ASA SNMP 기능 개선 구현

목차

소개

이 문서에서는 소프트웨어 릴리스 9.1.5 및 릴리스 9.2.(1) 이상에서 Cisco ASA(Adaptive Security Appliance) 5500-X Series 방화벽에 사용할 수 있는 새로운 SNMP(Simple Network Management Protocol) 기능에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 Cisco ASA® 소프트웨어 릴리스 9.1.5 및 릴리스 9.2.(1) 이상을 실행하는 Cisco ASA 5500-X Series 방화벽을 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

ASA 버전 9.1.5 및 9.2.1에서 다음과 같은 SNMP 개선 사항이 도입되었습니다.

- 128개의 SNMP 호스트에 대한 지원이 추가되었습니다.
- cpmCPUTotal5minRev SNMP OID(Object Identifiers)에 대한 지원이 추가되었습니다.
- 1,472바이트 SNMP 메시지에 대한 지원이 추가됩니다.

128개의 SNMP 호스트 지원

이 기능을 사용하면 ASA가 현재 32개 이상의 SNMP 호스트를 지원할 수 있습니다.

목적

현재 ASA는 총 32개의 SNMP 호스트 제한을 가집니다.여기에는 트랩 및 폴링을 위해 구성할 수 있는 호스트가 포함됩니다.다음 섹션에서는 이 기능이 단일 및 다중 컨텍스트 모드에서 가지는 영향을 설명합니다.

단일 컨텍스트 모드

- 4,096개 이상의 항목(총 호스트)을 훨씬 더 많이 구성할 수 있습니다. 그러나 이러한 항목 중 트랩에는 128개만 사용할 수 있습니다.
- 폴링 컨피그레이션을 위해 최대 4,096개의 폴링 호스트와 128개의 트랩 호스트를 구성할 수 있습니다.그러나 더 많은 수의 호스트에서 성능에 미치는 영향을 알 수 없으며 지원되지 않으므로 시스템을 폴링하는 실제 서버 수는 128개 미만으로 제한되어야 합니다.

다중 컨텍스트 모드

- 컨피그레이션을 위해 컨텍스트당 최대 4,000개의 호스트가 허용되고 시스템 전반의 64,000개의 총 호스트가 제한됩니다.
- 구성된 전체 호스트 중에서 트랩에는 컨텍스트당 128개만 사용할 수 있으며 다중 컨텍스트 모드의 트랩에 대한 전체 시스템 제한은 32,000입니다.
- 컨텍스트당 최대 4,000개의 총 호스트를 구성할 수 있지만, 어떤 컨텍스트를 폴링하는 서버의

실제 수는 128개로 제한되어야 합니다.

설명

대규모 SNMP 호스트 풀에서 네트워크 디바이스를 모니터링하는 것이 좋습니다.네트워크 디바이스를 모니터링할 수 있는 IP 주소의 IP 범위 및/또는 서브넷을 지정할 수 있는 기능을 사용하는 것이 좋습니다.ASA는 현재 이러한 유연성을 제공하지 않으며 최대 SNMP 호스트를 32개로 제한합니다.

이 기능에 대한 지원에는 두 가지 측면이 있습니다.

- ASA에서 최대 128개의 SNMP 호스트를 처리할 수 있는 기능을 제공합니다.
- 이전 섹션에서 설명한 단일 명령을 통해 호스트 수를 크게 늘릴 수 있도록 필요한 컨피그레이션 명령을 제공합니다.

ASA의 현재 설계에서는 CLI를 통해 개별 호스트를 구성할 수 있습니다.이 기능에서는 다음과 같은 추가적인 설계 요구 사항을 고려했습니다.

- snmp-server host CLI 명령 보존과 함께 **snmp-server host-group** CLI 명령**의** 소개
- snmp-server host-**group** 및 snmp-**server host** CLI 명령에서 항목을 가져오는 기능.
- SNMP 버전 3의 경우 snmp-**server user CLI** 명령 보존**과 함께 snmp-server userlist** CLI 명령을 소개합니다.
- 구성 중복도 지원해야 합니다.예를 들어, 여러 **host-group** 명령은 네트워크 객체에서 겹치는 호스트와 함께 지정할 수 있습니다.마찬가지로, 현재 호스트 또는 호스트 그룹과 겹치는 IP 주소를 가진 호스트를 지정할 수 있습니다.이렇게 하면 전체 그룹을 재구성할 필요 없이 그룹의 일부 호스트에 대한 매개변수를 덮어쓰는 데 사용할 수 있는 메커니즘이 제공됩니다.

