IBM Security QRadar

로그 소스 사용자 안내서

*2016*년 *4*월

IBM

참고

이 정보와 이 정보가 지원하는 제품을 사용하기 전에, 65 페이지의 『주의사항』의 정보를 읽으십시오.

제품 정보

본 문서의 업데이트된 버전에서 달리 대체되지 않는 한 본 문서는 IBM QRadar Security Intelligence Platform V7.2.5 및 후속 릴리스에 적용됩니다.

목차

이 안내서의 정보

로그 소스는 IBM® Security QRadar®에 수집, 저장, 구문 분석 및 처리를 위한 이벤트를 보내는 써드파티 디바이스입니다.

이 책의 사용자

관리자는 QRadar 액세스 권한과 회사 네트워크 및 네트워킹 기술에 대한 지식이 있어야 합니다.

기술 문서

번역된 모든 문서를 포함하여 IBM Security QRadar 제품 문서를 웹에서 찾으려면 IBM Knowledge Center(http://www.ibm.com/support/knowledgecenter/SS42VS/welcome)에 액세스하십시오.

QRadar 제품 라이브러리에 있는 추가 기술 문서에 액세스하는 방법에 대한 정보는 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 기술 노트 지원 및 다운로드 (http://www.ibm.com/support/docview.wss?uid=swg21616144)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 시스템, 제품 및 서비스는 추가적인 작동 프로시저가 필요한 합법적인 포괄적 보안 접근 방법의 일부가 되도록 디자인되었으며 최대의 효율을 발휘하기 위해 다른 시스템, 제품 또는 서비스가 필요할 수 있습니다. IBM은 시스템, 제품 또는 서비스가 외부의 악의적이거나 불법적인 행위로부터 안전하다거나 이러한 행위로부터 귀하의 엔터프라이즈를 안전하게 지킨다고 보증하지 않습니다.

참고:

이 프로그램의 사용은 여러 가지 법규 또는 규정과 관련될 수 있습니다(개인정보 보호정책, 데이터 보호, 고용, 전자 통신 및 스토리지에 관련된 법규 또는 규정을 포함). IBM Security QRadar는 합법적인 목적과 합법적인 방법으로만 사용될 수 있습니다. 고객은 해당 법률, 규정 및 정책에 따라 이 프로그램을 사용할 것에 동의하며, 이들을 준수할 모든 책임을 갖고 있습니다. 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 로그 소스 관리 소개

네트워크에 있는 로그 소스로부터의 이벤트 로그를 수락하도록 IBM Security QRadar를 구성할 수 있습니다. 로그 소스는 이벤트 로그를 작성하는 데이터 소스입니다.

예를 들어, 방화벽 또는 IPS(Intrusion Protection System)는 보안 기반 이벤트를 로그하고 스위치 또는 라우터는 네트워크 기반 이벤트를 로그합니다.

로그 소스에서 원시 이벤트를 수신하기 위해 QRadar는 다수의 프로토콜을 지원합니다. 수동 프로토콜은 특정 포트에서 이벤트를 청취합니다. 활성 프로토콜은 API 또는 다른 통신 방법을 사용하여 이벤트를 폴링하고 검색하는 외부 시스템에 연결합니다.

라이센스 한계에 따라, QRadar는 300개가 넘는 로그 소스에서 이벤트를 읽고 해석할 수 있습니다.

QRadar에 대한 로그 소스를 구성하려면 다음 태스크를 수행해야 합니다.

1. 로그 소스를 지원하는 디바이스 지원 모듈(DSM)을 다운로드하여 설치하십시오. *DSM*은 원래 형식의 이벤트 로그에서 이벤트를 식별하여 QRadar에서 사용할 수 있는 형식으로 구문 분석하는 데 필요한 이벤트 패턴이 포함된 소프트웨어 애플리케이션입니다. DSM과 지원되는 로그 소스에 대한 자세한 정보는 *DSM* 구성 안내서를 참조하십시오.
2. DSM에 자동 감지가 지원되는 경우, QRadar가 구성된 로그 소스 목록에 로그 소스를 자동으로 추가할 때까지 기다리십시오.
3. DSM에 자동 감지가 지원되지 않는 경우에는 로그 소스 구성을 수동으로 작성하십시오.

로그 소스 추가

로그 소스가 자동으로 감지되지 않는 경우, 네트워크 디바이스 또는 어플라이언스에서 이벤트를 수신하기 위해 로그 소스를 수동으로 추가할 수 있습니다.

이 태스크 정보

다음 표는 모든 로그 소스 유형에 공통되는 로그 소스 매개변수를 설명합니다.

표 *1.* 로그 소스 매개변수

매개변수	설명
로그 소스 ID	로그 소스를 식별하는 IPv4 주소 또는 호스트 이름입니다. 네트워크에서 단일 관리 콘솔에 여러 개의 디바이스가 연결된 경우, 이벤트를 작성한 개별 디바이스의 IP 주소를 지정하십시오. IP 주소와 같이 각각에 고유한 ID를 사용하면 이벤트 검색 시 관리 콘솔이 모든 이벤트의 소스로 식별되지 않습니다.
사용	이 옵션이 사용되지 않는 경우, 로그 소스는 이벤트를 수집하지 않으며 라이센스 한계에 포함되지 않습니다.
신뢰성	신뢰성은 로그 소스에서 작성한 이벤트의 무결성 또는 유효성을 나타냅니다. 로그 소스에 지정된 신뢰성 값은 수신되는 이벤트를 기반으로 증가 또는 감소되거나 사용자 작성 이벤트 규칙에 대한 응답으로서 조정될 수 있습니다. 로그 소스에 의한 이벤트의 신뢰성은 오펜스 위험지표의 계산에 기여하며 오펜스의 위험지표 값을 증가 또는 감소시킬 수 있습니다.
대상 이벤트 콜렉터	원격 로그 소스를 폴링하는 QRadar 이벤트 콜렉터를 지정합니다. 폴링 태스크를 이벤트 콜렉터로 이동시켜 콘솔 시스템 성능을 향상시키려면 분산 배치에서 이 매개변수를 사용하십시오.
통합 이벤트	짧은 간격 내에서 같은 이벤트가 여러 번 발생하는 경우 이벤트 수를 증가시킵니다. 통합 이벤트에서는 **로그 보기** 탭에서 단일 이벤트 유형이 발생하는 빈도를 보고 판별하는 방법을 제공합니다. 이 선택란이 선택 취소된 경우, 이벤트는 개별적으로 표시되며 번들화되지 않습니다. 신규 및 자동으로 감지되는 로그 소스는 **관리** 탭의 **시스템 설정** 구성에서 이 선택란의 값을 상속합니다. 이 선택란을 사용하여 개별 로그 소스에 대한 시스템 설정의 기본 작동을 겹쳐쓸 수 있습니다.

프로시저

1. **관리** 탭을 클릭하십시오.
2. **로그 소스** 아이콘을 클릭하십시오.

3. **추가**를 클릭하십시오.
4. 로그 소스의 공통 매개변수를 구성하십시오.
5. 로그 소스의 프로토콜 특정 매개변수를 구성하십시오.
6. **저장**을 클릭하십시오.
7. **관리** 탭에서 **변경사항 배치**를 클릭하십시오.

Blue Coat Web Security Service REST API 프로토콜 구성 옵션

Blue Coat Web Security Service로부터 이벤트를 수신하려면 Blue Coat Web Security Service REST API 프로토콜을 사용하도록 로그 소스를 구성하십시오.

Blue Coat Web Security Service REST API 프로토콜은 Blue Coat Web Security Service Sync API를 조회하여 클라우드에서 최근에 확정된 로그 데이터를 검색합니다.

다음 표는 Blue Coat Web Security Service REST API 프로토콜의 프로토콜 특정 매개변수에 대해 설명합니다.

표 *2. Blue Coat Web Security Service REST API* 프로토콜 매개변수

매개변수	설명
API 사용자 이름	Blue Coat Web Security Service에 인증하기 위해 사용되는 API 사용자 이름입니다. API 사용자 이름은 Blue Coat Threat Pulse Portal을 통해 구성합니다.
비밀번호	Blue Coat Web Security Service에 인증하기 위해 사용되는 비밀번호입니다.
비밀번호 확인	**비밀번호** 필드를 확인합니다.
프록시 사용	프록시를 구성하면 로그 소스의 모든 트래픽이 Blue Coat Web Security Service에 액세스하기 위해 QRadar의 프록시를 통해 이동합니다. **프록시 IP 또는 호스트 이름**, **프록시 포트**, **프록시 사용자 이름** 및 **프록시 비밀번호** 필드를 구성하십시오. 프록시에 인증이 필요하지 않은 경우 **프록시 사용자 이름** 및 **프록시 비밀번호** 필드를 비워둘 수 있습니다.
서버 인증서 자동 획득	목록에서 예를 선택하는 경우 QRadar는 인증서를 다운로드하고 대상 서버의 신뢰 처리를 시작합니다.
반복	로그에서 데이터를 수집하는 시간을 지정할 수 있습니다. 형식은 M/H/D(월/시간/일)입니다. 기본값은 5 M입니다.
EPS 제한	초당 최대 이벤트 수(EPS)의 상한입니다. 기본값은 5000입니다.

Cisco NSEL 프로토콜 구성 옵션

Cisco ASA(Adaptive Security Appliance)로부터의 NetFlow 패킷 플로우를 모니터하려면 Cisco NSEL(Network Security Event Logging) 프로토콜 소스를 구성하십시오.

Cisco NSEL을 QRadar와 통합하려면 NetFlow 이벤트를 수신하는 로그 소스를 수동으로 작성해야 합니다. QRadar는 Cisco NSEL로부터의 syslog 이벤트에 대한 로그 소스를 자동으로 감지하거나 작성하지 않습니다. 자세한 정보는 *DSM* 구성 안내서를 참조하십시오.

