Cisco FindIT Network Management FAQ

목표

Cisco FindIT Network Management는 웹 브라우저를 통해 Cisco 디바이스를 비롯한 전체 네트워크를 쉽게 관리할 수 있는 소프트웨어입니다.네트워크에서 지원되는 모든 Cisco 디바이스를 자동으로 검색, 모니터링 및 구성합니다.또한 이 소프트웨어는 워런티가 더 이상 지원되지 않는 네트워크 내 디바이스에 대한 정보 및 펌웨어 업데이트에 대한 알림을 전송합니다.

Cisco FindIT Network Management에는 두 가지 구성 요소가 있습니다.FindIT Network Manager라는 단일 관리자와 FindIT Network Probe라고 하는 하나 이상의 프로브.

이 문서에는 Cisco FindIT Network Management의 설정, 구성 및 문제 해결에 관한 질문과 대답이 포함되어 있습니다.

자주 묻는 질문

목차

원격 액세스

소프트웨어 업데이트

일반

1. FindIT Network Management에서 지원하는 언어는 무엇입니까?

FindIT Network Management는 다음 언어로 변환됩니다.

- 중국어
- 영어
- 프랑스어
- 독일어
- 일본어
- 스페인어

검색

2. FindIT에서 디바이스를 관리하는 데 사용하는 프로토콜은 무엇입니까?

FindIT는 다양한 프로토콜을 사용하여 네트워크를 검색하고 관리합니다.특정 디바이스에 사용되는 정확한 프로토콜은 디바이스 유형에 따라 달라집니다.이러한 프로토콜은 다음과 같습니다.

- mDNS(Multicast Domain Name System) 및 DNS 서비스 검색 — 이 프로토콜을 Bonjour라고도 합니다.프린터, 기타 컴퓨터 등의 장치 및 해당 장치가 로컬 네트워크에서 제공하는 서비스를 찾습니다.mDNS에 대해 자세히 알아보려면 여기를 클릭하십시오 .DNS 서비스 검색에 대한 자세한 내용을 보려면 여기를 클릭하십시오.
- CDP(Cisco Discovery Protocol) — 운영 체제 버전 및 IP 주소와 같이 직접 연결된 다른 Cisco 장비에 대한 정보를 공유하는 데 사용되는 Cisco 전용 프로토콜입니다.
- LLDP(Link Layer Discovery Protocol) — 운영 체제 버전 및 IP 주소와 같이 직접 연결된

다른 장비에 대한 정보를 공유하는 데 사용되는 벤더 중립적인 프로토콜입니다.
- SNMP(Simple Network Management Protocol) — IP(Internet Protocol) 네트워크에서 서버, 프린터, 허브, 스위치, 라우터 등의 네트워크 디바이스를 구성하고 정보를 수집하는 데 사용되는 네트워크 관리 프로토콜입니다.
- RESTCONF — RESTful 인터페이스에 아직 다른 YANG(Next Generation) 데이터 모델링 언어 사양을 매핑하는 방법을 설명하는 IETF(Internet Engineering Task Force) 초안 .자세히 알아보려면 여기를 클릭하십시오.

3. FindIT에서 내 네트워크를 어떻게 검색합니까?

FindIT Network Probe는 CDP, LLDP, mDNS 광고를 수신 대기하는 네트워크에서 디바이스의 초기 목록을 작성합니다.그런 다음 프로브는 지원되는 프로토콜을 사용하여 각 디바이스에 연결되고 CDP 및 LLDP 인접성 테이블, MAC(Media Access Control) 주소 테이블 및 관련 디바이스 목록과 같은 추가 정보를 수집합니다.이 정보는 네트워크에서 추가 디바이스를 식별하는 데 사용되며, 모든 디바이스가 검색될 때까지 프로세스가 반복됩니다.

4. FindIT에서 네트워크 스캔을 수행합니까?

FindIT는 네트워크 주소 범위를 적극적으로 검사하지 않습니다.특정 네트워크 프로토콜에 대한 패시브 모니터링과 정보를 위해 네트워크 디바이스에 능동적으로 쿼리하는 조합을 사용합니다.

