アラーム、イベント、ログ

アラーム

オーバーレイネットワークの個々のデバイスでイベントが発生すると、デバイスは通知をCisco vManage に送信して報告します。次に、Cisco vManage はイベント通知をフィルタリングしてから関連するイベントを相互に関連付けし、やや重大なイベントと重大なイベントをアラームに統合します。

Cisco vManage で生成されるアラームのリストについては、「永続的なアラームとアラームフィールド」を参照してください。

[Alarms] 画面では、オーバーレイネットワーク内のコントローラとルータによって生成されたアラームに関する詳細情報を表示できます。

アラームの状態

Cisco vManage アラームには、シビラリティ（重大度）に基づいてステータスが割り当てられます。

- Critical（赤）：オーバーレイネットワーク機能の動作を損なう、またはシャットダウンを引き起こす重大なイベント。
- Major（黄）：ネットワーク機能の動作に影響を与えるが、シャットダウンを引き起こすことのない重大なイベント。

- Medium（青）：ネットワーク機能のパフォーマンスを損なう可能性のあるイベント。
- Minor（緑）：ネットワーク機能のパフォーマンスを低下させる可能性のあるイベント。

通常、シビラリティ（重大度）が Critical または Major のアラームがアクティブとして一覧表示されます。

Cisco vManage が受信した通知イベントがアラーム条件が経過したことを示すと、ほとんどのアラームは自動的にクリアされます。その後、Cisco vManage はアラームをクリア済みとしてリストし、アラームの状態は通常、Medium または Minor に変わります。

Cisco vManage リリース 20.5.1 でのアラームの変更

表 *1*: 機能の履歴

機能	リリース情報	説明
アラームの最適化	Cisco IOS XE リリース 17.5.1a Cisco SD-WAN リリース 20.5.1 Cisco vManage リリース 20.5.1	この機能は、重複したアラームを自動的に抑制することで、Cisco vManage のアラームを最適化します。これにより、問題の原因となっているコンポーネントを簡単に特定できます。 これらのアラームを表示するには、Cisco vManage のメニューから**[Monitor]** > **[Logs]** > **[Alarms]**の順に選択します。

サイトがダウンすると、Cisco vManage は次のアラームを報告します。

- サイトの停止
- ノードの停止
- TLOC の停止

Cisco vManage は、停止しているコンポーネントごとにアラームを表示します。サイトのサイズによっては、ノードアラームだけでなく、ノード内の各 TLOC のアラームなど、重複したアラームが何度も表示される場合があります。Cisco vManage リリース 20.5.1 では、Cisco vManage が重複したアラームをインテリジェントに抑制します。たとえば、ノード内のすべての TLOC が停止している場合、Cisco vManage は各 TLOC からのアラームを抑制し、ノードからのアラームだけを表示します。マルチテナント構成の場合、各テナントでは、そのテナント内のサイトに関するアラームが表示されます。

シナリオ	表示されるアラーム	
Cisco vManage リリース 20.5.1	以前のリリース	

シナリオ	表示されるアラーム	
リンク 1 が停止 リンク 2 が稼働	bfd-tloc-1_down	bfd-tloc-1_down
リンク 1 が停止 リンク 2 が停止	bfd-site-1_down bfd-node-1_down、bfd-tloc-1_down、および bfd-tloc-2_down は、サイトアラームによって抑制されます。	bfd-site-1_down bfd-tloc-1_down
リンク 1 が稼働 リンク 2 が停止	bfd-site-1_up bfd-node-1_up bfd-tloc-1_up bfd-tloc-2_up	bfd-site-1_up bfd-tloc-1_up

アラーム表示

上部のバーにあるアラームベルアイコンをクリックすると、Cisco vManage ダッシュボードからアラームを表示できます。アラームベルでは、アクティブアラームまたはクリア済みアラームにグループ化されています。

または、次の手順に従って、Cisco vManage の [Alarms] 画面からアラームを表示します。

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

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

   アラームはグラフィック形式と表形式で表示されます。

2. 特定のアラームの詳細を表示するには、目的のアラームで[…]をクリックしてから、[Alarm Details] をクリックします。

   [Alarm Details] ウィンドウが開き、アラームの考えられる原因、影響を受けるエンティティなどの詳細が表示されます。

アラームフィルタの設定

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

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

2. [Filter] をクリックします。

3. [Severity] フィールドで、ドロップダウンリストからアラームのシビラリティ（重大度）レベルを選択します。複数のシビラリティ（重大度）レベルを指定できます。

4. [Active] フィールドで、ドロップダウンリストからアクティブアラーム、クリア済みのアラーム、または両方のタイプのアラームを選択します。アクティブアラームは、現在デバイス上にあるが、まだ認識されていないアラームです。
5. [Alarm Name] フィールドで、ドロップダウンリストからアラーム名を選択します。アラーム名は複数指定できます。
6. [Search] をクリックして、フィルタ条件に一致するアラームを検索します。

