IBM Security QRadar

버전 7.3.0

아키텍처 및 배치 안내서

참고

이 정보와 이 정보가 지원하는 제품을 사용하기 전에, 51 페이지의 『주의사항』의 정보를 읽으십시오.

제품 정보

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

목차

QRadar 배치 소개

IBM® Security QRadar® 배치 안내서는 QRadar 설치를 계획하는 데 도움이 됩니다.

이 책의 사용자

이 정보는 네트워크 보안을 연구하고 관리할 책임이 있는 보안 관리자용입니다. 이 안내서를 사용하려면 사용자의 기업 네트워크 인프라와 네트워킹 관련 기술에 대한 지식이 있어야 합니다.

기술 문서

추가 기술 문서, 기술 노트, 릴리스 정보에 액세스하는 방법에 대한 정보는 IBM 보안 문서 기술 노트에 액세스(http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861)를 참조하십시오.

고객 지원 문의

고객 지원 문의에 대한 정보는 기술 노트 지원 및 다운로드 (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861)를 참조하십시오.

우수 보안 관리제도에 대한 설명

IT 시스템 보안에는 엔터프라이즈 내외의 부적절한 액세스에 대한 예방, 발견 및 대처를 통해 시스템 및 정보를 보호하는 것이 포함됩니다. 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 시스템과 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 어떠한 시스템, 제품 또는 서비스도 외부의 악의적이나 불법적 행동으로부터 안전하며 귀하의 엔터프라이즈를 이러한 외부의 악의적 또는 불법적 행동으로부터 안전하게 지킨다고 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 용도 및 방식으로만 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 QRadar를 합법적으로 사용하는 데 필요한 동의나 권한 또는 라이센스를 획득하거나 획득했다는 것을 나타냅니다.

제 1 장 QRadar 아키텍처 개요

IBM Security QRadar 배치를 계획 또는 작성하는 경우, QRadar 구성요소가 네트워크에서 작동하는 방법을 평가한 후 QRadar 배치를 계획 및 작성하는 QRadar 아키텍처에 대해 아는 것이 도움이 됩니다.

IBM Security QRadar는 실시간으로 네트워크 데이터를 수집하고, 처리하고, 집계하고 저장합니다. QRadar는 실시간 정보 및 모니터링, 경보와 오펜스, 네트워크 위협에 대한 응답을 제공함으로써 해당 데이터를 사용하여 네트워크 보안을 관리합니다.

IBM Security QRadar SIEM(Security Information and Event Management)은 IT 인프라를 실시간으로 보여주는 모듈형 아키텍처로서, 위협을 발견하고 우선수위를 지정할 때 사용할 수 있습니다. 로그와 플로우 콜렉션 및 분석 요구사항에 맞도록 QRadar를 스케일링할 수 있습니다. QRadar Risk Manager, QRadar Vulnerability Manager 및 QRadar Incident Forensics와 같은 QRadar 플랫폼에 통합 모듈을 추가할 수 있습니다.

QRadar 보안 인텔리전스 플랫폼의 조작은 세 개의 계층으로 구성되며, 크기 및 복잡도에 관계없이 QRadar 배치 구조에 적용됩니다. 다음 다이어그램은 QRadar 아키텍처를 구성하는 계층을 표시합니다.

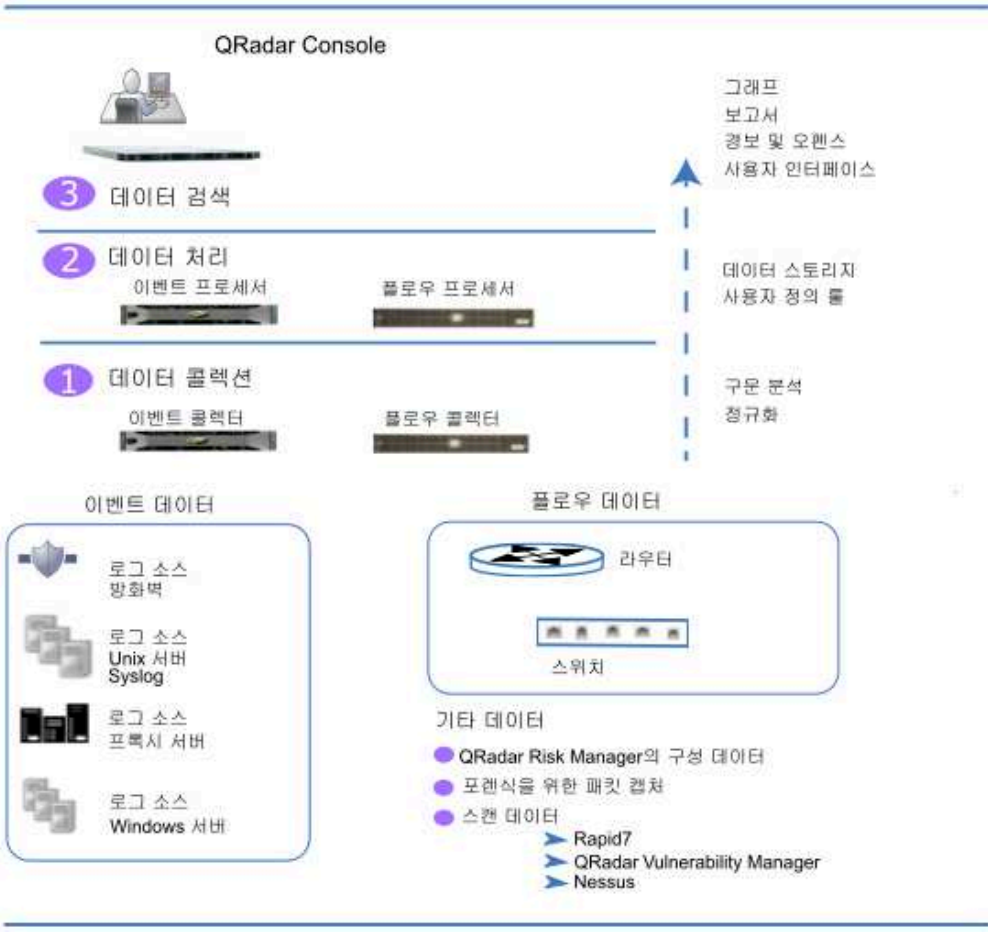


그림 *1. QRadar* 아키텍처

QRadar 아키텍처는 배치에서 구성요소의 크기 또는 수에 관계없이 같은 방식으로 동작합니다. 다이어그램에서 나타나는 다음 세 개의 계층은 QRadar 시스템의 핵심 기능을 나타냅니다.

데이터 콜렉션

데이터 콜렉션은 첫 번째 계층으로, 네트워크에서 이벤트 또는 플로우와 같은 데이터를 수집합니다. All-in-One 어플라이언스를 사용하여 네트워크에서 직접 데이터를 수집하거나 QRadar 이벤트 콜렉터 또는 QRadar QFlow Collectors와 같은 콜렉터를 사용하여 이벤트 또는 플로우 데이터를 수집할 수 있습니다. 데이터는 처리 계층으로 전달하기 전에 구문 분석하고 정규화됩니다. 원시 데이터를 구문 분석하는 경우, 정규화하여 구조화되고 사용 가능한 형식으로 제공합니다.

QRadar SIEM의 핵심 기능은 이벤트 데이터 콜렉션 및 플로우 콜렉션에 집중됩니다.

이벤트 데이터는 사용자 로그인, 이메일, VPN 연결, 방화벽 거부, 프록시 연결과 같이 사용자 환경에서 적절한 시점에 발생하는 이벤트 및 사용자 디바이스 로그에 로깅하려는 기타 이벤트를 나타냅니다.

플로우 데이터는 네트워크 상에 있는 두 호스트 사이에서의 네트워크 보기 정보 또는 세션 정보이며, QRadar는 이를 플로우 레코드로 변환합니다. QRadar는 원시 데이터를 IP 주소, 포트, 바이트 및 패킷 수로 변환 또는 정규화하고, 기타 정보는 플로우 레코드로 변환하거나 정규화하여 두 호스트 사이에서 세션을 효과적으로 나타냅니다. 플로우 콜렉터를 사용하여 플로우 정보를 수집할 뿐만 아니라 완전한 패킷 캡처는 QRadar Incident Forensics 구성요소로 사용할 수 있습니다.

데이터 처리

데이터 콜렉션 이후 두 번째 계층 또는 데이터 처리 계층에서는 이벤트 데이터 및 플로우 데이터가 오펜스 및 경보를 생성하는 CRE(Custom Rules Engine)를 통해 실행되고 데이터는 스토리지에 기록됩니다.

이벤트 프로세서 또는 플로우 프로세서를 추가하지 않고도 All-in-One 어플라이언스에서 이벤트 데이터 및 플로우 데이터를 처리할 수 있습니다. All-in-One 어플라이언스의 처리 용량이 초과되면, 이벤트 프로세서, 플로우 프로세서 또는 기타 처리 어플라이언스를 추가하여 추가 요구사항을 처리해야 합니다. 또한 더 많은 스토리지 용량이 필요할 수 있으며, 이는 데이터 노드를 추가하여 처리할 수 있습니다.

QRadar Risk Manager(QRM), QRadar Vulnerability Manager(QVM) 또는 QRadar Incident Forensics와 같은 기타 기능은 다른 유형의 데이터를 수집하고 더 많은 기능을 제공합니다.

QRadar Risk Manager는 네트워크 인프라 구성을 수집하고 네트워크 토폴로지 맵을 제공합니다. 네트워크에서 구성을 변경하고 룰을 구현하여 여러 네트워크 시나리오를 시뮬레이션함으로써 위험성 관리에 데이터를 사용할 수 있습니다.

QRadar Vulnerability Manager를 사용하면 네트워크를 스캔하고 취약성 데이터를 처리하거나 Nessus 및 Rapid7과 같은 다른 스캐너에서 수집된 취약성 데이터를 관리할 수 있습니다. 수집된 취약성 데이터를 사용하여 네트워크에서 여러 보안 위험을 식별합니다.

QRadar Incident Forensics는 상세한 포렌식 조사를 수행하고 전체 네트워크 세션을 재생하는 데 사용됩니다.

데이터 검색

세 번째 또는 맨 위 계층에서는 QRadar가 수집하고 처리하는 데이터를 검색, 분석, 보고 및 경보나 오펜스 조사에 사용할 수 있습니다. 사용자는 QRadar Console의 사용자 인터페이스에서 네트워크의 보안 관리 태스크를 검색하고 관리할 수 있습니다.

All-in-One 시스템에서는 모든 데이터를 수집하고 처리한 후 All-in-One 어플라이언스에 저장합니다.

분산 환경에서는 QRadar Console이 이벤트 및 플로우 처리나 스토리지를 수행하지 않습니다. 대신 QRadar Console이 사용자가 검색, 보고서, 경보 및 조사에 사용할 수 있는 사용자 인터페이스로서 주로 사용됩니다.

QRadar 구성요소

IBM Security QRadar 구성요소를 사용하여 QRadar 배치를 스케일링하고, 분산 네트워크에서 데이터 콜렉션 및 처리를 관리하십시오.

중요사항: 배치에서 모든 IBM Security QRadar 어플라이언스의 소프트웨어는 버전 및 수정팩 레벨이 동일해야 합니다. 혼합 버전을 사용하는 환경에서는 룰이 실행되지 않고, 오펜스가 작성 또는 업데이트되지 않고 검색 결과에 오류가 있을 수 있으므로 다른 버전의 소프트웨어를 사용하는 배치는 지원되지 않습니다.

QRadar 배치에는 다음 구성요소가 포함될 수 있습니다.

QRadar Console

QRadar Console에서는 QRadar 사용자 인터페이스, 실시간 이벤트 및 플로우 보기, 보고서, 오펜스, 자산 정보 및 관리 기능을 제공합니다.

분산 QRadar 배치에서는 QRadar Console을 사용하여 기타 구성요소를 포함하는 호스트를 관리합니다.

QRadar 이벤트 콜렉터

이벤트 콜렉터는 로컬 및 원격 로그 소스에서 이벤트를 수집하고, 원시 로그 소스 이벤트를 정규화하여 QRadar가 사용할 수 있도록 형식화합니다. 이벤트 콜렉터는 동일한 이벤트를 번들로 묶거나 통합시켜 시스템 사용량을 보존하고 이벤트 프로세서로 데이터를 전송합니다.

- 저속 WAN 링크가 있는 원격 위치에서는 QRadar 이벤트 콜렉터 1501을 사용하십시오. 이벤트 콜렉터 어플라이언스는 이벤트를 로컬로 저장하지 않습니다. 대신 스토리지를 위해 이벤트 프로세서 어플라이언스로 이벤트를 전송하기 전에 어플라이언스는 이벤트를 수집하고 구문 분석합니다.

- 이벤트 콜렉터는 간헐적 연결과 같은 WAN 한계를 극복하기 위해 대역폭 리미터와 스케줄을 사용하여 이벤트를 이벤트 프로세서에 전송할 수 있습니다.
- 이벤트 콜렉터는 연결된 이벤트 프로세서와 일치하는 EPS 라이센스에 지정됩니다.

QRadar 이벤트 프로세서

이벤트 프로세서는 하나 이상의 이벤트 콜렉터 구성요소에서 수집된 이벤트를 처리합니다. 이벤트 프로세서는 CRE(Custom Rules Engine)를 사용하여 이벤트를 처리합니다. 이벤트가 콘솔에 사전정의된 CRE 사용자 정의 룰과 일치하면, 이벤트 프로세서는 룰 응답에 정의된 조치를 실행합니다.

각 이벤트 프로세서에는 로컬 스토리지가 있고, 이벤트 데이터는 프로세서에 저장되거나 데이터 노드에 저장될 수 있습니다.

이벤트의 처리 비율은 초당 이벤트(EPS) 라이센스에 의해 판별됩니다. EPS 비율을 초과하면, 이벤트가 버퍼링되고 비율이 떨어질 때까지 이벤트 콜렉터 소스 큐에 남아 있습니다. 그러나 계속해서 EPS 라이센스 비율을 초과하고 큐가 가득 차면, 시스템은 이벤트를 제거하고 QRadar는 라이센스 EPS 비율 초과에 대한 경고를 발행합니다.

All-in-One 어플라이언스에 이벤트 프로세서를 추가한 경우, 이벤트 처리 기능은 All-in-One에서 이벤트 프로세서로 이동됩니다.

QRadar QFlow Collector

플로우 콜렉터는 SPAN 포트 또는 네트워크 TAP에 연결하여 플로우를 수집합니다. IBM Security QRadar QFlow Collector도 라우터에서의 NetFlow와 같은 외부 플로우 기반 데이터 소스 콜렉션을 지원합니다.

QRadar QFlow Collectors는 완전한 패킷 캡처 시스템이 되도록 디자인되지 않았습니다. 완전한 패킷 캡처의 경우, QRadar Incident Forensics 옵션을 검토하십시오. QRadar QFlow Collector 1310 어플라이언스는 특히 QRadar Packet Capture 어플라이언스에 패킷을 전달할 수 있고, 이를 통해 단일 패킷 소스에서 플로우 콜렉션 및 패킷 콜렉션이 가능해집니다.

자체 하드웨어에 QRadar QFlow Collector를 설치하거나 QRadar QFlow Collector 어플라이언스 중 하나를 사용할 수 있습니다.

제한사항: QRadar Log Manager는 플로우 콜렉션 또는 플로우 콜렉터를 지원하지 않으며, 이는 QRadar SIEM 배치에서만 지원됩니다.