다음 표는 Cisco NSEL 프로토콜의 프로토콜 특정 매개변수를 설명합니다.

표 *3. Cisco NSEL* 프로토콜 매개변수

매개변수	설명
프로토콜 구성	**Cisco NSEL**
로그 소스 ID	네트워크에서 여러 디바이스가 하나의 관리 콘솔에 연결된 경우, 이벤트를 작성한 개별 디바이스의 IP 주소를 지정할 수 있습니다. IP 주소와 같이 각각에 고유한 ID를 사용하면 이벤트 검색 시 관리 콘솔이 모든 이벤트의 소스로 식별되지 않습니다.
콜렉터 포트	Cisco ASA가 NSEL 이벤트를 전달하는 데 사용하는 UDP 포트 번호입니다. QRadar는 QRadar QFlow Collector에서 플로우 데이터에 포트 2055를 사용합니다. NetFlow의 경우 Cisco Adaptive Security Appliance에서 다른 UDP 포트를 지정해야 합니다.

EMC VMware 프로토콜 구성 옵션

가상 환경을 위한 VMWare 웹 서비스에서 이벤트 데이터를 수신하려면 EMC VMWare 프로토콜을 사용하는 로그 소스를 구성하십시오.

다음 표는 EMC VMware 프로토콜의 프로토콜 특정 매개변수를 설명합니다.

표 *4. EMC VMware* 프로토콜 매개변수

매개변수	설명
프로토콜 구성	**EMC VMware**
로그 소스 ID	이 매개변수의 값은 **VMware IP** 매개변수와 일치해야 합니다.
VMware IP	VMWare ESXi 서버의 IP 주소입니다(예: 1.1.1.1). VMware 프로토콜은 이벤트 데이터를 요청하기 전에 HTTPS와 함께 VMware ESXi 서버의 IP 주소를 추가합니다.

전달된 프로토콜 구성 옵션

배치에 포함된 다른 콘솔에서 이벤트를 수신하려면 전달된 프로토콜을 사용하는 로그 소스를 구성하십시오.

전달된 프로토콜은 주로 다른 QRadar 콘솔에 이벤트를 전달하는 데 사용됩니다. 예를 들어, 콘솔 A의 오프사이트 대상으로 콘솔 B가 구성되어 있습니다. 자동으로 발견되는 로그 소스의 데이터는 콘솔 B로 전달됩니다. 콘솔 A에서 수동으로 작성된 로그 소스도 전달된 프로토콜을 사용하여 콘솔 B에 로그 소스로 추가해야 합니다.

IBM Tivoli Endpoint Manager SOAP 프로토콜 구성 옵션

IBM Tivoli® Endpoint Manager 어플라이언스에서 LEEF(Log Extended Event Format) 형식화 이벤트를 수신하려면 IBM Tivoli Endpoint Manager SOAP 프로토콜을 사용하는 로그 소스를 구성하십시오.

이 프로토콜은 IBM Tivoli Endpoint Manager 버전 V8.2.x 이상과 Tivoli Endpoint Manager용 Web Reports 애플리케이션이 필요합니다.

Tivoli Endpoint Manager SOAP 프로토콜은 HTTP 또는 HTTPS를 통해 30초 간격으로 이벤트를 검색합니다. 이벤트가 검색되면 IBM Tivoli Endpoint Manager DSM이 이벤트를 구문 분석하고 분류합니다.

다음 표는 IBM Tivoli Endpoint Manager SOAP 프로토콜의 프로토콜 특정 매개변수를 설명합니다.

표 *5. IBM Tivoli Endpoint Manager SOAP* 프로토콜 매개변수

매개변수	설명
프로토콜 구성	**IBM Tivoli Endpoint Manager SOAP**
HTTPS 사용	HTTPS로 연결하는 데 인증서가 필요한 경우, 필요한 인증서를 /opt/qradar/conf/trusted_certificates 디렉토리에 복사하십시오. .crt, .cert 또는 .der 파일 확장자를 갖는 인증서가 지원됩니다. 로그 소스가 저장되고 배치되기 전에 인증서를 신뢰 인증서 디렉토리에 복사하십시오.
SOAP 포트	기본적으로 포트 80이 IBM Tivoli Endpoint Manager와 통신하기 위한 포트 번호입니다. 대부분의 구성에서는 HTTPS 통신에 포트 443을 사용합니다.

JDBC 프로토콜 구성 옵션

QRadar는 JDBC 프로토콜을 사용하여 여러 데이터베이스 유형의 이벤트 데이터가 포함된 테이블 또는 보기에서 정보를 수집합니다.

다음 표는 JDBC 프로토콜의 프로토콜 특정 매개변수를 설명합니다.

표 *6. JDBC* 프로토콜 매개변수

매개변수	설명
데이터베이스 유형	이 목록 상자에서 이벤트가 포함된 데이터베이스의 유형을 선택하십시오.
데이터베이스 이름	데이터베이스 이름은 **로그 소스 ID** 필드에 지정된 데이터베이스 이름과 일치해야 합니다.
포트	JDBC 포트는 원격 데이터베이스에 구성된 청취 포트와 일치해야 합니다. 데이터베이스는 수신 TCP 연결을 허용해야 합니다. MSDE 데이터베이스 유형과 함께 **데이터베이스 인스턴스**를 사용하는 경우, 로그 소스 구성에서 **포트** 매개변수를 비워 둬야 합니다.
사용자 이름	데이터베이스에서 QRadar의 사용자 계정입니다.

표 *6. JDBC* 프로토콜 매개변수 *(계속)*

매개변수	설명
비밀번호	데이터베이스에 연결하기 위해 필요한 비밀번호입니다.
비밀번호 확인	데이터베이스에 연결하기 위해 필요한 비밀번호입니다.
인증 도메인	하나의 Windows 도메인에 있는 MSDE 데이터베이스에 대해 도메인을 구성해야 합니다. 네트워크가 도메인을 사용하지 않는 경우에는 이 필드를 비워 두십시오.
데이터베이스 인스턴스	필요한 경우에 사용되는 데이터베이스 인스턴스입니다. MSDE 데이터베이스는 하나의 서버에서 여러 SQL 서버 인스턴스를 포함할 수 있습니다. 해당 데이터베이스에 표준 포트가 아닌 포트를 사용하거나 SQL 데이터베이스 분석을 위해 포트 1434에 대한 액세스가 차단되는 경우, 로그 소스 구성에서 **데이터베이스 인스턴스** 매개변수를 비워 둬야 합니다.
사전정의 조회	선택사항입니다.
테이블 이름	이벤트 레코드를 포함하는 테이블 또는 보기의 이름입니다. 테이블 이름에는 특수 문자인 달러 부호($), 숫자 부호(#), 밑줄(_), 엔 대시(-) 및 마침표(.)가 포함될 수 있습니다.
선택 목록	테이블에서 이벤트를 폴링할 때 포함시킬 필드 목록입니다. 쉼표로 구분된 목록을 사용하거나 *를 입력하여 테이블 또는 보기의 모든 필드를 선택할 수 있습니다. 쉼표로 구분된 목록을 정의하는 경우, **비교 필드**에 정의된 필드가 목록에 포함되어야 합니다.
비교 필드	조회 사이에 테이블에 추가되는 새 테이블 이벤트를 식별하는 테이블 또는 보기의 숫자 값 또는 시간소인 필드입니다. 중복 이벤트가 작성되지 않도록 하기 위해 프로토콜이 이전에 폴링한 이벤트를 식별할 수 있도록 합니다.
준비된 명령문 사용	준비된 명령문을 사용하면 JDBC 프로토콜 소스가 SQL문을 설정한 후 서로 다른 매개변수를 사용하여 해당 SQL문을 여러 번 실행할 수 있습니다. 보안 및 성능을 위해, 대부분의 JDBC 프로토콜 구성에서 준비된 명령문을 사용할 수 있습니다.
시작 날짜 및 시간	시작 날짜를 정의하지 않은 경우, 프로토콜은 로그 소스 구성이 저장되고 배치된 후 이벤트를 폴링하려고 시도합니다.
폴링 간격	기본 폴링 간격은 10초입니다.
EPS 제한	허용되는 초당 이벤트 수(EPS)의 상한입니다.
데이터베이스 로케일	다국어 설치는 **데이터베이스 로케일** 필드를 사용하여 사용할 언어를 지정하십시오.
데이터베이스 코드 세트	다국어 설치는 **코드 세트** 필드를 사용하여 사용할 문자 세트를 지정하십시오.
이름지정된 파이프 통신 사용	MSDE 데이터베이스에 대한 이름지정된 파이프 연결의 경우, 사용자 이름 및 비밀번호 필드에 데이터베이스 사용자 이름 및 비밀번호 대신 Windows 인증 사용자 이름 및 비밀번호를 사용해야 합니다. 로그 소스 구성은 MSDE 데이터베이스의 기본 이름 지정된 파이프를 사용해야 합니다.
NTLMv2 사용	**NTLMv2 사용** 선택란은 NTLMv2 인증이 필요 없는 MSDE 연결에 대해서는 통신을 인터럽트하지 않습니다.

표 *6. JDBC* 프로토콜 매개변수 *(계속)*

매개변수	설명
Oracle 암호화 사용	Oracle 암호화 및 데이터 무결성 설정은 Oracle 고급 보안으로도 알려져 있습니다. 선택하는 경우 Oracle JDBC 연결을 사용하려면 서버에서 클라이언트와 유사한 Oracle 데이터 암호화 설정을 지원해야 합니다.
SSL	연결에서 SSL을 지원하는 경우 SSL 선택란을 선택하십시오. 이 옵션은 MSDE에 대해서만 표시됩니다.

