Cisco vManage モニターの概要

表 *1*：機能の履歴

機能名	リリース情報	説明
統合型のモニタリングビュー向けに強化された Cisco vManage のユーザーインターフェイス	Cisco vManage リリース 20.7.1	Cisco vManage の強化されたユーザーインターフェイスがこの機能に導入されました。[Monitor] ウィンドウは、Cisco SD-WAN オーバーレイネットワークのすべてのモニタリングコンポーネントとサービスの統合ビューに対応した単一ページのリアルタイムのユーザーインターフェイスを提供します。[Main Dashboard]、[VPN Dashboard]、[Security]、[Multicloud] を含む Cisco vManage ダッシュボードすべてのエントリポイントになります。これらのダッシュボードは、以前は [Dashboard] メニューからアクセスできました。さらに、すべてのモニタリングコンポーネントがユーザーインターフェイス内でボタンとして表示されるため、別のページにすばやく移動できます。 このリリースでは、Cisco vManage の [Tools] メニューも拡充されています。以前は [Monitor] メニューからアクセスできた [Network Wide Path Insight] と [On Demand Troubleshooting] オプションが [Tools] メニューに移動し、これらの機能を簡単に見つけられるようになりました。
Cisco vManage のカスタマイズ可能な [Monitor Overview] ダッシュボード	Cisco vManage リリース 20.9.1	この機能により、[Monitor Overview] ダッシュボードがカスタマイズ可能になりました。好みに合わせて、表示するダッシュボードを自由に指定したり、並べ替えたりできます。

Cisco vManage の**[Monitor]** > **[Overview]**ダッシュボードには、次のダッシュレットがあります。Cisco vManage リリース 20.6.x 以前では、これらのダッシュレットは**[Dashboard]** > **[Main Dashboard]**ページ内にあります。

- WAN Edge Health
- Site BFD Connectivity
- Transport Interface Distribution
- WAN Edge Inventory
- Transport Health
- **Top Applications**
- **Application-Aware Routing**

[Monitor Overview] ダッシュボードのカスタマイズについて

最小リリース：Cisco vManage リリース 20.9.1

デフォルトでは、[Monitor Overview] ダッシュボードには、Cisco SD-WAN オーバーレイネットワークのさまざまなコンポーネントとサービスをモニタリングする際に役立つすべてのダッシュレットが表示されます。カスタマイズ可能なダッシュボード機能を使用すると、次のことができます。

- ダッシュレットの追加

- ダッシュレットの削除
- ダッシュレットの再配置
- デフォルト設定の復元

カスタマイズされたダッシュボード設定はデータベースに保存されます。Cisco vManage にログインするとき、または別のウィンドウから [Monitor Overview] ダッシュボードに移動するときに、これらの設定が取得されます。

この機能は、シングルテナント展開とマルチテナント展開の両方で使用できます。ただし、マルチテナント展開の場合、この機能はテナントダッシュボードでのみ使用できます。

（注） 標準およびカスタムユーザーグループに属するすべてのユーザーは、読み取り権限や書き込み権限に関係なく、[Monitor Overview] ダッシュボードをカスタマイズできます。

[Monitor Overview] ダッシュボードのカスタマイズのメリット

- 柔軟性：ダッシュボードをカスタマイズすることで、最も重要なダッシュレットを表示できます。目的に合わないダッシュレットを削除して煩雑さを軽減できます。
- 効率性：すべての主要メトリックを一目で確認し、迅速に評価および分析できます。
- 簡単な編成：ダッシュレットをドラッグアンドドロップして、要件に応じてダッシュボードを編成できます。たとえば、特に重要なダッシュレットを上部に簡単にドラッグできます。

[Monitor Overview] ダッシュボードのカスタマイズに関する制限事項

最小リリース：Cisco vManage リリース 20.9.1

- マルチテナント展開の場合、この機能はテナントダッシュボードでのみ使用できます。
- この機能は、[Monitor Overview] ダッシュボードでのみ使用できます。
- [Monitor Overview] ダッシュボードの上部にあるメニューバーはカスタマイズできません。
- ダッシュボードが編集モードの場合、データを表示する期間の選択、リアルタイムデータの表示などの他のアクションは無効になります。