포트 관리

5. 포트 관리에서 스택 포트를 표시하지 않는 이유는 무엇입니까?

포트 관리 그림은 관리 프로토콜을 통해 디바이스에서 제공하는 포트 목록을 기반으로 그려집니다.스태킹 모드에서는 스택 포트가 스택 내의 내부 연결로 간주되므로, 디바이스에서 관리 프로토콜을 통해 제공되는 목록에 이러한 포트를 포함하지 않습니다.

구성

6. 새 디바이스가 발견되면 어떻게 됩니까?구성이 변경됩니까?

새 디바이스가 기본 디바이스 그룹에 추가됩니다.컨피그레이션 프로파일이 기본 디바이스 그룹에 할당된 경우 해당 컨피그레이션도 새로 검색된 디바이스에 적용됩니다.

7. 한 장치 그룹에서 다른 장치 그룹으로 장치를 이동할 때 어떻게 됩니까?

현재 원래 장치 그룹에 적용되어 새 장치 그룹에 적용되지 않는 프로파일과 관련된 모든 VLAN(Virtual Local Area Network) 또는 WLAN(Wireless Local Area Network) 컨피그레이션이 제거되고 새 그룹에 적용되며 원래 그룹에 적용되지 않은 프로파일과 관련된 VLAN 또는 WLAN 컨피그레이션이 디바이스에 추가됩니다.새 그룹에 적용된 프로필에서 시스템 구성 설정을 덮어씁니다.새 그룹에 대해 정의된 시스템 컨피그레이션 프로파일이 없으면 디바이스의 시스템 컨피그레이션이 변경되지 않습니다.

보안 고려 사항

8. FindIT Network Manager에 필요한 포트 범위 및 프로토콜은 무엇입니까?

다음 표에는 FindIT Network Manager에서 사용하는 프로토콜 및 포트가 포함되어 있습니다.

포트	방향	프로토콜	사용
TCP 22	인바운드	SSH	관리자에 대한 명령줄 액세스
TCP 80	인바운드	HTTP	관리자에 대한 웹 액세스보안 웹 서버로 리디렉션(포트 443)
TCP 443	인바운드	HTTPS	관리자에 대한 보안 웹 액세스
TCP 1069	인바운드	NETCONF/TLS	프로브와 관리자 간 통신
TCP 9443	인바운드	HTTPS	프로브 GUI에 대한 원격 액세스
TCP 50000-51000	인바운드	장치에 따라 다름	장치에 대한 원격 액세스
UDP 53	아웃바운드	DNS	도메인 이름 확인
UDP 123	아웃바운드	NTP	시간 동기화
UDP 5353	아웃바운드	mDNS	관리자를 광고하는 로컬 네트워크에 대한 멀티캐스트 DNS 서비스 광고

9. FindIT Network Probe에 필요한 포트 범위 및 프로토콜은 무엇입니까?

다음 표에는 FindIT Network Probe에서 사용하는 프로토콜 및 포트가 나열되어 있습니다.

포트	방향	프로토콜	사용
TCP 22	인바운드	SSH	프로브에 대한 명령줄 액세스
TCP 80	인바운드	HTTP	관리자에 대한 웹 액세스보안 웹 서버로 리디렉션(포트 443)
TCP 443	인바운드	HTTPS	관리자에 대한 보안 웹 액세스
UDP 5353	인바운드	mDNS	로컬 네트워크의 멀티캐스트 DNS 서비스 광고입니다.디바이스 검색에 사용됩니다.
TCP 10000-10100	인바운드	장치에 따라 다름	장치에 대한 원격 액세스
UDP 53	아웃바운드	DNS	도메인 이름 확인
UDP 123	아웃바운드	NTP	시간 동기화
TCP 80	아웃바운드	HTTP	보안 웹 서비스를 사용하지 않고 장치 관리
UDP 161	아웃바운드	SNMP	네트워크 장치 관리
TCP 443	아웃바운드	HTTPS	보안 웹 서비스가 활성화된 장치 관리소프트웨어 업데이트, 지원, 상태, 단종 알림 등의 정보를 보려면 Cisco 웹 서비스에 액세스
TCP 1069	아웃바운드	NETCONF/TLS	프로브와 관리자 간 통신
UDP 5353	아웃바운드	mDNS	프로브를 광고하는 로컬 네트워크에 대한 멀티캐스트 DNS 서비스 광고