JDBC SiteProtector 구성 옵션

JDBC(Java™ Database Connectivity) SiteProtector™ 프로토콜을 사용하여 원격으로 IBM Proventia® Management SiteProtector® 데이터베이스에서 이벤트를 폴링하는 로그 소스를 구성할 수 있습니다.

JDBC - SiteProtector 프로토콜은 로그 소스 페이로드 작성에서 SensorData1과 SensorDataAVP1 테이블의 정보를 결합합니다. SensorData1 및 SensorDataAVP1 테이블은 IBM Proventia® Management SiteProtector® 데이터베이스에 있습니다. JDBC - SiteProtector 프로토콜이 단일 조회에서 폴링할 수 있는 최대 행 수는 30,000행입니다.

다음 표는 JDBC - SiteProtector 프로토콜의 프로토콜 특정 매개변수를 설명합니다.

표 *7. JDBC - SiteProtector* 프로토콜 매개변수

매개변수	설명
프로토콜 구성	**JDBC - SiteProtector**
데이터베이스 유형	목록에서 이벤트 소스에 사용할 데이터베이스 유형으로 **MSDE**를 선택하십시오.
데이터베이스 이름	프로토콜이 연결할 수 있는 데이터베이스의 이름인 `RealSecureDB`를 입력하십시오.
IP 또는 호스트 이름	데이터베이스 서버의 IP 주소 또는 호스트 이름입니다.
포트	데이터베이스 서버에 사용되는 포트 번호입니다. JDBC SiteProtector 구성 포트는 데이터베이스의 리스너 포트와 일치해야 합니다. 데이터베이스는 수신 TCP 연결을 허용해야 합니다. MSDE를 데이터베이스 유형으로 사용할 때 **데이터베이스 인스턴스**를 정의하는 경우, 로그 소스 구성에서 **포트** 매개변수를 비워 둬야 합니다.
사용자 이름	JDBC 프로토콜을 통한 데이터베이스 액세스를 추적하려는 경우 QRadar 시스템에 특정 사용자를 작성할 수 있습니다.
인증 도메인	MSDE를 선택하고 데이터베이스를 Windows용으로 구성한 경우에는 Windows 도메인을 정의해야 합니다. 네트워크가 도메인을 사용하지 않는 경우에는 이 필드를 비워 두십시오.

표 7. *JDBC - SiteProtector* 프로토콜 매개변수 *(계속)*

매개변수	설명
데이터베이스 인스턴스	MSDE를 선택하며 하나의 서버에 여러 SQL 서버 인스턴스가 있는 경우 연결하려는 인스턴스를 정의하십시오. 데이터베이스 구성에서 표준 포트가 아닌 포트를 사용하거나 SQL 데이터베이스 분석을 위해 포트 1434에 대한 액세스가 차단되는 경우, 구성에서 **데이터베이스 인스턴스** 매개변수를 비워 둬야 합니다.
사전정의 조회	사용하는 로그 소스에 대한 사전정의된 데이터베이스 조회입니다. 사전정의된 데이터베이스 조회는 특수 로그 소스 연결에만 사용 가능합니다.
테이블 이름	SensorData1
AVP 보기 이름	SensorDataAVP
응답 보기 이름	SensorDataResponse
선택 목록	테이블 또는 보기의 모든 필드를 포함시키려면 *를 입력하십시오.
비교 필드	SensorDataRowID
준비된 명령문 사용	준비된 명령문을 사용하면 JDBC 프로토콜 소스가 SQL문을 설정한 후 서로 다른 매개변수를 사용하여 해당 SQL문을 여러 번 실행할 수 있습니다. 보안 및 성능을 위해 준비된 명령문을 사용하십시오. 미리 컴파일된 명령문을 사용하지 않는 다른 조회 방법을 사용하려면 이 선택란을 선택 취소하십시오.
감사 이벤트 포함	IBM SiteProtector®에서 감사 이벤트를 수집하도록 지정합니다.
시작 날짜 및 시간	선택사항입니다. 프로토콜이 데이터베이스 폴링을 시작할 수 있는 시작 날짜 및 시간입니다.
폴링 간격	이벤트 테이블 조회 사이의 시간 간격입니다. 숫자 값에 H(시간의 경우) 또는 M(분의 경우)을 추가하여 보다 긴 폴링 간격을 정의할 수 있습니다. H 또는 M 지정자가 없는 숫자 값은 초 단위로 폴링합니다.
EPS 제한	이 프로토콜이 초과하지 못하도록 할 초당 이벤트 수(EPS)입니다.
데이터베이스 로케일	다국어 설치는 **데이터베이스 로케일** 필드를 사용하여 사용할 언어를 지정하십시오.
데이터베이스 코드 세트	다국어 설치는 **코드 세트** 필드를 사용하여 사용할 문자 세트를 지정하십시오.
이름지정된 파이프 통신 사용	데이터베이스 유형으로 MSDE를 선택하는 경우, TCP/IP 포트 연결의 대체 방법을 사용하려면 이 선택란을 선택하십시오. 이름지정된 파이프 연결을 사용하는 경우, 사용자 이름 및 비밀번호는 데이터베이스 사용자 이름 및 비밀번호가 아니라 해당 Windows 인증 사용자 이름 및 비밀번호이어야 합니다. 로그 소스 구성은 기본 이름지정된 파이프를 사용해야 합니다.
데이터베이스 클러스터 이름	이름지정된 파이프 통신이 제대로 작동하도록 하기 위한 클러스터 이름입니다.
NTLMv2 사용	NTLMv2 인증이 필요한 SQL 서버의 경우 MSDE 연결이 NTLMv2 프로토콜을 사용하도록 합니다. **NTLMv2 사용** 선택란은 NTLMv2 인증이 필요 없는 MSDE 연결에 대해서는 통신을 인터럽트하지 않습니다.
SSL 사용	JDBC 프로토콜에 SSL 암호화를 사용합니다.

표 *7. JDBC - SiteProtector* 프로토콜 매개변수 *(계속)*

매개변수	설명
로그 소스 언어	로그 소스가 생성하는 이벤트의 언어를 선택하십시오. 로그 소스 언어는 시스템이 여러 언어로 이벤트를 작성할 수 있는 외부 어플라이언스 또는 운영 체제로부터의 이벤트를 구문 분석하는 데 도움이 됩니다.

Juniper Networks NSM 프로토콜 구성 옵션

Juniper Networks NSM 및 Juniper Networks Secure Service Gateway(SSG) 로그 이벤트를 수신하려면 Juniper Networks NSM 프로토콜을 사용하는 로그 소스를 구성하십시오.

다음 표는 Juniper Networks NSM(Network and Security Manager) 프로토콜의 프로토콜 특정 매개변수를 설명합니다.

표 *8. Juniper Networks NSM* 프로토콜 매개변수

매개변수	설명
로그 소스 유형	**Juniper Networks Network and Security Manager**
프로토콜 구성	**Juniper NSM**

Juniper Security Binary Log Collector 프로토콜 구성 옵션

Security Binary Log Collector 프로토콜을 사용하는 로그 소스를 구성할 수 있습니다. Juniper 어플라이언스는 이 프로토콜을 사용하여 QRadar에 감사, 시스템, 방화벽 및 IPS(Intrusion Prevention System) 이벤트를 보낼 수 있습니다.

Juniper SRX 또는 J Series 어플라이언스로부터의 2진 로그 형식은 UDP 프로토콜을 통해 스트림됩니다. 2진 형식 이벤트를 스트림하기 위한 고유한 포트를 지정해야 합니다. 표준 syslog 포트 514는 2진 형식 이벤트에 사용할 수 없습니다. Juniper 어플라이언스에서 스트림되는 2진 이벤트를 수신하기 위해 지정되는 기본 포트는 40798 포트입니다.

다음 표는 Juniper Security Binary Log Collector 프로토콜의 프로토콜 특정 매개변수를 설명합니다.

표 *9. Juniper Security Binary Log Collector* 프로토콜 매개변수

매개변수	설명
프로토콜 구성	**Security Binary Log Collector**
XML 템플리트 파일 위치	Juniper SRX 또는 Juniper J Series 어플라이언스로부터의 2진 스트림을 디코드하는 데 사용되는 XML 파일의 경로입니다. 기본적으로, 디바이스 지원 모듈(DSM)에는 2진 스트림 디코드를 위한 XML 파일이 포함됩니다. 이 XML 파일은 `/opt/qradar/conf/security_log.xml` 디렉토리에 있습니다.

로그 파일 프로토콜 구성 옵션

원격 호스트에서 이벤트를 수신하려면 로그 파일 프로토콜을 사용하는 로그 소스를 구성하십시오.

로그 파일 프로토콜은 매일 이벤트 로그를 작성하는 시스템을 위한 것입니다. 해당 이벤트 파일에 정보를 추가하는 디바이스에 로그 파일 프로토콜을 사용하는 것은 적절하지 않습니다.

로그 파일은 한 번에 하나씩 검색됩니다. 로그 파일 프로토콜은 평문, 압축 파일 또는 파일 아카이브를 관리할 수 있습니다. 아카이브에는 한 번에 한 라인씩 처리할 수 있는 평문 파일이 포함되어야 합니다. 로그 파일 프로토콜이 이벤트 파일을 다운로드하면, 파일에서 수신되는 정보가 **로그 보기** 탭을 업데이트합니다. 다운로드가 완료된 후 파일에 추가 정보가 기록되는 경우, 추가된 정보는 처리되지 않습니다.

다음 표는 로그 파일 프로토콜의 프로토콜 특정 매개변수에 대해 설명합니다.

