Cisco Secure Network Analytics

v7.4.2 Customer Success Metrics コンフィギュレーションガイド

目次

概要

Customer Success Metrics は、システムの展開、正常性、パフォーマンス、使用状況に関する重要な情報にアクセスできるように、Cisco Secure Network Analytics（旧 Stealthwatch）データのクラウドへの送信を可能にします。

- **有効化**：Customer Success Metrics は Secure Network Analytics アプライアンスで自動的に有効になります。
- **インターネットアクセス**：Customer Success Metrics にはインターネットアクセスが必要です。
- **Cisco Security Service Exchange**：Cisco Security Service Exchange は v7.4.x で自動的に有効になります。Customer Success Metrics の必須要件です。
- **データファイル**：Secure Network Analytics はメトリックデータで JSON ファイルを生成します。このデータは、クラウドに送信されるとすぐにアプライアンスから削除されます。

このガイドでは次の内容について説明します。

- **ファイアウォールの設定**：アプライアンスからクラウドに通信できるようにネットワーク ファイアウォールを設定します。「**ネットワーク ファイアウォールの設定**」を参照してください。
- **Customer Success Metrics の無効化**：Customer Success Metrics を停止するには、「**Customer Success Metrics の無効化**」を参照してください。
- **Customer Success Metrics**：メトリックの詳細については、「**Customer Success Metrics データ**」を参照してください。

> サポートが必要な場合は、シスコサポートまでお問い合わせください。

ネットワーク ファイアウォールの設定

アプライアンスからクラウドに通信できるようにするには、Cisco Secure Network Analytics Manager（旧 Stealthwatch Management Console）でネットワーク ファイアウォールを設定します。

アプライアンスがインターネットにアクセスできることを確認してください。

マネージャの設定

マネージャから次の IP アドレスおよびポート 443 に通信できるように、ネットワーク ファイアウォールを設定します。

- api sse.cisco.com
- est.sco.cisco.com
- mx*.sse.itd.cisco.com
- dex.sse.itd.cisco.com
- eventing-ingest.sse.itd.cisco.com

パブリック DNS が許可されていない場合は、マネージャでローカルに解決方法を設定してください。

Customer Success Metrics の無効化

アプライアンスで Customer Success Metrics を無効にするには、次の手順を実行します。

1. マネージャにログインします。
2. **[構成（Configure）]** > **[グローバル集中管理（GLOBAL Central Management）]** を選択します。
3. アプライアンスの ••• （[省略記号（Ellipsis）]）アイコンをクリックします。[アプライアンス構成の編集（Edit Appliance Configuration）] を選択します。
4. [全般（General）] タブをクリックします。
5. [外部サービス（External Services）] セクションまでスクロールします。
6. [Customer Success Metricsの有効化（Enable Customer Success Metrics）] チェックボックスをオフにします。
7. [設定の適用（Apply settings）] をクリックします。
8. 画面に表示される指示に従って、変更を保存します。
9. [集中管理インベントリ（Central Management Inventory）] タブで、アプライアンスのステータスが **[接続済み（Connected）]** に戻っていることを確認します。
10. 別のアプライアンスで Customer Success Metrics を無効にするには、手順 3 ～ 9 を繰り返します。

Customer Success Metrics データ

Customer Success Metrics が有効になっている場合、メトリックがシステムで収集されて、24 時間ごとにクラウドにアップロードされます。このデータは、クラウドに送信されるとすぐにアプライアンスから削除されます。

ホストグループ、IP アドレス、ユーザー名、パスワードなどの識別データは収集されません。

> シスコによって収集されたデータの保持、および使用状況メトリックの削除をリクエストする方法については、Cisco Secure Network Analytics プライバシーデータシートを参照してください。