QRadar 플로우 프로세서

플로우 프로세서는 하나 이상의 QRadar QFlow Collector 어플라이언스로부터 플로우를 처리합니다. 플로우 프로세서 어플라이언스도 네트워크에 있는 라우터로부터 NetFlow, J-Flow 및 sFlow와 같은 직접적인 외부 네트워크 플로우를 수집할 수 있습니다. 플로우 프로세서 어플라이언스를 사용하면 QRadar 배치를 스케일링하여 더 높은 분당 플로우(FPM) 비율을 관리할 수 있습니다. 플로우 프로세서에는 온보드 플로우 프로세서 및 플로우 데이터에 대한 내부 스토리지가 포함됩니다. All-in-One 어플라이언스에 플로우 프로세서를 추가하는 경우, 처리 기능은 All-in-One 어플라이언스에서 플로우 프로세서로 이동됩니다.

QRadar 데이터 노드

데이터 노드를 사용하면 기존 및 새 QRadar 배치에서 요청 시 필요에 따라 스토리지와 처리 용량을 추가할 수 있습니다. 데이터 노드는 검색 조회를 실행하기 위한 더 많은 하드웨어 자원을 제공함으로써 배치에서 검색 속도를 높이는 데 도움이 됩니다.

QRadar 구성요소 관리에 대한 자세한 정보는 *IBM Security QRadar* 관리 안내서의 내용을 참조하십시오.

QRadar 어플라이언스 스펙

다음 표에서는 배치에서 특정 QRadar 어플라이언스를 사용하는 경우에 대한 안내를 제공합니다.

표 *1. QRadar* 어플라이언스 개요

어플라이언스	설명
QRadar 2100	10명 - 200명 직원이 있는 배치를 위한 확장 불가능 솔루션.
QRadar 3105(All-in-One)	QRadar 2100을 통해 용량을 증가시키며 이벤트 프로세서와 플로우 프로세서를 추가하는 기능을 제공합니다.
QRadar 3105(콘솔)	배치에서 처리하는 초당 이벤트(EPS)가 5000을 초과하는 경우 분배된 이벤트 프로세서와 함께 QRadar 3105(콘솔)를 사용해야 합니다. QRadar 3105(콘솔)에서는 오프보드 이벤트 처리와 스토리지를 사용하여 보고서, 검색 결과, 빠른 UI 조치에 사용할 자원을 확보합니다.
QRadar 3128(All-in-One)	QRadar 3105(All-in-One)를 통해 용량을 증가시킵니다.
QRadar 3128(콘솔)	QRadar 3105(콘솔)를 통해 용량을 증가시킵니다.
xx05 콜렉터 및 프로세서	12개의 프로세서 64GB의 RAM 6.2TB의 사용 가능한 스토리지

표 *1. QRadar* 어플라이언스 개요 *(*계속*)*

어플라이언스	설명
xx28 콜렉터 및 프로세서	28개의 프로세서 128GB의 RAM 40TB의 사용 가능한 스토리지 성능을 향상시키려면 xx28 콜렉터 및 프로세서와 QRadar 3128(콘솔)을 연결하십시오.

QRadar 어플라이언스에 대한 자세한 정보는 *IBM Security QRadar* 하드웨어 안내서를 참조하십시오.

QRadar 이벤트 및 플로우

IBM Security QRadar SIEM의 핵심 기능은 플로우와 이벤트를 모니터링하여 네트워크 보안을 관리하는 것입니다.

이벤트 데이터와 플로우 데이터 사이의 중요한 차이점은 이벤트는 특정 시간에서 발생하고 그러면 발생한 때 로깅됩니다. 이벤트는 일반적으로 사용자 로그인 또는 VPN 연결과 같은 특정한 동작의 로그입니다. 플로우 데이터는 세션 내에서의 활동에 따라 초, 분, 시 또는 일 동안 지속될 수 있는 네트워크 보기의 레코드입니다. 예를 들어 웹 요청이 다중 파일(예: 이미지, 광고, 비디오)을 다운로드하고 5초에서 10초 동안 지속되거나 Netflix 영화를 보는 사용자가 최대 몇 시간 동안 지속되는 네트워크 세션에 있을 수도 있습니다. 플로우는 두 호스트 사이에서의 네트워크 보기 레코드입니다.

이벤트

QRadar는 네트워크 상에 있는 로그 소스에서 이벤트 로그를 채택합니다. 로그 소스는 이벤트 로그를 작성하는 방화벽 또는 IPS(intrusion protection system)와 같은 데이터 소스입니다.

QRadar는 syslog, syslog-tcp 및 SNMP와 같은 프로토콜을 사용하여 로그 소스에서 이벤트를 채택합니다. QRadar는 SCP, SFTP, FTP, JDBC, Check Point OPSEC 및 SMB/CIFS와 같은 프로토콜을 사용하여 이벤트를 검색하는 아웃바운드 연결을 설정할 수도 있습니다.

이벤트 파이프라인

QRadar Console에서 이벤트 데이터를 보고 사용하기 전에, 로그 소스에서 이벤트를 수집하고 이벤트 프로세서가 이를 처리합니다. QRadar All-in-One 어플라이언스는 이벤트 콜렉터 및 이벤트 프로세서의 역할을 수행하며, QRadar Console의 역할도 수행합니다.

QRadar는 전용 이벤트 콜렉터 어플라이언스를 사용하거나 All-in-One 어플라이언스에서 이벤트 콜렉션 서비스 및 이벤트 처리 서비스가 실행하는 All-in-One 어플라이언스를 사용하여 이벤트를 수집합니다.

다음 다이어그램은 이벤트 파이프라인의 계층을 표시합니다.

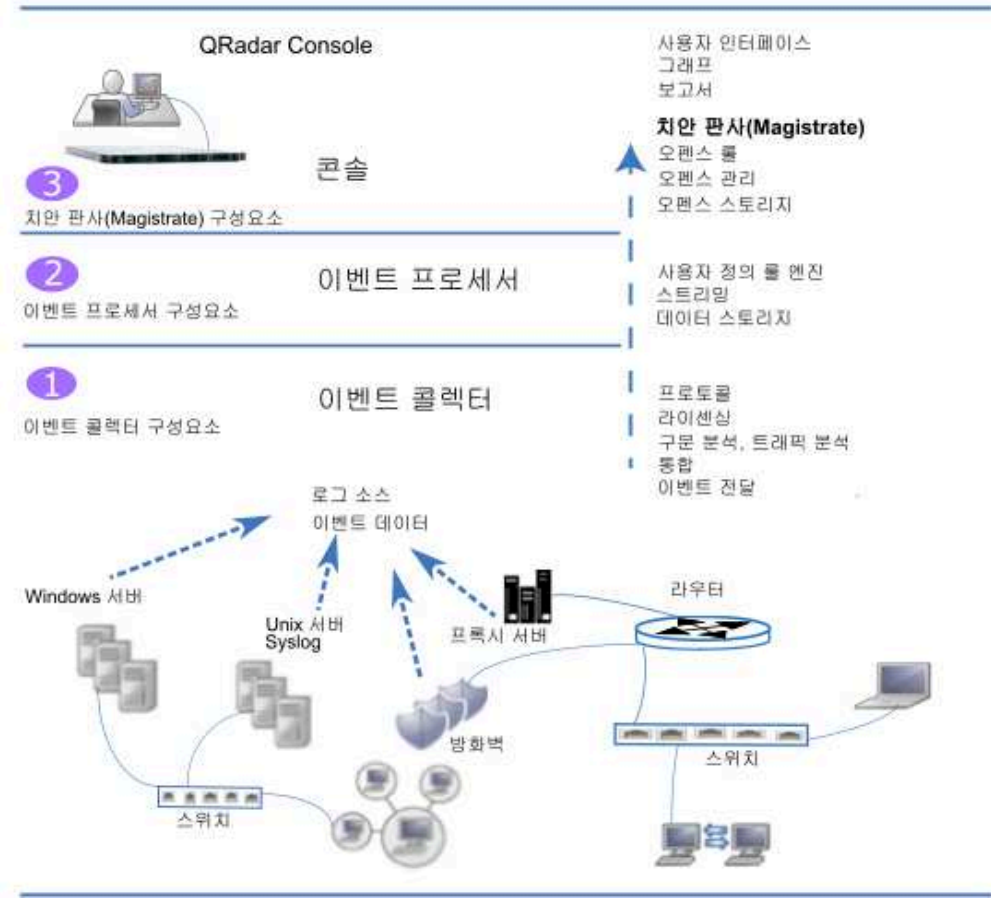


그림 2. 이벤트 파이프라인

이벤트 콜렉션

이벤트 콜렉터 구성요소는 다음 기능을 완료합니다.

- 프로토콜

  Syslog, JDBC, OPSEC, 로그 파일 및 SNMP와 같은 로그 소스 프로토콜에서 데이터를 수집합니다.

- 라이센스 조절

  시스템으로 들어오는 이벤트 수를 모니터하여 입력 큐 및 EPS 라이센스를 관리합니다.

- 구문 분석

소스 디바이스에서 원시 이벤트를 가져와 QRadar 사용 가능 형식으로 필드를 구문 분석합니다.

- 로그 소스 트래픽 분석 및 자동 감지

  자동 감지를 지원하는 DSM에 구문 분석하고 정규화한 이벤트 데이터를 적용합니다.

- 통합

  이벤트 사이의 공통 속성을 기반으로 이벤트를 구문 분석한 후 통합합니다.

- 이벤트 전달

  시스템의 라우팅 룰을 적용하여 오프사이트 대상, 외부 Syslog 시스템, JSON 시스템 및 기타 SIEM으로 데이터를 전달합니다.

이벤트 콜렉터에 방화벽과 같은 로그 소스로부터 이벤트가 수신되면, 이벤트는 처리를 위해 입력 큐에 배치됩니다.
큐의 크기는 사용되는 프로토콜 또는 메소드에 따라 다르며, 이 큐에서 이벤트를 구문 분석하고 정규화합니다. 정규화 프로세스에서는 QRadar가 사용할 수 있는 IP 주소와 같은 필드가 있는 형식으로 원시 데이터를 변환합니다.

QRadar는 헤더에 포함되는 소스 IP 주소 또는 호스트 이름으로 알려진 로그 소스를 인식합니다.
QRadar는 이벤트를 구문 분석하고 알려진 로그 소스에서 레코드로 통합시킵니다. 이전에 감지되지 않았던 신규이거나 알려지지 않은 로그 소스의 이벤트는 트래픽 분석(자동 감지) 엔진으로 경로 재지정됩니다.

새 로그 소스가 감지되면, 로그 소스를 추가하기 위한 구성 요청 메시지가 QRadar Console로 전송됩니다. 자동 감지가 사용 안함으로 설정되거나 로그 소스 라이센스 한도를 초과하는 경우, 새 로그 소스는 추가되지 않습니다.

이벤트 처리

이벤트 프로세서 구성요소는 다음 기능을 완료합니다.

- CRE(Custom Rules Engine)

  CRE(Custom Rules Engine)는 QRadar가 수신한 이벤트를 처리하고, 정의된 룰과 비교하고, 시간이 경과하면서 인시던트에 관련된 시스템을 계속 추적하고, 사용자에게 알림을 생성할 책임이 있습니다. 이벤트가 룰과 일치하면, 이벤트 프로세서에서 특정 이벤트가 룰을 트리거하는 QRadar Console의 치안 판사(Magistrate)로 알림이 전송됩니다. QRadar Console의 치안 판사(Magistrate) 구성요소는 오펜스를 작성

하고 관리합니다. 룰이 트리거되면, 알림, syslog, SNMP, 이메일 메시지, 새 이벤트 및 오펜스와 같은 응답 또는 조치가 생성됩니다.

- 스트리밍

  사용자가 **로그 보기** 탭에서 실시간으로 이벤트를 보는 경우(스트리밍) QRadar Console로 실시간 이벤트 데이터가 전송됩니다. 스트리밍된 이벤트는 데이터베이스에서 제공하지 않습니다.

- 이벤트 스토리지(Ariel)

  데이터가 분 단위로 저장되는 이벤트를 위한 시계열 데이터베이스. 이벤트가 처리되면 데이터가 저장됩니다.

이벤트 콜렉터는 CRE(Custom Rules Engine)에 의해 이벤트가 처리되는 이벤트 프로세서로 정규화된 이벤트 데이터를 전송합니다. 이벤트가 QRadar Console에 사전정의된 CRE 사용자 정의 룰과 일치하면, 이벤트 프로세서는 룰 응답에 정의된 조치를 실행합니다.

QRadar Console의 치안 판사(Magistrate)

치안 판사(Magistrate) 구성요소는 다음 기능을 완료합니다.

- 오펜스 룰

  이메일 알림 생성과 같이 오펜스를 모니터하고 이에 대해 조치합니다.

- 오펜스 관리

  활성 오펜스를 업데이트하고, 오펜스의 상태를 변경하고, **오펜스** 탭에서 오펜스 정보에 대한 사용자 액세스를 제공합니다.

- 오펜스 스토리지

  Postgres 데이터베이스에 오펜스 데이터를 기록합니다.

MPC(Magistrate Processing Core)는 여러 이벤트 프로세서 구성요소의 이벤트 알림을 오펜스와 연관시키는 기능을 수행합니다. QRadar Console 또는 All-in-One 어플라이언스에만 치안 판사(Magistrate) 구성요소가 있습니다.

플로우

QRadar 플로우는 IP 주소, 포트, 바이트 및 패킷 수, 기타 데이터를 플로우 레코드로 정규화시켜 네트워크 보기를 나타내며, 이 플로우 레코드는 두 호스트 사이의 네트워크 세션에 대한 레코드입니다. 플로우 정보를 수집하고 작성하는 QRadar의 구성요소를 QFlow라고 합니다.

QRadar 플로우 콜렉션은 완전한 패킷 캡처가 아닙니다. 여러 시간 간격(분)에 걸쳐 있는 네트워크 세션의 경우, 플로우 파이프라인은 바이트 및 패킷과 같은 지

표의 현재 데이터를 가진 레코드를 각 분 끝에서 보고합니다. "첫 번째 패킷 시간"은 같지만 "마지막 패킷 시간" 값은 시간 경과에 따라 점점 증가하는 여러 레코드(분당)가 QRadar에 있을 수 있습니다.

플로우 콜렉터가 고유한 소스 IP 주소, 대상 IP 주소, 소스 포트, 대상 포트 및 기타 특정 프로토콜 옵션을 가지고 있는 첫 번째 패킷을 발견하면 플로우가 시작됩니다.

새 패킷 각각을 평가합니다. 바이트와 패킷의 수가 플로우 레코드의 통계 카운터에 추가됩니다. 간격의 끝에서, 플로우의 상태 레코드가 플로우 프로세서로 전송되고 플로우의 통계 카운터는 재설정됩니다. 구성된 시간 내에 플로우에 대한 활동을 발견하지 못하면 플로우가 끝납니다.

QFlow는 다음 내부 또는 외부 소스로부터의 플로우를 처리할 수 있습니다.

- 외부 소스는 netflow, sflow, jflow와 같은 플로우 소스입니다.

  외부 소스는 QRadar 플로우 프로세서 1705 어플라이언스와 같은 전용 플로우 콜렉터 또는 플로우 프로세서로 전송될 수 있습니다. 플로우를 빌드하기 위해 모든 패킷이 처리되는 것은 아니므로 외부 소스에서 많은 CPU 처리가 필요하지 않습니다. 이 구성에는 플로우 데이터를 모두 수신하고 작성하는 플로우 콜렉터 및 플로우 프로세서가 있을 수 있습니다. 더 작은 환경(50Mbps 이하)에서는 All-in-One 어플라이언스가 모든 데이터 처리를 수행할 수도 있습니다.
- 플로우 콜렉터는 SPAN 포트 또는 네트워크 TAP에 연결하여 내부 플로우를 수집합니다.