표 *10.* 로그 파일 프로토콜 매개변수

매개변수	**설명**
프로토콜 구성	**로그 파일**
원격 포트	원격 호스트에서 표준 포트가 아닌 포트 번호를 사용하는 경우, 이벤트를 검색하기 위해 포트 값을 조정해야 합니다.
SSH 키 파일	시스템이 키 인증을 사용하도록 구성된 경우, SSH 키의 경로입니다. SSH 키 파일이 사용되면 **원격 비밀번호** 필드는 무시됩니다.
원격 디렉토리	FTP의 경우, 로그 파일이 원격 사용자의 홈 디렉토리에 있으면 원격 디렉토리를 비워 둘 수 있습니다. 빈 원격 디렉토리 필드는 작업 중인 디렉토리(CWD) 명령의 변경이 제한되는 시스템을 지원합니다.
반복	FTP 또는 SFTP 연결에서 이벤트 데이터에 대한 원격 디렉토리의 하위 폴더를 반복적으로 검색하도록 허용하려면 이 선택란을 사용하십시오. 하위 폴더에서 수집되는 데이터는 FTP 파일 패턴의 정규식과 일치하는 항목에 따라 달라집니다. SCP 연결의 경우 **반복** 옵션을 사용할 수 없습니다.
FTP 파일 패턴	원격 호스트에서 다운로드할 파일을 식별하는 데 필요한 정규식(regex)입니다.
FTP 전송 모드	FTP를 통한 ASCII 전송의 경우, **프로세서** 필드에서 NONE을 선택하고 **이벤트 생성기** 필드에서 LINEBYLINE을 선택해야 합니다.
반복	새 이벤트 로그 파일을 확인하기 위해 원격 디렉토리를 스캔하는 빈도를 결정하는 시간 간격입니다. 시간 간격에는 시간(H), 분(M) 또는 일(D) 단위의 값이 포함될 수 있습니다. 예를 들어, 2H 반복은 원격 디렉토리를 2시간마다 스캔합니다.

표 *10.* 로그 파일 프로토콜 매개변수 *(계속)*

매개변수	설명
저장 시 실행	로그 소스 구성을 저장하는 즉시 로그 파일 가져오기를 시작합니다. 이 선택란을 선택하면 이전에 다운로드하여 처리한 파일의 목록이 지워집니다. 첫 번째 파일 가져오기 후, 로그 파일 프로토콜은 관리자가 정의한 시작 시간 및 반복 스케줄을 따릅니다.
EPS 제한	이 프로토콜이 초과할 수 없는 초당 이벤트 수(EPS)입니다.
로컬 디렉토리를 변경하시겠습니까?	이벤트 로그가 처리되기 전에 이벤트 로그를 저장할 **대상 이벤트 콜렉터**의 로컬 디렉토리를 변경합니다.
로컬 디렉토리	**대상 이벤트 콜렉터**의 로컬 디렉토리입니다. 로그 파일 프로토콜이 이벤트를 검색하려고 시도하기 전에 이 디렉토리가 존재해야 합니다.
파일 인코딩	로그 파일의 이벤트에서 사용되는 문자 인코딩입니다.
폴더 구분 기호	사용하는 운영 체제에서 폴더를 구분하는 데 사용되는 문자입니다. 대부분의 구성은 **폴더 구분 기호** 필드에 기본값을 사용할 수 있습니다. 이 필드는 다른 문자를 사용하여 폴더를 구분하는 운영 체제를 위한 것입니다. 메인프레임 시스템에서 폴더를 구분하는 마침표를 예로 들 수 있습니다.

Microsoft DHCP 프로토콜 구성 옵션

Microsoft DHCP 서버에서 이벤트를 수신하려면 Microsoft DHCP 프로토콜을 사용하는 로그 소스를 구성하십시오.

로그 파일을 읽으려면, 관리 공유(C$)가 포함된 폴더 경로는 해당 관리 공유(C$)에 대해 NetBIOS 권한이 있어야 합니다. 로컬 또는 도메인 관리자는 관리 공유의 로그 파일에 액세스하기에 충분한 권한이 있습니다.

관리자는 파일 경로를 지원하는 Microsoft DHCP 프로토콜의 필드를 사용하여 드라이브 이름과 경로 정보를 정의할 수 있습니다. 예를 들어, 관리 공유의 경우 필드에 `c$/LogFiles/` 디렉토리가 포함되고 공용 공유 폴더 경로의 경우 필드에 `LogFiles/` 디렉토리가 포함될 수 있습니다. 단, `c:/LogFiles` 디렉토리는 포함될 수 없습니다.

제한사항: Microsoft 인증 프로토콜 NTLMv2는 Microsoft DHCP 프로토콜에서 지원하지 않습니다.

다음 표는 Microsoft DHCP 프로토콜의 프로토콜 특정 매개변수를 설명합니다.

표 *11. Microsoft DHCP* 프로토콜 매개변수

매개변수	설명
프로토콜 구성	**Microsoft DHCP**
도메인	선택사항입니다.
폴더 경로	DHCP 로그 파일의 디렉토리 경로입니다.

표 *11. Microsoft DHCP* 프로토콜 매개변수 *(계속)*

매개변수	설명
파일 패턴	이벤트 로그를 식별하는 정규식(regex)입니다. 로그 파일에는 요일을 나타내는 3자 약어가 포함되어야 합니다. 다음 파일 패턴 중 하나를 사용하십시오. • IPv4 파일 패턴: `DhcpSrvLog-(?:Sun|Mon|Tue|Wed|Thu|Fri|Sat) \.log`. • IPv6 파일 패턴: `DhcpV6SrvLog-(?:Sun|Mon|Tue|Wed|Thu|Fri|Sat) \.log`. • IPv4 및 IPv6 파일 혼합 패턴: `Dhcp.*SrvLog-(?:Sun|Mon|Tue|Wed|Thu|Fri|Sat) \.log`.

Microsoft Exchange 프로토콜 구성 옵션

SMTP, OWA 및 Microsoft Exchange 2007 및 2010 서버에서 이벤트를 수신하려면 지원할 Microsoft Windows Exchange 프로토콜을 사용하는 로그 소스를 구성하십시오.

로그 파일을 읽으려면, 관리 공유(C$)가 포함된 폴더 경로는 해당 관리 공유(C$)에 대해 NetBIOS 권한이 있어야 합니다. 로컬 또는 도메인 관리자는 관리 공유의 로그 파일에 액세스하기에 충분한 권한이 있습니다.

관리자는 파일 경로를 지원하는 Microsoft Exchange 프로토콜의 필드를 사용하여 드라이브 이름과 경로 정보를 정의할 수 있습니다. 예를 들어, 관리 공유의 경우 필드에 `c$/LogFiles/` 디렉토리가 포함되고 공용 공유 폴더 경로의 경우 필드에 `LogFiles/` 디렉토리가 포함될 수 있습니다. 단, `c:/LogFiles` 디렉토리는 포함될 수 없습니다.

중요사항: Microsoft Exchange 프로토콜은 Microsoft Exchange 2003 또는 Microsoft 인증 프로토콜 NTLMv2 Session을 지원하지 않습니다.

다음 표는 Microsoft Exchange 프로토콜의 프로토콜 특정 매개변수를 설명합니다.

표 *12. Microsoft Exchange* 프로토콜 매개변수

매개변수	설명
프로토콜 구성	**Microsoft Exchange**
도메인	선택사항입니다.
SMTP 로그 폴더 경로	이 폴더 경로가 선택 취소된 경우 SMTP 이벤트 콜렉션이 사용되지 않습니다.
OWA 로그 폴더 경로	이 폴더 경로가 선택 취소된 경우 OWA 이벤트 콜렉션이 사용되지 않습니다.

표 *12. Microsoft Exchange* 프로토콜 매개변수 *(계속)*

매개변수	설명
MSGTRK 로그 폴더 경로	허브 전송, 메일함 또는 에지 전송 서버 역할이 지정된 Microsoft Exchange 2007 또는 2010 서버에서 메시지 추적이 사용 가능합니다.
파일 패턴	이벤트 로그를 식별하는 정규식(regex)입니다. 기본값은 `.*\.(?:log|LOG)`입니다.
파일 읽기 강제 실행	이 선택란이 선택 취소된 경우, QRadar가 수정 시간 또는 파일 크기 변경을 발견할 때만 로그 파일을 읽습니다.
초당 이벤트 수 제한	Exchange 프로토콜이 전달할 수 있는 초당 최대 이벤트 수입니다.

Microsoft IIS 프로토콜 구성 옵션

Microsoft IIS 프로토콜을 사용하는 로그 소스를 구성할 수 있습니다. 이 프로토콜은 Microsoft IIS 웹 서버에 있는 W3C 형식 로그 파일에 대한 단일 콜렉션 지점을 지원합니다.

로그 파일을 읽으려면, 관리 공유(C$)가 포함된 폴더 경로는 해당 관리 공유(C$)에 대해 NetBIOS 권한이 있어야 합니다. 로컬 또는 도메인 관리자는 관리 공유의 로그 파일에 액세스하기에 충분한 권한이 있습니다.

관리자는 파일 경로를 지원하는 Microsoft IIS 프로토콜의 필드를 사용하여 드라이브 이름과 경로 정보를 정의할 수 있습니다. 예를 들어, 관리 공유의 경우 필드에 `c$/LogFiles/` 디렉토리가 포함되고 공용 공유 폴더 경로의 경우 필드에 `LogFiles/` 디렉토리가 포함될 수 있습니다. 단, `c:/LogFiles` 디렉토리는 포함될 수 없습니다.

제한사항: Microsoft 인증 프로토콜 NTLMv2는 Microsoft IIS 프로토콜에서 지원하지 않습니다.