Cisco vManage では、アラームが表形式とグラフィック形式の両方で表示されます。

アラームデータを CSV 形式でエクスポートする

すべてのアラームのデータを CSV 形式のファイルにエクスポートするには、[Download] アイコンをクリックします。

Cisco vManage では、すべてのデータが CSV 形式でアラームテーブルから Excel ファイルにダウンロードされます。ファイルはブラウザのデフォルトのダウンロード場所にダウンロードされ、Alarms.csv という名前が付けられます。

グラフに表示されるアラームデータは、Excel ファイルでも参照できます。

たとえば、2022 年 2 月 15 日午前 3:30 の日時でグラフにアラームデータ（Critical 2、Major 274、Medium 4、Minor 405）が表示される場合、2022 年 2 月 15 日午前 3:00 から 2022 年 2 月 15 日午前 3:29 までの日時の範囲で、同じアラームデータが Excel ファイルでも使用できます。

電子メール通知の有効化

オーバーレイネットワーク内のデバイスでアラームが発生したときに電子メール通知を送信するように Cisco vManage を設定できます。これには、最初に SMTP および電子メール受信者のパラメータを設定する必要があります。まず、次の画面で SMTP および電子メール受信者のパラメータを設定します。

1. Cisco vManage のメニューから **[Administration]** > **[Settings]** の順に選択します。
2. [Alarm Notifications] オプションの横にある [Edit] をクリックします。
3. [Enable Email Notifications] で [Enabled] を選択します。
4. [Email Settings] チェックボックスをオンにします。
5. 電子メール通知を送信する際のセキュリティレベルを選択します。セキュリティレベルには、[None]、[SSL]、または [TLS] を指定できます。
6. [SMTP Server] フィールドには、電子メール通知を受信する SMTP サーバーの名前または IP アドレスを入力します。
7. [SMTP Port] フィールドに、SMTP ポート番号を入力します。セキュリティなしの場合、デフォルトのポートは 25 です。 SSL の場合は 465、TLS の場合は 587 です。
8. [From Address] フィールドには、電子メール通知の送信者として表示する電子メールアドレスを入力します。

9. [Reply to address] フィールドには、電子メールの [Reply-To] フィールドに表示する電子メールアドレスを入力します。このアドレスには、noreply@cisco.com などの返信不可アドレスを指定できます。

10. [Use SMTP Authentication] チェックボックスをオンにして、SMTP サーバーへの SMTP 認証を有効にします。

    SMTP 認証で使用するユーザー名とパスワードを入力します。デフォルトユーザーの電子メールサフィックスが、ユーザー名に付加されます。入力したパスワードは非表示になります。

11. [Save] をクリックします。

（注） 電子メールは、送信元インターフェイスとして VPN0（トランスポート インターフェイス）の vManage パブリック IP から送信されます。

アラーム通知の送信

開始する前に、電子メール通知が**[Administration]** > **[Settings]**で有効になっていることを確認します。[Alarm Notifications] の横にある [Edit] をクリックして、[Alarm Notifications] が有効になっているかどうか、また [Email Settings] チェックボックスがオンになっているかどうかを確認します。

アラームの発生時に電子メール通知を送信するには、次の手順を実行します。

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

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

2. [Alarm Notifications] をクリックします。設定されている通知リストが、表に表示されます。

3. [Add Alarm Notification] をクリックします。

4. [Name] フィールドに、電子メール通知の名前を入力します。名前の最大長は 128 文字で、英数字のみを使用できます。

5. [Severity] フィールドで、ドロップダウンリストからアラームのシビラリティ（重大度）レベルを 1 つ以上選択します。

6. [Alarm Name] フィールドで、1 つ以上のアラームを選択します。

7. [Account Details] では、次の情報を入力します。

   1. [Email] フィールドに、電子メールアドレスを 1 つ以上入力します。

   2. （任意）[Add New Email List] をクリックし、必要に応じて電子メールリストを入力します。

   3. [Email Threshold] フィールドでは、1 分あたりに送信する電子メールの最大数を設定します。1 から 30 までの値を指定できます。デフォルトは 5 です。

4. [WebHook] チェックボックスをオンにすると。アラーム通知イベントが発生したときに HTTP コールバックをトリガーされます。
   1. [WebHook URL] フィールドには、ウェブフックサーバーの URL を入力します。
   2. ウェブフックサーバーを認証するためのユーザー名とパスワードを [Username] と [Password] にそれぞれ入力します。
   3. [WebHook Threshold] フィールドに、しきい値を入力します。

（注） 入力した値は、そのウェブフック URL で 1 分あたりに発行される通知の数を示します。たとえば、[WebHook Threshold] が 2 の場合、そのウェブフック URL の通知を 1 分あたり 2 つ受け取ります。しきい値を超えて生成された通知はドロップされます。

