Cisco Stealthwatch Cloud License v1.0.1

コンフィギュレーション ガイド

Cisco Stealthwatch Cloud License v1.0.1 コンフィギュレーション ガイド
© 2016 Lancope, Inc. All rights reserved.

ドキュメントの日付:2016 年 11 月 2 日

NOTICE

本資料は Lancope が所有する専有情報であり、一定の制限の下で機密情報として提供されるものです。Lancope は、法律が許す最大の範囲で、権利放棄、選択、または制限なく、本資料および本資料に含まれる情報に対する権利を留保します。本資料または本資料に含まれる情報の全部またはその一部の複製、使用、表示、またはその他の開示もしくは公開は、既知の方法でもその後開発された方法でも、方法の如何を問わず、Lancope の書面による同意がない限り、厳格に禁止されています。

Trademarks

Lancope、Stealthwatch、およびその他の商標は、Lancope, Inc. の登録商標または商標です。その他すべての商標は、それぞれの所有者の財産です。

目次

概要 5

対象読者 6
前提条件 6
アクセス コントロール リスト 6
プロセスの概要 7

Cloud License インスタンスの導入 8

Cloud License コンセントレータの設定 11

FlowCollector にデータを返すためのコンセントレータの設定 13

コンセントレータ ライセンスのインストールと確認 15

サービス ホスト インスタンスへのクラウド エージェントのインストール 18

最終手順 21

ホスト グループの作成 21
設定の確認 23
トラブルシューティングのためのエージェント GUID の確認 24
SMC クライアント インターフェイスでのフローの確認 24

付録 26

コンセントレータ AMI アップグレード プロセス 26
前提条件 26
情報の例 26
AMI のアップグレード手順 27

コンセントレータの停止と必要なファイルのバックアップ 28
AWS での新しいコンセントレータ インスタンスの作成 31
新しいコンセントレータの設定 31
Flexnet Operations での新しいコンセントレータの登録と古いコンセントレータの機能の無効化 34
新しいライセンスと新しいコンセントレータの関連付け 34
使用中の Elastic IP アドレスの再関連付け 36
エージェントの通信の確認 37

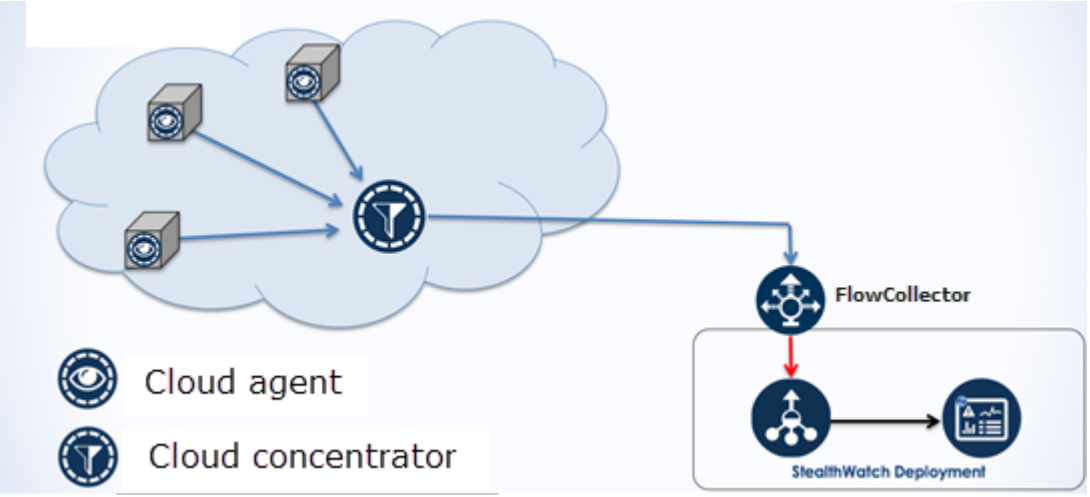
© 2016 Cisco Systems, Inc. All Rights Reserved

© 2016 Cisco Systems, Inc. All Rights Reserved

1

概要

このドキュメントでは、Cisco Stealthwatch Cloud License v1.0.0 およびそのエージェントのインストール手順と設定手順について説明します。このアプリケーションは、クラウド システムのデバイスからの IPFIX データを収集します。これらのデバイスには、データをコンセントレータに送信するクラウド エージェントがインストールされます。コンセントレータは、データを Stealthwatch FlowCollector に送信します。次の図は、システム設計を示しています。



次の IPFIX フィールドは、エージェントによって収集され、Cloud License と FlowCollector によって処理されます。

- プロトコル（Protocol）
- ソース IP
- 送信元ポート（Source Port）
- 宛先 IP（Destination IP）
- 宛先ポート（Destination Port）
- バイト（Bytes）
- パケット
- フローの開始
- フローの停止
- 方向（Direction）

© 2016 Cisco Systems, Inc. All Rights Reserved

現時点では、Stealthwatch Cloud License は、Linux オペレーティング システムの RedHat Enterprise（5 ～ 7）と CentOS（バージョン 5 ～ 7）をサポートしています。Windows は今後のリリースでサポートされる予定です。

注：このドキュメントでは、例として CentOS を使用します。

対象読者

このドキュメントは、Stealthwatch Cloud License の設定担当者を対象としています。

前提条件

Stealthwatch Cloud License を設定するには、次のものが必要です。

- Stealthwatch System v6.7.1 以降
- Stealthwatch Management Console（SMC）と FlowCollector
- 仮想プライベート クラウド(VPC)へのセキュアなチャネル（VPN または DirectConnect）
- ダウンロードおよびライセンス センターのリンク（『Downloading and Licensing StealthWatch Products』の説明に従ってライセンスを取得してください）
- サポートされるクラウド サーバ
- SSH クライアント（PuTTY など）を実行するクライアント
- Amazon Web Services のアカウント
- Cloud License コンセントレータ（Amazon AMI）

アクセス コントロール リスト

Cisco Stealthwatch Cloud License には次のポートが必要です。

クラウド エージェント：

- アウトバウンド：443（「任意の場所」へ、またはコンセントレータの IP アドレスへ）

クラウド コンセントレータ：

- インバウンド：443（エージェント サブネットから、または「任意の場所」から）
- インバウンド：22（SSH/管理アクセス用）
- アウトバウンド：2055（FlowCollector がコンセントレータからのデータの取得に使用）

© 2016 Cisco Systems, Inc. All Rights Reserved

- アウトバウンド：8080（stamp-agent.sh スクリプトがエージェントのプロビジョニングに使用）

プロセスの概要

Stealthwatch Cloud License の設定プロセスでは、次の手順を実行する必要があります。これらの手順については、このガイドで詳しく説明します。

1. Cloud License インスタンスを導入する。
2. Cloud License コンセントレータを設定する。
3. ライセンスを確認し、インストールする。
4. クラウド エージェントをサービス ホスト インスタンスにインストールする。
5. Final Steps：ホスト グループを追加し、設定を確認する。

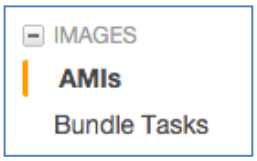
© 2016 Cisco Systems, Inc. All Rights Reserved

2

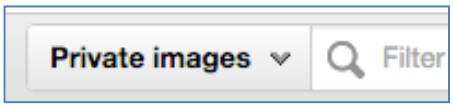
CLOUD LICENSE インスタンスの導入

Cloud License を導入するには、次の手順を実行します。

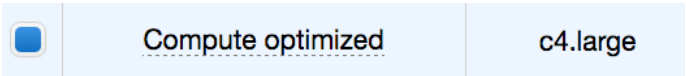
1. AWS のアカウントにログインし、[サービス(Services)] ドロップダウン メニューから [EC2] を選択します。
2. 左側の列の [イメージ(IMAGES)] の下にある [AMI(AMIs)] をクリックします。



3. 左上のドロップダウン リストから [プライベート イメージ(Private Images)] を選択します。



4. 自分の AMI のチェックボックスをオンにして、[作成(Launch)] ボタンをクリックします。
5. [インスタンス タイプの選択(Choose an Instance Type)] ページで、パフォーマンス要件に適したサイズのチェックボックスをオンにして、[次の手順:インスタンスの詳細の設定(Next: Configure Instance Details)] をクリックします。サイジング要件については、次の表を参照してください。



エージェント	推奨される AWS インスタンスのタイプ	同等の仮想アプライアンス			
		CPU コア	メモリ(GB)	ディスク(GB)	ネットワーク帯域幅
1000	c4.large	2	4	8	250 Mbps