다음 표는 Microsoft IIS 프로토콜의 프로토콜 특정 매개변수를 설명합니다.

표 *13. Microsoft IIS* 프로토콜 매개변수

매개변수	설명
프로토콜 구성	**Microsoft IIS**
파일 패턴	이벤트 로그를 식별하는 정규식(regex)입니다.
초당 이벤트 수 제한	IIS 프로토콜이 전달할 수 있는 초당 최대 이벤트 수입니다.

Microsoft Security Event Log 프로토콜 구성 옵션

Microsoft Security Event Log 프로토콜을 사용하는 로그 소스를 구성할 수 있습니다. Microsoft WMI(Windows Management Instrumentation)를 사용하여 사용자 정의 이벤트 로그 또는 에이전트 없는 Windows 이벤트 로그를 수집할 수 있습니다.

WMI API를 사용하려면, 방화벽 구성이 포트 135와 DCOM에 필요한 모든 동적 포트에서 수신되는 외부 통신을 승인해야 합니다. 다음 목록은 Microsoft Security Event Log 프로토콜을 사용할 때의 로그 소스 제한사항을 설명합니다.

- 초당 이벤트 수(eps)가 50개를 초과하는 시스템은 이 프로토콜의 기능을 능가할 수 있습니다. 50eps를 초과하는 시스템에는 WinCollect를 사용하십시오.
- QRadar 일체형 설치는 Microsoft Security Event Log 프로토콜로 최대 250개의 로그 소스를 지원할 수 있습니다.
- 전용 이벤트 콜렉터는 Microsoft Security Event Log 프로토콜을 사용하여 최대 500개의 로그 소스를 지원할 수 있습니다.

네트워크 링크를 통해 액세스되는 원격 서버, 예를 들어, 위성 또는 느린 WAN 네트워크와 같이 라운드트립 지연 시간이 긴 시스템에는 Microsoft Security Event Log 프로토콜이 권장되지 않습니다. 서버 ping 사이의 요청 및 응답 시간을 조사하여 라운드트립 지연을 확인할 수 있습니다. 느린 연결로 인한 네트워크 지연은 원격 서버에서 사용 가능한 EPS 처리량을 감소시킵니다. 또한, 사용 중인 서버 또는 도메인 컨트롤러로부터의 이벤트 콜렉션도 라운드트립 지연 시간이 짧아야만 수신 이벤트를 처리할 수 있습니다. 네트워크 라운드트립 지연 시간을 줄일 수 없는 경우, WinCollect를 사용하여 Windows 이벤트를 처리할 수 있습니다.

Microsoft Security Event Log는 Microsoft WMI(Windows Management Instrumentation) API로 다음 소프트웨어 버전을 지원합니다.

- Microsoft Windows 2000
- Microsoft Windows Server 2003
- Microsoft Windows Server 2008
- Microsoft Windows Server 2008R3
- Microsoft Windows XP
- Microsoft Windows Vista
- Microsoft Windows 7

다음 표는 Microsoft Security Event Log 프로토콜의 프로토콜 특정 매개변수를 설명합니다.

표 *14. Microsoft Security Event Log* 프로토콜 매개변수

매개변수	설명
프로토콜 구성	**Windows Security Event Log**

MQ 프로토콜 구성 옵션

메시지 큐(MQ) 서비스로부터 메시지를 수신하려면 MQ 프로토콜을 사용하도록 로그 소스를 구성하십시오. 프로토콜 이름은 IBM Security QRadar에 **MQ JMS**로 표시됩니다.

IBM MQ가 지원됩니다.

MQ 프로토콜은 로그 소스당 최대 50개까지의 복수 메시지 큐를 모니터할 수 있습니다.

다음 표는 MQ 프로토콜의 프로토콜 특정 매개변수에 대해 설명합니다.

표 *15. MQ* 프로토콜 매개변수

매개변수	설명
프로토콜 이름	**MQ JMS**
IP 또는 호스트 이름	기본 큐 관리자의 IP 주소 또는 호스트 이름입니다.
포트	기본 큐 관리자와 통신하기 위해 사용되는 기본 포트는 1414입니다.
스탠바이 IP 또는 호스트 이름	스탠바이 큐 관리자의 IP 주소 또는 호스트 이름입니다.
스탠바이 포트	스탠바이 큐 관리자와 통신하기 위해 사용되는 포트입니다.
큐 관리자	큐 관리자의 이름입니다.
채널	큐 관리자가 메시지를 전송하기 위해 사용하는 채널입니다. 기본 채널은 SYSTEM.DEF.SVRCONN입니다.
큐	모니터할 큐 또는 큐 목록입니다. 큐 목록은 쉼표로 구분된 목록으로 지정합니다.
사용자 이름	MQ 서비스에 인증하기 위해 사용되는 사용자 이름입니다.
비밀번호	**Optional:** MQ 서비스에 인증하기 위해 사용되는 비밀번호입니다.
EPS 제한	초당 최대 이벤트 수(EPS)의 상한입니다.
수신 메시지 인코딩	수신 메시지에서 사용하는 문자 인코딩입니다.

Okta REST API 프로토콜 구성 옵션

Okta로부터 이벤트를 수신하려면 Okta REST API 프로토콜을 사용하도록 로그 소스를 구성하십시오.

Okta REST API 프로토콜은 Okta 이벤트 및 사용자 API 엔드포인트를 조회하여 조직 내에서 사용자가 완료한 조치에 대한 정보를 검색합니다.

다음 표는 Okta REST API 프로토콜의 프로토콜 특정 매개변수에 대해 설명합니다.

표 *16. Okta REST API* 프로토콜 매개변수

매개변수	설명
IP 또는 호스트 이름	oktaprise.okta.com

표 *16. Okta REST API* 프로토콜 매개변수 *(계속)*

매개변수	설명
인증 토큰	Okta에서 생성되었으며 모든 API 트랜잭션에 대해 사용해야 하는 단일 인증 토큰입니다.
프록시 사용	프록시를 구성하면 로그 소스의 모든 트래픽이 Okta에 액세스하기 위해 QRadar의 프록시를 통해 이동합니다. **프록시 IP 또는 호스트 이름**, **프록시 포트**, **프록시 사용자 이름** 및 **프록시 비밀번호** 필드를 구성하십시오. 프록시에 인증이 필요하지 않은 경우 **프록시 사용자 이름** 및 **프록시 비밀번호** 필드를 비워둘 수 있습니다.
서버 인증서 자동 획득	목록에서 **예**를 선택하는 경우 QRadar는 인증서를 다운로드하고 대상 서버의 신뢰 처리를 시작합니다.
반복	로그 소스에서 데이터를 수집하는 시간을 지정할 수 있습니다. 형식은 M/H/D(월/시간/일)입니다. 기본값은 1 M입니다.
EPS 제한	초당 이벤트 수의 최대 한계입니다.

OPSEC/LEA 프로토콜 구성 옵션

포트 18184에서 이벤트를 수신하려면 OPSEC/LEA 프로토콜을 사용하도록 로그 소스를 구성하십시오.

다음 표는 OPSEC/LEA 프로토콜의 프로토콜 특정 매개변수를 설명합니다.

표 *17. OPSEC/LEA* 프로토콜 매개변수

매개변수	설명
프로토콜 구성	**OPSEC/LEA**
서버 포트	QRadar가 OPSEC/LEA 프로토콜을 사용하여 18184 포트에서 통신할 수 있는지 검증해야 합니다.
통계 보고 간격	`qradar.log` 파일에 syslog 이벤트 수가 기록되는 간격(초)입니다.
OPSEC 애플리케이션 오브젝트 SIC 속성(SIC 이름)	SIC(Secure Internal Communications) 이름은 애플리케이션의 구별 이름(DN)입니다(예: `CN=LEA, o=fwconsole..7psasx`).
로그 소스 SIC 속성(엔티티 SIC 이름)	서버의 SIC 이름입니다(예: `cn=cp_mgmt,o=fwconsole..7psasx`).
OPSEC 애플리케이션	인증서 요청을 작성하는 애플리케이션의 이름입니다.

중요사항: 업그레이드 후 **SSL 인증서를 가져올 수 없음**이라는 메시지를 수신하는 경우 다음 단계를 수행하십시오.

1. **인증서 지정** 선택란을 선택 취소하십시오.
2. **인증서 비밀번호 가져오기**에 비밀번호를 다시 입력하십시오.

Oracle Database Listener 프로토콜 구성 옵션

Oracle 데이터베이스 서버에서 생성되는 로그 파일을 원격으로 수집하려면 Oracle Database Listener 프로토콜 소스를 사용하는 로그 소스를 구성하십시오.

처리할 로그 파일을 모니터하도록 Oracle Database Listener 프로토콜을 구성하기 전, Oracle 데이터베이스 로그 파일의 디렉토리 경로를 얻어야 합니다.

다음 표는 Oracle Database Listener 프로토콜의 프로토콜 특정 매개변수를 설명합니다.

표 *18. Oracle Database Listener* 프로토콜 매개변수

매개변수	설명
프로토콜 구성	**Oracle Database Listener**
파일 패턴	이벤트 로그를 식별하는 정규식(regex)입니다.

PCAP Syslog Combination 프로토콜 구성 옵션

패킷 캡처(PCAP) 데이터를 전달하는 Juniper Networks SRX Series 어플라이언스에서 이벤트를 수집하려면 PCAP Syslog Combination 프로토콜을 사용하는 로그 소스를 구성하십시오.

PCAP Syslog Combination 프로토콜을 사용하는 로그 소스를 구성하기 전, Juniper Networks SRX 어플라이언스에 구성된 발신 PCAP 포트를 판별하십시오. PCAP 데이터는 514 포트로 전달할 수 없습니다.

