

Cisco Secure Network Analytics

v7.4.2 外部ルックアップ機能の使用



目次

外部ロックアップの管理	3
外部ロックアップの設定	4
このページを使用する目的	4
このページを見つける方法	4
このページで実行できる作業	4
例 1	5
例 2	6
次に実行できる作業	7
外部ロックアップの実行	8
この機能を使用する目的	8
この機能の使用方法	8
次に実行できる作業	8
サポートへの問い合わせ	9
変更履歴	10

外部ルックアップの管理

外部ルックアップ機能を使用すると、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。この Web アプリケーションやデータベースは、デスクトップ クライアント または Web アプリケーション から直接起動できます。

また、外部ルックアップ機能を使用して、デスクトップ クライアント から Web アプリケーション に即座に移動できるショートカットを作成することも可能です。

Cisco Secure Network Analytics (旧 Stealthwatch) には、外部ルックアップ機能とともに使用できる次のデフォルト Web アプリケーション (ルックアップオプション) が組み込まれています。それらのアプリケーションをシステムに追加する必要はありません。

- DShield.org
- Host Report
- OpenDNS Investigate
- Talos Reputation

管理者 (Secure Network Analytics にユーザー名 *admin* で組み込まれているデフォルトの管理ユーザー) が IP アドレスに関する詳細情報を表示するために追加できる Web アプリケーションの例は以下のとおりです。

- BigFix
- CiscoWorks
- Cisco ISE (Identity Services Engine)
- スプラック
- トリップワイヤ
- ジフテン

デフォルト以外のルックアップオプションを追加するには、Web アプリケーション の外部ルックアップ設定ツールを使用する必要があります。詳細な操作手順については、「[外部ルックアップの設定](#)」を参照してください。

外部ルックアップの設定

このページを使用する目的

このページは、次のことを実行する場合に使用します。

- 追加したルックアップオプションを表示する。
- ルックアップオプションを追加、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。構成するパラメータは、ルックアップを実行する IP アドレスを利用できる場合にのみ送信されます。

このページを見つける方法

メインメニューで、[設定 (Configure)] > [グローバル外部ルックアップ (GLOBAL External Lookup)] の順に選択します。

このページで実行できる作業



- DShield.org、Host Report、OpenDNS Investigate、および Talos Reputation は、外部ルックアップ機能とともに使用できるようにデフォルトで組み込まれており、Secure Network Analytics に追加する必要はありません。他の Web アプリケーションを外部ルックアップ機能とともに使用するには、Secure Network Analytics にそのアプリケーションを追加する必要があります。

ルックアップオプションの表示

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、必要なルックアップオプションが一覧に含まれているかどうか、また外部ルックアップ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。
- 外部ルックアップ機能を使用できないルックアップオプションを無効にする (ただし、後の使用のためにその構成を保持する) には、該当する行で [有効 (Enable)] をクリックします。ボタンが [無効 (Disabled)] に切り替わります。今後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。
- ルックアップ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) アイコン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。

ルックアップオプションの追加およびパラメータの設定

[外部ルックアップ (External Lookup)] セクションの右上隅にある [外部ルックアップの追加 (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 アドレスのルックアップを有効にする (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、ルックアップの対象となる 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。
- 各ルックアップオプションに対して、最大 20 個のクエリパラメータをマッピングできます。
- 特定の Web アプリケーションを使用して、検索を実行する際にパラメータを使用したい場合は、[Required (必須)] チェックボックスを選択します。特定の Web アプリケーションに対して必要となるよう指定したパラメータはすべて、参照を実行する IP アドレスに対して利用できる必要があります。1 つ以上の必須パラメータが関連する IP アドレスに対して利用可能でない場合、そのルックアップオプションはポップアップメニューで有効化されません。
- URL スクリプトビルダファイルには、Web アプリケーションでクエリを実行するために必要な URL 形式にクエリパラメータを設定するスクリプトが含まれています。

i アップロードできるスクリプトは 100 KB 未満です。

- スクリプトビルダファイルをアップロードしない場合、Secure Network Analytics では以下に示すデフォルトの標準クエリパラメータが使用されます。

```
BaseURL?[ParameterName1]=[ParameterValue1]&[ParameterName2]=[ParameterValue2]&[ParameterName3]=[ParameterValue3 (追加する各属性に対して、このようなクエリパラメータを使用)
```