コレクション タイプ（Collection Types）

各メトリックは、次のコレクションタイプのいずれかとして収集されます。

- **アプリの開始（App Start）**：1 分ごとに 1 回のエントリ（アプリケーション開始以降のすべてのデータを収集）。
- **累計（Cumulative）**：24 時間に 1 回のエントリ
- **インターバル（Interval）**：5 分に 1 回のエントリ（24 時間に合計 288 回のエントリ）
- **スナップショット（Snapshot）**：レポート生成時に 1 回のエントリ

> 一部のコレクションタイプは、ここで説明したデフォルトとは異なる頻度で収集されるか、または別の頻度が設定されている場合があります（アプリケーションによって異なります）。詳細については、「**メトリックの詳細**」を参照してください。

メトリックの詳細

収集したデータをアプライアンスのタイプ別にリストアップしています。Ctrl + F を使用して、表をキーワードで検索してください。

フローコレクタ

メトリック ID	説明	収集タイプ
devices_cache.active	デバイスキャッシュの ISE からのアクティブな MAC アドレスの数	Snapshot
devices_cache.deleted	タイムアウトしたため、デバイスキャッシュの ISE から削除された MAC アドレスの数	累計
devices_cache.dropped	デバイスキャッシュがいっぱいであるため、ISE からドロップされた MAC アドレスの数	累計
devices_cache.new	ISE からデバイスキャッシュに追加された新しい MAC アドレスの数	累計
flow_stats.fps	直前の 1 秒あたりのアウトバウンドフロー	インターバル
flow_stats.flows	処理されたインバウンドフロー	インターバル
flow_cache.active	Flow Collector フローキャッシュでのアクティブなフローの数	Snapshot
flow_cache.dropped	Flow Collector フローキャッシュがいっぱいであるためドロップされたフローの数	累計
flow_cache.ended	Flow Collector フローキャッシュで終了したフローの数	インターバル
flow_cache.max	Flow Collector フローキャッシュの最大サイズ	インターバル
flow_cache.percentage	Flow Collector フローキャッシュのキャパシティの割合	インターバル
flow_cache.started	Flow Collector フローキャッシュに追加されたフローの数	累計
hosts_cache.cached	ホストキャッシュ内のホスト数	インターバル
hosts_cache.deleted	ホストキャッシュで削除されたホストの数	累計
hosts_cache.dropped	ホストキャッシュがいっぱいであるためにドロップされたホストの数	累計
hosts_cache.max	ホストキャッシュの最大サイズ	インターバル

メトリック ID	説明	収集タイプ
hosts_cache.new	ホストキャッシュに新規に追加されたホストの数	累計
hosts_cache.percentage	ホストキャッシュの容量の割合	インターバル
hosts_ cache.probationary_ deleted	ホストキャッシュで削除された試用ホストの数* *試用ホストは、パケットおよびバイトの送信元ではないホストです。これらのホストは、ホストキャッシュの領域をクリアするときに最初に削除されます。	累計
interfaces.fps	Vertica にエクスポートされた 1 秒あたりのインターフェイス統計情報のアウトバウンド数	インターバル
security_events_ cache.active	セキュリティ イベント キャッシュ内のアクティブなセキュリティイベントの数	スナップショット
security_events_ cache.dropped	セキュリティ イベント キャッシュがいっぱいであるためにドロップされたセキュリティイベントの数	累計
security_events_ cache.ended	セキュリティ イベント キャッシュ内の終了したセキュリティイベントの数	累計
security_events_ cache.inserted	データベーステーブルに挿入されたセキュリティイベントの数	インターバル
security_events_ cache.max	セキュリティ イベント キャッシュの最大サイズ	インターバル
security_events_ cache.percentage	セキュリティ イベント キャッシュの容量の割合	インターバル
security_events_ cache.started	セキュリティ イベント キャッシュ内の開始されたセキュリティイベントの数	累計
session_cache.active	セッションキャッシュでの ISE からのアクティブなセッションの数	Snapshot
session_cache.deleted	セッションキャッシュで ISE から削除されたセッションの数	累計
session_cache.dropped	セッションキャッシュがいっぱいであるため、ISE からドロップされたセッションの数	累計
session_cache.new	ISE からセッションキャッシュに追加された新しいセッションの数	累計

