

Mist 検証手引き
PoC テストシナリオ Day2
- 運用 -

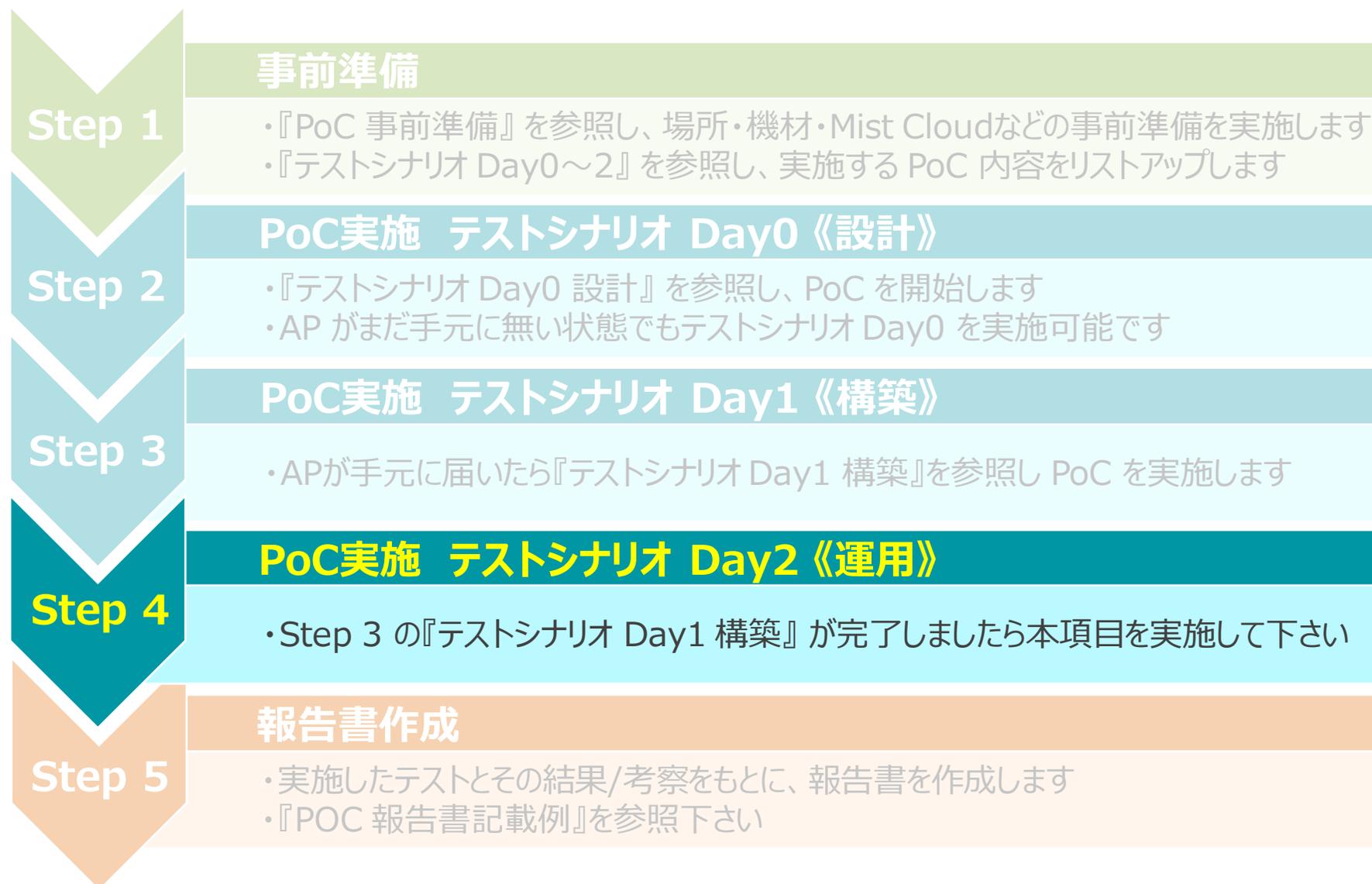
ジュニパーネットワークス株式会社
2022年11月 Ver 1.1

JUNIPER 
driven by Mist AI

はじめに

- ❖ 本資料は、PoC（検証）における Mist 独自の機能を利用した『運用』について記載しています
- ❖ PoC を実施する際の設定内容やパラメータは導入する環境や構成によって異なります
本資料では一例として PoC の準備、実施、報告までのシナリオを記載しております
- ❖ 設定内容の詳細は「ソリューション&テクニカル情報サイト」の Mist 日本語マニュアルをご確認ください
<https://www.juniper.net/jp/ja/local/solution-technical-information/mist.html>

準備から報告書作成までの全体の流れ



テストシナリオ Day2 《運用》

APとクライアントの可視化

ユーティリティ (テストツール)

ヒートマップ

SLE・RCA

認証失敗時のトラブルシューティング

RRM

電波干渉時の自動電波調整

Marvis

Marvis Action

ダイナミックパケットキャプチャ

アラート設定/Eメール通知

ネイバーAPと不正APの検出

レポート作成機能

AP ファームウェアの
マニュアルアップグレード

APの設置場所確認

AP 交換時の手順

APとクライアントの可視化

❖ Mist によるワイヤレスネットワークの可視化を確認します。

目的

AP やクライアントがどのように可視化されているのか確認します

手順

AP とクライアントの一覧表示や Insights 画面を確認します

参考マニュアル

[アクセスポイント 各種情報確認手順](#)

[アクセスポイント ログ確認手順](#)

[アクセスポイント アプリケーション通信 確認手順](#)

[アクセスポイント 接続クライアント 確認手順](#)

7 Access Points site Hatsudai

7 Access Points 0 Wireless Clients

100% Connection Status 100% VLANs 57

Filter

Status	Name	MAC Address	Site	IP Address
Connected	45.1.104	5c5b351e7e86	Hatsudai	10.233.45.123
Connected	FrontDesk	5c5b351e69dd	Hatsudai	102.168.20.10
Connected				

Monitor Wireless Wired WAN Location insights

access point 5c5b350e:bf:f1 Today

Site Live-Demo

Access Point Client Search by name or MAC

Switch 5c5b350e:bf:f1 5c5b350e:bf:f1

Gateway Collin AP1 d420b0c0:15:77

Wired Client LD_BC-Test 5c5b351e:c0:2b

Mist Edge LD_EBC 5c5b350e:3c:f5

LD_GPS_AP d420b080:ee:d4

LD_IDF_B_AP 5c5b353e:4e:ca

LD_JSW_AP d420b080:ef:60

LD_Kitchen 5c5b350e:06:6d

LD_Kitchen-2 d420b080:ef:01

LD_Marvis 5c5b3550:73:91

LD_MCB_AP 5c5b352f:57:89

LD_RS_Support 5c5b352f:5c:5c

LD_Sales_area 5c5b3550:03:cf

LD_Testbed_MD 5c5b358e:6f:ea

Simulated AP-1 5c5b351e:bf:9f

12:00 AM Feb 21 - 09:20 PM Feb 21

Total bytes 12:00 am 3:00 am 6:00 am

12:00 am - 12:10 am, Feb 21: Bytes: no data, 0.00 Mbps



APやクライアントが可視化されることで、運用管理やトラブル対応が効率化されます

APとクライアントの可視化

APと同様に、無線クライアントも可視化されます

1. [Clients] から [WiFi Clients] を選択し、
接続しているクライアントの一覧を確認します

	IPv4 Address	MAC Address	Device Type
<input type="checkbox"/>	android-d626bc4af02417ce	192.168.1.64	40:83:de:de:d5:7b Zebra TC51
<input type="checkbox"/>	LAPTOP-8H85JO35	192.168.1.80	68:ec:c5:09:2e:87 ThinkPad X1 C

2. [Monitor] から [Insights] を選択し、
[Client] の項目から、対象のクライアントの選択します
ログや使用したアプリケーション等の詳細を確認します

	Site	Access Point	Client	Switch	WAN Edge	Wired Client	Mist Edge
	Live-Demo						
			aconcagua				b8:27:eb:cc:0d:49
			Alejandro				34:af:b3:e9:83:57
			android-3aa38bbf31a27...				fe:40:4a:0d:f6:37
			android-3aa38bbf31a27...				94:fb:29:a6:7c:48
			android-d626bc4af0241...				40:83:de:de:d5:7b
			anselmallenj-mbp				bc:d0:74:5b:53:2f
			Apple				b2:2e:28:3c:21:64
			Apple				06:80:4b:4d:57:c5
			Apple				46:94:22:f4:6d:a5
			Apple				36:83:fe:64:af:80
			APPLICON				00:00:40:00:40:ff
			ashinde				00:91:9e:31:84:a4
			bvargas-T14				58:6c:25:5c:29:57
			denali				50:32:37:ea:c3:c2
			everest				50:32:37:e8:72:7e
			Falaks-MBP				34:36:3b:cf:8b:1e

APとクライアントの可視化

APと無線クライアントの可視化

- APや無線クライアントの一覧表示では、一覧で表示する内容をカスタマイズ出来ます
これにより、素早く確認したい情報を、簡単にピックアップする事ができます

The image shows a screenshot of a network management interface. On the left, a table displays wireless clients with columns for 'Device Type' and 'AP Name'. A red box highlights a menu icon in the top right corner of the table. An arrow points from this icon to a 'Table Settings' dialog box on the right. The dialog box has an 'Auto Refresh' section with options 'Off', '5 sec', '10 sec', and '30 sec'. Below this, there are 38 numbered items, each with a checkbox and a label. The checked items are: 1. User, 4. IPv4 Address, 7. Device Type, 11. AP Name, 14. SSID, and 37. Pre-shared Key.