  QRadar QFlow Collector 1310은 캡처 카드에서 패킷 캡처 어플라이언스로 전체 패킷을 전달하지만 전체 패킷 자체를 캡처하지는 않습니다.

다음 다이어그램은 네트워크에서 플로우를 수집하기 위한 옵션을 표시합니다.

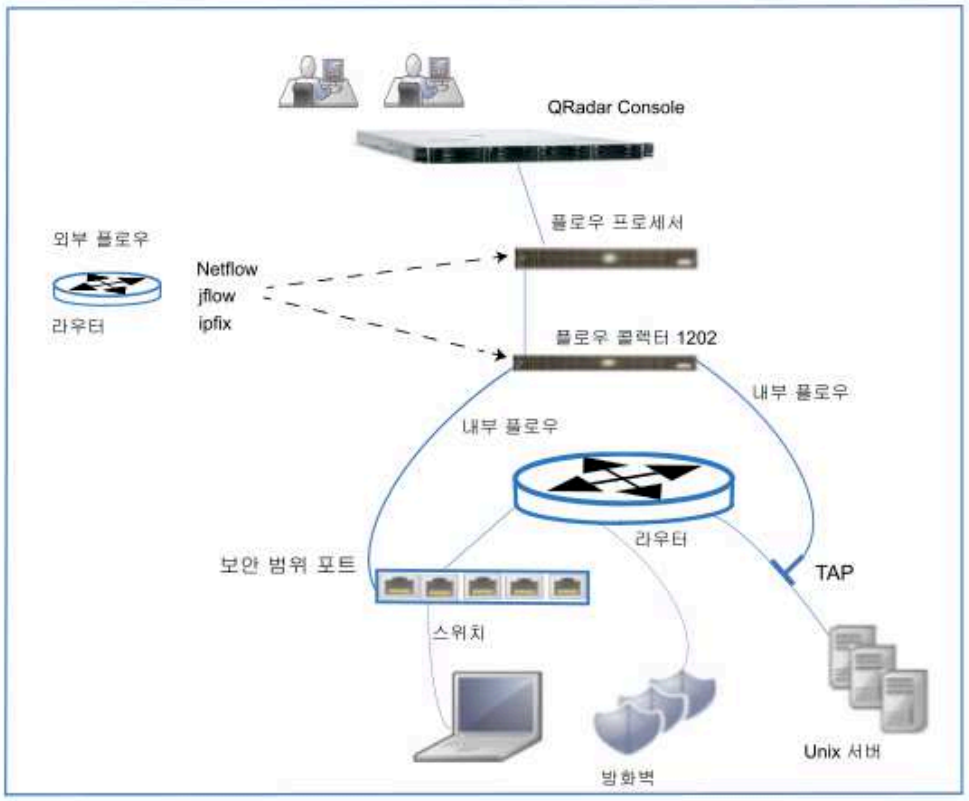


그림 *3. QRadar* 플로우

플로우 파이프라인

플로우 콜렉터는 SPAN, TAP 및 모니터 세션과 같은 모니터 포트에서 수집하거나 netflow, sflow, jflow와 같은 외부 플로우 소스에서 수집한 원시 패킷에서 플로우 데이터를 생성합니다. 그런 다음 이 데이터는 QRadar 플로우 형식으로 변환된 후 처리를 위해 파이프라인으로 보내집니다.

플로우 프로세서는 다음 기능을 실행합니다.

- 플로우 중복 제거

  플로우 중복 제거는 여러 플로우 콜렉터가 플로우 프로세서 어플라이언스에 데이터를 제공하는 경우 중복 플로우를 제거하는 프로세스입니다.

- 비대칭 재결합

  데이터가 비대칭적으로 제공될 경우 각 플로우의 양측을 결합하는 기능을 수행합니다. 이 프로세스는 양측의 플로우를 인식하고 이들을 하나의 레코드에 결합시킬 수 있습니다. 그러나 가끔은 플로우에 한 측만 존재합니다.

- 라이센스 조절

시스템으로 수신되는 플로우의 수를 모니터하여 입력 큐와 라이센스를 관리합니다.

- 전달

  오프사이트 대상, 외부 Syslog 시스템, JSON 시스템 및 기타 SIEM으로의 플로우 데이터 전송과 같은 시스템의 라우팅 룰을 적용합니다.

플로우 데이터는 CRE(Custom Rules Engine)를 통해 전달되고, 구성된 룰을 기준으로 연관되며 이 상관관계를 기반으로 오펜스가 생성될 수 있습니다. **오펜스** 탭에서 오펜스를 볼 수 있습니다.

제 2 장 QRadar 배치 개요

IBM Security QRadar 아키텍처는 모든 소프트웨어 구성요소가 단일 시스템에서 실행되는 단일 호스트 배치에서 이벤트 콜렉터 및 플로우 콜렉터, 데이터 노드, 이벤트 프로세서 및 플로우 프로세서와 같은 어플라이언스가 특정 역할을 담당하는 다중 호스트까지 크기와 토폴로지가 다양한 배치를 지원합니다.

첫 번째 배치 예제의 주요 초점은 중간 크기 회사를 위한 단일 All-in-One 어플라이언스 배치에 대해 설명하는 것입니다. 이후 예제는 회사가 확장되면서 배치 옵션에 대해 설명합니다. 예제에서는 플로우 프로세서, 이벤트 콜렉터 및 데이터 노드와 같은 QRadar 구성요소를 추가하는 경우 및 특정 구성요소가 공통적으로 위치해야 하는 경우에 대해 설명합니다.

QRadar 배치에 대한 요구사항은 네트워크에서 분석하려는 모든 데이터를 처리하고 저장하기 위해 선택한 배치의 용량에 따라 달라집니다.

배치를 계획하기 전에 다음 질문을 고려하십시오.

- 회사에서 인터넷을 어떻게 사용합니까? 다운로드만큼 업로드합니까? 사용량이 증가하면 잠재적인 보안 문제에 대한 노출이 증가할 수 있습니다.
- 모니터링해야 하는 초당 이벤트(EPS) 및 분당 플로우(FPM)은 얼마입니까?

  EPS 및 FPM 라이센스 용량 요구사항은 배치가 증가하면서 함께 늘어납니다.
- 저장해야 하는 정보의 양과 보존 기간은 얼마입니까?

다음 다이어그램은 QRadar 배치에서 이벤트 및 플로우 데이터를 수집, 처리 및 저장하기 위해 사용할 수 있는 QRadar 구성요소를 표시합니다. All-in-One 어플라이언스에는 데이터 콜렉션, 처리, 스토리지, 모니터링, 검색, 보고서 및 오펜스 관리 기능이 포함됩니다.

이벤트 콜렉터는 네트워크의 로그 소스에서 이벤트 데이터를 수집한 후 이벤트 데이터를 이벤트 프로세서로 전송합니다. 플로우 콜렉터는 스위치 SPAN 포트와 같은 네트워크 디바이스에서 플로우 데이터를 수집한 후 데이터를 플로우 프로세서로 전달합니다. 두 프로세서 모두 콜렉터로부터의 데이터를 처리하고 QRadar Console에 데이터를 제공합니다. 프로세서 어플라이언스가 데이터를 저장할 수 있지만 데이터 노드를 사용하여 데이터를 저장할 수도 있습니다. QRadar Console 어플라이언스는 QRadar 배치의 모니터링, 데이터 검색, 보고, 오펜스 관리 및 관리에 사용됩니다.

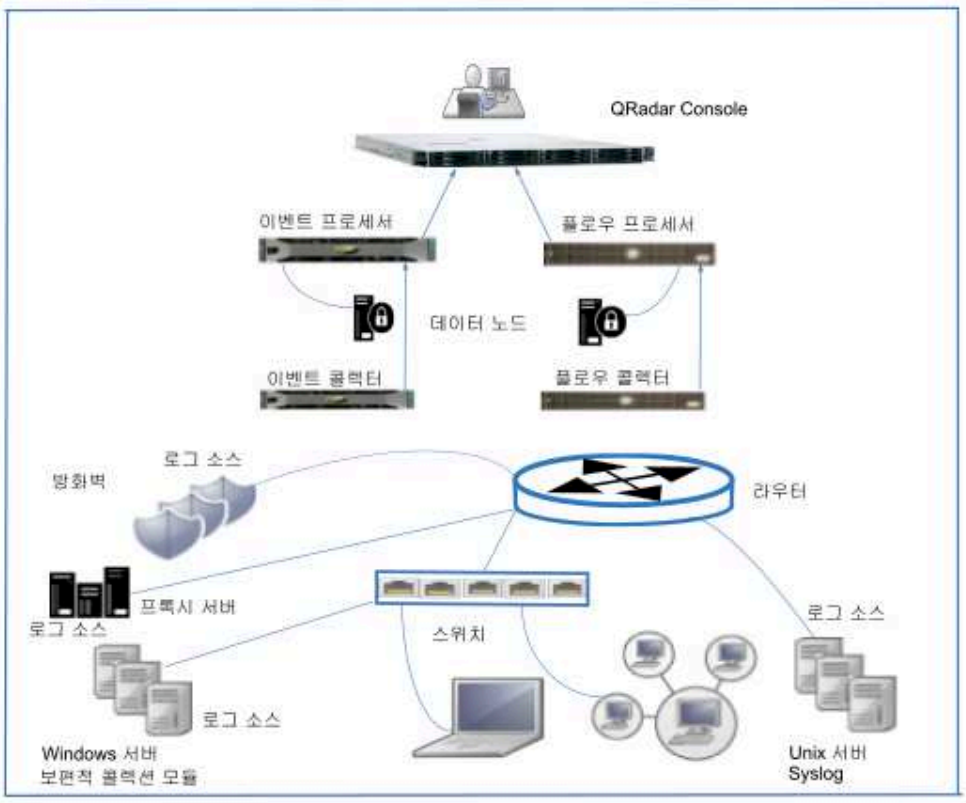


그림 *4. QRadar* 이벤트 및 플로우 구성요소

All-in-One 배치

단일 호스트 QRadar 배치에는, 네트워크에서 syslog 이벤트 데이터 로그와 같은 데이터와 Windows 이벤트, 플로우 데이터를 수집하는 단일 서버인 All-in-One QRadar 어플라이언스가 있습니다.

All-in-One 어플라이언스는 인터넷에 자주 노출되지 않는 중기업이나 테스트 및 평가 목적에 적합합니다. 단일 서버 배치는 인증 서비스 및 방화벽 활동과 같은 네트워크 보기 및 이벤트를 모니터링하는 회사에 적합합니다.

All-in-One 어플라이언스는 라이센스와 시스템의 하드웨어 스펙으로 결정되는 특정 기능까지 사용자에게 필요한 기능을 제공합니다. 예를 들어 QRadar 3105(All-in-One)는 보통 5000 초당 이벤트(EPS) 및 200,000 분당 플로우(FPM)까지 처리하는 반면, QRadar 3128(All-in-One)은 보통 15,000 EPS 및 300,000 FPM까지 처리합니다.

제조업체 회사는 단일 QRadar 서버를 배치합니다.

직원이 1000명 미만인 중간 크기의 제조업체입니다. QRadar 3105 All-in-One 어플라이언스를 배치하여 이벤트 및 플로우 데이터를 수집, 처리 및 모니터링합니다. 해당 배치에서는 최대 5,000 초당 이벤트(EPS) 및 200,000 분당 플로우(FPM)까지 수집할 수 있습니다.

다음 다이어그램에서는 이벤트 및 플로우 소스에서 데이터를 수집하고, 데이터를 처리하고, 보안 위협을 검색, 모니터링 및 이에 응답할 수 있는 웹 애플리케이션을 제공하는 All-in-One 어플라이언스를 표시합니다.

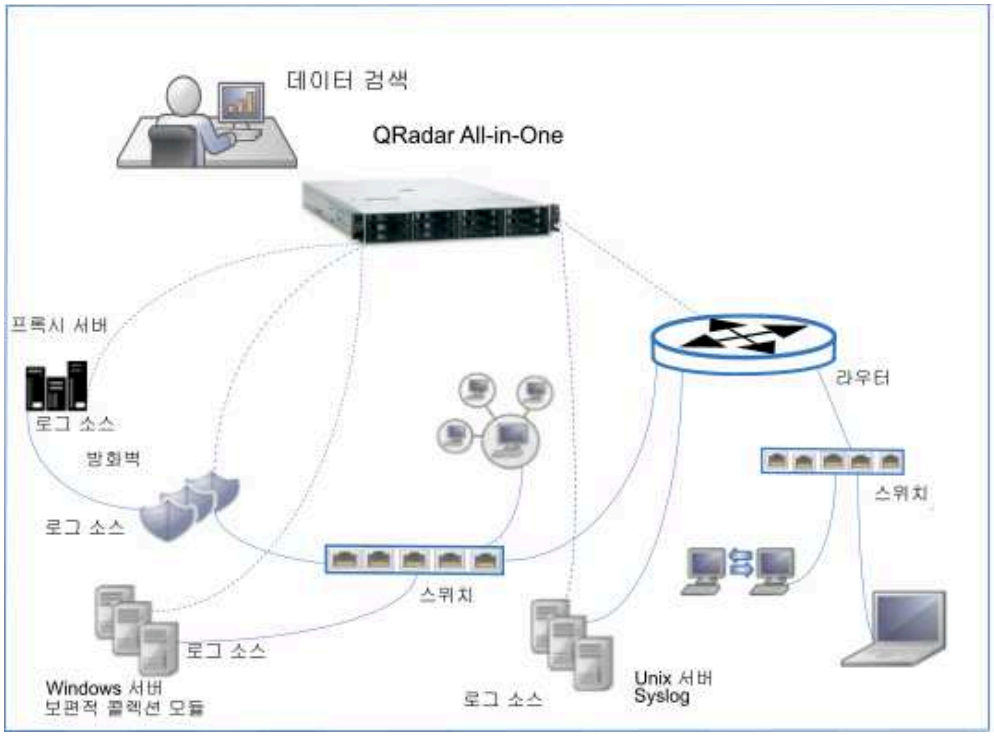


그림 *5. All-in-One* 배치

QRadar All-in-One 어플라이언스는 다음 태스크를 수행합니다.

- 이벤트 및 네트워크 플로우 데이터를 수집하고 QRadar가 사용할 수 있는 데이터 형식으로 데이터를 정규화합니다.
- 데이터를 분석 및 저장하고 회사에 보안 위협을 알립니다.
- QRadar 웹 애플리케이션에 대한 액세스를 제공합니다.

데이터 소스가 커지거나 처리 또는 스토리지에 대한 요구사항이 증가하면 어플라이언스를 추가하여 배치를 확장시킬 수 있습니다.

배치를 확장하여 많은 용량 추가

사용자 비즈니스에서 처리 또는 데이터 스토리지 용량 부족으로 인해 또는 특정 데이터 콜렉션 요구사항이 있는 경우 IBM Security QRadar All-in-One 어플라이언스의 능력 이상으로 배치를 작성하거나 확장할 수 있습니다.

QRadar 배치의 토폴로지 및 컴포지션은 네트워크에서 분석하려는 모든 데이터를 수집, 처리 및 저장하는 해당 배치의 기능과 용량의 영향을 받습니다.

배치에서 처리해야 하는 초당 이벤트(EPS) 또는 분당 플로우(FPM)을 대략적으로 추정하려면, 방화벽, 프록시 서버 및 Windows 상자에서 수집되는 로그의 크기를 사용하십시오.

All-in-One 배치에 이벤트 또는 플로우 콜렉터를 추가하는 이유

다음 조건에서는 배치에 플로우 또는 이벤트 콜렉터를 추가해야 합니다.

