外部検索

(Stealthwatch System v6.9.0 用)

著作権および商標

NOTICE

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェアライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

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。

ハードコピーおよびソフトコピーの複製は公式版とみなされません。最新版はオンライン版を参照してください。

シスコは世界各国200箇所にオフィスを開設しています。各オフィスの住所、電話番号、FAX番号は当社のWebサイト(www.cisco.com/go/offices) をご覧ください。

目次

目次

1

外部参照の管理

外部参照機能を使用すると、Web アプリケーション(または内部アセット データベース) を起動し、IP アドレスに関する追加情報を表示することができます。Stealthwatch 管理コンソール(SMC) クライアント インターフェイスまたは SMC Web App インターフェイスから、この Web アプリケーションまたはデータベースを直接起動できます。

また、外部参照機能を使用してショートカットを作成すると、SMC クライアント インターフェイスから SMC Web App インターフェイスにすばやくジャンプできます。

Stealthwatch システムには、外部参照機能とともに使用できる以下のデフォルト Web アプリケーション(参照オプション) が含まれています。Stealthwatch システムにこれらを追加する必要はありません。

- Cisco SenderBase
- DShield
- Host Report

IP アドレスの追加情報を表示するために Stealthwatch システム管理者が追加できる Web アプリケーションには、たとえば以下のものがあります。

- BigFix
- CiscoWorks
- Cisco Identity Services Engine(ISE)
- Splunk
- Tripwire
- Ziften

重要: デフォルト以外の参照オプションを追加するには、SMC Web App インターフェイスで外部参照設定ツールを使用する必要があります。これを行う方法については、「外部参照の設定」を参照してください。

2

外部参照の設定

このページの用途

このページは、次のことを実行する場合に使用します。

- 追加した参照オプションを表示する。
- 参照オプションを追加、編集、削除、有効化または無効化にする。
- Web アプリケーションに送信する特定のパラメータを設定する。設定したパラメータは、参照の対象となる IP アドレスでそれが利用可能な場合にのみ、送信されます。

(注) Stealthwatch システムをバージョン 6.7 以降にアップグレードすると、それまで外部参照機能に使用していた webLinks.xml が新しい形式に移行され、古い webLinks.xml は使用されなくなります。

このページを見つける方法

ヘッダーから [グローバル設定 (Global Settings)] アイコンをクリックし、[外部参照の設定 (External Lookup Configuration)] をクリックします。

このページで実行すること

(注)

- 外部参照機能とともに使用できる Cisco SenderBase、DShield、および Host Report がデフォルトで組み込まれています。これらを Stealthwatch システムに追加する必要はありません。その他の Web アプリケーションを一緒に使用するには、それを Stealthwatch システムに追加する必要があります。
- v6.7 にアップグレードすると、以前に追加した外部参照オプションごとに、v.6.7 では 2 つずつ存在することになります。
- Stealthwatch システムでは、外部参照の設定を管理する目的で webLinks.xml ファイルを使用しなくなります。

参照オプションを表示します。

以下の該当する操作を実行します。

- Web アプリケーション(検索オプション) の一覧を表示し、必要な参照オプションが一覧に含まれているかどうか、また外部参照機能で使用するためにそれが有効になっているかどうかを確認します。
- 外部参照機能で使用できないように参照オプションを無効にする(ただし将来の使用のために設定は保持する) には、該当する行で [有効(Enabled)] をクリックします。ボタンが [無効(Disabled)] に切り替わります。将来、このベンダーを有効にするには、[無効(Disabled)] をクリックします。ボタンが [有効(Enabled)] に切り替わります。
- 参照オプションを編集または削除するには、[アクション(Actions)] 列で省略記号をクリックしてコンテキスト メニューを開き、該当するオプションを選択します。

参照オプションを追加し、パラメータを設定します。

[外部参照(External Lookup)] セクションの右上隅にある [外部参照の追加(Add External Lookup)] をクリックします。パラメータを設定する方法については、下記の情報を参照してください。

- Web アプリケーションの内部 IP アドレスに関する情報を表示するには、[内部 IP アドレスの参照を有効にする(Enable lookup of internal IP addresses)] チェックボックスをオンにします。
- 設定したパラメータは、参照の対象となる IP アドレスでそれが利用可能な場合にのみ、Web アプリケーションに表示されます。
- 参照オプションごとに、最大 20 個のクエリ パラメータをマップできます。
- 特定の Web アプリケーションを使って参照を行うときにパラメータを必須にするには、[必須(Required)] チェックボックスをオンにします。特定の Web アプリケーションに関して必須と指定したすべてのパラメータは、参照の対象となる IP アドレスで利用可能でなければなりません。該当する IP アドレスで使用不可な必須パラメータが 1 つ以上存在する場合、ポップアップ メニューでその参照オプションが無効になります。
- URL スクリプト ビルダー ファイルには、クエリ実行のために Web アプリケーションで必要な URL 形式としてクエリ パラメータを設定するスクリプトが含まれます。