- 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 およびスクリプト例

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/flashtimeline  
?q=search index=* {0}&earliest=-1d&latest=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());
```

次のリンクをクリックし、前の画像に示したスクリプトの .txt ファイルをダウンロードします。

[Splunk スクリプト](#)

この例で前に示したように、クエリパラメータを URL 形式に設定するスクリプトを作成するには、次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 エントリーを使用します。

External Lookup : Splunk Lookup (Source IP) ●

Name: *

Splunk Lookup (Source IP)

Enable lookup of internal IP addresses

Base URL: *

https://splunk-ip-or-url/en-US/app/search/flashtimeline?q=search index="{0}&earliest=-1&la

QUERY PARAMETER MAPPING:

Parameter Name: {0} Stealthwatch Attribute Name: Source IP Address Required

URL SCRIPT BUILDER FILE UPLOAD: ●

必要な数だけ属性を設定することができますが、同じ数のパラメータを設定してください。

例 2

次の URL とスクリプトの例は、rest に似たパラメータ (Secure Network Analytics Host Report など) を使用する Web アプリケーションで使用されます。

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);
    }
    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;

```

次のリンクをクリックし、前の画像に示したスクリプトの .txt ファイルをダウンロードします。

[Secure Network Analytics Host Report スクリプト](#)

この例で前に示したように、クエリパラメータを URL 形式に設定するスクリプトを作成するには、次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 エントリーを使用します。

External Lookup : Host Report (Source IP) ⓘ

Name: *

 Enable lookup of internal IP addresses

Base URL: *

QUERY PARAMETER MAPPING:

Parameter Name:	Stealthwatch Attribute Name:	
<input type="text" value="host"/>	<input type="text" value="Source IP Address"/> ▼	<input checked="" type="checkbox"/> Required

URL SCRIPT BUILDER FILE UPLOAD: ⓘ

次に実行できる作業

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、外部ルックアップを実行します。詳細な操作手順については、「[外部ルックアップの実行](#)」を参照してください。

外部ルックアップの実行

この機能を使用する目的

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. 該当する IP アドレスが表示される Web アプリケーション または デスクトップ クライアントの任意のページを開きます。次のいずれかを実行します。
 - Web アプリケーション で以下のいずれかの操作を行うと、Web アプリケーション のほとんどのページにあるメニューにアクセスできます。
 - 該当する IP アドレスの横にある(省略記号)アイコンをクリックします。
 - データテーブルまたは設定テーブルの [アクション (Actions)] 列の省略記号アイコンをクリックします。
 - 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。
 - デスクトップ クライアント 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 [[外部ルックアップ \(External Lookup\)](#)] オプションにアクセスできない場所がいくつかあります)。
2. 表示されるポップアップメニューで [[外部ルックアップ \(External Lookup\)](#)] をクリックします。第 2 のポップアップ メニューが表示されます。
3. 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ルックアップオプションをクリックします。選択したルックアップオプションに対する 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)、ルックアップを実行する IP アドレスに対するクエリ結果が表示されます。

特定の Web アプリケーションで必要となるよう指定したパラメータはすべて、ルックアップを実行する IP アドレスに対して利用できる必要があります。関連する IP アドレスに対して、1 つまたは複数の必須パラメータが利用可能でない場合、ポップアップメニューでそのルックアップオプションは有効化されません。詳細については、「[外部ルックアップの設定](#)」を参照してください。

次に実行できる作業

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 (緩和処置を開始できるように、Secure Network Analytics を設定する必要があります。)

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。
- シスコサポートの連絡先
- 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>

変更履歴

マニュアルのバージョン	公開日	説明
1_0	2023 年 2 月	最初のバージョン

著作権情報

Cisco および Cisco ロゴは、シスコまたはその関連会社の米国およびその他の国における商標または登録商標です。シスコの商標の一覧については、URL: <https://www.cisco.com/go/trademarks> をご覧ください。記載されている第三者機関の商標は、それぞれの所有者に帰属します。「パートナー」という用語の使用はシスコと他社との間のパートナーシップ関係を意味するものではありません。(1721R)