# トラブルシューティング



# トラブルシューティング

### セキュリティ分析とロギング（オンプレミス） 一般的なトラブルシューティング情報

マネージャ VE では、次のログファイルに セキュリティ分析とロギング（オンプレミス） に関連するトラブルシューティング情報が記載されています。

- `/lancope/var/logs/containers/sal.log`：一般的なアプリケーションのロギング情報（Manager、展開のみ）
- `/lancope/var/logs/sal_preinstall.log`：アプリケーションのインストールプロセスに固有の情報

フローコレクタでは、次のログファイルにセキュリティ分析とロギング（オンプレミス）データストア 展開に関連するトラブルシューティング情報が記載されています。

- `lancope/var/sw/today/logs/sw.log`：テレメトリロギングに固有の情報
- `/lancope/var/logs/containers/svc-db-ingest.log`：イベントの取り込みとデータベースに固有の情報

### Flow Collectorの詳細設定を使用した構成(のみ)セキュリティ分析とロギング（オンプレミス）データストア

初回セットアップ時にファイアウォールログを保存しないようにフローコレクタを設定した場合は、[フローコレクタの詳細設定（Flow Collector Advanced Settings）] ページを使用して取り込み設定を更新できます。[詳細設定（Advanced Settings）]には、次の手順でアクセスします。

1. フローコレクタ（旧アプライアンス管理（Admin）インターフェイス）にログインします。
2. **[サポート（Support）] > [詳細設定（Advanced Settings）]** の順にクリックします。
3. **enable_sal** フィールドに 1 を入力して、ファイアウォール イベント ログの取り込みを有効にします。

4. ファイアウォールログのポートを変更する場合は、**sal_syslog_port** フィールドに新しい値を入力します（デフォルトのポートは 8514）。
5. [適用 (Apply)] をクリックし、[OK] をクリックします。

### マネージャのみ 展開時の セキュリティ分析とロギング（オンプレミス） アプリのインストールの失敗

スタンドアロンのアプライアンス（マネージャのみ）としての マネージャ のインストール、またはフローコレクタとデータノード（データストア）を管理する マネージャ のインストールがサポートされています。1 つのデータノードを管理せずに 1 つ以上のフローコレクタを管理する場合、マネージャにアプリケーションをインストールすることはできません。この状況でアプリケーションをインストールしようとすると、インストールは失敗します。これが原因であることを確認するには、`/lancope/var/logs/sal_preinstall.log` でログファイルを確認します。次のメッセージまたは同様のメッセージが表示された場合、インストールで管理対象フローコレクタが検出されたことになります。

```
Checking flow collectors...
1 Flow Collector(s) detected
Flow Collector(s) are present in inventory -- aborting installation.
```

アプリケーションをインストールするには、すべての管理対象フローコレクタを Central Manager のアプライアンスインベントリから削除したうえで再試行してください。

### セキュリティ分析とロギング（オンプレミス）アプリケーションのドロップイベント

アプリケーションは、次のような状況でイベントをドロップすることがあります。

- 接続、ファイル、マルウェア、および侵入イベントだけでなく、すべてのイベントタイプを syslog でエクスポートします。
- 1 秒あたりのイベント (EPS) の平均取り込み速度またはバースト EPS 取り込み速度が、「セキュアネットワーク分析リソース割り当て」セクションの推奨仕様を超えています。

マネージャのみ の展開の場合、Manager の `/lancope/var/logs/containers/sal.log` ログファイルの情報を確認し、アプリケーションがイベントをドロップしているかどうかを判断します。「`events_dropped`」を含むエントリがないかファイルを検索します。

データストア の展開の場合、フローコクレクタ `lancope/var/sw/today/logs/sw.log` ログファイルの情報を確認し、アプリケーションがイベントをドロップしているかどうかを判断します。「`sal_event`」を含むエントリがないかファイルを検索します。

問題が解消されない場合は、シスコサポートまでお問い合わせください。

### セキュリティ分析とロギング（オンプレミス）アプリケーションのクラッシュ

セキュリティ分析とロギング（オンプレミス）アプリケーションがクラッシュした場合（過剰な取り込みレートを起因とする場合など）、マネージャを再起動します。これにより、アプリケーションも再起動されます。

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。