8. [Selected Devices] では、[All Devices] または [Custom] を選択します。

   [Custom] を選択すると、デバイスリストが表示されます。
   1. 左側の [Available Devices] リストで、1 つ以上のデバイスを選択します。
   2. 右矢印をクリックして、デバイスを右側の [Selected Devices] リストに移動します。
   3. [Add] をクリックします。
9. [Add] をクリックします。

電子メール通知の表示および編集

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

   Cisco vManage のメニューから**[Monitor]** > **[Alarms]**の順に選択します。
2. [Alarm Notifications] をクリックします。設定されている通知リストが、表に表示されます。
3. 目的の通知で、行の右側にある [View] アイコンをクリックします。
4. 通知の表示が完了したら、[OK] をクリックします。

電子メール通知の編集

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

   Cisco vManage のメニューから**[Monitor]** > **[Alarms]**の順に選択します。
2. [Alarm Notifications] をクリックします。設定されている通知リストが、表に表示されます。
3. 目的の電子メール通知で、[Edit] アイコンをクリックします。
4. 通知の編集が完了したら、[Update] をクリックします。

電子メール通知の削除

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

   Cisco vManage のメニューから**[Monitor]** > **[Alarms]**の順に選択します。
2. [Alarm Notifications] をクリックします。設定されている通知リストが、表に表示されます。
3. 目的の電子メール通知で、[Trash Bin] アイコンをクリックします。
4. 確認ダイアログボックスで、[OK] をクリックします。

イベント

表 *2 :* 機能の履歴

機能名	リリース情報	説明
Cisco IOS XE SD-WAN デバイス のイベント通知サポート	Cisco IOS XE リリース 17.2.1r	Cisco IOS XE SD-WAN デバイス でイベント通知のサポートが追加されました。

[Events screen] 画面を使用して、Cisco SD-WAN デバイスで生成されたイベントに関する詳細情報を表示できます。

イベントフィルタの設定

1 つ以上の Cisco SD-WAN デバイスで生成されたイベントを検索するためのフィルタを設定するには、次の手順を実行します。

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

   Cisco vManage のメニューから**[Monitor]** > **[Events]**の順に選択します。
2. [Filter] をクリックします。
3. [Severity] フィールドをクリックし、ドロップダウンリストからシビラリティ（重大度）レベルを選択します。

   Cisco SD-WAN デバイスで生成されたイベントは Cisco vManage によって収集されて、次のように分類されます。

   - Critical：すぐにアクションを実行する必要があることを示します。
   - Major：問題を調査する必要があるが、ネットワークをダウンさせるほど重大ではないことを示します。
   - Minor：情報提供のみです。

   複数のシビラリティ（重大度）レベルを指定できます。

1. [Component] フィールドでは、ドロップダウンリストから、イベントの原因となった 1 つ以上の構成コンポーネントを選択します。
2. [System IP] フィールドでは、生成されたイベントを表示するデバイスのシステム IP をドロップダウンリストから選択します。
3. [Event Name] フィールドでは、生成されたイベントを表示するイベント名をドロップダウンリストから選択します。複数のイベント名を選択できます。
4. [Search] をクリックして、フィルタ条件に一致するイベントを検索します。

Cisco vManage では、イベントが表形式とグラフィック形式の両方で表示されます。

イベントデータを CSV 形式でエクスポートする

すべてのイベントのデータを CSV 形式のファイルにエクスポートするには、[Download] アイコンをクリックします。

Cisco vManage では、すべてのデータが CSV 形式でイベントテーブルから Excel ファイルにダウンロードされます。ファイルはブラウザのデフォルトのダウンロード場所にダウンロードされ、Events.csv という名前が付けられます。

デバイスの詳細の表示

イベントが生成されたデバイスに関する詳細情報を表示するには、次の手順を実行します。

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

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

   このウィンドウには、イベントがグラフィック形式と表形式の両方で表示されます。
2. デバイスで生成されたイベントに関する詳細情報を表示するには、表からイベントの行を選択します。
3. 目的のデバイスで […] をクリックし、[Device Details] を選択します。

