2024年1月25日リリース
Mist 新機能のご紹介

ジュニパーネットワークス株式会社

JUNIPer driven by Mist AI

はじめに

❖ 本ドキュメントは以下のリリースノートを抄訳したものです

https://www.mist.com/documentation/january-25th-2024-updates/

本ドキュメントは2024年1月時点のMist cloudのGUIを使用しております

❖ 実際の画面と表示が異なる場合がございます

❖ 内容について不明な点、ご質問等がございましたら担当営業までお問い合わせください

本リリースで追加された機能一覧（1/2）

Simplified Operations
- Webhookメッセージ内にクライアントIPアドレスを追加
- サービスレベルメトリクスページ内の対象アイテムへのフィルタの追加

Marvis
- シャプレー特徴ランキングを用いたZoomセッションのトラブルシューティング
- Marvisアクションと対話型アシスタント機能の継続使用に必要な最低サブスクリプション数の変更

Access Assurance
- マイクロソフトIntuneとの統合
- 認証ポリシーでのルールのヒットカウントを表示

Wired Assurance
- ポートの一括編集におけるポート設定の上書き
- IPアドレスならびに静的ルーティング設定でのサイト変数の使用
- ルートパスワード設定箇所の追加
- スイッチ-APアフィニティメトリックで用いる接続AP数しきい値の変更オプション

本リリースで追加された機能一覧（2/2）

WAN Assurance

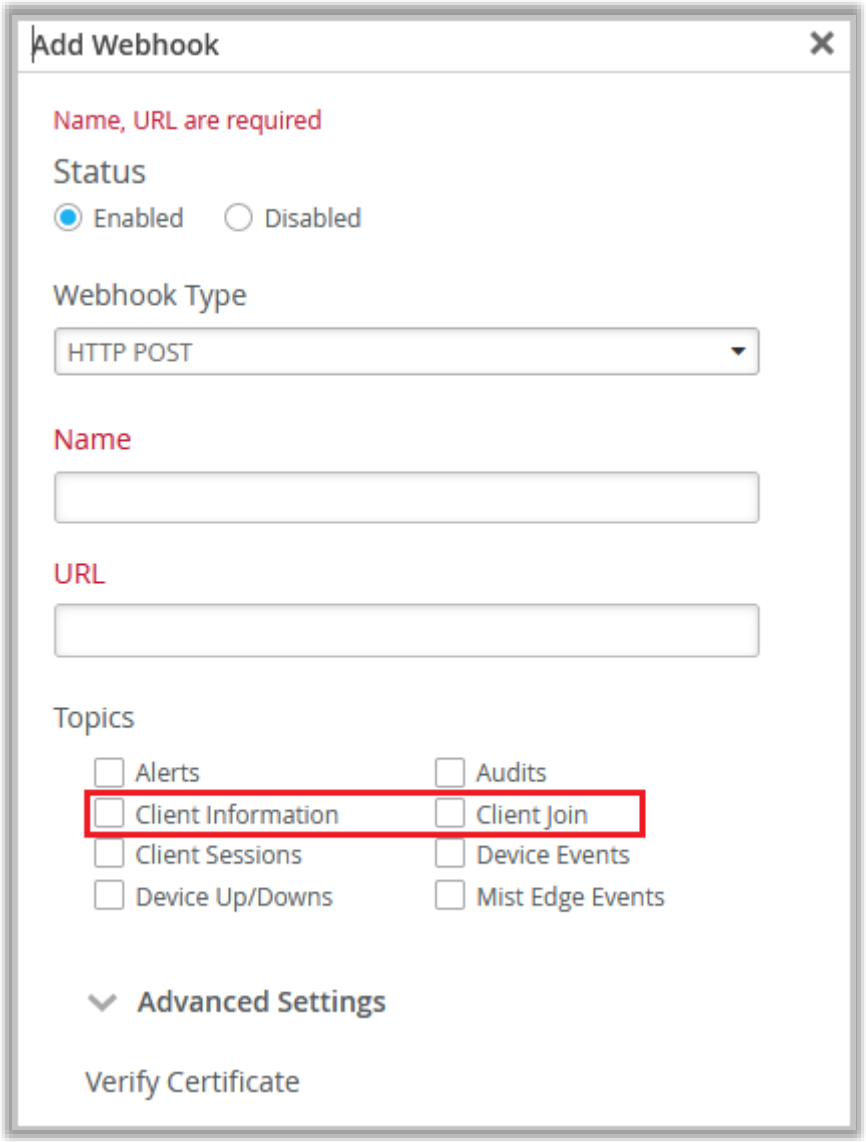
- ダイナミックパケットキャプチャ（SSR）
- SLAしきい値を超えた場合のローカルブレークアウト経路の変更（SSR）
- アプリケーションリストの拡大によるポリシーフレームワークの改良
- Cellularエッジデバイスのサイトへの自動割り当て
- SSRクラスタ内のSSRノードの交換
- SRXでのVDSLサポート

Mist Edge

- アラートページでのMist Edge関連のイベントの表示
- Mist Edgeクラスタでのトンネル終端IPアドレスの自動生成
- Mist Edge VM ISOイメージのダウンロードリンクの表示
- Mist Edgeの交換ボタンの表示
- Mist Edgeサービスのアップグレードワークフローの簡素化

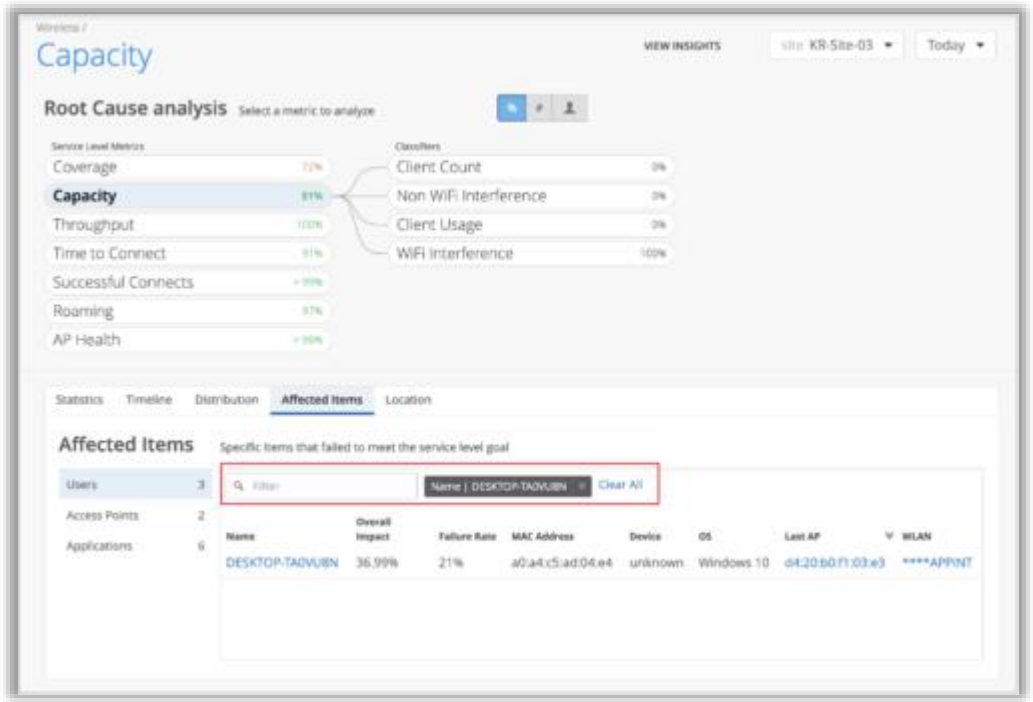
Simplified Operations

Webhookメッセージ内にクライアントIPアドレスを追加



- Webhookのクライアントジョイン（Client Join）トピックに、ネットワークに接続したクライアントデバイスのIPアドレスを含めました
- クライアントデバイスのIPアドレスの変更を取得できるように、新しくクライアント情報（Client Information）トピックを追加しました
- これらのトピックを用いるとクライアントデバイスがネットワークに接続された際のIPアドレスの情報を取得できます
- 変更、追加の詳細は以下となります
  - クライアントジョイントピック：
    - MACアドレス、RSSI、無線バンド、接続APに加え、クライアントデバイスのIPアドレス（IPv4とIPv6）を含めました
    - Webhookメッセージが送信される際に有効なIPアドレスがある場合に含まれます
  - クライアント情報トピック
    - 新しいWebhookトピックとなり、クライアントデバイスのIPアドレスの変更をMistが検知した場合に送信されます
    - IPアドレスに加え、クライアントデバイスのMACアドレスも確認できます
- Organization（Organization > Settings）またはサイト（Organization > Sites）の設定から有効にすることが可能です（左図）