© 2016 Cisco Systems, Inc. All Rights Reserved

エージェント	推奨される AWS インスタンスのタイプ	同等の仮想アプライアンス			
		CPU コア	メモリ（GB）	ディスク（GB）	ネットワーク帯域幅
2000	c4.xlarge	4	8	16	500 Mbps
4000	c4.2xlarge	8	16	32	1 Gbps
10,000	c4.4xlarge	16	32	64	2 Gbps
20,000	c4.8xlarge	32	64	64	4 Gbps

6. 必要なインスタンス設定パラメータを設定し、[確認と作成（Review and Launch）] をクリックします。

   [インスタンス起動のレビュー（Review Instance Launch）] ページが開きます。

7. [セキュリティ グループ（Security Groups）] セクションで、右にある [セキュリティ グループの編集（Edit security groups）] リンクをクリックします。

   [セキュリティ グループの設定（Configure Security Group）] ページが開きます。

8. [ルールの追加（Add Rule）] ドロップダウン リストをクリックし、[HTTPS] 選択します。
9. セキュリティ グループのルールがデフォルトでアウトバウンド アクセスを許可するため、UDP 2055 と TCP 8080 のアウトバウンド ルールは不要です。
10. [確認と作成（Review and Launch）] ボタンをクリックします。

    [インスタンス起動のレビュー（Review Instance Launch）] ページが開きます。

11. [作成（Launch）] をクリックします。
12. [既存のキー ペアを選択するか、新しいキー ペアを作成します。（Select an existing key pair or create a key pair）] ダイアログが開きます。ここで、既存のキー ペアを使用するか、新しいキー ペアを作成します。
13. キー ペアを選択し、[インスタンスの作成（Launch Instance）] をクリックします。

    [作成ステータス（Launch Status）] ページが開きます。

© 2016 Cisco Systems, Inc. All Rights Reserved

14. インストールされたインスタンスのリンクをクリックします。

    [インスタンスの作成（Launch Instance）] ページが開きます。

15. [説明（Description）] ページの下部にあるパブリック DNS IP アドレスをクリックします。

    コンソール画面が開きます。

© 2016 Cisco Systems, Inc. All Rights Reserved

3

Cloud License コンセントレータの設定

このセクションでは、Cloud License コンセントレータ インスタンスのシステム生成サムプリントと完全修飾ドメイン名（FQDN）を使用して、カスタム エージェント（RPM インストール ファイル）にサムプリントを付加してダウンロードします。これにより、カスタム エージェントが Cloud License コンセントレータ インスタンスに結び付けられます。

Cloud License コンセントレータで次の設定が完了していることを確認してください。

1. 以前に選択したキー ペアを使用して以前に作成した Cloud License コンセントレータに SSH を使用してログインします。

```
bash-3.2$ ssh -i keypair.pem admin@swcconc.example.com
```

2. hostname コマンドを使用してコンセントレータの FQDN を設定します。これには AWS で割り当てられた FQDN またはカスタマイズされた解決可能な FQDN を使用できます。

```
-bash-4.1$ sudo hostname swcconc.example.com
```

3. 「127.0.0.1」行でコンセントレータの FQDN を `/etc/hosts` ファイルに追加します。

```
127.0.0.1    swcconc.example.com localhost ….
```

4. 次の行を追加することによってコンセントレータの FQDN を `/etc/sysconfig/network` ファイルに追加します。

```
HOSTNAME=swcconc.example.com
```

5. ログアウトし、ログインしなおして、FQDN の変更が受け入れられたことを確認します。

```
-bash-4.1$ hostname
swcconc.example.com
```

© 2016 Cisco Systems, Inc. All Rights Reserved

クラウド エージェント インストール RPM にサムプリントを付加するには、次の手順を実行します。

1. Cloud License コンセントレータ シェルにログインし、次のコマンドを実行して新しいサーバ キーと証明書を生成します。

```
sudo /opt/swcconc/bin/gen-keypair.sh -d [public.DNS.name] -I
```

結果の例は、次のとおりです。

```
-bash-4.1$ sudo /opt/swcconc/bin/gen-keypair.sh -d
swcconc.example.com -I
Generating new key pair for host swcconc.example.com

    Created new keypairs
    Hostname:  swcconc.example.com
    JKS keyfile:   swcconc_example_com.jks
    P12 keyfile:   swcconc_example_com.p12
    Expires in :   1000 days from now
    Key strength:  2048 bits
    Passphrase:    r4myz8ff5yESDfyb
    Thumbprint:    f56664120cf21dc89f0188878c7557d575485ef4
    SHA1 (P12):    2ccbb441eb50e7430f787840ff30a164ce6d921d
    SHA1 (JKS):    ceee158792e032783a897f68810531e981130c0f

Changing SSL keypair served...
Setting SSL keypair to
/opt/swcconc/ssl_keys/swcconc_example_com.jks ...
Changing settings in Jetty's SSL config file
Restarting service swcconc

Stopping  [done]

Starting  [done]
The Jetty KeyStore has been installed and Jetty has been
restarted

-bash-4.1$
```

2. `/opt/swcconc/bin/stamp-agent.sh` スクリプトを実行して、コンセントレータ用に設定されたエージェントの .rpm ファイルと swcagent.conf ファイルにサムプリントを付加し、ダウンロードします。.conf ファイルは、.rpm に書き込まれたものと同じで、導入の柔軟性を高めるためにのみ提供されています。

© 2016 Cisco Systems, Inc. All Rights Reserved

結果の例は、次のとおりです。

```
-bash-4.1$ sudo /opt/swcconc/bin/stamp-agent.sh
[SUCCESS] Files below are available for download!

/opt/swcconc/agent/1.0.0.490_swcconc.example.com_swcagent.conf
/opt/swcconc/agent/swcagent-1.0.0.490_swcconc.example.com.rpm
-bash-4.1$
```

3. `/opt/swcconc/agent` ディレクトリの内容を確認します。

   結果の例は、次のとおりです。

```
-bash-4.1$ ls /opt/swcconc/agent/
1.0.0.490_swcconc.example.com_swcagent.conf
swcagent-1.0.0.490_swcconc.example.com.rpm
-bash-4.1$
```

FlowCollector にデータを返すためのコンセントレータの設定

フローを FlowCollector または UDP Director に送信するように Cloud License コンセントレータを設定するには、次の手順を実行します。

1. Cloud License コンセントレータで、任意のテキスト エディタ（vi、nano、Emacs など）を使用して次のファイルを開きます。

```
sudo vi /opt/swcconc/swcconc.settings
```

2. FlowCollector（または UDP Director）の IP アドレスを使用して次の行を検索し、編集してアンコメントします。

   結果の例は、次のとおりです。

```
IPFIX_COLLECTOR_HOST=<FlowCollector IP/FQDN>
IPFIX_COLLECTOR_PORT=<FlowCollector Port>
```

3. ファイルを保存して、閉じます。

© 2016 Cisco Systems, Inc. All Rights Reserved

4. Cloud License コンセントレータのライセンス ステータスを確認するために、

   `/opt/swcconc/bin` ディレクトリにある swcconc スクリプトを呼び出します。

```
-bash-4.1$ sudo /opt/swcconc/bin/swcconc --describe-server
19:56:55.275 ZSERVER [main] INFO com.ziften.server.cli.Cli -
Cli started.Options: [--describe-server]
Showing server info
{
  "serverHostId": "CLVE-EEC19E60-CADE-4BC5-AF6D-0AD752B36CD3",
  "licenses": [
    {
      "license": {
        "hostId": "CLVE-EEC19E60-CADE-4BC5-AF6D-0AD752B36CD3",
        "feature": "ZFLOW_IPFIX_CONCENTRATOR",
        "maxAllowedAgents": 0,
        "licenseSource": "noLicenseAvailableSource"
      },
      "utilization": {
        "limitExceeded": true,
        "maxAllowedAgents": 0,
        "connectedAgentsNumber": 0,
        "overLimitAgentCount": 0,
        "connectedAgentsGuids": []
      }
    }
  ]
}
-bash-4.1$
```

   Cloud License コンセントレータに有効なライセンスがないため、"limitExceeded" の値は「true」に設定され、"maxAllowedAgents" の値は「0」に設定されています。

   注:hostID は登録時にアプライアンスのシリアル番号として使用される文字列です。

5. Cloud License コンセントレータ サービスを再起動します。

```
-bash-4.1$ sudo service swcconc restart
Stopping     [done]
Starting     [done]
-bash-4.1$
```


