Cisco Secure Intrusion Detection System(버전 3.1 이하) FAQ

목차

소개

이 문서에는 Cisco Secure Intrusion Detection System(IDS)(이전의 NetRanger 버전 3.1 이하)에 대한 FAQ(자주 묻는 질문)가 포함되어 있습니다.

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

일반

Q. Cisco Secure IDS에 대한 추가 정보는 어디에서 찾을 수 있습니까?

A. Cisco Secure IDS에 대한 자세한 내용은 전체 제품 문서를 참조하십시오.

Q. 전체 IDS 시스템(IDS Sensor + IDS Management Software)에 대한 서명을 업데이트하려면 어떻게 해야 합니까?

A. 센서 및 관리 플랫폼 서명을 별도로 업그레이드해야 합니다.관리 소프트웨어는 센서에서 서명을 *학습할* 수 없으므로 업데이트해야 합니다.Cisco Secure Downloads(등록된 고객만)에서 각 애플리케이션에 대한 최신 서명 업데이트 파일을 다운로드합니다. 동일한 위치에서 제공되는 Readme 파일에는 업그레이드 절차에 대한 지침이 포함되어 있습니다.

Q. 서명 전체 목록은 어디에서 찾을 수 있습니까?

A. IDS 서명 목록은 Cisco Secure Encyclopedia(등록된 고객만 해당)를 통해 제공됩니다.

Q. UNIX IDS 및 독립형 센서의 사용자에 대한 기본 비밀번호는 무엇입니까?

A. UNIX IDS 독립형 센서 및 IDS 관리 소프트웨어에서 기본 비밀번호는 사용자 **네트워크** 및 **루트**에 대한 "공격"입니다.**su** 명령을 실행하여 루트 사용자가 되면 기본 비밀번호는 "attack"입니다. IDSM(Intrusion Detection System Module) 블레이드에서 기본 비밀번호는 사용자 이름 ciscoid의

"공격"입니다.

Q. IDSM(Intrusion Detection System Module) 블레이드에서 컨피그레이션을 덤프하려면 어떻게 해야 합니까?

A. 구성을 업로드할 수 있도록 로컬 FTP 서버가 필요합니다.

1. 블레이드의 진단 모드에서 이 명령을 입력합니다.

   ```
   report systemstatus site user dir
   ```
2. "시스템 보고서 생성 계속"을 묻는 메시지가 나타나면 y를 입력합니다.
3. 프롬프트가 표시되면 지정된 사용자의 FTP 비밀번호를 입력합니다.프로세스가 완료되면 프로세스가 실패했는지 또는 파일이 전송되었는지 여부를 나타내는 메시지가 표시됩니다.

Q. IDS를 설치/제거할 때 로그 파일은 어디에 있습니까?

A. 설치/업데이트 로그는 다음 위치에서 찾을 수 있습니다.

- 디렉터 설치 로그는 /var/adm/nrInstall.log에 있습니다.
- 센서 서비스 팩 업데이트 로그는 /usr/nr/sp-update/에 있습니다.
- 서명 업데이트 로그는 /usr/nr/sig-update/에 있습니다.

Q. IDS용 PIX에서 사용할 수 있는 시그니처는 무엇입니까?

A. IDS는 PIX 6.0 이상에만 사용할 수 있습니다.시그니처는 syslog 메시지 40000~400051에 포함되어 있으며, 이를 Cisco Secure IDS 서명 메시지라고 합니다.각 서명에 대한 자세한 내용은 PIX 시스템 로그 메시지 설명서를 참조하십시오.

