IBM Security QRadar Incident Forensics
버전 7.3.0

QRadar Packet Capture
사용자 안내서

IBM

참고

이 정보와 이 정보가 지원하는 제품을 사용하기 전에, 29 페이지의 『주의사항』의 정보를 읽으십시오.

제품 정보

본 문서는 본 문서의 업데이트된 버전에서 달리 대체되지 않는 한, IBM QRadar Security Intelligence Platform V7.3.0 및 후속 릴리스에 적용됩니다.

목차

이 Packet Capture 사용자 안내서의 정보

이 문서에서는 IBM® QRadar® Packet Capture를 설치하고 구성하는 데 필요한 정보를 제공합니다.

대상 독자

QRadar Packet Capture 설치를 담당하는 시스템 관리자는 네트워크 보안 개념과 디바이스 구성에 대해 잘 알고 있어야 합니다.

기술 문서

QRadar 제품 라이브러리에서 IBM Security QRadar 제품 문서를 찾으려면 IBM 보안 문서 기술 노트 액세스(www.ibm.com/support/docview.wss?rs=0&uid=swg21614644)를 참조하십시오.

고객 지원 문의

고객 지원 문의에 대한 정보는 지원 및 기술 노트 다운로드 (http://www.ibm.com/support/docview.wss?uid=swg21616144)를 참조하십시오.

우수 보안 관리제도에 대한 설명

IT 시스템 보안은 귀사 내/외부로부터의 부적절한 접근을 방지, 감지, 대응함으로써 시스템과 정보를 보호하는 일을 포함합니다. 부적절한 접근은 정보의 변경, 파괴 또는 유용을 초래하거나, 타 시스템에 대한 공격을 포함한 귀사 시스템에 대한 피해나 오용을 초래할 수 있습니다. 어떠한 IT 시스템이나 제품도 완벽하게 안전할 수 없으며, 단 하나의 제품이나 보안 조치만으로는 부적절한 접근을 완벽하게 방지하는 데 효과적이지 않을 수 있습니다. IBM 시스템, 제품 및 서비스는 합법적이며 종합적인 보안 접근방법의 일부로서 고안되며, 이러한 접근방법은 필연적으로 추가적인 실행절차를 수반하며 가장 효과적이기 위해서는 다른 시스템, 제품 또는 서비스가 필요할 수도 있습니다. IBM은 시스템, 제품 또는 서비스가 임의의 당사자의 악의적 또는 불법적 행위로부터 영향을 받지 않는다는 것을 보장하지는 않습니다.

참고:

본 프로그램의 사용은 개인 정보, 정보 보호, 고용, 전기 통신 및 저장과 관련된 법률 또는 규정을 포함하여 다양한 법률 또는 규정과 연관될 수 있습니다. IBM Security QRadar는 합법적인 목적과 합법적인 방법으로만 사용될 수 있습니다.

고객은 적용되는 법률, 규정 또는 정책에 의거하여 본 프로그램을 사용하고, 적용되는 법률, 규정 또는 정책을 준수할 모든 책임이 있다는 것에 동의합니다. 라이센스 사용자는 IBM Security QRadar의 합법적인 사용이 가능하게 하기 위해 필요한 모든 동의, 허가 및 라이센스를 이미 취득했거나 취득할 것임을 진술하고 보증합니다.

제 1 장 QRadar Packet Capture 소개

IBM Security QRadar Packet Capture는 네트워크 트래픽 캡처 및 검색 애플리케이션입니다. QRadar Packet Capture 어플라이언스는 하나의 캡처 포트(DNA0)만 가지며 10G 또는 1G SFP 트랜시버 중 하나를 설치할 수 있습니다.

QRadar Packet Capture를 사용하여 라이브 네트워크 인터페이스에서 최대 10Gbps의 비율로 네트워크 패킷을 캡처할 수 있으며 패킷 손실 없이 파일에 쓸 수 있습니다.

QRadar Packet Capture를 사용하여 시간 및 패킷 엔벨로프 데이터별로 캡처된 네트워크 트래픽을 검색할 수 있습니다. 충분한 어플라이언스 자원과 맞춤 검색을 사용하여 검색과 레코더 데이터를 데이터 유실 없이 동시에 사용할 수 있습니다.

10G 트랜시버가 있는 QRadar Packet Capture 어플라이언스는 클러스터를 지원하며, 단일 독립형 서버와 비교할 때 전체 데이터 스토리지 및 계산 기능이 확장됩니다. 1G 트랜시버가 있는 QRadar Packet Capture 어플라이언스는 클러스터를 지원하지 않습니다.

QRadar Packet Capture 기능

QRadar Packet Capture에 포함된 몇 가지 기능:

표준 PCAP 파일 형식

네트워크 트래픽을 저장하는 데 사용되는 파일 형식입니다. 파일 형식은 기존 써드파티 분석 도구와 통합됩니다.

고성능 패킷-투-디스크 기록

라이브 네트워크의 네트워크 패킷을 캡처합니다.

멀티코어 지원

QRadar Packet Capture는 멀티코어 아키텍처와 함께 사용하도록 설계되어 있습니다.

직접-IO 디스크 액세스

QRadar Packet Capture는 최대 디스크 쓰기 처리량을 얻기 위해 디스크에 대한 직접 IO 액세스를 사용합니다.

실시간 인덱싱

QRadar Packet Capture는 패킷 캡처 중에 자동으로 인덱스를 작성할 수 있습니다. 인덱스는 BPF(Berkeley Packet Filter)와 같은 구문 및/또는

HTTP 도메인이나 기본 URL 문자열로 조회되어 지정된 시간 간격으로 흥미있는 패킷을 빠르게 검색할 수 있습니다.

클러스터 가능으로 캡처 데이터 용량 증가(10G 에디션만).
데이터 노드를 사용하여 추가 스토리지 용량에 대해 클러스터를 작성할 수 있습니다.

덤프 형식

캡처 파일은 마이크로초 해상도의 시간소인을 사용하여 표준 PCAP 형식으로 저장됩니다. 캡처 파일은 파일 크기에 따라 순차적으로 저장됩니다. 캡처 파일은 디렉토리에 저장됩니다. 디렉토리의 공간이 가득 차게 되면 사전구성된 레코딩 매개변수에 따라 캡처 파일이 겹쳐쓰여집니다.

캡처 속도

패킷 캡처 어플라이언스의 경우, 네트워크 트래픽 캡처 속도는 데이터 노드가 마스터 노드에 연결되어 있는지 여부에 따라 다릅니다.

- 데이터 노드가 연결되지 않은 패킷 캡처 어플라이언스의 경우, 최대 캡처 속도는 최대 7Gbps입니다.
- 데이터 노드가 마스터 노드에 연결된 패킷 캡처 어플라이언스의 경우, 캡처 속도가 최대 10Gbps까지 증가합니다.

QRadar Packet Capture에 패킷을 전달하는 데 대한 자세한 정보는 *IBM Security QRadar* 관리 안내서를 참조하십시오.