   [Device Details] ダイアログボックスが開き、イベントを発生させたデバイスのホスト名などの詳細が表示されます。

CLI の使用

CLI を使用して、Cisco vEdge デバイス でイベントが生成されたデバイスに関する情報を表示する場合は、**show notification stream viptela** コマンドを使用できます。コマンドの出力例を以下に示します。出力の最初の行は、メッセージが生成された時刻（SNMP eventTime）を示しています。時刻はデバイスの現地時間ではなく、UTC 形式で表示されます。通知の 2 行目にはイベントの説明が表示され、3 行目ではシビラリティ（重大度）レベルが示されます。

```
vEdge# show notification stream viptela
notification
 eventTime 2015-04-17T14:39:41.687272+00:00
 bfd-state-change
  severity-level major
  host-name vEdge
```

```
  system-ip 1.1.4.2
  src-ip 192.168.1.4
  dst-ip 108.200.52.250
  proto ipsec
  src-port 12346
  dst-port 12406
  local-system-ip 1.1.4.2
  local-color default
  remote-system-ip 1.1.9.1
  remote-color default
  new-state down
 !
!
notification
 eventTime 2015-04-17T15:12:20.435831+00:00
 tunnel-ipsec-rekey
  severity-level minor
  host-name vEdge
  system-ip 1.1.4.2
  color default
 !
!
notification
 eventTime 2015-04-17T16:56:50.314986+00:00
 system-login-change
  severity-level minor
  host-name vEdge
  system-ip 1.1.4.2
  user-name admin
  user-id 9890
 !
```

CLI を使用して、Cisco IOS XE SD-WAN デバイス でイベントが生成されたデバイスに関する情報を表示する場合は、**show sdwan notification stream** コマンドを使用できます。コマンドの出力例を以下に示します。出力の最初の行は、メッセージが生成された時刻（SNMP eventTime）を示しています。時刻はデバイスの現地時間ではなく、UTC 形式で表示されます。通知の 2 行目にはイベントの説明が表示され、3 行目ではシビラリティ（重大度）レベルが示されます。

```
Device# show sdwan notification stream
notification
 eventTime 2020-03-03T02:50:04.211317+00:00
sla-change
  severity-level major
  host-name SanJose
  system-ip 4.4.4.103
  src-ip 10.124.19.15
  dst-ip 10.74.28.13
  proto ipsec
  src-port 12426
  dst-port 12346
  local-system-ip 4.4.4.103
  local-color default
  remote-system-ip 4.4.4.106
  remote-color biz-internet
  mean-loss 17
  mean-latency 13
  mean-jitter 19
  sla-classes None
  old-sla-classes Voice-And-Video
!
!
```

Cisco IOS XE リリース 17.6.3 以降では、**alarms alarm bfd-state-change syslog** コマンドを使用して、デバイスの BFD 状態変化イベントが発生した場合に BFD 状態変化の syslog メッセージを表示できます。詳細については、alarms alarm bfd-state-change syslog のコマンドページを参照してください。

```
Device(config-system)# alarms alarm bfd-state-change syslog
Device(config-alarm-bfd-state-change)# commit
```

BFD 状態変化の syslog メッセージの例を以下に示します。

```
Jul 10 07:09:07.583: %Cisco-SDWAN-vm5-FTMD-5-NTCE-1000009: BFD-session 10.1.15.15:12346
 -> 10.1.16.16:12366,
local-tloc-index: 32775 -> remote-tloc-index: 32777, TLOC- local sys-ip: 172.16.255.15,
 local color: lte -> remote
sys-ip: 172.16.255.16, remote color: lte, encap: IPSEC, new state->UP delete:false,
reason:REMOTE_FSM
```

BFD 状態変化を有効にした後の実行コンフィギュレーション：

```
 Device# show sdwan running-config
system
 gps-location latitude 35.0
 gps-location longitude -120.0
 system-ip             170.16.1.1
 simulated-devices     27 2
 simulated-color       red blue
 simulated-wan-ip      192.168.1.1
 domain-id             1
 site-id               10000
 admin-tech-on-failure
 organization-name     "vIPtela Inc Regression"
 vbond 10.0.12.26
 alarms alarm bfd-state-change
  syslog
 !
!
```

イベント通知のモニタリング

表 *3*: 機能の履歴

機能名	リリース情報	説明
OMP エージェントおよび SD-WAN サブシステムのイベントトレースのモニタリング	Cisco IOS XE リリース 17.2.1r Cisco SD-WAN リリース 20.1.1	この機能により、指定した SD-WAN サブシステムのイベントトレース機能をモニタリングおよび制御できます。イベントトレースは、SD-WAN デーモンと SD-WAN サブシステム間の SD-WAN トレースをキャプチャする機能を提供します。

オーバーレイネットワーク内の個々のデバイスで問題が発生すると、デバイスは次の方法でイベントを報告します。

- Cisco vManage に通知を送信します。Cisco vManage はイベント通知をフィルタリングしてイベントを相互に関連付けて、やや重大なイベントと重要なイベントをアラームに統合します。
- 設定されたトラップターゲットに SNMP トラップを送信します。デバイスは SNMP トラップを生成するたびに、対応する通知メッセージも生成します。
- システムロギング（syslog）メッセージを生成し、ローカルデバイスの /var/log ディレクトリにある syslog ファイルに保存します。設定に応じて、リモートデバイスにも保存します。