이 기능과 관련된 일부 소프트웨어 제한 및 주의 사항은 다음과 같습니다.

- snmp-**server host-group** 명령의 일부로서, 기본값은 **[trap|poll]이** 지정되지 않은 **경우 poll**입니다.이 명령에서는 트랩 및 폴링을 동일한 호스트 그룹에 대해 모두 활성화할 수 없다는 점에 유의해야 합니다.필요한 경우 관련 호스트에 snmp-**server host** 명령을 사용하는 것이 좋습니다.
- 서로 다른 **host-group** 명령에서 겹치는 네트워크 객체를 지정할 수 있습니다.마지막 호스트 그룹에 지정된 값은 서로 다른 네트워크 객체의 공통 호스트 집합에 적용됩니다.

예를 들면 다음과 같습니다.

```
object network network1
range 64.103.236.40 64.103.236.50
object network network2
range 64.103.236.35 64.103.236.55

snmp-server host-group inside network1 poll version 3 user-list SNMP-List
snmp-server host-group inside network2 poll version 3 user-list SNMP-List
```

호스트 항목을 보려면 **show snmp-server host** 명령을 입력합니다.

```
asa(config)# show snmp-server host
host ip = 64.103.236.35, interface = inside poll version 3 cisco1
```

```
host ip = 64.103.236.36, interface = inside  poll version 3 cisco1
host ip = 64.103.236.37, interface = inside  poll version 3 cisco1
host ip = 64.103.236.38, interface = inside  poll version 3 cisco1
host ip = 64.103.236.39, interface = inside  poll version 3 cisco1
host ip = 64.103.236.40, interface = inside  poll version 3 cisco1
host ip = 64.103.236.41, interface = inside  poll version 3 cisco1
host ip = 64.103.236.42, interface = inside  poll version 3 cisco1
host ip = 64.103.236.43, interface = inside  poll version 3 cisco1
host ip = 64.103.236.44, interface = inside  poll version 3 cisco1
host ip = 64.103.236.45, interface = inside  poll version 3 cisco1
host ip = 64.103.236.46, interface = inside  poll version 3 cisco1
host ip = 64.103.236.47, interface = inside  poll version 3 cisco1
host ip = 64.103.236.48, interface = inside  poll version 3 cisco1
host ip = 64.103.236.49, interface = inside  poll version 3 cisco1
host ip = 64.103.236.50, interface = inside  poll version 3 cisco1
host ip = 64.103.236.51, interface = inside  poll version 3 cisco1
host ip = 64.103.236.52, interface = inside  poll version 3 cisco1
host ip = 64.103.236.53, interface = inside  poll version 3 cisco1
host ip = 64.103.236.54, interface = inside  poll version 3 cisco1
host ip = 64.103.236.55, interface = inside  poll version 3 cisco1
```

다음은 이 기능의 사용에 대한 몇 가지 중요한 참고 사항입니다.

- 다른 호스트 그룹과 겹치는 호스트 그룹 또는 호스트가 삭제되면 구성된 호스트 그룹에 사용되는 값으로 호스트가 다시 설정됩니다.
- 호스트와 연결된 값 또는 매개변수는 명령이 실행되는 순서에 따라 달라집니다.
- 특정 호스트 그룹에서 목록을 사용하는 경우 구성된 사용자 목록을 삭제할 수 없습니다.
- 특정 사용자 목록에서 사용자를 참조하는 경우 SNMP 사용자를 삭제할 수 없습니다.
- 네트워크 객체가 host-group CLI 명령에서 사용되는 경우 삭제할 수 없습니다.

구성

이 새 기능이 구현되도록 ASA를 구성하려면 이 섹션에 설명된 정보를 사용합니다.

> **참고:**이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 Command Lookup Tool(등록된 고객만 해당)을 사용합니다.

CLI 명령

SNMP 버전 3의 경우 관리자는 다양한 사용자를 지정된 호스트 그룹과 연결할 수 있습니다.이는 관리자가 호스트 그룹에서 ASA에 액세스할 수 있는 권한을 가진 사용자 집합을 원하는 경우에 유용합니다.이 CLI 명령은 여러 사용자에 대한 사용자 목록을 구성하는 데 사용됩니다.

```
ASA(config)# [no] snmp-server user-list
```

사용자 목록을 호스트 그룹과 연결하려면 CLI에 다음 명령을 입력합니다.

```
[no] snmp-server host-group
```

이 단일 명령을 사용하면 추가할 여러 호스트를 나타내기 위해 네트워크 객체를 지정할 수 있습니다.네트워크 객체를 사용하면 단일 명령을 사용하여 추가할 IP 주소 범위 또는 서브넷 마스크를 지정할 수 있습니다.네트워크 객체의 일부로 나열되는 모든 IP 주소가 SNMP 호스트 항목으로 추가됩니다.마찬가지로 사용자 목록에 지정된 각 사용자에 대해 별도의 SNMP 호스트 항목이 있습니다.

