Cisco Stealthwatch

Customer Success Metrics Configuration Guide 7.3

Table of Contents

Overview

Customer Success Metrics (CSM) enables Stealthwatch system data to be sent to the cloud so that Customer Success can access vital information regarding the deployment, health, performance, and usage of your system.

- **Enabled:** Customer Success Metrics is automatically enabled on your Stealthwatch appliances.
- **Internet Access:** Internet access is required for Customer Success Metrics.
- **Cisco Security Service Exchange:** Cisco Security Service Exchange is enabled automatically in v7.3 and is required for Customer Success Metrics.
- **Data Files:** Stealthwatch generates a JSON file with the metrics data. The data is deleted from the appliance immediately after it is sent to the cloud.

This guide includes the following information:

- **Configuring the Firewall:** Configure your network firewall to allow communication from your appliances to the cloud. Refer to **Configuring the Network Firewall**.
- **Disabling Customer Success Metrics:** To opt out of CSM, refer to **Disabling Customer Success Metrics**.
- **Customer Success Metrics:** For details about the metrics, refer to **Customer Success Metrics Data**.

For assistance, please contact Cisco Stealthwatch Support.

Configuring the Network Firewall

To allow communication from your appliances to the cloud, configure your network firewall on your Stealthwatch Management Console (SMC).

> Make sure your appliances have Internet access.

Configuring the Stealthwatch Management Console

Configure your network firewall to allow communication from your Stealthwatch Management Consoles to the following IP addresses and port 443:

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

> If public DNS is not allowed, make sure you configure the resolution locally on your Stealthwatch Management Consoles.

Disabling Customer Success Metrics

Use the following instructions to disable CSM on an appliance.

1. Log in to Stealthwatch Management Console.
2. Click the **Global Settings** icon. Choose **Central Management**.
3. Click the Actions menu for the appliance. Choose **Edit Appliance Configuration**.
4. Click the **General** tab.
5. Scroll to the **External Services** section.
6. Uncheck the **Enable Customer Success Metrics** check box.
7. Click **Apply Settings**.
8. Follow the on-screen prompts to save your changes.
9. On the Appliance Manager Inventory, confirm the Appliance Status returns to **Up**.
10. To disable CSM on another appliance, repeat steps 3 through 9.

Customer Success Metrics Data

When Customer Success Metrics is enabled, the metrics are collected in the system and uploaded every 24 hours to the cloud. The data is deleted from the appliance immediately after it is sent to the cloud.

We do not collect identification data such as host groups, IP addresses, user names, or passwords. If you deploy a Data Store as part of your Stealthwatch deployment, we do not collect metrics.

> For information on data retention and how to request deletion of usage metrics collected by Cisco, refer to Stealthwatch Enterprise Privacy Data Sheet.

Data Types

Each metric is collected as one of the following data types:

- **App Start**: One entry every 1 minute (collects all the data since the application started).
- **Cumulative**: One entry for a 24-hour period
- **Interval**: One entry every 5 minutes (total of 288 entries per 24-hour period)
- **Snapshot**: One entry for the point in time the report is generated

> Some of the data types are collected at different frequencies than the defaults we've described here, or they may be configured (depending on the application). Refer to **Metrics Details** for more information.

Metrics Details

The following table lists the data collected by Customer Success Metrics:

Metric Identification	Description	Data Type
collector.collect.duration_s	Duration it took to collect all metrics	Snapshot Freq: Hourly
devices.cache.active	Number of active MAC addresses from ISE in the devices cache	Snapshot