通知はデバイスから Cisco vManage サーバーに送信されるメッセージです。

指定した SD-WAN サブシステムのイベントトレース機能をモニタリングおよび制御するには、特権 EXEC モードで **monitor event-trace** コマンドを実行します。イベントトレースは、SD-WAN デーモンと SD-WAN サブシステム間の SD-WAN トレースをキャプチャする機能を提供します。コマンドの詳細については、monitor event-trace sdwan および show monitor event-trace sdwan のコマンドページを参照してください。

ACL ログ

[ACL Log] 画面では、ルータに設定されているアクセスリスト（ACL）のログを表示できます。ルータは 10 分ごとに ACL ログを収集します。

ACL ログフィルタの設定

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

   Cisco vManage リリース 20.6.x 以前：Cisco vManage のメニューから**[Monitor]** > **[ACL Log]** の順に選択します。
2. [Filter] をクリックします。
3. [VPN] フィールドで、ドロップダウンリストから ACL ログを収集するエンティティを選択します。選択できる VPN は 1 つだけです。
4. [Search] をクリックして、フィルタ条件に一致するログを検索します。

Cisco vManage ではアクティビティのログが表形式で表示されます。

監査ログ情報の表示

監査ログフィルタの設定

表 *4:* 機能の履歴

機能名	リリース情報	説明
監査ログを使用したテンプレート設定変更の比較	Cisco IOS XE リリース 17.9.1a Cisco vManage リリース 20.9.1	この機能には、デバイステンプレートと機能テンプレートの監査ログ用の **Config Diff** オプションが導入されています。**Config Diff** オプションにより、現在の設定と以前の設定を比較してテンプレート設定の変更箇所が表示されます。 テンプレートがデバイスにアタッチされていない場合、**Config Diff** オプションを監査ログで使用して、設定の変更箇所を表示できます。

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

   Cisco vManage リリース 20.6.x 以前：Cisco vManage のメニューから**[Monitor]** > **[Audit Log]** の順に選択します。

2. [Filter] をクリックします。
3. [Module] フィールドで、監査ログを収集するエンティティを選択します。複数のエンティティを選択できます。
4. [Search] をクリックして、フィルタ条件に一致するログを検索します。

Cisco vManage ではアクティビティのログが表形式とグラフィック形式の両方で表示されます。

監査ログデータを CSV 形式でエクスポートする

すべての監査ログのデータを CSV 形式のファイルにエクスポートするには、[Export] をクリックします。

Cisco vManage では、すべてのデータが CSV 形式で監査ログテーブルから Excel ファイルにダウンロードされます。ファイルはブラウザのデフォルトのダウンロード場所にダウンロードされ、Audit_Logs.csv という名前が付けられます。

監査ログの詳細を表示する

監査ログに関する詳細情報を表示するには、次の手順を実行します。

1. テーブルからの監査ログの行を選択します。
2. 目的の行で […] をクリックし、[Audit Log Details] を選択します。

[Audit Log Details] ダイアログボックスが開き、監査ログの詳細が表示されます。

設定テンプレートの変更箇所の表示

テンプレートの以前の設定と現在の設定を比較した変更箇所を表示できます。テンプレート設定の変更箇所を表示するには、次の手順を実行します。

1. テーブル内の監査ログの行をクリックします。テーブルではモジュールタイプがテンプレートになります。
2. テンプレートモジュールの隣にある [...] をクリックし、[Config Diff] をクリックします。

   [Config Difference] ペインには、テンプレートの元の設定と、設定に加えられた変更との相違点が並べて表示されます。変更をインラインで表示するには、[Inline Diff] をクリックします。

デバイスの更新後の設定を表示するには、[Configuration] をクリックします。

Cisco IOS XE リリース 17.6.1a および Cisco SD-WAN リリース 20.6.1 以降では、テンプレートとポリシー設定の変更については、[Audit Logs] オプションを使用すると、実行されたアクションが表示されます。アクション前の設定と現在の設定を表示するには、[Audit Log Details] をクリックします。デバイステンプレート、機能テンプレート、ローカライズされたポリシー、一元化されたポリシー、およびセキュリティポリシーを作成、更新、削除すると、監査ログが収集されます。監査ログには、テンプレートやポリシーがアタッチされている場合とアタッチされていない場合の API ペイロードの変更箇所が表示されます。

設定テンプレートアクティビティのログの表示

設定テンプレートの作成に関連するアクティビティのログ、デバイスと設定テンプレートの関連付けのステータスを表示するには、次の手順を実行します。

1. Cisco vManage のメニューから、**[Configuration]** > **[Devices]** の順に選択します。
2. [WAN Edge List] または [Controllers] を選択し、デバイスを選択します。
3. 目的のデバイスで […] をクリックし、[Template Log] を選択します。

syslog メッセージ

オーバーレイネットワーク内の個々のデバイスで問題が発生した場合、デバイスは報告方法の 1 つとして、システムログ （syslog） メッセージを生成し、ローカルデバイスの /var/log ディレクトリ内にある syslog ファイルに記録します。設定すれば、リモートデバイスに記録することも可能です。