© 2016 Cisco Systems, Inc. All Rights Reserved

4

コンセントレータ ライセンスのインストールと確認

Cloud License コンセントレータのライセンスを取得するには、次の手順を実行します。

1. ライセンスを取得するために https://lancope.flexnetoperations.com（Lancope のダウンロードおよびライセンス センター [英語]）にアクセスします。ログイン ページが開きます。
2. ログイン ID とパスワードを該当するフィールドに入力し、[ログイン（Login）] をクリックします。製品ホームページが開きます。
3. hostID を使用して、Cloud License コンセントレータ製品の登録に必要な手順に従います。

注：インターネットにアクセスできないCloud License コンセントレータのライセンスを適用する場合は、そのシリアル番号に関連付けられている Cisco Stealthwatch Cloud ライセンス ファイルを見つけてダウンロードしてください。オフラインでのライセンス適用を完了するには、このファイルを Cloud License コンセントレータに配備する必要があります。

4. インターネットにアクセスできる環境で Cloud License コンセントレータ ライセンスを適用するには、次のコマンドを実行します。

```
sudo /opt/swcconc/bin/swcconc --lancope-fetch-license
```

結果の例は、次のとおりです。

```
-bash-4.1$ sudo /opt/swcconc/bin/swcconc --lancope-fetch-
license
04:21:03.184 ZSERVER [main] INFO com.ziften.server.cli.Cli -
Cli started.Options: [--lancope-fetch-license]
Fetching Lancope license from licensing server
{
  "licenseServerUrl":
"https://lancope.flexnetoperations.com/control/lncp/deviceservi
ces",
```

© 2016 Cisco Systems, Inc. All Rights Reserved

```
  "applianceHostId": "CLVE-EEC19E60-CADE-4BC5-AF6D-
1235C96A0B59",
  "featureCount": 1,
  "features": [
    {
      "name": "CloudLicenseAgents",
      "agentCount": 10,
      "issued": "2016-05-12 12:00:00+0000",
      "startDate": "2015-11-03 12:00:00+0000",
      "expiration": "2016-11-03 11:59:59+0000"
    }
  ]
}
```

5. オフライン環境で Cloud License コンセントレータ ライセンスを適用するには、ライセンス ファイルをダウンロードし、セキュア コピーによって .bin ファイルをクラウド コンセントレータにコピーします。

```
bash-3.2$ scp -i keypair.pem CLVE-EEC19E60-CADE-4BC5-AF6D-
0AD752B36CD3.bin admin@swcconc.example.com:~/.
```

Cloud License コンセントレータ シェルで、次のコマンドを実行します。

```
sudo /opt/swcconc/bin/swcconc --lancope-load-license <filepath>
```

結果の例は、次のとおりです。

```
-bash-4.1$ sudo /opt/swcconc/bin/swcconc --lancope-load-license
~/CLVE-EEC19E60-CADE-4BC5-AF6D-0AD752B36CD3.bin
20:12:58.018 ZSERVER [main] INFO com.ziften.server.cli.Cli -
Cli started.Options: [--lancope-load-license, /home/admin/CLVE-
EEC19E60-CADE-4BC5-AF6D-0AD752B36CD3.bin]
Loading Lancope license from file /home/admin/CLVE-EEC19E60-
CADE-4BC5-AF6D-0AD752B36CD3.bin
{
  "applianceHostId": "CLVE-EEC19E60-CADE-4BC5-AF6D-
0AD752B36CD3",
  "featureCount": 1,
  "features": [
    {
      "name": "CloudLicenseAgents",
      "agentCount": 10,
      "issued": "2016/05/19 12:00:00+0000",
      "startDate": "2015-11-03 12:00:00+0000",
      "expiration": "2016-11-03 11:59:59+0000"
    }
  ]
}
-bash-4.1$
```


© 2016 Cisco Systems, Inc. All Rights Reserved

6. 次のコマンドを使用して Cloud License コンセントレータ サービスを再起動します。

```
sudo service swcconc restart
```

数分待ってから次のコマンドを実行します。

```
sudo /opt/swcconc/bin/swcconc --describe-server
```

注：Cloud License コンセントレータ サービスの初期化が完了する前に `-describe-server` コマンドを実行すると、接続が拒否されたことを示す Java 例外が表示される場合があります。その場合は、しばらくしてからもう一度試してください。

「`"limitExceeded": False`」というメッセージと許可されるエージェントの数が表示されます。

結果の例は、次のとおりです。

```
-bash-4.1$ sudo /opt/swcconc/bin/swcconc --describe-server
18:26:22.610 ZSERVER [main] INFO com.ziften.server.cli.Cli -
Cli started.Options: [--describe-server]
Showing server info
{
  "serverHostId": " CLVE-EEC19E60-CADE-4BC5-AF6D-0AD752B36CD3",
  "licenses": [
    {
      "license": {
        "hostId": "CLVE-EEC19E60-CADE-4BC5-AF6D-22000B480702",
        "feature": "ZFLOW_IPFIX_CONCENTRATOR",
        "maxAllowedAgents": 10,
        "licenseSource": "flexnetTrustedStorageLicenseSource"
      },
      "utilization": {
        "limitExceeded": false,
        "maxAllowedAgents": 10,
        "connectedAgentsNumber": 0,
        "overLimitAgentCount": 0,
        "connectedAgentsGuids": []
      }
    }
  ]
}
-bash-4.1$
```

© 2016 Cisco Systems, Inc. All Rights Reserved

5

サービス ホスト インスタンスへのクラウド エージェントのインストール

クラウド エージェントをダウンロードしてサービス ホスト インスタンスにインストールするには、次の手順を実行します。

1. セキュア コピー（scp）によってコンセントレータからホストにエージェントをコピーします。

   結果の例は、次のとおりです。

```
bash-3.2$ scp -i keypair.pem
admin@swcconc.example.com:/opt/swcconc/agent/* .
swcagent-1.0.0.490_swcconc.example.com.rpm     100%
bash-3.2$
```

2. サービス ホスト インスタンスで、次のコマンドを実行してエージェントをインストールします。

   RedHat/CentOS の場合：

```
-bash-4.1$ sudo rpm -ivh swcagent-
1.0.0.490_swcconc.example.com.rpm
Preparing...                          ####################
[100%]
Updating / installing...
   1:swcagent-1.0.0-490                 ####################
[100%]
-bash-4.1$
```

3. （任意）エージェントのインストールが完了したら、次のコマンドを実行して、システムの起動時にサービスが起動するように設定します。

   SysV ベースのシステムの場合：

```
-bash-4.1$ sudo chkconfig --add swcagent
```


© 2016 Cisco Systems, Inc. All Rights Reserved

systemd ベースのシステムの場合:

```
-bash-4.1$ sudo systemctl enable swcagent.service
-bash-4.1$ sudo systemctl daemon-reload
```

4. エージェント サービスを起動するために、次のコマンドを実行します。

   SysV ベースのシステムの場合:

```
-bash-4.1$ sudo service swcagent start
```

   systemd ベースのシステムの場合:

```
-bash-4.1$ sudo systemctl start swcagent.service
```

5. エージェント インスタンスとコンセントレータの間の接続を確認するために、curl または wget を使用して接続を確認します。「401 Unauthorized」という HTTP メッセージが表示されます。

```
-bash-4.1$ curl -k "https://swcconc.example.com"
<html>
<head>
<meta http-equiv="Content-Type" content="text/html;
charset=UTF-8"/>
<title>Error 401 Unauthorized</title>
</head>
<body><h2>HTTP ERROR 401</h2>
<p>Problem accessing /.Reason:
<pre>    Unauthorized</pre></p><hr><i><small>Powered by
Jetty://</small></i><hr/>

</body>
</html>
-bash-4.1$
```

6. フロー データが Cloud License コンセントレータに送信されていることを確認するために、`tcpdump` をインストールできます。

```
-bash-4.1$ sudo yum install tcpdump
```

注:エージェント インスタンスとコンセントレータの間の通信は、HTTPS(tcp/443)を介して行われます。

© 2016 Cisco Systems, Inc. All Rights Reserved

7. クラウド エージェント インスタンスから次のコマンドを実行して、コンセントレータに送信される暗号化された HTTPS（443/tcp）トラフィックを表示します。

```
sudo tcpdump -i eth0 port 443
```

注：大規模な導入の場合は、これらの手動手順を自動プロビジョニング手法（Puppet、Chef、Ansible、Elastic Beanstalk など）に組み込む必要があります。