  スクリプト ビルダ ファイルをアップロードしない場合は、以下に示すデフォルトの標準クエリ パラメータが Stealthwatch システムで使用されます。

  BaseURL?[ParameterName1]=[ParameterValue1]&[ParameterName2]=[ParameterValue2]&[ParameterName3]=[ParameterValue3](以降、追加する属性ごとに指定)

  クエリ パラメータが前述の標準クエリ パラメータと一致しない場合は、カスタマイズされたスクリプト ビルダ設定をアップロードする必要があります。カスタマイズされたスクリプト ビルダ ファイルを設定する際に参考となるいくつかのスクリプト例を以下に示します。

URL とスクリプトの例。

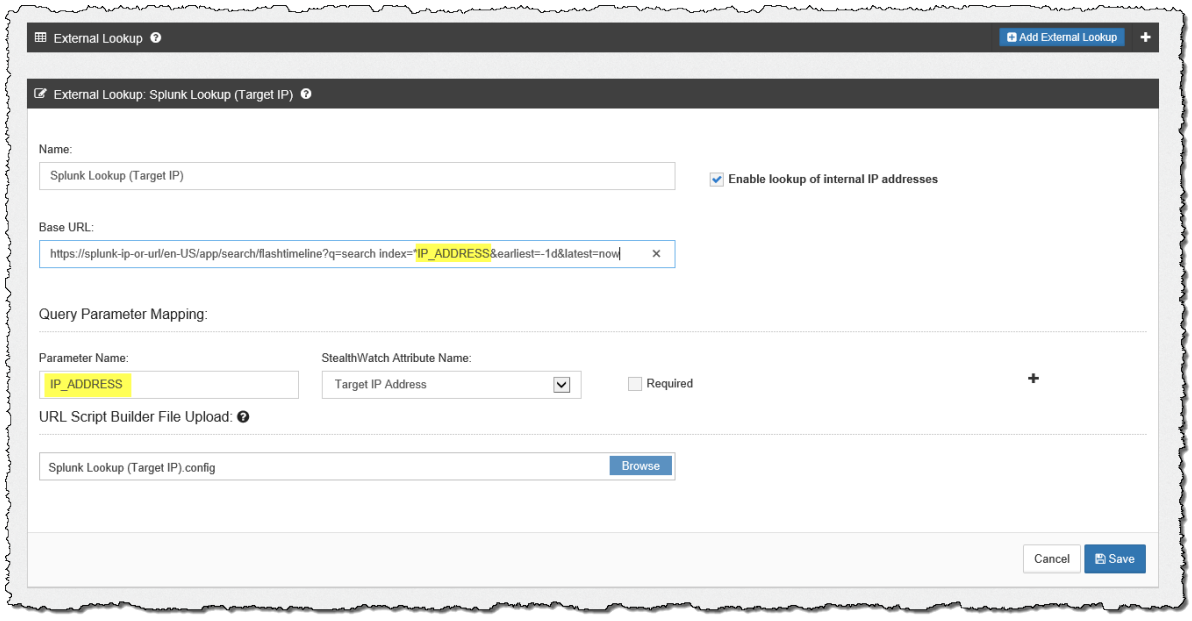
例 1

パラメータ名 のない値 を使 用 する Web アプリケーション(Splunk など) には、次 の URL とス クリプト の例 を使 用 します。

```
https://splunk-ip-or-url/en-US/app/search/flash-timeline
?q=search index=* 192.10.20.43 &earliest=-1d&lastest=now
```

```
import java.util.ArrayList;
import java.util.List;
import java.text.*;

def List<String> values = new ArrayList<String>();

vendorValues.each { valueOperand ->
    values.add(valueOperand.getFromValue().toString());
};

MessageFormat messageFormat = new MessageFormat(baseUrl);
return messageFormat.format(values.toArray());
```

この例 で示 した URL 形 式 としてクエリ パラメータを設 定 するスクリプト を作 成 するには、以 下 の画 像 で強 調 表 示 されている [パラメータ名 (Parameter Name)] フィールド エントリを 使 用 します。