관련 개념:

9 페이지의 제 3 장 『캡처 사용 개요』
디스크에 트래픽을 캡처하려면 캡처 애플리케이션을 시작하십시오. 레코더 구성 요소는 네트워크 트래픽 데이터를 사전구성된 디렉토리에 저장합니다. 디렉토리의 공간이 가득 차게 되면 기존 파일이 겹쳐쓰여집니다.

제 2 장 QRadar Packet Capture 설정

IBM Security QRadar Packet Capture를 사용하려면 일부 기본 구성이 필요합니다.

지원되는 웹 브라우저

다음 웹 브라우저가 지원됩니다.

- Google Chrome 버전 44.0.2403.157 이상.
- Mozilla Firefox 버전 40.0.3 이상.

네트워크 설정

QRadar Packet Capture를 원격으로 사용 가능하도록 하려면 IP 주소를 이더넷 포트 중 하나(일반적으로 eth2, eth3 또는 eth4)에 지정해야 합니다. 기본적으로 시스템은 DHCP를 사용하도록 구성됩니다. 초기 구성의 경우 VGA 호환 가능 모니터를 연결해야 할 수 있습니다.

초기 구성의 경우 다음 단계를 수행하십시오.

1. QRadar Packet Capture 어플라이언스를 켜십시오.
2. SSH 및 포트 4477을 사용하여 root 사용자로 로그인하십시오.

   기본 사용자 이름은 root입니다. 기본 비밀번호는 P@ck3t08..입니다.

   기본 비밀번호를 변경하려면 6 페이지의 『운영 체제 계정 비밀번호 변경』의 내용을 참조하십시오.
3. 시스템이 최신인지 확인하려면 IBM Fix Central(www.ibm.com/support/fixcentral/)에서 사용 가능한 소프트웨어 수정사항을 적용하십시오.
4. 자체 네트워크의 정적 IP 주소를 구성하십시오.
   a. MAC 주소 또는 eth2 인터페이스를 가져오려면 다음 명령을 입력하십시오.

      ```
      ifconfig | grep eth2
      ```

      eth0 및 eth1 인터페이스는 사용 불가능합니다. M4 xSeries 하드웨어에는 eth2를 사용하십시오.
   b. MAC 주소를 적어 두십시오.
   c. /etc/sysconfig/network-scripts/ifcfg-eth2 파일에서 설정을 편집하십시오.

- 다음 텍스트를 첫 번째 행으로 추가하십시오. DEVICE=eth2
- eth2 포트의 MAC 주소를 주석 해제하십시오. HWADDR=xx:xx:xx:xx:xx
- 다음 설정이 구성되었는지 확인하십시오. BOOTPROTO=static
- 네트워크와 관련된 정보를 사용하며 출력이 다음의 정적 예제와 같이 표시되는지 확인하십시오.

```
DEVICE=eth2
#HWADDR=xx:xx:xx:xx:xx
BOOTPROTO="static"
BROADCAST="192.168.1.255"
DNS1="0.0.0.0"
DNS2="0.0.0.0"
GATEWAY="192.168.1.2"
IPADDR="192.168.1.1"
NETMASK="255.255.255.0"
NM_CONTROLLED="no"
ONBOOT="yes"
```

5. 파일을 저장하십시오.
6. 설정을 적용하려면 다음 명령을 실행하십시오.

```
service network restart
```

7. 다음 명령을 실행하여 인터페이스 설정을 검증하십시오.

```
ifconfig | more
```

DHCP 예제: CentOS6.2의 경우 /etc/sysconfig/network-scripts/ifcfg-eth0 파일 또는 /etc/sysconfig/network-scripts/ifcfg-eth1 파일에서 다음 설정을 편집하십시오.

```
BOOTPROTO="dhcp"
NM_CONTROLLED="no"
ONBOOT="yes"
```

원격 로그인

로컬로 IP 주소를 설정한 후에 4477 포트에서 SSH를 사용하여 원격으로 로그인함으로써 어플라이언스를 관리할 수 있습니다.

사용자 라이센스 구성

QRadar Packet Capture를 사용하기 전에, QRadar Packet Capture 어플라이언스 및 QRadar Packet Capture 소프트웨어에 대한 라이센스를 구성해야 합니다.

프로시저

1. SFP 1G 트랜시버가 설치된 QRadar Packet Capture 어플라이언스에 대한 라이센싱을 구성하려면 다음 단계를 완료하십시오.

a. 마스터 노드에 대한 라이센스 키를 얻으려면 IBM 담당자에게 문의하십시오.

b. QRadar Packet Capture에서 **도움말** > **마스터 라이센스 업데이트**를 클릭하십시오.

c. 라이센스를 QRadar Packet Capture 어플라이언스에 적용하려면 값을 **라이센스 키** 필드에 붙여 넣으십시오.

d. **시스템 ID** 및 **라이센스 키**의 값을 해당 필드에 붙여 넣으십시오.

e. **마스터 라이센스 업데이트**를 클릭하여 변경사항을 적용하십시오.

2. SFP+ 10G 트랜시버가 설치된 QRadar Packet Capture 어플라이언스에 대한 라이센싱을 구성하려면 다음 단계를 완료하십시오.

a. 데이터 노드에 대한 라이센스 키를 얻으려면 IBM 담당자에게 문의하십시오.

b. QRadar Packet Capture에서 마스터 라이센스를 적용하려면 **도움말** > **마스터 라이센스 업데이트**를 클릭하십시오.

c. **라이센스 키** 및 **시스템 ID**에 대한 값을 해당 필드에 붙여 넣으십시오.

d. **마스터 라이센스 업데이트**를 클릭하여 변경사항을 적용하십시오.

e. 클러스터에 있는 데이터 노드의 수에 따라 **도움말** > **Node1**을 클릭하여 업데이트해야 합니다.

f. 데이터 노드 라이센스를 업데이트하려면 **라이센스 키** 및 **시스템 ID**의 값을 해당 필드에 붙여 넣으십시오.

g. 데이터 노드를 업데이트하려면 **Node1 라이센스 업데이트**를 클릭하여 변경사항을 적용하십시오.

사용자 관리

사용자가 IBM Security QRadar Packet Capture에 액세스하여 이를 사용하도록 하려는 경우, 사용자를 추가하고 적절한 역할을 지정하고 로그인 신임 정보를 구성해야 합니다.

시작하기 전에

root 사용자로 QRadar Packet Capture에 로그인되어 있는지 확인하십시오. 또는 sudo 명령을 사용하여 사용자를 작성할 수 있어야 합니다.

프로시저

1. 사용자를 작성하려면 다음 명령을 실행하십시오.

```
./usr/local/nc/bin/nc_user_manager add <username> <password>
<Admin|Guest>
```

기존 사용자 이름 *<username>*이 이미 있는 경우 이 명령은 실패합니다.