Metric Identification	Description	Data Type
devices.cache.deleted	Number of deleted MAC addresses from ISE in the devices cache because they have timed out	Cumulative
devices.cache.dropped	Number of dropped MAC addresses from ISE because the devices cache is full	Cumulative
devices.cache.max	Maximum number of MAC addresses from ISE	Interval
devices.cache.new	Number of new MAC addresses from ISE added into the devices cache	Cumulative
events.vertica.day.{event_id}.count	Total number of each type of security event over one day (delayed by one day)	Interval Freq: Daily
flow_stats	Flow statistics per minute exported to Vertica and ZMQ	Interval
flow_stats.fps	Outbound flows per second in the last minute	Interval
flows	Inbound flows processed	Interval
flows.cache.active	Number of active flows in the Flow Collector's flow cache	Snapshot
flows.cache.dropped	Number of flows dropped because the Flow Collector's flow cache is full	Cumulative
flows.cache.ended	Number of flows ended in the Flow Collector's flow cache	Interval

Metric Identification	Description	Data Type
flows.cache.max	Maximum size of the Flow Collector's flow cache	Interval
flows.cache.percent	Percent of capacity of the Flow Collector's flow cache	Interval
flows.cache.started	Number of flows added to the Flow Collector's flow cache	Cumulative
flows.dropped	Inbound number of flows dropped	Interval
flows.fps	Inbound number of flows per second	Interval
flows.vertica.all.count	Total number of flow in the database	Snapshot Freq: Daily
flows.vertica.all.last_time.min	Approximation of the oldest flow in database	Snapshot Freq: Daily
flows.vertica.hour.client_ip_address.distinct.catch_all.count	Total number of distinct client IPs belonging to the catch-all group (one hour of data sampled)	Interval Freq: Hourly
flows.vertica.hour.client_ip_address.distinct.count	Total number of distinct client IPs (one hour of data sampled)	Interval Freq: Hourly
flows.vertica.hour.count	Total number of flows in one hour (one hour of data sampled)	Interval Freq: Hourly
flows.vertica.hour.distinct.count	Approximate number and ratio of unique flow (based on the flow id). Ratio in [0,1] (one hour of data sampled).	Interval Freq: Hourly
flows.vertica.hour.*	Total number of flows grouped	Interval

Metric Identification	Description	Data Type
- inside.inside.count - inside.outside.count - outside.inside.count - outside.outside.count	by direction (one hour of data sampled)	Freq: Hourly
flows.vertica.hour.server_ip_address.distinct.catch_all.count	Total number of distinct server IPs belonging to the catch-all group (one hour of data sampled)	Interval Freq: Hourly
flows.vertica.hour.server_ip_address.distinct.count	Total number of distinct server IPs (one hour of data sampled)	Interval Freq: Hourly
flows.vertica.sample.client_ip_address.distinct.catch_all.ratio	Ratio of client IPs belonging to the catch-all group. Ratio in [0,1] (one hour of data sampled)	Interval Freq: Hourly
flows.vertica.sample.distinct.ratio	Approximate number and ratio of unique flow (based on the flow id). Ratio in [0,1] (one hour of data sampled).	Interval Freq: Hourly
flows.vertica.sample.server_ip_address.distinct.catch_all.ratio	Ratio of server IPs belonging to the catch-all group. Ratio in [0,1] (one hour of data sampled)	Interval Freq: Hourly
hosts.cache.cached	Number of hosts in the host cache	Interval
hosts.cache.deleted	Number of hosts deleted in the host cache	Cumulative
hosts.cache.dropped	Number of hosts dropped because the host cache is full	Cumulative
hosts.cache.max	Maximum size of the host cache	Interval
hosts.cache.new	Number of new hosts added into	Cumulative

Metric Identification	Description	Data Type
	the host cache	
hosts.cache.percent	Percent of capacity of the host cache	Interval
hosts.cache.probationary.deleted	Number of probationary hosts* deleted in the hosts cache *Probationary hosts are hosts that have never been the source of packets and bytes. These hosts are deleted first when clearing up space in the host cache.	Cumulative
interfaces	Outbound number of interface statistics exported to Vertica	Interval
interfaces.fps	Outbound number of interface statistics per second exported to Vertica	Interval
platform	Hardware platform (ex: Dell 13G, KVM Virtual Platform)	N/A
product	Stealthwatch product (ex: SMC, Flow Collector NetFlow)	N/A
report.complete	Name of the report and the run-time in milliseconds (SMC only)	N/A
report.filters	Filters used when the SMC queries the FC databases. Data exported per query: • maximum number of rows • include-interface-data flag • fast-query flag	Snapshot Freq: Per Request