다음 표는 PCAP Syslog Combination 프로토콜의 프로토콜 특정 매개변수를 설명합니다.

표 *19. PCAP Syslog Combination* 프로토콜 매개변수

매개변수	설명
프로토콜 구성	**PCAP Syslog Combination**
수신 PCAP 포트	Juniper Networks SRX Series 어플라이언스에서 발신 PCAP 포트를 편집하는 경우, 로그 소스를 편집하여 수신 PCAP 포트를 업데이트해야 합니다. **수신 PCAP 포트** 필드를 편집한 후에는 변경사항을 배치해야 합니다.

SDEE 프로토콜 구성 옵션

SDEE(Security Device Event Exchange) 프로토콜을 사용하는 로그 소스를 구성할 수 있습니다. QRadar는 이 프로토콜을 사용하여 SDEE 서버를 사용하는 어플라이언스에서 이벤트를 수집합니다.

다음 표는 SDEE 프로토콜의 프로토콜 특정 매개변수를 설명합니다.

표 *20. SDEE* 프로토콜 매개변수

매개변수	설명
프로토콜 구성	**SDEE**

표 *20. SDEE* 프로토콜 매개변수 *(계속)*

매개변수	설명
URL	로그 소스에 액세스하는 데 필요한 HTTP 또는 HTTPS URL입니다(예: https://www.mysdeeserver.com/cgi-bin/sdee-server). SDEE/CIDEE(Cisco IDS v5.x 이상)의 경우, URL은 /cgi-bin/sdee-server로 끝나야 합니다. RDEP(Cisco IDS v4.x)가 있는 관리자의 경우, URL은 /cgi-bin/event-server로 끝나야 합니다.
등록 강제 실행	이 선택란을 선택하는 경우, 이 프로토콜은 서버가 최소 활성 연결을 삭제하고 로그 소스에 대한 새 SDEE 등록 연결을 허용하도록 합니다.
이벤트에 대한 최대 차단 대기	수집 요청이 작성될 때 새 이벤트가 없는 경우, 이 프로토콜은 이벤트 차단이 사용되도록 설정합니다. 차단이 사용되면 새 이벤트가 없는 원격 디바이스에 대해 다른 이벤트 요청이 작성되지 않습니다. 이 제한시간은 시스템 자원을 보호하기 위한 것입니다.

SMB Tail 프로토콜 구성 옵션

SMB Tail 프로토콜을 사용하는 로그 소스를 구성할 수 있습니다. 이 프로토콜을 사용하면 원격 Samba 공유에서 이벤트를 감시하고 이벤트 로그에 새 라인이 추가될 때 Samba 공유에서 이벤트를 수신할 수 있습니다.

다음 표는 SMB Tail 프로토콜의 프로토콜 특정 매개변수를 설명합니다.

표 *21. SMB Tail* 프로토콜 매개변수

매개변수	설명
프로토콜 구성	**SMB Tail**
로그 폴더 경로	로그 파일에 액세스하기 위한 디렉토리 경로입니다. 예를 들어, 관리자는 c$/LogFiles/ 디렉토리(관리 공유의 경우) 또는 LogFiles/ 디렉토리(공용 공유 폴더 경로의 경우)를 사용할 수 있습니다. 그러나 c:/LogFiles 디렉토리는 지원되는 로그 폴더 경로가 아닙니다. 로그 폴더 경로에 관리 공유(C$)가 포함되는 경우, 관리 공유(C$)에 대해 NetBIOS 액세스 권한이 있는 사용자는 로그 파일을 읽는 데 필요한 권한을 가집니다. 로컬 시스템 또는 도메인 관리자 권한도 관리 공유에 있는 로그 파일에 액세스하기에 충분합니다.
파일 패턴	이벤트 로그를 식별하는 정규식(regex)입니다.
파일 읽기 강제 실행	이 선택란이 선택 취소된 경우, QRadar가 수정 시간 또는 파일 크기 변경을 발견할 때만 로그 파일이 읽혀집니다.
초당 이벤트 수 제한	SMB Tail 프로토콜이 전달할 수 있는 초당 최대 이벤트 수입니다.

SNMPv2 프로토콜 구성 옵션

SNMPv2 프로토콜을 사용하여 SNMPv2 이벤트를 수신하는 로그 소스를 구성할 수 있습니다.

다음 표는 SNMPv2 프로토콜의 프로토콜 특정 매개변수를 설명합니다.

표 *22. SNMPv2* 프로토콜 매개변수

매개변수	설명
프로토콜 구성	**SNMPv3**
커뮤니티	SNMP 이벤트가 포함된 시스템에 액세스하는 데 필요한 SNMP 커뮤니티 이름입니다.
이벤트 페이로드에 OID 포함	이벤트 페이로드 형식 대신 이름-값 쌍을 사용하여 SNMP 이벤트 페이로드를 구성하도록 지정합니다. **로그 소스 유형** 목록에서 특정 로그 소스를 선택하는 경우, SNMPv2 또는 SNMPv3 이벤트를 처리하기 위해 이벤트 페이로드의 OID가 필요합니다.

SNMPv3 프로토콜 구성 옵션

SNMPv3 프로토콜을 사용하여 SNMPv3 이벤트를 수신하는 로그 소스를 구성할 수 있습니다.

다음 표는 SNMPv3 프로토콜의 프로토콜 특정 매개변수를 설명합니다.

표 *23. SNMPv3* 프로토콜 매개변수

매개변수	설명
프로토콜 구성	**SNMPv3**
인증 프로토콜	SNMP 트랩을 인증하는 데 사용할 알고리즘입니다.
이벤트 페이로드에 OID 포함	표준 이벤트 페이로드 형식 대신 이름-값 쌍을 사용하여 SNMP 이벤트 페이로드를 구성하도록 지정합니다. **로그 소스 유형** 목록에서 특정 로그 소스를 선택하는 경우, SNMPv2 또는 SNMPv3 이벤트를 처리하기 위해 이벤트 페이로드의 OID가 필요합니다.

Seculert Protection REST API 프로토콜 구성 옵션

Seculert으로부터 이벤트를 수신하려면 Seculert Protection REST API 프로토콜을 사용하도록 로그 소스를 구성하십시오.

Seculert Protection은 활성 통신 또는 탈취 정보인 악성 코드의 확정된 인시던트에 대해 경보를 전송합니다.

Seculert의 로그 소스를 구성하려면 먼저 Seculert 웹 포털에서 API 키를 얻어야 합니다.

1. Seculert 웹 포털에 로그인하십시오.
2. 대시보드에서 **API** 탭을 클릭하십시오.

3. **귀하의 API 키** 값을 복사하십시오.

다음 표는 Seculert Protection REST API 프로토콜의 프로토콜 특정 매개변수에 대해 설명합니다.

표 *24. Seculert Protection REST API* 프로토콜 매개변수

매개변수	설명
API 키	Seculert Protection REST API에 인증하기 위해 사용되는 API 키입니다. API 키 값은 Seculert 웹 포털에서 얻을 수 있습니다.
프록시 사용	프록시를 구성하면 로그 소스의 모든 트래픽이 Seculert Protection REST API에 액세스하기 위해 QRadar의 프록시를 통해 이동합니다. **프록시 IP 또는 호스트 이름**, **프록시 포트**, **프록시 사용자 이름** 및 **프록시 비밀번호** 필드를 구성하십시오. 프록시에 인증이 필요하지 않은 경우 **프록시 사용자 이름** 및 **프록시 비밀번호** 필드를 비워둘 수 있습니다.
서버 인증서 자동 획득	목록에서 **예**를 선택하는 경우 QRadar는 인증서를 다운로드하고 대상 서버의 신뢰 처리를 시작합니다.
반복	로그에서 데이터를 수집하는 시간을 지정합니다. 형식은 M/H/D(월/시간/일)입니다. 기본값은 1 M입니다.
EPS 제한	API로부터 수신되는 이벤트에 대한 초당 최대 이벤트 수(EPS)의 상한입니다.

Sophos Enterprise Console JDBC 프로토콜 구성 옵션

Sophos Enterprise Console에서 이벤트를 수신하려면 Sophos Enterprise Console JDBC 프로토콜을 사용하는 로그 소스를 구성하십시오.

Sophos Enterprise Console JDBC 프로토콜은 vEventsCommonData 테이블에 애플리케이션 제어 로그, 디바이스 제어 로그, 데이터 제어 로그, 변조 보호 로그 및 방화벽 로그로부터의 페이로드 정보를 결합합니다. Sophos Enterprise Console에 Sophos Reporting Interface가 없는 경우, 표준 JDBC 프로토콜을 사용하여 안티바이러스 이벤트를 수집할 수 있습니다.

다음 표는 Sophos Enterprise Console JDBC 프로토콜의 매개변수를 설명합니다.

표 *25. Sophos Enterprise Console JDBC* 프로토콜 매개변수

매개변수	설명
프로토콜 구성	**Sophos Enterprise Console JDBC**
데이터베이스 유형	**MSDE**
데이터베이스 이름	데이터베이스 이름은 **로그 소스 ID** 필드에 지정된 데이터베이스 이름과 일치해야 합니다.

