외부 조회

(Stealthwatch System v6.9.0용)

저작권 및 상표

알림

이 설명서의 제품 관련 사양 및 정보는 예고 없이 변경될 수 있습니다. 이 설명서의 모든 설명, 정보 및 권장 사항이 정확하다고 판단되더라도 어떠한 형태의 명시적이거나 묵시적인 보증도 하지 않습니다. 모든 제품의 해당 애플리케이션에 대한 사용은 전적으로 사용자에게 책임이 있습니다.

동봉한 제품의 소프트웨어 라이선스 및 제한된 보증은 제품과 함께 제공된 정보 패킷에 설명되어 있으며 본 문서에 참조를 통해 포함됩니다. 소프트웨어 라이선스 또는 제한된 보증을 찾을 수 없는 경우 CISCO 담당자에게 문의하여 복사본을 요청하십시오.

Cisco의 TCP 헤더 압축은 UNIX 운영 체제의 UCB 공개 도메인 버전의 일부로서 UCB(University of Berkeley)에서 개발된 프로그램을 적용하여 구현합니다. All rights reserved. Copyright © 1981, Regents of the University of California.

여기에 명시된 다른 모든 보증에도 불구하고 이러한 공급업체의 모든 문서 파일 및 소프트웨어는 모든 결점을 포함하여 "있는 그대로" 제공됩니다. CISCO 및 위에 언급된 모든 공급업체는 상품성, 특정 목적에의 적합성, 타인의 권리 비침해 또는 처리, 사용, 거래 행위로 발생하는 문제에 대한 묵시적 보증을 포함하여(단, 이에 한하지 않음) 묵시적이든 명시적이든 모든 종류의 보증을 부인합니다.

CISCO 또는 그 공급업체는 이 설명서의 사용 또는 사용할 수 없음으로 인한 모든 파생적, 부수적, 직접, 간접, 특별, 징벌적 또는 기타 모든 손해(영업 이익 손실, 영업 중단, 영업 정보 손실, 또는 그 밖의 금전적 손실로 인한 손해를 포함하되 이에 제한되지 않음)에 대하여 어떠한 경우에도 책임을 지지 않으며, 이는 CISCO 또는 그 공급업체가 그와 같은 손해의 가능성을 사전에 알고 있던 경우에도 마찬가지입니다.

이 문서에서 사용된 모든 IP(인터넷 프로토콜) 주소와 전화번호는 실제 주소와 전화번호가 아닙니다. 이 문서에 포함된 예제, 명령 표시 출력, 네트워크 토폴로지 다이어그램 및 다른 그림은 이해를 돕기 위한 자료일 뿐이며, 실제 IP 주소나 전화번호가 사용되었다면 이는 의도하지 않은 우연의 일치입니다.

모든 인쇄 사본 및 소프트 카피 복제본은 비통제 사본으로 간주되며 원본 온라인 버전을 최신 버전으로 참조해야 합니다.

Cisco는 전 세계에 200개가 넘는 지사를 운영하고 있습니다. 각 지사의 주소, 전화번호 및 팩스 번호는 Cisco 웹사이트(www.cisco.com/go/offices)에서 확인하십시오.

목차

1

외부 조회 관리

외부 조회(External Lookup) 기능을 사용하면 IP 주소에 대한 추가 정보를 확인하기 위해 웹 애플리케이션(또는 내부 자산 데이터베이스)을 실행할 수 있습니다. 이 웹 애플리케이션 또는 데이터베이스를 SMC(Stealthwatch Management Console) 클라이언트 인터페이스 또는 SMC 웹 애플리케이션 인터페이스에서 직접 실행할 수 있습니다.

또한 외부 조회 기능을 사용하여 SMC 클라이언트 인터페이스에서 SMC 웹 애플리케이션 인터페이스로 신속하게 이동할 수 있는 바로가기를 만들 수 있습니다.

Stealthwatch System에는 외부 조회(External Lookup) 기능에서 사용할 수 있는 다음과 같은 기본 웹 애플리케이션(조회 옵션)이 포함되어 있습니다. 이러한 옵션은 Stealthwatch System에 추가할 필요가 없습니다.

- Cisco SenderBase
- DShield
- 호스트 보고서

Stealthwatch System 관리자가 IP 주소에 대한 추가 정보를 확인하기 위해 추가할 수 있는 몇 가지 웹 애플리케이션의 예는 다음과 같습니다.

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

중요: 기본 제공 이외의 조회 옵션을 추가하려면 SMC 웹 애플리케이션 인터페이스에서 외부 조회 컨피그레이션(External Lookup Configuration) 툴을 사용해야 합니다. 이 작업을 수행하는 방법에 대한 자세한 내용은 외부 조회 구성을 참조하십시오.