© 2016 Cisco Systems, Inc. All Rights Reserved

6

最終手順

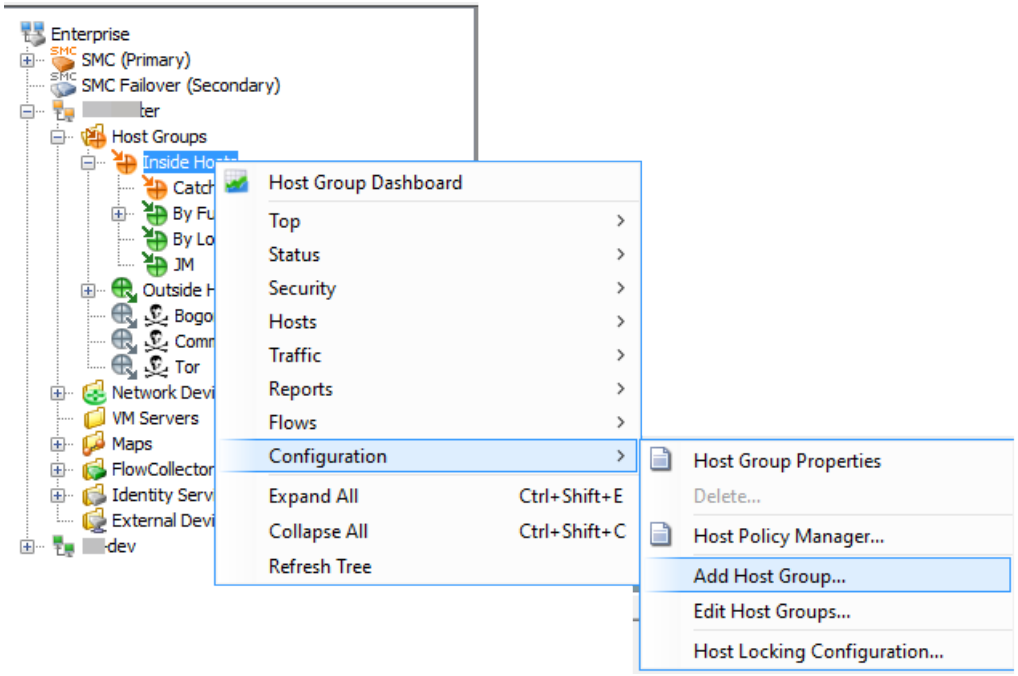
プロセスの最後の手順では、ホスト グループを作成し、設定を確認します。

ホスト グループの作成

仮想プライベート クラウド（VPC）のプライベート IP アドレスを含むホスト グループを作成します。

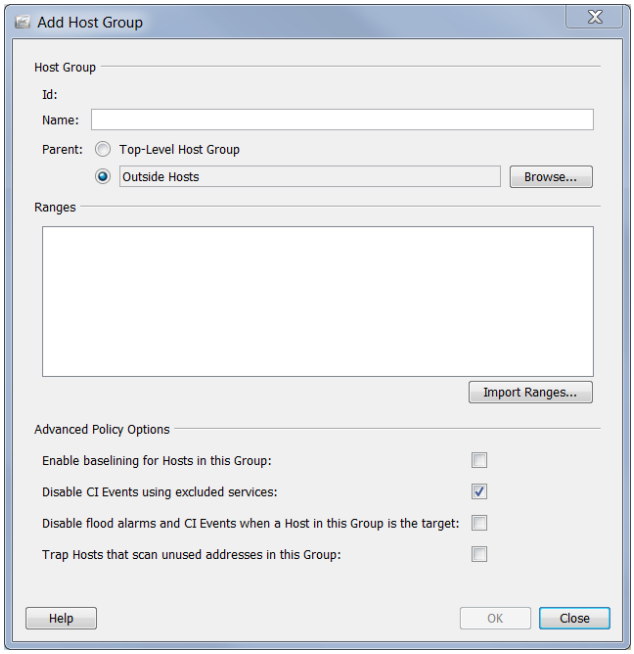
ホスト グループを作成するには、次の手順を実行します。

1. SMC クライアント インターフェイスで、[企業（Enterprise）] ページ ツリー メニューから [内部ホスト（Inside Hosts）] フォルダをクリックします。
2. [内部ホスト（Inside Hosts）] ホスト グループを右クリックし、[設定（Configuration）] > [ホスト グループの追加（Add Host Group）] の順に選択します。



© 2016 Cisco Systems, Inc. All Rights Reserved

[ホスト グループの追加（Add Host Group）] ダイアログが開きます。



3. [名前（Name）] フィールドに、追加するホスト グループの名前（例：Partners）を入力します。
4. [親（Parent）] フィールドで、新しいホスト グループの親をクリックします（デフォルトが正しくない場合）。
5. [範囲（Ranges）] フィールドに、必要な IP アドレスの範囲を入力します。このホスト グループの IP アドレスが含まれている既存のファイルがある場合は、[範囲をインポート（Import Ranges）] をクリックします。
6. [詳細ポリシー オプション（Advanced Policy Options）] セクションで、新しいホスト グループに適用するオプションをクリックします。
7. [OK] をクリックして [ホスト グループの追加（Add Host Group）] ダイアログを閉じます。[企業（Enterprise）] ページ ツリー メニューが自動的に更新され、新しいホスト グループが含まれます。

© 2016 Cisco Systems, Inc. All Rights Reserved

設定の確認

このセクションでは、Stealthwatch Cloud License の設定を確認する方法について説明します。

コンセントレータで次のコマンドを実行して、サービス インスタンスから HTTPS を介してデータを受信していることを確認します。

```
sudo yum install tcpdump
```

つづいて、次のコマンドを実行します。

```
sudo tcpdump -i eth0 port 443
```

また、コンセントレータで次のコマンドを実行して、トラフィックが FlowCollector（または UDP Director）に送信されていることを確認します。

```
sudo tcpdump -i eth0 -n dst host <FlowCollector IP>
```

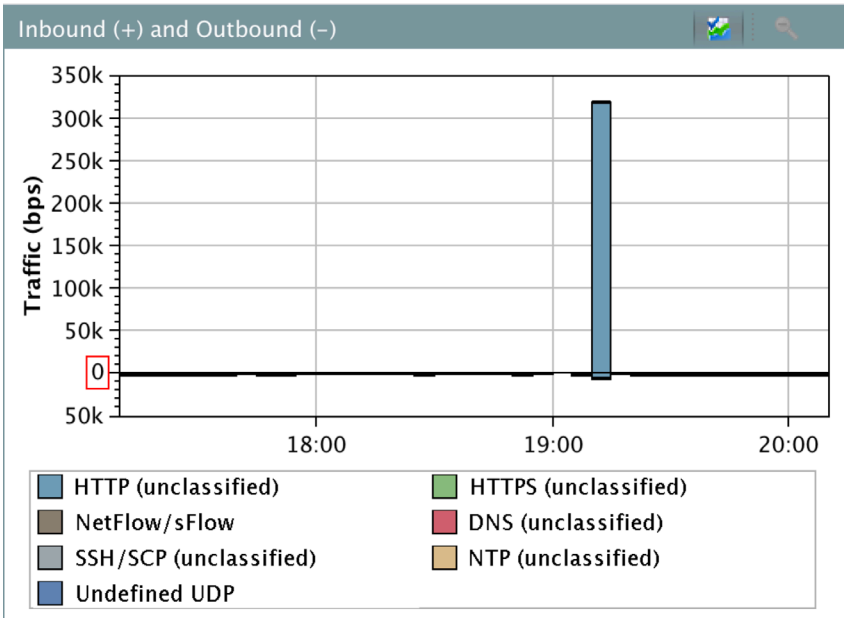
クラウド エージェントで、AWS から NetFlow を受信していることを確認します。

例：

```
sudo yum install curl
```

次の curl コマンドを実行して、この 11MB のファイルをダウンロード（/dev/null へ）します。

```
curl http://speedtest.wdc01.softlayer.com/downloads/test10.zip
>/dev/null
```



© 2016 Cisco Systems, Inc. All Rights Reserved

Top Conversations - 2 records

	% of Bytes	Host	Host R...	Peer	Port	Byt...
1	100%	10.151.1.11	Client	speedtest.wdc01.softlayer.com (208.43.102.250)	80/tcp (http)	11.4M
	100%	Total (1)	Client	Total (1)	Total (1)	11.4M