10. FindIT Network Manager와 FindIT Network Probe 간의 통신은 얼마나 안전합니까?

관리자와 프로브 간의 모든 통신은 클라이언트 및 서버 인증서로 인증된 TLS(Transport Layer Security) 1.2 세션을 사용하여 암호화됩니다.프로브에서 관리자로 세션이 시작됩니다.관리자와 프로브 간의 연결이 처음 설정될 때 사용자는 프로브에서 관리자에 로그온해야 합니다. 이때 관리자 및 프로브 교환 인증서는 향후 통신을 인증합니다.

11. FindIT에서 내 장치에 대한 '백도어' 액세스 권한을 가지고 있습니까?

아니요. FindIT는 지원되는 Cisco 디바이스를 검색할 때 기본 사용자 이름 및 비밀번호로 해당 디바이스에 대한 공장 기본 자격 증명을 사용하여 디바이스에 액세스하려고 시도합니다.cisco 또는 기본 SNMP 커뮤니티:공개입니다.디바이스 컨피그레이션이 기본값에서 변경된 경우 사용자가 FindIT에 올바른 자격 증명을 제공해야 합니다.

12. 자격 증명은 FindIT에 얼마나 안전합니까?

FindIT에 액세스하기 위한 자격 증명은 SHA512 알고리즘을 사용하여 되돌릴 수 없습니다.디바이스 및 기타 서비스(예: **Cisco Active Advisor**)에 대한 자격 증명은 AES-128 알고리즘을 사용하여 버전 재암호화됩니다.

13. 관리 GUI의 분실된 비밀번호를 복구하려면 어떻게 해야 합니까?

관리 GUI에서 모든 관리자 계정의 비밀번호를 잊어버린 경우 Probe 또는 Manager의 콘솔에 로그온하고 **recoverpassword** 툴을 실행하여 비밀번호를 재설정할 수 있습니다.이 도구는 cisco 계정의 비밀번호를 기본 cisco로 재설정하거나, cisco 계정이 제거된 경우 기본 비밀번호로 계정을 재생성합니다.다음은 이 툴을 사용하여 비밀번호를 재설정하기 위해 제공되는 명령의 예입니다.

```
cisco@FindITProbe:~# recoverpassword

?(y/n) y

Cisco

cisco@FindITProbe:~#
```

원격 액세스

14. FindIT Network Management에서 디바이스의 관리 GUI에 연결할 때 세션이 안전합니까?

FindIT Network Management는 디바이스와 사용자 간에 원격 액세스 세션을 터널링합니다.사용되는 프로토콜은 최종 디바이스 컨피그레이션에 따라 달라지지만, FindIT는 활성화된 경우 항상 보안 프로토콜을 사용하여 세션을 설정합니다(예: HTTPS가 HTTP보다 우선함). 사용자가 관리자를 통해 디바이스에 연결하는 경우 디바이스에서 활성화된 프로토콜과 상관없이, 세션은 관리자와 프로브 간에 암호화된 터널을 통과하면서 통과됩니다.

15. 다른 디바이스에 대한 원격 액세스 세션을 열 때 디바이스로 원격 액세스 세션이 즉시 로그아웃되는 이유는 무엇입니까?

FindIT Network Management를 통해 디바이스에 액세스하면 브라우저는 각 연결이 동일한 웹 서버(FindIT)와 연결되어 있는 것으로 인식하므로 각 디바이스의 쿠키를 모든 다른 디바이스에 제공합니다.여러 디바이스에서 동일한 쿠키 이름을 사용하는 경우 한 디바이스 쿠키를 다른 디바이스에서 덮어쓸 가능성이 있습니다.이는 세션 쿠키에서 가장 자주 나타나며, 그 결과 쿠키는 가장 최근에 방문한 장치에서만 유효합니다.동일한 쿠키 이름을 사용하는 다른 모든 디바이스는 쿠키가 유효하지 않은 것으로 표시되며 세션을 로그아웃합니다.