Device Type	AP Name
7548 Zebra TC72	Collins

Auto Refresh		
Off	5 sec	10 sec 30 sec
1. <input checked="" type="checkbox"/>	User	2. <input type="checkbox"/> Connected Time
3. <input type="checkbox"/> Idle Time	4. <input checked="" type="checkbox"/> IPv4 Address	5. <input type="checkbox"/> IPv6 Addresses
6. <input checked="" type="checkbox"/> MAC Address	7. <input checked="" type="checkbox"/> Device Type	8. <input type="checkbox"/> Hostname
9. <input type="checkbox"/> Device OS	10. <input type="checkbox"/> SDK Version	11. <input checked="" type="checkbox"/> AP Name
12. <input type="checkbox"/> AP MAC	13. <input type="checkbox"/> BSSID	14. <input checked="" type="checkbox"/> SSID
15. <input type="checkbox"/> Authorized	16. <input type="checkbox"/> Protocol	17. <input type="checkbox"/> Security
18. <input type="checkbox"/> Channel	19. <input type="checkbox"/> Band	20. <input type="checkbox"/> RSSI
21. <input type="checkbox"/> SNR	22. <input type="checkbox"/> RX Bit Rate	23. <input type="checkbox"/> TX Bit Rate
24. <input type="checkbox"/> Total Bytes	25. <input type="checkbox"/> RX Bytes	26. <input type="checkbox"/> TX Bytes
27. <input type="checkbox"/> Total Packets	28. <input type="checkbox"/> RX Packets	29. <input type="checkbox"/> TX Packets
30. <input type="checkbox"/> Total Retries	31. <input type="checkbox"/> RX Retries	32. <input type="checkbox"/> TX Retries
33. <input type="checkbox"/> Labels	34. <input type="checkbox"/> Username	35. <input type="checkbox"/> Vlan ID
36. <input type="checkbox"/> Last Seen	37. <input checked="" type="checkbox"/> Pre-shared Key	38. <input type="checkbox"/> Classification

ユーティリティ (テストツール)

❖ ユーティリティ (テストツール) を使用し疎通確認を行います。

目的

Utility の [Testing Tools] を使用し、AP からクライアント、AP からインターネット等への疎通確認を実施します

手順

以下のマニュアルを参考に、Testing Tools を使用した試験を行います

[アクセスポイント Ping実施手順](#)

[アクセスポイント Traceroute実施手順](#)

[アクセスポイント ARP 確認手順](#)

The screenshot displays the 'AP Testing Tools' interface. At the top, there are three tabs: 'Ping', 'Traceroute', and 'ARP'. The 'Ping' tab is selected, and the 'Hostname' field contains '162.159.200.123' with a 'Ping' button next to it. Below the input fields, the output of the ping test is shown in a dark terminal window. The output indicates that 10 packets were sent and received successfully, with round-trip times ranging from approximately 54.885 ms to 55.116 ms. The 'ARP' tab is also visible, showing a table of ARP entries.

DEV	Src MAC	Dest MAC	Source IP	Dest IP
aximac0	00-10-db-ff-50-02	5c-5b-35-1e-7e-86	54.219.74.133	
aximac0	00-10-db-ff-50-02	5c-5b-35-1e-7e-86	162.159.200.123	
aximac0	00-10-db-ff-50-02	5c-5b-35-1e-7e-86	162.159.200.123	
vlan1	5c-5b-35-1e-7e-86	00-10-db-ff-50-02	10.233.45.123	
vlan1	5c-5b-35-1e-7e-86	00-10-db-ff-50-02	10.233.45.123	



ping や traceroute など、GUI上で L3 レベルの疎通確認を簡単に実施できます

ヒートマップ

❖ ヒートマップを確認します。

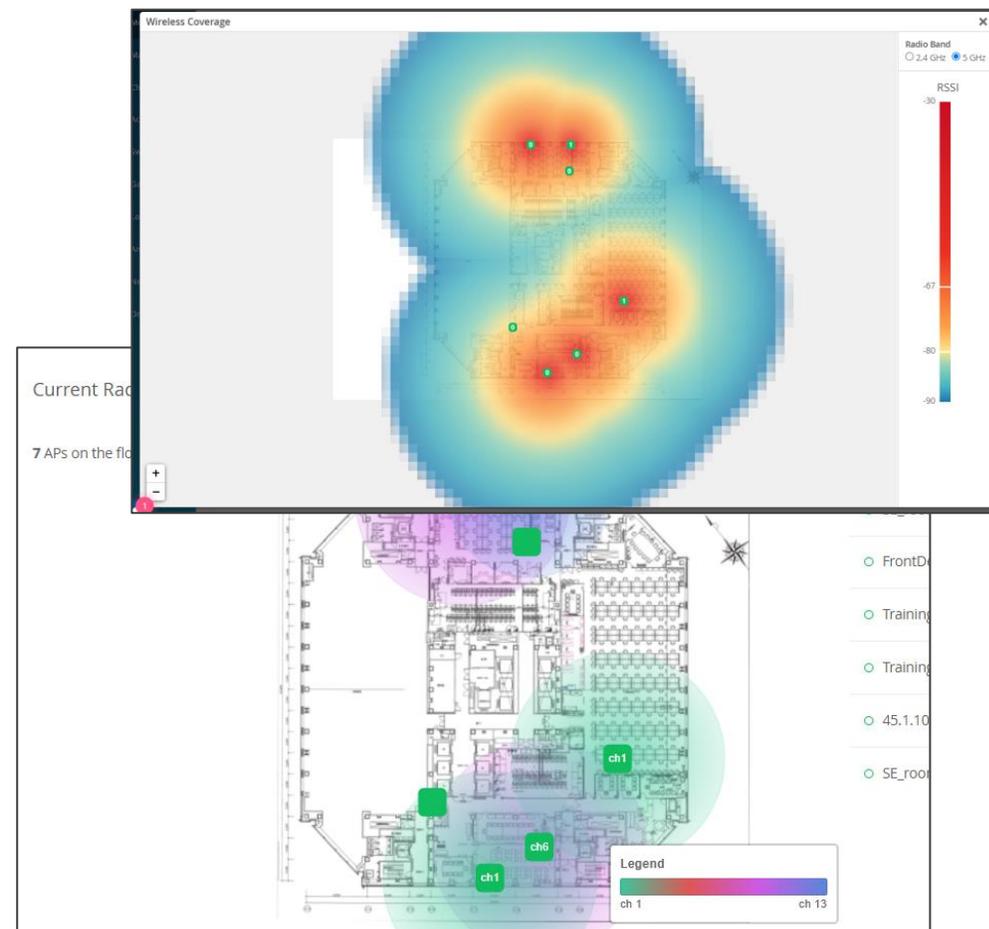
目的

電波の強度、カバレッジ、使用チャンネルなどの情報はヒートマップに視覚的に一目で確認することができます

手順

マニュアルを参照し、ヒートマップを確認します

[ヒートマップ 確認手順](#)



クライアントの電波受信強度では、訪問者が使用するゲストクライアントをリアルタイムに表示し、訪問者が不満なく通信が行えているのが確認することができます

SLE ・ Root Cause Analysis

- ❖ SLE および Root Cause Analysis によってネットワークの品質が可視化されます。

目的

SLE および Root Cause Analysis によって、
どのように無線ネットワークの品質が可視化されるのかを確認します

検証手順

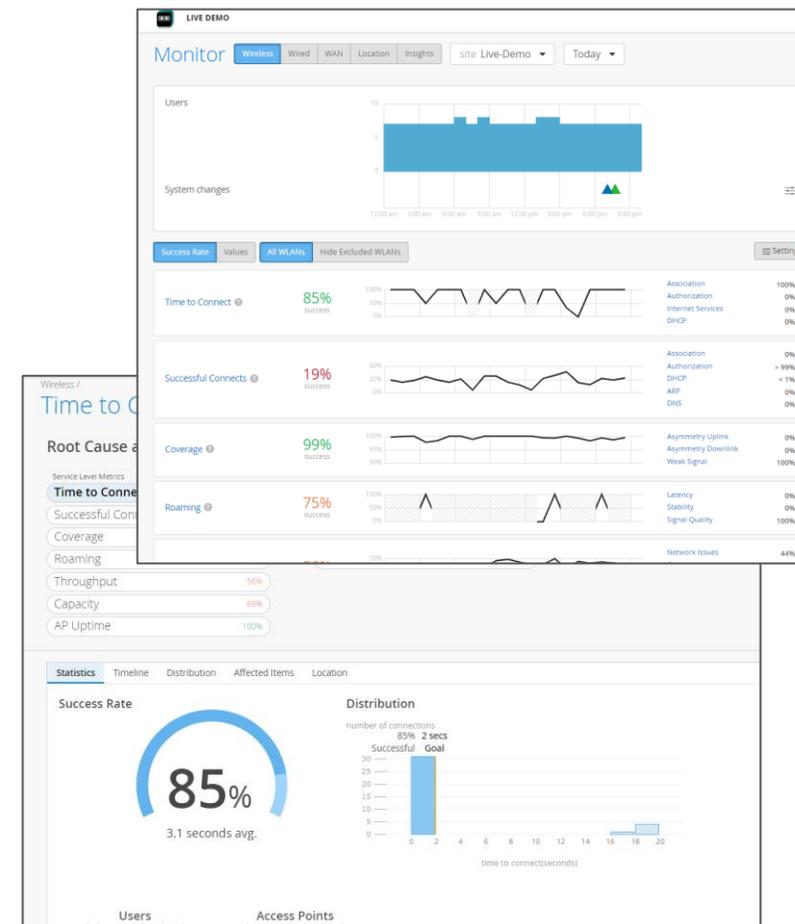
① 正常状態の確認

参考マニュアル

[Mist Wi-Fi Assurance SLE \(Service Levels Expectation\)](#)