トラブルシューティングのためのエージェント GUID の確認

サービス ノードにインストールされているモニタによる GUID の識別を確認するには、次の手順を実行します。

1. 目的のノードに SSH でログインします。
2. 次の例のように、`/var/local/swcagent/agentguid` の内容を調べます。

```
-bash-4.1$ echo $(cat /var/local/swcagent/agentguid)
{15FB0832-5112-435E-B87A-5F7E030DA371}
-bash-4.1$
```

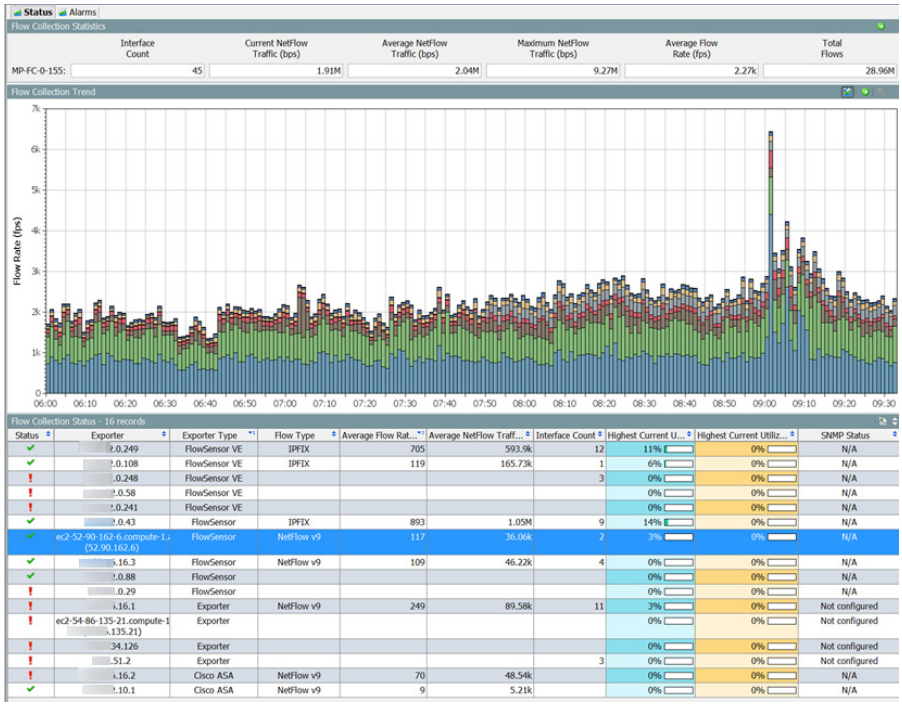
注：大規模な導入の場合は、必要に応じて、これをモニタリング メカニズムに追加する必要があります。たとえば、Puppet を使用する場合は、顧客ファクトを Facter に追加します。

SMC クライアント インターフェイスでのフローの確認

FlowCollector によってフローが受信されていることを確認するには、次の手順を実行します。

1. SMC クライアント インターフェイスにログインします。
2. [企業（Enterprise）] ツリーで、Cloud License フロー用に指定した FlowCollector を選択し、[ステータス（Status）] を選択します。

© 2016 Cisco Systems, Inc. All Rights Reserved



© 2016 Cisco Systems, Inc. All Rights Reserved

付録

コンセントレータ AMI アップグレード プロセス

ここでは、古いコンセントレータから新しいコンセントレータへとエージェント通信を維持しながら新しい AMI を使用してコンセントレータをアップグレードする方法を簡単に説明します。現在、コンセントレータの各リリース用に新しい AMI が作成されています。このプロセスでは、古いコンセントレータから引き継いで維持する必要があるものについて詳しく説明します。また、このプロセスは、エージェントにコンセントレータを指し示すために環境で Route53 DNS または Elastic IP が使用されていることを前提としています。これらがどちらもない場合、このプロセスは機能せず、アップグレードでは、新しいコンセントレータから生成される、サムプリントが付加されたエージェントをプッシュする必要があります。

前提条件

以下の説明は、次のことを前提としています。

- 既存のコンセントレータが、承認された AMI を使用して Amazon AWS にインストールされている。
- 既存のコンセントレータ上で、提供された .p12 ファイルまたはそれ自体によって作成された .p12 ファイルによって gen-keypair.sh スクリプトが実行されており、その .p12 が `/ opt / swcconc / ssl_keys` に存在する。
- エージェントが、Route53 DNS によって解決可能なホスト名または Elastic IP から割り当てられた IP アドレスにより、前の前提で述べた .p12 のサムプリントを使用して、既存のコンセントレータ上の stamp-agent.sh から生成されている。
- ライセンスが、`--lancope-fetch-license` ダウンロード オプションを使用して既存のコンセントレータに追加されているか、コンセントレータに直接アップロードされ、`--lancope-load-license` オプションを使用して追加されている。
- コンセントレータが、UDP フローをコレクタに転送するように設定されている。
- エージェントが、コンセントレータにプルされた、サムプリントが付加された .rpm を実行しており、データをレポートしている。

情報の例

手順例で使用する情報を、次の表に示します。顧客の環境の値を、手順例に示されているディレクティブおよびコマンドで置き換えて使用してください。

名前	値の例	説明
既存のコンセントレータ	該当なし	現在、エージェントのトラフィックを受信してフローをコレクタに転送しているコンセントレータ。これは、廃棄しようとしているコンセント

© 2016 Cisco Systems, Inc. All Rights Reserved

名前	値の例	説明
		レータです。
新しいコンセントレータ	該当なし	既存のコンセントレータと交換する、更新されたコードを含むコンセントレータ。これは、既存のコンセントレータと同じエージェント トラフィックを受け入れ、フローを同じコレクタに転送するように設定されます。
既存のコンセントレータの *AWS インスタンス* ID	i-de4c0d58	既存のコンセントレータの Amazon インスタンス ID。
新しいコンセントレータの *AWS インスタンス* ID	i-81470507	新しいコンセントレータの Amazon インスタンス ID。
新しいコンセントレータのパブリック DNS	ec2-54-172-250-45.compute-1.amazonaws.com	新しいコンセントレータのパブリック DNS。
割り当て済みの Elastic IP	`52.206.4.227`	この例で既存のコンセントレータによって使用されており、新しいコンセントレータに割り当てなおす Amazon Elastic IP アドレス。
FlowCollector の IP	52.200.4.202	この例の FlowCollector の IP アドレス。両方のコンセントレータが、フローを転送するために解決できる必要があります。
FlowCollector のポート	`4739`	この例で FlowCollector がフロー トラフィックをリッスンするポート。
AWS 秘密キー	example.pem	すべてのインスタンス化された Amazon インスタンスにアクセスするために使用されるキー。両方のコンセントレータに **admin** ユーザとして SSH でログインし、ファイルをセキュア コピーするために使用されます。
既存のコンセントレータの *デバイス* ID	CLVE-EEC19E60-CADE-4BC5-AF6D-0AB936671551	既存のコンセントレータのデバイス ID として Flexnet Operations によって使用されるシリアル番号。
新しいコンセントレータの *デバイス* ID	`CLVE-EEC19E60-CADE-4BC5-AF6D-0A685706A535`	新しいコンセントレータのデバイス ID として Flexnet Operations によって使用されるシリアル番号。

AMI のアップグレード手順

以下の手順では、エージェントがコンセントレータに関する要求を解決する方法の例を示すために Elastic IP を使用します。割り当て済みの Elastic IP が既存のコンセントレータの AWS インスタンス ID に関連付けられており、その Elastic IP が gen- keypair.sh スクリプトに渡されるホスト名（-d オプション）として使用されています。AWS の Elastic IP の詳細については、こちらのドキュメントを参照してください。このガイドでは、AWS の Elastic IP の割り当てについては説明しません。