- 데이터 콜렉션 요구사항이 All-in-One 어플라이언스의 콜렉션 능력을 초과합니다.
- All-in-One 어플라이언스 설치 위치와 다른 위치에서 이벤트 및 플로우를 수집해야 합니다.
- All-in-One에서 연결 속도가 50Mbps보다 빠른 대형이거나 더 빠른 비율 패킷 기반 플로우 소스를 모니터링 중입니다.

3128 All-in-One 어플라이언스는 최대 15,000 초당 이벤트(EPS) 및 300,000 분당 플로우(FPM)까지 수집할 수 있습니다. 콜렉션 요구사항이 더 크면 이벤트 콜렉터 및 플로우 콜렉터를 배치에 추가할 수 있습니다. 예를 들어 최대 3Gbps까지 수집하는 QRadar QFlow Collector 1202를 추가할 수 있습니다.

All-in-One 어플라이언스는 수집되는 이벤트 및 플로우를 처리합니다. 이벤트 콜렉터 및 플로우 콜렉터를 추가하면 All-in-One 어플라이언스가 검색 및 기타 보안 태스크에 사용하는 처리를 사용할 수 있습니다.

패킷 기반 플로우 소스에서는 플로우 프로세서에 연결되거나 플로우 프로세서 어플라이언스가 없는 배치의 All-in-One 어플라이언스에 연결되는 플로우 콜렉터가 필요합니다. NetFlow 또는 IPFIX와 같은 외부 플로우 소스를 수집하거나 플로우 프로세서 또는 All-in-One 어플라이언스에서 직접 수집할 수 있습니다.

배치에 원격 콜렉터 추가

로컬로 더 많은 이벤트를 수집하고 원격 위치에서는 이벤트 및 플로우를 수집해야 하는 경우 QRadar 이벤트 콜렉터 또는 QRadar 플로우 콜렉터를 추가하여 배치를 확장하십시오.

예를 들어 QRadar All-in-One 배치가 있는 제조업체 회사이고 전자 상거래 및 원격 영업 사무실을 추가합니다. 이제 보안 위협에 대해 모니터링하고 PCI 감사도 수행해야 합니다.

더 많은 직원을 고용하고 인터넷 사용은 대부분 다운로드에서 직원과 인터넷 사이에서의 양방향 트래픽으로 변경됩니다. 다음은 회사에 대한 세부사항입니다.

- 현재 초당 이벤트(EPS) 라이센스는 1000 EPS입니다.
- 영업 사무실에서 이벤트 및 플로우를 수집하고 전자 상거래 플랫폼에서는 이벤트를 수집하려 합니다.
- 전자 상거래 플랫폼의 이벤트 콜렉션에서는 최대 2000 초당 이벤트(EPS)가 필요합니다.
- 원격 영업 사무실의 이벤트 콜렉션에서는 최대 2000 초당 이벤트(EPS)가 필요합니다.
- 원격 사무실에서 플로우를 수집하기에 분당 플로우(FPM) 라이센스가 충분합니다.

다음 조치를 수행하십시오.

1. 본사에서 전자 상거래 플랫폼을 추가한 후 원격 영업 사무실에서 엽니다.
2. 인터넷을 통해 본사의 All-in-One 어플라이언스에 데이터를 전송하는 이벤트 콜렉터 및 플로우 콜렉터를 원격 영업 사무실에 설치합니다.
3. 원격 사무실에서 수집되는 추가 이벤트의 요구사항에 맞도록 EPS 라이센스를 1000 EPS에서 5000 EPS로 업그레이드합니다.

다음 다이어그램은 이벤트 콜렉터 및 플로우 콜렉터가 원격 사무실에 추가되는 경우의 예제 배치를 표시합니다.

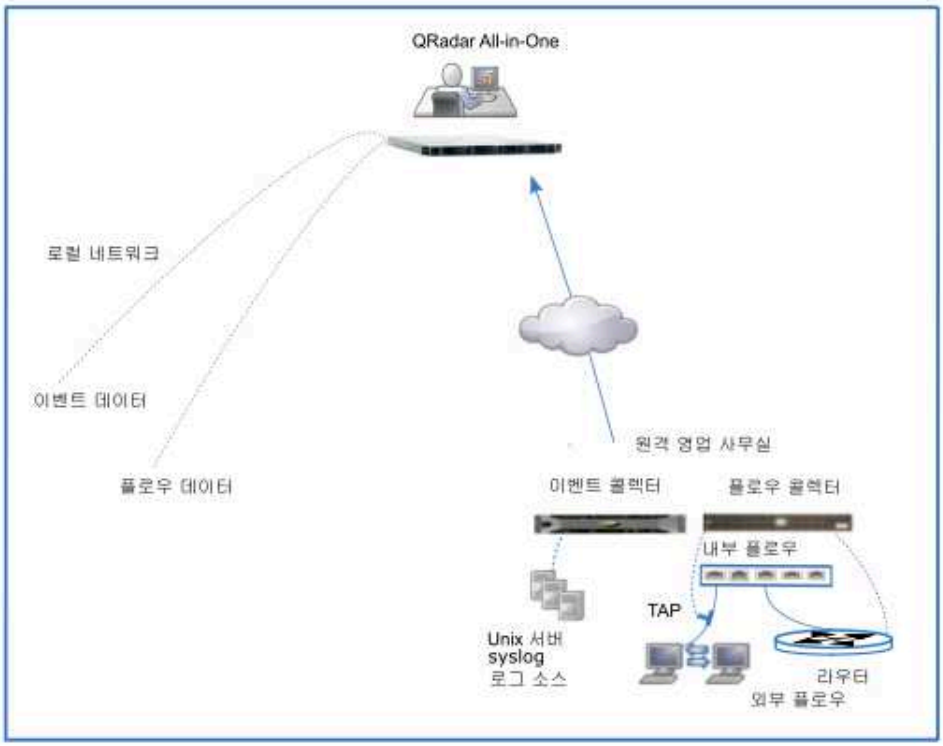


그림 *6.* 원격 사무실의 콜렉터

이 배치에서는 다음 프로세스가 발생합니다.

- 원격 사무실에서 이벤트 콜렉터는 로그 소스에서 데이터를 수집하고 플로우 콜렉터는 라우터 및 스위치에서 데이터를 수집합니다. 콜렉터는 데이터를 통합하고 정규화합니다.
- 콜렉터는 데이터를 압축하고 광역 네트워크를 통해 All-in-One 어플라이언스에 데이터를 전송합니다.
- All-in-One 어플라이언스가 데이터를 처리하고 저장합니다.
- 회사는 QRadar 웹 애플리케이션을 사용하여 검색, 분석, 보고하고 경보와 오펜스를 관리함으로써 네트워크 보기를 모니터링합니다.
- All-in-one은 로컬 네트워크에서 이벤트를 수집하고 처리합니다.

All-in-One 배치에 처리 용량 추가

이벤트 프로세서 및 플로우 프로세서를 QRadar 배치에 추가하여 처리 용량 및 스토리지를 늘리십시오. 프로세스를 추가하면 처리 및 스토리지 로드가 전용 서버로 이동되어 QRadar Console에서 자원이 해제됩니다.

이벤트 프로세서 또는 플로우 프로세서를 All-in-One 어플라이언스로 추가하는 경우, All-in-One은 QRadar Console로 동작합니다. All-in-One 어플라이언스에서의 처리 능력은 프로세서가 전송한 데이터를 관리하고 검색하기 위한 것이며, 데이터는 이제 콘솔이 아닌 이벤트 프로세서 및 기타 스토리지 디바이스에 저장됩니다.

일반적으로 다음과 같은 이유로 QRadar 배치에 이벤트 프로세서 및 플로우 프로세서를 추가합니다.

- 배치가 커지면서 워크로드가 All-in-One 어플라이언스의 처리 용량을 초과합니다.
- 보안 조작 센터는 더 많은 동시 검색을 수행하는 분석가를 더 많이 고용합니다.
- 모니터링하는 데이터의 유형 및 해당 데이터의 보존 기간이 늘어나며, 처리 및 스토리지 요구사항도 증가합니다.
- 보안 분석 팀이 커지면서 더 나은 검색 성능이 필요합니다.

동시에 여러 QRadar 검색을 실행하고 모니터링하는 로그 소스 유형을 더 많이 추가하면 All-in-One 어플라이언스의 처리 성능에 영향이 있습니다. 검색 횟수와 모니터링하는 데이터 양이 증가하면, 이벤트 프로세서 및 플로우 프로세서를 추가하여 QRadar 배치의 성능을 개선하십시오.

가장 강력한 All-in-One 어플라이언스에서 15,000 EPS 및 300,000 FPM 이상으로 QRadar 배치를 스케일링하는 경우, 해당 데이터를 처리하려면 프로세서 어플라이언스를 추가해야 합니다.

예제: 배치에 QRadar 이벤트 프로세서 추가

QRadar 이벤트 프로세서 1628을 추가할 수 있으며, 이는 최대 40,000 EPS까지 수집하고 처리합니다. 배치에 QRadar 이벤트 프로세서 1628을 추가할 때마다 다른 40,000 EPS에 의해 용량이 증가합니다. 최대 1,200,000 FPM까지 수집하고 처리하는 QRadar 플로우 프로세서 1728을 추가하십시오.

QRadar 이벤트 프로세서 1628은 콜렉터 및 프로세서입니다. 분산 네트워크가 있는 경우, 이벤트 콜렉터를 추가하여 로드를 분산시키고 이벤트 프로세서에서 시스템 자원을 해제하는 것이 좋습니다.

다음 다이어그램에서는 이벤트 프로세서 및 플로우 프로세서가 QRadar 3128(All-in-One)에 추가될 때 처리 용량이 추가되고 다음사항이 변경됩니다.

- 이벤트 및 플로우 처리가 All-in-One 어플라이언스에서 이벤트 및 플로우 처리로 이동됩니다.

- 이벤트 처리 용량이 40,000 EPS로 증가되고, 여기에는 All-in-One에 있었던 15,000 EPS가 포함됩니다.
- 플로우 처리 용량이 1,200,000 FPM으로 증가하고, 여기에는 All-in-One에 있었던 300,000 FPM이 포함됩니다.
- 이벤트 및 플로우 콜렉터가 전송한 데이터를 처리하고 이벤트 및 플로우 프로세서에 저장합니다.

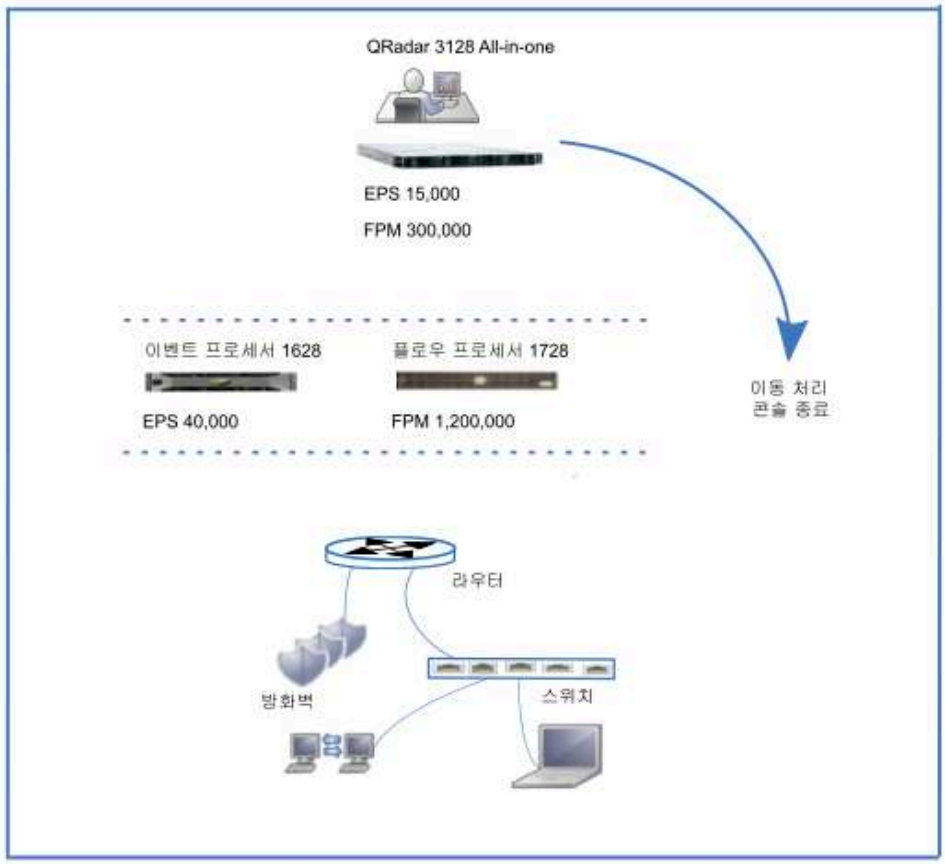


그림 7. 처리 용량 추가

QRadar Console과 같은 네트워크에 이벤트 프로세서 및 플로우 프로세서를 설치하면 검색 성능이 빨라집니다.

프로세서 및 콜렉터를 추가하면 QRadar 배치의 처리 용량이 확장됩니다. 배치의 스토리지 용량도 증가할 수 있습니다. 트래픽이 늘어나고 보존 정책이 변경되면 회사의 데이터 보존 요구사항이 늘어날 수 있습니다. 배치에 데이터 노드를 추가하면 데이터 스토리지 용량이 확장되고 검색 성능이 향상됩니다.

프로세서에 콜렉터를 추가하는 시기

All-in-One 어플라이언스에 콜렉터를 추가한 것과 같은 이유로 이벤트 프로세서 및 플로우 프로세서에 이벤트 콜렉터 및 플로우 콜렉터를 추가하십시오.

- 데이터 콜렉션 요구사항이 프로세서의 콜렉션 능력을 초과합니다.
- 프로세서가 설치된 것과 다른 위치에서 이벤트 및 플로우를 수집해야 합니다.
- 패킷 기반 플로우 소스를 모니터링합니다.

참고: 이벤트 콜렉터는 이벤트를 버퍼링할 수 있지만 플로우 콜렉터는 플로우를 버퍼링할 수 없습니다.

콘솔과 같은 네트워크에 프로세서가 설치되면 검색 성능이 개선되므로, 원격 위치에 콜렉터를 추가하고 프로세서에 해당 데이터를 전송하면 QRadar 검색 속도가 빨라집니다.

지리적으로 분산된 배치

지리적으로 분산된 배치에서는 IBM Security QRadar 배치가 원격 데이터 센터에 대한 간헐적이거나 부족한 연결의 영향을 받습니다. 또한 원래 위치에서 데이터를 보존하라는 특정 지역 또는 국가 규정 준수와 같은 로컬 규정에도 영향을 받습니다. 이러한 두 상황 모두에서는 콜렉터가 사이트에 있어야 합니다. 원래 위치에 데이터를 보존해야 하는 경우 사이트에서 프로세서를 유지시켜야 합니다.

예를 들어 회사가 커지면서 네트워크에서의 활동도 늘어나고 QRadar 배치를 다른 국가로 확장도 해야 합니다. 데이터 보존 법률은 국가마다 다르므로 QRadar 배치는 이러한 규정을 고려하여 계획해야 합니다.

다음 조건을 주의하십시오.

- 회사는 간헐적으로 연결되는 사무실 위치 중 하나에서 이벤트 데이터를 수집해야 합니다.
- 회사는 데이터를 수집하는 국가의 데이터 보존 규정을 준수해야 합니다. 예를 들어 독일에서는 데이터가 국내에 있어야 하는 경우, 해당 데이터를 해당 국가 외부에 저장하지 않아야 합니다.