② トラブルシューティング

PSK 認証または 802.1x 認証失敗時のSLE表示を確認します
Radius サーバを利用している環境のみ802.1x認証が可能です



SLE により、視覚的にも分かりやすく、どこで・どのような問題が発生しているのか確認することができます
また、Root Cause Analysis によりさらにその問題の詳細が確認可能です

PSK 認証失敗時のトラブルシューティング

❖ 疑似トラブルを発生させ、PSK 認証失敗時の SLE を確認します

• 検証方法：

ネットワーク接続時に、わざとパスワードを間違えネットワーク接続を失敗させます

以下のマニュアル参照し、認証失敗時の SLE を確認します

※環境によって SLE への結果の反映は時間がかかることがあります

[認証エラー 確認手順 \(拠点単位\)](#)

[認証エラー 確認手順 \(クライアント単位\)](#)

PSK 認証失敗時のトラブルシューティング

❖ 疑似トラブルを発生させ、PSK 認証失敗時の SLE を確認します

• 結果 :

Client Events にて以下のログが出力されます

Event title : [Authorization Failure](#)



The screenshot displays the 'Client Events' section of a network management interface. It shows a summary of 20 total events, with 12 Good, 5 Neutral, and 3 Bad. A table lists three events: two 'Authorization Failure' events and one 'DHCP Denied' event. The first 'Authorization Failure' event is selected, showing detailed information in a right-hand pane. This pane includes fields for AP (AP43), Reason (2), RSSI (-46 dBm), Protocol (802.11ac), Band (5 GHz), and Description (Reason code 2 'Previous authentication no longer valid' WPA 4way handshake timeout(15)). Other fields include Last Association (4.0 sec ago), BSSID (d4:20:b0:e4:a8:6c), SSID (Mist), Number of Streams (1), Capabilities (80Mhz/40Mhz), and Channel (108).

Client Events			20 Total	12 Good	5 Neutral	3 Bad
Authorization Failure ⓘ	AP43	02:31:35.657 PM, Mar 8	AP	AP43	Last Association	4.0 sec ago
Authorization Failure ⓘ	AP43	02:29:27.781 PM, Mar 8	Reason	2	BSSID	d4:20:b0:e4:a8:6c
DHCP Denied ⓘ	AP43	09:53:54.355 AM, Mar 8	RSSI	-46 dBm	SSID	Mist
			Protocol	802.11ac	Number of Streams	1
			Band	5 GHz	Capabilities	80Mhz/40Mhz
			Description	Reason code 2 "Previous authentication no longer valid" WPA 4way handshake timeout(15).	Channel	108

802.1x 認証失敗時のトラブルシューティング（Radius サーバ利用）

❖ 疑似トラブルを発生させ、802.1x 認証失敗時の SLE を確認します

• 検証方法：

ネットワーク接続時に、わざとパスワードを間違えネットワーク接続を失敗させます

以下のマニュアル参照し、認証失敗時の SLE を確認します

※環境によって SLE への結果の反映は時間がかかることがあります

[認証エラー 確認手順（拠点単位）](#)

[認証エラー 確認手順（クライアント単位）](#)

802.1x 認証失敗時のトラブルシューティング（Radius サーバ利用）

❖ 疑似トラブルを発生させ、802.1x 認証失敗時の SLE を確認します

• 結果：

Client Events にて以下のログが出力されます

Event title : [Authorization Failure](#)

The screenshot displays the 'Client Events' interface. At the top, it shows a summary: '40 Total', '23 Good', '10 Neutral', and '7 Bad'. The 'Bad' count is highlighted in blue. Below this is a table of events:

Event Title	AP	Time
Authorization Failure	AP43	02:55:58.304 PM, Mar 8
Authorization Failure	AP43	02:55:55.794 PM, Mar 8
DHCP Denied	AP43	02:55:34.533 PM, Mar 8
Authorization Failure	AP43	02:55:17.201 PM, Mar 8
Authorization Failure @	AP43	02:31:35.657 PM, Mar 8
Authorization Failure @	AP43	02:29:27.781 PM, Mar 8
DHCP Denied @	AP43	09:53:54.355 AM, Mar 8

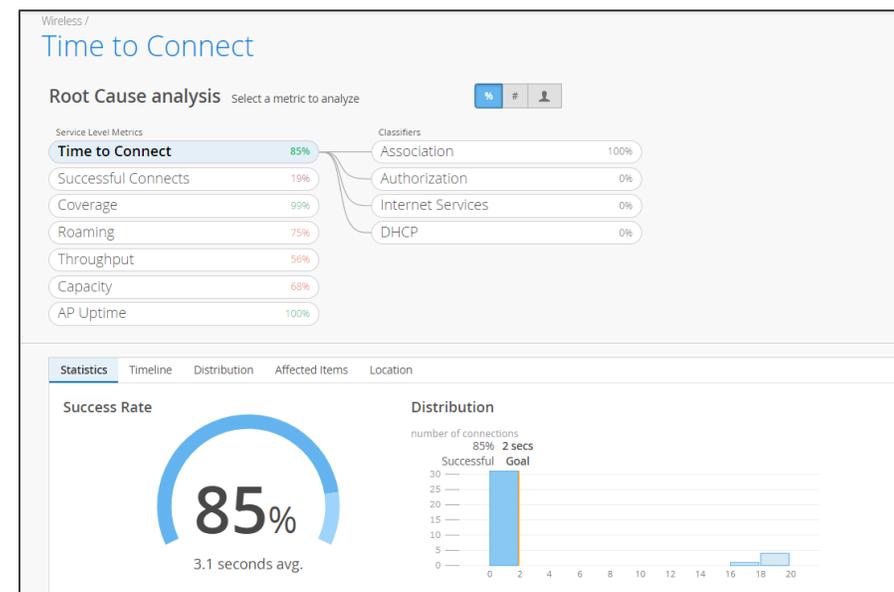
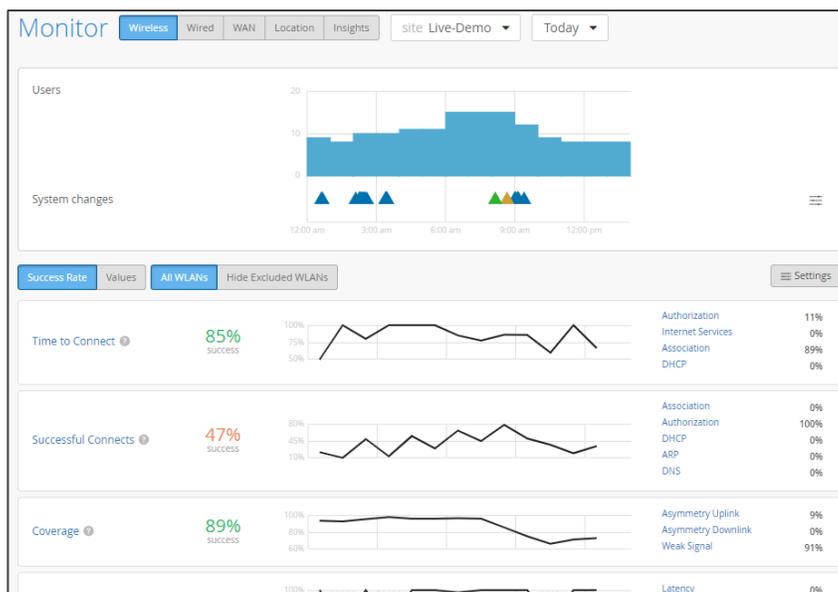
The selected event, 'Authorization Failure', is expanded to show details:

Field	Value
AP	AP43
Last Association	1.2 sec ago
Reason	23
RSSI	-40 dBm
Protocol	802.11n
Band	2.4 GHz
Channel	6
Auth Server IP Address	192.168.0.5
Server Port	1812
BSSID	d4:20:b0:e4:a8:81
SSID	radius
Number of Streams	2
Description	Reason code 23 "IEEE 802.1X authentication failed" AP deauthenticate STA, before authorization complete(771). 802.1x Auth Fail(23).

SLE · Root Cause Analysis

❖ SLE および Root Cause Analysis の考察

- SLE により、視覚的にも分かりやすく、どこで・どのような問題が発生しているのか確認することができます
また、Root Cause Analysis によりさらにその問題の詳細が確認可能です
これにより、障害解析スキルがなくても、スムーズな障害解析が可能になります
- 検索機能が優れており、ユーザー・端末から絞り込み、短時間で問題の要因を確認できます