2

외부 조회 구성

이 페이지를 참조하는 이유

이 페이지를 참조하여 다음 작업을 수행합니다.

- 추가한 조회 옵션을 봅니다.
- 조회 옵션을 추가, 수정, 삭제, 활성화 또는 비활성화합니다.
- 웹 애플리케이션에 보내고자 하는 특정 파라미터를 구성합니다. 구성하는 파라미터는 조회를 수행 중인 IP 주소에서 사용할 수 있는 경우에만 전송됩니다.

참고: Stealthwatch System 버전 6.7 이상으로 업그레이드하는 경우, 외부 조회 기능에 사용한 모든 webLinks.xml이 새로운 형식으로 마이그레이션되며, 기존 webLinks.xml은 더 이상 사용되지 않습니다.

이 페이지를 찾는 방법

헤더에서 **Global Settings(글로벌 설정)** 아이콘을 클릭한 다음 **External Lookup Configuration(외부 조회 컨피그레이션)**을 클릭합니다.

이 페이지에서 수행해야 할 작업

참고:

- Cisco SenderBase, Dshield 및 Host Report(호스트 보고서)는 외부 조회 기능에 사용하도록 기본적으로 포함되어 있으므로 Stealthwatch System에 추가할 필요가 없습니다. 이 기능에 다른 웹 애플리케이션을 사용하려면 해당 애플리케이션을 Stealthwatch System에 추가해야 합니다.
- 이전에 추가한 각 외부 조회 옵션에 대해 v6.7로 업그레이드할 경우, v.6.7에서 항목이 2개가 됩니다.
- Stealthwatch System은 외부 조회 컨피그레이션을 관리하기 위해 더 이상 webLinks.xml 파일을 사용하지 않습니다.

조회 옵션 보기.

옵션을 적용할 때 다음을 수행합니다.

- 이 목록에 필요한 조회 옵션이 포함되어 있으며 해당 옵션이 외부 조회 기능에서 사용하도록 활성화되어 있는지 확인하려면 웹 애플리케이션 목록(조회 옵션)을 확인합니다.
- 외부 조회 기능에서 사용하지 않도록 조회 옵션을 비활성화하려면(하지만 나중에 사용하기 위해 컨피그레이션은 유지), 해당하는 행에서 **Enabled(활성화됨)**를 클릭합니다. 이 버튼은 *Disabled(비활성화됨)* 상태 표시를 설정/해제합니다. 외부 조회 기능에서 이 벤더를 활성화하려면 **Disabled(비활성화됨)**를 클릭합니다. 이 버튼은 *Enabled(활성화됨)* 상태 표시를 설정/해제합니다.
- 조회 옵션을 수정하거나 삭제하려면, Actions(작업) 열에서 줄임표를 클릭하여 상황 정보 메뉴를 연 다음 적절한 옵션을 선택하십시오.

조회 옵션을 추가하고 파라미터를 구성합니다.

External Lookup(외부 조회) 섹션의 오른쪽 상단에서 Add External Lookup(외부 조회 추가)을 클릭합니다. 파라미터 구성에 대한 정보는 다음을 참조하십시오.

- 웹 애플리케이션에서 내부 IP 주소에 대한 정보를 확인하려면 "Enable lookup of internal IP addresses(내부 IP 주소 조회 활성화)" 확인란을 선택하십시오.
- 구성하는 파라미터는 조회를 수행 중인 IP 주소에서 사용할 수 있는 경우에만 웹 애플리케이션에 나타납니다.
- 각 조회 옵션에 대해 최대 20개의 쿼리 파라미터를 매핑할 수 있습니다.
- 특정 웹 애플리케이션을 사용하여 조회를 수행할 때 파라미터를 필수로 설정하려면, Required(필수) 확인란을 선택합니다. 특정 웹 애플리케이션에 대해 필수로 지정하는 모든 파라미터는 조회를 수행 중인 IP 주소에 사용할 수 있어야 합니다. 필수 파라미터 중 하나 이상을 관련 IP 주소에 사용할 수 없는 경우, 해당 조회 옵션이 팝업 메뉴에서 활성화되지 않습니다.
- URL 스크립트 빌더 파일에는 쿼리 파라미터를 웹 애플리케이션의 쿼리 실행에 필요한 URL 형식으로 구성하는 스크립트가 포함됩니다.

  스크립트 빌더 파일을 업로드하지 않는 경우, Stealthwatch System은 아래에 표시된 기본 표준 쿼리 파라미터를 사용합니다.

  BaseURL?[ParameterName1]=[ParameterValue1]&[ParameterName2]=[ParameterValue2]&[ParameterName3]=[ParameterValue3](등등, 추가한 각 특성에 대해)

  쿼리 파라미터가 이전에 표시된 표준 쿼리 파라미터와 일치하지 않는 경우, 맞춤 설정된 스크립트 빌더 컨피그레이션을 업로드해야 합니다. 아래는 맞춤화된 스크립트 빌더 파일을 구성할 때 참조하는 몇 가지 스크립트 예입니다.