16. 다음 오류가 발생하여 원격 액세스 세션이 실패하는 이유액세스 오류:요청 엔터티가 너무 커서 HTTP 헤더 필드가 지원되는 크기를 초과합니까?

여러 디바이스에서 원격 액세스 세션을 여러 번 수행한 후 브라우저에는 Probe 도메인에 대해 많은 수의 쿠키가 저장됩니다.이 문제를 해결하려면 브라우저 컨트롤을 사용하여 도메인에 대한 쿠키를 지운 다음 페이지를 다시 로드하십시오.

소프트웨어 업데이트

17. Manager 운영 체제를 최신 상태로 유지하려면 어떻게 해야 합니까?

관리자는 운영 체제에 CentOS Linux 배포를 사용합니다.패키지와 커널은 표준 CentOS 프로세스를 사용하여 업데이트할 수 있습니다.예를 들어 수동 업데이트를 수행하려면 콘솔에 cisco 사용자로 로그온하고 sudo yum -y update 명령을 입력합니다.시스템을 새 CentOS 릴리스로 업그레이드하지 않아야 하며, Cisco에서 제공하는 가상 머신 이미지에 포함된 것 이상의 추가 패키지를 설치하지 않아야 합니다.

18. Manager에서 Java를 업데이트하려면 어떻게 합니까?

Java 업데이트는 Oracle에서 다운로드하여 다음 명령을 사용하여 수동으로 설치해야 합니다.

새 Java 패키지를 관리자에게 직접 다운로드하려면

```
curl -L -O -H ":oraclenses=accept-securebackup-cookie" -k http://download.oracle.com/otn-pub/java/jdk/<version>-<build>/jre-<version>-linux-x64.rpm
```

다음은 예입니다.

```
curl -L -O -H ":oraclelicense=accept-securebackup-cookie" -k "http://download.oracle.com/otn-pub/java/jdk/8u102-b14/jre-8u102-linux-x64.rpm"
```

업데이트된 Java 버전을 설치하려면

1단계. sudo yum -y remove jre*1.8.0_102* 명령을 사용하여 이전 버전*을 제거합니다.*

2단계. sudo yum -y localinstall jre *-<version>-linux-x64.rpm* 명령을 사용하여 새 버전*을 설치합니다.*

19. Probe 운영 체제를 최신 상태로 유지하려면 어떻게 해야 합니까?

프로브는 운영 체제에 OpenWRT를 사용합니다.포함된 패키지는 opkg 툴을 사용하여 업데이트할 수 **있습니다**.예를 들어 시스템의 모든 패키지를 업데이트하려면 cisco 사용자로 콘솔에 로그온하고 update-packages 명령을 입력합니다.필요한 경우 Cisco에서 새 버전의 프로브의 일부로 커널 업데이트를 제공합니다.Cisco에서 제공하는 가상 머신 이미지에 포함된 것 이상의 추가 패키지는 설치할 수 없습니다.

20. Cisco FindIT Kaseya Plugin이란 무엇입니까?

Cisco FindIT Kaseya Plugin은 Cisco FindIT Network Manager를 Kaseya VSA(Virtual System Administrator)와 긴밀하게 통합하여 운영 효율성을 높이도록 설계되었습니다. Cisco FindIT Kaseya Plugin은 작업 관리, 대시보드, 디바이스 검색, 네트워크 토폴로지, 원격 디바이스 관리, 실행 가능한 알림 및 이벤트 기록 등의 강력한 기능을 제공합니다.

이 플러그인은 매우 쉽게 설치할 수 있도록 설계되었으며, 클릭 몇 번만 하면 됩니다.Kaseya 온프레미스 VSA 버전 9.3 및 9.4에 대한 모든 서드파티 통합 요구 사항을 준수합니다. 자세한 내용을 보려면 여기를 클릭하십시오.