RRM

❖ RRM（無線情報:Radio Resource Management）を確認します。

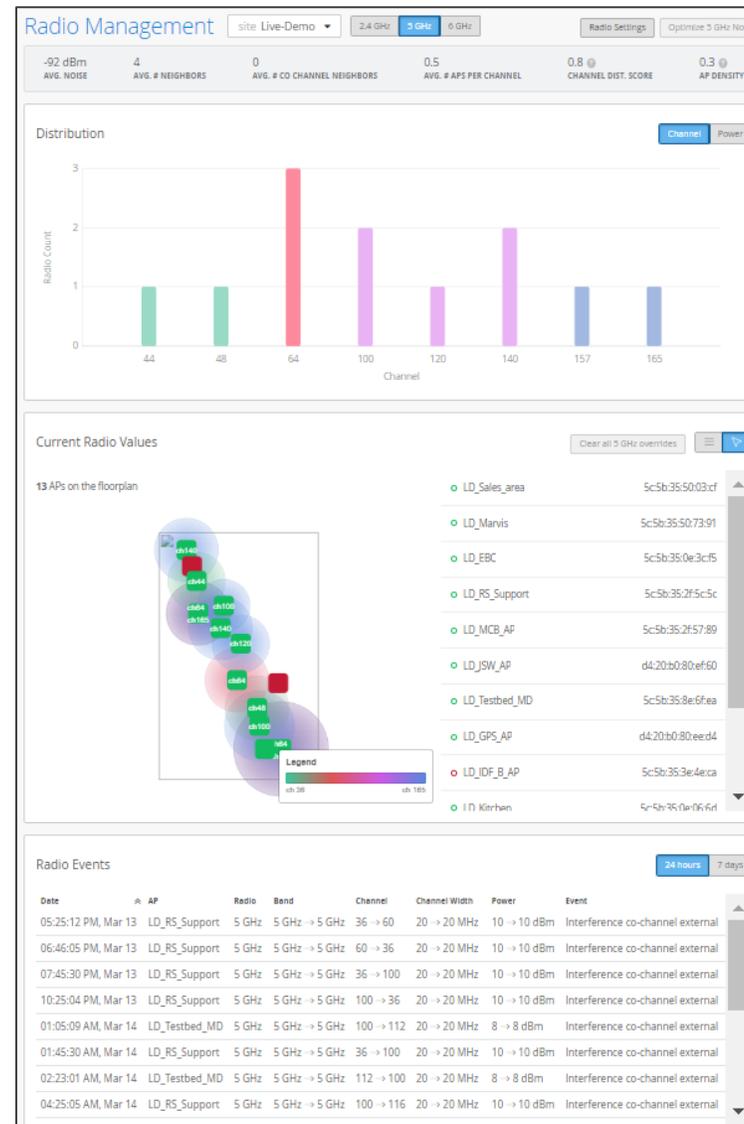
目的

RRM の表示内容を確認します

手順

以下のマニュアルを参考に、RRM を確認します

[無線情報\(RRM\) 確認手順](#)



電波の統計情報や各 AP の電波状況など詳細に確認できます

RRM 電波干渉時の自動電波調整

- ❖ 疑似的に電波を干渉させ、Mist が自動的に電波を調整しチャンネルが変更されることを確認します。

目的

Mist の電波自動調整機能を確認します

検証手順

電波干渉試験

「AP_01」と同一のチャンネルを「AP_02」に手動設定し

「AP_01」が自動的にチャンネルを変更する過程を確認します

(※手順の詳細は次項に記載)

結果

チャンネルが自動調整され、ログに記載されます

	Band	Channel	Channel Width	Power
z	5 GHz → 5 GHz	108 → 149	20 → 20 MHz	9 → 10 dB
z	5 GHz → 5 GHz	149 → 40	20 → 20 MHz	9 → 9 dBm
z	5 GHz → 5 GHz	48 → 165	20 → 20 MHz	10 → 8 dB
z	5 GHz → 5 GHz	36 → 161	20 → 20 MHz	8 → 8 dBm
z	Disabled → 5 GHz	128 → 128	20 → 20 MHz	8 → 11 dB
z	5 GHz → 5 GHz	56 → 56	20 → 20 MHz	13 → 14 dB



自動的に電波調整され、空いてるチャンネルに切り替えることで、効率よく通信を行います

RRM 電波干渉時の自動電波調整

1. AP のチャンネルを最適化します

[Site] の [Radio Management] を開きます

帯域を [5GHz] に合わせ、[Optimize 5 GHz Now] をクリックするとチャンネルが最適化されます

The screenshot shows the Juniper NMS interface for Radio Management. The left sidebar has 'Site' highlighted. The main menu has 'Radio Management' highlighted. The top navigation shows '2.4 GHz', '5 GHz' (selected), and '6 GHz'. The 'Optimize 5 GHz Now' button is highlighted. The main content area shows metrics: 0 AVG. # CO CHANNEL NEIGHBORS, 0.5 AVG. # APS PER CHANNEL, 1.0 CHANNEL DIST. SCORE, and 0.2 AP DENSITY. A bar chart below shows channel usage for various channels, with the 5 GHz channel showing the highest usage.

RRM 電波干渉時の自動電波調整

2. AP-01 のチャンネルを確認します

[Radio Management] の「Current Radio Values」の項目で AP_01 の Channel を確認します

この画像では「100+104」となってます



RRM 電波干渉時の自動電波調整

3. AP-02 のチャンネルを固定します

[Access Points] から「AP_02」を選択し AP の設定画面を開きます

「5 GHz Configuration」の項目にて、前項で確認した「AP_01」で使用中の Channel に変更します

(デフォルトの設定では「Use site setting」になっています)

	Status	Name	MAC Address	Site	IP Address
<input type="checkbox"/>	Connected	AP_01	5c:5b:35:be:2b:25	新宿 (本社)	192.168.1.1
<input type="checkbox"/>	Connected	AP_02	5c:5b:35:be:2b:de	新宿 (本社)	192.168.1.2

以下の値に変更します

Enable : Yes

Channel Width : 40 MHz

Channel : AP_01 の Channel

5 GHz Configuration
See Radio Management for site settings

Enable	Yes
Channel Width	40 MHz
Channel	100 (dfs)
Power	<input type="range"/>

Use site setting

RRM 電波干渉時の自動電波調整

4. 再度 AP のチャンネルを最適化します

AP_02 の設定変更内容を反映させるため、再度 [Site] の [Radio Management] を開きます
帯域を [5GHz] に合わせ、[Optimize 5 GHz Now] をクリックしチャンネルを最適化させます

The screenshot shows the Juniper Mist Radio Management interface. The left navigation menu has 'Site' highlighted. The main area displays 'Radio Management' for 'site Live-Demo'. The frequency selection is set to '5 GHz'. The 'Optimize 5 GHz Now' button is highlighted. The interface shows four metrics: 'AVG. # CO CHANNEL NEIGHBORS' (0), 'AVG. # APS PER CHANNEL' (0.5), 'CHANNEL DIST. SCORE' (1.0), and 'AP DENSITY' (0.2). A bar chart at the bottom shows channel usage for various APs, with a 'Channel' button selected.

RRM 電波干渉時の自動電波調整

5. 2台の AP が同じ Channel になっていることを確認します

Current Radio Values Clear all 5 GHz over

	Name	MAC Address	Status	Radio	No. Clients	Channel	Channel Width	Power	Radio Enabled
^	AP_01	5c:5b:35:be:2b:25	Connected	5 GHz	1	100+104	40 MHz	14 dBm	Yes
^	AP_02	5c:5b:35:be:2b:de	Connected	5 GHz	0	100+104	40 MHz	18 dBm	Yes

6. クライアントから通信を行います

AP_01 もしくは AP_02 にクライアントを Wi-Fi 接続し通信を行います

出来るだけ帯域を使用し、継続的に通信を行うために動画再生等の通信を行ってください



RRM 電波干渉時の自動電波調整

7. Channel が変更されたことを確認します

[Site] の [Radio Management] を開き、「Current Radio Values」および「Radio Events」の Channel の項目で AP_01 の Channel が変更されていることが確認できます

Current Radio Values											Clear all 5 GHz
Name	MAC Address	Status	Radio	No. Clients	Channel	Channel Width	Power	Radio Enabled	Config Over		
AP_01	5c:5b:35:be:2b:25	Connected	5 GHz	2	60+64	40 MHz	14 dBm	Yes	No		
AP_02	5c:5b:35:be:2b:de	Connected	5 GHz	2	100+104	40 MHz	18 dBm	Yes	Yes		

Date	AP	Radio	Band	Channel	Channel Width	Power	Event
11:58:55 AM, Mar 16	AP_01	5 GHz	5 GHz → 5 GHz	100 → 60	40 → 40 MHz	14 → 15 dBm	Triggered site RRM
11:58:55 AM, Mar 16	AP_02	5 GHz	5 GHz → 5 GHz	100 → 100	40 → 40 MHz	18 → 16 dBm	Triggered site RRM
11:42:54 AM, Mar 16	AP_01	5 GHz	5 GHz → 5 GHz	52 → 100	40 → 40 MHz	14 → 14 dBm	Interference AP non wifi
11:20:53 AM, Mar 16	AP_01	5 GHz	5 GHz → 5 GHz	100 → 52	40 → 40 MHz	15 → 15 dBm	Triggered site RRM