Cisco SD-WAN デバイスでは、イベント通知システムログ（syslog）メッセージをローカルデバイスまたはリモートホスト、あるいはその両方のファイルに記録できます。ローカルデバイスでは、syslog ファイルは /var/log ディレクトリに配置されます。

システムロギングの設定

デフォルトでは、優先度レベルが「エラー」の syslog メッセージをローカルデバイスのハードディスクに記録するように設定されています。ログファイルは、ローカルの /var/log ディレクトリに配置されます。デフォルトでは、ログファイルのサイズは 10 MB で、最大 10 個のファイルが保存されます。10 個のファイルが作成されると、最も古いファイルが破棄され、新しい syslog メッセージ用のファイルが作成されます。

デフォルトの syslog パラメータを変更するには、Cisco vManage からロギング機能テンプレートを使用します。CLI から、デバイス設定で **logging disk** または **logging server** コマンドを含めます。

syslog ロギング情報の表示

1. Cisco vManage のメニューから**[Administration]** > **[Settings]**の順に選択し、[Data Stream] が有効になっていることを確認します。
2. Cisco vManage のメニューから**[Monitor]** > **[Devices]**の順に選択し、表示されるデバイスリストからデバイスを選択します。

   Cisco vManage リリース 20.6.x 以前：Cisco vManage のメニューから**[Monitor]** > **[Network]** の順に選択し、表示されるデバイスリストからデバイスを選択します。
3. 左ペインで [Troubleshooting] をクリックします。
4. [Logs] 領域で [Debug Log] をクリックします。
5. [Log Files] フィールドで、ログファイル名を選択します。画面の下部にログ情報が表示されます。

CLI から syslog ファイルの内容を表示するには、**show log** コマンドを使用します。次に例を示します。

```
Device# show log auth.log tail 10==> /var/log/auth.log <==auth.info: Nov 14 14:33:35
vedge sshd[2570]: Accepted publickey for admin from 10.0.1.1 port 39966 ssh2: RSA
SHA256:pkFQ5wE//DmiA0d0JU1rOt91CMTVGkscm9wLSYQrI1sauth.info: Nov 14 14:39:42 vedge
sshd[2578]: Received disconnect from 10.0.1.1 port 39966:11: disconnected by userauth.info:
 Nov 14 14:39:42 vedge sshd[2578]: Disconnected from 10.0.1.1 port 39966auth.info: Nov
16 10:51:45 vedge sshd[6106]: Accepted publickey for admin from 10.0.1.1 port 40012 ssh2:
 RSA SHA256:pkFQ5wE//DmiA0d0JU1rOt91CMTVGkscm9wLSYQrI1sauth.info: Nov 16 11:21:55 vedge
```

```
 sshd[6108]: Received disconnect from 10.0.1.1 port 40012:11: disconnected by
userauth.info: Nov 16 11:21:55 vedge sshd[6108]: Disconnected from 10.0.1.1 port
40012auth.info: Nov 17 12:59:52 vedge sshd[15889]: Accepted publickey for admin from
10.0.1.1 port 40038 ssh2: RSA SHA256:pkFQ5wE//DmiA0d0JU1rOt91CMTVGkscm9wLSYQrI1sauth.info:
 Nov 17 13:45:13 vedge sshd[15894]: Received disconnect from 10.0.1.1 port 40038:11:
disconnected by userauth.info: Nov 17 13:45:13 vedge sshd[15894]: Disconnected from
10.0.1.1 port 40038auth.info: Nov 17 14:47:31 vedge sshd[30883]: Accepted publickey for
 admin from 10.0.1.1 port 40040 ssh2: RSA
SHA256:pkFQ5wE//DmiA0d0JU1rOt91CMTVGkscm9wLSYQrI1s
```

デバイスのシステムロギングの設定を表示するには、CLI から **show logging** コマンドを実行します。次に例を示します。

```
Device# show logging
System logging to host  in vpn 0 is disabled
Priority for host logging is set to: emerg

System logging to disk is disabled
Priority for disk logging is set to:  err
File name for disk logging is set to:  /var/log/vsyslog
File size for disk logging is set to:  10 MB
File recycle count for disk logging is set to:  10

Syslog facility is set to: all facilities
```

システムのログファイル

デフォルトまたは設定された優先度の値以上の syslog メッセージは、ローカルデバイスの /var/log ディレクトリ内にあるいくつかのファイルに記録されます。ファイルの種類は次のとおりです。