[Monitor Overview] ダッシュボードのカスタマイズ

最小リリース：Cisco vManage リリース 20.9.1

ダッシュレットの追加

1. Cisco vManage のメニューから**[Monitor]** > **[Overview]**の順に選択します。
2. [Actions] ドロップダウンリストから、[Edit Dashboard] を選択します。
3. [Add Dashlet] をクリックします。

（注） [Add Dashlet] オプションは、追加できるダッシュレットがある場合にのみ使用できます。デフォルトのダッシュボードでは使用できません。

4. 追加するダッシュレットを選択します。
5. [Add] をクリックします。
6. [Save] をクリックします。

ダッシュレットの削除

1. Cisco vManage のメニューから**[Monitor]** > **[Overview]**の順に選択します。
2. [Actions] ドロップダウンリストから、[Edit Dashboard] を選択します。
3. 対応するダッシュレット名の横にある [Delete] アイコンをクリックします。
4. ダッシュレットの削除を確定するには、[Yes] をクリックします。
5. [Save] をクリックします。

ダッシュレットの再配置

1. Cisco vManage のメニューから**[Monitor]** > **[Overview]**の順に選択します。
2. [Actions] ドロップダウンリストから、[Edit Dashboard] を選択します。
3. 要件に応じてダッシュレットをドラッグアンドドロップします。
4. [Save] をクリックします。

デフォルト設定の復元

1. Cisco vManage のメニューから**[Monitor]** > **[Overview]**の順に選択します。
2. [Actions] ドロップダウンリストから、[Reset to Default View] を選択します。
3. [Apply] をクリックします。

コントローラとデバイス情報の表示

[Monitor] > **[Overview]**ページの上部にあるメニューバーの [Controllers] および [WAN Edges] 領域には、オーバーレイ ネットワーク内の Cisco vSmart コントローラ、Cisco vBond オーケストレーション、Cisco vManage インスタンスの総数が表示されます。また、ネットワーク内のデバイスのステータスも表示されます。

デバイス番号をクリックすると、**[Monitor]** > **[Devices]**ページに各デバイスの詳細情報が表示されます。対応するデバイスの隣にある [...] をクリックして、デバイスダッシュボードまたはリアルタイムビューにアクセスするか、**[Tools]** > **[SSH Terminal]**にアクセスします。

Cisco vManage リリース 20.6.x 以前では、Cisco vManage の挙動は次のようになります。

- [Controllers] 領域と [WAN Edges] 領域は、[Summary] 領域にまとめられています（[Summary] 領域は**[Dashboard]** > **[Main Dashboard]** ページ内にあります）。
- デバイス番号をクリックすると、各デバイスの詳細情報が表示されたポップアップウィンドウが開きます。
- デバイスダッシュボードやリアルタイムビューは、**[Monitor]** > **[Network]**ページ内にあります。

Cisco vManage ステータスの表示

デバイスやコントローラの状態、およびCPUとメモリの使用状況に関する詳細をCisco vManageで表示できます。

1. Cisco vManage のメニューから**[Monitor]** > **[Devices]**の順に選択します。

   表の [Health] 列には、デバイスやコントローラの正常性が表示されます。列のアイコンにカーソルを合わせると、[Good]、[Fair]、[Poor] のいずれの状態であるかが表示されます。

   Cisco vManage コントローラの場合、正常性ステータスは次の状態を示します。

   - [Good]：使用可能なメモリの 75% 未満、および CPU リソースの 75% 未満が Cisco vManage で使用されています。
   - [Fair]：合計メモリまたは CPU の 75% ～ 90% が Cisco vManage で使用されています。
   - [Poor]：合計メモリまたは CPU の 90% 超が Cisco vManage で使用されています。

2. 表から Cisco vManage コントローラをクリックします。
3. [ECURITY MONITORING] で [System Status] をクリックします。

   [Device 360] ページには、CPU とメモリの使用率が表示されます。

（注） Cisco vManage コントローラで合計メモリまたは CPU の 90% 超が使用されている場合、パフォーマンスが低下する可能性があります。Cisco vManage にログインできない場合は、Cisco TAC までご連絡ください。