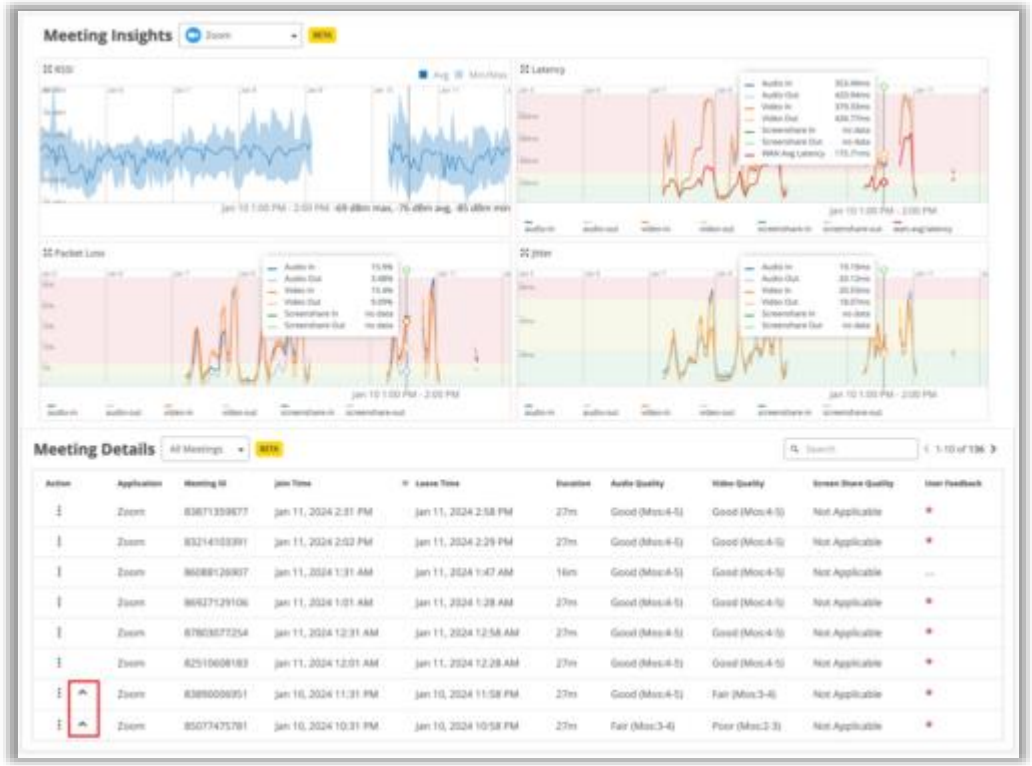
サービスレベルメトリクスページ内の対象アイテムへのフィルタの追加



- サービスレベルメトリクスページの対象アイテムタブ（Affected Item）にフィルターを追加しました（左図）
- フィルターにより、根本原因分析の際に該当する対象アイテムの調査がしやすくなります

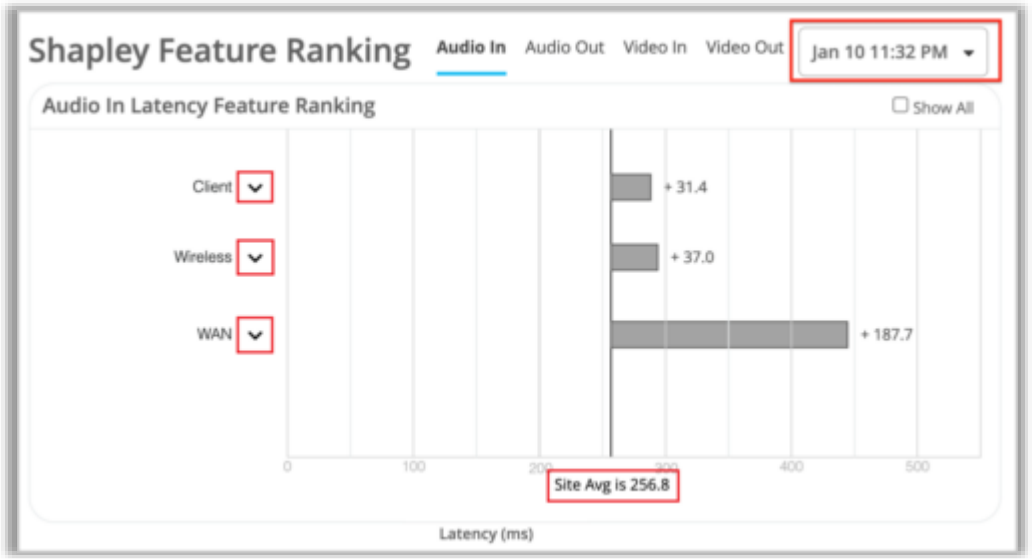
Marvis

シャプレー特徴ランキングを用いたZoomセッションのトラブルシューティング



- シャプレー特徴ランキングを用いることにより、問題のあるZoomコールをより的確に分析、トラブルシューティングできるようになります
- ネガティブなユーザ体験に対する各シャプレー特徴の平均限界寄与度を確認することができます
  - 平均限界寄与度は特徴の全ての可能な順列を考慮しています
  - 使用している特徴にはRSSI、遅延、ジッタなどのネットワークパラメータが含まれています
- Zoomコール中にユーザが体験した音声や映像の不良について、1分毎にシャプレー特徴ランキングが計算されます
- クライアントインサイトページ内のミーティング詳細項目にて確認することができます
- ネガティブなZoomコールが報告され、シャプレー特徴ランキングが紐づけられている場合は、Zoomコールに脱字記号（^）が表示され、拡張して確認することができます（左図）

シャプレー特徴ランキングを用いたZoomセッションのトラブルシューティング（続き）



- 入力音声のレイテンシに関するシャプレー特徴ランキングの場合、以下を表示します（左図）
  - サイト平均のレイテンシ
  - X軸：報告されたレイテンシ（ミリ秒）
  - Y軸：レイテンシに影響を及ぼした要素
    （クライアント、ワイヤレス、WAN）
- クライアント、ワイヤレス、WANをクリックすることにより、レイテンシに影響を及ぼした詳細な項目を確認できます
- Zoomコール内でのネガティブな体験について、シャプレー特徴ランキングビューでは、入力音声、出力音声、ビデオ入力、ビデオ出力の影響項目を提供します
- 同じZoomコール内で複数のネガティブな体験があった場合、右上のドロップダウンリストから発生した時間を選択し、特定の体験に対する特徴ランキングを表示できます（左図）

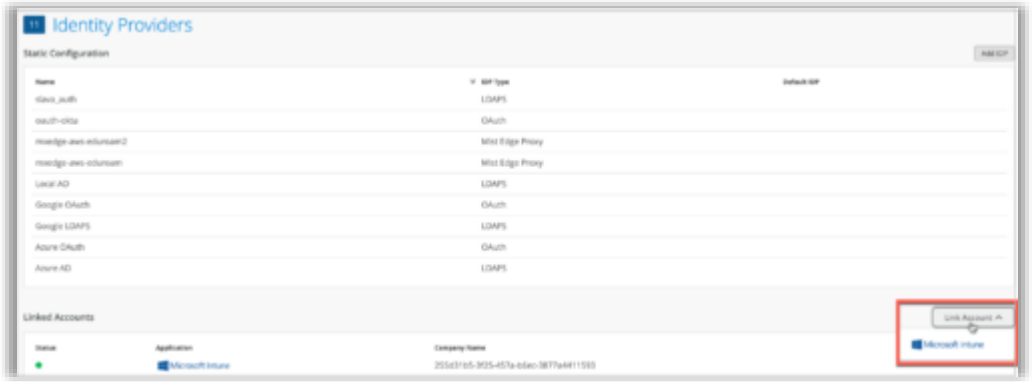
Marvisアクションと対話型アシスタント機能の継続使用に必要な最低サブスクリプション数の変更

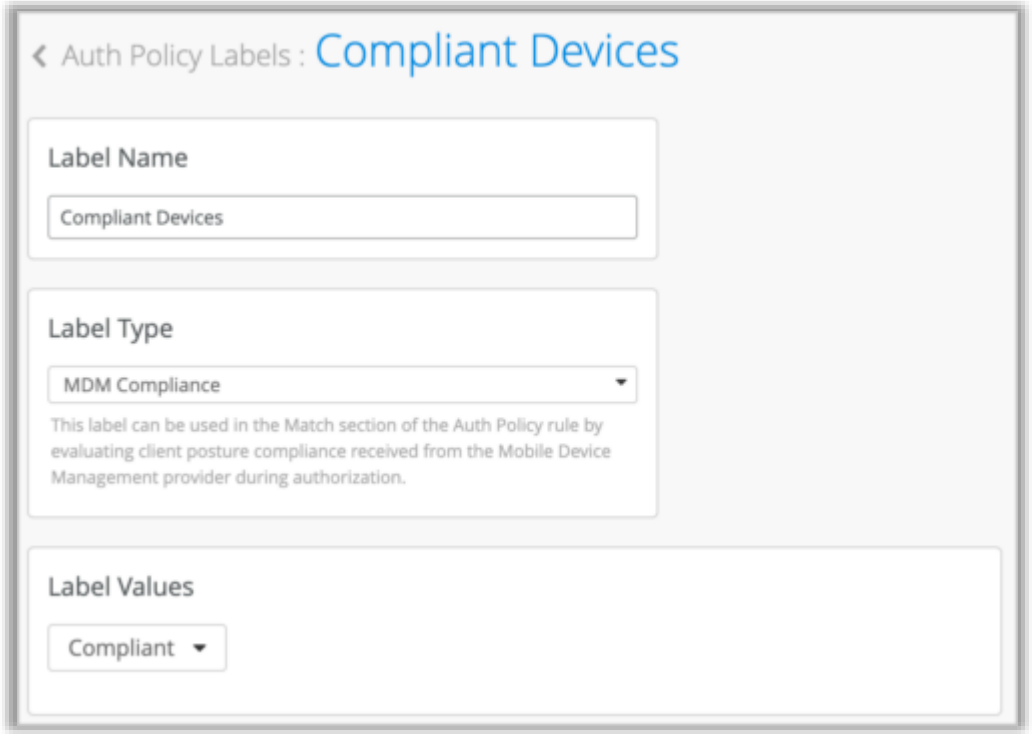
- Marvis機能への継続的なアクセスに必要なMarvisサブスクリプションの最小数を更新しました
  - Marvis機能を使用するには、インベントリ内の各デバイスにMarvisサブスクリプションが必要です
  - アクセスポイント、スイッチ、WANエッジに対し、それぞれ異なるMarvisサブスクリプションがあります
- アクティブな各Marvisサブスクリプション数が、インベントリ内の対応する機器の数の50%を超えている場合に限り、以下のMarvis機能を継続して使用できます
  - Marvis対話型アシスタント
  - トラブルシューティングAPI
  - Marvisアクション
- Marvisサブスクリプションが無い場合、Organization内に登録されている機器が10台以下の場合にのみ、Marvis機能が継続使用できます
- Marvisサブスクリプションとそれに対応する機器の種類は以下となります