지정된 역할이 관리자도 아니고 게스트도 아닌 경우, 이 명령은 실패합니다.

사용자가 추가되면 제품 로그인과 REST API 로그인 둘 다에 대해 동일한 사용자 이름 및 비밀번호를 사용할 수 있습니다.

2. 사용자를 삭제하려면 다음 명령을 실행하십시오.

```
./usr/local/nc/bin/nc_user_manager delete <username> <password>
```

기존 사용자 이름 *<username>*이 이미 있는 경우 이 명령은 실패합니다.

<username> 및 *<password>*가 QRadar Packet Capture에 레코드된 항목과 일치하지 않는 경우 이 명령은 실패합니다.

사용자가 삭제되면 제품 로그인과 REST API 로그인 둘 다에 대해 동일한 사용자 이름 및 비밀번호를 사용할 수 있습니다.

운영 체제 계정 비밀번호 변경

어플라이언스를 설정한 후에 IBM Security QRadar Packet Capture의 기본 운영 체제 비밀번호를 변경하십시오.

운영 체제 계정을 변경하려면 root 사용자이어야 합니다.

QRadar Packet Capture 애플리케이션 비밀번호는 운영 체제 비밀번호와는 별도입니다.

프로시저

1. SSH를 사용하여 `root` 사용자로 로그인하십시오.

   root 사용자의 기본 비밀번호는 `P@ck3t08..`입니다.

2. `root` 사용자 계정의 비밀번호를 변경하려면 **`passwd`** *username* 명령을 사용하십시오.

QRadar Packet Capture 서버 시간을 QRadar Console 서버 시간과 동기화

IBM Security QRadar 배치의 시간 설정이 일관되게 하여 검색 및 데이터 관련 기능이 제대로 작동하도록 보장하려면 모든 어플라이언스가 QRadar Console 어플라이언스와 동기화되어야 합니다. 관리자는 QRadar Console 어플라이언스의 iptables를 업데이트한 다음 포트 37에서 rdate 통신을 수락하도록 구성해야 합니다.

시작하기 전에

QRadar Console의 IP 주소 또는 호스트 이름을 알고 있어야 합니다. nslookup을 사용하여 호스트 이름을 올바로 확인해야 합니다.

기본적으로 QRadar Packet Capture 디바이스의 시간대는 협정 세계시(UTC)로 설정되어 있습니다.

프로시저

1. SSH를 사용하여 `root` 사용자로 QRadar Packet Capture 어플라이언스에 로그인하십시오.
2. NTP(Network Time Protocol) 서비스를 해제하려면 `service ntpd stop` 명령을 입력하십시오.
3. NTP의 구성 확인을 해제하려면 `chkconfig ntpd off` 명령을 입력하십시오.
4. `crontab`(crontable) 파일을 편집하여 동기화를 cron 작업으로 스케줄하십시오.
   a. `crontab -e` 명령을 입력하십시오.
   b. 10초마다 어플라이언스가 QRadar Console과 동기화하도록 구성하려면 `*/10 * * * * rdate -s` *`Console_IP_Address`* 명령을 입력하십시오.

      Console_IP_Address 변수에 대해 IP 주소 또는 호스트 이름을 사용하십시오.
   c. 구성 변경사항을 저장하십시오.
   d. 다음 명령을 입력하여 crond를 켜십시오.

      ```
      service crond start
      chkconfig crond on
      ```
5. QRadar Console의 iptables를 사용하여 QRadar Packet Capture 디바이스의 rdate 트래픽을 허용하십시오.
   a. SSH를 사용하여 `root` 사용자로 QRadar Console 어플라이언스에 로그인하십시오.
   b. `/opt/qradar/conf/iptables.pre` 파일을 편집하십시오.
   c. 다음 명령을 입력하십시오.

      ```
      -A QChain -m tcp -p tcp --dport 37 -j ACCEPT --src <PCAP_IP address>
      ```

      여러 QRadar Packet Capture 어플라이언스가 있는 경우 각 IP 주소를 한 줄로 추가하십시오.

      예제:

      ```
      QChain -m tcp -p tcp --dport 37 -j ACCEPT --src 100.100.1.10
      QChain -m tcp -p tcp --dport 37 -j ACCEPT --src 100.100.1.11
      QChain -m tcp -p tcp --dport 37 -j ACCEPT --src 100.100.1.12
      ```

d. `iptables.pre` 파일을 저장하십시오.

e. 다음 명령을 입력하여 QRadar Console의 iptables를 업데이트하십시오.

```
./opt/qradar/bin/iptables_update.pl
```

관련 개념:

9 페이지의 제 3 장 『캡처 사용 개요』

디스크에 트래픽을 캡처하려면 캡처 애플리케이션을 시작하십시오. 레코더 구성 요소는 네트워크 트래픽 데이터를 사전구성된 디렉토리에 저장합니다. 디렉토리의 공간이 가득 차게 되면 기존 파일이 겹쳐쓰여집니다.

제 3 장 캡처 사용 개요

디스크에 트래픽을 캡처하려면 캡처 애플리케이션을 시작하십시오. 레코더 구성 요소는 네트워크 트래픽 데이터를 사전구성된 디렉토리에 저장합니다. 디렉토리의 공간이 가득 차게 되면 기존 파일이 겹쳐쓰여집니다.

문제점 해결: 데이터가 수집되지 않는 것으로 표시될 경우 연결 트래픽이 있는지 확인하십시오. 트래픽을 캡처하려면 TAP 또는 SPAN(미러) 포트를 사용해야 합니다. 스위치에서 SPAN 포트를 사용할 경우 스위치가 SPAN 포트에 더 낮은 우선순위를 지정하면 일부 패킷이 삭제될 수 있습니다.

시작하기

시스템을 설정한 후 다음 단계를 따라 IBM Security QRadar Packet Capture에 로그인하십시오.

1. 웹 브라우저를 열고 다음 URL을 입력하십시오.

   `https://`*`PCAP_IP_Address`*`:41390`

2. 다음 사용자 계정 정보를 사용하여 로그인하십시오.

   사용자: `continuum`

   비밀번호: `P@ck3t08..`

문제점 해결: 사용자가 10분이라는 기간 내에 한 행에 5회 안에 올바른 비밀번호를 제공하는 데 실패할 경우 해당 사용자는 30분 동안 잠깁니다. 사용자 계정은 시스템 관리자가 수동으로 잠금 해제할 수 있습니다.

기본적으로 캡처 상태 페이지가 표시됩니다. **캡처 시작** 또는 **캡처 중지**를 클릭하여 기록을 제어할 수 있습니다.

캡처 상태

캡처 상태 페이지에서는 다음 정보가 제공됩니다.