[Certificate Status] ペインの表示

[Certificate Status] ペインには、すべてのコントローラデバイス上にあるすべての証明書の状態が表示されます。また、期限切れや無効になった証明書の総数が表示されます。[Certificate Status] ペインをクリックして**[Monitor]** > **[Devices]** > **[Certificate]** ページを開きます。このページには、証明書がインストールされているデバイスのホスト名とシステム IP、証明書のシリアル番号、および有効期限の日付とステータスが表示されます。

（注） Cisco vManage リリース 20.6.x 以前では、Cisco vManage の挙動は次のようになります。

- [Certificate Status] ペインは**[Dashboard]** > **[Main Dashboard]**ページ内にあります。
- [Certificate Status] ペインをクリックすると、**[Monitor]** > **[Devices]** > **[Certificate]** ページの代わりにポップアップウィンドウが開きます。

[Licensing] ペインの表示

[Licensing] ペインには、設定されたデバイスの総数とライセンス付与されたデバイスの数が表示されます。[Licensing] ペインをクリックして**[Monitor]** > **[Devices]** > **[Licensing]**ページを開きます。このページには、デバイスに関する次の情報が表示されます。

- ホスト名
- シャーシ番号とデバイスモデル
- IP アドレス
- テンプレート名
- デバイスのスマートアカウントとバーチャルアカウント
- マスターソフトウェアライセンス契約（MSLA）

- デバイスのライセンスステータス
- ライセンスタイプとライセンス名
- サブスクリプション ID

（注） Cisco vManage リリース 20.6.x 以前では、Cisco vManage の挙動は次のようになります。

- [Licensing] ペインは**[Dashboard]** > **[Main Dashboard]**ページ内にあります。
- [Licensing] ペインをクリックすると、**[Monitor]** > **[Devices]** > **[Licensing]**ページの代わりにポップアップウィンドウが開きます。ポップアップウィンドウには、デバイス名、ライセンスが付与されたデバイス数、ライセンスの総数、および最後に割り当てられたステータスが表示されます。

[Reboot] ペインの表示

[Reboot] ペインには、ネットワーク内にあるすべてのデバイスについて、過去 24 時間の再起動の合計数が表示されます。これには、ソフト再起動とコールド再起動、およびデバイスの電源再投入の結果として発生した再起動が含まれます。[Reboot] をクリックすると、[Reboot] サイドバーが表示され、再起動のたびに再起動したデバイスのシステム IP とホスト名、再起動が発生した時刻、および再起動の理由が一覧で表示されます。同じデバイスが 2 回以上再起動すると、各再起動オプションが個別に報告されます。

[Reboot] サイドバーで [Crashes] をクリックすると、すべてのデバイスクラッシュについて、クラッシュが発生したデバイスのシステム IP とホスト名、クラッシュインデックス、コア時刻とファイル名が一覧で表示されます。

（注） Cisco vManage リリース 20.6.x 以前では、Cisco vManage の挙動は次のようになります。

- [Reboot] ペインは**[Dashboard]** > **[Main Dashboard]**ページ内にあります。
- [Reboot] をクリックすると、サイドバーの代わりにポップアップウィンドウが開きます。

[Control Status] ペインの表示

[Control Status] ペインは、Cisco vManage リリース 20.7.x 以前にのみ実装されています。

[Control Status] ペインには、Cisco vSmart および WAN エッジデバイスが必要な数の Cisco vSmart コントローラ に接続されているかどうかが表示されます。それぞれの Cisco vSmart コントローラ が、ネットワーク内の他のすべての Cisco vSmart コントローラ に接続されている必要があ

ります。各 WAN エッジルータは、設定された最大数の Cisco vSmart コントローラ に接続する必要があります。

[Control Status] ペインには、次の 3 つのカウントが表示されます。

- [Up]：必要な数の動作可能なコントロールプレーンが Cisco vSmart コントローラ に接続されているデバイスの総数。
- [Partial]：動作可能なコントロールプレーンの一部（すべてではない）が Cisco vSmart コントローラ に接続されているデバイスの総数。
- [Down]：Cisco vSmart コントローラ にコントロールプレーンが接続されていないデバイスの総数。