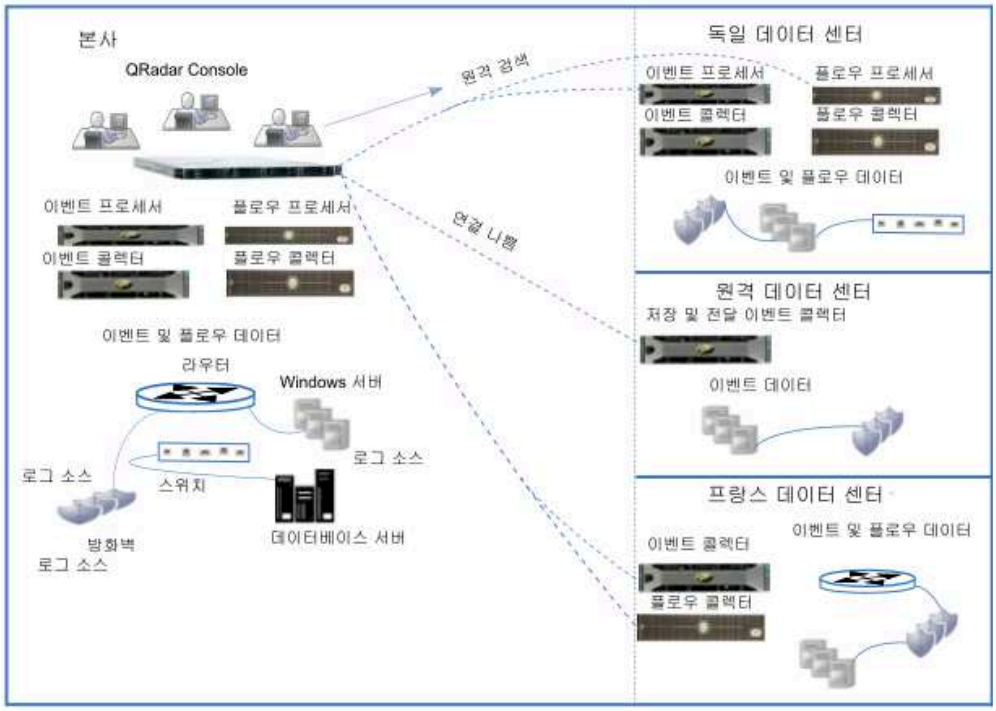


그림 *8.* 지리적으로 분산된 배치

지리적으로 분산된 배치에서는 다음 프로세스가 발생합니다.

- 회사가 로컬 데이터 법률을 준수하기 위해 독일 데이터 센터에 콜렉터와 프로세서를 설치합니다.
- 프랑스 데이터 센터에서는 콜렉터가 본사에 데이터를 전송하여 본사에서 처리 및 저장될 수 있도록 회사에서 콜렉터를 설치합니다. 검색 속도는 QRadar Console과 같은 고속 네트워크 세그먼트에 프로세서 어플라이언스가 있으면 증가합니다.
- 회사는 원격 데이터 센터에서 스케줄링된 비율 제한 전달 연결이 있는 저장 및 전달 이벤트 콜렉터를 추가합니다. 스케줄링된 비율 제한 연결로 간헐적 네트워크 연결을 보충하며, 정규 비즈니스 시간 동안 더 많은 대역폭에 필요하지 않게 됩니다.

원격 프로세서에서 연속적으로 데이터를 검색하는 경우, 해당 프로세서가 QRadar Console과 같은 고속 네트워크 세그먼트에 있는 것이 좋습니다. QRadar Console과 원격 프로세서 사이의 대역폭이 좋지 않으면, 특히 동시에 여러 검색을 수행할 때 검색이 지연됨을 경험하게 됩니다.

QRadar Vulnerability Manager 배치

IBM Security QRadar Vulnerability Manager를 배치하면 네트워크에서 취약성을 찾아 관리할 수 있습니다. IBM BigFix® 및 IBM Security SiteProtector™와 같은 추가 기능을 통합하여 네트워크 보안을 강화하십시오.

IBM Security QRadar Vulnerability Manager는 네트워크 디바이스, 애플리케이션에서 취약성을 감지하고 소프트웨어는 취약성에 컨텍스트를 추가하며, 네트워크에서 자산 위험성의 우선순위를 지정하고, 감지한 취약성을 개선합니다.

추가 보호를 위해 QRadar Risk Manager를 통합할 수 있으며, 이는 정책 준수를 기반으로 자산에 네트워크 토폴로지, 활성 공격 경로 및 고위험성 자산 위험 점수 조정을 제공합니다. QRadar Vulnerability Manager 및 QRadar Risk Manager는 하나의 오퍼링으로 결합되고 모두는 단일 기본 라이센스를 통해 사용할 수 있습니다.

설치하는 제품 및 IBM Security QRadar를 업그레이드하는지 또는 새 시스템을 설치하는 지 여부에 따라 **취약성** 탭이 표시되지 않을 수 있습니다. **취약성** 탭을 사용하여 IBM Security QRadar Vulnerability Manager에 액세스하십시오. IBM Security QRadar SIEM을 설치하는 경우 **취약성** 탭은 임시 라이센스 키를 사용하여 기본적으로 사용으로 설정됩니다. QRadar Log Manager를 설치하는 경우, **취약성** 탭을 사용할 수 없습니다. **시험판** 옵션을 사용하여 30일 동안 QRadar Vulnerability Manager를 사용할 수 있습니다. QRadar Vulnerability Manager에 대한 라이센스를 별도로 구매하고 라이센스 키를 사용하여 이를 사용으로 설정하십시오. 업그레이드에 대한 자세한 정보는 *IBM Security QRadar* 업그레이드 안내서의 내용을 참조하십시오.

QRadar Vulnerability Manager 구성요소

다음 정보는 QRadar Vulnerability Manager 프로세서에 대해 설명합니다.

- 스캔 프로세서는 스캔을 스케줄링 및 관리하고, 네트워크 전반에 걸쳐 분포될 수 있는 스캐너에 작업을 위임하는 작업을 수행합니다.
- QRadar 배치에서는 하나의 스캔 프로세서만 가질 수 있습니다.
- All-in-One 시스템에 QRadar Vulnerability Manager를 설치하고 라이센스를 부여하는 경우, 취약성 프로세서가 자동으로 QRadar Console에 배치되고 스캐닝 구성요소가 포함됩니다.
- 취약성 프로세서는 기본적으로 스캐닝 구성요소를 제공합니다. 필요한 경우에는 취약성 프로세서를 배치 내의 다른 관리 호스트로 이동할 수 있습니다.
- 600 관리 호스트 어플라이언스를 추가하고 QRadar Vulnerability Manager를 처음 사용하는 경우, 스캔 프로세서가 600 관리 호스트 어플라이언스에 지정됩니다.

- 스캐닝 프로세서는 처리 라이센스가 관리하고, 여기에서는 QRadar Vulnerability Manager가 처리할 수 있는 최대 자산 수가 결정됩니다.
- 스캔 프로세서는 QRadar Console 또는 관리 호스트에서 실행할 수 있습니다.

다음 정보는 QRadar Vulnerability Manager 스캐너에 대해 설명합니다.

- 가상 머신에 또는 소프트웨어 전용으로서 스캐너를 배치할 수 있습니다.
- QRadar Vulnerability Manager 스캐너 전용 스캐너 어플라이언스를 배치할 있으며, 이것이 610 어플라이언스입니다.
- QRadar Console 또는 다음 관리 호스트에 스캐너를 배치할 수 있습니다: 플로우 콜렉터, 플로우 프로세서 이벤트 콜렉터, 이벤트 프로세서 또는 데이터 노드.
- 스캐너로 스캔할 수 있는 자산 수는 스캐너 용량으로 판별되고 라이센스의 영향을 받지 않습니다.

구성요소 및 스캔 프로세스

스캔 작업은 프로세서 및 스캐너 구성요소가 완료합니다. 다음 다이어그램은 실행되는 스캔 구성요소 및 프로세스를 표시합니다.

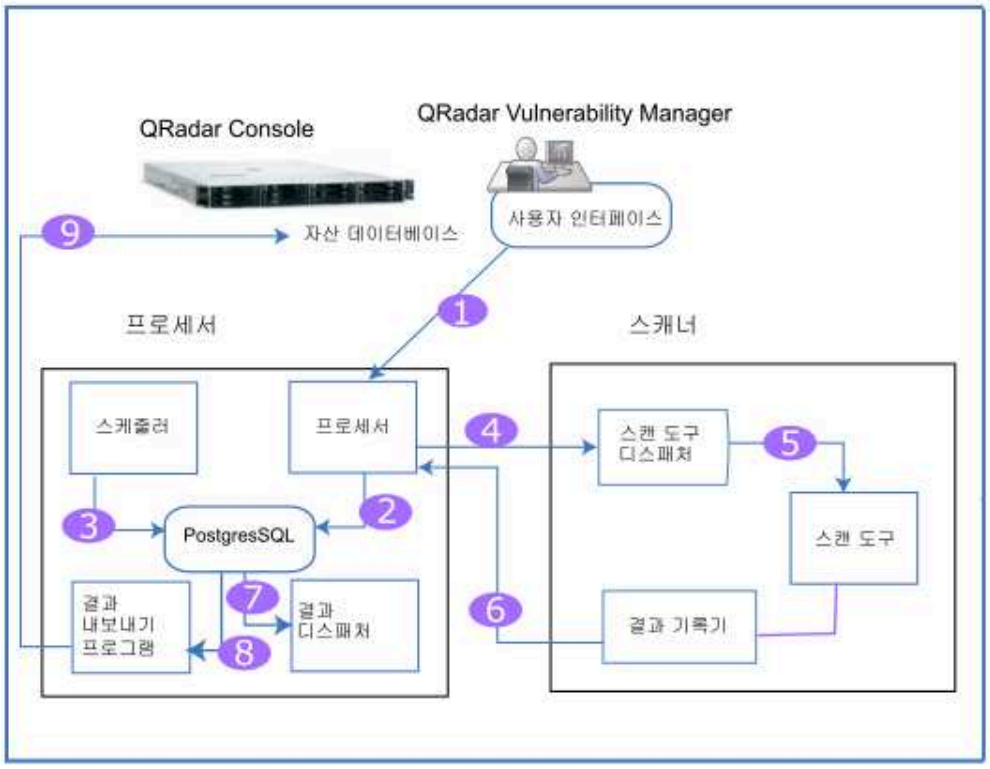


그림 *9.* 스캔 구성요소 및 프로세스

다음 목록은 스캔 프로세스의 단계에 대해 설명합니다.

1. 자산의 IP 주소, 스캔 유형, 인증된 스캔의 필수 신임 정보와 같은 매개변수를 지정하여 스캔 작업을 작성합니다.
2. 스캔 작업은 프로세서가 채택하고, 로깅하고, 스케줄링 정보와 함께 데이터베이스에 추가되어 작업 실행 시기를 판별합니다.
3. 스케줄러 구성요소는 스캔 스케줄링을 관리합니다. 스케줄러가 스캔을 시작하면, 필요한 도구 목록을 판별한 후 호출을 위해 큐에 넣고 도구에는 관련 스캐너가 지정됩니다.
4. 스캐너는 고유한 스캐너 ID를 전송하여 스캔 프로세서에서 반드시 실행해야 하는 스캔 도구를 계속해서 폴링합니다. 스케줄러가 특정 스캐너와 관련된 도구를 큐에 넣은 경우, 도구는 호출을 위해 스캐너로 전송됩니다.

   QRadar Vulnerability Manager는 공격 트리 방법론을 사용하여 스캔을 관리하고 실행할 도구를 판별합니다. 단계는 자산 감지, 포트/서비스 감지, 서비스 스캔, 패치 스캔 단계로 구성됩니다.
5. 디스패처가 목록에 있는 각 스캔 도구를 실행하고 관리합니다. 실행되는 각 도구에 대해 디스패처는 프로세서에 스캔 도구의 시작 및 종료 시기를 나타내는 메시지를 전송합니다.

6. 스캔 도구의 결과물은 결과 기록기가 읽고, 이러한 결과를 다시 프로세서로 전달합니다.
7. 결과 디스패처는 스캔 도구의 원시 결과를 처리하고 이를 Postgres 데이터베이스에 기록합니다.
8. 결과 내보내기 프로그램은 프로세서 데이터베이스에서 완료된 스캔을 찾아 결과를 QRadar Console로 내보냅니다.
9. 내보낸 결과는 사용자가 스캔 결과를 보고 관리할 수 있는 QRadar 데이터베이스에 추가됩니다.

All-in-one 배치

All-in-one 시스템에서 QRadar Vulnerability Manager를 실행할 수 있습니다. 여기에서는 스캐닝 및 처리 기능이 콘솔에 있습니다. 다음 정보는 기본 설정에서 수행할 수 있는 작업에 대해 설명합니다.

- 최대 255개의 자산 설정.
- 무제한 감지 스캔.
- DMZ 스캐닝을 위한 호스트 스캐너 사용.
- QRadar와 통합되는 써드파티 스캐너에서 스캔 데이터 관리.
- 관리 호스트에 스캐너 배치.
- 무제한 독립형 소프트웨어 또는 가상 스캐너 배치.

배치 확장

배치가 증가하면서, QRadar Console에서 처리 기능을 이동시켜 자원을 해제해야 하거나 사용자 자산과 가깝게 스캐너를 배치할 수도 있습니다.

다음 목록은 배치에 스캐너를 추가하는 이유에 대해 설명합니다.

- QRadar Vulnerability Manager 프로세서와 다른 지역에서 자산 스캔.
- 짧은 시간 프레임 내에 동시에 많은 자산을 스캔하려는 경우.
- 로그 소스인 방화벽을 통해 스캔하지 않도록 스캐너 추가하려 합니다. 방화벽을 통과하는 스캐너 호스트에 인터페이스를 추가하여 직접 네트워크에 스캐너를 추가하는 것에 대해 고려할 수도 있습니다.

다음 다이어그램은 관리 호스트에 스캐너 및 외부 스캐닝이 배치되어 있는 스캐닝 배치를 표시합니다.

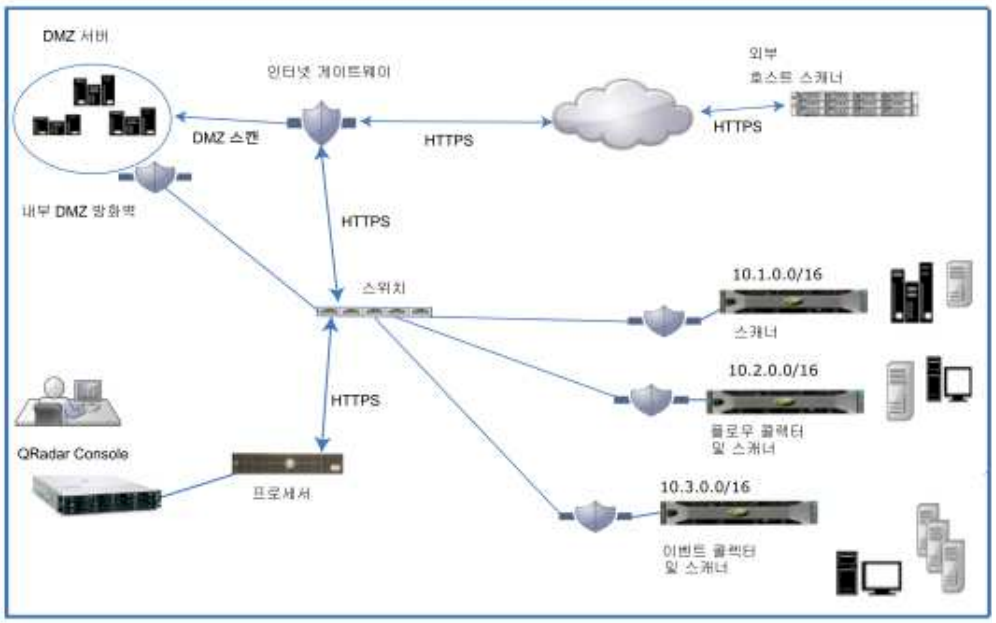


그림 *10.* 배치 스캐닝

DMZ 호스트 스캐너

호스트 스캐너는 공용 IP 주소를 사용하여 인터넷에서 DMZ를 스캔합니다. DMZ에 있는 자산에서 취약성을 스캔하기 위해 DMZ에 스캐너를 배치할 필요는 없습니다. 네트워크 외부에 있는 호스트 IBM 스캐너를 사용하여 QRadar Vulnerability Manager를 구성해야 합니다. 자세한 정보는 *IBM Security QRadar Vulnerability Manager* 사용자 안내서의 내용을 참조하십시오.