이러한 명령은 관리자가 SNMP 서버에 대한 새 구성 옵션을 지우고 볼 수 있도록 하기 위해 사용됩니다.

- snmp-server user-list 구성 지우기
- snmp-server host-group 구성 지우기
- show running-config snmp-server user-list
- show running-config snmp-server host-group

컨피그레이션 예

새 SNMP 그룹 옵션을 사용하고 버전 2c 폴링을 위한 SNMP 서버 호스트 그룹을 생성하려면 다음 단계를 완료합니다.

1. 네트워크 객체를 생성합니다.

```
asa(config)# object network network1
asa(config-network-object)# range 64.103.236.40 64.103.236.50
```

2. SNMP 호스트 그룹을 정의합니다.

```
asa(config)#snmp-server host-group inside network1 poll community ***** version 2c
```

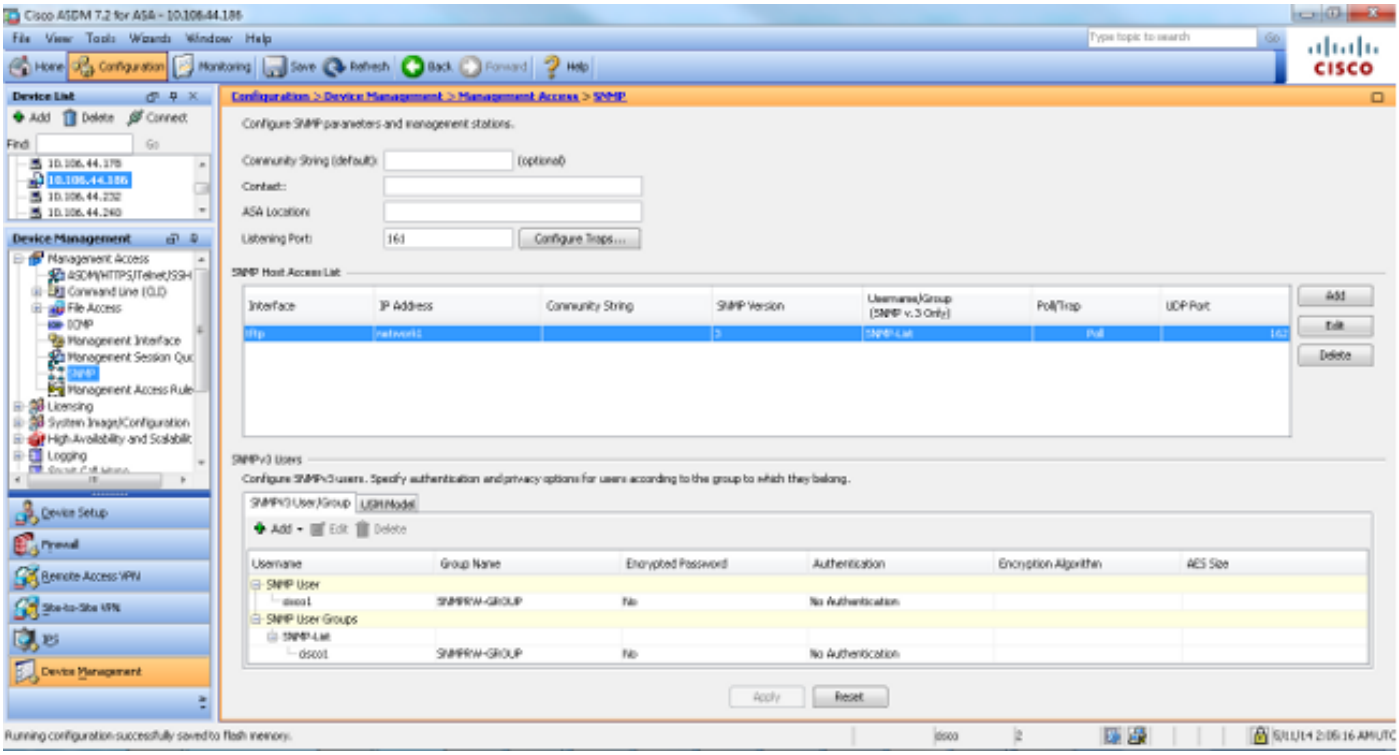
3. SNMP 버전 3 그룹을 정의합니다.

```
asa(config)#snmp-server group SNMPRW-GROUP v3 noauth
```