- auth.log：ログイン、ログアウト、スーパーユーザーのアクセスイベント、および認可システムの使用状況。
- kern.log：カーネルメッセージ
- messages：すべてのソースからの syslog メッセージが記録された統合ログファイル
- vconfd：設定に関するすべての syslog メッセージ
- vdebug：デバッグ機能が有効になっているモジュールのすべてのデバッグメッセージ、および設定された優先度の値を超えるすべての syslog メッセージ。デバッグロギングは、モジュールに基づいてさまざまなレベルのロギングをサポートします。実装されているロギングレベルは、モジュールごとに異なります。たとえば、システムマネージャ（sysmgr）には 2 つのロギングレベル（オンとオフ）があり、シャーシマネージャ（chmgr）には 4 つの異なるロギングレベル（オフ、低、標準、高）があります。デバッグメッセージをリモートホストに送信することはできません。デバッグを有効にするには、**debug** 操作コマンドを使用します。
- vsyslog：設定された優先度の値を超える Cisco SD-WAN プロセス（デーモン）からのすべての syslog メッセージ。デフォルトの優先度の値は「informational」（重大度レベル 6）であるため、デフォルトでは「notice」、「warning」、「error」、「critical」、「alert」、および「emergency」のすべての syslog メッセージ（重大度レベル 5 ～ 0）が保存されます

Cisco SD-WAN ソフトウェアは、/var/log にある標準の Linux ファイル（cron.log、debug、lpr.log、mail.log、syslog）をロギングに使用しません。

syslog ファイルへのメッセージの書き込みに、レート制限はありません。つまり、短時間に多くの syslog メッセージが生成された場合、オーバーフローメッセージはバッファに入れられ、syslog ファイルに書き込まれるまでキュー内に置かれます。オーバーフローメッセージはドロップされません。

syslog メッセージが繰り返された場合（連続して同一メッセージが複数回発生）、メッセージは 1 回だけ syslog ファイルに記録されます。メッセージの発生回数を示す注釈がメッセージに付けられています。

syslog メッセージの最大長は 1024 バイトです。それより長いメッセージは切り捨てられます。

AAA 認証および Netconf CLI のアクセス状況と使用状況に関連する syslog メッセージは、auth.log およびメッセージファイルに記録されます。Cisco vManage が Cisco vEdge デバイス にログインして統計情報とステータス情報を取得し、ファイルをルータにプッシュするたびに、ルータは AAA 認証と Netconf のログメッセージを生成します。したがって、時間の経過とともに、これらのメッセージでログファイルがいっぱいになる可能性があります。これらのメッセージでログファイルがいっぱいにならないようにするには、AAA 認証と Netconf の syslog メッセージのロギングを無効にします。

```
Device(config)# system aaa logsViptela(config-logs)# audit-disableViptela(config-logs)#
 netconf-disable
```

syslog メッセージ形式

Cisco SD-WAN ソフトウェアによって生成される syslog メッセージの形式は次のとおりです。

```
facility.source
date - source - module - level - MessageID: text-of-syslog-message
```

syslog メッセージの例を次に示します。このログのファシリティは local7、レベルは「notice」です。

syslog メッセージの頭字語

次の頭字語は、syslog メッセージやメッセージの説明で使用されます。

表 *5:*

略語	意味
confd	CLI 設定プロセス
FIM	転送テーブルマネージャ
FP	転送プロセス
RIM	ルートテーブルマネージャ

略語	意味
TIM	トンネルテーブルマネージャ

生成された各種 syslog メッセージのリストを表示するには、付録の「syslog メッセージ」を参照してください。

認定アクティビティログの表示

証明書関連のアクティビティのステータスを表示するには、Cisco vManage の**[Configuration]** > **[Certificates]**ウィンドウを使用します。

1. Cisco vManage ツールバーから、タスクアイコンをクリックします。Cisco vManage には、すべての実行中タスクのリストと、成功と失敗の合計数が表示されます。
2. 行をクリックして、タスクの詳細を表示します。Cisco vManage ではステータスウィンドウが開き、タスクのステータスとタスクが実行されたデバイスの詳細が表示されます。

Cisco SD-WAN デーモンのバイナリトレース

表 *6:* 機能の履歴

機能名	リリース情報	説明
Cisco SD-WAN デーモンのバイナリトレース	Cisco IOS XE リリース 17.4.1a	バイナリトレースにより、Cisco SD-WAN デーモンのトラブルシューティングが強化されます。バイナリトレース機能は、デーモンからのメッセージをバイナリ形式で記録します。メッセージはバイナリ形式で高速に記録されるため、ロギングのパフォーマンスが向上し、記憶領域も ASCII 形式より少なくなります。バイナリトレースの CLI を使用すると、**debug** コマンドと比較して、追加のプロセスモジュールでデバッグレベルを設定できます。 Cisco IOS XE リリース 17.4.1a 以降では、バイナリトレースは次の Cisco SD-WAN デーモンでサポートされています。 • fpmd • ftm • ompd • vdaemon • cfgmgr

