

# Using Airwave and SNMP traps

## 1 Overview

This tutorial will cover how to create triggers in Airwave to react to certain events received via SNMP Traps from your Aruba controller as well some sample IDS events you would want to be notified about.

## 2 Airwave – Aruba best practices

Read and implement the Aruba and Airwave best practices guide. Here are some of the key elements: (related only to this tutorial)

1. Configure an SNMP Community string on your controller
2. Create an AMP specific root username/password on your controller
3. On the controller, configure a management server. Enabling these commands allows the ability to obtain RF Utilization metrics.

```
(controller) # configure terminal
(controller) (config) # mgmt-server type amp primary-server <AMP-IP>
(controller) (config) # write mem
```

4. Define AMP as a Trap Host using the AOS CLI (Page 23 of guide)

```
(controller) # configure terminal
(controller) (config) # snmp-server host <AMP-IP> version 2c <SNMP
Community string of controller>
(controller) (config) # snmp-server trap source <controller-ip>
(controller) (config) # write mem
```

5. Ensure that IDS traps are enabled (Page 23 of guide)

```
(controller) # show snmp-trap list
```

If any of the traps are not enabled, enter configure terminal mode and enable them like so

```
(controller) (config) # snmp-server trap enable <TRAP NAME FROM LIST
ABOVE>
(controller) (config) # write mem
```

## 3 Get a copy of the Aruba MIBs and Syslog guide

These guides contain the information you need in terms of what to trigger on. Therefore if you want to be alert for something very specific, you can by leveraging the information within these guides.

## 4 Triggers

### 4.1 Triggers based off Device Events

#### 4.1.1 Monitoring controller processes

If a process dies on a controller, currently Airwave will not be able to tell you unless you create a trigger for it.

Here is a way of setting up a trigger to be alert if ever a process should die on the controller

The screenshot displays the AMP configuration interface for setting up a trigger. It is divided into four main sections: Device Event Trigger, Conditions, Trigger Restrictions, and Alert Notifications.

**Device Event Trigger**

Type: Device Event  
Severity: Critical

**Conditions**

Matching conditions: ☒ All ☐ Any

Available Conditions: Event Contents, Event Type, SNMP Trap Category, Syslog Category, Syslog Severity

New Trigger Condition

Option	Condition	Value
Event Type	is	SNMP Trap
Event Contents	matches	died

**Trigger Restrictions**

Folder: Top

Include Subfolders: ☒ Yes ☐ No

Group: - All Groups -

**Alert Notifications**

Notes:

Additional Notification Options:

☐ Email  
☐ NMS

Add NMS servers on the [AMP Setup NMS page](#)

Logged Alert Visibility: By Triggering Agent

Suppress Until Acknowledged: ☒ Yes ☐ No

By matching the event contents with the word died, AMP will be able to send you an email (if configured) when a process dies so you can validate whether it was restarted or be alerted whenever it fails so you can open a case with TAC.

To note: because we are matching against the word “died”, you may receive an alert if the system detects an interferingAP with the word died in the SSID, like below:

Device: wlc-18.tdl.c6.dv - [https://aw-1.tdl.c6.dv/ap\\_monitoring?id=33](https://aw-1.tdl.c6.dv/ap_monitoring?id=33)  
Group: wlc-18  
Folder: Top > WLC-18  
Location:

Message: wlsxNInterferingAPDetected wlsxTrapAPChannel.0: 6, wlsxTrapTargetAPBSSID.0: 20:02:AF:69:61:7E, wlsxTrapTargetAPSSID.0: **JesusDiedLol**, wlsxTrapTime: 2/8/2014 21:9:34 UTC-5

#### 4.1.2 Combining device events for health of the controller

We can also combine several Device Events into one single trigger to be alerted when the controller is running low on memory, one of the fans has failed, or a certificate will be expiring soon. See configuration below:

Making sure the matching conditions are “any”

The screenshot displays the 'Device Event Trigger' configuration window. It is divided into several sections:

- Device Event Trigger:** Type is set to 'Device Event' and Severity is set to 'Critical'.
- Conditions:** Matching conditions are set to 'Any'. Available conditions include Event Contents, Event Type, SNMP Trap Category, Syslog Category, and Syslog Severity. A table lists the configured conditions:

Option	Condition	Value
Event Type	is	SNMP Trap
Event Contents	matches	wlsxNLowMemory
Event Contents	matches	wlsxNFanFailure
Event Contents	matches	wlsxColdStart
Event Contents	matches	wlsxWMSOffloadRecommended
Event Contents	matches	wlsxCertExpiringSoon
- Trigger Restrictions:** Folder is set to 'Top', Include Subfolders is set to 'Yes', and Group is set to '- All Groups -'.
- Alert Notifications:** Notes field is empty. Additional Notification Options include 'Email' and 'NMS'. Logged Alert Visibility is set to 'By Triggering Agent'. Suppress Until Acknowledged is set to 'Yes'.

At the bottom, there are 'Save' and 'Cancel' buttons.

### 4.1.3 Creating thresholds on the controller and being alerted in Airwave

In AOS 6.3, you can configure thresholds on the controller but then use Airwave to alert you if those thresholds have exceeded or cleared.

