



Cisco Success Network とテレメトリデータ

この章では、Cisco Success Network についてと、Cisco Success Network を ASA で有効にする方法について説明します。また、Security Service Engine (SSE) クラウドに送信されるテレメトリデータポイントも示します。

- [Cisco Success Network について](#) (1 ページ)
- [Cisco Success Networkの有効化または無効化](#) (2 ページ)
- [ASA テレメトリデータの表示](#) (3 ページ)
- [Cisco Success Network - テレメトリデータ](#) (4 ページ)
- [デバッグテレメトリデータ](#) (10 ページ)

Cisco Success Network について

Cisco Success Network は、ASA の使用率情報と統計情報をストリーミングする Security Service Exchange (SSE) クラウドとのセキュアな接続を確立するユーザーが有効なクラウドサービスです。テレメトリをストリーミングすることによって、ASA 使用率とその他の詳細を構造化形式 (JSON) でリモートの管理ステーションに送信するメカニズムが提供されるため、次のメリットが得られます。

- 製品に利用可能な、追加のテクニカルサポートサービスとモニタリングについて通知します。
- シスコ製品の改善に役立ちます。

デフォルトでは、Cisco Success Network は、(ブレードレベルで) ASA デバイスをホストする Firepower 4100/9300 プラットフォームで有効になっています。ただし、テレメトリデータを送信するには、シャーシレベルで FXOS の設定を有効にするか (『[Cisco Firepower 4100/9300 FXOS CLI Configuration Guide](#)』を参照)、シャーシマネージャで Cisco Success Network を有効にする必要があります (『[Cisco Firepower 4100/9300 FXOS Firepower Chassis Manager Configuration Guide](#)』を参照)。

ASA デバイスで収集されるテレメトリデータには、CPU、メモリ、ディスク、または帯域幅、ライセンスの使用状況、設定されている機能リスト、クラスタ/フェールオーバー情報などが含まれます。「[Cisco Success Network - テレメトリデータ](#) (4 ページ)」を参照してください。

サポートされるプラットフォームと必要な設定

- ASA バージョン 9.13.1 以降を実行している FP9300/4100 プラットフォームでサポートされます。
- クラウドに接続するには、FXOS バージョン 2.7.1 以降が必要です。
- FXOS の SSE コネクタは、SSE クラウドに接続されている必要があります。この接続は、スマートライセンスバックエンドでスマートライセンスを有効にして登録することによって確立されます。FXOS の SSE コネクタは、スマートライセンスを登録することによって、SSE クラウドに自動的に登録されます。
- Cisco Success Network の設定は、シャーシマネージャで有効にする必要があります。
- テレメトリ設定は、ASA で有効にする必要があります。

ASA テレメトリデータが SSE クラウドに到達する仕組み

Cisco Success Network は、ASA 9.13(1) の Firepower 4100/9300 プラットフォームでデフォルトでサポートされています。FXOS サービスマネージャは、そのプラットフォームで実行されている ASA アプリケーションにテレメトリ要求を毎日送信します。ASA エンジンには、設定および接続ステータスに基づいて、スタンドアロンモードまたはクラスタモードのいずれかでテレメトリデータを FXOS に送信します。つまり、テレメトリのサポートが ASA で有効になっている、SSE コネクタのステータスが接続済みの場合、テレメトリスレッドは、システムやプラットフォーム、またはデバイス API、ライセンス API、CPU API、メモリ API、ディスク API、Smart Call Home 機能の API などさまざまなソースから必要な情報を取得します。ただし、テレメトリのサポートが ASA で無効になっているか、または SSE コネクタのステータスが切断である場合、ASA は、テレメトリの設定ステータスを示す応答を FXOS (appAgent) に送信し、テレメトリデータは送信しません。

FXOS では、1 つの SSE コネクタインスタンスのみが実行されます。これが SSE クラウドに登録されると、1 つのデバイスと見なされ、SSE インフラでは FXOS に 1 つのデバイス ID が割り当てられます。SSE コネクタを介して送信されるテレメトリレポートは、同じデバイス ID で分類されます。したがって、FXOS は、各 ASA からのテレメトリレポートを 1 つのレポートに集約します。スマートライセンス アカウント情報などのその他の内容が、レポートに追加されます。その後、FXOS は、最終的なレポートを SSE クラウドに送信します。テレメトリデータは、SSE データ交換 (DEX) に保存され、シスコの IT チームで使用できるようになります。