Q. 서명 업데이트가 릴리스되면 알림을 받을 수 있습니까?

A. Cisco Secure IDS 관련 제품 뉴스에 대한 이메일 알림을 받으려면 Cisco IDS Active Update 알림에 등록하십시오.

Q. IDS 센서를 관리하는 데 어떤 애플리케이션을 사용해야 하며, 두 애플리케이션의 차이점은 무엇입니까?

A. 버전 3.1 이전의 관리 옵션은 Cisco CSPM(Secure Policy Manager) 또는 UNIX Director를 사용하는 것입니다.두 가지 차이점은 CSPM이 Windows 서버에서 독립 애플리케이션으로 실행되는 반면 UNIX Director는 UNIX Solaris 서버에서 HP OpenView를 기반으로 실행된다는 점입니다.IDS 3.1에서는 PC에 설치된 IDS Event Viewer(IEV)를 통해 센서를 관리하거나 버전 3.1 센서의 일부인 IDS Device Manager를 사용할 수도 있습니다.Device Manager는 센서를 설정한 후 SSL(Secure Socket Layer)을 사용하여 기본적으로 활성화됩니다.

Q. SDK(Software Development Kit) 소프트웨어는 어디에서 얻을 수 있습니까?

A. SDK 소프트웨어는 일반인에게 제공되지 않습니다.

IDS 센서

Q. 센서 버전 3.x와 4.x의 차이점은 무엇입니까?

A. 버전 4.0은 여러 새로운 기능을 제공합니다.가장 눈에 띄는 새로운 기능은 Cisco IOS®와 유사한 CLI(Command-Line Interface)입니다.

Q. IDS에서 인터페이스 속도를 하드 코딩하려면 어떻게 해야 합니까?

A. 3.x 및 4.0 코드에서 속도/듀플렉스를 하드 설정하는 것은 지원되지 않으며 기능 요청에 대한 버그가 있습니다(Cisco 버그 ID CSCdy43054(등록된 고객만 해당). 이 기능은 5.0 코드에서 사용할 수 있으며, 이제 인터페이스 구성에서 사용할 수 있습니다.

Q. 센서 소프트웨어를 버전 3.0에서 3.1로 업그레이드하려면 어떻게 해야 합니까?

A. 고객은 Cisco Secure Downloads(등록된 고객만)에서 버전 3.1에 대한 업데이트 파일을 다운로드할 수 있습니다.

Q. 센서 소프트웨어를 버전 2.5에서 3.0으로 업그레이드하려면 어떻게 해야 합니까?

A. 고객은 Cisco Secure Downloads(등록된 고객만)에서 버전 3.0에 대한 업데이트 파일을 다운로드할 수 있습니다. 버전 2.5에서 서비스 팩 및 서명 업데이트가 설치되는 것과 동일한 방법으로 소프트웨어 업데이트를 설치합니다. 이 절차는 Cisco IDS Sensor Configuration Note Version 3.0에서 자세히 설명합니다.

Q. 센서 소프트웨어를 버전 2.2에서 3.0으로 업그레이드하려면 어떻게 해야 합니까?

A. 3.0 업그레이드 파일은 Cisco Secure Downloads에서 다운로드할 수 있습니다(등록된 고객만 해당). 이 파일은 2.5 이전 버전을 업데이트할 수 없습니다. 제품 업그레이드 도구(등록된 고객만 해당)를 통해 제공되는 업그레이드/복구 CD를 사용하여 소프트웨어 버전 2.2에서 3.0으로 업그레이드해야 합니다. 이 CD의 부품 번호는 IDS-SW-U입니다.

참고: 업그레이드/복구 CD를 주문하려면 유효한 지원 계약이 있어야 합니다.

Q. 센서에 키보드 및 모니터를 연결했지만 제대로 부팅되지 않습니다.어떻게 해야 합니까?

A. 지원되는 키보드 및 모니터를 사용하고 있는지 확인합니다.일부 브랜드 및 모델은 Cisco Secure IDS와 호환되지 않으므로 IDS 센서가 제대로 부팅되지 않습니다.특정 브랜드 세부사항은 Cisco Secure IDS Appliance 부팅 실패를 참조하십시오.