Marvisサブスクリプションの種類	対応する機器
Marvis for Wireless	アクセスポイント（AP）
Marvis for Wired	スイッチ
Marvis for WAN	WANエッジ

Access Assurance

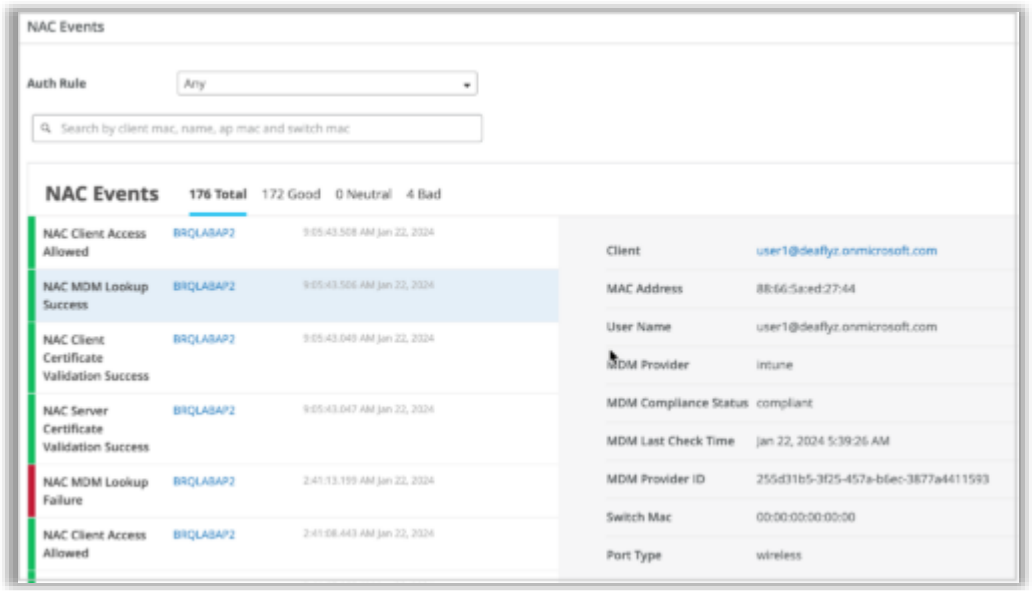
マイクロソフトIntuneとの統合





- マイクロソフトIntuneアカウントをAccess Assuranceに統合することができます
  - マイクロソフトIntune：
    MDM（Mobile Device Management）ソリューション
- Intuneから報告されたデバイスのコンプライアンス状況に基づいて、モバイルデバイスのアクセス制御を決定します
- デバイスがIntuneのコンプライアンスポリシーに準拠していない場合、Access Assuranceがデバイスを隔離VLANまたは修復対象のロールに移動することができます
- Intuneとの統合手順は以下となります
  1. Identity Provider ページ（Organization > Identity Providers）にて、マイクロソフトIntuneアカウントとAccess Assuranceを連携させます（左上図）
  2. MDMコンプライアンスの種類の認証ポリシーラベルを作成します（Organization > Auth Policy Labels）（左下図）
     - ラベルの値として以下を選択できます
       - Compliant（準拠）
       - Non-Compliant（非準拠）
       - Unknown（不明）

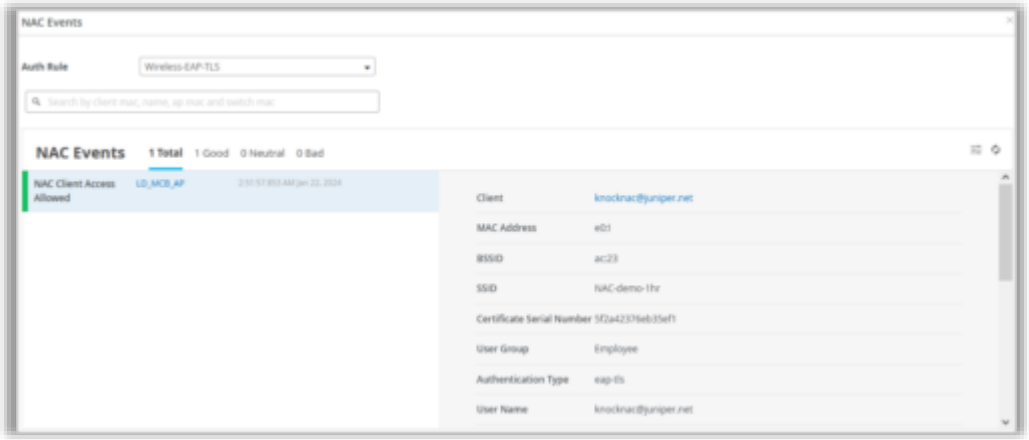
マイクロソフトIntuneとの統合（続き）



3. 認証ポリシールール（Organization > Auth Policies）でMDMコンプライアンスラベルを活用することにより、認証時にMDMプロバイダから受け取ったクライアントのコンプライアンス準拠状況を用いてポリシーを照合します（左上図）

- MDM固有のイベントはクライアントイベント、またはNACイベントに表示されます（左下図）

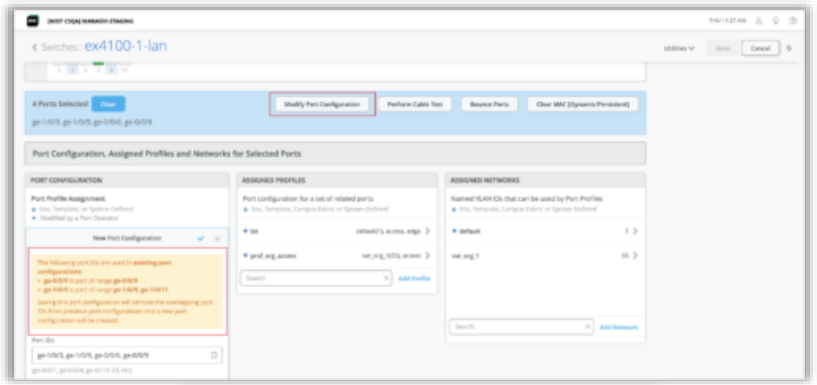
認証ポリシーでのルールのヒットカウントを表示



- 認証ポリシーページ（Organization > Auth Policies）に「ヒットカウント」という新しい列が追加され、各ルールに該当したNACイベント数が表示されるようになりました
- ヒットカウント情報は、以下の範囲でフィルタが可能です（左上図）
  - 過去60分
  - 過去24時間
  - 過去7日間
  - 今日
  - 昨日
  - 今週
  - カスタムの日付、または範囲
- 「Show NAC Events」ボタンをクリックすることにより、全てのNACイベントを表示することができます
- NACルールに紐づくヒットカウントをクリックすると、その特定のNACルールに該当したNACイベントが表示されます（左下図）