（注） [Control Status] ペインは、Cisco vManage コントロール接続と vSmart コントロール接続の両方の状態に依存します。

[UP]/[Down]/[Partial] データをクリックすると、**[Monitor]** > **[Devices]**ページが表示されます。目的のデバイスで [...] をクリックして、デバイスダッシュボードまたはリアルタイムビューにアクセスするか、**[Tools]** > **[SSH Terminal]**にアクセスします。

（注） Cisco vManage リリース 20.6.x 以前では、Cisco vManage の挙動は次のようになります。

- [Control Status] ペインは**[Dashboard]** > **[Main Dashboard]**ページ内にあります。
- [Up]、[Partial]、[Down] の各ステータスには、それぞれ [Control Up]、[Partial]、[Control Down] というタイトルが付けられています。
- ドーナツグラフの代わりにステータスバーにデータが表示されます。
- データをクリックすると、**[Monitor]** > **[Devices]**ページの代わりにポップアップウィンドウが開きます。

[BFD Connectivity] ペインの表示

サイトは、分散拠点、データセンター、キャンパスなど、 Cisco SD-WAN オーバーレイネットワーク内にある特定の物理的な場所です。各サイトは、サイト ID と呼ばれる一意の整数によって識別されます。サイトの各デバイスは、同じサイト ID で識別されます。

[Site BFD Connectivity] ペインには、サイトのデータ接続の状態が表示されます。サイトに複数の WAN エッジルータがある場合、このペインには、個々のデバイスではなくサイト全体の状態が表示されます。[Site BFD Connectivity] ペインには、次の 3 つの状態が表示されます。

- [Full]：すべての WAN Edge ルータのすべての BFD セッションが稼働状態にあるサイトの総数。

- [Partial]：TLOC またはトンネルが停止状態にあるサイトの総数。これらのサイトでは、データプレーン接続が制限されています。
- [Unavailable]：すべての WAN エッジルータのすべての BFD セッションが停止状態にあるサイトの総数。これらのサイトにはデータプレーン接続がありません。

（注） サイト数には、稼働中のデバイスが設置されているサイトのみが含まれます。サイトに設置されているデバイスのいずれかがダウンしている場合、または TLOC やトンネルがダウンしている場合（2 つのデバイスがあるサイト）、一部のサイトはサイト数から除外されます。

[Full]、[Partial]、または [Unavailable] ステータスをクリックすると、サイドバーが表示され、各サイト、ノード、トンネルの詳細情報が表示されます。**[Monitor]** > **[Devices]**ページで目的のデバイスの [...] をクリックして、デバイスダッシュボードまたはリアルタイムビューにアクセスするか、**[Tools]** > **[SSH Terminal]**にアクセスします。

（注） Cisco vManage リリース 20.6.x 以前では、Cisco vManage の挙動は次のようになります。

- [Site BFD Connectivity] ペインのタイトルは [Site Health] になります。[Site Health] ペインは **[Dashboard]** > **[Main Dashboard]**ページ内にあります。
- [Full]、[Partial]、[Unavailable] のステータスのタイトルは、それぞれ [Full WAN Connectivity]、[Partial WAN Connectivity]、[No WAN Connectivity] になります。
- データをクリックすると、サイドバーの代わりにポップアップウィンドウが開きます。
- デバイスダッシュボードやリアルタイムビューは、**[Monitor]** > **[Network]**ページ内にあります。

[Transport Interface Distribution] ペインの表示

[Transport Interface Distribution] ペインには、VPN 0 のすべての WAN エッジインターフェイスにおける過去 24 時間のインターフェイスの使用状況が表示されます。これには、すべての TLOC インターフェイスが含まれます。使用統計情報をクリックすると、サイドバーが現れ、システム IP、インターフェイス、およびインターフェイス使用状況の平均的な詳細が表示されます。

[View Percent Utilization] をクリックすると、すべての WAN エッジインターフェイスの過去 24 時間の使用状況がグラフィック形式で表示されます。このグラフでは、インターフェイス数に対する TLOC 使用率の分散 （%） について示されています。表形式の統計には、ホスト名、インターフェイス、平均/低/高アップストリーム（%）、平均/低/高ダウンストリーム（%）、および帯域幅使用率の情報が表示されます。

（注） Cisco vManage リリース 20.6.x 以前では、Cisco vManage の挙動は次のようになります。

- [Transport Interface Distribution] ペインは**[Dashboard]** > **[Main Dashboard]**ページ内にあります。
- 使用統計情報をクリックすると、サイドバーの代わりにポップアップウィンドウが開きます。

