



Cisco StealthWatch

Customer Success Metrics 7.2 コンフィギュレーションガイド



目次

概要	3
サポートへの問い合わせ	3
設定	4
ネットワークファイアウォールの設定	4
Stealthwatch 管理コンソールの設定	4
フローコレクタの設定	4
Customer Success Metrics の無効化	5
Customer Success Metrics データ	6

概要

Customer Success Metrics (CSM)を使用すると、Stealthwatch システムのデータをクラウドに送信して、Customer Experience からシステムの導入状況、状態、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なります。このデータは、アプライアンスの .csv ファイルからもアクセスできます。

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。
- Cisco Stealthwatch サポートのお問い合わせ先：
 - 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>

設定

Customer Success Metrics は、Stealthwatch 管理コンソールとフローコレクタで自動的に有効になります。「[ネットワークファイアウォールの設定](#)」セクションの指示に従って、アプライアンスからクラウドへの通信を許可するようにネットワークファイアウォールを設定する必要があります。CSMを無効にするには、「[Customer Success Metrics の無効化](#)」セクションの手順を使用します。

- Customer Success Metrics では、すべての有効なアプライアンスにインターネットアクセスが必要です。
- 各アプライアンスでは、それぞれ .csv ファイルが生成されます。

ネットワークファイアウォールの設定

Stealthwatch 管理コンソールの設定

Stealthwatch 管理コンソールから次の IP アドレスおよびポート 443 への通信を許可するように、ネットワークのファイアウォールを設定します。

AWS の Elastic IP	• 34.242.41.248 • 34.242.94.137 • 34.251.54.105
シスコの合理化 IP	• 146.112.59.0/24 • 208.69.38.0/24

 パブリック DNS が許可されていない場合は、StealthWatch Management Console でローカルに解決方法を設定する必要があります。

フローコレクタの設定

フローコレクタから次の IP アドレスおよびポート 443 への通信を許可するように、ネットワークのファイアウォールを設定します。

AWS の Elastic IP	• 34.242.41.248 • 34.242.94.137 • 34.251.54.105	• 34.251.210.21 • 34.255.162.33 • 54.194.49.205
シスコの合理化 IP	• 146.112.59.0/24 • 208.69.38.0/24	



パブリック DNS が許可されていない場合は、フローコレクタでローカルに解決方法を設定する必要があります。

Customer Success Metrics の無効化

アプライアンスの CSM を無効にするには、次の手順を実行します。

1. StealthWatch Management Console にログインします。
2. [グローバル設定 (Global Settings)] アイコンをクリックし、[集中管理 (Central Management)] をクリックします。
3. [アクション (Actions)] 列のコンテキストメニューから、[アプライアンス設定の編集 (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)] セクションまで下にスクロールし、[カスタマーサクセスのメトリクスを有効にする (Enable Customer Success Metrics)] チェックボックスをオフにします。
6. [設定の適用 (Apply settings)] をクリックします。

Customer Success Metrics データ

Customer Success Metrics には、次の 3 つのデータタイプがあります。

- **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

次の表に、Customer Success Metrics によって収集されるデータを示します。

システムデータ	説明	データタイプ
collector.collect.duration_s	すべてのメトリックの収集にかかった時間	スナップショット 頻度: 毎時
devices.cache.active	デバイスキャッシュ内の ISE からのアクティブ MAC アドレスの数	スナップショット
devices.cache.deleted	タイムアウトになったためにデバイスキャッシュで 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に ISE からドロップされた MAC アドレスの数	累計
devices.cache.max	ISE の MAC アドレスの最大数	インターバル
devices.cache.new	ISE からデバイスキャッシュに新規に追加された MAC アドレスの数	累計
events.vertica.day.{event_id}.count	1 日の各タイプのセキュリティイベントの合計数 (1 日遅延)	インターバル 頻度: 毎日
flow_stats	Vertica および ZMQ にエクスポートされた 1 分あたりのフロー統計情報	インターバル
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
flows	処理されたインバウンドフロー	インター