Metric Identification	Description	Data Type
	• exclude-counts flag • flows direction filters • order-by column • default-columns flag • Time window start date and time • Time window end date and time • Number of device ids criteria • Number of interface ids criteria • Number of IPs criteria • Number of IP ranges criteria • Number of hostgroups criteria • Number of hosts pairs criteria • Whether results are filtered by MAC addresses • Whether results are filtered by TCP/UDP ports • Number of usernames criteria • Whether results are filtered by number of bytes/packets • Whether results are filtered by total number of bytes/packets • Whether results are filtered by URL • Whether results are filtered	

Metric Identification	Description	Data Type
	by protocols • Whether results are filtered by applications ids • Whether results are filtered by process name • Whether results are filtered by process hash • Whether results are filtered by TLS version • Number of ciphers in cipher suite criteria	
security_events.cache.active	Number of active security events in the security events cache	Snapshot
security_events.cache.dropped	Number of security events dropped because the security events cache is full	Cumulative
security_events.cache.ended	Number of ended security events in the security events cache	Cumulative
security_events.cache.inserted	Number of security events inserted into the database table	Interval
security_events.cache.max	Maximum size of the security events cache	Interval
security_events.cache.percent	Percent of capacity of the security events cache	Interval
security_events.cache.started	Number of started security events in the security events cache	Cumulative
serial	Serial number of the appliance	N/A

Metric Identification	Description	Data Type
sessions.cache.active	Number of active sessions from ISE in the session cache	Snapshot
sessions.cache.deleted	Number of deleted sessions from ISE in the session cache	Cumulative
sessions.cache.dropped	Number of sessions from ISE dropped because the sessions cache is full	Cumulative
sessions.cache.max	Maximum size of the sessions cache	Interval
sessions.cache.new	Number of new sessions from ISE added into the session cache	Cumulative
users.cache.active	Number of active users in the users cache	Snapshot
users.cache.deleted	Number of deleted users in the users cache because they have timed out	Cumulative
users.cache.dropped	Number of users dropped because the users cache is full	Cumulative
users.cache.max	Maximum size of the users cache	Interval
users.cache.new	Number of new users in the users cache	Cumulative
version	Stealthwatch version number (ex: 7.1.0)	N/A
version.build	Build number (ex: 2018.07.16.2249-0)	N/A
version.patch	Patch number	N/A

Metric Identification	Description	Data Type
vertica.health.node.{node_name}.disk.* - used_bytes - free_bytes - used_ratio	Disk current status	Snapshot Freq: Hourly
vertica.health.node.{node_name}.event.{event_severity}	Count events (one hour of data)	Interval Freq: Daily
vertica.health.node.{node_name}.state	Node current state	Snapshot Freq: Hourly
reset.hour	Flow Collector reset hour	N/A
csm.version	Customer Success Metrics code version (ex: 1.0.24-SNAPSHOT)	N/A
power.{sensorId}.status	SMC and Flow Collector power supply statistics	Snapshot
integration.ad.{domainId}.count	Number AD connections	Cumulative
rpe.{domainId}.count	Number of role policies configured	Cumulative
rp.{domainId}.count	Number of relationship policies configured	Cumulative
sw.app.{appId}	Stealthwatch Apps installed on the system	N/A
hostgroups.changes.{domainId}.count	Changes to the Host Group configuration	Cumulative
integration.snmp	SNMP agent usage	N/A
integration.cognitive	Cognitive Intelligence integration	N/A