Q. Cisco Secure Downloads의 IDS 섹션에 두 가지 유형의 업데이트 파일(서비스 팩 및 서명)이 표시됩니다. 이 파일의 차이점은 무엇입니까?

A. 이러한 각 파일에는 여기에 설명된 명명 규칙에 따라 지정된 소프트웨어 업데이트 또는 추가 세트가 포함되어 있습니다.

- IDS Sensor Appliance 소프트웨어의 서비스 팩 업데이트에는 IDS Sensor 코어 애플리케이션 소프트웨어에 대한 개선 사항과 버그 픽스가 포함되어 있습니다.예를 들어 IDSk**9-sp-3.0-5-S17.bin**이라는 파일은 소프트웨어 버전 3.0(5)에 대한 업데이트와 서명 세트 번호 17을 포함합니다.

- 시그니처 업데이트 파일에는 시그니처 업데이트(공격 핑거프린트)만 포함됩니다. 예를 들어 IDSk**9-sig-3.0-5-S18.bin**이라는 파일은 3.0(5) 센서 소프트웨어에 대한 서명 세트 번호 18을 포함합니다.

고객은 Cisco Secure Downloads(등록된 고객만 해당) 사이트에서 이러한 파일을 다운로드할 수 있습니다.

Q. 센서가 라우터를 차단하도록 올바르게 구성되었는지 어떻게 알 수 있습니까?

A. 사용자 netranger로 센서에 로그인하고 다음 명령을 실행합니다.

```
nrgetbulk
```

공격을 차단하는 데 사용된 디바이스의 IP 주소를 표시하는 "*<IP_address>* Active"와 유사한 응답을 받아야 합니다.이 출력은 명령 구문 및 예상 응답의 예를 보여줍니다.

```
netrangr@sensor:/usr/nr
>nrgetbulk 10003 38 1000 1 NetDeviceStatus
10.48.66.68 Active
Success
```

라우터에 로그인하고 **who** 명령을 실행하여 센서가 로그인되었는지 확인할 수도 있습니다.

Q. nrconns 명령을 실행할 때 "value not set"을 나타내는 오류 메시지가 나타납니다.이 문제를 어떻게 해결할 수 있습니까?

A. 이 오류 메시지는 센서의 /usr/nr/etc/routes 및/또는 /usr/nr/etc/hosts 파일에 발생할 수 있는 문제를 나타냅니다..../routes 파일은 센서와 디렉터 간의 사후 통신을 정의합니다..../hosts 파일은 센서 및 디렉터의 이름과 IP 주소를 정의합니다.

사용자 **루트**로 로그인하고, sysconfig-**sensor** 명령을 실행하고 IDS Communications Infrastructure 정보를 다시 입력할 수도 있습니다.

Q. FTP를 사용하여 센서에서 로그 파일을 복사하여 다른 곳에 저장하려면 어떻게 해야 합니까?

A. 이 절차에 대한 자세한 내용은 볼 IP 로그 파일 복사를 참조하십시오.

Q. Sensor 소프트웨어 버전 2.5 및 3.1에서 구성된 데몬은 어떻게 되었습니까?

A. Configd는 UNIX 디렉터와 2.2.x 코드 베이스의 센서에서 모든 명령을 처리하는 데몬입니다.2.5 및 3.0 코드 베이스에서 이 기능은 다른 데몬에 흡수되고 구성된 데몬이 더 이상 존재하지 않습니다.

Q. 센서에서 서명을 업데이트하면 가 . **NetRanger** . ." 오류 메시지.어떻게 해야 하죠?

A. nr.packetd가 데몬 목록에 있는지 확인하려면 센서에서 /usr/nr/etc/daemons 파일을 편집합니다.그런 다음 서비스를 중지하고 시작합니다.

Q. IDS 4210에서 컨트롤 인터페이스이며 스니핑 인터페이스는 무엇입니까?

A. 상단의 제어 인터페이스는 iprb**1:**이고 하단의 스니핑 인터페이스는 iprb**0:**입니다.

Q. 센서에서 ifconfig -a 명령을 실행할 때 인터페이스 하나만 표시되는 이유는 무엇입니까?

A. ifconfig 명령은 제어 인터페이스만 표시해야 합니다.센서에서 다른 인터페이스(스니핑 인터페이스)를 계속 사용하지만 사용자는 이를 볼 수 없습니다.이 인터페이스를 확인해야 하는 경우 루트로 로그인하고 ifconfig -a 명령**을 실행하여** 인터페이스 이름을 확인합니다.ifconfig *<interface>* ***plumb*** 명령을 실행하여 특정 인터페이스의 상태를 확인합니다.