4. 그룹을 사용자와 연결:

```
asa(config)#snmp-server user cisco1 SNMPRW-GROUP v3
asa(config)#snmp-server user-list SNMP-List username cisco1
asa(config)#snmp-server host-group inside  network1 poll version 3 user-list SNMP-List
```

이 그림에서는 Cisco ASDM(Adaptive Security Device Manager) 내에서 수행된 변경 사항을 보여줍니다.



cpmCPUTotal5minRev SNMP OID 지원

이 기능을 사용하면 ASA가 cpmCPUTOTALominRev **SNMP OID를** 지원할 수 있습니다.

목적

이 기능은 ASA에서 cpmCPUT**OTAL5MINReV** 및 CPMCPUTotal**1minRev** OID에 대한 지원을 추가하며 현재 지원되는 OID cpmCPUTotal**5min** 및 **cpmCPUTotal1min을에 사용하지 않습니다**.이러한 OID의 목적은 CPU 사용량을 모니터링하는 것입니다.현재 지원되는 OID의 범위는 1~100이고 새로 지원되는 OID의 범위는 0~100입니다. 따라서 더 넓은 범위를 포괄하면서 새로운 OID에 대한 지원이 추가되었습니다.

더 이상 사용되지 않는 OID(cpmCPUTotal**5min** 및 cpmCPUTotal**1min**)가 ASA에서 지원되지 않으므로 ASA가 업그레이드되고 사용되지 않는 OID가 폴링되면 ASA는 해당 OID에 대한 정보를 반환하지 않습니다.ASA를 업그레이드한 후 이제 CPU 사용량에 대해 cpmCPUTotal**5minRev** 및 cpmCPUTotal**1minRev**를 모니터링해야 합니다.

CLI 명령

이 새 기능에 도입된 CLI 변경 사항이 없습니다.