メトリック ID	説明	収集タイプ
users_cache.active	ユーザーキャッシュ内のアクティブユーザーの数	スナップショット
users_cache.deleted	タイムアウトしたためにユーザーキャッシュから削除されたユーザーの数	累計
users_cache.dropped	ユーザーキャッシュがいっぱいであるためにドロップされたユーザーの数	累計
users_cache.new	ユーザーキャッシュ内の新規ユーザーの数	累計
reset_hour	Flow Collector リセット時間	該当なし
vertica_stats.query_duration_sec_max	クエリの最大応答時間	累計
vertica_stats.query_duration_sec_min	クエリの最小応答時間	累計
vertica_stats.query_duration_sec_avg	クエリの平均応答時間	累計
exporters.fc_count	Flow Collector あたりのエクスポータの数	インターバル

フローコレクタ StatsD

メトリック ID	説明	収集タイプ
netflow	すべての Netflow エクスポータから送られた NetFlow レコードの総数。NVM レコードが含まれます。	累計 毎日リセット
fs_netflow	フローセンサーからのみ受信した Netflow レコード数	累計 毎日リセット
netflow_bytes	NetFlow エクスポータから受信した NetFlow 合計バイト数。NVM レコードが含まれます。	累計 毎日リセット
fs_netflow_bytes	フローセンサーからのみ受信した NetFlow バイト数	累計 毎日リセット
sflow	sFlow エクスポータから受信した sFlow レコード数	累計

メトリック ID	説明	収集タイプ
		毎日リセット
sflow_bytes	sFlow エクスポータから受信した sFlow バイト数	累計 毎日リセット
nvm_endpoint	本日確認された一意の NVM エンドポイント（毎日のリセット前）。	累計 毎日リセット
nvm_bytes	受信した NVM バイト数（フロー、エンドポイント、endpoint_interface レコードを含む）	累計 毎日リセット
nvm_netflow	受信した NVM バイト数（フロー、エンドポイント、endpoint_interface レコードを含む）	累計 毎日リセット
all_sal_event	受信したイベントの数でカウントする、受信したすべての セキュリティ分析とロギング（オンプレミス） イベント（Adaptive Security Appliance および非 Adaptive Security Appliance を含む）	累計 毎日リセット
all_sal_bytes	受信したバイト数でカウントする、受信したすべての セキュリティ分析とロギング（オンプレミス） イベント（Adaptive Security Appliance および非 Adaptive Security Appliance を含む）	累計 毎日リセット
ftd_sal_event	Firepower Threat Defense/NGIPS デバイスのみから受信した セキュリティ分析とロギング（オンプレミス）（非 Adaptive Security Appliance）イベント	累計 毎日リセット
ftd_sal_bytes	Firepower Threat Defense/NGIPS デバイスのみから受信した セキュリティ分析とロギング（オンプレミス）（非 Adaptive Security Appliance）バイト	累計 毎日リセット
ftd_lina_bytes	Firepower Threat Defense デバイスからのみ受信したデータプレーンのバイト数	累計 毎日リセット
ftd_lina_event	Firepower Threat Defense デバイス から受信したデータプレーンイベントのみ	累計 毎日リセット
asa_asa_event	Adaptive Security Appliance デバイスから受信した Adaptive Security Appliance イベントのみ	累計 毎日リセット
asa_asa_bytes	Adaptive Security Appliance デバイスから受信した ASA バイトのみ	累計 毎日リセット