© 2016 Cisco Systems, Inc. All Rights Reserved

コンセントレータの停止と必要なファイルのバックアップ

1. 既存のコンセントレータにログインした後、`--describe-server` コマンドを実行することにより、サムプリントが付加されたエージェントがレポートしており、既存のコンセントレータのデバイス ID を取得していることを確認できます。

```
-bash-4.1$ sudo /opt/swcconc/bin/swcconc --describe-server
20:33:36.776 ZSERVER [main] INFO com.ziften.server.cli.Cli - Cli
started.Options: [--describe-server]
Showing server info
{
  "serverHostId": "CLVE-EEC19E60-CADE-4BC5-AF6D-0AB936671551",
  "licenses": [
    {
      "license": {
        "hostId": "CLVE-EEC19E60-CADE-4BC5-AF6D-0AB936671551",
        "feature": "ZFLOW_IPFIX_CONCENTRATOR",
        "maxAllowedAgents": 50,
        "licenseSource": "flexnetTrustedStorageLicenseSource"
      },
      "utilization": {
        "limitExceeded": false,
        "maxAllowedAgents": 50,
        "connectedAgentsNumber": 26,
        "overLimitAgentCount": 0,
        "connectedAgentsGuids": [
          "{18452185-4AB7-4418-BC43-E3C3B8FEE6F2}"
          "{0242282F-3134-11E5-8796-0021CCCD0CB6}"
            "{88524BF3-A5A9-11E5-825F-78DD08C2B587}"
            "{028434DE-3243-11E5-9390-60D819B073C2}"
            "{02F093F4-352A-11E5-B49F-5C514F796ACA}"
            "{9CB50BFA-A9AE-11E5-8260-3402867A79C4}"
            "{03497CA3-3460-11E5-B42F-28D24477FE3A}"
            "{93A58D60-3244-11E5-8363-28D2443C25EF}"
            "{2995AA3A-3462-11E5-A758-E4D53DD6C8F3}"
            "{D5B3AFB2-A03A-11E5-825F-DC53600B1CCD}"
            "{040735CD-345B-11E5-8537-28D2447D3918}"
            "{061DDDE4-345C-11E5-A2B1-3C970E8965CB}"
            "{26610E7C-A8B6-11E5-825F-C417FEF4E667}"
            "{087DD36E-324D-11E5-828D-CC3D8252545D}"
            "{08C07C19-3460-11E5-B620-F4B7E2E88FBF}"

            "{2F47A685-1177-11E6-9D74-7CE9D3DFC979}"
            "{900CBF24-A886-11E5-8260-28B2BD76AA29}"
            "{A6457C8A-5C97-11E5-8266-3CA82ADE3958}"
            "{0AB466C7-3243-11E5-8743-F4B7E2E669A2}"
            "{EE273CAC-0562-11E6-8264-A434D9EBE0B9}"
            "{131D114B-3242-11E5-A3C1-00247E0DD5C3}"
            "{0D3852FC-944D-11E5-8260-40F02F040877}"
            "{0DC47012-3273-11E5-A1D2-7CE9D3E30548}"
            "{AE6E61BB-345E-11E5-8247-28D24402522F}"
            "{115BF95F-32EA-11E5-84A4-0021CCCD0C08}"
            "{0C4591F7-3472-11E5-A1F5-2016D8D864E4}"
        ]
      }
    }
  ]
}
-bash-4.1$
```


© 2016 Cisco Systems, Inc. All Rights Reserved

2. コンセントレータ サービスを停止します。

   - エージェントは、メッセージを伝えることができなくなります。デフォルトでは、エージェントは 7 日間または 125,000 のメッセージのバックログを保持します。各メッセージは、複数のフローを含むことができ、最大サイズは 1472 バイトです。
   - エージェントは、コンセントレータへの HTTPS 接続に失敗すると、デフォルトでは 5 分間待機して再試行します。
   - 接続が新しいコンセントレータに復元される前にメッセージのいずれかのしきい値を超えると、エージェントは、メッセージ キュー内の最も古いメッセージを破棄します。

```
-bash-4.1$ sudo service swcconc stop

Stopping  [done]
       -bash-4.1$
```

   コンセントレータの `/opt/swcconc/swcconc.settings` ファイルでは、FlowCollector で最初に指し示された時点で 2 つの設定が操作されます。これらの設定は新しいコンセントレータに転送する必要があります。これにより、新しいコンセントレータでも、フローが同じコレクタに転送されます。これらの設定は実際には任意の方法でアーカイブできますが、この例では、それらの設定をファイルから grep 検索し、それらを後で使用できるように .txt ファイルに書き込みます。

3. **どのような方式を使用する場合でも、それらが新しいコンセントレータで認識され、複製される必要があります**。ここで、.txt ファイルの内容に対して cat コマンドを使用して操作を確認します。

```
-bash-4.1$ sudo grep 'IPFIX_COLLECTOR' /opt/swcconc/swcconc.settings >
~/flowCollectorSettings.txt

-bash-4.1$ cat ~/flowCollectorSettings.txt
IPFIX_COLLECTOR_HOST=52.200.4.202
IPFIX_COLLECTOR_PORT=4739
       -bash-4.1$
```

4. **ssl_keys** ディレクトリと **agent** ディレクトリの .p12 および .txt を admin のホーム ディレクトリにコピーします。
   .p12 は、コンセントレータによってエージェント認証のために使用されます。この .p12 は、新しいコンセントレータによって、既存のエージェントも認証できる Java キーストアを生成するために使用されます。agent ディレクトリには、このコンセントレータの、サムプリントが付加された .rpm ファイルと、関連付けられた .conf ファイル（エージェント 1.0.0.490 以降）が含まれています。これらは、将来必要になる場合に備えてアーカイブされます。

© 2016 Cisco Systems, Inc. All Rights Reserved

5. 完了したら、admin のホーム ディレクトリの内容を確認します。

```
-bash-4.1$ sudo cp -v /opt/swcconc/ssl_keys/52_206_4_227.p12
/opt/swcconc/ssl_keys/52_206_4_227.txt ~
`/opt/swcconc/ssl_keys/52_206_4_227.p12' ->
`/home/admin/52_206_4_227.p12'
`/opt/swcconc/ssl_keys/52_206_4_227.txt' ->
`/home/admin/52_206_4_227.txt'
-bash-4.1$ sudo cp -v /opt/swcconc/agent/* ~
`/opt/swcconc/agent/1.0.0.490_52.206.4.227_swcagent.conf' ->
`/home/admin/1.0.0.490_52.206.4.227_swcagent.conf'
`/opt/swcconc/agent/swcagent-1.0.0.490_52.206.4.227.rpm' ->
`/home/admin/swcagent-1.0.0.490_52.206.4.227.rpm'
-bash-4.1$ ll ~
total 1620
-rw-r--r--.1 root  root     4450 Jul 13 22:11
1.0.0.490_52.206.4.227_swcagent.conf
-rw-r--r--.1 root  root     2592 Jul 13 22:10 52_206_4_227.p12
-rw-r--r--.1 root  root      305 Jul 13 22:10 52_206_4_227.txt
-rw-rw-r--.1 admin admin      82 Jul 13 20:47 flowCollectorSettings.txt
-rw-r--r--.1 root  root  1633741 Jul 13 22:11 swcagent-
1.0.0.490_52.206.4.227.rpm
-bash-4.1$
```

6. 新しいコンセントレータに転送するために必要なファイルをアーカイブします。この例では、tar コマンドを使用します。また、FlowCollector 設定を容易に移植できるように、手順 3 で作成した .txt ファイルをアーカイブします。生成される tar ファイルは admin のホーム ディレクトリに保存されます。

```
-bash-4.1$ tar -czvf ~/i-de4c0d58_archive.tar.gz
1.0.0.490_52.206.4.227_swcagent.conf 52_206_4_227.* swcagent-
1.0.0.490_52.206.4.227.rpm flowCollectorSettings.txt
1.0.0.490_52.206.4.227_swcagent.conf
52_206_4_227.p12

52_206_4_227.txt
swcagent-1.0.0.490_52.206.4.227.rpm
flowCollectorSettings.txt
-bash-4.1$
```

7. tar アーカイブ ファイルをローカル システムにダウンロードします。

```
joes-mbp:~ Joe$ scp -i ~/.ssh/example.pem admin@52.206.4.227:~/i-
de4c0d58_archive.tar.gz ~/Desktop
i-de4c0d58_archive.tar.gz                 100% 1575KB   1.5MB/s   00:00
joes-mbp:~ Joe$
```


© 2016 Cisco Systems, Inc. All Rights Reserved

AWS での新しいコンセントレータ インスタンスの作成

AWS で新しいコンセントレータ インスタンスを作成するには、次の手順を実行します。

1. AWS のアカウントで、Updated Concentrator AMI を使用して新しいインスタンスを生成します。Stealthwatch Cloud License AMI からインスタンスを作成する場合は、既存のドキュメンテーションに示されている手順に従ってください。
2. 生成される新しいコンセントレータのインスタンス ID とパブリック DNS を書き留めておきます。
   - この例では、生成される新しいコンセントレータの AWS インスタンス ID は **i-81470507** です。
   - この時点では、新しいインスタンスで gen-keypair.sh または stamp-agent.sh を使用しないでください。
   - この時点では、コレクタを指し示すように設定しないでください。