[WAN Edge Inventory] ペインの表示

[WAN Edge Inventory] ペインには、次の 4 つのカウントが表示されます。

- [Total]：認可されたシリアル番号が vManage サーバーにアップロードされている WAN エッジルータの総数。シリアル番号は**[Configuration]** > **[Devices]**ページでアップロードします。
- [Authorized]：オーバーレイネットワーク内で認可されている WAN エッジルータの総数。**[Configuration]** > **[Certificates]** > **[WAN Edge List]**ページで [Valid] と表示されているルータを指します。
- [Deployed]：導入されている WAN エッジルータの総数。ネットワークで現在稼働中で、[Valid] と表示されているルータを指します。
- [Staging]：ステージング状態の WAN エッジルータの総数。実際のブランチに出荷してオーバーレイネットワークの構成要素にする前に、ステージングサイトで構成するルータです。これらのルータは、ルーティングの決定には関与せず、 Cisco vManage によるネットワークモニタリングに影響を与えることもありません。

統計情報のいずれかをクリックするとサイドバーが現れ、ホスト名、システム IP、サイト ID などの各ルータの詳細が記載されたテーブルが表示されます。

（注） Cisco vManage リリース 20.6.x 以前では、Cisco vManage の挙動は次のようになります。

- [WAN Edge Inventory] ペインは**[Dashboard]** > **[Main Dashboard]**ページ内にあります。
- データをクリックすると、サイドバーの代わりにポップアップウィンドウが開きます。

[WAN Edge Health] ペインの表示

[WAN Edge Health] ペインには、各ルータの状態に関する集約されたビューと、その状態にある WAN エッジルータの数が表示され、ハードウェアノードの正常性が示されます。次の 3 つの状態があります。

- [Good]：メモリ、ハードウェア、CPUが良好な状態にあるルータの数。合計メモリまたは合計 CPU の使用率が 75% 未満の場合は、良好な状態に分類されます。
- [Fair]：メモリ、ハードウェア、CPU が普通の状態にあるルータの数。合計メモリまたは合計 CPU の使用率が 75% ～ 90% の場合は、普通の状態に分類されます。
- [Fair]：メモリ、ハードウェア、CPU が不良な状態にあるルータの数。合計メモリまたは合計 CPU の使用率が 90% を超える場合は、不良な状態に分類されます。

統計をクリックすると、サイドバーが表示され、過去 1 時間のメモリ使用量や CPU 使用率に加えて、温度、電源、PIMモジュールなどのハードウェア関連のアラームが記載されたテーブルが表示されます。**[Monitor]** > **[Devices]**ページで目的のホスト名の [...] をクリックして、デバイスダッシュボードまたはデバイス詳細ビューにアクセスするか、**[Tools]** > **[SSH Terminal]** ページにアクセスします。

（注） Cisco vManage リリース 20.6.x 以前では、Cisco vManage の挙動は次のようになります。

- [WAN Edge Health] ペインは**[Dashboard]** > **[Main Dashboard]**ページ内にあります。
- [Good]、[Fair]、および [Poor] ステータスには、それぞれ、[Normal]、[Warning]、および [Error] というタイトルが付けられています。
- ハードウェアノードは、合計メモリまたは合計 CPU の 75% ではなく 70% を使用している場合、正常状態に分類されます。同様に、合計メモリまたは合計 CPU の 70% ～ 90% の範囲ではなく、75% ～ 90% を使用している場合、警告状態に分類されます。
- データをクリックすると、サイドバーの代わりにポップアップウィンドウが開きます。
- デバイスダッシュボードやデバイス詳細ビューは、**[Monitor]** > **[Network]**ページ内にあります。

[Transport Health] ペインの表示

[Transport Health] ペインには、すべてのリンクとすべてのカラーの組み合わせ（すべての LTE-to-LTE リンク、すべての LTE-to-3G リンクなど）の集約された平均損失、遅延、およびジッターが表示されます。

- [Type] ドロップダウンリストから、損失、遅延、またはジッターを選択します。

- [Time] ドロップダウンリストをクリックして、データを表示する期間を選択できます。
- [View Details] をクリックすると、サイドバーに表形式で情報が表示されます。前述したように、表示するデータの種類と期間を変更できます。