- **인터페이스 캡처 위치**
- **캡처 상태**
- **시작/중지 시간**
- **시스템이 캡처된 기간**
- **처리량 속도**
- **캡처된 패킷**

- **캡처된 바이트**
- **삭제된 패킷**
- **사용 가능한 스토리지 공간**

클러스터 구성에서 사용되는 각 데이터 노드의 스토리지 사용량이 표시됩니다. 네트워크 구성 문제 또는 부적절한 연결 때문에 QRadar Packet Capture 데이터 노드에 도달 불가능한 경우, 스토리지 통계 대신 슬레이브 노드가 사용되지만 현재 도달 불가능합니다.라는 메시지가 표시됩니다.

문제점 해결

구성된 캡처 인터페이스에 대한 시스템 정보를 보려면 **문제점 해결**을 클릭하십시오.

서버 정보

서버 스토리지 정보를 보려면 **서버 정보**를 클릭하십시오.

네트워크 특성화

네트워크 처리량을 그래프 형식으로 표시합니다.

기본 최대 캡처-투-디스크(capture-to-disk) 처리량은 10Gbps입니다.

캡처 히스토리

발생했거나 진행 중인 패킷 캡처 히스토리를 보십시오.

인라인 압축

포렌식 조사를 지원하기 위해 실제 디스크를 추가하지 않고도 사용 가능한 가상 스토리지 용량을 늘림으로써 원시 패킷 컨텐츠를 더 오랜 기간 보관할 수 있습니다. 이제 새로운 인라인 압축 옵션을 사용하여 더 많은 양의 데이터를 QRadar Packet Capture 어플라이언스에 저장할 수 있습니다.

압축 양은 페이로드의 압축된 비디오 컨텐츠 양과 관련이 있습니다. 예를 들어, 페이로드에 5% 압축 비디오가 있으면 압축 비율은 13:1입니다. 압축:스토리지 비율은 압축 해제된 크기와 압축된 크기 간의 비율입니다.

표 *1.* 인라인 압축 비율

압축된 비디오 페이로드의 백분율(%)	압축:스토리지 확대 비율
0	17:1
5	13:1
10	6:1
20	4:1

표 *1.* 인라인 압축 비율 *(*계속*)*

압축된 비디오 페이로드의 백분율(%)	압축:스토리지 확대 비율
40	2.4:1

관련 개념:

1 페이지의 제 1 장 『QRadar Packet Capture 소개』

IBM Security QRadar Packet Capture는 네트워크 트래픽 캡처 및 검색 애플리케이션입니다. QRadar Packet Capture 어플라이언스는 하나의 캡처 포트(DNA0)만 가지며 10G 또는 1G SFP 트랜시버 중 하나를 설치할 수 있습니다.

관련 태스크:

6 페이지의 『QRadar Packet Capture 서버 시간을 QRadar Console 서버 시간과 동기화』

IBM Security QRadar 배치의 시간 설정이 일관되게 하여 검색 및 데이터 관련 기능이 제대로 작동하도록 보장하려면 모든 어플라이언스가 QRadar Console 어플라이언스와 동기화되어야 합니다. 관리자는 QRadar Console 어플라이언스의 iptables를 업데이트한 다음 포트 37에서 rdate 통신을 수락하도록 구성해야 합니다.

제 4 장 클러스터

독립형 단일 서버 또는 서버의 클러스터로 QRadar Packet Capture 어플라이언스를 사용하십시오.

10G 에디션은 단일 독립형 서버와 비교할 때 전체 데이터 스토리지 용량 및 계산 기능이 확장된 클러스터를 지원합니다. 클러스터에는 마스터가 하나 포함되어 있습니다. 최대 두 개의 QRadar Packet Capture 데이터 노드 어플라이언스를 각 QRadar Packet Capture 마스터 시스템에 연결할 수 있습니다.

클러스터 탭은 현재 상태와 함께 두 개의 노드를 표시합니다.

기본적으로 데이터 노드는 클러스터의 파트가 아니며 사용 안함 상태를 가집니다.

데이터 노드 사용

IBM Security QRadar Packet Capture 데이터 노드를 QRadar Packet Capture 마스터 노드에 물리적으로 연결한 후에 QRadar Packet Capture 데이터 노드를 사용으로 설정해야 합니다. 사용으로 설정되고 연결된 QRadar Packet Capture 데이터 노드는 추가된 스토리지 용량 및 개선된 캡처 성능을 위해 클러스터를 작성합니다.

어플라이언스 연결에 대한 정보는 *QRadar Packet Capture* 빠른 참조 안내서를 참조하십시오.

시작하기 전에

캡처 서버가 실행 중인지 확인하십시오.

프로시저

1. 데이터 노드를 사용으로 설정하려면 다음 단계를 따르십시오.
   a. **클러스터** 탭에서 각 데이터 노드에 대해 **사용**을 선택하십시오. 상태가 **연결됨**으로 표시됩니다.
   b. 캡처 서버를 다시 시작하십시오. 이제 QRadar Packet Capture 데이터 노드를 사용할 수 있습니다.

   QRadar Packet Capture 데이터 노드가 연결되어 실행 중이며 클러스터에서 이에 대한 상태가 "연결됨"으로 변경됩니다.

마스터 노드를 데이터 노드에 연결하고 나면 대시보드에 표시된 압축된(가상) 스토리지 크기에 연결된 데이터 노드의 스토리지 크기가 포함됩니다.

2. 데이터 노드를 사용 안함으로 설정하려면 다음 단계를 따르십시오.
   a. 클러스터 탭에서 각 데이터 노드에 대해 **사용 안함**을 선택하십시오. 상태가 **연결되지 않음**으로 표시됩니다.
   b. 캡처 서버를 다시 시작하십시오. QRadar Packet Capture 데이터 노드는 이제 사용 불가능하며 더 이상 마스터와 연관되지 않습니다.

   연결이 끊긴 데이터 노드는 더 이상 데이터를 저장하지 않습니다.

   마스터 노드가 사용 안함으로 설정되고 나면 대시보드에서 압축된(가상) 스토리지 크기가 줄어듭니다.

   Data Node1 또는 Data Node2에 라이센스가 부여되면 사용한 라이센스에 따라 라이센스 컬럼이 **영구** 또는 **평가** 중 하나를 표시합니다.

제 5 장 QRadar Packet Capture 그래프

IBM Security QRadar Packet Capture에서 사용자는 라이브 또는 히스토리 그래프 중 하나를 사용하여 패킷 캡처 통계를 시각화합니다.

라이브 그래프

라이브 그래프는 현재 패킷 캡처에 대한 다음 패킷 캡처 통계를 추적합니다.

- 처리량(Gbps, 초당 기가바이트 수)
- 초당 총 패킷 수
- 초당 TCP 패킷 수
- 초당 UDP 패킷 수
- 비 UDP 트래픽에 대한 초당 패킷 수
- 시스템 이벤트 수
- 패킷 압축 비율

마우스를 그래프 위로 움직여 그래프의 해당 지점에 대한 통계를 얻으십시오.

특정 시점에 그래프를 클릭할 수 있으며, 검색 요청을 자동으로 생성할 수 있습니다. 표시 스타일 아이콘을 클릭하여 그래프의 보기를 변경할 수도 있습니다.