マネージャ

メトリック ID	説明	収集タイプ
report_complete	レポートの名前とミリ秒単位の実行時間（マネージャのみ）	該当なし
report_params	マネージャが FC データベースを照会するときに使用するフィルタ。 クエリごとにエクスポートされるデータ： • 行の最大数 • include-interface-data フラグ • fast-query フラグ • exclude-counts フラグ • フロー方向フィルタ • order-by 列 • default-columns フラグ • 時間枠の開始日時 • 時間枠の終了日時 • デバイス ID 数の基準 • インターフェイス ID 数の基準 • IP 数の基準 • IP 範囲数の基準 • ホストグループ数の基準 • ホストペア数の基準 • 結果を MAC アドレスでフィルタリングするかどうか • 結果を TCP/UDP ポートでフィルタリングするかどうか • ユーザー名数の基準 • 結果をバイト数/パケット数でフィルタリングするかどうか • 結果をバイト/パケットの総数でフィルタリングするかどうか • 結果を URL でフィルタリングするかどうか • 結果をプロトコルでフィルタリングするかどうか • 結果をアプリケーション ID でフィルタリングするかどうか • 結果をプロセス名でフィルタリングするかど	スナップショット 頻度：リクエストごと

メトリック ID	説明	収集タイプ
	うか • 結果をプロセスハッシュでフィルタリングするかどうか • 結果を TLS バージョンでフィルタリングするかどうか • 暗号スイートの暗号数の基準	
domain.integration_ad_count	AD 接続数	累計
domain.rpe_count	設定されているロールポリシーの数	累計
domain.hg_changes_count	ホストグループ設定への変更の回数	累計
integration_snmp	SNMP エージェントの使用状況	該当なし
integration_cognitive	有効化されている グローバル脅威アラート（旧 Cognitive Intelligence）統合	該当なし
domain.services	定義済みサービスの数	スナップショット
applications_default_count	定義済みアプリケーションの数	スナップショット
smc_users_count	Web アプリケーションのユーザー数	スナップショット
login_api_count	API ログインの数	累計
login_ui_count	Web アプリケーションのログイン数	累計
report_concurrency	同時に実行されているレポートの数	累計
apicall_ui_count	Web アプリを使用したマネージャ API コールの数	累計
apicall_api_count	API を使用したマネージャ API コールの数	累計
ctr.enabled	Cisco SecureX Threat Response（旧 Cisco Threat Response）との統合が有効	該当なし
ctr.ats_integration_enabled	Cisco SecureX リボンが有効	該当なし
ctr.alarm_sender_enabled	有効化されている SecureX Threat Responseへの Secure Network Analytics アラーム	該当なし

メトリック ID	説明	収集タイプ
ctr.alarm_sender_minimal_severity	SecureX Threat Response に送信されるアラームの最小重大度	該当なし
ctr.enrichment_enabled	SecureX Threat Response のエンリッチメント要求が有効	該当なし
ctr.enrichment_limit	SecureX Threat Response に返された上位のセキュリティイベントの数	累計
ctr.enrichment_period	SecureX Threat Response に返されたセキュリティイベントの期間	累計
ctr.number_of_alarms	SecureX Threat Response に送信されたアラームの数	累計
ctr.number_of_enrichment_requests	SecureX Threat Response から受信したエンリッチメント要求の数	累計
ctr.number_of_refer_requests	SecureX Threat Response から受信したマネージャ ピボットリンクのリクエスト数	累計
failover_role	クラスタ内のマネージャ プライマリまたはセカンダリ フェールオーバー ロール	該当なし
domain.cse_count	ドメイン ID のカスタム セキュリティ イベントの数	スナップショット

マネージャ StatsD

メトリック ID	説明	収集タイプ
swrm_is_in_use	応答管理：応答管理が使用されている場合、値は 1 です。使用されていない場合の値は 0 です。	スナップショット
swrm_rules	応答管理：カスタムルールの数	スナップショット
swrm_action_email	応答管理：電子メールタイプのカスタムアクションの数	スナップショット
swrm_action_syslog_message	応答管理：Syslog メッセージタイプのカスタムアクションの数	スナップショット
swrm_action_snmp_trap	応答管理：SNMP トラップタイプのカスタムアクションの数	スナップショット