Q. 센서에서 인터페이스 속도를 하드코딩하려면 어떻게 해야 합니까?

A. 센서의 인터페이스 속도를 하드코딩할 필요가 없으며 Cisco 기술 지원에서 지원하지 않습니다.스위치가 자동 협상을 위해 설정된 경우 인터페이스는 연결된 스위치와 속도를 협상합니다.네트워크에서 센서로의 트래픽은 단방향입니다(즉, 센서가 수신함). 따라서 스위치에서 100개의 반이중(half-duplex)이 협상되었다고 표시하면 일반적으로 적합합니다(스위치 포트가 100M라고 가정).

UNIX 디렉터

Q. 2.2.x 버전의 Director와 함께 새로운 3.0 Sensor를 사용할 수 있습니까?

A. 예, 하지만 Director 소프트웨어를 버전 2.2.3 이상으로 업그레이드해야 합니다.등록된 고객은 Cisco Secure Downloads에서 이러한 파일을 다운로드할 수 있습니다(등록된 고객만 해당).

Q. 사용 중인 Director 데몬의 버전을 어떻게 알 수 있습니까?

A. cat **/usr/nr/VERSION** 명령을 실행하고 출력에 포함된 버전 번호를 확인합니다.

참고: Director 명령의 출력은 Director에서 실행되는 데몬의 버전을 알려주지만 Director 소프트웨어 자체의 버전은 알려주지 않습니다.

Q. Director가 구성을 덤프하도록 하려면 어떻게 해야 합니까?

A. 사용자 **netrangr**로 로그인하고 /usr/nr/bin/director/nrCollectInfo 스크립트를 실행하여 구성 정보를 /usr/nr/var/tmp/Report_For_Director.html라는 파일로 전송합니다.

Q. HP OpenView 디스플레이에 오류가 많이 있습니다(1,000개가 넘을 수도 있음).삭제했는데 계속 돌아옵니다왜?

A. IDS Director에 오류가 가득 차서 모두 표시할 수 없으면 파일에 버퍼링하기 시작합니다.IDS 데몬을 중지하고 파일을 제거하기 위해 열려 있는 OpenView 맵을 모두 종료합니다 ./usr/nr/var/nrDirmap.buffer**.default** 파일**을 삭제한** 다음 IDS 데몬과 OpenView 맵을 다시 시작합니다.

Q. HP OpenView 맵에 알람을 가져오는 데 문제가 있습니다 ./usr/nr/var/errors.nrdirmap에서 오류가 계속 발생합니다.어떻게 해야 합니까?

A. 2.2.2 이전 IDS 버전에서는 OpenView 데이터베이스를 삭제하는 것이 가장 쉽습니다.데이터베이스는 /var/opt/OV/share/databases/openview에 상주합니다.OpenView 데이터베이스를 삭제하려면 다음 단계를 완료하십시오.

1. ovstop 명령으로 열려 있는 모든 OpenView 맵을 **닫은** 다음 nrstop 명령으로 IDS 서비스를 **중지합니다**.
2. 사용자 **루트**로 로그인하고/usr/nr/bin/director/nrDeleteOVwDb**를 실행합니다**.
3. /usr/nr/var 디렉토리의 모든 "error.*" 파일을 제거합니다(예: errors.configd).
4. nrstart 명령을 사용하여 서비스를 **다시** 시작한 다음 **ovstart** 명령을 사용하여 OpenView를 다시 시작합니다. **참고:** Director 버전 2.2.2에서는 전체 데이터베이스 대신 OpenView 데이터베이스의 IDS 부분만 제거할 수 있습니다.이 절차는 IDS Director 컨피그레이션 가이드에 설명되어 있습니다.