For example, if you want to be alerted that the number of APs has exceeded a certain threshold (in case you are worried about licensing), you can set that up like below:

```
(dnoc-wlc-2.rdlab.dv) (config) #threshold ?
controlpath-cpu          Alert threshold for ControlPath CPU
controlpath-memory       Alert threshold for ControlPath Memory consumption
datapath-cpu             Alert threshold for Datapath CPU
no-of-APs               Alert threshold for No of APs connected
no-of-locals             Alert threshold for No of locals
total-tunnel-capacity    Alert threshold for Total Tunnel capacity
user-capacity            Alert threshold for USER capacity
```

```
(dnoc-wlc-2.rdlab.dv) (config) #threshold no-of-APs 10
```

In AMP now, threshold exceed or cleared

**Trigger**  
Type: Device Event  
Severity: Normal

**Conditions**  
Matching conditions: ☐ All ☒ Any  
Available Conditions: Event Contents, Event Type, SNMP Trap Category, Syslog Category, Syslog Severity  
 New Trigger Condition  

Option	Condition	Value
Event Type	is	SNMP Trap
Event Contents	matches	wlsxThresholdExceeded
Event Contents	matches	wlsxThresholdCleared

**Trigger Restrictions**  
Folder: Top  
Include Subfolders: ☒ Yes ☐ No  
Group: - All Groups -

**Alert Notifications**  
Notes:  

Additional Notification Options:  
☐ Email  
☐ NMS  
[Add NMS servers on the AMP Setup NMS page](#)

Logged Alert Visibility: By Role  
Suppress Until Acknowledged: ☒ Yes ☐ No

#### 4.1.4 Monitoring controller resources

You can use the Device Resources trigger to alert you if a controller's resources such as CPU or Memory is being over utilized.

This particular trigger will alert you if a controller's CPU or Memory's utilization is more than 90% for a duration of 30 minutes or more.

Device Resources Trigger	
Type:	Device Resources
Severity:	Normal
Duration: e.g. '15 minutes', '75 seconds', '1 hr 15 mins'	30 minutes

Conditions	
Matching conditions:	<input type="radio"/> All <input checked="" type="radio"/> Any
Available Conditions: Device Type, Percent CPU Utilization, Percent Memory Utilization	
<input type="button" value="Add"/> New Trigger Condition	
<b>Option</b>	<b>Condition Value</b>
Device Type	is Controller
Percent CPU Utilization	>= 90
Percent Memory Utilization	>= 90

Trigger Restrictions	
Folder:	Top
Include Subfolders:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Group:	- All Groups -

Alert Notifications
Notes:

Accompanying alert:

Device Resources: Device Type is Controller, Percent CPU Utilization >= 90% or Percent Memory Utilization >= 90% for 30 minutes

Severity: Normal

Time: Fri Jan 10 13:58:20 2014

Device: uat-wlc-1.tdl.c6.dv - [https://aw-1.tdl.c6.dv/ap\\_monitoring?id=5089](https://aw-1.tdl.c6.dv/ap_monitoring?id=5089)

Group: UAT-WLC

Folder: Top > UAT-WLC

Location:

### 4.1.5 Device IDS Events

Since we have configured SNMP Traps on the controller and have enabled the controller to send those traps to AMP, we can get alert if particular IDS events occur. It is great that we can get visibility into rogues and IDS events within Airwave but when action is required, we need to be alerted.

The trigger below will alert us if the following IDS events occur:

Ad-Hoc Using Valid SSID

Ad-Hoc network using valid SSID

**Device IDS Events Trigger**

Type: Device IDS Events

Severity: Major

Duration: 5 minutes  
e.g. '15 minutes', '75 seconds', '1 hr 15 mins'

**Conditions**

Matching conditions: ☒ All ☐ Any

Available Conditions: Count, Trap Category, Trap Name, Trap Severity

Add New Trigger Condition

Option	Condition	Value
Trap Name	is	Ad-hoc Using Valid SSID
Trap Name	is	Adhoc Network Using Valid SSID

**Trigger Restrictions**

Folder: [Redacted]

Include Subfolders: ☒ Yes ☐ No

Group: - All Groups -

**Alert Notifications**

Notes:

Additional Notification Options: ☒ Email ☐ NMS

Add NMS servers on the [AMP Setup NMS page](#)

Sender Address: [Redacted]@datavalet.com

Enter multiple email addresses of the form user@domain separated by spaces, commas, or semicolons.



Recipient Email Addresses: alarms-wlan@[Redacted]

Logged Alert Visibility: By Triggering Agent

Suppress Until Acknowledged: ☒ Yes ☐ No

#### 4.1.6 User associates to Rogue AP

Trigger	
Type:	Device Event
Severity:	Normal

Conditions			
Matching conditions:		<input type="radio"/> All <input checked="" type="radio"/> Any	
Available Conditions: Event Contents, Event Type, SNMP Trap Category, Syslog Category, Syslog Severity			
<input type="button" value="Add"/> New Trigger Condition			
Option	Condition	Value	
Event Type	is	SNMP Trap	
Event Contents	matches	wlxxStaAssociatedToUnse cureAP	

Trigger Restrictions	
Folder:	Top
Include Subfolders:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Group:	- All Groups -

Alert Notifications	
Notes:	
<div></div>	
Additional Notification Options:	<input type="checkbox"/> Email <input type="checkbox"/> NMS
Add NMS servers on the <a href="#">AMP Setup NMS page</a>	
Logged Alert Visibility:	By Role
Suppress Until Acknowledged:	<input checked="" type="radio"/> Yes <input type="radio"/> No

## 5 Conclusion

This is a brief tutorial on some of the triggers I have used in the past. The possibilities are endless in my opinion and it all depends how you want to be alerted, what you want to be alerted on.

This tutorial simply shows SNMP traps but you can also be alerted on syslog messages.

Aruba MIB and Syslog guides are your best friend.