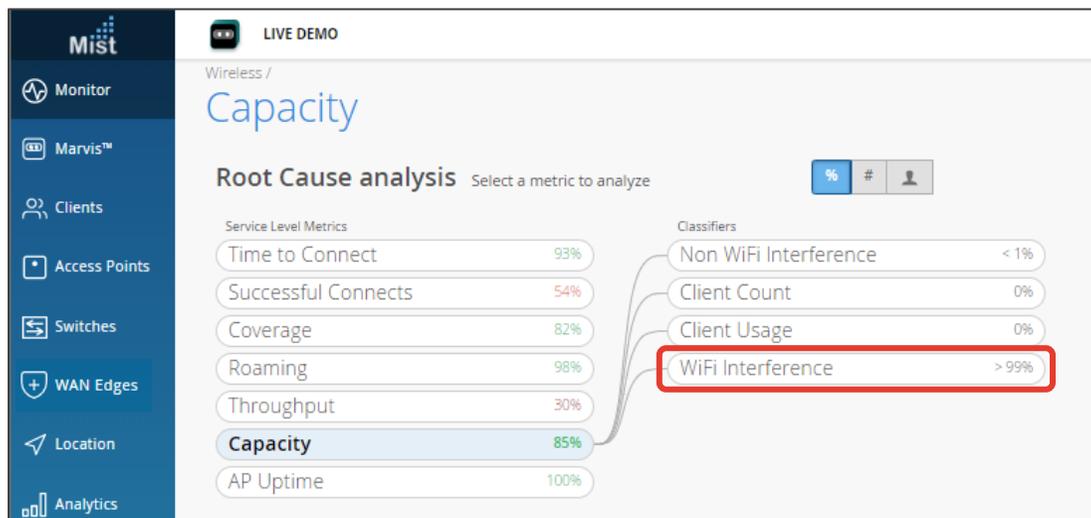
RRM 電波干渉時の自動電波調整

8. 以下のマニュアルを参考に、電波干渉の有無を特定します

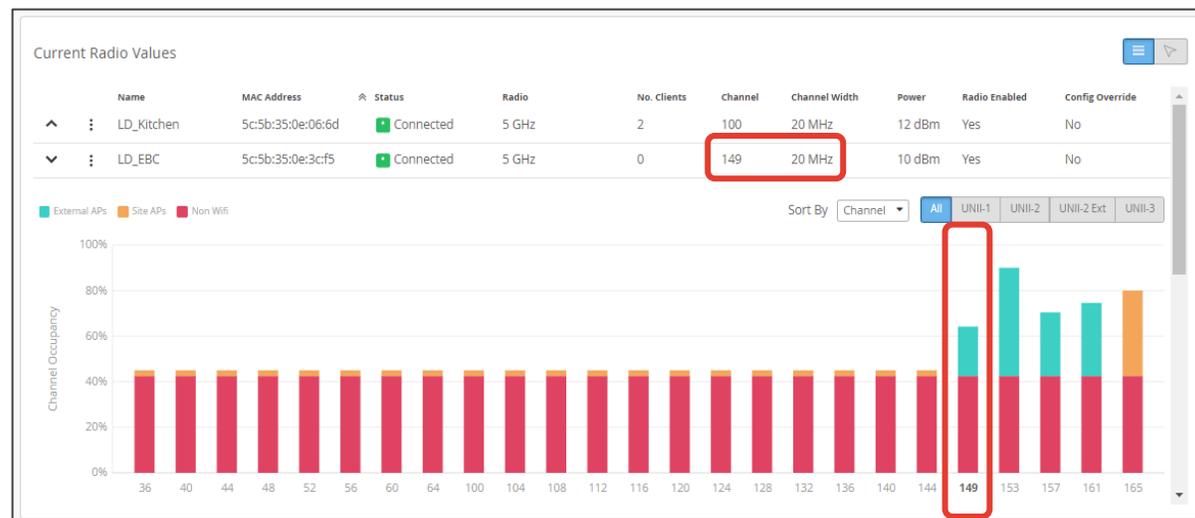
[電波干渉 有無の確認手順（拠点単位）](#)

[電波干渉 有無の確認手順（クライアント単位）](#)

❖ SLE の Capacity で Wi-Fi Interference の割合が増加していることを確認



❖ [Site] の [Radio Management] で自身の利用するチャンネルにSite APsの割合が高いことを確認



RRM 電波干渉時の自動電波調整

❖ RRM および自動電波調整についての考察

- 自動的に電波調整され、空いてるチャンネルに切り替えることで、効率よく通信を行います
 - カバレッジ、容量、スループット、パフォーマンスなどの RF 情報や問題をユーザーごとに常に収集
 - ディープラーニングにてデータを理解
 - リアルタイムの要件に基づいて自動変更を実施
 - Wi-Fi サービス品質が常に最適化されるように、これらの変更の影響を測定このプロセスにより “self-healing (自己修復) WLAN” を提供します
- これは、世界初の、唯一 Mist のみが発現した、RRM の革新です
- 本シナリオでは Channel の自動調整を確認するために、AP の Channel を固定しましたが、通常の運用で特別な理由が無い限り Channel の固定を行う事はありません

Marvis

❖ Marvis は Mist Cloud が提供している AI です。

目的

Marvis に問い合わせを行い、その結果を確認します

検証方法

Marvis への問い合わせ例 :

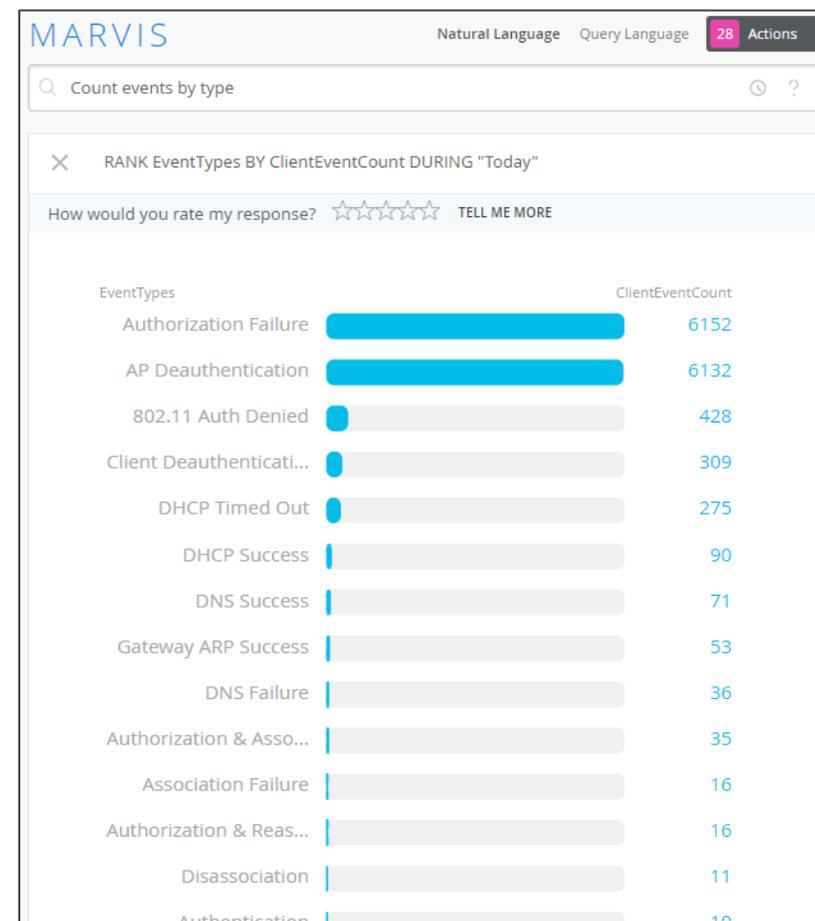
MAC アドレスのリスト化・・・「List MAC addresses」と入力

タイプ別イベントのリスト化・・・「Count events by type」と入力

参考URL :

<https://www.mist.com/resources/mist-marvis-overview/>

<https://manage.mist.com/admin/vnadocs.html>



Marvisは、自然言語処理、会話型インターフェイスにより、運用の効率化に役立てることができます

Marvis Action

- ❖ Marvis Action で対処すべき問題を特定し、解決方法を提案します。

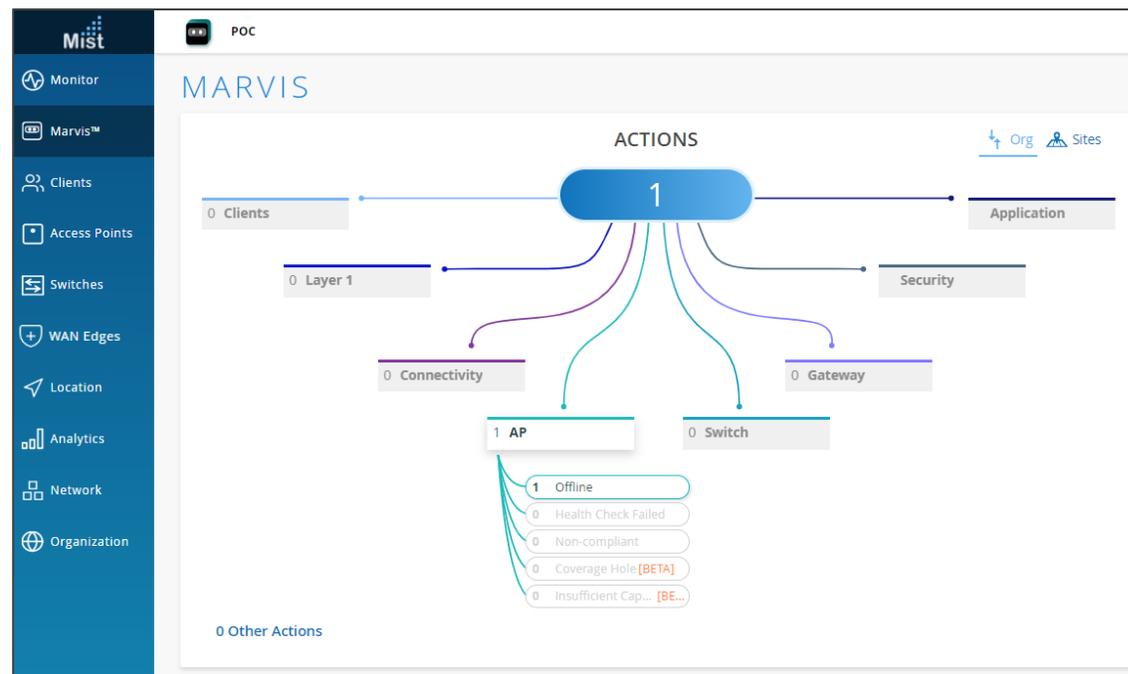
目的

Marvis Action で対処すべき問題を特定し、
解決方法を確認します

検証方法

参考URL :