Metric Identification	Description	Data Type
	enabled	
services.{domainId}.count	Number of services defined	Snapshot
applications.default.count	Number of applications defined	Snapshot
smc.users.count	Number of users in the Web App	Snapshot
login.api.count	Number of API log ins	Cumulative
login.ui.count	Number of Web App log ins	Cumulative
report.concurency	Number of reports running concurrently	Cumulative
vertica.stats.query.{user}.duration_sec	Query response time by user	Cumulative
vertica.stats.query.duration_sec.max	Maximum query response time	Cumulative
vertica.stats.query.duration_sec.min	Minimum query response time	Cumulative
vertica.stats.query.duration_sec.avg	Average query response time	Cumulative
exporters.fc.count	Number of exporters per Flow Collector	Interval
apicall.ui.count	Number of SMC API calls using the Web App	Cumulative
apicall.api.count	Number of SMC API calls using the API	Cumulative
licensing.smart.smartAccount	Smart licensing account for the SMC	N/A

Metric Identification	Description	Data Type
licensing.smart.virtualAccount	Smart licensing virtual account for the SMC	N/A
licensing.smart.registrationStatus	Smart licensing registration status for the SMC	N/A
licensing.smart.productInstance Name	Smart licensing product identifier	N/A
ctr.ctr_enabled	CTR integration enabled	N/A
ctr.ats_integration_enabled	ATS integration enabled	N/A
ctr.alarm_sender_enabled	Stealthwatch alarms to CTR enabled	N/A
ctr.alarm_sender_minimal_severity	Minimal severity of alarms sent to CTR	N/A
ctr.enrichment_enabled	Enrichment request from CTR enabled	N/A
ctr.enrichment_limit	Number of top Security Events to be returned to CTR	Cumulative
ctr.enrichment_period	Time period for Security Events to be returned to CTR	Cumulative
ctr.number_of_alarms	Number of alarms sent to CTR	Cumulative
ctr.number_of_enrichment_ requests	Number of enrichment requests received from CTR	Cumulative
ctr.number_of_refer_requests	Number of requests for SMC pivot link received from CTR	Cumulative
ctr.swe_visibility_app_metrics	Number of data requests to Visibility Assessment SecureX tile	Cumulative

Metric Identification	Description	Data Type
ctr.swe_visibility_app_network_metrics	Number of data requests to Network Visibility SecureX tile	Cumulative
ctr.swe_alarming_hosts_by_category	Number of data requests to Alarming Hosts By Category SecureX tile	Cumulative
ctr.swe_top_inside_groups_by_traffic	Number of data requests to Top Inside Hosts SecureX tile	Cumulative
ctr.swe_top_outside_groups_by_traffic	Number of data requests to Top Outside Hosts SecureX tile	Cumulative
ctr.swe_top_alarming_hosts	Number of data requests to Top Alarming Hosts SecureX tile	Cumulative
ctr.swe_top_alarms_by_type_overall	Number of data requests to Top Alarms By Count SecureX tile	Cumulative
swrm_is_in_use	Response Management: Value is 1 if Response Management is used. Value is 0 if it is not used.	Snapshot
swrm_rules	Response Management: Number of custom rules	Snapshot
swrm_action_email	Response Management: Number of custom actions of Email type	Snapshot
swrm_action_syslog_message	Response Management: Number of custom actions of Syslog Message type	Snapshot
swrm_action_snmp_trap	Response Management: Number of custom actions of SNMP Trap type	Snapshot
swrm_action_ise_anc	Response Management: Number	Snapshot

Metric Identification	Description	Data Type
	of custom actions of ISE ANC Policy type	
swrm_action_webhook	Response Management: Number of custom actions of Webhook type	Snapshot
swrm_action_ctr	Response Management: Number of custom actions of Threat Response Incident type	Snapshot
va_ct	Visibility Assessment: Calculated run-time in milliseconds	Snapshot
va_ce	Visibility Assessment: Number of errors (when calculation crashes)	Snapshot
va_hcs	Visibility Assessment: Host count API response size in bytes (detect excessive response size)	Snapshot
va_ss	Visibility Assessment: Scanners API response size in bytes (detect excessive response size)	Snapshot
va_ses	Visibility Assessment: Security Events API response size in bytes (detect excessive response size)	Snapshot
sources_count	UDP Director: Daily > Number of sources	Snapshot
rules_count	UDP Director: Daily > Number of rules	Snapshot
packets_unmatched	UDP Director: Daily > Maximum unmatched packets	Snapshot