히스토리 그래프

히스토리 그래프는 패킷 캡처 히스토리의 장기 개요를 제공합니다. 히스토리 타임라인 옵션에는 1시간, 1일 및 1주일이 있습니다.

마우스를 그래프 위로 움직여 그래프의 해당 지점에 대한 통계를 얻으십시오.

자동으로 생성할 특정 시점에 그래프를 클릭하면 검색 요청이 자동으로 생성됩니다.

제 6 장 진단 테스트를 위해 시간 범위 내의 패킷 검색

캡처 시에 작성된 인덱스 데이터는 지정된 기간의 패킷 및 패킷 메타데이터 정보를 포함하는 패킷 캡처(pcap) 파일을 생성하는 데 사용됩니다.

제한사항: 이러한 검색은 진단 용도로만 사용됩니다. 추출 파티션을 채우지 않도록 방지하기 위해 수동 정리가 필요합니다.

프로시저

1. **검색** 페이지를 클릭하십시오.

   기본값이 이미 입력되어 있습니다.
2. 캡처된 트래픽에 대해 검색할 인터페이스를 선택하십시오.

   단일 인터페이스 구성만 있는 경우에는 자동으로 선택됩니다.
3. 검색할 시간 범위의 시작 및 종료에 대한 값을 지정하거나 기본값을 변경하십시오.
4. BPF(Berkeley Packet Filter)를 지정하십시오.

   BPF 구문을 사용하여 BPF 필터를 지정할 수 있습니다. 표현식은 하나 이상의 기초로 구성됩니다. 복합 필터 표현식은 AND, OR 및 NOT 연산자를 사용하여 빌드됩니다.

   다음 예제는 기초 필터입니다.

   ```
   ether host 00:11:22:33:44:55
   ether src host 00:11:22:33:44:55

   ip host 192.168.0.1
   ip dst host 192.168.0.1

   ip6 host 2001:0db8:85a3:0042:0000:8a2e:0371:7334
   ip6 src host 2001:0db8:85a3:0042:0000:8a2e:0371:7334

   ip net 192.168.1.0/24
   ip src net 192.168.1

   port 80
   udp port 9000
   tcp src port 80
   ```

   다음 예제는 복합 필터입니다.

   ```
   ip host 192.168.1.1 and 192.168.1.2
   ip src 192.168.1.1 and dst 192.168.1.2
   ip host 192.168.1.1 and tcp port (80 or 443)
   (ip host 192.168.1.1 or 192.168.1.2) and (port 80 or 443)
   ```

5. 추출할 패킷 수를 지정하십시오.

   추출할 패킷의 기본 최대 수는 10,000입니다. 이 수를 0으로 변경하면 타임라인 및 필터에 일치하는 모든 패킷이 추출됩니다.
6. **검색 시작**을 클릭하십시오.
7. 전체 검색 요청이 아직 실행 중인 동안 데이터에 액세스할 수 있도록 검색 페이지의 **조치** 컬럼에서 **청킹** 옵션을 사용하여 검색 요청을 더 작은 데이터 세그먼트로 분할하십시오. 먼저 PCAP 필터 번호를 지정한 후 **PCAP 파일 다운로드**를 클릭하여 검색을 요청합니다.

   데이터 세그먼트는 128MB이고, 마지막 데이터 세그먼트는 128MB보다 작을 수 있습니다.
8. 검색 큐의 상태를 보려면 **검색 요청 큐**를 확인하십시오.
9. 완료된 모든 검색의 히스토리를 보려면 **요청 로그**를 확인하십시오.
10. 수동 검색을 정리하여 포렌식 복구 프로세스를 위한 충분한 공간이 있는지 확인하십시오.
    a. root로 로그인하십시오.

       사용자 이름: root

       비밀번호: P@ck3t08..
    b. 다음 명령을 실행하십시오.

       ```
       rm -r /extraction/<name_of_search>
       ```

       <*name_of_search*> 변수는 완료된 검색 페이지의 이름 컬럼입니다.

제 7 장 캡처 전 필터 구성

캡처 전 필터는 캡처된 데이터를 디스크에 쓰기 전에 네트워크 트래픽을 필터링합니다.

프로시저

1. 캡처 전 필터를 작성하십시오.
   a. **캡처 전 필터** 메뉴를 클릭하십시오.
   b. 필터 이름 및 검색 필터 옵션에 대한 설정을 입력하십시오.

      캡처 필터는 접속사(and/or)로 연결되고 선택적으로 not이 선행되는 기초 표현식 양식을 사용합니다.

      다음 예제에서는 포트 80에 예정된 모든 트래픽이 삭제됩니다.

      ```
      not dst port 80
      ```

      다음 예제에서는 다음 두 개의 호스트에 대한 트래픽만 캡처되며 다른 모든 트래픽은 삭제됩니다.

      ```
      host 1.2.3.4 or host 1.1.1.1
      ```

   c. **추가**를 클릭하여 캡처 전 필터를 완료하십시오. 목록에 추가된 마지막 캡처 전 필터는 활성 필터입니다. 이전 필터의 히스토리도 표시됩니다.
2. 새로 추가된 필터를 활성화하려면 캡처 서버를 다시 시작하십시오.
3. **삭제**를 선택하여 필터를 영구적으로 삭제하십시오. 캡처 서버를 다시 시작해야 합니다.

제 8 장 활성 트리거 구성

활성 트리거는 사용자가 지정한 이벤트가 네트워크에서 발생할 경우 이를 사용자에게 알립니다. 예를 들어, IP 주소가 포함된 트래픽이 캡처될 때 이를 알리도록 검색 필터로 IP 주소를 지정합니다.

프로시저

1. 활성 트리거를 작성하십시오.
   a. **활성 트리거** 메뉴를 클릭하십시오.
   b. 트리거 이름 및 시간 프레임 옵션에 대한 설정을 입력하십시오.
   c. **추가**를 클릭하여 활성 트리거를 완료하십시오.

      제한사항: 최대 5개의 활성 트리거를 지정할 수 있습니다.
2. 발생에 따라 **이벤트 로그**에서 트리거 이벤트를 검토하십시오. 활성 트리거 이벤트를 클릭하면 트리거되는 이벤트에 대해 지정된 시간 매개변수 내에 자동으로 검색 요청이 생성됩니다. 검색 시간에는 이벤트 전후의 초 수가 포함됩니다.
3. **삭제**를 선택하여 구성된 트리거를 삭제하십시오.

제 9 장 QRadar Packet Capture 문제점 해결

문제점 해결은 문제점을 해결하는 체계적인 방법입니다. 문제점 해결의 목적은 무언가가 예상대로 작동하지 않는 이유를 판별하고 문제점을 해결하는 방법을 설명하는 것입니다.

QRadar Packet Capture 소프트웨어의 최신 버전이 설치되어 있습니까?