URL 및 스크립트 예.

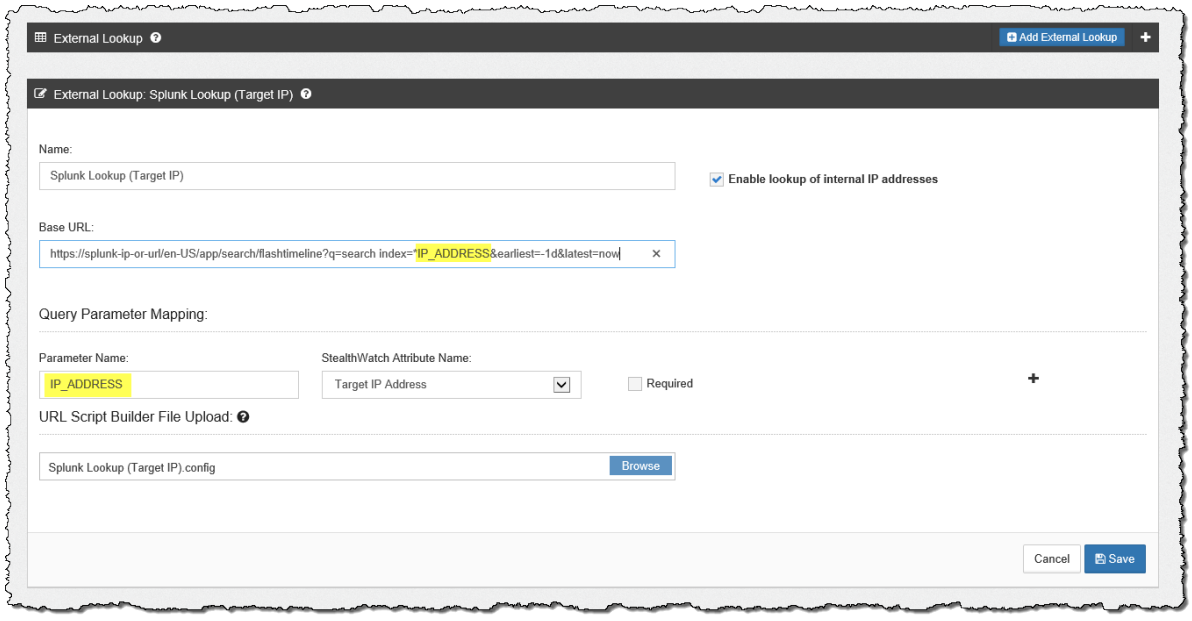
예 1

다음 URL 및 스크립트 예는 파라미터 이름(예: Splunk) 없이 값을 사용하는 웹 애플리케이션에 사용됩니다.

```
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());
```

앞서 이 예에 나와 있는 URL 형식으로 쿼리 파라미터를 구성하는 스크립트를 작성하려면, 아래 이미지에서 강조 표시된 Parameter Name(파라미터 이름) 필드 항목을 사용합니다.



참고: 필요한 만큼 많은 특성을 구성할 수 있지만, 동일한 수의 파라미터를 구성해야 합니다.