システムデータ	説明	データ タイプ
		バル
flows.cache.active	フローコレクタのフローキャッシュ内のアクティブフローの数	スナップ ショット
flows.cache.dropped	フローコレクタのフローキャッシュがいっぱいであるためにドロップされたフローの数	累計
flows.cache.ended	フローコレクタのフローキャッシュで終了したフローの数	インター バル
flows.cache.max	フローコレクタのフローキャッシュの最大サイズ	インター バル
flows.cache.percent	フローコレクタのフローキャッシュの容量の割合	インター バル
flows.cache.started	フローコレクタのフローキャッシュに追加されたフローの数	累計
flows.dropped	ドロップされたインバウンドフローの数	インター バル
flows.fps	1 秒あたりのインバウンドフローの数	インター バル
flows.vertica.all.count	データベース内のフローの合計数	スナップ ショット 頻度: 毎日
flows.vertica.all.last_time.min	データベース内の最も古いフローの概算	スナップ ショット 頻度: 毎日
flows.vertica.hour.client_ip_address.distinct.catch_all.count	catch-all グループに属する各クライアント IP の合計数 (サンプリングされた 1 時間のデータ)	インター バル 頻度: 毎時
flows.vertica.hour.client_ip_address.distinct.count	各クライアント IP の合計数 (サンプリングされた 1 時間のデータ)	インター バル

システムデータ	説明	データ タイプ
		頻度: 毎時
flows.vertica.hour.count	1 時間あたりのフローの合計数(サンプリングされた 1 時間のデータ)	インター バル 頻度: 毎時
flows.vertica.hour.distinct.count	特定フロー(フロー ID に基づく)の概数と割合。割合の値の範囲は [0,1](サンプリングされた 1 時間のデータ)。	インター バル 頻度: 毎時
flows.vertica.hour.* – inside.inside.count – inside.outside.count – outside.inside.count – outside.outside.count	方向別にグループ化されたフローの合計数(サンプリングされた 1 時間のデータ)	インター バル 頻度: 毎時
flows.vertica.hour.server_ip_address.distinct.catch_all.count	catch-all グループに属する各サーバ IP の合計数(サンプリングされた 1 時間のデータ)	インター バル 頻度: 毎時
flows.vertica.hour.server_ip_address.distinct.count	各サーバ IP の合計数(サンプリングされた 1 時間のデータ)	インター バル 頻度: 毎時
flows.vertica.sample.client_ip_address.distinct.catch_all.ratio	catch-all グループに属するクライアント IP の割合。割合の値の範囲は [0,1](サンプリングされた 1 時間のデータ)	インター バル 頻度: 毎時
flows.vertica.sample.distinct.ratio	特定フロー(フロー ID に基づく)の概数と割合。割合の値の範囲は [0,1](サンプリングされた 1 時間のデータ)。	インター バル 頻度: 毎時
flows.vertica.sample.server_ip_	catch-all グループに属するサーバ IP の割合。割	インター

システムデータ	説明	データタイプ
address.distinct.catch_all.ratio	合の値の範囲は [0,1] (サンプリングされた 1 時間のデータ)	バル 頻度: 毎時
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
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.percent	ホストキャッシュの容量の割合	インター バル
hosts.cache.probatinary.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	Vertica にエクスポートされた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
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
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
product	Stealthwatch 製品 (例: SMC、Flow Collector NetFlow)	該当なし
report.complete	レポートの名前と実行時間 (ミリ秒単位) (SMC のみ)	該当なし
report.filters	SMC が FC データベースを照会するときに使用されるフィルタ。	スナップ ショット

システムデータ	説明	データ タイプ
	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	頻度: 要求ごと

システムデータ	説明	データタイプ
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.percent	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
serial	アプライアンスのシリアル番号	該当なし
sessions.cache.active	セッションキャッシュ内の ISE のアクティブセッションの数	スナップショット
sessions.cache.deleted	セッションキャッシュ内の ISE から削除されたセッションの数	累計
sessions.cache.dropped	セッションキャッシュがいっぱいであるために ISE からドロップされたセッションの数	累計
sessions.cache.max	セッションキャッシュの最大サイズ	インターバル
sessions.cache.new	ISE からセッションキャッシュに新規に追加されたセッションの数	累計
users.cache.active	ユーザキャッシュ内のアクティブユーザの数	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キャッシュから削除されたユーザの数	累計