（注） Cisco vManage リリース 20.6.x 以前では、Cisco vManage の挙動は次のようになります。

- [Transport Health] ペインは**[Dashboard]** > **[Main Dashboard]**ページ内にあります。
- ドロップダウンリストの代わりにフィルタアイコンを使用して、データの表示期間を指定します。
- [View Details] ボタンの代わりに展開アイコンを使用して、[Transport Health] ポップアップウィンドウを開きます。

[Top Applications] ペインの表示

Cisco vManage の**[Monitor]** > **[Overview]**ページの [Top Applications] ペインには、オーバーレイネットワーク内の WAN エッジルータを通過するトラフィックの SD-WAN アプリケーションインテリジェンス エンジン（SAIE）フロー情報が表示されます。

（注） Cisco vManage リリース 20.7.x 以前では、SAIE フローはディープ パケット インスペクション（DPI）フローと呼ばれていました。

VPN 別に上位のアプリケーションを一覧表示するには、ドロップダウンリストから VPN を選択します。データを表示する期間を選択するには、[Time] ドロップダウンリストをクリックします。

サイドバーに上位のアプリケーションを一覧表示するには、次の手順を実行します。

1. [View Details] をクリックして、[Top Applications] サイドバーを開くと、同じ情報がより詳細なビューで表示されます。
2. **SAIE アプリケーション**で [VPN] ドロップダウンリストから目的の VPN を選択し、[Search] をクリックします。

（注） Cisco vManage リリース 20.7.x 以前では、**SAIE アプリケーション**は **DPI アプリケーション**と呼ばれていました。

- [Chart] をクリックすると、アプリケーションの一覧が表示されます。
- [Details] をクリックすると、アプリケーションに関する詳細情報が表示されます。

3. [SSL Proxy] をクリックし、[View by Policy Actions] ドロップダウンリストからポリシーアクションを選択します。すべてのポリシーアクション（暗号化、非暗号化、復号）のビューがサポートされています。[VPN] ドロップダウンリストから目的の VPN を選択し、[Search] をクリックします。[Hour] オプションには、選択した時間の統計情報が表示されます。
   - [Chart] をクリックすると、SSL アプリケーションの一覧が表示されます。
   - [Details] をクリックすると、SSL アプリケーションに関する詳細情報が表示されます。
4. [X] をクリックしてウィンドウを閉じて、**[Monitor]** > **[Overview]**ページに戻ります。

（注） Cisco vManage リリース 20.6.x 以前では、Cisco vManage の挙動は次のようになります。

- [Top Applications] ペインは**[Dashboard]** > **[Main Dashboard]**ページ内にあります。
- ドロップダウンリストの代わりにフィルタアイコンを使用して、VPN オプションの一覧を表示し、データの表示期間を指定します。
- [View Details] ボタンの代わりに展開アイコンを使用して、[Top Applications] ポップアップウィンドウを開きます。

（注） フロー DPI データは、スケジュールに従って Cisco vManage によって収集されますが、ユーザーの要求に応じて処理されます。Flow DPI ベースのレポートは、データが処理された後に利用できます。

[Application-Aware Routing] ペインの表示

[Application-Aware Routing] ペインには、[Type] ドロップダウンリストで指定した基準（損失、遅延、ジッターなど）に基づいて、状態の最も悪い 10 のトンネルが表示されます。したがって、損失を選択した場合、このペインには、過去 24 時間の平均損失が最も大きい 10 のトンネルが表示されます。

任意の行をクリックすると、データがグラフィック形式で表示されます。データを表示する期間を選択するか、[Custom] をクリックして、カスタム期間を指定するためのドロップダウンを表示します。

[View Details] をクリックして、[Application-Aware Routing] サイドバーを開きます。[Type] ドロップダウンリストで指定した基準（損失、遅延、ジッターなど）に基づいて、状態の最も悪い 25 のトンネルが表示されます。

（注） Cisco vManage リリース 20.6.x 以前では、Cisco vManage の挙動は次のようになります。

- [Application-Aware Routing] ペインは**[Dashboard]** > **[Main Dashboard]**ページ内にあります。
- [View Details] ボタンの代わりに展開アイコンを使用して、[Application-Aware Routing] ポップアップウィンドウを開きます。