（注）必要に応じて任意の数の属性を設定することができます。ただし、必ず同じ数のパラメータを設定してください。

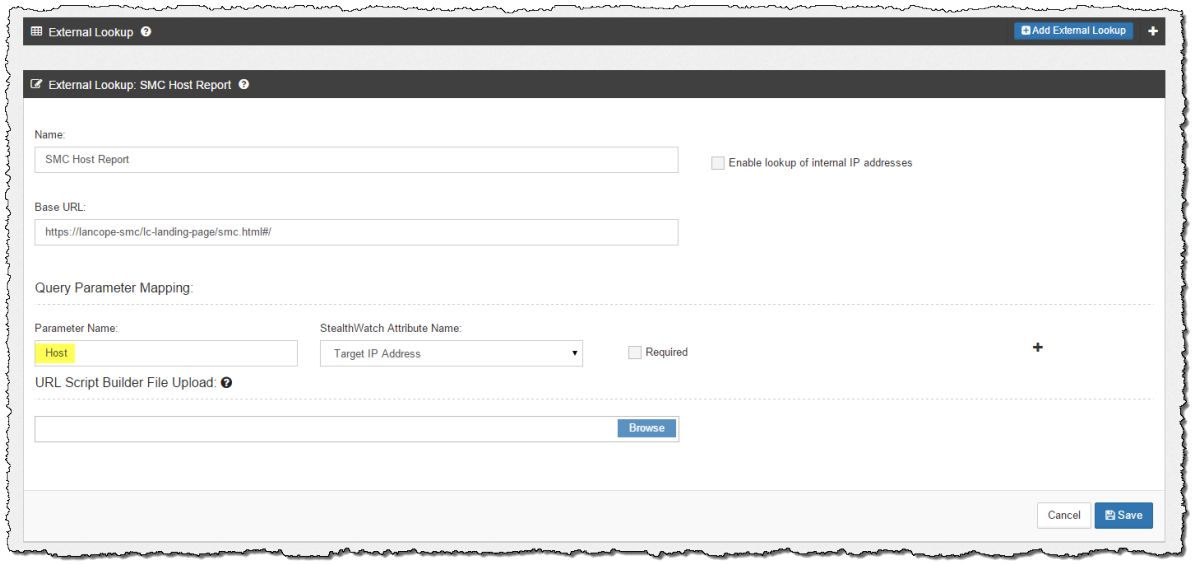
例 2

REST に似たパラメータを使用する Web アプリケーション(Stealthwatch Host Report など)には、次の URL とスクリプトの例を使用します。

```
https://lancope-smc/lc-landing-page/smc.html#/host
/172.21.114.17
```

```
def String query = "";

vendorValues.each { valueOperand ->


    query += valueOperand.getName() + "/";
    def String convertedStr = "";
    if (valueOperand.getFromValue() instanceof String || valueOperand.getFromValue() instanceof Integer) {
        convertedStr = valueOperand.getFromValue().toString();
    } else if (valueOperand.getFromValue() instanceof Date) {
        convertedStr = new SimpleDateFormat("yyyy-MM-dd'T'HH:mm:ss").format(valueOperand.getFromValue().time);
    }
    String.valueOf('java.lang.Integer');
    query += URLEncoder.encode(convertedStr,"UTF-8");
};

def char lastChar = baseUrl.charAt(baseUrl.length() - 1);
if (lastChar != '?' && lastChar != '/' && lastChar != '&') {
    baseUrl = baseUrl + "?";
};

query = baseUrl + query;
return query;
```

この例で示した URL 形式としてクエリパラメータを設定するスクリプトを作成するには、以下の画像で強調表示されている [パラメータ名 (Parameter Name)] フィールド エントリを使用します。



次に実行すること

ベンダーの Web アプリケーションまたは内部アセット データベースを起動して、IP アドレスに関する追加情報を表示するには、外部参照を実行します。これを行う方法については、「外部参照の実行」を参照してください。

3

外部参照の実行

この機能の用途

Web アプリケーションを照会して IP アドレスに関する追加情報を表示するには、この機能を使用します。

この機能の使用方法

1. SMC Web App インターフェイスまたは Stealthwatch 管理コンソール(SMC) クライアント インターフェイスのいずれかで、該当する IP アドレスを含むページを開きます。
2. 次のいずれかを実行します。
   - SMC Web アプリで以下のいずれかを実行して、コンテキスト メニューにアクセスします (SMC Web アプリのほとんどのページに存在します) 。
     - 該当する IP アドレスの横にある省略記号をクリックします。
     - [アクション(Actions)] 列の省略記号をクリックします。
     - グラフ内の点をクリックします。([ホスト レポート (Host Report)] ページの [ピア ホスト グループごとのトラフィック(Traffic by Peer Host Group)] グラフおよび [ホスト グループ レポート (Host Group Report)] ページの [トラフィックごとの上位ホスト グループ(Top Host Groups by Traffic)] グラフでは、ホスト グループ、列、または 2 つのホスト グループ間の線をクリックする必要があります。
   - SMC クライアント インターフェイスで、該当する IP アドレスを右クリックします(IP アドレスから外部参照オプションにアクセスできない場所もいくつかあります) 。
3. 表示されるポップアップ メニューで、[外部参照(External Lookup)] をクリックします。2 番目のポップアップ メニューが表示されます。
4. 手順 3 で表示された 2 番目のポップアップ メニューから目的の参照オプションをクリックします。選択した参照オプション用の Web アプリケーションが開き(Web アプリケーションにログインするよう求められる場合があります) 、参照対象の IP アドレスのクエリ結果が表示されます。

   特定の Web アプリケーションに関して必須と指定したすべてのパラメータは、参照の対象となる IP アドレスで利用可能でなければなりません。該当する IP アドレスで使用不可な必須パラメータが 1 つ以上存在する場合、ポップアップ メニューでその参照オプションが無効になります。詳細については、「外部参照の設定」を参照してください。

次に実行すること

ベンダーから返される情報に応じて、次の 1 つ以上を実行することができます。

- モニタリングまたは分離の目的で、このIPアドレスを特定のホスト グループに追加する。
- アナリストや調査担当者にさらに調べてもらうためにIPにフラグを立てる。
- IPアドレスに対する緩和処置を開始する。(これを実行できるようにStealthwatchシステムを設定しておく必要があります。)