<https://www.mist.com/documentation/category/marvis-actions/>



Marvis Action は、問題が発生する前に予測したり、トラブル解決に役立ちます

Marvis

❖ Marvis および Marvis Action についての考察

- Marvis は、自然言語処理、会話型インターフェイス、規定のアクション、内蔵されたヘルプデスク機能により、クライアントからクラウドまでの各領域で、洞察力と自動化を提供し、運用を効率化し最適化します
- AIにより、データが取り込まれるにつれて継続的に学習し、増大した知識を活用して問題をリアルタイムで発生前に修正したり、問題が発生する前に予測したり、トラブルチケットを解決します
- クライアントレベルのネットワークビューを表示し、エンドユーザーのデバイスから直接イベントをキャプチャします
- 検証された Mist AI ドリブンサポートにより、ユーザーによって作成されるチケットを最大90%減少させることが可能
- リアルタイムのインサイト、クライアント、デバイス、およびサイトレベルでのトラブルシューティングを簡素化し、サービス品質を向上します

ダイナミック パケットキャプチャー

❖ Mistでは問題発生時に必要になるキャプチャーデータを自動的に取得しています

目的

自動取得されたキャプチャーデータを確認します

検証方法

記録されている Bad Event のキャプチャーデータをダウンロードして確認
します

CloudShark (有料)を契約している場合は、WEB でも確認できます

参考マニュアル :

[CloudSharkの利用](#)

Client Events	86 Total	75 Good	5 Neutral	6 Bad
Success				
Authorization & Association	LD_Sales_area	12:35:13.799 PM, Jul 9		
11r FBT Failure	LD_Kitchen	12:32:36.778 PM, Jul 9		
DNS Success	LD_EBC			
Gateway ARP Success	LD_EBC			
11r Reassociation	LD_EBC	12:32:26.689 PM, Jul 9		
11r Reassociation	LD_Kitchen	12:32:07.158 PM, Jul 9		
11r Reassociation	LD_EBC	12:31:51.069 PM, Jul 9		
DNS Success				

AP	LD_Kitchen
RSSI	-85 dBm
Band	5 GHz
Description	Status code 79 "Transmission failure"

CloudShark(有料)

No.	Time	Source	Destination	Protocol	Length	Info
44	2022-10-18 07:23:19.5...	0.0.0.0	255.255.255.255	BOOTP	176	Boot Request from 26:25:d5:02:dd:90
45	2022-10-18 07:23:19.6...	26:25:d5:02:dd:90	Mist_e4:a8:61	802.11	71	Null function (No data), SN=2742
46	2022-10-18 07:23:19.7...	26:25:d5:02:dd:90	Mist_e4:a8:61	802.11	71	Null function (No data), SN=2743
47	2022-10-18 07:23:19.7...	fe80::bf:809b:46db::...	ff02::fb	MDNS	176	Standard query 0x0000[Malformed]
48	2022-10-18 07:23:19.7...	fe80::bf:809b:46db::...	ff02::fb	MDNS	171	Standard query 0x0000 PTR lb...
49	2022-10-18 07:23:19.7...	26:25:d5:02:dd:90	Mist_e4:a8:61	802.11	71	Null function (No data), SN=2744

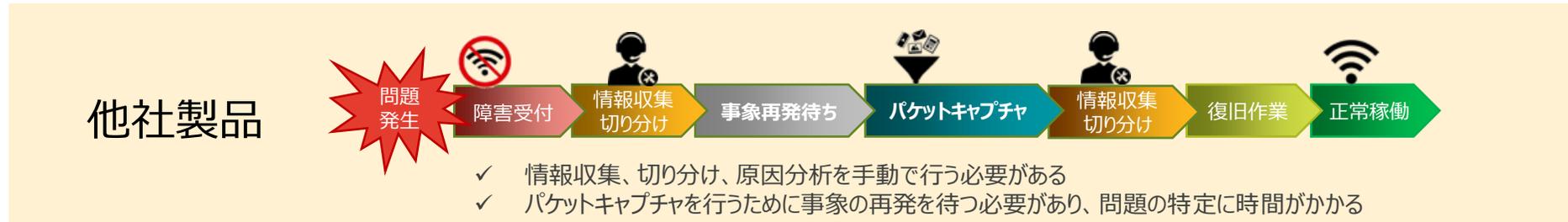


事象再発を待つ必要がなく、迅速な問題解決を可能にします

ダイナミック パケットキャプチャー

❖ ダイナミックパケットキャプチャーの考察

- すべてのパケットのヘッダ情報のみが Mist Cloud に送信されています (ペイロード部はセキュリティ上の理由のため収集されません)
- SLE を下回るなど必要と判断された場合、パケットが保存され Mist Cloud で確認できます
- 同一または類似事象の重複したパケットは破棄される場合があります
- 必要な情報が収集されているため、事象の再現待ちは不要です



アラート設定/Eメール通知

❖ 検知したいアラートを設定し、必要に応じてメール通知を設定することができます

目的

アラートの設定とアラート通知メールを確認します

検証手順

1. アラート通知メールの対象範囲と通知先を設定します
2. Device offline のしきい値を5分に設定します
3. AP からケーブルを抜線します

結果

アラート内容がメール通知されます

Alert	Recur
Client Connection to rogue AP detected	1
Rogue AP detected	1
	1
	1
r Added	1
ogue AP detected	2
	1
ogue AP detected	2

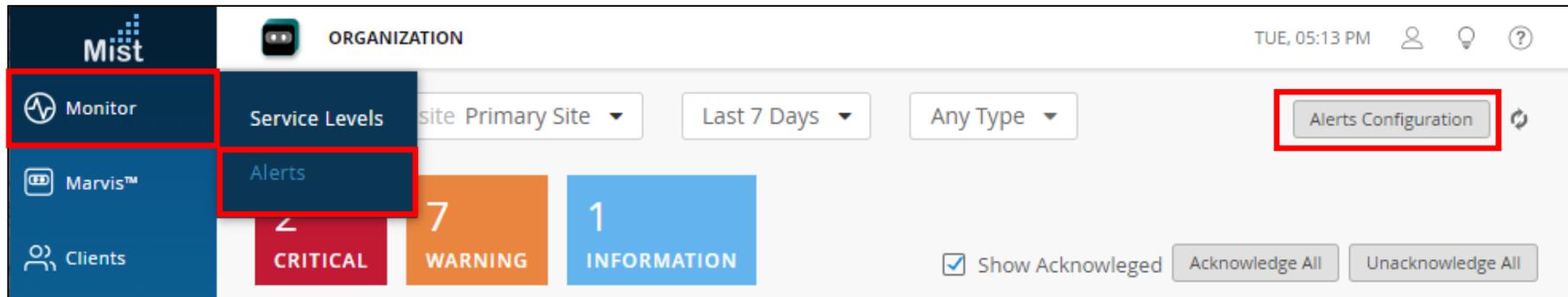


50種以上のアラートが設定できます
テンプレート機能を使うことで、管理者やSite別に検知項目をカスタマイズできます

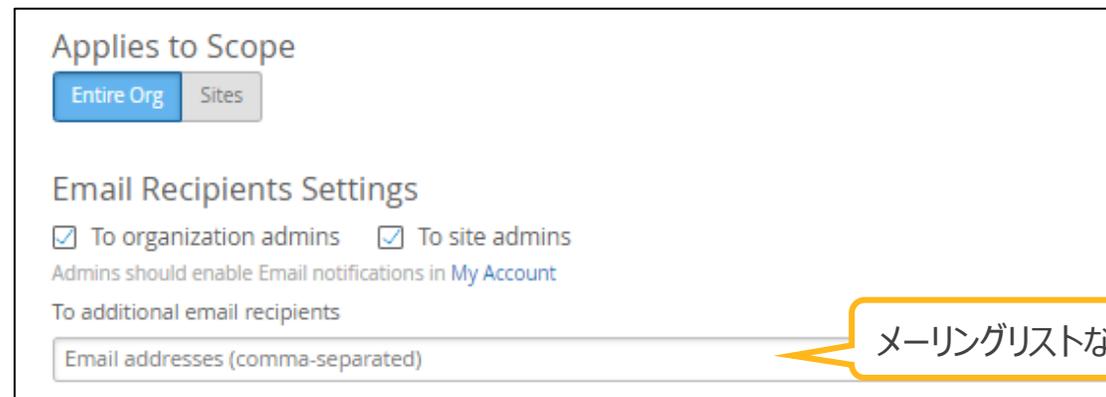
アラート設定/Eメール通知

❖ アラート通知メールの対象範囲と通知先を設定します

1. [Monitor] から [Alerts] を選択し、[Alerts Configuration] をクリックします



2. メール通知対象範囲 (Organization全体、各サイト) と通知先を設定します

A screenshot of the 'Alerts Configuration' form. The 'Applies to Scope' section has two radio buttons: 'Entire Org' (selected) and 'Sites'. The 'Email Recipients Settings' section has two checked checkboxes: 'To organization admins' and 'To site admins'. Below these is a note: 'Admins should enable Email notifications in My Account'. There is a text input field for 'To additional email recipients' with the placeholder text 'Email addresses (comma-separated)'. A yellow callout bubble points to this field.