Web サーバーの証明書期限日通知の表示

認証証明書を使用して Web ブラウザと Cisco vManage サーバーの間のセキュアな接続を確立する際、**[Administration]** > **[Settings]**画面で証明書の有効期間を設定します。この期間が終了すると、証明書が期限切れになります。[Web Server Certificate] バーに、有効期限の日時が表示されます。

証明書の有効期限が切れる 60 日前から、Cisco vManage の**[Monitor]** > **[Overview]**ページには証明書の有効期限が近づいていることを示す通知が表示されます。この通知は、有効期限の 30 日前、15 日前、および 7 日前に再表示され、その後は毎日表示されます。

（注） Cisco vManage リリース 20.6.x 以前では、証明書の有効期限の通知は**[Dashboard]** > **[Main Dashboard]**ページに表示されます。

メンテナンス時間帯のアラート通知の表示

Cisco vManage サーバーで**[Administration]** > **[Settings]**に次のメンテナンス時間帯が設定されている場合、Cisco vManage の**[Monitor]** > **[Overview]** ページには、メンテナンス時間帯が開始する 2 日前にアラート通知が表示されます。

（注） Cisco vManage リリース 20.6.x 以前では、メンテナンス時間帯のアラート通知は **[Dashboard]** > **[Main Dashboard]**ページに表示されます。

セキュリティ

Cisco vManage では、**[Monitor]** > **[Security]**ページに次のペインがあります。

（注） Cisco vManage リリース 20.6.x 以前では、これらのペインは**[Dashboard]** > **[Security]**ページ内にあります。

- Firewall Enforcement
- Top Signature Hits
- URL Filtering
- Advanced Malware Protection

[Firewall Enforcement] ペインの表示

Cisco vManage のメニューから**[Monitor]** > **[Security]**の順に選択します。[Firewall Enforcement] ペインには、指定された期間に検査またはドロップされたセッションの数が表示されます。

アプリケーション認識機能を備えたシスコのエンタープライズファイアウォールは、柔軟で理解しやすいゾーンベースのモデルを使用してデータトラフィックを検査します。ゾーンベースのファイアウォールにより、TCP、UDP、および ICMP データトラフィックの検査が可能になります。ゾーンには、1 つ以上の VPN グループを含めることができます。VPN をゾーンにグループ化すると、ユーザーはオーバーレイネットワークにセキュリティ境界を確立できるため、ゾーン間を通過するすべてのデータトラフィックを制御できます。

ファイアウォールポリシーにより、送信元ゾーンから宛先ゾーンへのデータトラフィックフローを許可するために必要な一致条件が定義されます。ファイアウォールポリシーでは、IP プレフィックス、IP ポート、プロトコル TCP、UDP、ICMP、およびアプリケーションを一致条件にできます。プレフィックス、ポート、およびプロトコルが一致するフローを許可またはドロップし、パケットヘッダーをログに記録できます。

[Inspected] をクリックすると、検査されたデータセッション数が表示されます。

[Dropped] をクリックすると、ドロップされたパケット数が表示されます。

[Time] ドロップダウンリストをクリックして、データを表示する期間を選択できます。

[View Details] をクリックすると、[Firewall Enforcement] サイドバーが開き、同じ情報がより詳細なビューで表示されます。情報を表形式で表示するには、[Details] をクリックします。期間を変更して、指定した期間の詳細情報を表示できます。

（注） Cisco vManage リリース 20.6.x 以前では、Cisco vManage の挙動は次のようになります。

- [FireWall Enforcement] ペインは、**[Dashboard]** > **[Security]**ページ内にあります。
- ドロップダウンリストの代わりにフィルタアイコンを使用して、データの表示期間を指定します。

- [View Details] ボタンの代わりに展開アイコンを使用して、[FireWall Enforcement] ポップアップウィンドウを開きます。

[Top Signature Hits] ペインの表示

Cisco vManage のメニューから**[Monitor]** > **[Security]**の順に選択します。[Top Signature Hits] ペインには、指定された期間のシビラリティ（重大度）別またはカウント別に、侵入防御システム（IPS）のシグネチャ違反が表示されます。IPS では、Cisco Talos のシグネチャを使用してネットワークトラフィックがモニタリングされます。