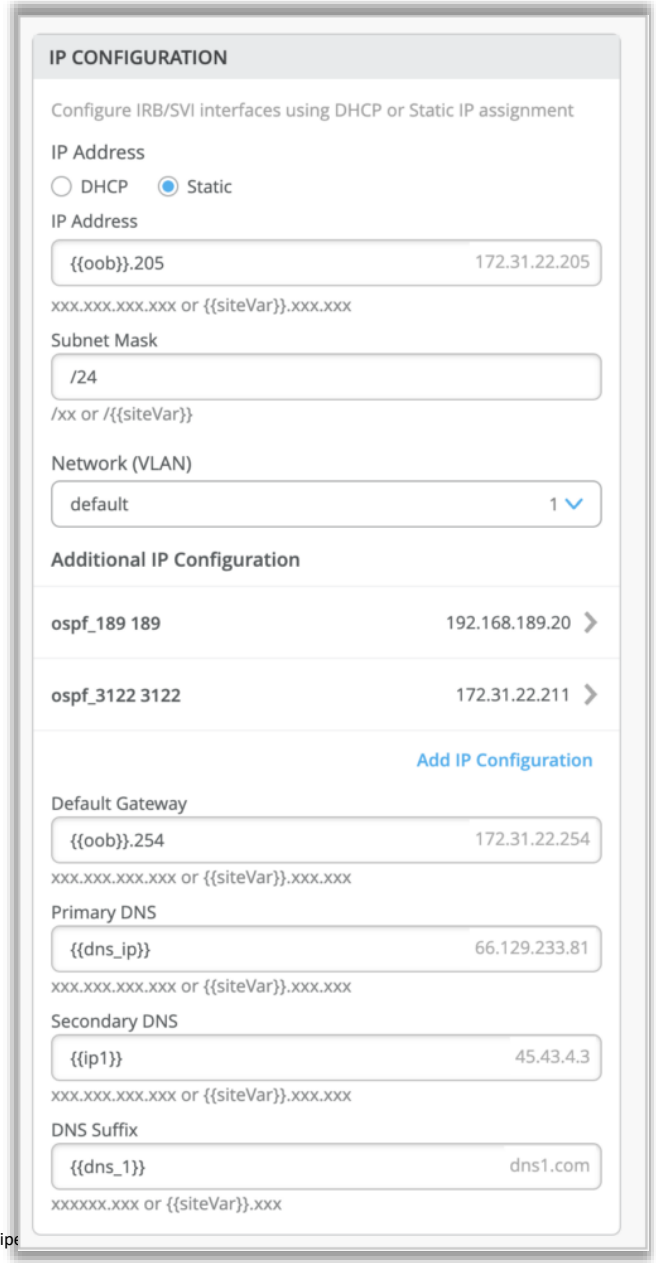
Wired Assurance

ポートの一括編集におけるポート設定の上書き



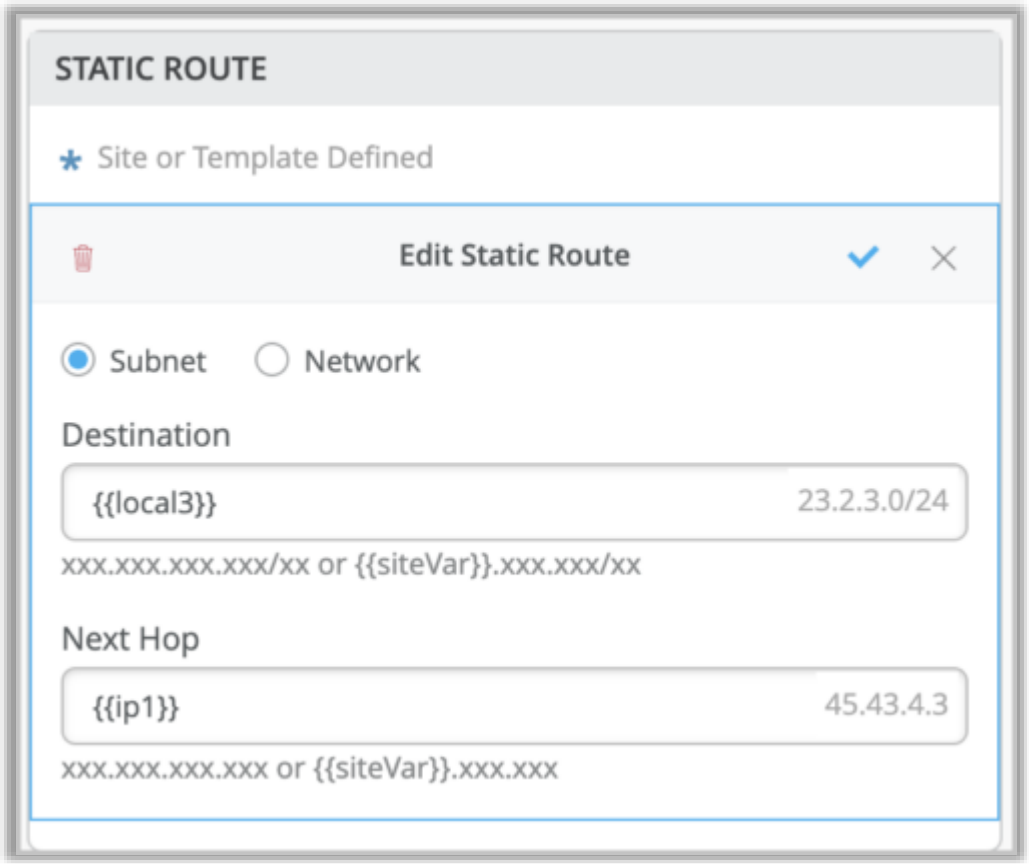
- スイッチの詳細ページ内にある一括ポート設定オプションを用いて既存のポート設定を上書きすることができます
- これまでは一括ポート設定の前に、重複するポート設定を手動で削除する必要がありましたが、本機能により、ポートの設定の上書きが可能となります
- スイッチの詳細ページのスイッチのフロントパネルから設定したいポートを複数選択し、「Modify Port Configuration」をクリックします（左上図）
- 選択したポートが既に他のポート範囲（Port Range）設定に含まれている場合、警告メッセージが出力されます（左上図）
- 新しい設定を保存すると、選択したポートの設定が上書きされます
- 以下のいづれかの方法でポートの設定を上書きする場合も、重複がある場合は警告メッセージが出力されます
  - スイッチテンプレート（Organizationまたはサイトレベル）のポート設定タブ（左下図）
  - スイッチ詳細ページのポート設定（PORT CONFIGURATION）項目

IPアドレスならびに静的ルーティング設定でのサイト変数の使用



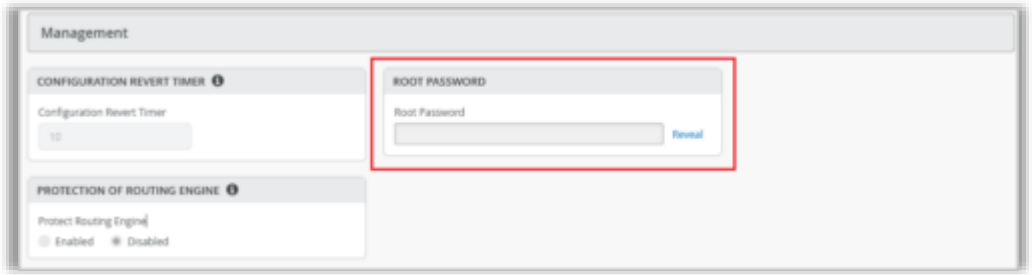
- デバイス、サイト、OrganizationレベルでのIPアドレスおよび静的ルートの設定でサイト編須賀使用できるようになりました
- それぞれのサイトで固有のIPアドレスや静的ルートを設定したい場合に役立ちます
- サイト変数はタグにより実際の値を表す方法を提供します
- サイト変数を用いることにより、同じ変数でも異なるサイトで異なる値を設定することが可能となります
- IP設定内で、以下の項目でサイト変数を使用することができます（左図）
  - IPアドレス
  - サブネットマスク
  - デフォルトゲートウェイ
  - プライマリDNS
  - セカンダリDNS
  - DNSサフィックス

IPアドレスならびに静的ルーティング設定でのサイト変数の使用（続き）



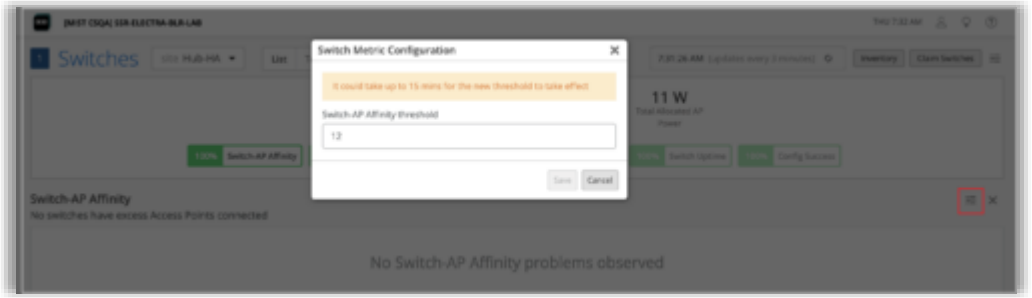
- 静的ルートの設定では、以下の項目でサイト変数を使用することができます（左図）
  - 宛先
  - ネクストホップ
- デバイスレベル（スイッチの詳細）、サイトレベル（スイッチテンプレート）、Organizationレベル（スイッチテンプレート）の以下の項目でもサイト変数を使用することができます
  - DNSサーバとDNSサフィックス
  - NTP
  - RADIUSサーバ
  - 静的ルート
  - ネットワーク（VLAN ID、サブネット、サブネットマスク）
  - IP設定（OOB）

ルートパスワード設定箇所の追加



- Super Userの権限でログイン時に、スイッチテンプレート（サイトまたはOrganizationレベル）やスイッチ詳細ページでJunosルートパスワードを設定することができます（左図）
  - これまではサイトの設定ページ（Organization > Site Configuration）でのみ設定が可能でした
- Organization > Site Configurationページで設定したルートパスワードが、サイトレベルのテンプレート（Site > Switch Configuration）で使用できるようになり、関連するデバイスに継承されます
- ルートパスワードはサイト設定ページに加え、以下のページからも設定できるようになります
  - Organizationレベルのスイッチテンプレート（Organization > Switch Templates）
  - サイトレベルスイッチテンプレート（Site > Switch Configuration）
  - スイッチ詳細ページ（Switches > スイッチ名）
- Super Userの権限でログインしていない場合、ルートパスワード項目はオプション項目となり、暗号化された文字列で表示されます