メーリングリストなども通知先として登録可能です

アラート設定/Eメール通知

❖ アラート通知メールの対象範囲と通知先を設定します

3. Alert Types の項目から “Device offline” のアラートとメール通知にチェックを入れ、しきい値を「5分」で設定します

Alerts	Enable Alert	Send Email Notification
Infrastructure	<input type="checkbox"/>	<input type="checkbox"/>
ARP Failure (beta)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
DHCP Failure (beta)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Switch restarted	<input type="checkbox"/>	<input type="checkbox"/>
Virtual Chassis Member Added	<input type="checkbox"/>	<input type="checkbox"/>
Device offline (alert after 2 minutes when device offline 	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Gateway DHCP Pool Exhausted	<input type="checkbox"/>	<input type="checkbox"/>

Device offline for minutes

This is a global setting - it applies to all Device Offline alerts in the entire organization

アラート設定/Eメール通知

❖ APを切り離しアラート通知メールを確認します

4. AP からケーブルを抜線します

登録したメールアドレスに送付されたアラート通知メールを確認します



From : no-reply@mist.com

Subject : [Mist.com] Alert Device offline in サイト名

ネイバーAPと不正APの検出

❖ ネイバーAPと不正APを検出します。

目的

ネイバーAPと不正APを検出し、Mist AP 以外も可視化します
不正APが検出された場合はクライアントの接続をブロックします

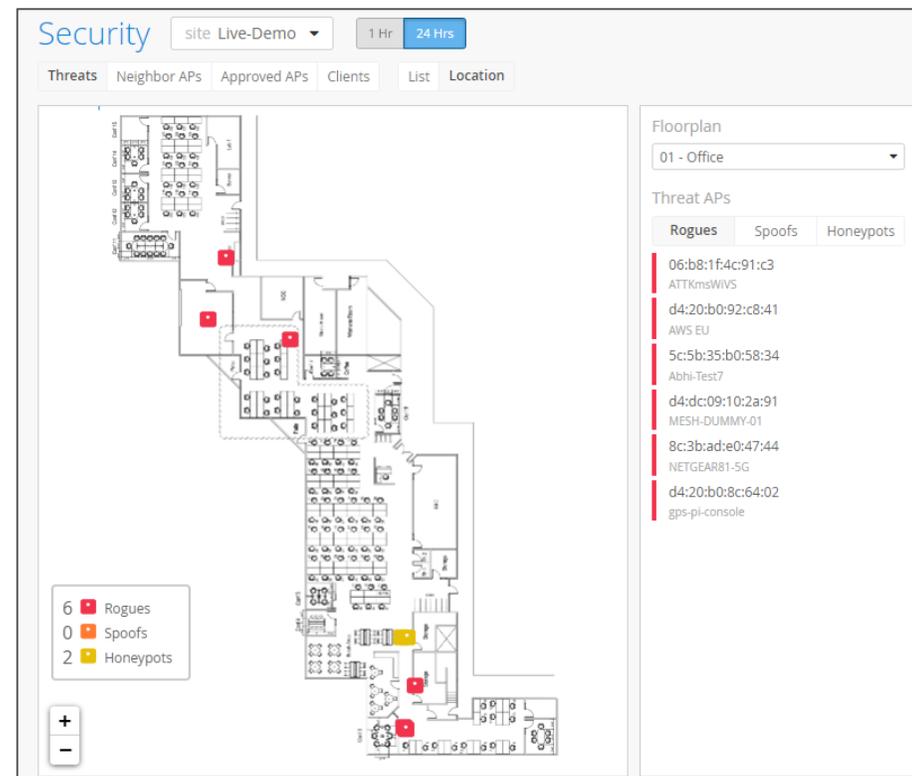
検証方法

マニュアルを参照し、ネイバーAPと不正APを確認します

[周囲のAP, SSID情報 確認手順](#)

[サイトの設定 不正APの検出](#)

(※詳細な手順は次項に記載)



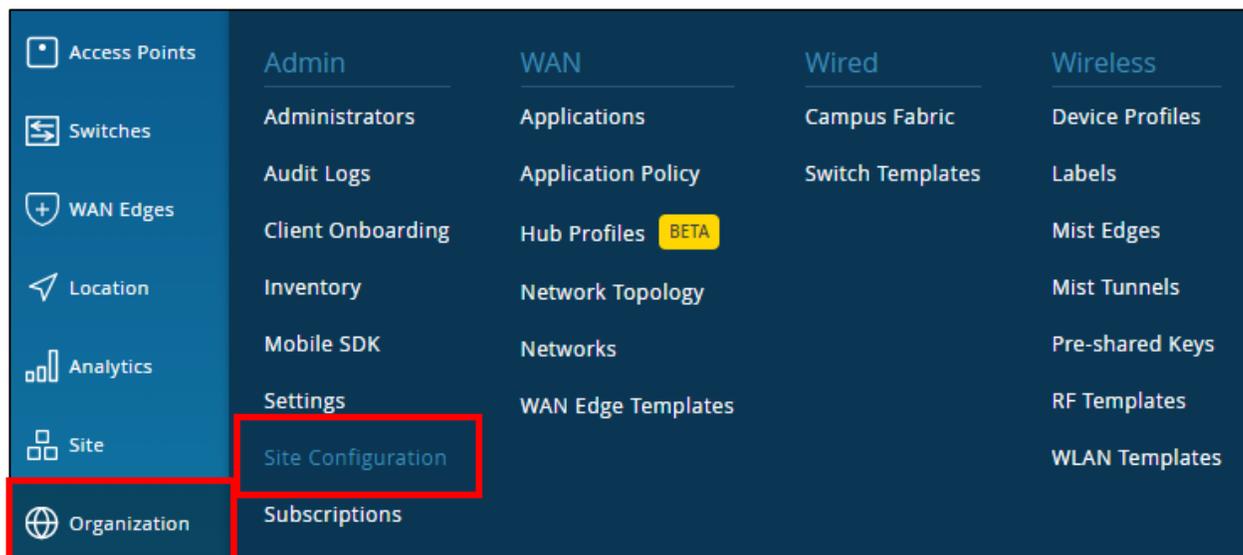
悪意ある Honeypot AP の検出をはじめ、近隣のAP、正規に使用が認められていないシャドーIT機器や今後増加が予想されるIoT機器の可視化ができます

ネイバーAPと不正APの検出

❖ ネイバーAPと不正APの確認方法

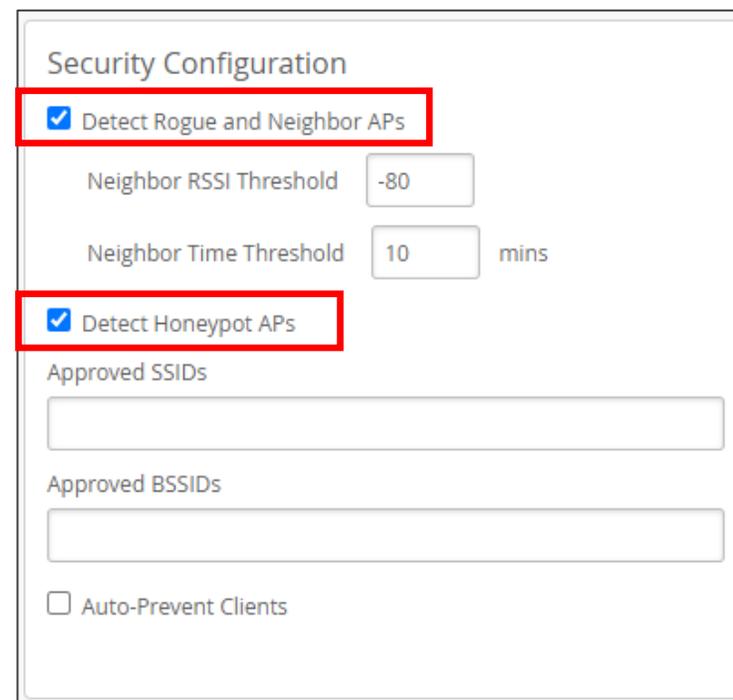
1. ネイバーAPと不正APの検知を有効化

[Organization] から [Site Configuration] を選択し
PoC で使用している Site を選択します



2. Security Configuration の項目で

Detect Rogue and Neighbor APs (デフォルト無効) と
Detect Honeypot APs にチェックを入れます



ネイバーAPと不正APの検出

❖ ネイバーAPと不正APの確認方法

3. 不正APの確認

[Site] から [Security] を選択し、PoCで使用している Site を選択します

[Threats] を選択し Type Rogueを確認します

全体的位置情報を確認したい場合は [Location] の表示に切り替えます

Action列のリンクをクリックし、[Terminate Rogue] を選択することで、選択した不正APに接続されているすべてのクライアントがネットワークからキックオフされます

特定の位置情報を確認したい場合は Location列のリンクをクリックします

SSID	Type	No. of Clients	BSSID	Band	Channel	Avg. RSSI	Seen By	Nearest AP	Location	Action
	Rogue	1					1 APs	LD_Kitchen-2	01 - Office	⋮
vlan10	Rogue	0					1 APs	LD_RS_Support	01 - Office	⋮
vlan10	Rogue	0	5c:5b:35:20:64:61	5GHz	52	-74.0 dBm	1 APs	LD_Testbed_MD	Unknown	⋮
	Rogue	7	ac:8f:a9:46:fd:d8	5GHz					01 - Office	⋮

ネイバーAPと不正APの検出

❖ ネイバーAPと不正APの確認方法

4. ネイバーAPの確認

[Site] から [Security] を選択し、PoCで使用している Site を選択します

[Neighbors Aps] を選択し Mistの管理下でない周囲のアクセスポイント, SSID, Channelを確認します

The screenshot shows the Mist Security interface for a site named 'Live-Demo'. The 'Neighbor Aps' tab is selected, and the 'Location' view is active. A table lists detected APs with columns for SSID, BSSID, Band, Channel, Avg. RSSI, Seen By, Nearest AP, and Location. The 'Location' column contains links to specific office locations or 'Unknown'.