Cisco Success Networkの有効化または無効化

始める前に

- FXOS でスマートライセンスを有効にして登録します。

- シャーシレベルでFXOSのテレメトリサポートを有効にするか（『[Cisco Firepower 4100/9300 FXOS CLI Configuration Guide](#)』を参照）、シャーシマネージャで Cisco Success Network を有効にします（『[Cisco Firepower 4100/9300 FXOS Firepower Chassis Manager Configuration Guide](#)』を参照）。

手順

ASAでテレメトリサービスを有効にするには、グローバルコンフィギュレーションモードで、次のコマンドを入力します。テレメトリサービスを無効にするには、このコマンドの **no** 形式を使用します。

[no] service telemetry

例：

```
ciscoasa(config)# service telemetry  
ciscoasa(config)# no service telemetry
```

次のタスク

- テレメトリの設定とアクティビティのログまたはテレメトリデータを表示できます。「[ASA テレメトリデータの表示（3 ページ）](#)」を参照してください
- テレメトリデータおよびデータフィールドのサンプルを表示するには、次を参照してください。[Cisco Success Network - テレメトリデータ（4 ページ）](#)

ASA テレメトリデータの表示

始める前に

- ASAでテレメトリサービスを有効にします。「[Cisco Success Networkの有効化または無効化（2 ページ）](#)」を参照してください

手順

ネットワークの ASA デバイスのテレメトリデータを表示するには、特権 EXEC モードで次のコマンドを入力します。

show telemetry [history | last-report | sample]

例：

```
ciscoasa# show telemetry history
17:38:24 PDT Apr 30 2019: Telemetry support on the blade: enabled
17:38:03 PDT Apr 30 2019: Telemetry support on the blade: disabled
11:49:47 PDT Apr 29 2019: msgId 3. Telemetry support on the chassis: disabled
11:48:47 PDT Apr 29 2019: msgId 2. Telemetry request from the chassis received. SSE
connector status: enabled. Telemetry config on the blade: enabled. Telemetry data Sent
11:47:47 PDT Apr 29 2019: msgId 1. Telemetry request from the chassis received. SSE
connector status: enabled. Telemetry config on the blade: enabled. Telemetry data Sent.
```

テレメトリの設定とアクティビティに関連する過去 100 のイベントを表示するには **history**、FXOS に送信された最新のテレメトリデータを JSON 形式で表示するには **last-report**、即座に生成されたテレメトリデータを JSON 形式で表示するには **sample** を使用します。

Cisco Success Network - テレメトリデータ

Cisco Success Network は、Firepower 4100/9300 プラットフォームでデフォルトでサポートされています。FXOS サービスマネージャは、このプラットフォームで実行されている ASA エンジンにテレメトリ要求を毎日送信します。ASA エンジンには、要求を受信すると、接続ステータスに基づいて、スタンドアロンモードまたはクラスタモードのいずれかでテレメトリデータを FXOS に送信します。次の表に、テレメトリデータポイント、その説明、およびサンプル値を示します。

表 1: Device Info

データ ポイント	説明	値の例
Device Model	デバイス モデル	Cisco Adaptive Security Appliance
シリアル番号	デバイスのシリアル番号	FCH183771EZ
System Time	システムの動作期間	11658000
プラットフォーム	ハードウェア	FPR9K-SM-24
構成モード	展開タイプ	Native
セキュリティ コンテキスト モード	単一/複数	シングル

表 2: バージョン情報

データ ポイント	説明	値の例
バージョングローバル変数	ASA のバージョン	9.13.1.5
デバイスマネージャのバージョン	デバイスマネージャのバージョン	7.10.1

表 3: ライセンス情報

データ ポイント	説明	値の例
スマートライセンスのグローバル変数	有効化されているライセンス	regid.2015-01.com.cisco.ASA - SSP-STRONG-ENCRYPTION、 1.0_555507e9-85f8-4e41-96de- 860b59f10bbe

表 4: プラットフォームに関する情報

データ ポイント	説明	値の例
CPU	過去 5 分間の CPU 使用率	fiveSecondsPercentage : 0.2000000、 oneMinutePercentage : 0、 fiveMinutesPercentage : 0
メモリ	メモリ使用量	freeMemoryInBytes : 225854966384、 usedMemoryInBytes : 17798281616、 totalMemoryInBytes : 243653248000
ディスク	ディスク使用量	freeGB : 21.237285、 usedGB : 0.238805、 totalGB : 21.476090
Bandwidth	帯域幅の使用方法	receivedPktsPerSec : 3、 receivedBytesPerSec : 212、 transmittedPktsPerSec : 3、 transmittedBytesPerSec : 399