メトリック ID	説明	収集タイプ
swrm_action_ise_anc	応答管理：ISE ANC ポリシータイプのカスタムアクションの数	スナップショット
swrm_action_webhook	応答管理：ウェブフックタイプのカスタムアクションの数	スナップショット
swrm_action_ctr	応答管理：Threat Response インシデントタイプのカスタムアクションの数	スナップショット
va_ct	可視性アセスメント：ミリ秒単位で計算された実行時間	スナップショット
va_ce	可視性アセスメント：エラーの数（計算がクラッシュした場合）	スナップショット
va_hcs	可視性アセスメント：バイト単位のホストカウント API 応答サイズ（過剰な応答サイズを検出）	スナップショット
va_ss	可視性アセスメント：バイト単位のスキャナ API 応答サイズ（過剰な応答サイズを検出）	スナップショット
va_ses	可視性アセスメント：バイト単位のセキュリティイベント API 応答サイズ（過剰な応答サイズを検出）	スナップショット
sal_input_size	パイプライン入力キューのエントリ数	スナップショット 頻度： 1 分
sal_completed_size	完了したバッチキューのエントリ数	スナップショット 頻度： 1 分
sal_flush_time	最後のパイプラインフラッシュから経過した時間（ミリ秒単位）。 セキュリティ分析とロギング（オンプレミス）単一ノードのみで利用可能。	Snapshot 頻度： 1 分
sal_batches_succeeded	ファイルに正常に書き込まれたバッチの数。 セキュリティ分析とロギング（オンプレミス）単一ノードのみで利用可能。	インターバル 頻度： 1 分

メトリック ID	説明	収集タイプ
sal_batches_processed	処理されたバッチの数。 セキュリティ分析とロギング（オンプレミス）単一ノードのみで利用可能。	インターバル 頻度： 1 分
sal_batches_failed	ファイルへの書き込みを完了できなかったバッチの数。 セキュリティ分析とロギング（オンプレミス）単一ノードのみで利用可能。	インターバル 頻度： 1 分
sal_files_moved	準備完了ディレクトリに移動されたファイルの数。 セキュリティ分析とロギング（オンプレミス）単一ノードのみで利用可能。	インターバル 頻度： 1 分
sal_files_failed	移動に失敗したファイルの数。 セキュリティ分析とロギング（オンプレミス）単一ノードのみで利用可能。	インターバル 頻度： 1 分
sal_files_discarded	エラーのために破棄されたファイルの数。 セキュリティ分析とロギング（オンプレミス）単一ノードのみで利用可能。	インターバル 頻度： 1 分
sal_rows_written	参照ファイルに書き込まれた行数。 セキュリティ分析とロギング（オンプレミス）単一ノードのみで利用可能。	インターバル 頻度： 1 分
sal_rows_processed	処理された行数。 セキュリティ分析とロギング（オンプレミス）単一ノードのみで利用可能。	インターバル 頻度： 1 分
sal_rows_failed	書き込みに失敗した行数。 セキュリティ分析とロギング（オンプレミス）単一ノードのみで利用可能。	インターバル 頻度： 1 分
sal_total_batches_succeeded	ファイルに正常に書き込まれたバッチの総数。 セキュリティ分析とロギング（オンプレミス）単一ノードのみで利用可能。	アプリの開始 頻度： 1 分
sal_total_batches_processed	処理されたバッチの総数。 セキュリティ分析とロギング（オンプレミス）単一ノードのみで利用可能。	アプリの開始 頻度： 1 分