インスタンスを単にインスタンス化します。この例では、インスタンスには、既存のコンセントレータと同じ秘密キーの「**example.pem**」を使用してアクセスできます。

新しいコンセントレータの設定

AWS で新しいコンセントレータ インスタンスを設定するには、次の手順を実行します。

1. tar ファイルをコピーしたローカル システムで、tar ファイルを新しいコンセントレータにアップロードします。**Elastic IP アドレスはまだ新しいコンセントレータに関連付けられていないため、新しいコンセントレータに到達するにはパブリック DNS を使用します。**

```
joes-mbp:~ Joe$ scp -i ~/.ssh/example.pem ~/Desktop/i-
de4c0d58_archive.tar.gz admin@ec2-54-172-250-45.compute-
1.amazonaws.com:~
i-de4c0d58_archive.tar.gz                         100% 1575KB   1.5MB/s
00:00
joes-mbp:~ Joe$
```

2. パブリック DNS と SSH 秘密キー（example.pem）を使用して新しいコンセントレータに admin ユーザとして SSH でログインします。

3. 新しいコンセントレータにアーカイブがコピーされていることを確認します。

```
-bash-4.1$ ll
total 1576
-rw-r--r--.1 admin admin 1613043 Jul 13 22:06 i-de4c0d58_archive.tar.gz
-bash-4.1$
```

© 2016 Cisco Systems, Inc. All Rights Reserved

4. アーカイブを圧縮解除します。出力を確認します。flowCollectorSettings.txt が含まれている場合は、次の手順で使用するために、その内容に対して cat コマンドを使用します。

```
-bash-4.1$ tar -xvf i-de4c0d58_archive.tar.gz
1.0.0.490_52.206.4.227_swcagent.conf
52_206_4_227.p12
52_206_4_227.txt
swcagent-1.0.0.490_52.206.4.227.rpm
flowCollectorSettings.txt
-bash-4.1$ cat flowCollectorSettings.txt
IPFIX_COLLECTOR_HOST=52.200.4.202
IPFIX_COLLECTOR_PORT=4739
-bash-4.1$
```

5. **sudo** プレフィックスを使用して Vim などのテキスト エディタで `/opt/swcconc/swcconc.settings` ファイルを開き、`IPFIX_COLLECTOR_HOST` 設定と `IPFIX_COLLECTOR_PORT` 設定を編集して、使用する FlowCollector の設定にします。

   a. **設定がアンコメントされている（行頭の # が削除されている）ことを確認します。**

   b. 編集後にファイルを保存します。設定ファイルの編集を有効にするには swcconc サービスを再起動する必要がありますが、次の手順で gen-keypair.sh スクリプトによって再起動されることで、これが実行されます。

6. すでに admin のホーム ディレクトリに保存されている、アーカイブされた .p12 と、既存のコンセントレータの ssl_keys ディレクトリからアーカイブされた .txt ファイルにある、それに関連付けられたパスワードを使用して、gen-keypair.sh スクリプトを実行します。**-d ホスト名オプションと同じ Elastic IP アドレスを使用します**。-h オプションを最初に実行してヘルプ メニューと使用方法を表示することができます。

```
-bash-4.1$ grep 'Passphrase' ~/52_206_4_227.txt
    Passphrase:    H16pwmMsLoQvAcLM


-bash-4.1$ sudo /opt/swcconc/bin/gen-keypair.sh -d 52.206.4.227 -k
/home/admin/52_206_4_227.p12 -p 'H16pwmMsLoQvAcLM' -I
Converting supplied keystore...
Entry for alias 52.206.4.227 successfully imported.
Import command completed:  1 entries successfully imported, 0 entries
failed or cancelled
`/home/admin/52_206_4_227.p12' ->
`/opt/swcconc/ssl_keys/52_206_4_227.p12'
`/home/admin/52_206_4_227.jks' ->
`/opt/swcconc/ssl_keys/52_206_4_227.jks'

`/opt/swcconc/ssl_keys/52_206_4_227.jks' ->
`/opt/swcconc/jetty/etc/keys/52_206_4_227.jks'

    Created new keypairs
    Hostname:      52.206.4.227
    JKS keyfile:   52_206_4_227.jks
    P12 keyfile:   52_206_4_227.p12
```


© 2016 Cisco Systems, Inc. All Rights Reserved

```
    Expires on :   Tue Apr 09 03:51:30 UTC 2019
    Passphrase:    H16pwmMsLoQvAcLM
    Thumbprint:    dc936dbb9d7c5b8616f0ba78b7955c2c25d4cf99

    SHA1 (P12):    4bffe4ca11e5bfc49a022f80e795777f5e1c22ec
    SHA1 (JKS):    07df4dfb241533b0c038da17390f427c6ba65125

Changing SSL keypair served...
Setting SSL keypair to /opt/swcconc/ssl_keys/52_206_4_227.jks ...
Changing settings in Jetty's SSL config file
Restarting service swcconc

      Stopping    [done]

Starting  [done]
The Jetty KeyStore has been installed and Jetty has been restarted
-bash-4.1$
```

7. Jetty の初期化が完了するまで 2 ～ 3 分待ちます。その後、`--describe-server` コマンドを実行して新しいコンセントレータのデバイス ID を取得します。

```
-bash-4.1$ sudo /opt/swcconc/bin/swcconc --describe-server
22:54:08.581 ZSERVER [main] INFO com.ziften.server.cli.Cli - Cli
started.Options: [--describe-server]
Showing server info
{
  "serverHostId": "CLVE-EEC19E60-CADE-4BC5-AF6D-0A685706A535",
  "licenses": [
    {
      "license": {
        "hostId": "CLVE-EEC19E60-CADE-4BC5-AF6D-0A685706A535",
        "feature": "ZFLOW_IPFIX_CONCENTRATOR",
        "maxAllowedAgents": 0,
        "licenseSource": "noLicenseAvailableSource"
      },
      "utilization": {
        "limitExceeded": true,
        "maxAllowedAgents": 0,
        "connectedAgentsNumber": 0,
        "overLimitAgentCount": 0,
        "connectedAgentsGuids": []
      }
    }
  ]
}
-bash-4.1$
```

8. 次のセクションのために serverHostId（デバイス ID）を書き留めておきます。

© 2016 Cisco Systems, Inc. All Rights Reserved

Flexnet Operations での新しいコンセントレータの登録と古いコンセントレータの機能の無効化

Flexnet で新しいコンセントレータを登録するには、次の手順を実行します。

1. Flexnet Operations のコンソールにログインし、[ライセンス(Licensing)] → [アプライアンスの登録(Register Appliances)] の順に選択して、新しいデバイス ID を登録します。
2. 既存のコンセントレータのシリアル番号をクリックします。機能の一覧が表示されます。
3. [機能の削除(Remove Features)] を選択して、[削除する数(Quantity to Remove)] ボックスに削除する機能の数を入力し、[機能の削除(Remove Features)] ボタンをクリックして削除します。
4. 既存のコンセントレータの機能の画面に戻るので、[ライセンスのダウンロード(Download License)] を選択します。これにより、それらのライセンス適用済みの機能を追加のライセンス適用のために使用できるようになります。
5. ここで、[マイ アプライアンス(My Appliances)] に戻り、新しいコンセントレータのデバイス ID を選択します。
6. [機能の追加(Add Features)] リンクをクリックして、[追加する数(Qty to Add)] ボックスに追加する機能の数を入力し、[機能の追加(Add Features)] をクリックして新しいコンセントレータの機能にライセンスを適用します。
7. ライセンスは、ライセンスのページからダウンロードされるか、コンセントレータによってプルされるまで、[生成されていない(not generated)] と表示されます。

新しいライセンスと新しいコンセントレータの関連付け

新しいライセンスを新しいコンセントレータと関連付けるには、次の手順を実行します。

1. 既存のドキュメンテーションに示されている手順に従って、手動でダウンロードしたライセンスを新しいコンセントレータにアップロードするか、コンセントレータにライセンスを Flexnet Operations から直接プルさせます。

   - **必ず、ライセンスの追加後に新しいコンセントレータで swcconc サービスを再起動(`sudo service swcconc restart`)してください。**
   - この例では、`--lancope-fetch-license` 方式を使用して新しいコンセントレータにライセンスをプルさせます。
   - その前に、ライセンスの取得前にライセンスが存在しないことを示すための `-describe-server` コマンドも含まれています。

```
-bash-4.1$ sudo /opt/swcconc/bin/swcconc --describe-server
22:01:06.767 ZSERVER [main] INFO com.ziften.server.cli.Cli - Cli
started.Options: [--describe-server]
Showing server info
{
  "serverHostId": "CLVE-EEC19E60-CADE-4BC5-AF6D-0A685706A535",
```