表 5: 機能情報

データ ポイント	説明	値の例
機能リスト	有効な機能リスト	name : cluster status : enabled

表 6: クラスタ情報

データ ポイント	説明	値の例
クラスタ情報	クラスタ情報	clusterGroupName : ssp-cluster interfaceMode : spanned unitName : unit-3-3 unitState : SLAVE otherMembers : items : memberName : unit-2-1 memberState : MASTER memberSerialNum : FCH183771BA

表 7: フェールオーバー情報

データ ポイント	説明	値の例
フェールオーバー	フェールオーバー情報	myRole : Primary、 peerRole : Secondary、 myState : active、 peerState : standby、 peerSerialNum : FCH183770EZ

表 8: ログイン情報

データ ポイント	説明	値の例
ログイン	ログイン履歴	loginTimes : 2 times in last 2 days、 lastSuccessfulLogin : 12:25:36 PDT Mar 11 2019

ASA テレメトリデータの例

次に、JSON 形式で ASA から送信されるテレメトリデータの例を示します。サービスマネージャは、この入力を受信すると、すべての ASA のデータを集約し、SSE コネクタに送信する前に必要なヘッダー/フィールドを追加します。ヘッダー/フィールドには、“version”、“metadata”、“payload” (“recordedAt”、“recordType”、“recordVersion”、および ASA テレメトリ

データの "smartLicenseProductInstanceIdentifier"、"smartLicenseVirtualAccountName" などを含む) があります。

```
{
  "version": "1.0",
  "metadata": {
    "topic": "ASA.telemetry",
    "contentType": "application/json"
  },
  "payload": {
    "recordType": "CST_ASA",
    "recordVersion": "1.0",
    "recordedAt": 1557363423705,
    "SSP": {
      "SSPdeviceInfo": {
        "deviceModel": "Cisco Firepower FP9300 Security Appliance",
        "serialNumber": "JMX2235L01J",
        "smartLicenseProductInstanceIdentifier": "f85a5bb0-xxxx-xxxx-xxxx-xxxxxxxxxx",
        "smartLicenseVirtualAccountName": "SSP-general",
        "systemUptime": 198599,
        "udiProductIdentifier": "FPR-C9300-AC"
      },
      "versions": {
        "items": [
          {
            "type": "package_version",
            "version": "92.7(1.342g)"
          }
        ]
      }
    },
    "asaDevices": {
      "items": [
        {
          "deviceInfo": {
            "deviceModel": "Cisco Adaptive Security Appliance",
            "serialNumber": "AANNXXXX",
            "systemUptime": 285,
            "udiProductIdentifier": "FPR9K-SM-36",
            "deploymentType": "Native",
            "securityContextMode": "Single"
          },
          "versions": {
            "items": [
              {
                "type": "asa_version",
                "version": "201.4(1)82"
              },
              {
                "type": "device_mgr_version",
                "version": "7.12(1)44"
              }
            ]
          }
        }
      ],
      "licenseActivated": {
        "items": [
          {
            "type": "Strong encryption",
            "tag":
"regid.2015-01.com.cisco.ASA-SSP-STRONG-ENCRYPTION,1.0_xxxxxxx-xxxx-xxxx-96de-860b59f10bbe",
            "count": 1
          }
        ]
      }
    }
  }
}
```

```

        "type": "Carrier",
        "tag":
"regid.2015-01.com.cisco.ASA-SSP-MOBILE-SP,1.0_XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXX",
        "count": 1
    }
]
},
"CPUUsage": {
    "fiveSecondsPercentage": 0,
    "oneMinutePercentage": 0,
    "fiveMinutesPercentage": 0
},
"memoryUsage": {
    "freeMemoryInBytes": 99545662064,
    "usedMemoryInBytes": 20545378704,
    "totalMemoryInBytes": 120091040768
},
"diskUsage": {
    "freeGB": 21.237027,
    "usedGB": 0.239063,
    "totalGB": 21.476090
},
"bandwidthUsage": {
    "receivedPktsPerSec": 3,
    "receivedBytesPerSec": 268,
    "transmittedPktsPerSec": 4,
    "transmittedBytesPerSec": 461
},
"featureStatus": {
    "items": [
        {
            "name": "call-home",
            "status": "enabled"
        },
        {
            "name": "cluster",
            "status": "enabled"
        },
        {
            "name": "firewall_user_authentication",
            "status": "enabled"
        },
        {
            "name": "inspection-dns",
            "status": "enabled"
        },
        {
            "name": "inspection-esmtp",
            "status": "enabled"
        },
        {
            "name": "inspection-ftp",
            "status": "enabled"
        },
        {
            "name": "inspection-netbios",
            "status": "enabled"
        },
        {
            "name": "inspection-rsh",
            "status": "enabled"
        },
        {
            "name": "inspection-sip",