QRadar Vulnerability Manager 통합

IBM Security QRadar Vulnerability Manager와 IBM BigFix를 통합하면, 수정 가능한 취약성을 필터링하고 우선순위를 지정할 수 있습니다. BigFix는 IT 조작과 보안 사이에서 공유 가시성 및 제어를 제공합니다. BigFix는 QRadar Vulnerability Manager가 식별하고 BigFix에 보낸 높은 우선순위 취약성에 Fixlet을 적용합니다. Fixlet은 특정 취약성을 개선하기 위해 자산 또는 엔드포인트에 배치하는 패키지입니다.

QRadar Vulnerability Manager는 IBM Security SiteProtector와 통합되어 침입 방지 시스템(IPS) 정책을 관리하는 데 도움이 됩니다. IBM Security SiteProtector를 구성하는 경우, 스캔으로 감지된 취약성은 IBM Security SiteProtector에 자동으로 전달됩니다. IBM Security SiteProtector는 IBM Security SiteProtector에 연결하여 통합을 구성한 후에만 실행되는 QRadar Vulnerability Manager 스캔에서 취약성 데이터를 수신합니다. .

써드파티 스캐너

QRadar Vulnerability Manager는 스캔 데이터의 소스에 관계없이 효과적인 취약성 관리 플랫폼을 전달합니다. QRadar Vulnerability Manager는 Nessus, nCircle 및 Rapid 7과 같은 써드파티 스캐너와 완벽하게 통합합니다.

다음 옵션을 사용하려면 QRadar Vulnerability Manager 스캐닝이 필요합니다.

- 이벤트 구동 및 요청 시 스캐닝
- 자산 데이터베이스 및 관심 목록 기반 스캐닝
- 기존 QRadar 어플라이언스 및 관리 호스트에서 스캐닝
- 스캔 결과에 없는 새로 게시된 취약성 발견

다음 옵션을 사용하려면 QRadar Risk Manager가 필요합니다.

- 자산, 취약성 및 트래픽 기반 취약성 관리
- 조정된 취약성 점수 및 컨텍스트 인식 위험 스코어링.

QRadar Risk Manager 및 QRadar Vulnerability Manager

IBM Security QRadar Risk Manager를 IBM Security QRadar Vulnerability Manager와 통합하여 네트워크 보안을 강화하십시오. 스캔 데이터와 같은 데이터 소스를 사용하면 QRadar Risk Manager가 네트워크에서 보안, 정책 및 준수성 위험을 식별하고 위험 개발의 확률을 계산할 수 있습니다.

QRadar Vulnerability Manager 및 QRadar Risk Manager는 하나의 오퍼링으로 결합되고 모두는 단일 기본 라이센스를 통해 사용할 수 있습니다.

다음 기능을 얻으려면 QRadar Risk Manager 700 어플라이언스를 추가하십시오.

- 준수 평가
- 고위험 취약성을 신속하게 식별하는 데 도움이 되는 취약성 데이터 및 위험 점수를 기반으로 하는 위험 정책.
- 네트워크 토폴로지 보기를 통해 잠재적인 위협 및 신뢰할 수 없는 네트워크에서의 잠재적 탐색 경로 표시.
- 위험 정책 기반 필터링.
- 토폴로지 시각화
- 취약성 평가에서의 False Positive 감소.
- 방화벽 및 IPS(Intrusion Prevention Systems)에 의해 차단되는 취약성 표시.

QRadar Risk Manager 어플라이언스

QRadar Risk Manager 700 어플라이언스에 QRadar Risk Manager를 개별적으로 설치하십시오.

QRadar Risk Manager 어플라이언스를 설정 및 구성하려면 IBM Security QRadar Console을 설치해야 합니다. QRadar 및 QRadar Risk Manager를 같은 네트워크 스위치에 설치하는 것이 좋습니다.

배치당 하나의 QRadar Risk Manager 어플라이언스가 필요합니다.

다음 다이어그램에서는 스캐너 및 QRadar Risk Manager가 있는 배치를 표시합니다.

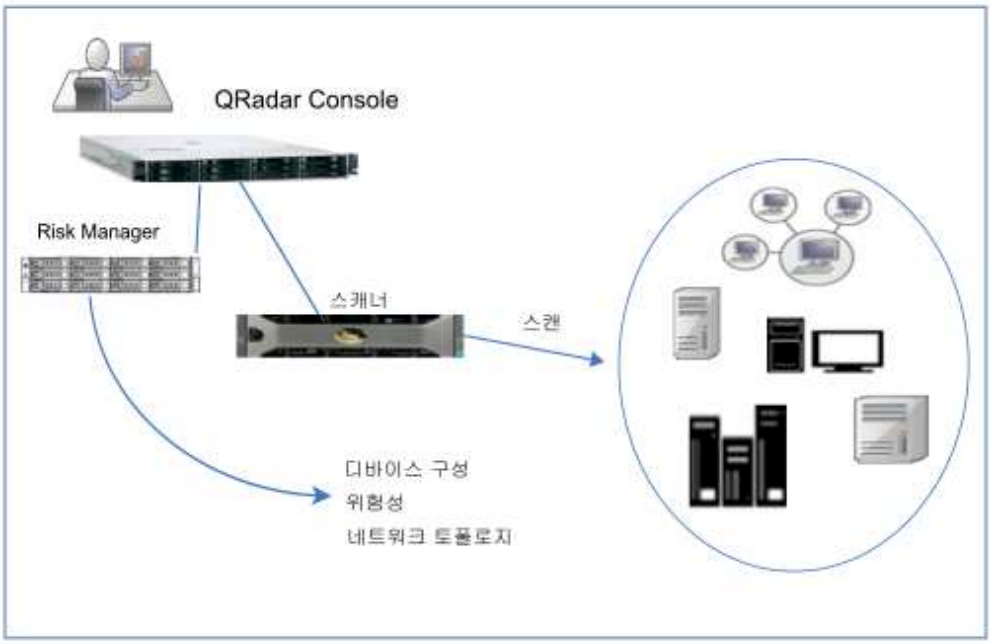


그림 *11. Risk Manager*를 가진 배치 스캐닝

Risk Manager를 사용하여 다음 태스크를 완료하십시오.

- 중앙 집중식 위험 관리.
- 네트워크 토폴로지 보기 및 필터링
- 디바이스 구성 가져오기 및 비교
- 네트워크 디바이스 사이의 연결 보기
- 방화벽 룰 검색
- 기존 룰과 트리거된 룰의 이벤트 수 보기
- 디바이스 및 경로 검색

- 네트워크 연결 조회
- 디바이스 구성 업데이트 결과 시뮬레이션
- 네트워크 모니터링 및 감사를 통해 준수 확인
- 가상 모델에 대한 위협 또는 공격 시뮬레이션
- 취약성 검색

포렌식 및 전체 패킷 콜렉션

배치에서 IBM Security QRadar Incident Forensics를 사용하여 잠재적인 공격자의 단계별 조치를 다시 추적하고, 의심되는 악의적 네트워크 보안 인시던트에 대해 깊이있는 포렌식 조사를 수행하십시오.

QRadar Incident Forensics는 보안 인시던트와 관련된 원시 네트워크 데이터를 원래 양식으로 다시 구성합니다.

QRadar Incident Forensics는 IBM QRadar Security Intelligence Platform과 통합되며 많은 써드파티 패킷 캡처 오퍼링과 호환이 가능합니다.

QRadar Incident Forensics는 다른 네트워크 패킷 캡처(PCAP) 디바이스가 배치되지 않은 경우 QRadar Incident Forensics가 사용하는 데이터를 저장 및 관리하는 선택적 QRadar Packet Capture 어플라이언스를 제공합니다. 네트워크 또는 서브네트워크에 TAP으로서 이러한 어플라이언스를 설치하여 원시 패킷 데이터를 수집할 수 있습니다.

QRadar Packet Capture 구성요소

QRadar 배치에는 다음 구성요소가 포함될 수 있습니다.

QRadar Console

QRadar 제품 사용자 인터페이스를 제공합니다. 분산 배치에서는 QRadar Console을 사용하여 여러 QRadar Incident Forensics Processor 호스트를 관리하십시오.

QRadar Incident Forensics Processor

QRadar Incident Forensics 제품 인터페이스를 제공합니다. 인터페이스는 사이버 범죄의 단계별 조치를 재추적하고 보안 인시던트와 관련된 원시 네트워크 데이터를 재구성하고 사용 가능한 비구조화 데이터에서 검색하고 세션 및 이벤트를 시각적으로 재구성하는 도구를 전달합니다.

보안 인텔리전스 포렌식 기능을 사용하려면 우선 QRadar Incident Forensics Processor를 관리 호스트로 추가해야 합니다.

QRadar Incident Forensics Standalone

QRadar Incident Forensics 제품 사용자 인터페이스를 제공합니다.

QRadar Incident Forensics Standalone을 설치하면 포렌식 조사를 수행하는 데 필요한 도구를 제공합니다. 포렌식 조사 및 관련 관리 기능만 사용 가능합니다.

QRadar Packet Capture

선택적 QRadar Packet Capture 어플라이언스를 설치할 수 있습니다. 다른 네트워크 패킷 캡처(PCAP) 디바이스가 배치되지 않은 경우, 이 어플라이언스를 사용하여 QRadar Incident Forensics에서 사용된 데이터를 저장할 수 있습니다. 원시 패킷 데이터를 수집하기 위해 네트워크 탭 또는 서브네트워크로서 설치할 수 있는 이러한 어플라이언스의 수에는 제한이 없습니다.

패킷 캡처 디바이스가 첨부되지 않은 경우에는 사용자 인터페이스에서 또는 FTP를 사용하여 패킷 캡처 파일을 수동으로 업로드할 수 있습니다.

네트워크 및 패킷 캡처 요구사항에 따라 최대 5개의 패킷 캡처 디바이스를 QRadar Incident Forensics 어플라이언스에 연결할 수 있습니다.

QRadar Packet Capture Data Node 어플라이언스

추가 스토리지 용량을 위해 최대 두 개의 QRadar Packet Capture Data Node 어플라이언스를 각 QRadar Packet Capture 마스터 시스템에 연결할 수 있습니다.

All-in-One 배치

독립형 또는 all-in-one 배치에서는 IBM Security QRadar Incident Forensics Standalone 소프트웨어를 설치합니다. 이러한 단일 어플라이언스 배치는 QRadar Console 및 QRadar Incident Forensics 관리 호스트를 단일 어플라이언스에 설치하는 것과 유사하지만 로그 관리, 네트워크 보기 모니터링 또는 기타 보안 인텔리전스 기능이 없습니다. 독립형 네트워크 포렌식 솔루션을 위해 중소 규모 배치에 QRadar Incident Forensics Standalone을 설치하십시오.

다음 다이어그램은 기본적인 QRadar Incident Forensics All-in-One 배치를 표시합니다.

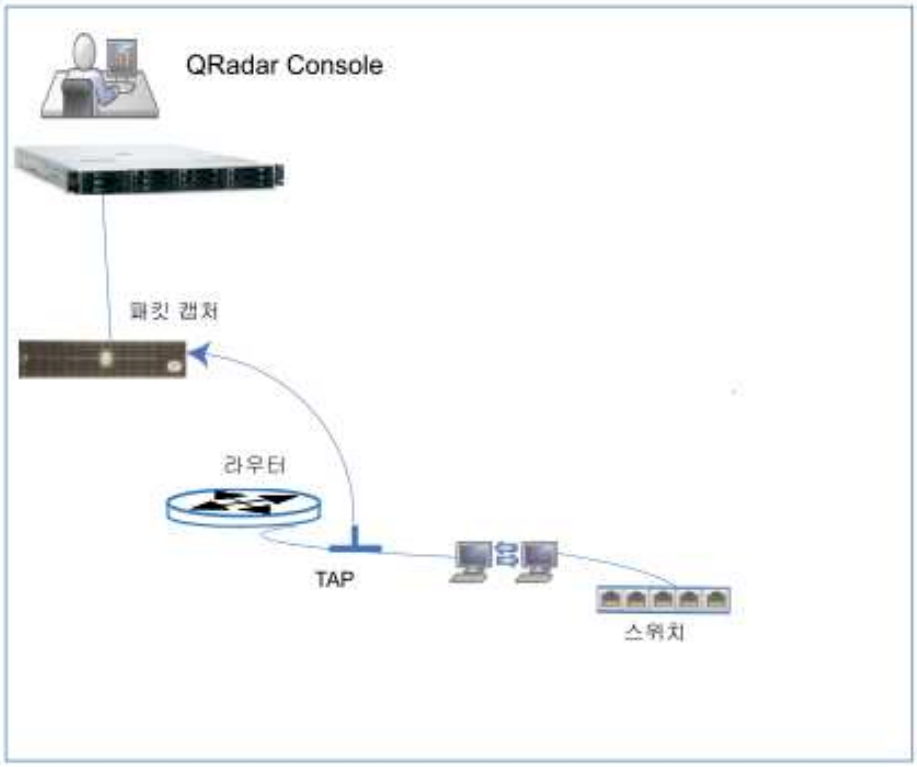


그림 *12. All-in-one* 배치

분산 배치

분산 배치에는 다음 세 가지 어플라이언스가 있을 수 있습니다.

- QRadar Console
- QRadar Packet Capture 관리 호스트(QRadar Packet Capture 프로세서)
- QRadar Packet Capture(선택사항)

단일 배치에서 모든 IBM Security QRadar 어플라이언스의 소프트웨어는 버전 및 수정사항 레벨이 동일해야 합니다. 다른 버전의 소프트웨어를 사용하는 배치는 지원되지 않습니다.

다음 다이어그램은 QRadar Incident Forensics 분산 배치를 표시합니다.