スイッチ-APアフィニティメトリックで用いる接続AP数しきい値の変更オプション

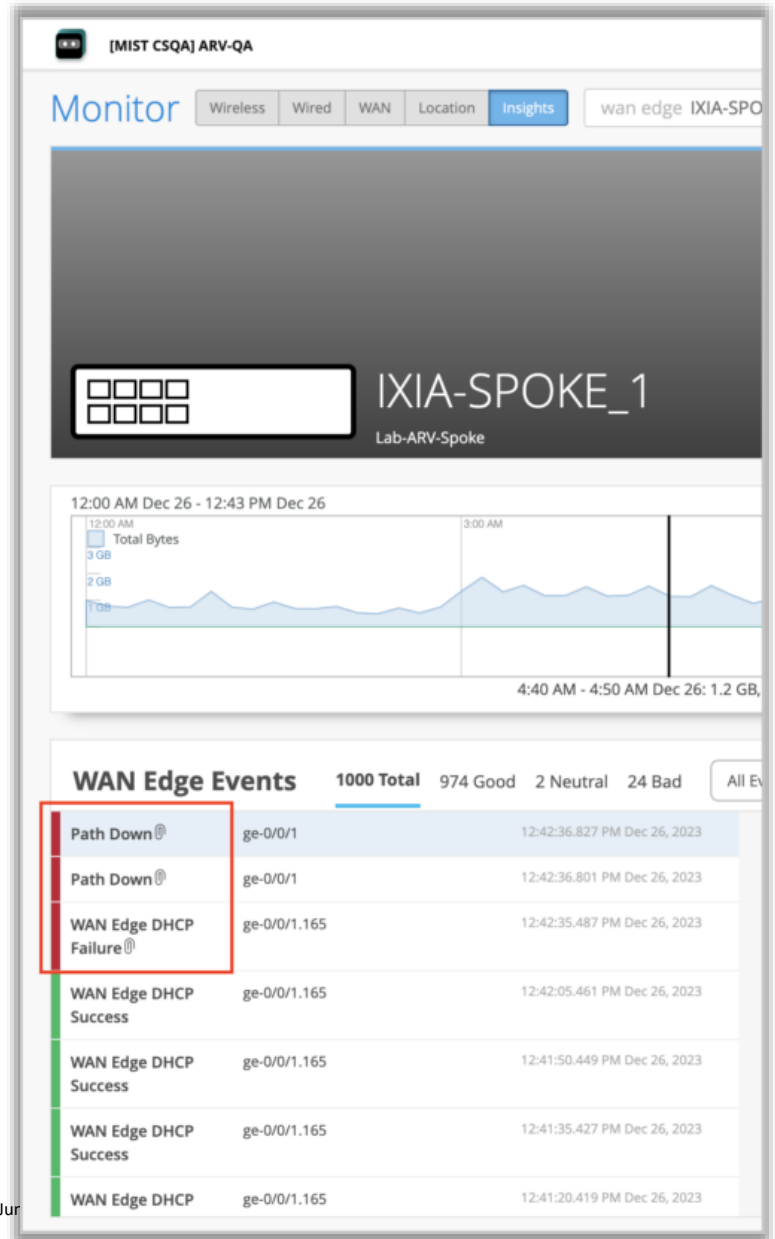


- スイッチ-APアフィニティメトリックの計算で用いる、スイッチあたりに接続されたアクセスポイント数のしきい値を設定できるようになりました
  - スイッチ-APアフィニティ：

    スイッチのパフォーマンスを追跡するために使用されるコンプライアンスパラメータの一つであり、スイッチの加重率を示します
- デフォルトのスイッチ-APアフィニティのしきい値は以下となります
  - 1スイッチにつき、12アクセスポイント
- アクセスポイント数のしきい値の設定は以下の手順にて可能です
  1. スイッチ-APアフィニティの表示をクリック
  2. 右側に表示される三重線をクリック（左図）

WAN Assurance

ダイナミックパケットキャプチャ（SSR）

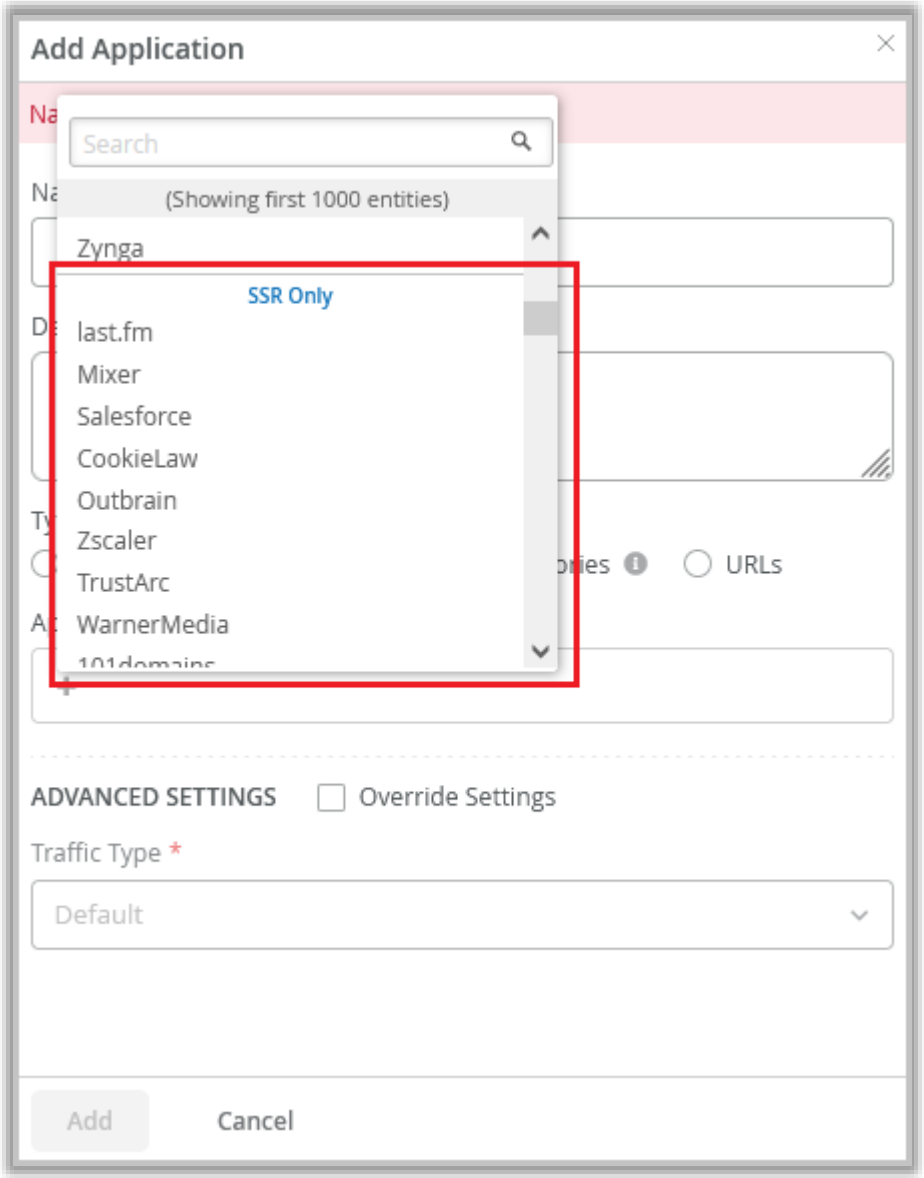


- SSRでダイナミックパケットキャプチャ機能（dPCAP）が搭載されました
- ダイナミックパケットキャプチャはWANエッジインサイトページのWANエッジイベント項目で確認、ダウンロードできます
- ダイナミックパケットキャプチャが利用可能なイベントは、イベント横にペーパークリップのアイコンが表示されます（左図）
- パケットキャプチャファイルをダウンロードするには、イベントをクリックし、右側のイベント詳細の下部にある「Download Packet Capture」ボタンをクリックします
- SSRでダイナミックパケットキャプチャを生成可能なイベントは以下となります
  - Next-hopゲートウェイへのARPリクエストの失敗
  - DHCPアドレス解決の失敗
  - WANエッジのBGPピアリング確立の失敗
  - WANエッジのSVRピアリング確立の失敗