Metric Identification	Description	Data Type
packets_dropped	UDP Director: Daily > Dropped packets eth0	Snapshot
failover_role	SMC primary or secondary failover role in the cluster	N/A
sal_input_size	Number of entries in the pipeline input queue	Snapshot Freq: 1 minute
sal_completed_size	Number of entries in the completed batch queue	Snapshot Freq: 1 minute
sal_flush_time	Amount of time in milliseconds since the last pipeline flush	Snapshot Freq: 1 minute
batches_succeeded	Number of batches successfully written to the file	Interval Freq: 1 minute
batches_processed	Number of batches that were processed	Interval Freq: 1 minute
batches_failed	Number of batches that have failed to complete writing to the file	Interval Freq: 1 minute
files_moved	Number of files moved to the ready directory	Interval Freq: 1 minute
files_failed	Number of files that have failed to be moved	Interval

Metric Identification	Description	Data Type
		Freq: 1 minute
files_discarded	Number of files discarded due to error	Interval Freq: 1 minute
rows_written	Number of rows written to the referenced file	Interval Freq: 1 minute
rows_processed	Number of rows that were processed	Interval Freq: 1 minute
rows_failed	Number of rows that failed to be written	Interval Freq: 1 minute
total_batches_succeeded	Total number of batches successfully written to the file	App Start Freq: 1 minute
total_batches_processed	Total number of batches that were processed	App Start Freq: 1 minute
total_batches_failed	Total number of files that have failed to complete writing to the file	App Start Freq: 1 minute
total_files_moved	Total number of files moved to the ready directory	App Start Freq: 1 minute

Metric Identification	Description	Data Type
total_files_failed	Total number of files that have failed to be moved	App Start Freq: 1 minute
total_files_discarded	Total number of files discarded due to error	App Start Freq: 1 minute
total_rows_written	Total number of rows written to the referenced file	App Start Freq: 1 minute
total_rows_processed	Total number of rows that were processed	App Start Freq: 1 minute
total_rows_failed	Total number of rows that failed to be written	App Start Freq: 1 minute
sal_transformer_<transformer id>	Number of transformation errors in this transformer	Interval Freq: 1 minute
sal_bytes_per_event	Average number of bytes per event received	Interval Freq: 1 minute
sal_bytes_received	Number of bytes received from the UDP server	Interval Freq: 1 minute
sal_events_received	Number of events received from the UDP server	Interval Freq: 1 minute

Metric Identification	Description	Data Type
sal_total_events_received	Total number of events received by the router	App Start
sal_events_dropped	Number of unparsable events dropped	Interval Freq: 1 minute
sal_total_events_dropped	Total number of unparsable events dropped	App Start Freq: 1 minute
sal_events_ignored	Number of ignored/unsupported events	Interval Freq: 1 minute
sal_total_events_ignored	Total number of ignored/unsupported events	App Start Freq: 1 minute
sal_receive_queue_size	Number of events in the receive queue	Snapshot Freq: 1 minute
sal_events_per second	Ingest rate (events per second)	Interval Freq: 1 minute
sal_bytes_per_second	Ingest rate (bytes per second)	Interval Freq: 1 minute
cse.{domain id}.count	Number of custom security events for a domain ID	Snapshot
sna_trustsec_report_runs	Number of daily TrustSec report requests	Cumulative

Contacting Support

If you need technical support, please do one of the following:

- Contact your local Cisco Partner
- Contact Cisco Support
- To open a case by web: http://www.cisco.com/c/en/us/support/index.html
- To open a case by email: tac@cisco.com
- For phone support: 1-800-553-2447 (U.S.)
- For worldwide support numbers: https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

Copyright Information

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.