Q. OpenView 맵에서 경보를 가져올 수 없습니다.Director의 /usr/nr/var/errors.postofficed 파일에는 nrdimap이 이 시스템에서 실행할 수 있는 라이센스가 없다는 메시지가 포함되어 있습니다.이 문제를 어떻게 해결합니까?

A. 이 명령을 실행합니다.

```
cp /usr/nr/etc/.lt/license-all.lic /usr/nr/etc/licenses
```

사용자 **netrangr**이 파일을 소유하는지 확인한 다음 IDS 서비스를 다시 시작합니다.

Q. nrConfigure 유틸리티를 실행하고 Director를 두 번 클릭하면 다음과 같은 메시지가 표시됩니다."*<director_name>*의 센서 유형을 찾을 수 없습니다.Postoffice 및 패킷이 실행 중인지 확인하십시오." 어떻게 해야 합니까?

A. nrConfigure는 디렉터의 데몬 파일에서 패킷 프로세스를 확인하므로 문제가 발생합니다. nrConfigure가 Director의 버전을 Sensor인 것처럼 쿼리하면 Director가 Sensor 버전으로 응답할 수 없습니다.

이 문제를 해결하려면 다음 단계를 완료하십시오.

1. /usr/nr/etc/daemons 파일을 편집하고 nr.packetd, nr.sendsord 및 nr.managed에 대한 항목을 제거합니다. 이러한 프로세스는 센서에서만 실행되어야 합니다.
2. nrstop 명령으로 서비스를 중지한 다음 nrstart 명령을 사용하여 서비스를 **다시** 시작합니다.
3. nrConfigure가 종료되었는지 확인합니다.
4. ovw 명령을 사용하여 OpenView**를** 시작합니다.
5. Security **> Advanced > Configure DB > Delete를 선택하여** 손상된 nrConfigure 데이터베이스를 삭제합니다.
6. **예**를 계속 진행하라는 메시지가 나타나면 입력합니다.
7. 기본 OpenView 창에서 디렉터와 모든 센서를 강조 표시합니다.
8. Security(**보안) > Advanced(고급) > Configure DB(DB 구성) > Create(생성)를 선택하여** 시스템의 현재 컨피그레이션 버전으로 새 데이터베이스를 생성합니다.

Q: OpenView 맵에서 기본적으로 nrdimap 애플리케이션이 활성화되지 않도록 하려면 어떻게 해야 합니까?

A. UNIX Director에서 IDS 애플리케이션을 실행하는 사용자는 OpenView에서 다른 애플리케이션을 실행할 수도 있습니다.이는 권장되지 않지만 어떤 경우에는 피할 수 없습니다.문제는 모든 OpenView 맵에 대해 기본적으로 nrdimap이 활성화되어 있다는 점입니다. 다른 응용 프로그램이 OpenView에서 실행되는 경우에는 바람직하지 않습니다.

UNIX Director에서 다음 단계를 수행하여 기본값을 변경하여 어떤 맵에서 Nrdimap이 활성화되었는지 선택할 수 있습니다.

1. 사용자 netrangr로 **로그인합니다**.
2. cd **$OV_REGISTRATION/C를 입력합니다**. OV_REGISTRATION은 환경 변수의 일부입니다.일반적인 경로는 /etc/opt/OV/share/registration/C입니다.)
3. su **root를 입력합니다**.
4. nrdirmap 파일을 편집하고 다음 출력에 표시된 대로 "Command" 줄을 변경합니다.

```
Command -Shared -Initial "nrdirmap";
!--- Changes to: Command -Shared -Initial "nrdirmap -d";
```

5. nrdirmap 파일을 저장합니다.
6. OpenView를 재생합니다.이제 ovw 명령을 사용하여 맵이 나타나면 **ps -ef를 입력합니다. | grep dirmap은** 여기에 표시된 것과 유사한 출력을 생성해야 합니다.nrdirmap `-d` 스위치로 확인합니다.

```
>ps -ef | grep dirmap
netrangr 7175 6820 0 09:50:47 pts/2 0:00 grep dirmap
netrangr 7158 7152 0 09:50:21 ? 0:00 nrdirmap -d
```

이제 OpenView에서 생성된 새 맵에는 기본적으로 nrdimap이 활성화되어 있지 않습니다.nrdirmap이 설치된 맵을 만들려면 OpenView GUI에서 다음 절차에 따라 맵을 만들어야 합니다.