SLAしきい値を超えた場合のローカルブレークアウト経路の変更（SSR）

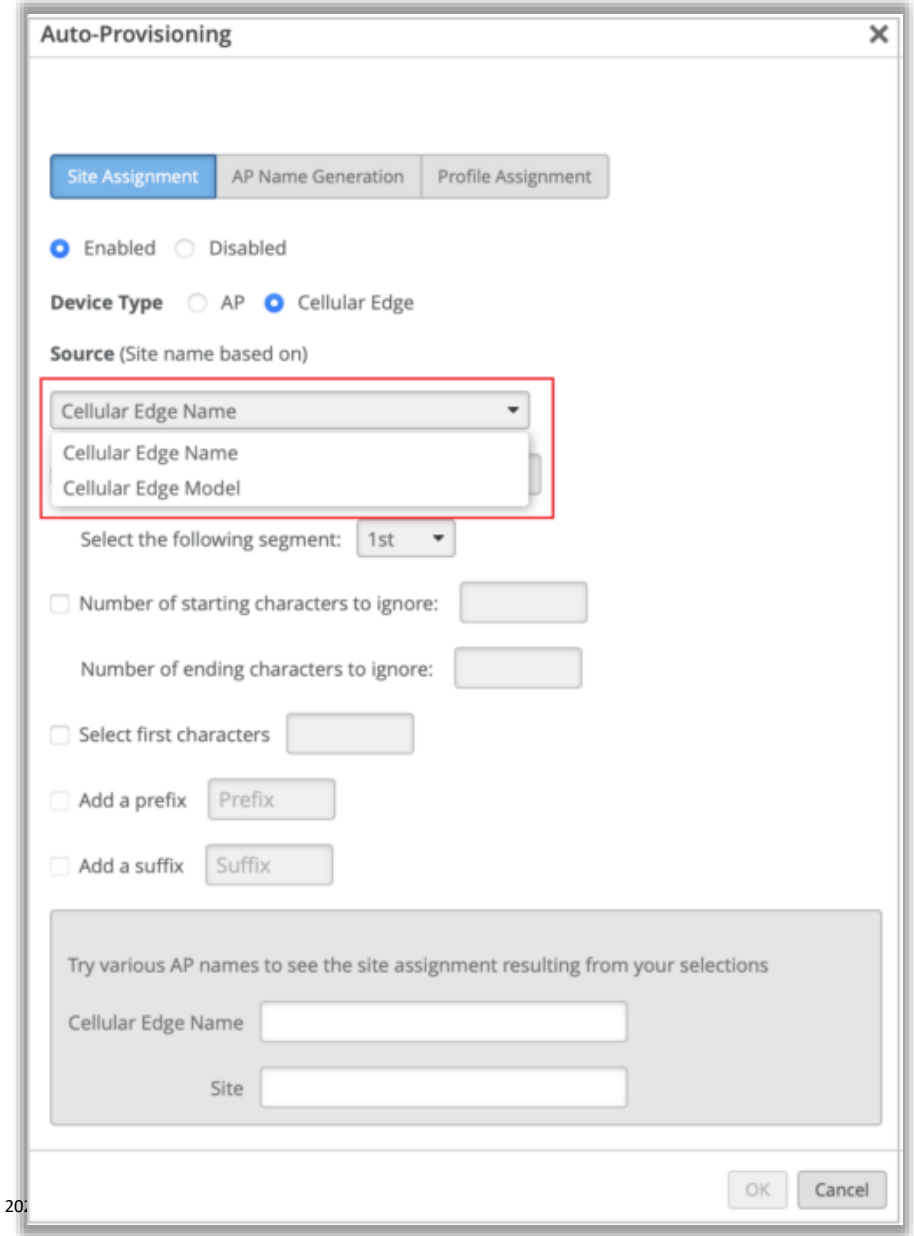
- レイテンシ、ジッタ、損失パラメータのSLA要件を使用経路が満たさない場合に、ローカルブレークアウトトラフィックを別の経路へ切り替えることができるようになりました（SVR経路では既に本機能は実装済みです）
- 設定されたSLAパラメータのしきい値を超えた（SLA要件を満たさない）場合、トラフィックステアリングの設定に基づいて別の経路にトラフィックを切り替えます
  - SSRは各ローカルブレークアウト経路のSLAパラメータ（レイテンシ、ジッタ、損失）と各アプリケーションに設定されたSLAパラメータのしきい値を比較しています
- トラフィックの経路の切り替えはアプリケーションポリシーダッシュボードのApplication Routing Visibilityグラフで確認することができます（左図）
- 以下の手順にて設定が可能です
  1. Addアプリケーション画面（Organization > Application > Add Applications）で各アプリケーションのレイテンシ、ジッタ、損失のしきい値を設定します
  2. サイトに紐づいたWANエッジテンプレート（Organization > WAN Edge Templates）またはWANエッジ詳細ページ（WAN Edges > WAN Edges > WANエッジ名）でトラフィックステアリングを設定します
  3. WANエッジテンプレート（Organization > WAN Edge Templates）またはWANエッジ詳細ページ（WAN Edges > WAN Edges > WANエッジ名）でアプリケーションポリシーにトラフィックステアリング設定を含めます

アプリケーションリストの拡大によるポリシーフレームワークの改良



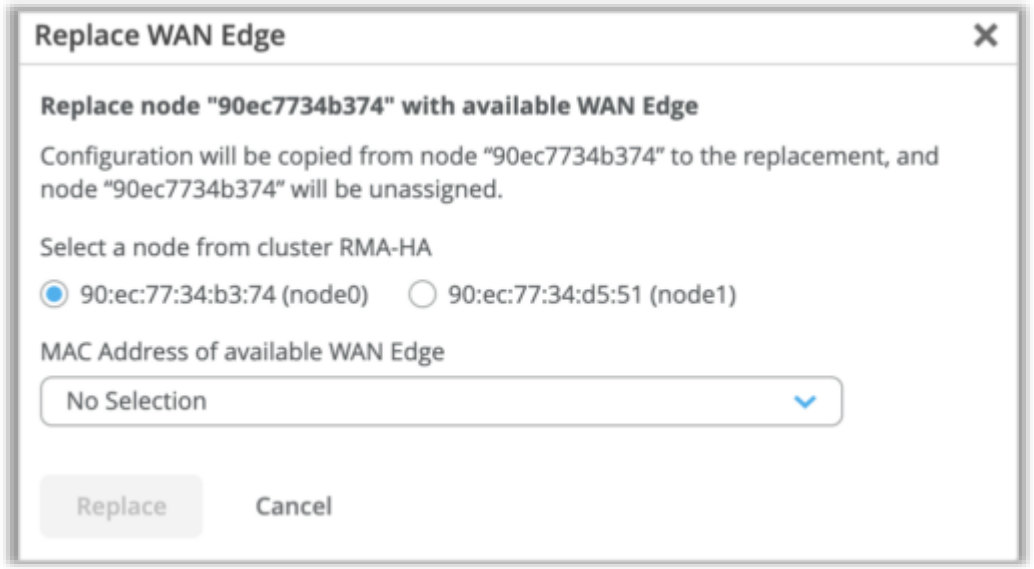
- WANエッジでサポートされる多くのアプリケーションをMistクラウドのアプリケーションリストにも追加しました
- アプリケーションリストでは、以下のセクションにアプリケーションリストをグループ化し、選択しやすくなりました（左図）
  - Application
  - SSR Only
  - SRX Only
- アプリケーション作成画面（Organization > Applications > Add Applications）で、アプリケーションを確認、選択することができます
- アプリケーションポリシーでは、これらのアプリケーションをトラフィックをブロックやトラフィックステアリングの決定で使用できます
  - これまではアプリケーショントラフィックステアリングで使用できたアプリケーションは限られたアプリケーションのみでした