표 *25. Sophos Enterprise Console JDBC* 프로토콜 매개변수 *(계속)*

매개변수	설명
포트	Sophos Enterprise Console에서 MSDE의 기본 포트는 1168입니다. QRadar와 통신하려면 JDBC 구성 포트는 Sophos 데이터베이스의 리스너 포트와 일치해야 합니다. Sophos 데이터베이스는 수신 TCP 연결을 허용해야 합니다. MSDE 데이터베이스 유형과 함께 **데이터베이스 인스턴스**를 사용하는 경우에는 **포트** 매개변수를 비워 둬야 합니다.
인증 도메인	네트워크가 도메인을 사용하지 않는 경우에는 이 필드를 비워 두십시오.
데이터베이스 인스턴스	필요한 경우에 사용되는 데이터베이스 인스턴스입니다. MSDE 데이터베이스는 하나의 서버에서 여러 SQL 서버 인스턴스를 포함할 수 있습니다. 해당 데이터베이스에 표준 포트가 아닌 포트를 사용하거나 관리자가 SQL 데이터베이스 분석을 위해 포트 1434에 대한 액세스를 차단하는 경우, **데이터베이스 인스턴스** 매개변수를 비워 둬야 합니다.
테이블 이름	`vEventsCommonData`
선택 목록	*
비교 필드	`InsertedAt`
준비된 명령문 사용	준비된 명령문을 사용하면 프로토콜 소스가 SQL문을 설정한 후 서로 다른 매개변수를 사용하여 해당 SQL문을 여러 번 실행할 수 있습니다. 보안 및 성능을 위해, 대부분의 구성에서 준비된 명령문을 사용할 수 있습니다. 미리 컴파일된 명령문을 사용하지 않는 다른 조회 방법을 사용하려면 이 선택란을 선택 취소하십시오.
시작 날짜 및 시간	선택사항입니다. 프로토콜이 데이터베이스 폴링을 시작할 수 있는 시작 날짜 및 시간입니다. 시작 날짜를 정의하지 않은 경우, 프로토콜은 로그 소스 구성이 저장되고 배치된 후 이벤트를 폴링하려고 시도합니다.
폴링 간격	데이터베이스 조회 사이의 시간 간격입니다. 숫자 값에 H(시간의 경우) 또는 M(분의 경우)을 추가하여 보다 긴 폴링 간격을 정의할 수 있습니다. 최대 폴링 간격은 1주일(모든 시간 형식이 가능함)입니다. H 또는 M 지정자가 없는 숫자 값은 초 단위로 폴링합니다.
EPS 제한	이 프로토콜이 초과하지 않도록 할 초당 이벤트 수(EPS)입니다.
이름지정된 파이프 통신 사용	데이터베이스 유형으로 MSDE를 선택하는 경우, 관리자는 TCP/IP 포트 연결의 대체 방법을 사용하기 위해 이 선택란을 선택할 수 있습니다. MSDE 데이터베이스에 대한 이름지정된 파이프 연결의 경우, 사용자 이름 및 비밀번호 필드에 데이터베이스 사용자 이름 및 비밀번호 대신 Windows 인증 사용자 이름 및 비밀번호를 사용해야 합니다. 로그 소스 구성은 MSDE 데이터베이스의 기본 이름지정된 파이프를 사용해야 합니다.
데이터베이스 클러스터 이름	클러스터 환경에서 SQL 서버를 사용하는 경우, 이름지정된 파이프 통신이 제대로 작동하도록 클러스터 이름을 정의하십시오.

표 *25. Sophos Enterprise Console JDBC* 프로토콜 매개변수 *(계속)*

매개변수	설명
NTLMv2 사용	NTLMv2 인증이 필요한 SQL 서버의 경우 MSDE 연결이 NTLMv2 프로토콜을 사용하도록 합니다. 이 선택란의 기본값이 선택됩니다. **NTLMv2 사용** 선택란은 NTLMv2 인증이 필요 없는 MSDE 연결에 대해서는 통신을 인터럽트하지 않습니다.

Sourcefire Defense Center Estreamer 프로토콜 구성 옵션

Sourcefire Defense Center Estreamer(Event Streamer) 서비스에서 이벤트를 수신하려면 Sourcefire Defense Center Estreamer 프로토콜을 사용하는 로그 소스를 구성하십시오.

Sourcefire Defense Center DSM이 구성된 후, 이벤트 파일은 처리를 위해 QRadar로 스트림됩니다.

다음 표는 Sourcefire Defense Center Estreamer 프로토콜의 프로토콜 특정 매개변수를 설명합니다.

표 *26. Sourcefire Defense Center Estreamer* 프로토콜 매개변수

매개변수	설명
프로토콜 구성	**Sourcefire Defense Center Estreamer**
서버 포트	QRadar가 Sourcefire Defense Center Estreamer에 사용하는 기본 포트는 8302입니다.
키 저장소 파일 이름	키 저장소 개인 키 및 연관된 인증서의 디렉토리 경로 및 파일 이름입니다. 기본적으로, 가져오기 스크립트는 `/opt/qradar/conf/estreamer.keystore` 디렉토리에 키 저장소 파일을 작성합니다.
신뢰 저장소 파일 이름	신뢰 저장소 파일에는 클라이언트가 신뢰하는 인증서가 포함됩니다. 기본적으로, 가져오기 스크립트는 `/opt/qradar/conf/estreamer.truststore` 디렉토리에 신뢰 저장소 파일을 작성합니다.
추가 데이터 요청	Sourcefire Defense Center Estreamer의 추가 데이터를 요청하려면 이 옵션을 선택하십시오. 예를 들어, 추가 데이터로는 이벤트의 원본 IP 주소가 있습니다.
확장 요청 사용	다른 방법을 사용하여 eStreamer 소스의 이벤트를 검색하려면 이 옵션을 선택하십시오. 확장 요청은 Sourcefire DefenseCenter Estreamer 버전 5.0 이상에서 지원됩니다.

Syslog Redirect 프로토콜 개요

Syslog Redirect 프로토콜은 Syslog 프로토콜의 대안으로 사용됩니다. QRadar에서 이벤트를 보낸 특정 디바이스 이름을 식별하도록 하려면 이 프로토콜을 사용하십시오. QRadar는 UDP 포트 517에서 Syslog 이벤트를 수동적으로 청취할 수 있습니다.

다음 표는 Syslog Redirect 프로토콜의 프로토콜 특정 매개변수를 설명합니다.

표 *27. Syslog Redirect* 프로토콜 매개변수

매개변수	설명
프로토콜 구성	**Syslog Redirect**
로그 소스 ID RegEx	devname=([\w-]+)
청취 포트	517
프로토콜	**UDP**

TCP 다중 라인 syslog 프로토콜 구성 옵션

TCP 다중 라인 syslog 프로토콜을 사용하는 로그 소스를 구성할 수 있습니다. 단일 라인 이벤트를 작성하기 위해 이 프로토콜은 정규식을 사용하여 다중 라인 이벤트의 시작 및 종료 패턴을 식별합니다.

다음은 다중 라인 이벤트 예제입니다.

```
06/13/2012 08:15:15 PM
LogName=Security
SourceName=Microsoft Windows security auditing.
EventCode=5156
EventType=0
TaskCategory=Filtering Platform Connection
Keywords=Audit Success
Message=The Windows Filtering Platform permitted a connection.
Process ID: 4
Application Name: System
Direction: Inbound
Source Address: 1.1.1.1
Source Port: 80
Destination Address: 1.1.1.12
Destination Port:444
```

다음 표는 TCP 다중 라인 syslog 프로토콜의 프로토콜 특정 매개변수를 설명합니다.

표 *28. TCP* 다중 라인 *syslog* 프로토콜 매개변수

매개변수	설명
프로토콜 구성	**TCP 다중 라인 Syslog**
청취 포트	기본 청취 포트는 12468입니다.
이벤트 형식기	Windows용으로 형식화된 다중 라인 이벤트에 **Windows 다중 라인** 옵션을 사용하십시오.

표 *28. TCP* 다중 라인 *syslog* 프로토콜 매개변수 *(계속)*

매개변수	설명
이벤트 시작 패턴	TCP 다중 라인 이벤트 페이로드의 시작을 식별하는 데 필요한 정규식(regex)입니다. Syslog 헤더는 일반적으로 날짜 또는 시간소인으로 시작합니다. 이 프로토콜은 시간소인과 같이 이벤트 시작 패턴만을 기반으로 하는 단일 라인 이벤트를 작성할 수 있습니다. 시작 패턴만 사용 가능한 경우, 프로토콜은 각 시작 값 사이의 모든 정보를 캡처하여 유효한 이벤트를 작성합니다.
이벤트 종료 패턴	TCP 다중 라인 이벤트 페이로드의 마지막 필드를 식별하는 데 필요한 정규식(regex)입니다. syslog 이벤트가 동일한 값으로 끝나는 경우, 정규식을 사용하여 이벤트의 끝을 판별할 수 있습니다. 이 프로토콜은 이벤트 종료 패턴만을 기반으로 하는 이벤트를 캡처할 수 있습니다. 종료 패턴만 사용 가능한 경우 프로토콜은 각 종료 값 사이의 모든 정보를 캡처하여 유효한 이벤트를 작성합니다.

TLS syslog 프로토콜 구성 옵션

TLS Syslog 이벤트 전달을 지원하는 최대 50개의 네트워크 디바이스에서 암호화된 syslog 이벤트를 수신하려면 TLS Syslog 프로토콜을 사용하는 로그 소스를 구성하십시오.

로그 소스는 수신 TLS Syslog 이벤트에 대한 청취 포트를 작성하고 네트워크 디바이스에 대한 인증서 파일을 생성합니다. 최대 50개의 네트워크 어플라이언스가 로그 소스용으로 작성된 청취 포트에 이벤트를 전달할 수 있습니다. 50개 이상의 네트워크 어플라이언스가 필요한 경우 추가 청취 포트를 작성하십시오.

다음 표는 TLS Syslog 프로토콜의 프로토콜 특정 매개변수를 설명합니다.