항상 소프트웨어의 최신 릴리스 버전으로 업그레이드하십시오. 소프트웨어 업데이트를 적용한 직후에 또는 새 설치 후에는 변경사항이 적용되도록 시스템을 다시 시작했는지 확인하십시오. 클러스터 구성에서는 항상 마스터와 모든 데이터 노드 시스템이 둘 다 동일한 버전으로 업그레이드되었는지 확인하십시오.

RAID 컨트롤러 및 하드 드라이브에 대해 제안된 펌웨어를 가지고 있습니까?

3650 M4 RAID 컨트롤러 및 하드 드라이브에 설치된 펌웨어 버전과 관련된 안정성 또는 성능 문제를 발견하면 최소 펌웨어 버전이 있는지 확인하십시오.

- 3650 M4의 경우, M5200 RAID 컨트롤러 펌웨어 버전: 2015년 5월 27일의 버전 24.7.0-0052 이상.

  Red Hat Linux 명령행에서 `.bin` 파일을 실행하십시오.
- IBM Lenovo의 경우, 2015년 5월 15일 이후의 버전.

  Red Hat Linux 명령행에서 `.bin` 파일을 실행하십시오.

BIOS에서 HyperThreading이 사용으로 설정되어 있습니까?

기본적으로 HyperThreading은 BIOS에서 사용으로 설정되어 있습니다. `lscpu` 명령을 사용하고 출력을 검토하여 "코어당 스레드가 2와 동일"한지 확인하십시오. 다음은 IBM 3650-M4에 대한 명령의 샘플 출력입니다.

```
[root@3650M4-001 bin]# lscpu
Architecture:          x86_64
CPU op-mode(s):        32-bit, 64-bit
Byte Order:            Little Endian
CPU(s):                40
On-line CPU(s) list:   0-39
Thread(s) per core:    2
Core(s) per socket:    10
Socket(s):             2
NUMA node(s):          2
Vendor ID:             GenuineIntel
CPU family:            6
Model:                 62
Stepping:              4
CPU MHz:               2800.000
BogoMIPS:              5592.04
Virtualization:        VT-x
L1d cache:             32K
L1i cache:             32K
L2 cache:              256K
L3 cache:              25600K
NUMA node0 CPU(s):     0-9,20-29
NUMA node1 CPU(s):     10-19,30-39
```

캡처 포트가 올바르게 연결되었습니까?

IBM Security QRadar Packet Capture 디바이스는 인터페이스 0에서만 캡처할 수 있습니다.

이더넷 네트워크 연결이 올바르게 구성되었습니까?

이더넷 인터페이스가 IP 주소에 지정되도록 하려면 연결되는 인터페이스에 대해 `ifconfig` 명령을 실행하십시오.

구성된 주소가 없으면 해당 `ifcfg-eth*` 파일을 편집하여 주소를 구성하십시오.

- 이 DHCP 예제에서, `/etc/sysconfig/network-scripts/ifcfg-`*`eth2`*의 다음 설정을 편집하고 *eth2*를 해당 설정으로 대체하십시오.

  ```
  BOOTPROTO="dhcp"
  NM_CONTROLLED="no"
  ONBOOT="yes"
  ```

- 이 정적 IP 주소 예제에서, `/etc/sysconfig/network-scripts/ifcfg-`*`eth2`*의 다음 설정을 편집하고 *eth2*를 해당 설정으로 대체하십시오.

  ```
  BOOTPROTO="static"
  BROADCAST="192.168.1.255"
  DNS1="0.0.0.0"
  DNS2="0.0.0.0"
  GATEWAY="192.168.1.2"
  ```

```
IPADDR="192.168.1.1"
NETMASK="255.255.255.0"
NM_CONTROLLED="no"
ONBOOT="yes
```

설정을 변경한 후, ifconfig 명령을 실행하여 네트워크 인터페이스를 구성하십시오.

시스템 시간이 올바르게 구성되었습니까?

기본적으로 시스템 시간은 협정 세계시(UTC)로 설정되며 NTP(Network Time Protocol) 및 공용 서버를 사용하여 올바른 시스템 시간을 유지보수하도록 구성됩니다.

시스템 하드웨어 문제가 있습니까?

1. 트래픽이 올바르게 생성되고 네트워크 인터페이스 카드(NIC)를 통해 수신되고 있는지 확인하십시오.

   인터페이스 0 연결의 바로 오른쪽에 있는 등을 보십시오. 맨 아래에 있는 등은 계속 켜져 있어야 하며, 이는 링크를 나타냅니다. 맨 위에 있는 등은 깜박여야 하며 이는 트래픽 활동을 나타냅니다.

2. /usr/local/nc/bin/dpdk_nic_bind.py –status 명령을 실행하십시오.

   이 명령의 결과는 다음 출력과 유사해야 합니다.

```
Network devices using DPDK-compatible driver
============================================
0000:0f:00.0 '82599ES 10-Gigabit SFI/SFP+ Network Connection' drv=igb_uio
unused=ixgbe
0000:0f:00.1 '82599ES 10-Gigabit SFI/SFP+ Network Connection' drv=igb_uio
unused=ixgbe
Network devices using kernel driver
===================================
0000:07:00.0 'I350 Gigabit Network Connection' if=eth2 drv=igb unused=igb_uio
*Active*
0000:07:00.1 'I350 Gigabit Network Connection' if=eth3 drv=igb unused=igb_uio
0000:07:00.2 'I350 Gigabit Network Connection' if=eth4 drv=igb unused=igb_uio
Other network devices
=====================
<none>
```

시스템이 트래픽을 캡처 중입니까?

캡처 세션이 시작된 후 시스템이 트래픽을 캡처 중인지 확인하려면 다음 방법 중 하나를 사용하십시오.

- 인터페이스 0 연결의 바로 오른쪽에 있는 등을 보십시오. 맨 위에 있는 등은 깜박여야 하며 이는 트래픽 활동을 나타냅니다.
- 네트워크 특성화 페이지에서 그래픽 출력을 보십시오.
- 명령행에서 du –h /storage0/int0 명령을 실행하십시오.

결과는 다음 출력과 유사합니다.

```
4.4G /storage0/int0/1_0
4.9G /storage0/int0/2_0
6.4G /storage0/int0/3_0
4.9G /storage0/int0/4_0
4.9G /storage0/int0/5_0
4.9G /storage0/int0/6_0
.
.
.
1.4T /storage0/int0/
```

이 명령을 반복해서 실행하면 리턴되는 서브디렉토리 수와 할당량이 늘어납니다.

QRadar Packet Capture 데이터 노드가 사용으로 설정되어 있습니까?

QRadar Packet Capture 데이터 노드가 물리적으로 마스터 노드에 연결된 경우, 마스터 서버에서 작동하도록 UI에서 사용으로 설정되어 있는지도 확인해야 합니다. 시스템은 현재 최대 두 개의 QRadar Packet Capture 데이터 노드를 지원합니다.