SSID	BSSID	Band	Channel	Avg. RSSI	Seen By	Nearest AP	Location
	d4:20:b0:8c:68:39	5GHz	36	-40.5 dBm	6 APs	LD_RS_Support	01 - Office
	5c:5b:35:54:4d:81	5GHz	108	-67.9 dBm	1 APs	LD_MHMD	01 - Office
	ac:23:16:fc:4c:d3	5GHz	149	-39.0 dBm	6 APs	LD_RS_Support	01 - Office
	ac:23:16:fc:4c:c1	6GHz	69	-65.2 dBm	2 APs	LD_JSW	01 - Office
	d4:20:b0:ac:06:cb	5GHz	36	-44.4 dBm	3 APs	LD_Testbed_MD	Unknown
	d4:20:b0:ac:26:42	5GHz	36	-44.4 dBm	3 APs	LD_Testbed_MD	01 - Office

全体的位置情報を確認したい場合は [Location] の表示に切り替えます

特定の位置情報を確認したい場合は Location列のリンクをクリックします

レポート作成機能

❖ レポート作成機能を使用しレポートを作成します。

目的

Engagement Analytics または Network Analytics を使用し、TOPクライアント、TOP WLAN、接続の問題の割合、接続数の多いAP、TOPアプリケーションなどの必要な情報を登録しレポートを作成します

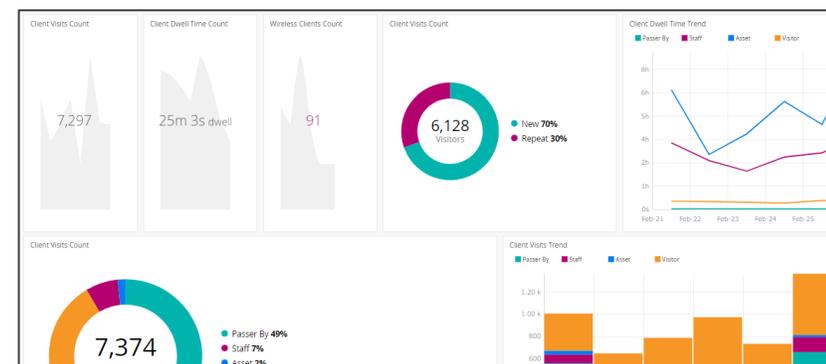
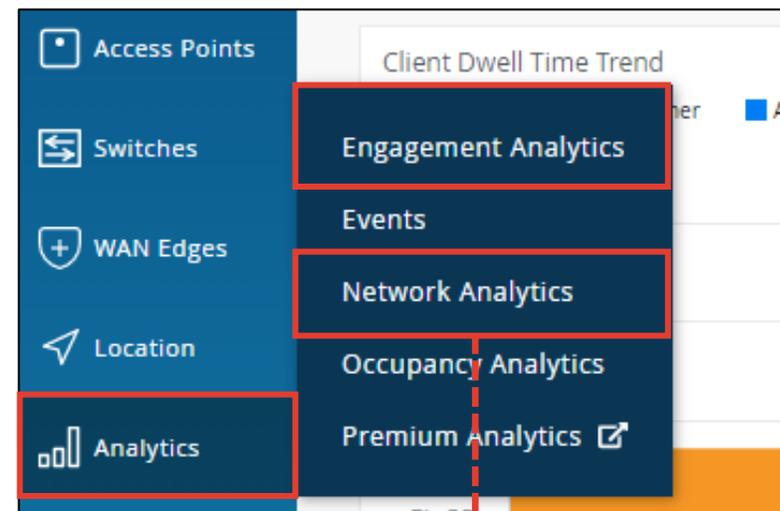
検証方法

マニュアルを参照し、レポートを作成します

[エンゲージメントアナリティクスの設定](#)

参考 URL :

<https://www.mist.com/documentation/network-and-engagement-analytics/>



レポートは複数登録可能ですので、報告先に合わせて何度もレポートを作成する必要はありません

APファームウェアのマニュアルアップグレード

❖ AP のファームウェアを手動でアップグレードします。

目的

production から rc1 へ、GUI 上から AP の手動アップグレードを実行し、
断時間や影響範囲を確認します

検証方法

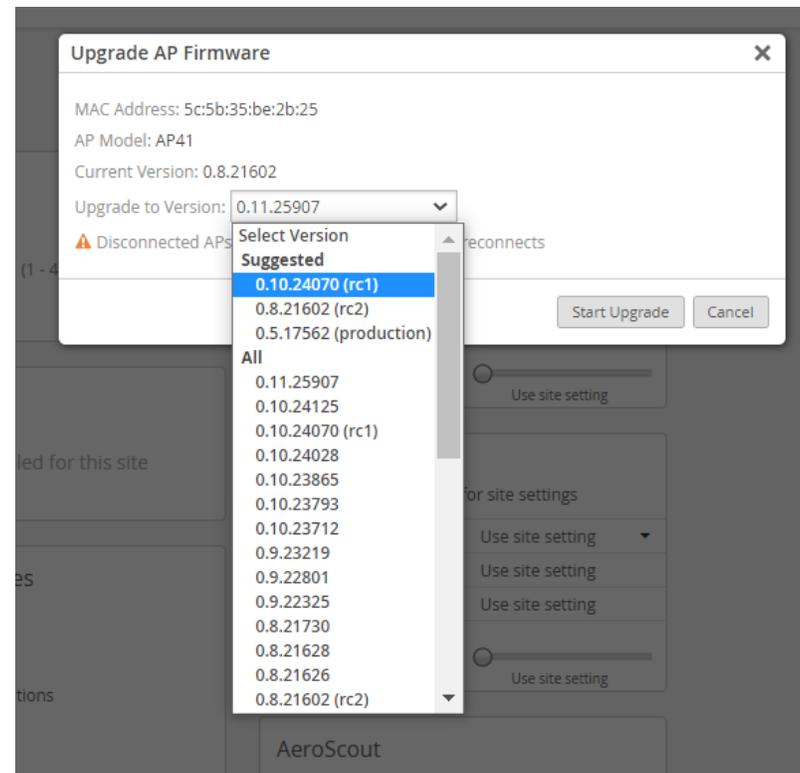
マニュアルを参照し、AP ファームウェアを手動でアップグレードします

[ファームウェア 手動アップグレード手順](#)

以下のバージョンへアップグレードします

現在のバージョン : production firmware の最新バージョン

ターゲットバージョン : rc1 firmware の最新バージョン



このシナリオでは手動でバージョンを変更しましたが、通常は指定したタイミングに
自動でアップグレードされるため運用コストを抑えることが可能です

APの設置場所確認

❖ Locating 機能を使いAPの設置場所を特定します。

目的

[Locating] ボタンをクリックし、AP の LED 点灯パターンを確認します
Locating 機能は、AP の場所を特定する際に役立ちます

手順

[Access Points] から 任意のAPを選択します
AP 設定画面右上にある [Locating] ボタンをクリックします
AP の LED がカラフルに点灯します
再度 [Locating] ボタンをクリックすると、通常のLED表示に戻ります

	Status	Name	MAC Address
<input type="checkbox"/>	Connected	AP_01	5c:5b:35
<input type="checkbox"/>	Connected	AP_02	5c:5b:35

TUE, 04:51 PM

Locating Utilities Save Cancel



例えば、APIリプレイス作業時に、現地の作業員が、素早く、間違いなく作業対象のAPを特定することが可能です

AP 交換時の手順

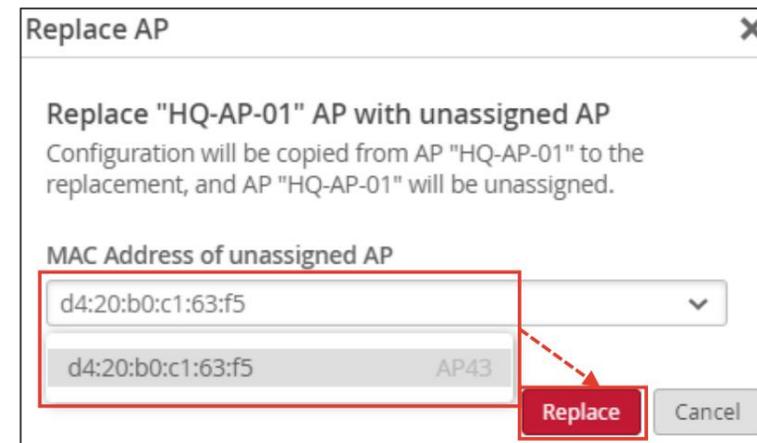
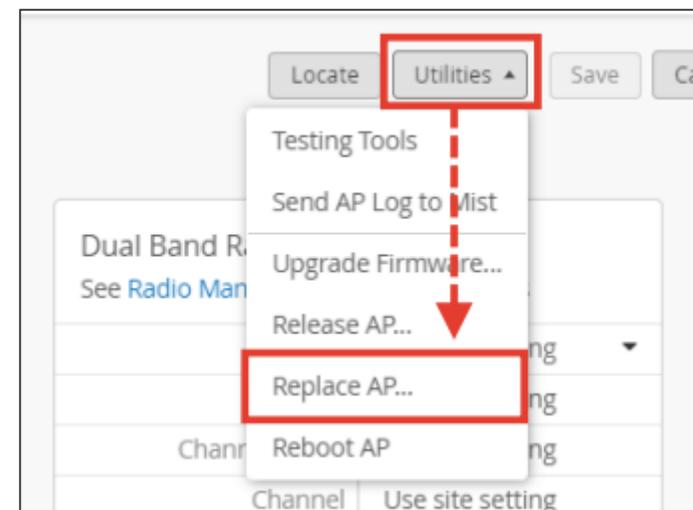
❖ AP の交換を実施します。

目的

遠隔の拠点の AP をリプレースすると仮定し、AP のリプレースを実施します
- 遠隔の拠点で AP をリプレースすると仮定したとき
拠点へ代替 AP と取付を行う作業員を手配し、物理的な取付作業と AP のクレームを行います
同時に本社のシステム担当者は、マニュアルにある登録変更を行います

検証方法

AP を1台登録解除し、代替 AP として扱い、AP のリプレースを実施します
以下のマニュアルを参照し、AP のリプレースを実施します
[アクセスポイント 交換手順](#)



リプレースが必要になったとしても、システム担当者が拠点に向かう必要はなく、登録変更も簡単に行うことができます

Thank you

JUNIPER
driven by Mist AI 