メトリック ID	説明	収集タイプ
sal_total_batches_failed	ファイルへの書き込みを完了できなかったファイルの総数。 セキュリティ分析とロギング（オンプレミス）単一ノードのみで利用可能。	アプリの開始 頻度： 1 分
sal_total_files_moved	準備完了ディレクトリに移動されたファイルの総数。 セキュリティ分析とロギング（オンプレミス）単一ノードのみで利用可能。	アプリの開始 頻度： 1 分
sal_total_files_failed	移動に失敗したファイルの総数。 セキュリティ分析とロギング（オンプレミス）単一ノードのみで利用可能。	アプリの開始 頻度： 1 分
sal_total_files_discarded	エラーのために破棄されたファイルの総数。 セキュリティ分析とロギング（オンプレミス）単一ノードのみで利用可能。	アプリの開始 頻度： 1 分
sal_total_rows_written	参照ファイルに書き込まれた行の総数。 セキュリティ分析とロギング（オンプレミス）単一ノードのみで利用可能。	アプリの開始 頻度： 1 分
sal_total_rows_processed	処理された行の総数。 セキュリティ分析とロギング（オンプレミス）単一ノードのみで利用可能。	アプリの開始 頻度： 1 分
sal_total_rows_failed	書き込みに失敗した行の総数。 セキュリティ分析とロギング（オンプレミス）単一ノードのみで利用可能。	アプリの開始 頻度： 1 分
sal_transformer_ <transformer id>	このトランスフォーマーの変換エラー数。 セキュリティ分析とロギング（オンプレミス）単一ノードのみで利用可能。	インターバル 頻度： 1 分
sal_bytes_per_event	受信したイベントあたりの平均バイト数	インターバル 頻度： 1 分
sal_bytes_received	UDP サーバーから受信したバイト数	インターバル 頻度： 1 分

メトリック ID	説明	収集タイプ
sal_events_received	UDP サーバーから受信したイベントの数	インターバル 頻度： 1 分
sal_total_events_received	ルータで受信したイベントの総数	アプリの開始
sal_events_dropped	破棄された解析不能イベントの数	インターバル 頻度： 1 分
sal_total_events_dropped	破棄された解析不能イベントの総数	アプリの開始 頻度： 1 分
sal_events_ignored	無視された/サポートされていないイベントの数	インターバル 頻度： 1 分
sal_total_events_ignored	無視された/サポートされていないイベントの総数	アプリの開始 頻度： 1 分
sal_receive_queue_size	受信キューのイベント数。	スナップショット 頻度： 1 分
sal_events_per second	取り込み率（イベント数/秒）	インターバル 頻度： 1 分
sal_bytes_per_second	取り込み率（バイト/秒）	インターバル 頻度： 1 分
sna_trustsec_report_runs	日次 TrustSec レポートのリクエスト数	累計

UDP Director

メトリック ID	説明	収集タイプ
sources_count	ソースの数	スナップショット
rules_count	Number of rules	スナップショット
packets_unmatched	一致しない最大パケット数	スナップショット
packets_dropped	ドロップされたパケット eth0	Snapshot

すべてのアプライアンス

メトリック ID	説明	収集タイプ
platform	ハードウェア プラットフォーム（例：Dell 13G、KVM 仮想プラットフォーム）	該当なし
serial	アプライアンスのシリアル番号	該当なし
version	Secure Network Analytics バージョン番号（例：7.1.0）	該当なし
version_build	ビルド番号（例：2018.07.16.2249-0）	該当なし
version_patch	パッチ番号	該当なし
version_patch	Customer Success Metrics コードバージョン（例：1.0.24-SNAPSHOT）	該当なし
power_supply.status	マネージャおよび Flow Collector の電源統計	Snapshot
productInstanceName	スマートライセンス製品 ID	該当なし

サポートへの問い合わせ

テクニカル サポートが必要な場合は、次のいずれかを実行してください。

- 最寄りのシスコ パートナーにご連絡ください。
- シスコサポートの連絡先
- Web でケースを開く場合：http://www.cisco.com/c/en/us/support/index.html
- 電子メールでケースを開く場合：tac@cisco.com
- 電話でサポートを受ける場合：800-553-2447（米国）
- ワールドワイド サポート番号：
  https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

変更履歴

マニュアルのバージョン	公開日	説明
1_0	2023 年 3 月 3 日	最初のバージョン。

著作権情報