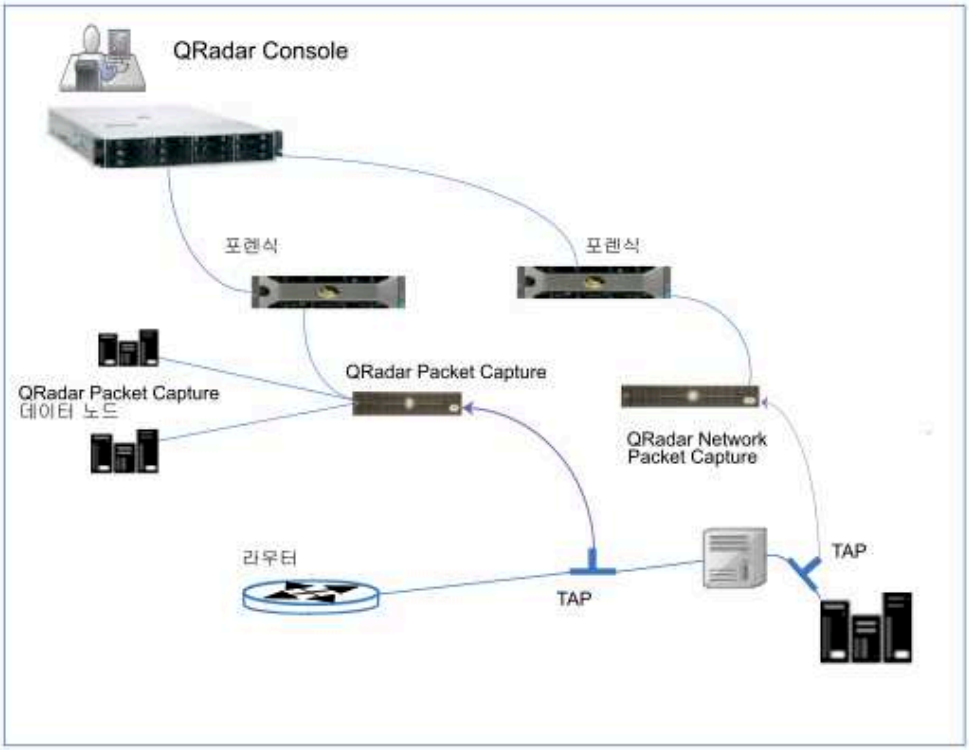


그림 *13.* 분산 배치

다음 다이어그램은 10G Napatech 네트워크 카드를 가진 IBM QRadar QFlow Collector 1310에서 QRadar Packet Capture 어플라이언스로 전달되는 패킷을 표시합니다.

QRadar QFlow Collector에서는 전용 Napatech 모니터링 카드를 사용하여 카드의 한 포트에서 IBM Security QRadar Packet Capture 어플라이언스에 연결된 두 번째 포트로 수신 패킷을 복사합니다.

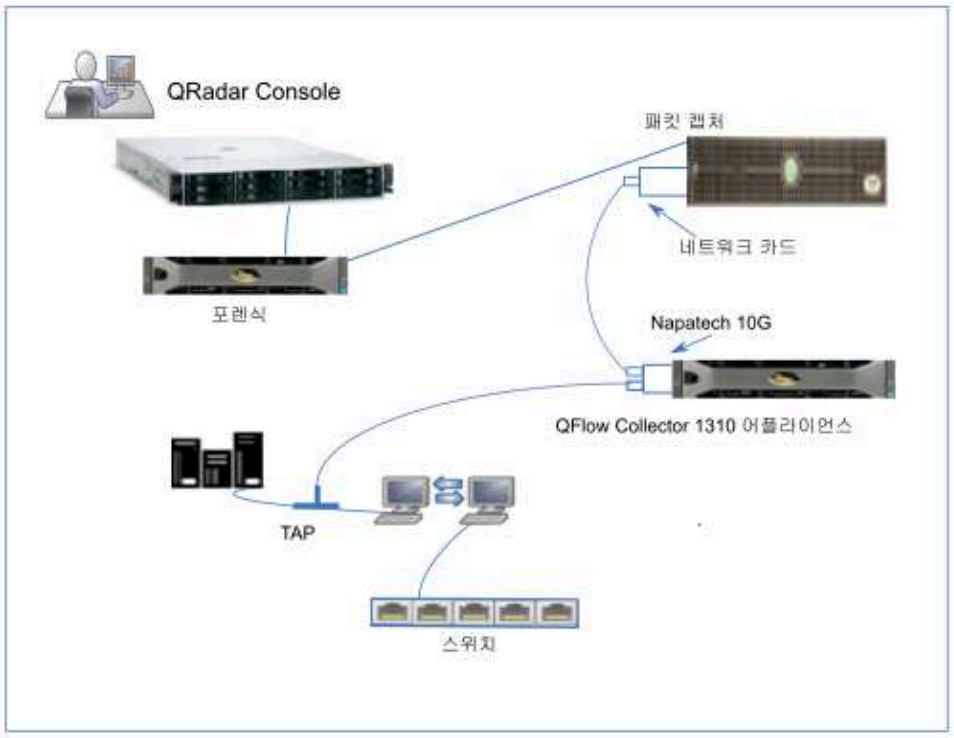


그림 *14.* 패킷 전달

QRadar Packet Capture에 패킷 전달

IBM Security QRadar QFlow Collector 1310 어플라이언스에 원시 데이터 패킷을 전송하여 네트워크 트래픽을 모니터링할 수 있습니다. QRadar QFlow Collector에서는 전용 Napatech 모니터링 카드를 사용하여 카드의 한 포트에서 IBM Security QRadar Packet Capture 어플라이언스에 연결된 두 번째 포트로 수신 패킷을 복사합니다.

10G Napatech 네트워크 카드가 장착된 QRadar QFlow Collector 1310이 이미 있는 경우 트래픽을 QRadar Packet Capture로 미러링할 수 있습니다.

다음 다이어그램과 같이, 10G Napatech 네트워크 카드가 장착된 QRadar QFlow Collector 1310이 이미 있는 경우 트래픽을 QRadar Packet Capture로 미러링할 수 있습니다.

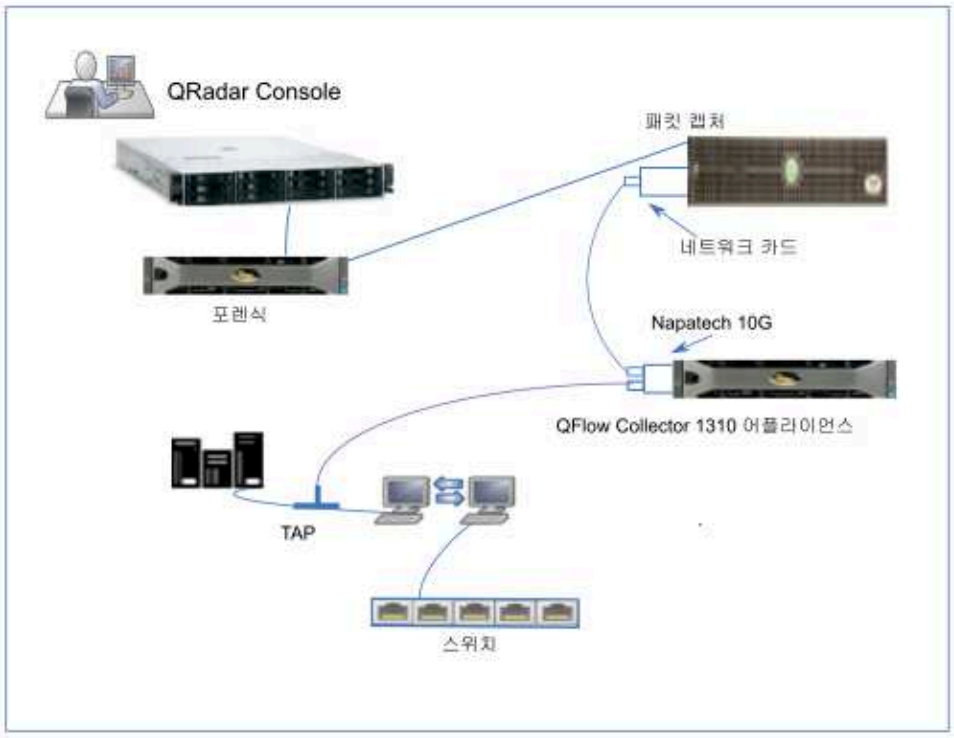


그림 *15. Napatech* 카드를 사용하여 *QRadar QFlow Collector*에서 *QRadar Packet Capture*로 패킷 데이터 전달

시작하기 전에

다음 하드웨어가 사용자 환경에 설정되어 있는지 확인하십시오.

- QRadar QFlow Collector 1310 어플라이언스에 있는 Napatech 카드의 포트 1에 케이블을 연결했습니다.
- 전달 포트인 Napatech 카드의 포트 2에 연결된 케이블을 QRadar Packet Capture 어플라이언스에 연결했습니다.
- 두 어플라이언스에서 링크 표시등을 확인하여 계층 2 연결을 검증하십시오.

프로시저

1. IBM Security QRadar 콘솔에서 SSH를 사용하여 QRadar QFlow Collector에 root 사용자로 로그인하십시오. QRadar QFlow Collector 어플라이언스에서 다음 파일을 편집하십시오.

   ```
   /opt/qradar/init/apply_tunings
   ```

   a. 라인 137 주위에 있는 다음 라인을 찾으십시오.

```
apply_multithread_qflow_changes()
{
     APPLIANCEID=`$NVABIN/myver -a`
     if [ "$APPLIANCEID" == "1310" ]; then
          MODELNUM=$(/opt/napatech/bin/AdapterInfo 2>&1 | grep "Active FPGA Image" | cut -d'-' -f2)
          if [ "$MODELNUM" == "9220" ]; then..
```

b. 이전 단계의 코드 다음에 오는 AppendToConf 라인에 다음 라인을 추가하십시오.

```
AppendToConf SV_NAPATECH_FORWARD YES
AppendToConf SV_NAPATECH_FORWARD_INTERFACE_SRCDST "0:1"
```

이 명령문은 패킷 전달이 가능하게 하고 포트 0에서 포트 1로 패킷을 전달합니다.

c. /opt/qradar/conf/nva.conf 파일에서 다음 라인을 확인하여 멀티스레딩이 가능하도록 하십시오.

```
MULTI_THREAD_ON=YES
```

2. 다음 명령을 입력하여 apply_tunings 스크립트를 실행하고 QRadar QFlow Collector의 구성 파일을 업데이트하십시오.

```
./apply_tunings restart
```

3. 다음 명령을 입력하여 IBM Security QRadar 서비스를 다시 시작하십시오.

```
systemctl restart hostcontext
```

4. 옵션: 사용자의 Napatech 카드가 데이터를 수신 및 전송 중인지 검증하십시오.

a. Napatech 카드가 데이터를 수신 중인지 검증하려면 다음 명령을 입력하십시오.

```
/opt/napatech/bin/Statistics -dec -interactive
```

카드가 데이터를 수신 중인 경우 "RX" 패킷 및 바이트 통계가 증가됩니다.

b. Napatech 카드가 데이터를 전송 중인지 검증하려면 다음 명령을 입력하십시오.

```
/opt/napatech/bin/Statistics -dec -interactive
```

카드가 데이터를 전송 중인 경우 "TX" 통계가 증가됩니다.

5. 옵션: QRadar Packet Capture가 QRadar QFlow Collector 어플라이언스에서 패킷을 수신 중인지 확인하십시오.

a. QRadar Console에서는 SSH를 사용함으로써 포트 4477에서 root 사용자로 QRadar Packet Capture 어플라이언스에 로그인하십시오.

b. 다음 명령을 입력하여 QRadar Packet Capture 어플라이언스가 패킷을 수신 중인지 확인하십시오.

```
watch -d cat /var/www/html/statisdata/int0.txt
```

데이터가 QRadar Packet Capture 어플라이언스로 플로우되면서 `int0.txt` 파일이 업데이트됩니다.

패킷 캡처에 대한 자세한 정보는 *IBM Security QRadar Packet Capture* 빠른 참조 안내서를 참조하십시오.

제 3 장 데이터 노드 및 데이터 스토리지

IBM Security QRadar 프로세서 어플라이언스와 All-in-One 어플라이언스는 데이터를 저장할 수 있지만 많은 회사에서는 특정 스토리지 요구사항을 처리하고 데이터 보유 정책을 구현하는 데 도움이 되는 데이터 노드의 독립형 스토리지 및 처리 기능을 필요로 합니다. 많은 회사는 특정 기간 동안 데이터 레코드를 필수적으로 보존하도록 하는 규정 및 법률의 적용을 받습니다.

데이터 노드 정보

다음 목록은 데이터 노드에 대한 정보에 대해 설명합니다.

- 데이터 노드는 스토리지 및 처리 용량을 추가합니다.
- 데이터 노드는 플러그 앤 플레이이므로 언제든지 배치에 추가할 수 있습니다.
- 데이터 노드는 기존 배치와 완벽하게 통합됩니다.
- 데이터 노드를 사용하면 프로세서에서 데이터 스토리지 처리 로드를 제거하여 프로세서 어플라이언스에 대한 처리 로드를 줄일 수 있습니다.
- 사용자는 데이터 콜렉션과 관계없이 스토리지 및 처리 능력을 측정할 수 있습니다.
- QRadar V.7.2.7부터는 데이터를 저장할 때 원시 데이터 압축을 사용하여 데이터를 압축합니다. 원시 데이터 압축을 사용하면 QRadar의 이전 버전에서 데이터를 압축할 때 사용했던 이전 압축 알고리즘보다 검색 성능이 더 많이 개선됩니다.

다음 다이어그램은 배치에서 데이터 노드의 일부 사용 예제를 표시합니다.

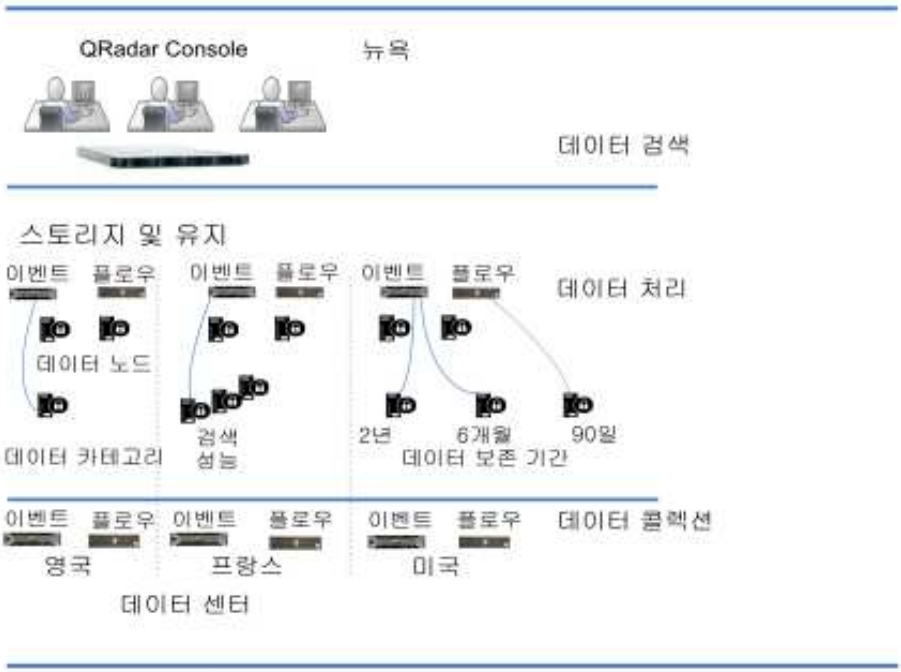


그림 *16.* 데이터 노드 어플라이언스를 사용한 데이터 스토리지 관리

다음 목록은 데이터 노드를 배치할 때 고려해야 하는 다른 요소에 대해 설명합니다.

데이터 클러스터링

데이터 노드는 배치에 스토리지 용량을 추가하고, 여러 스토리지 볼륨 전체에 걸쳐 수집되는 데이터를 분배하여 성능도 향상시킵니다. 데이터를 검색할 경우, 여러 호스트 또는 하나의 클러스터가 검색합니다. 클러스터는 검색 성능을 개선할 수 있지만, 사용자가 여러 이벤트 프로세서를 추가할 필요는 없습니다. 데이터 노드는 각 프로세서의 스토리지를 배가시킵니다.

참고: 한 번에 하나의 프로세서에만 데이터 노드를 연결할 수 있지만 프로세서는 여러 데이터 노드를 지원할 수 있습니다.

배치 고려사항

배치에서 데이터 노드를 설정하면서 다음 정보를 유의하십시오.