Cellularエッジデバイスのサイトへの自動割り当て



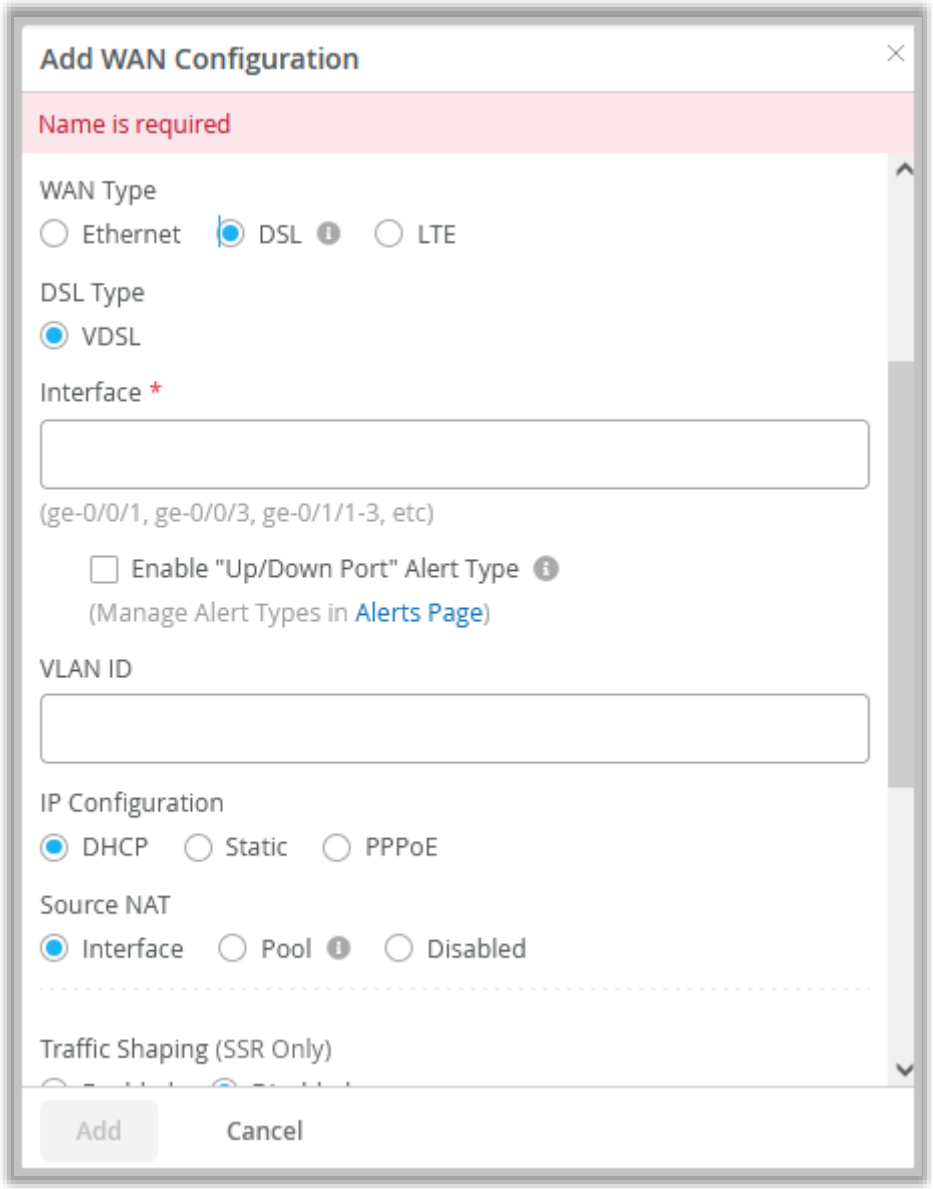
- Cellularエッジデバイスを自動的にサイト割り当てることができるようになりました
  - Cradlepoint社製デバイスでのみ、サポートする機能です
- Cradlepoint社製デバイスを自動的に関連サイトに割り当てるルールを設定できます
- Organization > Settingsページで自動登録を設定します
- 自動登録には、以下のいづれかの方法を使用できます（左図）
  - Name-based：デバイス名（Cellularエッジ名）に基づいてサイト名を選出するルールを設定します
  - Model-based：デバイスの種類（Cellularエッジモデル）毎にサイトを割り当てるルールを設定します
- Cradlepoint社製デバイスを検知すると、設定されている自動割り当てルールに基づいてサイトにデバイスを割り当てます
- 自動割り当てルールが設定されていない場合は、Cradlepoint社製デバイスのLLDP情報を使用して、デバイスに直接接続されているJuniperデバイスが所属しているサイトに割り当てます
  - Cradlepoint社製デバイスとJuniperデバイスでLLDPが有効になっている必要があります
- 自動サイト割り当て機能は、デバイスが最初にMistダッシュボードに接続する際にのみ、適用されます

SSRクラスタ内のSSRノードの交換



- SSRクラスタ内で障害があったSSRノードを交換できるようになりました
- SSRクラスタ詳細ページ（WAN Edges > WAN Edges > WANエッジ名）内のユーティリティメニューの「Replace WAN Edge」オプションで交換できます
- Replace WAN Edgeウィンドウで交換したいSSRノードと、新しいSSRノードのMACアドレス（「MAC Address of available WAN Edge」ドロップダウンリスト）を選択します（左図）
- 「Replace」ボタンをクリック後、約15分で交換が終了します
- SSRノードの交換前に、以下の内容を確認、実施ください
  - 交換するSSRノードからクラスタファブリック用ケーブルを抜去し、新しいSSRノードに接続します
  - 新しいSSRノードが交換するSSRノードと同じモデルである必要があります
  - 新しいSSRノードのファームウェアが6.0より後発のバージョンである必要があります
  - 新しいSSRノードが新品である場合、以下を事前に実施ください
    - SSRクラスタが登録されているサイトと同じサイトに新しいSSRノードを登録ください
    - 新しいSSRノードのファームウェアを6.0より後発のバージョンにアップグレードください

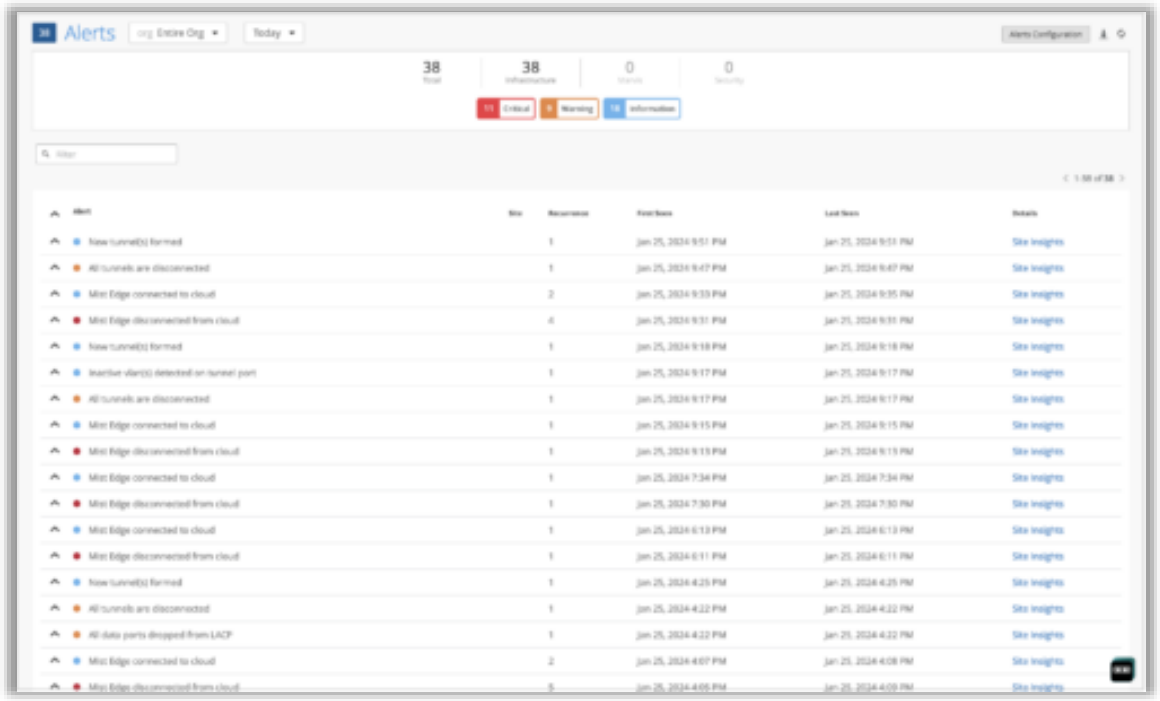
SRXでのVDSLサポート



- DSL MPIMカードがインストールされたSRXでVDSLをサポートします
- 以下のいづれかの設定ページから設定が可能です（左図）
  - WANエッジ詳細ページ（WAN Edges > WAN Edges > WANエッジ名）のWAN設定セクション
  - WANエッジテンプレート（Organization > WAN Edge Templates）

Mist Edge

アラートページでのMist Edge関連のイベントの表示



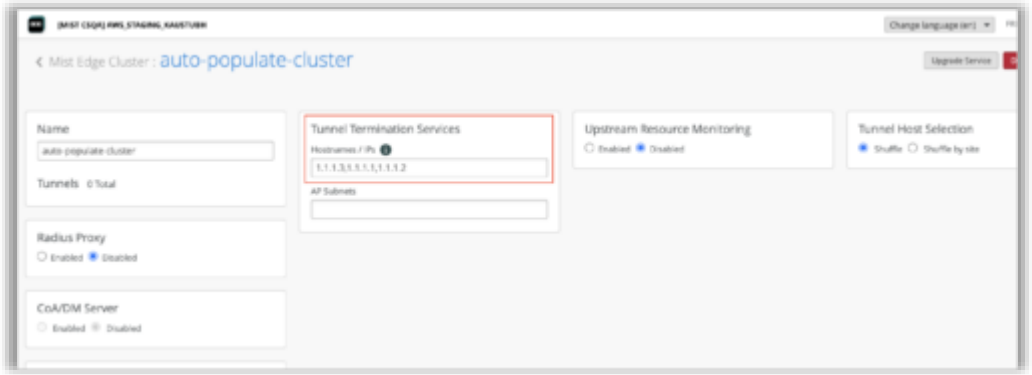
- Monitor ＞ AlertsページでMist Edgeイベントを表示できるようになりました（左図）
- Critical、Warning、Informationのメッセージを表示します
  - Criticalメッセージ：

    Mistクラウドとの切断、Mist Edgeサービスのクラッシュ、全トンネルの切断などのイベント
  - Warningメッセージ：

    Mist Edgeサービスの障害、CPU/メモリ/ディスクの高使用率の検知などのイベント
  - Informationメッセージ：

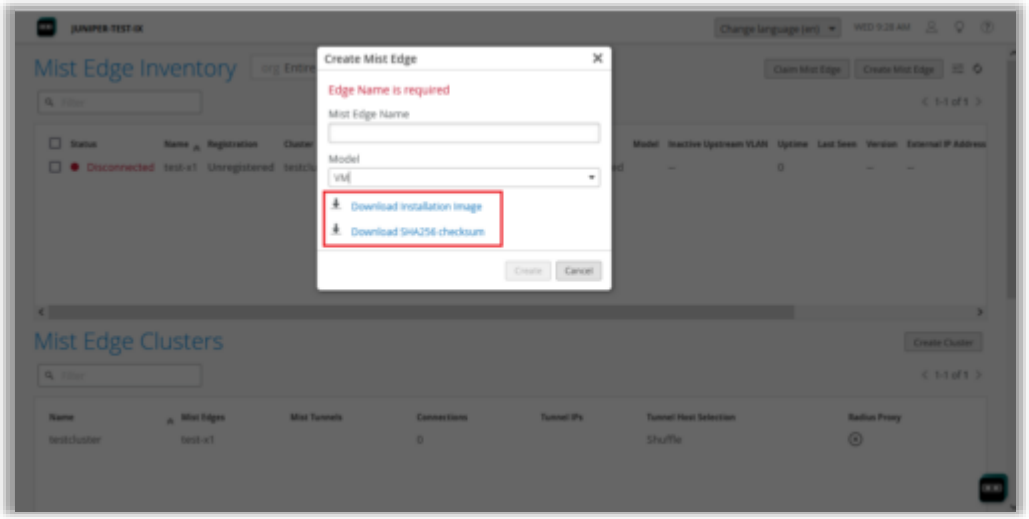
    トンネルの確立、クラウドへの接続完了、トンネルポートでの未使用VLANの検知などのイベント