```

```

        "status": "enabled"
    },
    {
        "name": "inspection-sqlnet",
        "status": "enabled"
    },
    {
        "name": "inspection-sunrpc",
        "status": "enabled"
    },
    {
        "name": "inspection-tftp",
        "status": "enabled"
    },
    {
        "name": "inspection-xdmcp",
        "status": "enabled"
    },
    {
        "name": "logging-console",
        "status": "informational"
    },
    {
        "name": "management-mode",
        "status": "normal"
    },
    {
        "name": "sctp-engine",
        "status": "enabled"
    },
    {
        "name": "threat_detection_basic_threat",
        "status": "enabled"
    },
    {
        "name": "threat_detection_stat_access_list",
        "status": "enabled"
    },
    {
        "name": "webvpn-activex-relay",
        "status": "enabled"
    },
    {
        "name": "webvpn-dtls",
        "status": "enabled"
    }
    ]
},
"clusterInfo": {
    "clusterGroupName": "ssp-cluster",
    "interfaceMode": "spanned",
    "unitName": "unit-3-3",
    "unitState": "SLAVE",
    "otherMembers": {
        "items": [
            {
                "memberName": "unit-2-1",
                "memberState": "MASTER",
                "memberSerialNum": "FCH183771BA"
            },
            {
                "memberName": "unit-2-3",
                "memberState": "SLAVE",
                "memberSerialNum": "FLM1949C6JR"
            }
        ]
    }
}

```

```

    },
    {
      "memberName": "unit-2-2",
      "memberState": "SLAVE",
      "memberSerialNum": "xxxxxxxx"
    },
    {
      "memberName": "unit-3-2",
      "memberState": "SLAVE",
      "memberSerialNum": "xxxxxxxx"
    },
    {
      "memberName": "unit-3-1",
      "memberState": "SLAVE",
      "memberSerialNum": "xxxxxxxx"
    }
  ]
},
"loginHistory": {
  "loginTimes": "1 times in last 1 days",
  "lastSuccessfulLogin": "12:25:36 PDT Mar 11 2019"
}
}

```

デバッグテレメトリデータ

始める前に

- ASA でテレメトリサービスを有効にします。「[Cisco Success Networkの有効化または無効化（2 ページ）](#)」を参照してください

手順

- ステップ 1** テレメトリに関連するデバッグメッセージを表示するには、特権 EXEC モードで次のコマンドを使用してデバッグテレメトリサービスを有効にします。

debug telemetry<1-255>

例：

```
asa# debug telemetry ?
<1-255> Specify an optional debug level (default is 1)
```

デバッグテレメトリサービスを無効にするには、このコマンドの **no** 形式を使用します。

- ステップ 2** 選択したデバッグレベルのデバッグテレメトリメッセージを表示するには、次のコマンドを使用します。

show debug telemetry

例：

```
asa# show debug telemetry
debug telemetry  enabled at level 1

[telemetry_collect_device_info]: telemetry successfully collected device info
[telemetry_collect_versions]: telemetry successfully collected version info
[telemetry_collect_licenses]: no smart-lic entitlement in use
[telemetry_collect_cpu]: telemetry successfully collected cpu info
[telemetry_collect_memory]: telemetry successfully collected mem info
[telemetry_collect_disk_usage]: telemetry successfully collected disk info
[telemetry_collect_bandwidth_usage]: telemetry successfully collected bandwidth usage
info
[telemetry_collect_enabled_feature_status]: telemetry successfully collected enabled
feature info
[telemetry_collect_cluster_info]: telemetry successfully collected cluster info
[telemetry_collect_failover_info]: ha is not configured
[telemetry_get_user_login_hist]: telemetry successfully collected login history
[telemetry_collect_blocks]: telemetry successfully collected block info
[telemetry_collect_perfmon]: telemetry successfully collected perfmon stats
[telemetry_collect_resource_usage]: telemetry successfully collected res usage
[telemetry_collect_process_cpu_usage]: telemetry successfully collected res usage
[telemetry_collect_crashinfo]: telemetry successfully collected crashinfo
[telemetry_collect]: the serialized string is generated
[telemetry_collect]: successfully allocated mem for serialized string
[telemetry_history_add_record]: telemetry has a new history record: 16:23:29 PDT Oct 22
2019: Telemetry support on the blade: enabled
[telemetry_history_add_record]: telemetry has a new history record: 16:24:01 PDT Oct 22
2019: Telemetry support on the blade: disabled
```

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。