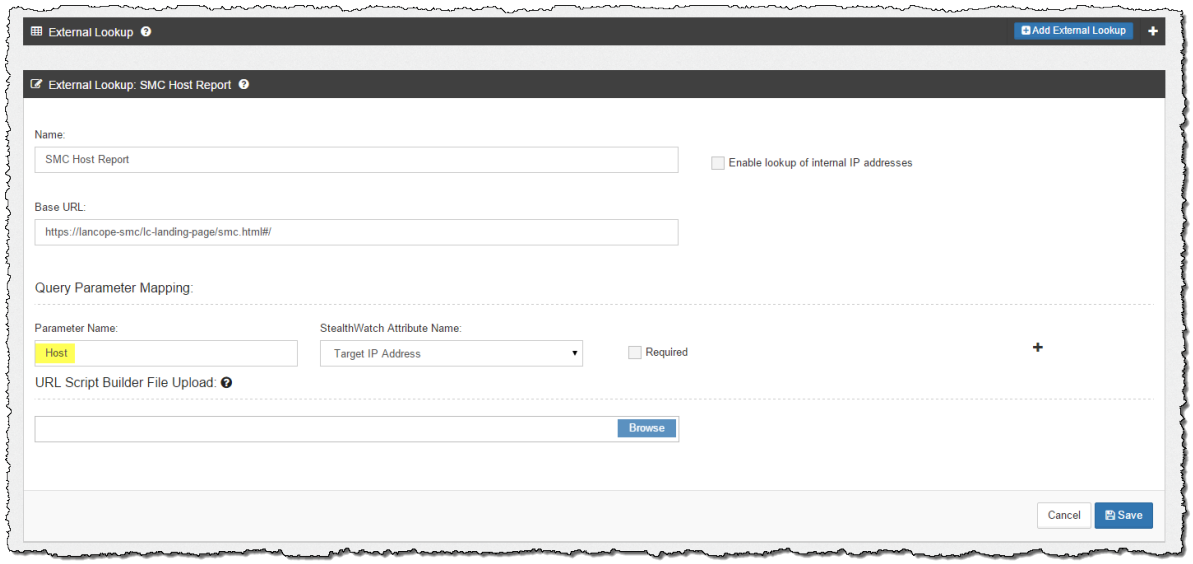
예 2

다음 URL 및 스크립트 예는 나머지 유사한 파라미터(예: Stealthwatch 호스트 보고서)를 사용하는 웹 애플리케이션에 사용됩니다.

```
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;
```

앞서 이 예에 나와 있는 URL 형식으로 쿼리 파라미터를 구성하는 스크립트를 작성하려면, 아래 이미지에서 강조 표시된 Parameter Name(파라미터 이름) 필드 항목을 사용합니다.



다음으로 수행해야 할 작업

IP 주소에 대한 추가 정보를 확인하기 위해 벤더의 웹 애플리케이션 또는 내부 자산 데이터베이스를 실행하려면 외부 조회를 수행합니다. 이 작업을 수행하는 방법에 대한 자세한 내용은 외부 조회 수행을 참조하십시오.

3

외부 조회 수행

이 기능을 사용하는 이유

이 기능을 사용하면 IP 주소에 대한 추가 정보를 확인하기 위해 웹 애플리케이션을 쿼리할 수 있습니다.

이 기능 사용 방법

1. SMC 웹 애플리케이션 인터페이스 또는 관련된 IP 주소를 포함하는 SMC(Stealthwatch Management Console) 클라이언트 인터페이스 중 하나에서 페이지를 엽니다.
2. 다음 중 하나를 수행합니다.
   - SMC 웹 애플리케이션에서 전체 SMC 웹 애플리케이션의 대부분의 페이지에 있는 상황 정보 메뉴에 액세스하려면 다음 중 하나를 수행합니다.
     - 해당하는 IP 주소 옆에 있는 줄임표를 클릭합니다.
     - Actions(작업) 열에서 줄임표를 클릭합니다.
     - 그래프에서 점을 클릭합니다. (Host Report(호스트 보고서) 페이지에 있는 Traffic by Peer Host Group(피어 호스트 그룹별 트래픽) 그래프 및 Host Group Report(호스트 그룹 보고서) 페이지에 있는 Top Host Groups by Traffic(트래픽별 상위 호스트 그룹) 그래프에서 호스트 그룹, 열 또는 두 개의 호스트 그룹 간에 있는 선을 클릭해야 합니다.)
   - SMC 클라이언트 인터페이스에서 관련 IP 주소(IP 주소에서 외부 조회 옵션에 액세스할 수 없는 몇 개의 위치가 있음)를 마우스 오른쪽 단추로 클릭합니다.
3. 표시되는 팝업 메뉴에서 **External Lookup(외부 조회)**을 클릭합니다. 보조 팝업 메뉴가 나타납니다.
4. 3단계에서 표시되는 보조 팝업 메뉴에서 원하는 조회 옵션을 클릭합니다. 선택한 조회 옵션에 해당하는 웹 애플리케이션이 열리고(웹 애플리케이션에 로그인하라는 메시지가 표시될 수 있음) 조회를 수행 중인 IP 주소의 쿼리 결과가 표시됩니다.

   특정 웹 애플리케이션에 대해 필수로 지정하는 모든 파라미터는 조회를 수행 중인 IP 주소에 사용할 수 있어야 합니다. 필수 파라미터 중 하나 이상을 관련 IP 주소에 사용할 수 없는 경우, 해당 조회 옵션이 팝업 메뉴에서 활성화되지 않습니다. 자세한 내용은 외부 조회 구성을 참조하십시오.

다음으로 수행해야 할 작업

벤더에서 반환한 정보에 따라 다음 중 하나 이상을 수행할 수 있습니다.

- 모니터링 또는 격리를 위해 특정 호스트 그룹에 이 IP 주소를 추가합니다.
- 분석가 또는 조사자가 수행하는 추가 연구에 IP 플래그를 지정합니다.
- IP 주소에 대해 완화 작업을 실행합니다. (이 작업을 수행할 수 있도록 Stealthwatch System을 구성해야 합니다.)