Mist Edgeクラスタでのトンネル終端IPアドレスの自動生成



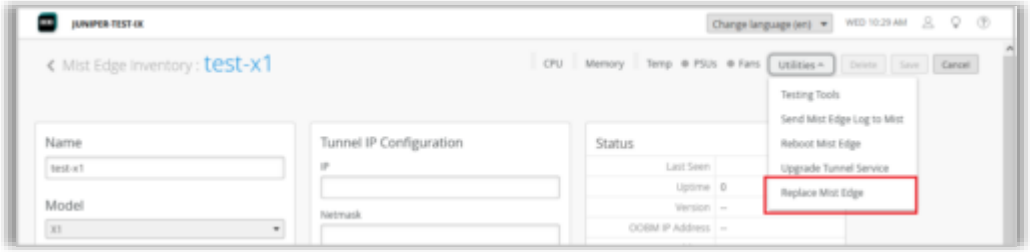
- Mist Edgeクラスタ作成ページにおいて、Tunnel Termination Servicesセクションの「Hostnames/IPs」フィールドに、選択したMist Edgeに設定したIPアドレスが自動的に入力されるようになりました（左図）
- 自動生成機能により、誤ったトンネルIPアドレスを入力することを防ぐことができます
- Mist Edgeをクラスタから削除した場合、紐づいたトンネルIPアドレスは削除されます
- リモートのMistテレワーカーの場合、Mist Edgeの外部向けIPアドレスを手動で入力する必要があります

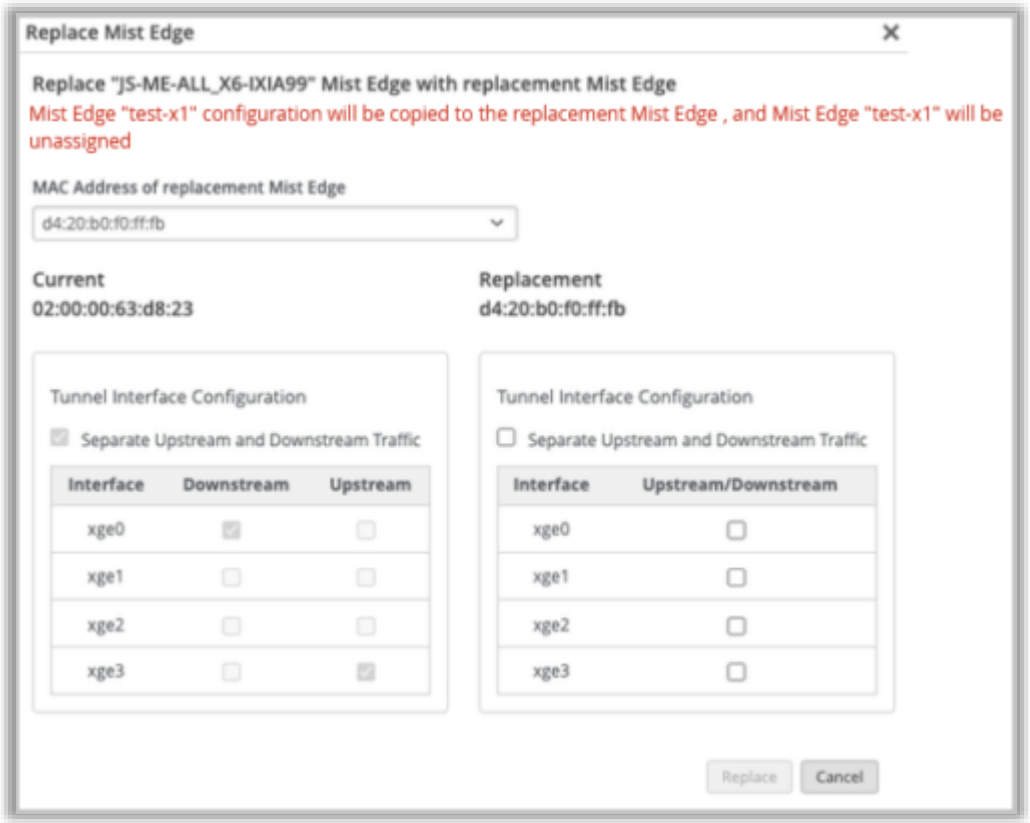
Mist Edge VM ISOイメージのダウンロードリンクの表示



- Create Mist EdgeページにMist Edgeの仮想マシン（VM）のISOイメージをダウンロードするリンクを追加しました（左図）
- VMware上でハイパーバイザとして仮想Mist Edgeを稼働させることにより、仮想アプライアンスとしてMist Edgeを使用することができます
- セキュリティの向上のために、ダウンロードしたVMイメージのコピーが改ざんされていないことを確認するのに役立つSHA-256チェックサムをダウンロードするオプションも提供しています

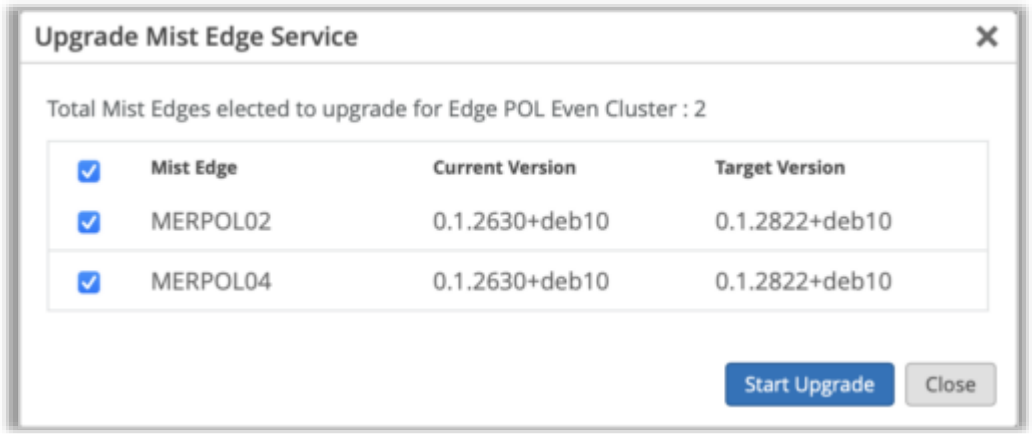
Mist Edgeの交換ボタンの表示





- Mist Edge詳細ページのユーティリティメニューの「Replace Mist Edge」を選択することにより、新しいMist Edgeに交換できるようになりました（左上図）
- 「Replace Mist Edge」をクリックすることにより、Mist Edgeを交換できるReplace Mist Edgeページに遷移します（左下図）
- 交換プロセスを実施する前に、交換用の新しいMist Edgeで以下のことを確認ください
  - Organizationのインベントリに登録されている
  - サイトには登録・追加されていない
- 古いMist Edgeの設定は新しいMist Edgeにコピーされます
- 交換プロセスが終了後、古いMist Edgeはサイトの登録から削除されます
- ポートの設定も新しいMist Edgeにコピーされていますが、arm-modeを変更することも可能です
  - Dual-armモード：
    アップストリームとダウンストリームで異なるポートを使用
  - Single-armモード：
    アップストリームとダウンストリームで同じポートを使用

Mist Edgeサービスのアップグレードワークフローの簡素化



- Mist Edgeをバージョンアップする際に、自動的に最新の推奨バージョンを用いるようになりました
- アップグレードの際にファームウェアのバージョンを選択する必要がなるため、誤って非推奨のバージョンを選択してしまうことを防ぎます
- 以下のいづれかのページからMist Edgeサービスアップグレードウィンドウにアクセスできます
  - Mist Edge詳細ページのユーティリティメニュー
  - Mist Edgeクラスタ詳細ページ
- アップグレードウィンドウではMist Edge名、現在のバージョン、アップグレード後のバージョンを表示します（左図）
- アップグレードするには、デバイスを選択し、「Start Upgrade」をクリックします
  - クラスタの場合は複数のMist Edgeが出力されます
  - クラスタの場合は、1台、または複数台のMist Edgeをアップグレードできます
  - １台のMist Edgeのアップグレードの場合は、常に1台のMist Edgeが対象となります
- Mist Edgeで既に最新のバージョンが稼働している場合は、推奨バージョンは表示されません


Thank you
JUNIPER
driven by Mist AI