클러스터 탭에 QRadar Packet Capture 데이터 노드가 연결되어 사용으로 설정되어 있는지가 표시되고 **시스템 ID** 설정이 **관리** 탭 아래의 **노드(n) 라이센스 업데이트** 화면에서 누락된 경우, 특정 QRadar Packet Capture 데이터 노드에 마스터 노드와 동일한 QRadar Packet Capture 데이터 노드 소프트웨어 버전이 설치되어 있는지 확인해야 합니다. 최신 소프트웨어 버전으로 업데이트한 후에 이 요구사항이 충족되는지 확인하십시오.

root 사용자로서 다음 명령을 실행하여 QRadar Packet Capture 데이터 노드 및 마스터 노드에 설치된 소프트웨어 버전을 확인하십시오.

```
cat /root/version.txt
```

QRadar Packet Capture 데이터 노드 소프트웨어 버전은 마스터 노드에 설치된 것과 동일한 버전이어야 합니다.

QRadar Packet Capture 데이터 노드용 라이센스를 명령행으로부터 적용하는 방법은 무엇입니까?

사용자가 QRadar Packet Capture 데이터 노드에 있는지 확인하려면 root 사용자로서 다음 명령을 실행하십시오.

```
cat /root/version.txt
```

QRadar Packet Capture 데이터 노드에 연결되어 있는지 확인하려면 버전 번호의 끝에 D가 붙는지 확인하십시오(예: 7.2.7.256D).

라이센스를 QRadar Packet Capture 데이터 노드에 적용하려면 root 사용자로서 다음 스크립트를 실행하십시오. nc_set_license.sh as root

참고:

- 새 라이센스가 유효하도록 하려면 QRadar Packet Capture 데이터 노드를 다시 시작해야 합니다.
- QRadar Packet Capture 데이터 노드 제조 시 이미 라이센스가 부여된 경우, 스크립트를 실행할 필요가 없습니다. 시스템이 시작되면 즉시 라이센스가 적용됩니다.

적용한 라이센스가 유효하지 않은 경우, 다음 오류 메시지가 표시됩니다.

```
Warning: LicenseKey is *NOT* valid.
```

LEEF 2.0 로깅 형식이 무엇입니까?

LEEF(Log Event Extended Format) 메시지는 다음 형식으로 /var/log/messages 파일에 추가됩니다.

```
<DateTime> <ServerIP> LEEF: 2.0|IBM|QRadar Packet
Capture|7.2.7.256|<ID>|cat=<category> msg=<message>
```

예를 들어 패킷 캡처 서버가 IP 주소가 10.91.170.20인 시스템에서 시작될 경우, 다음 LEEF 메시지가 /var/log/messages 파일에 추가됩니다.

```
May 24 22:27:49 IP_10_91_170_20 LEEF: 2.0|IBM|QRadar Packet
Capture|7.2.7.256|Started|cat=PacketCapture
```

검색 작성 요청이 *NoSpace* 오류를 리턴하는 이유가 무엇입니까?

검색을 작성할 때 /extraction 디렉토리가 가득 차면 서버가 NoSpace 오류를 리턴합니다.

검색이 일시정지될 경우 어떤 일이 발생합니까?

/extraction 디렉토리에서 사용한 공간이 6.7GB를 초과할 경우 검색이 일시정지됩니다. 검색이 일시정지되었음을 표시하는 LEEF 메시지가 Syslog로 보내집니다. 이벤트 로그가 다음과 유사한 경고를 표시합니다.

```
!WARNING: Extraction Storage Full! Search cannot proceed!!
```

일시정지된 검색이 재개되었는지 확인하려면 오래된 이전에 완료된 검색을 삭제하여 공간을 작성해야 합니다. 이전 검색을 삭제하려면 다음 단계를 따르십시오.

1. **검색** 기본 메뉴 옵션을 클릭하십시오.
2. **검색 요청 로그** 프레임에서 **검색 삭제**를 클릭하여 이전 검색을 삭제하십시오.

주의사항

이 정보는 미국에서 제공되는 제품 및 서비스용으로 작성된 것입니다.

IBM은 다른 국가에서 이 책에 기술된 제품, 서비스 또는 기능을 제공하지 않을 수도 있습니다. 현재 사용할 수 있는 제품 및 서비스에 대한 정보는 한국 IBM 담당자에게 문의하십시오. 이 책에서 IBM 제품, 프로그램 또는 서비스를 언급했다고 해서 해당 IBM 제품, 프로그램 또는 서비스만을 사용할 수 있다는 것을 의미하지는 않습니다. IBM의 지적 재산권을 침해하지 않는 한, 기능상으로 동등한 제품, 프로그램 또는 서비스를 대신 사용할 수도 있습니다. 그러나 비IBM 제품, 프로그램 또는 서비스의 운영에 대한 평가 및 검증은 사용자의 책임입니다.

IBM은 이 책에서 다루고 있는 특정 내용에 대해 특허를 보유하고 있거나 현재 특허 출원 중일 수 있습니다. 이 책을 제공한다고 해서 특허에 대한 라이센스까지 부여하는 것은 아닙니다. 라이센스에 대한 의문사항은 다음으로 문의하십시오.

07326
서울특별시 영등포구
국제금융로 10, 3IFC
한국 아이.비.엠 주식회사
대표전화서비스: 02-3781-7114

2바이트 문자 세트(DBCS) 정보에 관한 라이센스 문의는 한국 IBM에 문의하거나 다음 주소로 서면 문의하시기 바랍니다.

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

IBM은 타인의 권리 비침해, 상품성 및 특정 목적에의 적합성에 대한 묵시적 보증을 포함하여(단, 이에 한하지 않음) 묵시적이든 명시적이든 어떠한 종류의 보증 없이 이 책을 "현상태대로" 제공합니다. 일부 국가에서는 특정 거래에서 명시적 또는 묵시적 보증의 면책사항을 허용하지 않으므로, 이 사항이 적용되지 않을 수도 있습니다.

이 정보에는 기술적으로 부정확한 내용이나 인쇄상의 오류가 있을 수 있습니다. 이 정보는 주기적으로 변경되며, 변경된 사항은 최신판에 통합됩니다. IBM은 이 책에서 설명한 제품 및/또는 프로그램을 사전 통지 없이 언제든지 개선 및/또는 변경할 수 있습니다.

이 정보에서 언급되는 비IBM 웹 사이트는 단지 편의상 제공된 것으로, 어떤 방식으로든 이들 웹 사이트를 옹호하고자 하는 것은 아닙니다. 해당 웹 사이트의 자료는 본 IBM 제품 자료의 일부가 아니므로 해당 웹 사이트 사용으로 인한 위험은 사용자 본인이 감수해야 합니다.

IBM은 귀하의 권리를 침해하지 않는 범위 내에서 적절하다고 생각하는 방식으로 귀하가 제공한 정보를 사용하거나 배포할 수 있습니다.