© 2016 Cisco Systems, Inc. All Rights Reserved

```
  "licenses": [
    {
      "license": {
        "hostId": "CLVE-EEC19E60-CADE-4BC5-AF6D-0A685706A535",
        "feature": "ZFLOW_IPFIX_CONCENTRATOR",
        "maxAllowedAgents": 0,
        "licenseSource": "noLicenseAvailableSource"
      },
      "utilization": {
        "limitExceeded": true,
        "maxAllowedAgents": 0,
        "connectedAgentsNumber": 0,
        "overLimitAgentCount": 0,
        "connectedAgentsGuids": []
      }
    }
  ]
}
-bash-4.1$ sudo /opt/swcconc/bin/swcconc --lancope-fetch-license
22:01:52.348 ZSERVER [main] INFO com.ziften.server.cli.Cli - Cli
started.Options: [--lancope-fetch-license]
Fetching Lancope license from licensing server
{
  "licenseServerUrl":
"https://lancope.flexnetoperations.com/control/lncp/deviceservices",
  "applianceHostId": "CLVE-EEC19E60-CADE-4BC5-AF6D-0A685706A535",
  "featureCount": 1,
  "features": [
    {
      "name": "CloudLicenseAgents",
      "agentCount": 50,
      "issued": "2016/07/15 12:00:00+0000",
      "startDate": "2015-11-03 12:00:00+0000",
      "expiration": "2016-11-03 11:59:59+0000"
    }
  ]
}
-bash-4.1$
```

2. Flexnet Operations のサイトに戻り、新しいコンセントレータのデバイス ID に用にライセンスが生成されていることを確認できます。

3. もう一度 `--describe-server` によってライセンスの取得を確認します。

```
-bash-4.1$ sudo /opt/swcconc/bin/swcconc --describe-server
22:04:34.595 ZSERVER [main] INFO com.ziften.server.cli.Cli - Cli
started.Options: [--describe-server]
Showing server info
{
  "serverHostId": "CLVE-EEC19E60-CADE-4BC5-AF6D-0A685706A535",
  "licenses": [
    {
      "license": {

        "hostId": "CLVE-EEC19E60-CADE-4BC5-AF6D-0A685706A535",
        "feature": "ZFLOW_IPFIX_CONCENTRATOR",
```

© 2016 Cisco Systems, Inc. All Rights Reserved

```
            "maxAllowedAgents": 50,
            "licenseSource": "flexnetTrustedStorageLicenseSource"
          },
          "utilization": {
            "limitExceeded": true,
            "maxAllowedAgents": 50,
            "connectedAgentsNumber": 0,
            "overLimitAgentCount": 0,
            "connectedAgentsGuids": []
          }
        }
      ]
    }
    -bash-4.1$
```

4. ライセンスを有効にするために新しいコンセントレータを再起動します。

```
-bash-4.1$ sudo service swcconc restart

Stopping  [done]

Starting  [done]
-bash-4.1$
```

使用中の Elastic IP アドレスの再関連付け

この時点で、新しいコンセントレータは、同じ FlowCollector を指し示すように `swcconc.settings` で設定されており、既存のコンセントレータと同じ Java キーストアを提供します。残っている作業は、使用中の Elastic IP アドレスを新しいコンセントレータの AWS インスタンス ID に関連付けなおすことだけです。

Elastic IP アドレスを新しいコンセントレータの AWS インスタンス ID に関連付けなおすには、次の手順を実行します。

1. AWS の管理コンソールに戻り、[サービス（Services）] → [EC2] → [Elastic IP（Elastic IPs）] の順に選択します。
2. IP の一覧の上にある検索バーで、既存のコンセントレータに関連付けられている IP を検索します。IP の左にあるチェックボックスをオンにして IP を強調表示します。
3. 検索バーの上にある [アクション（Actions）] ボタンをクリックし、[アドレスの関連付け（Associate Address）] を選択します。
4. 新しいコンセントレータの AWS インスタンス ID（新しく作成されたコンセントレータ インスタンスから取得）を入力します。

   - **Elastic IP を新しいインスタンスに関連付けることを示すために [再関連付け（Reassociation）] ボックスをオンにします。**
   - [関連付け（Associate）] ボタンをクリックします。

5. IP アドレスが、Elastic IP の一覧にある新しいコンセントレータ のAWS インスタンス ID と関連付けられます。

© 2016 Cisco Systems, Inc. All Rights Reserved

エージェントの通信の確認

前述のように、エージェントは、通信が失われると、コンセントレータとの接続を 5 分ごとに試行します。そのため、Elastic IP アドレスの再関連付けとエージェントのバックオフ期間を合わせると、エージェントの通信が再開するまでに最大 10 分かかる場合があります。

> **注**：パブリック DNS を使用して新しいコンセントレータに SSH でログインしていた場合は、その接続のパイプが Elastic IP アドレスの再割り当てによって壊れます。新しいコンセントレータに SSH でログインしなおす必要がありますが、今度はそれに Elastic IP アドレスを使用できます。

エージェントの通信を確認するには、次の手順を実行します。

1. 新しく関連付けなおした Elastic IP アドレスを使用して新しいコンセントレータに SSH でログインします。

   > **注：スプラッシュ画面に新しいコンセントレータのデバイス ID が表示されることで、再関連付けを確認できます。**

   ```
   joes-mbp:Downloads Joe$ ssh -i ~/.ssh/example.pem admin@52.206.4.227
   Linux 2.6.32-573.26.1.el6.x86_64 #1 SMP Wed May 4 00:57:44 UTC 2016
   x86_64
   ip-10-0-24-247

   Welcome to the StealthWatch Cloud License Concentrator
   Version 1.0.0 - Build 560
   Serial CLVE-EEC19E60-CADE-4BC5-AF6D-0A685706A535

   Agents Connected: 8
   Agents Licensed:  50
   -bash-4.1$
   ```

2. この出力例では、8 つのエージェントがすでに接続を再確立し、新しいコンセントレータにレポートしていることを確認できます。詳細を調べるには、--describe-server コマンドを実行します。

   ```
   -bash-4.1$ sudo /opt/swcconc/bin/swcconc --describe-server
   22:27:43.701 ZSERVER [main] INFO com.ziften.server.cli.Cli - Cli
   started.Options: [--describe-server]
   Showing server info
   {
     "serverHostId": "CLVE-EEC19E60-CADE-4BC5-AF6D-0A685706A535",
     "licenses": [
       {
         "license": {
           "hostId": "CLVE-EEC19E60-CADE-4BC5-AF6D-0A685706A535",
           "feature": "ZFLOW_IPFIX_CONCENTRATOR",
           "maxAllowedAgents": 50,
           "licenseSource": "flexnetTrustedStorageLicenseSource"
         },
   ```

© 2016 Cisco Systems, Inc. All Rights Reserved

```
        "license": {
          "hostId": "CLVE-EEC19E60-CADE-4BC5-AF6D-0A685706A535",
          "feature": "ZFLOW_IPFIX_CONCENTRATOR",
          "maxAllowedAgents": 50,
          "licenseSource": "flexnetTrustedStorageLicenseSource"
        },
        "utilization": {
          "limitExceeded": false,
          "maxAllowedAgents": 50,
          "connectedAgentsNumber": 8,
          "overLimitAgentCount": 0,
          "connectedAgentsGuids": [
              "{EE273CAC-0562-11E6-8264-A434D9EBE0B9}"
              "{08C07C19-3460-11E5-B620-F4B7E2E88FBF}"
              "{115BF95F-32EA-11E5-84A4-0021CCCD0C08}"
              "{0D3852FC-944D-11E5-8260-40F02F040877}"
              "{88524BF3-A5A9-11E5-825F-78DD08C2B587}"
              "{9CB50BFA-A9AE-11E5-8260-3402867A79C4}"
              "{2F47A685-1177-11E6-9D74-7CE9D3DFC979}"
              "{900CBF24-A886-11E5-8260-28B2BD76AA29}"
          ]
        }
      }
    ]
  }
  -bash-4.1$
```


3. FlowCollector を調べて、新しいコンセントレータからフローが転送されていることを確認します。

© 2016 Cisco Systems, Inc. All Rights Reserved