[By Severity] をクリックして、シビラリティ（重大度）別にシグネチャ違反をフィルタリングできます。

[By Count] をクリックして、カウント別にシグネチャ違反をフィルタリングできます。

[Time] ドロップダウンリストをクリックして、データを表示する期間を選択できます。

[View Details] をクリックして、[Top Signature Hits] サイドバーを開くと、同じ情報がより詳細なビューで表示されます。情報を表形式で表示するには、[Details] をクリックします。期間を変更して、指定した期間の情報を表示できます。

（注） Cisco vManage リリース 20.6.x 以前では、Cisco vManage の挙動は次のようになります。

- [Top Signature Hits] ペインは、**[Dashboard]** > **[Security]**ページ内にあります。
- ドロップダウンリストの代わりにフィルタアイコンを使用して、データの表示期間を指定します。
- [View Details] ボタンの代わりに展開アイコンを使用して、[Top Signature Hits] ポップアップウィンドウを開きます。

[URL Filtering] ペインの表示

Cisco vManage のメニューから**[Monitor]** > **[Security]**の順に選択します。[URL Filtering] ウィンドウには、指定した期間にブロックまたは許可された URL の数と種類が表示されます。

[Blocked] をクリックすると、ブロックされた Web サイトのリストが表示されます。

[Allowed] をクリックすると、許可された Web サイトのリストが表示されます。

[Time] ドロップダウンリストをクリックして、データを表示する期間を選択できます。

[View Details] をクリックすると、[URL Filtering] サイドバーが開き、同じ情報がより詳細なビューで表示されます。情報を表形式で表示するには、[Details] をクリックします。期間を変更して、指定した期間の情報を表示できます。

（注） Cisco vManage リリース 20.6.x 以前では、Cisco vManage の挙動は次のようになります。

- [URL Filtering] ペインは、**[Dashboard]** > **[Security]**ページ内にあります。
- ドロップダウンリストの代わりにフィルタアイコンを使用して、データの表示期間を指定します。
- [View Details] ボタンの代わりに展開アイコンを使用して、[URL Filtering] ポップアップウィンドウを開きます。

[Advanced Malware Protection] ペインの表示

Cisco vManage のメニューから**[Monitor]** > **[Security]**の順に選択します。Cisco Advanced Malware Protection（AMP）は、ファイルレピュテーションに基づいてマルウェアをブロックし、不明なファイルを Cisco AMP Threat Grid にアップロードして詳細な分析を行います。このペインには、指定した期間のファイルレピュテーションおよびファイル分析イベントの数が表示されます。

[File Reputation] をクリックすると、選択した時間内に AMP によって検出された悪意のあるファイルの数が表示されます。

[File Analysis] をクリックすると、選択した時間間隔で Cisco AMP Threat Grid にアップロードされた不明ファイルの数が表示されます。

[Time] ドロップダウンリストをクリックして、データを表示する期間を選択できます。

[View Details] をクリックすると、[Advanced Malware Protection] サイドバーが開き、同じ情報がより詳細なビューで表示されます。情報を表形式で表示するには、[Details] をクリックします。期間を変更して、指定した期間の情報を表示できます。

（注） Cisco vManage リリース 20.6.x 以前では、Cisco vManage の挙動は次のようになります。

- [Advanced Malware Protection] ペインは**[Dashboard]** > **[Security]**ページ内にあります。
- ドロップダウンリストの代わりにフィルタアイコンを使用して、データの表示期間を指定します。
- [View Details] ボタンの代わりに展開アイコンを使用して、[Advanced Malware Protection] ポップアップウィンドウを開きます。

マルチクラウド

Cisco vManage では、**[Monitor]** > **[Multicloud]**ページに次のペインがあります。

（注） Cisco vManage リリース 20.6.x 以前では、これらのペインは**[Dashboard]** > **[Multicloud]**ページ内にあります。

- Amazon Web Service
- Google Cloud Platform
- Microsoft Azure
- Megaport

これらのペインの詳細については、『Cisco SD-WAN Cloud OnRamp Configuration Guide』[英語]を参照してください。

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。