```

```
06/12/2018 16:45:30.630342 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:45:28.822780 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:28.822672 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:15.172073 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:45:12.738367 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:12.738261 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:01.162689 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:44:55.757643 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:44:55.757542 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:44:04.468749 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:44:02.18857 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:44:02.18717 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:38:20.164304 2 :READY 3 :FSM_AFM_SWEEP 0 2
06/12/2018 16:35:20.163877 2 :READY 1 :FSM_AFM_BIND 0 2
06/12/2018 16:35:18.593257 1 :INIT 1 :FSM_AFM_BIND 0 2
06/12/2018 16:35:18.593152 1 :INIT 24:CREATE_FSM 0 0
```

```
AVC key: [1,wlan_avc,fm_avc,v4-In,default-policy-tag]
Current state : READY
Wlan-id : 1
Wlan-name : wlan_avc
Feature type : Flow monitor IPv4 Ingress
Flow-mon-name : fm_avc
Policy-tag : default-policy-tag
Switching Mode : CENTRAL
```

```
Timestamp FSM State Event RC Ctx
-----
```

```
06/12/2018 16:45:30.664772 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
```

```

06/12/2018 16:45:28.822499 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:28.822222 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:15.207605 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:45:12.738105 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:12.737997 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:01.164225 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:44:55.757266 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:44:55.757181 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:44:04.472778 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:44:02.15413 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:44:02.15263 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:38:20.164254 2 :READY 3 :FSM_AFM_SWEEP 0 2
06/12/2018 16:35:20.163209 1 :INIT 1 :FSM_AFM_BIND 0 2
06/12/2018 16:35:20.163189 1 :INIT 24:CREATE_FSM 0 0

```

```

AVC key: [1,wlan_avc,fm_avc,v4-Ou,default-policy-tag]
Current state : READY
Wlan-id : 1
Wlan-name : wlan_avc
Feature type : Flow monitor IPv4 Egress
Flow-mon-name : fm_avc
Policy-tag : default-policy-tag
Switching Mode : CENTRAL

```

```
Timestamp FSM State Event RC Ctx
```

```

-----
06/12/2018 16:45:30.630764 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:45:28.822621 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:28.822574 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:15.172357 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:45:12.738212 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:12.738167 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:01.164048 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:44:55.757403 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:44:55.757361 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:44:04.472561 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:44:02.18660 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:44:02.18588 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:38:20.164293 2 :READY 3 :FSM_AFM_SWEEP 0 2
06/12/2018 16:35:20.163799 1 :INIT 1 :FSM_AFM_BIND 0 2
06/12/2018 16:35:20.163773 1 :INIT 24:CREATE_FSM 0 0

```

```
Device# show platform software wlavc status wncmgrd
```

```
Event history of WNCMgr DB:
```

```

AVC key: [1,wlan_avc,N/A,Reanc,default-policy-tag]
Current state : READY
Wlan-id : 1
Wlan-name : wlan_avc
Feature type : Reanchoring
Flow-mon-name : N/A
Policy-tag : default-policy-tag
Switching Mode : CENTRAL
Policy-profile : AVC_POL_PYATS

```

```
Timestamp FSM State Event RC Ctx
```

```

-----
06/12/2018 16:45:30.629278 3 :WLAN_READY 24:BIND_WNCD 0 0
06/12/2018 16:45:30.629223 3 :WLAN_READY 4 :FSM_BIND_ACK 0 0
06/12/2018 16:45:30.629179 3 :WLAN_READY 4 :FSM_BIND_ACK 0 0
06/12/2018 16:45:30.510867 2 :PLUMB_READY 22:BIND_IOSD 0 0
06/12/2018 16:45:30.510411 2 :PLUMB_READY 2 :FSM_WLAN_UP 0 0
06/12/2018 16:45:30.510371 2 :PLUMB_READY 1 :FSM_WLAN_FM_PLUMB 0 0

```

```
06/12/2018 16:45:28.886377 2 :PLUMB_READY 20:UNBIND_ACK_IOSD 0 0
!
```

```
AVC key: [1,wlan_avc,fm_avc,v4-In,default-policy-tag]
Current state : READY
Wlan-id : 1
Wlan-name : wlan_avc
Feature type : Flow monitor IPv4 Ingress
Flow-mon-name : fm_avc
Policy-tag : default-policy-tag
Switching Mode : CENTRAL
Policy-profile : AVC_POL_PYATS
```

```
Timestamp FSM State Event RC Ctx
```

```
-----
06/12/2018 16:45:30.664032 3 :WLAN_READY 24:BIND_WNCD 0 0
06/12/2018 16:45:30.663958 3 :WLAN_READY 4 :FSM_BIND_ACK 0 0
06/12/2018 16:45:30.663921 3 :WLAN_READY 4 :FSM_BIND_ACK 0 0
06/12/2018 16:45:30.511151 2 :PLUMB_READY 22:BIND_IOSD 0 0
06/12/2018 16:45:30.510624 2 :PLUMB_READY 2 :FSM_WLAN_UP 0 0
06/12/2018 16:45:30.510608 2 :PLUMB_READY 1 :FSM_WLAN_FM_PLUMB 0 0
06/12/2018 16:45:28.810867 2 :PLUMB_READY 20:UNBIND_ACK_IOSD 0 0
06/12/2018 16:45:28.807239 4 :READY 25:UNBIND_WNCD 0 0
06/12/2018 16:45:28.807205 4 :READY 23:UNBIND_IOSD 0 0
06/12/2018 16:45:28.806734 4 :READY 3 :FSM_WLAN_DOWN 0 0
!
```

```
AVC key: [1,wlan_avc,fm_avc,v4-Ou,default-policy-tag]
Current state : READY
Wlan-id : 1
Wlan-name : wlan_avc
Feature type : Flow monitor IPv4 Egress
Flow-mon-name : fm_avc
Policy-tag : default-policy-tag
Switching Mode : CENTRAL
Policy-profile : AVC_POL_PYATS
```

```
Timestamp FSM State Event RC Ctx
```

```
-----
06/12/2018 16:45:30.629414 3 :WLAN_READY 24:BIND_WNCD 0 0
06/12/2018 16:45:30.629392 3 :WLAN_READY 4 :FSM_BIND_ACK 0 0
06/12/2018 16:45:30.629380 3 :WLAN_READY 4 :FSM_BIND_ACK 0 0
06/12/2018 16:45:30.510954 2 :PLUMB_READY 22:BIND_IOSD 0 0
06/12/2018 16:45:30.510572 2 :PLUMB_READY 2 :FSM_WLAN_UP 0 0
06/12/2018 16:45:30.510532 2 :PLUMB_READY 1 :FSM_WLAN_FM_PLUMB 0 0
06/12/2018 16:45:28.886293 2 :PLUMB_READY 20:UNBIND_ACK_IOSD 0 0
06/12/2018 16:45:28.807844 4 :READY 25:UNBIND_WNCD 0 0
06/12/2018 16:45:28.807795 4 :READY 23:UNBIND_IOSD 0 0
06/12/2018 16:45:28.806990 4 :READY 3 :FSM_WLAN_DOWN 0 0
!
```

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。