システムデータ	説明	データタイプ
users.cache.dropped	ユーザ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の数	累計
users.cache.max	ユーザキャッシュの最大サイズ	インターバル
users.cache.new	ユーザキャッシュ内の新規ユーザの数	累計
version	Stealthwatch 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
vertica.health.node.{node_name}.disk.* – used_bytes – free_bytes – used_ratio	ディスクの現在のステータス	スナップショット 頻度: 毎時
vertica.health.node.{node_name}.event.{event_severity}	イベント数 (1 時間のデータ)	インターバル 頻度: 毎日
vertica.health.node.{node_name}.state	ノードの現在の状態	スナップショット 頻度: 毎時
reset.hour	フローコレクタのリセット時間	該当なし
csm.version	Customer Success Metrics コードバージョン (例: 1.0.24-SNAPSHOT)	該当なし
power.{sensorId}.status	SMC およびフローコレクタ電源の統計情報	スナップショット

システムデータ	説明	データタイプ
integration.ad.{domainId}.count	AD 接続数	累計
rpe.{domainId}.count	設定されているロールポリシーの数	累計
rp.{domainId}.count	設定されている関係ポリシーの数	累計
sw.app.{appId}	システムにインストールされている Stealthwatch アプリケーション	該当なし
hostgroups.changes.{domainId}.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	Cognitive Intelligence 統合が有効	該当なし
services.{domainId}.count	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
vertica.stats.query.{user}.duration_sec	ユーザ別のクエリ応答時間	累計
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

システムデータ	説明	データタイプ
exporters.fc.count	フローコレクタあたりのエクスポートの数	インターバル
apicall.ui.count	Web アプリケーションを使用する SMC API コールの数	累計
apicall.api.count	API を使用する SMC API コールの数	累計
licensing.smart.smartAccount	SMC のスマートライセンス アカウント	該当なし
licensing.smart.virtualAccount	SMC のスマートライセンス仮想アカウント	該当なし
licensing.smart.registrationStatus	SMC のスマートライセンス登録ステータス	該当なし
licensing.smart.productInstanceName	スマートライセンス製品 ID	該当なし
ctr.ctr_enabled	CTR 統合が有効	該当なし
ctr.ats_integration_enabled	ATS 統合が有効	該当なし
ctr.alarm_sender_enabled	Stealthwatch の CTR へのアラームが有効	該当なし
ctr.alarm_sender_minimal_severity	CTR に送信されるアラームの最小重大度	該当なし
ctr.enrichment_enabled	CTR からのエンリッチメント要求が有効	該当なし
ctr.enrichment_limit	CTR 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	CTR に返されたセキュリティイベントの期間	累計
ctr.number_of_alarms	CTR に送信されたアラームの数	累計
ctr.number_of_enrichment_requests	CTR から受信したエンリッチメント要求の数	累計

システムデータ	説明	データ タイプ
ctr.number_of_refer_requests	CTR から受信した SMC ピボットリンクの要求数	累計
ctr.swe_visibility_app_metrics	可視性アセスメント SecureX タイルへのデータ要求の数	累計
ctr.swe_visibility_app_network_metrics	ネットワーク可視性 SecureX タイルへのデータ要求の数	累計
ctr.swe_alarming_hosts_by_category	アラームホストへのデータ要求の数(カテゴリ SecureX タイル別)	累計
ctr.swe_top_inside_groups_by_traffic	上位内部ホスト SecureX タイルへのデータ要求の数	累計
ctr.swe_top_outside_groups_by_traffic	上位外部ホスト SecureX タイルへのデータ要求の数	累計
ctr.swe_top_alarming_hosts	上位アラームホスト SecureX タイルへのデータ要求の数	累計
ctr.swe_top_alarms_by_type_overall	上位アラームへのデータ要求の数(カウント SecureX タイル別)	累計

著作権情報

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワークトポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際の IP アドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。