- 데이터 노드는 QRadar V7.2.2 이상에서 사용할 수 있습니다.
- 데이터 노드는 QRadar 배치의 이벤트 및 플로우 프로세서와 유사한 검색 및 분석 기능을 수행합니다.

  클러스터에서의 작동 속도는 가장 느린 클러스터 멤버의 영향을 받습니다. 배치에서 데이터 노드의 크기가 이벤트 프로세서 및 플로우 프로세서의 크기와 비슷하게 지정되면 데이터 노드 시스템 성능이 향상됩니다. 데이터 노드와 이벤트 및 플로우 프로세서 사이에서 비슷한 크

기를 지정하기 쉽도록 하기 위해 데이터 노드는 XX05 및 XX28 코어 어플라이언스 모두에서 사용할 수 있습니다.

- 데이터 노드는 세 개의 형식(소프트웨어(자체 하드웨어), 물리적, 어플라이언스)으로 사용할 수 있습니다. 단일 클러스터에서 형식을 혼합할 수 있습니다.

대역폭 및 대기 시간

클러스터에 있는 호스트 사이에서 1Gbps 링크가 있고 대기 시간은 10ms 미만이 되도록 하십시오. 많은 결과를 생성하는 검색에는 더 넓은 대역폭이 필요합니다.

어플라이언스 호환성

데이터 노드는 All-In-One 어플라이언스를 포함하여 이벤트 프로세서 또는 플로우 프로세서 구성요소가 있는 기존의 모든 QRadar 어플라이언스와 호환이 가능합니다. 데이터 노드는 QRadar Incident Forensics PCAP 어플라이언스와 호환되지 않습니다.

데이터 노드는 고가용성(HA)을 지원합니다.

데이터 노드 설치

데이터 노드는 표준 TCP/IP 네트워킹을 사용하지만 독점적이거나 전문화된 상호 연결 하드웨어는 필요하지 않습니다.

다른 QRadar 어플라이언스에 설치하는 것과 같이 배치에 추가하려는 각 데이터 노드를 설치하십시오. QRadar 배치 편집기에서 데이터 노드와 이벤트 또는 플로우 프로세서를 연관시키십시오. 자세한 정보는 *IBM Security QRadar* 관리 안내서를 참조하십시오.

다대일 구성에서는 여러 데이터 노드를 단일 이벤트 프로세서 또는 플로우 프로세서에 첨부할 수 있습니다.

데이터 노드 어플라이언스로 고가용성(HA)쌍을 배치하는 경우, HA쌍을 동기화하기 전에 HA 어플라이언스로 데이터를 설치, 배치 및 밸런스 재조정하십시오. HA에 활용되는 데이터 밸런스 재조정과 복제 프로세스를 결합하면 성능이 현저히 저하됩니다. 데이터 노드가 도입되는 어플라이언스에서 HA가 설정되면, 어플라이언스에서 HA의 연결을 끊은 다음 클러스터의 밸런스 재조정이 완료되면 다시 연결하십시오.

데이터 노드 해체

기타 QRadar 어플라이언스에서와 같이 배치 편집기로 배치에서 데이터 노드를 제거하십시오. 해체 작업은 호스트에서 데이터를 지우지도 않고 다른 어플라이언스로 데이터를 이동시키지도 않습니다. 데이터 노드에 있었던 데이터에 대한 액세스를 그대로 유지하려는 경우, 데이터를 이동시킬 위치를 식별해야 합니다.

데이터 밸런스 재조정

클러스터에 데이터 노드를 추가하면 각 데이터 노드에 데이터가 분배됩니다. 가능하면 각 데이터 노드에서 사용 가능한 공간의 비율이 같아지도록 데이터 밸런스를 재조정하십시오. 클러스터에 추가된 새 데이터 노드는 클러스터 이벤트 및 플로우 프로세서에서 더 많은 밸런스 재조정을 시작하여 새로 추가된 데이터 노드 어프라이언스에서 디스크를 효율적으로 사용하려 합니다.

QRadar V7.2.3부터는 데이터 밸런스 재조정이 자동이며 조회 및 데이터 콜렉션과 같은 다른 클러스터 활동과 동시에 발생합니다. 데이터 밸런스 재조정 중 작동 중지 시간이 발생하지 않습니다.

데이터 밸런스 재조정이 완료될 때까지 클러스터에서 데이터 노드 성능이 향상되지 않습니다. 밸런스 재조정으로 인해 검색 조작 중 약간의 성능 저하가 유발될 수 있지만 데이터 콜렉션 및 처리에는 계속해서 아무 영향이 없습니다.

참고: 데이터 노드 및 이벤트 프로세서 사이에서는 암호화된 데이터 전송이 지원되지 않습니다. 이벤트 프로세서와의 데이터 노드 통신을 위해서는 다음 방화벽 포트가 열려야 합니다.

- 데이터 노드 및 이벤트 프로세서 어플라이언스 사이에서는 포트 32006.
- 데이터 노드 및 콘솔의 이벤트 프로세서 사이에서는 포트 32011.

관리 및 조작

데이터 노드는 자체적으로 관리되므로 일반 조작을 위해 정기적인 사용자 간섭이 필요하지 않습니다. QRadar는 데이터 노드 어플라이언스를 포함하여 모든 호스트에 대한 데이터 백업, 고가용성 및 유지 정책과 같은 활동을 관리합니다.

데이터 노드 장애

데이터 노드가 실패해도, 클러스터의 나머지 멤버는 계속해서 데이터를 처리합니다.

실패한 데이터 노드가 서비스로 돌아가면, 클러스터에서 적절한 데이터 분배를 위해 데이터 밸런스 재조정을 수행한 후 정상 처리를 재개합니다. 가동 중단 시간 동안 실패한 데이터 노드의 데이터는 사용할 수 없고, 발생한 입/출력 오류는 QRadar 사용자 인터페이스의 로그와 네트워크 보기 뷰어에 있는 검색 결과에 표시됩니다.

어플라이언스 대체 또는 QRadar의 재설치가 필요한 치명적 실패의 경우, 배치에서 데이터 노드를 해체하고 표준 설치 단계를 사용하여 대체하십시오. 실패에서 유실되지 않은 데이터는 배치하기 전에 새 데이터 노드로 복

사하십시오. 밸런스 재조정 알고리즘은 데이터 노드에 있는 데이터를 고려하고, 실패 도중 수집된 데이터만 이동시킵니다.

HA 쌍과 함께 배치된 데이터 노드의 경우, 하드웨어 실패로 인해 장애 조치가 발생하지만, 조작은 정상적으로 작동합니다.

SAN 개요

어플라이언스에서 스토리지 공간의 양을 늘리기 위해 데이터 부분을 오프보드 스토리지 디바이스로 이동시킬 수 있습니다. /store, /store/ariel 또는 /store/backup 파일 시스템을 이동시킬 수 있습니다.

외부 스토리지를 추가하기 위해 iSCSI, 파이버 채널 및 NFS(Network File System)를 포함하는 여러 방법이 사용될 수 있습니다. iSCSI 또는 파이버 채널을 사용하여 /store/ariel 디렉토리와 같은 UI에서 액세스 가능하고 검색 가능한 데이터를 저장하고, 데이터 백업 전용으로 NFS를 사용하도록 예약해야 합니다.

/store 파일 시스템을 외부 디바이스로 이동시키면 QRadar 성능에 영향을 미칠 수 있습니다.

마이그레이션 이후 /store 파일 시스템에 대한 모든 데이터 입/출력은 로컬 디스크에서 수행되지 않습니다. QRadar 데이터를 외부 스토리지 디바이스로 이동하기 전에 다음 정보를 고려해야 합니다.

- 저장됨으로 표시되는 검색도 /transient 디렉토리에 있습니다. 로컬 디스크 장애가 발생하면, 이러한 검색은 저장되지 않습니다.
- 데이터를 이동하기 전에 있던 임시 파티션은 이동 후에도 그대로 유지되고, iSCSI 또는 파이버 채널 스토리지 마운트에 마운트할 수 있습니다.

오프보드 스토리지에 대한 자세한 정보는 *IBM QRadar Security Intelligence* 오프보드 스토리지 안내서를 참조하십시오.

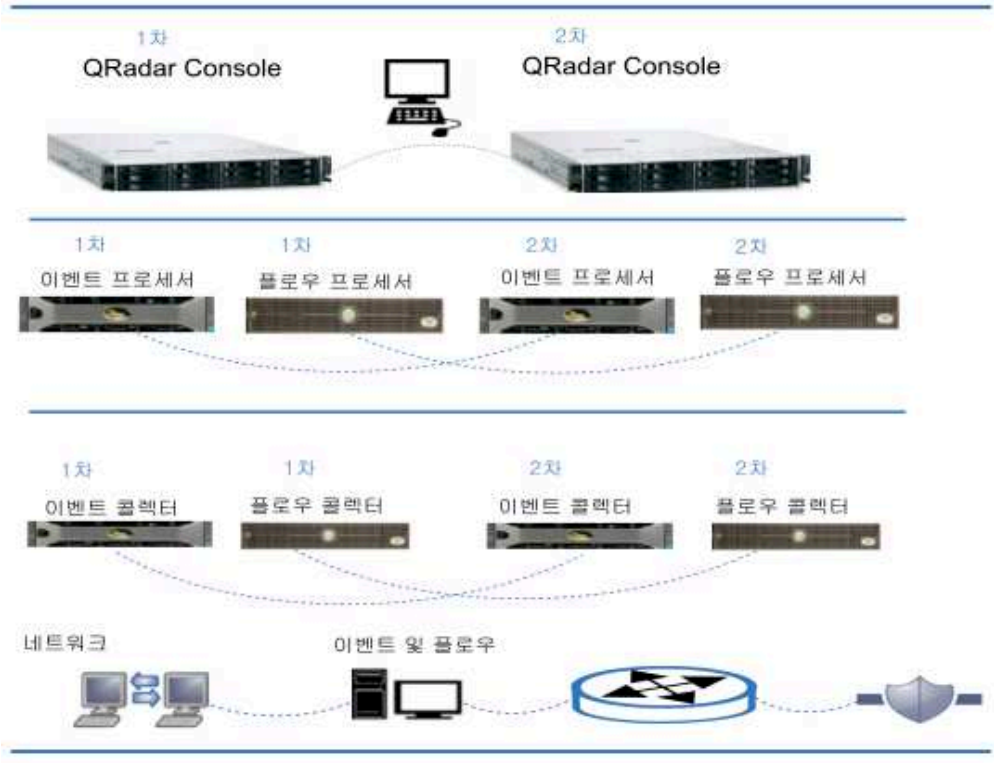
제 4 장 HA 배치 개요

배치에 하드웨어 또는 소프트웨어 장애가 있는 경우 QRadar 기능이 계속 실행되도록 IBM Security QRadar 배치에서 고가용성(HA)을 구현하십시오.

고가용성을 사용하면 장애가 발생해도 이벤트 및 플로우 데이터를 계속해서 수집하고, 저장하고 처리할 수 있습니다.

HA를 사용으로 설정하기 위해 QRadar는 1차 HA 호스트를 2차 HA 호스트에 연결하여 HA 클러스터를 작성합니다.

다음 다이어그램은 기본적인 HA 설정을 표시합니다.



HA 개요

HA 배치에서는 다음 시나리오 중 하나에서 1차 어플라이언스가 실패할 경우 디바이스의 역할을 인계하는 두 번째 어플라이언스를 설치 및 구성합니다.

- 전원 공급 장치 장애
- 네트워크 연결 테스트에서 발견되는 네트워크 장애

- 하트비트 ping 테스트를 지연시키거나 중지하는 운영 체제 고장
- 1차 HA 호스트에서 전체 RAID 장애
- 수동 장애 조치
- 1차 HA 호스트에서의 관리 인터페이스 장애

대형 배치에서 최고의 성능을 위해서는 HA 크로스오버에 대해 10Gbps 인터페이스를 사용하는 것이 좋습니다. 10Gbps 인터페이스를 사용하면 시스템 동기화에 필요한 시간이 줄어들고 쌍에 대한 최적의 성능을 보증합니다. 10Gbps 인터페이스를 사용할 수 없는 경우 크로스오버를 위해 1Gbps 인터페이스를 여러 개 연결하는 것을 고려해 보십시오.

HA에 대한 자세한 정보는 *IBM Security QRadar SIEM* 고가용성 안내서를 참조하십시오.

제 5 장 백업 전략

비즈니스에서 중요한 정보는 유실되지 않도록 안전한 곳에 백업하십시오. 다른 유형의 데이터에서는 다른 백업 전략이 필요합니다.

QRadar 데이터 백업

데이터 분류는 다음과 같은 이유로 백업 전략에서 중요한 고려사항입니다.

- PII(personal identity information)와 같은 데이터는 안전하게 저장되어야 하고, 벌크 데이터 백업과 분리하여 보관되어야 하며, 규정 준수 이유로 장기간 유지되어야 합니다.
- QRadar 시스템 구성 데이터는 이벤트 및 플로우와 같은 보안 데이터와 별도로 보관하십시오. 시스템 구성을 분리하여 보관하는 것이 더 안전하며 분리하여 저장하는 경우 데이터 복원이 쉬워집니다.
- 감사원이 보려고 할 때 데이터에 쉽게 액세스할 수 있도록 PCI 데이터와 같은 데이터는 별도의 위치에 저장하십시오.
- 백업 전략을 개발할 때 데이터 유형과 보존 기간에 대해 생각하십시오.
- 일부 유형의 데이터는 다른 유형보다 더 자주 백업할 수 있고 일부 데이터는 유실되지 않도록 하기 위해 오프사이트 스토리지를 사용할 수 있습니다.

보존 설정

QRadar 백업 보존의 기본 설정은 7일입니다. 주요 구성을 변경한 후 요청 시 백업을 수행할 수도 있습니다. 이 구성으로 돌아가야 하는 경우 변경사항을 쉽게 찾을 수 있도록 이 요청 시 백업에 설명 이름을 지정할 수 있습니다.

스케줄링된 백업은 이전에 스케줄링된 백업을 겹쳐씁니다. 요청 시 백업은 무기한으로 유지됩니다. QRadar 백업 볼륨이 용량의 75%에 도달하면, 스케줄링된 백업이 더 이상 실행되지 않습니다.

백업 위치

백업 위치도 QRadar를 배치할 때 중요한 고려사항입니다. 백업이 호스트에 남아 있고 해당 호스트가 실패하면, 모든 백업 데이터는 유실됩니다.

외부 시스템에서 백업을 작성하거나 외부 시스템으로 백업을 복사할 수 있습니다.

추가된 데이터 보안에 대해 로컬 및 원격으로 중요 데이터 사본을 저장하십시오.

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 구체적인 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 확인할 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 웹상의 "저작권 및 상표 정보"(www.ibm.com/legal/copytrade.shtml)에 있습니다.

Linux는 미국 또는 기타 국가에서 사용되는 Linus Torvalds의 등록상표입니다.

Java™ 및 모든 Java 기반 상표와 로고는 Oracle 및/또는 그 계열사의 상표 또는 등록상표입니다.

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 IBM

의 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.

해당 용도의 쿠키를 포함하여 다양한 기술의 사용에 대한 자세한 정보는 IBM 개인보호 보호정책(http://www.ibm.com/privacy/kr/ko), IBM 온라인 개인정보

보호정책(http://www.ibm.com/privacy/details/kr/ko) 및 "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.

개인정보 보호정책 고려사항

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.

해당 용도의 쿠키를 포함하여 다양한 기술의 사용에 대한 자세한 정보는 IBM 개인보호 보호정책(http://www.ibm.com/privacy), IBM 온라인 개인정보 보호정책(http://www.ibm.com/privacy/details) 및 "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.