1. 기본 OpenView 메뉴에서 **Map > New를** 선택하고 새 맵의 이름을 입력합니다.
2. 구성 가능한 애플리케이션 아래에 NetRanger/Director가 표시됩니다.NetRanger**/Director를** 선택하고 **이 맵에 대한 구성을 클릭합니다**.
3. "이 맵에 대해 ndirmap을 활성화해야 합니까?"라는 옵션의 경우 nrdirmap을 활성화하려면 **True**를 선택합니다.
4. Verify(**확인**)를 선택하고 **OK(확인)**를 클릭합니다.

Q. Director 버전 2.2.3으로 업그레이드했지만 이전 버전에서 이벤트 심각도를 5보다 높게 설정할 수 없습니다.왜 그럴까?

A. 심각도 레벨이 1~5의 범위만 지원하도록 디렉터 버전 2.2.3에서 변경되었습니다.

IDS Cisco CSPM(Secure Policy Manager)

Q. IDS 센서를 관리하려면 어떤 버전의 CSPM을 사용해야 합니까?

A. 현재 CSPM 2.3i 버전은 IDS 센서를 관리할 수 있는 반면 CSPM 3.0은 관리할 수 없습니다.CSPM을 사용하여 센서와 기타 Cisco Secure 디바이스(예: PIXes, 라우터)를 관리하는 경우 두 개의 서로 다른 CSPM 버전(2.3i 및 3.x)을 두 개의 개별 Windows 서버에 설치해야 합니다.각 서버를 사용하여 해당 디바이스를 관리할 수 있습니다.센서용 CSPM 2.3i, PIXes, 라우터 등의 경우 CSPM 3.x

Q. IDS 센서를 관리하고 통신이 제대로 작동하도록 CSPM을 구성하려면 어떻게 해

야 합니까?

A. IDS 센서를 관리하고 통신이 작동하는지 확인하기 위해 CSPM을 구성하는 방법에 대한 자세한 내용은 CSPM에서 Cisco Secure IDS Sensor 구성을 참조하십시오.

Q. CSPM을 사용하여 어플라이언스의 서명을 조정할 수 있습니까?

A. 튜닝에는 서명이 실행되는 데 필요한 사항(예: sweep의 호스트 수)이 변경되며 작업 및 심각도 수준을 설정하는 것을 의미하지 않습니다.

CSPM은 어플라이언스에 대한 서명을 조정할 수 없습니다(어떤 버전에서도).시그니처의 작업과 심각도만 설정할 수 있습니다.다시 말해, CSPM은 어떤 심각도와 어떤 작업을 서명에 연결할지 설정할 수 있지만 어떤 작업을 발생시키는지는 설정할 수 없습니다.센서의 SigWizMenu를 사용하여 센서를 조정해야 합니다.SigWizMenu와 CSPM을 모두 사용하여 동일한 센서를 구성할 수 있습니다. 이러한 센서는 구성의 다른 부분에 영향을 주기 때문입니다.

참고: UNIX Director 버전 2.2.3 이상을 사용하는 경우 nrConfigure 유틸리티는 SigWizMenu에서 구성하는 모든 것을 구성할 수 있습니다.2.2.3으로 업그레이드한 후 SigWizMenu 대신 nrConfigure를 사용하여 서명을 조정해야 합니다.

관련 정보

- Cisco Intrusion Prevention System 제품 지원
- Cisco Secure Intrusion Detection System 설명서
- Cisco Secure Intrusion Detection System의 필드 알림
- 기술 지원 및 문서 – Cisco Systems