バイナリトレース機能は、プロセスモジュールからメッセージを収集し、その情報をバイナリ形式で記録します。バイナリトレースのログメッセージのレベルを設定し、記録されたメッセージを表示して、プロセス実行中のエラーのトレースとトラブルシューティングを行うことができます。

バイナリトレースは、ASCII 形式よりも高速なバイナリ形式でメッセージをで記録することで、ランタイムパフォーマンスを向上させます。また、バイナリ形式は ASCII 形式よりも効率的に格納できます。トレース結果を表示またはファイルに保存すると、メッセージはバイナリ形式から ASCII 形式に復号化されます。

サポートされる Cisco SD-WAN デーモン

バイナリトレースは、次の Cisco SD-WAN デーモンとそのモジュールでサポートされています。

Cisco SD-WAN デーモン	サポートされているリリース
• fpmd • ftm • ompd • vdaemon • cfgmgr	Cisco IOS XE リリース 17.4.1a

バイナリトレースレベルの設定

特定のハードウェアスロットで実行されている 1 つまたはすべての Cisco SD-WAN プロセスモジュールのバイナリトレースレベルを設定します。

始める前に

Cisco vManage を使用してデバイスの SSH ターミナルにアクセスするか、Telnet セッションを開いて CLI にアクセスします。

ステップ 1 **enable**

例：

```
Device> enable
```

特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。

ステップ 2 **set platform software trace** *process slot module level*

例：

```
Device# set platform software trace fpmd R0 config debug
```

特定のハードウェアスロットで実行されている 1 つまたはすべての Cisco SD-WAN プロセスモジュールのトレースレベルを設定します。

- *process*：fpmd、ftm、ompd、vdaemon、cfgmgr から Cisco SD-WAN プロセスを指定します。
- *slot*：プロセスメッセージを記録するハードウェアスロットを指定します。
- *module*：1 つまたはすべてのプロセスモジュールのトレースレベルを設定します。
- *level*：次のトレースレベルから 1 つ選択します。
  - debug：Debug（デバッグ）メッセージ
  - emergency：Emergency（致命的）エラーの可能性があるメッセージ
  - error：エラーメッセージ
  - info：Informational（情報提供）メッセージ

- noise：可能性のある最大メッセージ
- notice：通知メッセージ
- verbose：詳細デバッグメッセージ
- warning：警告メッセージ

バイナリトレースレベルの表示

特定のハードウェアスロットで実行されている Cisco SD-WAN プロセスモジュールのバイナリトレースレベルを表示します。

始める前に

Cisco vManage を使用してデバイスの SSH ターミナルにアクセスするか、Telnet セッションを開いて CLI にアクセスします。

ステップ 1 **enable**

例：

```
Device> enable
```

特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。

ステップ 2 **show platform software trace level** *process slot*

例：

```
Device# show platform software trace level fpmd R0
```

指定したハードウェアスロット上のすべてのプロセスモジュールについて、バイナリトレースレベルが表示されます。

- *process*：fpmd、ftm、ompd、vdaemon、cfgmgr から Cisco SD-WAN プロセスを指定します。
- *slot*：プロセスメッセージを記録するハードウェアスロットを指定します。

CiscoSD-WANプロセスのバイナリトレースで記録されたメッセージの表示

始める前に

Cisco vManage を使用してデバイスの SSH ターミナルにアクセスするか、Telnet セッションを開いて CLI にアクセスします。

ステップ 1 **enable**

例：

```
Device> enable
```

特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。

ステップ 2 **show logging process** *process-name* [*filtering-options*]

例：

```
Device# show logging process fpmd internal fru R0 reverse
```

指定したプロセスのログを表示します。

process-name には、fpmd、ftm、ompd、vdaemon、cfgmgr からプロセスを指定します。プロセスのカンマ区切りリストを指定することもできます（例：`fpmd, ftm`）。

filtering-options を指定しない場合、コマンドは過去 10 分間に収集されたバイナリトレースレベル情報とシビラリティ（重大度）レベルの高いログを表示します。

フィルタリングオプションの詳細については、**show logging process** のコマンドページを参照してください。

すべてのCiscoSD-WANプロセスのバイナリトレースで記録されたメッセージの表示

始める前に

Cisco vManage を使用してデバイスの SSH ターミナルにアクセスするか、Telnet セッションを開いて CLI にアクセスします。

ステップ 1 **enable**

例：

```
Device> enable
```

特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。

ステップ 2 **show logging profile sdwan** [*filtering-options*]

例：

```
Device# show logging profile sdwan start last boot
```

すべての Cisco SD-WAN プロセスとそのモジュールのログを時系列で表示します。

filtering-options を指定しない場合、コマンドは過去 10 分間に収集されたバイナリトレースレベル情報とシビラリティ（重大度）レベルの高いログを表示します。

フィルタリングオプションの詳細については、**show logging profile sdwan** のコマンドページ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。