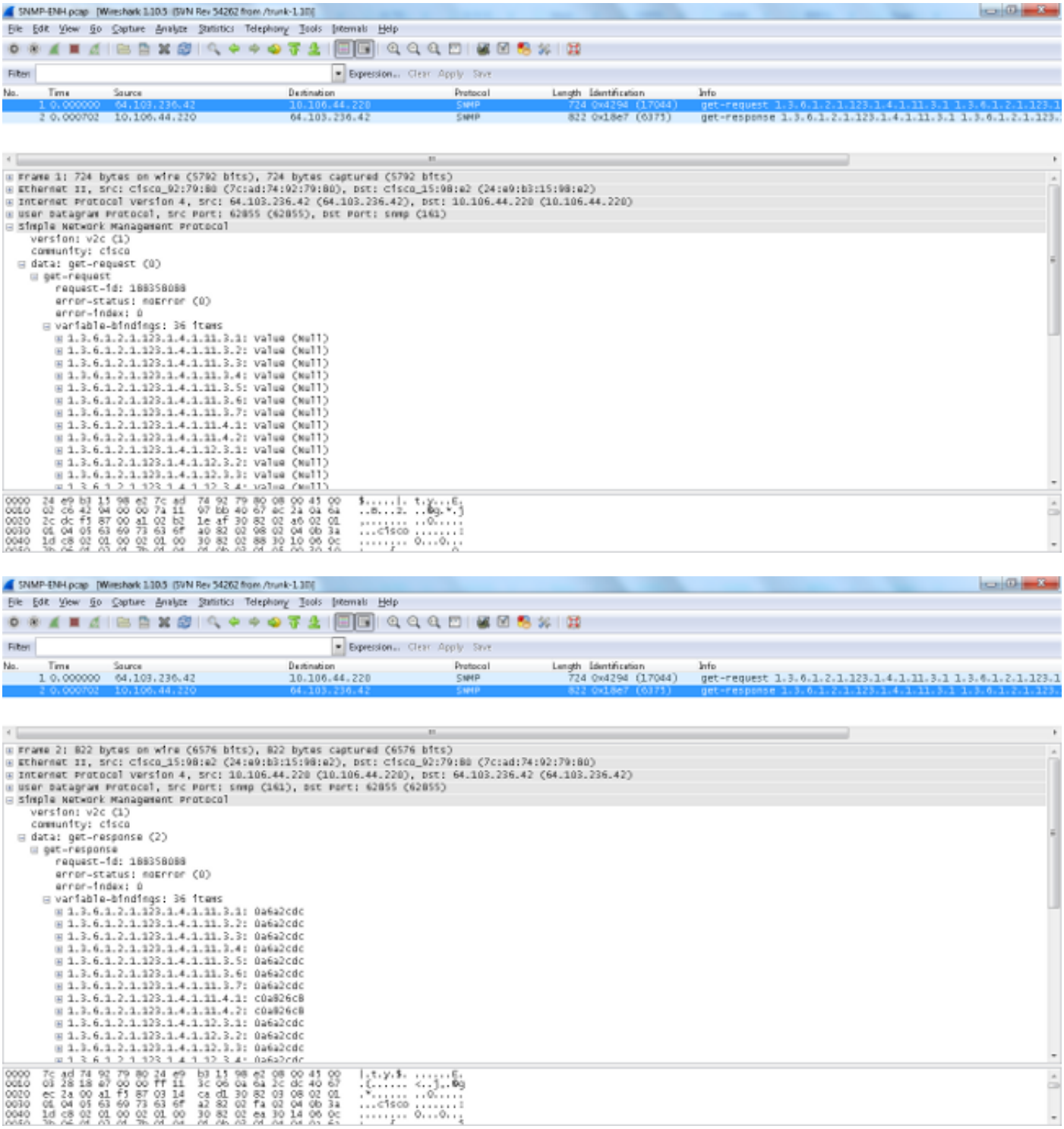
새 OID

다음은 이 기능과 함께 추가된 새 OID입니다.

- 1.3.6.1.4.1.9.9.109.1.1.1.1.7. cpmCPUTtotal1minRev
- 1.3.6.1.4.1.9.9.109.1.1.1.1.8. cpmCPUTotal5minRev

1,472바이트 SNMP 메시지 지원

ASA 플랫폼은 SNMP 요청의 최대 패킷 크기를 512바이트로 제한합니다.단일 SNMP 요청 내에서 많은 수의 MIB OID에 대해 대량 쿼리를 수행하면 SNMP 연결 시간 초과 및 오류 syslog가 ASA에 생성됩니다.RFC3417은 SNMP 요청에 대한 최대 패킷 크기는 1,472바이트여야 한다고 제안합니다.패킷에 대한 SNMP 페이로드의 크기입니다.또한 패킷의 총 크기를 계산하려면 이더넷 헤더 및 IP 헤더 크기를 추가해야 합니다.



참고:이 기능에서는 단일 컨텍스트 모드와 다중 컨텍스트 모드가 모두 지원됩니다.

문제 해결

이 섹션에서는 ASA에서 시스템 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

명령 표시

이러한 **show** 명령은 ASA에서 문제를 해결하기 위해 시도할 때 유용합니다.

- asa# **show run snmp-server host-group**
  snmp-server host-group inside network1 poll version 3 user-list SNMP-List

- asa# **show run snmp-server user-list**
  SNMP-server user-list 사용자 이름 cisco1

- asa# **show snmp-server host**

이 CLI 명령은 호스트 및 호스트 그룹 컨피그레이션을 모두 포함하는 SNMP 서버 주소 테이블에 있는 항목을 표시합니다.

```
asa(config)#show run object network
object network network1
range 64.103.236.40 64.103.236.50
object network network2
range 64.103.236.35 64.103.236.55
object network network3
range 64.103.236.60 64.103.236.70

ciscoasa/admin(config)# show run snmp-server
snmp-server group cisco-group v3 noauth
snmp-server user user1 cisco-group v3
snmp-server user user2 cisco-group v3
snmp-server user user3 cisco-group v3
snmp-server user-list cisco username user1
snmp-server user-list cisco username user2
snmp-server user-list cisco username user3
snmp-server host-group management0/0 net2 poll version 3 user-list cisco
no snmp-server locationno snmp-server contact

ciscoasa/admin(config)# show snmp-server host
host ip = 64.103.236.35, interface = inside poll version 3 cisco1
host ip = 64.103.236.36, interface = inside  poll version 3 cisco1
host ip = 64.103.236.37, interface = inside  poll version 3 cisco1
host ip = 64.103.236.38, interface = inside  poll version 3 cisco1
host ip = 64.103.236.39, interface = inside  poll version 3 cisco1
host ip = 64.103.236.40, interface = inside  poll version 3 cisco1
host ip = 64.103.236.41, interface = inside  poll version 3 cisco1
host ip = 64.103.236.42, interface = inside  poll version 3 cisco1
```

표시된 대로, 이 명령은 **host-group** 명령을 통해 구성된 모든 호스트를 표시합니다.모든 항목을 사용할 수 있는지 확인하고 겹치는 호스트 그룹을 상호 검증하기 위해 이 명령을 사용할 수 있습니다.