(i) 독립적으로 작성된 프로그램과 기타 프로그램(본 프로그램 포함) 간의 정보 교환 및 (ii) 교환된 정보의 상호 이용을 목적으로 본 프로그램에 관한 정보를 얻고자 하는 라이센스 사용자는 다음 주소로 문의하십시오.

07326
서울특별시 영등포구
국제금융로 10, 3IFC
한국 아이.비.엠 주식회사
대표전화서비스: 02-3781-7114

이러한 정보는 해당 조건(예를 들면, 사용료 지불 등)하에서 사용될 수 있습니다.

이 정보에 기술된 라이센스가 부여된 프로그램 및 이 프로그램에 대해 사용 가능한 모든 라이센스가 부여된 자료는 IBM이 IBM 기본 계약, IBM 프로그램 라이센스 계약(IPLA) 또는 이와 동등한 계약에 따라 제공한 것입니다.

인용된 성능 데이터와 고객 예제는 예시 용도로만 제공됩니다. 실제 성능 결과는 특정 구성과 운영 조건에 따라 다를 수 있습니다.

비IBM 제품에 관한 정보는 해당 제품의 공급업체, 공개 자료 또는 기타 범용 소스로부터 얻은 것입니다. IBM에서는 이러한 제품들을 테스트하지 않았으므로, 비IBM 제품과 관련된 성능의 정확성, 호환성 또는 기타 청구에 대해서는 확신할 수 없습니다. 비IBM 제품의 성능에 대한 의문사항은 해당 제품의 공급업체에 문의하십시오.

IBM이 제시하는 방향 또는 의도에 관한 모든 언급은 특별한 통지 없이 변경될 수 있습니다.

여기에 나오는 모든 IBM의 가격은 IBM이 제시하는 현 소매가이며 통지 없이 변경될 수 있습니다. 실제 판매가는 다를 수 있습니다.

이 정보에는 일상의 비즈니스 운영에서 사용되는 자료 및 보고서에 대한 예제가 들어 있습니다. 이들 예제에는 개념을 가능한 완벽하게 설명하기 위하여 개인, 회사, 상표 및 제품의 이름이 사용될 수 있습니다. 이들 이름은 모두 가공의 것이며 실제 인물 또는 기업의 이름과 유사하더라도 이는 전적으로 우연입니다.

상표

IBM, IBM 로고 및 ibm.com®은 전세계 여러 국가에 등록된 International Business Machines Corp.의 상표 또는 등록상표입니다. 기타 제품 및 서비스 이름은 IBM 또는 타사의 상표입니다. 현재 IBM 상표 목록은 웹 "저작권 및 상표 정보"(www.ibm.com/legal/copytrade.shtml)에 있습니다.

Microsoft, Windows, Windows NT 및 Windows 로고는 미국 또는 기타 국가에서 사용되는 Microsoft Corporation의 상표입니다.

제품 문서의 이용 약관

다음 이용 약관에 따라 이 책을 사용할 수 있습니다.

적용성

본 이용 약관은 IBM 웹 사이트의 모든 이용 약관에 추가됩니다.

개인적 사용

모든 소유권 사항을 표시하는 경우에 한하여 귀하는 이 책을 개인적, 비상업적 용도로 복제할 수 있습니다. 귀하는 IBM의 명시적 동의 없이 본 발행물 또는 그 일부를 배포 또는 전시하거나 2차적 저작물을 만들 수 없습니다.

상업적 사용

모든 소유권 사항을 표시하는 경우에 한하여 귀하는 이 책을 귀하 기업집단 내에서만 복제, 배포 및 전시할 수 있습니다. 귀하는 귀하의 기업집단 외에서는 IBM의 명시적 동의 없이 이 책의 2차적 저작물을 만들거나 이 책 또는 그 일부를 복제, 배포 또는 전시할 수 없습니다.

권한

본 허가에서 명시적으로 부여된 경우를 제외하고, 이 책이나 이 책에 포함된 정보, 데이터, 소프트웨어 또는 기타 지적 재산권에 대한 어떠한 허가나 라이센스 또는 권한도 명시적 또는 묵시적으로 부여되지 않습니다.

IBM은 이 책의 사용이 IBM의 이익을 해친다고 판단하거나 위에서 언급된 지시사항이 준수되지 않는다고 판단하는 경우 언제든지 부여한 허가를 철회할 수 있습니다.

귀하는 미국 수출법 및 관련 규정을 포함하여 모든 적용 가능한 법률 및 규정을 철저히 준수하는 경우에만 본 정보를 다운로드, 송신 또는 재송신할 수 있습니다.

IBM은 이 책의 내용과 관련하여 아무런 보장을 하지 않습니다. 타인의 권리 비침해, 상품성 및 특정 목적에의 적합성에 대한 묵시적 보증을 포함하여 (단 이에 한하지 않음) 묵시적이든 명시적이든 어떠한 종류의 보증 없이 현 상태대로 제공합니다.

IBM 온라인 개인정보 보호정책

SaaS(Software as a Service) 솔루션을 포함한 IBM 소프트웨어 제품(이하 "소프트웨어 오퍼링")은 제품 사용 정보를 수집하거나 일반 사용자의 사용 경험을 개선하거나 일반 사용자와의 상호 작용을 조정하거나 그 외의 용도로 쿠키나 기타 다른 기술을 사용할 수 있습니다. 많은 경우에 있어서, 소프트웨어 오퍼링은 개인 식별 정보를 수집하지 않습니다. IBM의 일부 소프트웨어 오퍼링은 귀하가 개인 식별 정보를 수집하도록 도울 수 있습니다. 본 소프트웨어 오퍼링이 쿠키를 사용하여 개인 식별 정보를 수집할 경우, 본 오퍼링의 쿠키 사용에 대한 특정 정보가 다음에 규정되어 있습니다.

본 소프트웨어 오퍼링은 배치된 구성에 따라 세션 관리 및 인증의 용도로 각 사용자의 세션 ID를 수집하는 세션 쿠키를 사용할 수 있습니다. 쿠키를 사용하지 못하도록 할 수 있지만 이 경우 쿠키를 통해 사용 가능한 기능도 제거됩니다.

본 소프트웨어 오퍼링에 배치된 구성이 쿠키 및 기타 기술을 통해 최종 사용자의 개인 식별 정보 수집 기능을 고객인 귀하에게 제공하는 경우, 귀하는 통지와 동의를 위한 요건을 포함하여 이러한 정보 수집과 관련된 법률 자문을 스스로 구해야 합니다.

이러한 목적의 쿠키를 포함한 다양한 기술의 사용에 대한 자세한 정보는 IBM 개인정보 보호정책(http://www.ibm.com/privacy/kr/ko), IBM 온라인 개인정보 보호정책(http://www.ibm.com/privacy/details/kr/ko), "쿠키, 웹 비콘 및 기타 기술" 및 "IBM 소프트웨어 제품 및 SaaS(Software-as-a-Service) 개인정보 보호정책"(http://www.ibm.com/software/info/product-privacy) 부분을 참조하십시오.