표 *29. TLS syslog* 프로토콜 매개변수

매개변수	설명
프로토콜 구성	**TLS Syslog**
TLS 청취 포트	기본 TLS 청취 포트는 6514입니다.
인증 모드	TLS 연결이 인증되는 모드입니다. **TLS 및 클라이언트 인증** 옵션을 선택하는 경우 인증서 매개변수를 구성해야 합니다.
클라이언트 인증서 경로	디스크에서 클라이언트 인증서의 절대 경로입니다. 인증서는 이 로그 소스의 콘솔 또는 Event Collector에 저장되어 있어야 합니다.
인증서 유형	인증에 사용할 인증서의 유형입니다. **인증서 제공** 옵션을 선택하는 경우, 서버 인증서 및 개인 키의 파일 경로를 구성해야 합니다.
제공된 서버 인증서 경로	서버 인증서의 절대 경로입니다.
제공된 개인 키 경로	개인 키의 절대 경로입니다. **참고:** 해당 개인 키는 DER 인코딩 PKCS8 키여야 합니다. 다른 키 형식인 경우 구성이 실패합니다.

표 29. *TLS syslog* 프로토콜 매개변수 (계속)

매개변수	설명
최대 연결 수	**최대 연결 수** 매개변수는 TLS Syslog 프로토콜에서 각 Event Collector에 대해 허용할 수 있는 동시 연결 수를 제어합니다. 모든 TLS syslog 로그 소스 구성에는 각 Event Collector에 대한 1000개의 연결 제한이 있습니다. 각 디바이스 연결의 기본값은 50입니다. **참고:** 다른 로그 소스와 리스너를 공유하는 자동으로 감지된 로그 소스는 제한을 계수할 때 한 번만 계수됩니다. 예를 들면 동일한 이벤트 콜렉터의 동일한 포트입니다.

TLS syslog 유스 케이스

다음 유스 케이스는 작성 가능한 구성을 나타냅니다.

클라이언트 인증

프로토콜이 클라이언트 인증을 수행하는 데 필요한 클라이언트 인증서를 제공할 수 있습니다. 이 옵션을 선택하고 인증서를 제공하면 클라이언트 인증서에 대해 수신 연결의 유효성이 검증됩니다.

사용자 제공 서버 인증서

사용자 소유의 서버 인증서와 해당 개인 키를 구성할 수 있습니다. 구성된 TLS Syslog 제공자는 이 인증서와 키를 사용합니다. 수신 연결에는 자동으로 생성된 TLS Syslog 인증서가 아니라 사용자 제공 인증서가 제공됩니다.

기본 인증

기본 인증 방법을 사용하려면 **인증 모드** 및 **인증 유형** 매개변수에 기본값을 사용하십시오. 로그 소스가 저장되면 로그 소스 디바이스에 대한 `syslog-tls` 인증서가 작성됩니다. 이 인증서는 암호화된 syslog 데이터를 전달하는 네트워크의 임의 디바이스로 복사해야 합니다.

UDP 다중 라인 syslog 프로토콜 구성 옵션

다중 라인 이벤트에서 단일 라인 syslog 이벤트를 작성하려면 UDP 다중 라인 프로토콜을 사용하는 로그 소스를 구성하십시오. UDP 다중 라인 syslog 프로토콜은 정규식을 사용하여 다중 라인 syslog 메시지를 식별하고 단일 이벤트 페이로드로 다시 어셈블합니다.

다중 라인 이벤트를 식별하고 다시 어셈블할 수 있는 정규식을 반복하는 값이 원래 이벤트에 있어야 합니다. 예를 들어, 다음 이벤트에는 반복되는 값이 있습니다.

```
15:08:56 1.1.1.1 slapd[517]: conn=2467222 op=2 SEARCH RESULT tag=101
15:08:56 1.1.1.1 slapd[517]: conn=2467222 op=2 SRCH base="dc=iso-n,dc=com"
15:08:56 1.1.1.1 slapd[517]: conn=2467222 op=2 SRCH attr=gidNumber
15:08:56 1.1.1.1 slapd[517]: conn=2467222 op=1 SRCH base="dc=iso-n,dc=com"
```

다음 표는 UDP 다중 라인 syslog 프로토콜의 프로토콜 특정 매개변수를 설명합니다.

표 *30. UDP* 다중 라인 *syslog* 프로토콜 매개변수

매개변수	설명
프로토콜 구성	**UDP 다중 라인 Syslog**
메시지 ID 패턴	이벤트 페이로드 메시지를 필터링하는 데 필요한 정규식(regex)입니다. UDP 다중 라인 이벤트 메시지는 이벤트 메시지의 각 라인에 반복되는 공통 식별 값이 있어야 합니다.

로그 소스가 저장되면 로그 소스에 대한 syslog-tls 인증서가 작성됩니다. 이 인증서는 암호화된 syslog를 전달하도록 구성된 네트워크의 임의 디바이스로 복사해야 합니다. syslog-tls 인증서 파일과 TLS 청취 포트 번호가 있는 기타 네트워크 디바이스는 TLS syslog 로그 소스로 자동으로 감지될 수 있습니다.

VMware vCloud Director 프로토콜 구성 옵션

VMware vCloud Director 가상 환경에서 이벤트를 수집하기 위해 VMware vCloud Director 프로토콜을 사용하는 로그 소스를 작성할 수 있습니다.

다음 표는 VMware vCloud Director 프로토콜의 프로토콜 특정 매개변수를 설명합니다.

표 *31. VMware vCloud Director* 프로토콜 매개변수

매개변수	설명
프로토콜 구성	**VMware vCloud Director**
vCloud URL	VMware vCloud 어플라이언스에서 REST API에 액세스하기 위해 구성된 URL입니다. 이 URL은 vCloud Server에서 VCD 공용 REST API 기반 URL로 구성된 주소(예: `https://1.1.1.1.`)와 일치해야 합니다.
사용자 이름	vCloud Server에 원격으로 액세스하는 데 필요한 사용자 이름입니다(예: `console/user@organization`). vCloud Director 프로토콜과 함께 사용할 읽기 전용 계정을 구성하려면 사용자에게 콘솔 액세스 전용 권한이 있어야 합니다.

벌크 로그 소스 추가

한 번에 최대 500개의 Microsoft Windows 또는 Universal DSM 로그 소스를 추가할 수 있습니다. 한 번에 여러 로그 소스를 추가할 때는 QRadar에서 벌크 로그 소스를 추가합니다. 벌크 로그 소스는 공통 구성을 공유해야 합니다.

프로시저

1. **관리** 탭을 클릭하십시오.
2. **로그 소스** 아이콘을 클릭하십시오.

3. **벌크 조치** 목록에서 **벌크 추가**를 선택하십시오.
4. 벌크 로그 소스의 매개변수를 구성하십시오.
   - 파일 업로드 - 행당 호스트 이름이나 IP가 하나인 텍스트 파일을 업로드합니다.
   - 수동 - 추가하려는 호스트의 호스트 이름이나 IP를 입력합니다.
5. **저장**을 클릭하십시오.
6. **계속**을 클릭하여 로그 소스를 추가하십시오.
7. **관리** 탭에서 **변경사항 배치**를 클릭하십시오.

로그 소스 구문 분석 순서 추가

대상 이벤트 콜렉터가 이벤트를 구문 분석할 때 우선순위를 지정할 수 있습니다.

이 태스크 정보

공통 IP 주소 또는 호스트 이름을 공유하는 로그 소스에 대한 구문 분석 순서를 정의하여 로그 소스의 중요도를 지정할 수 있습니다. 로그 소스의 구문 분석 순서를 정의하면 로그 소스 구성의 변경에 관계 없이 특정 순서에 따라 특정 로그 소스를 구문 분석할 수 있습니다. 구문 분석 순서를 사용하면 불필요한 구문 분석을 방지하여 로그 소스 구성에 대한 변경사항이 발생해도 시스템 성능이 영향을 받지 않습니다. 구문 분석 순서를 사용하면 더 중요한 로그 소스가 구문 분석된 후에 하위 레벨 이벤트가 구문 분석됩니다.

프로시저

1. **관리** 탭을 클릭하십시오.
2. **로그 소스 구문 분석 순서 지정** 아이콘을 클릭하십시오.
3. 로그 소스를 선택하십시오.
4. 옵션: **선택된 이벤트 콜렉터** 목록에서 로그 소스 구문 분석 순서를 정의하는 이벤트 콜렉터를 선택하십시오.
5. 옵션: **로그 소스 호스트** 목록에서 로그 소스를 선택하십시오.
6. 로그 소스 구문 분석 순서를 지정하십시오.
7. **저장**을 클릭하십시오.

제 2 장 사용자 정의 로그 소스

확장 문서는 특정 로그 소스의 요소가 구문 분석되는 방식을 확장하거나 수정할 수 있습니다. 확장 문서를 사용하여 구문 분석 문제를 정정하거나, 기존 DSM에서 이벤트의 기본 구문 분석을 겹쳐쓸 수 있습니다.

네트워크에 있는 어플라이언스 또는 보안 디바이스의 이벤트를 구문 분석하는 DSM이 없는 경우, 확장 문서가 이벤트 지원을 제공할 수도 있습니다.

확장 문서는 공통 텍스트, 코드 또는 마크업 편집기를 사용하여 작성하거나 편집할 수 있는 XML(Extensible Markup Language) 형식 문서입니다. 여러 개의 확장 문서를 작성할 수 있지만 한 로그 소스에 한 확장 문서만 적용할 수 있습니다.

XML 형식의 경우, 정규식에 필요한 특수 문자가 마크업 형식의 간섭을 받지 않도록 모든 정규식(regex) 패턴은 문자 데이터(CDATA) 섹션에 포함되어야 합니다. 예를 들어, 다음 코드는 프로토콜을 찾기 위한 정규식을 보여줍니다.

```
<pattern id="ProtocolPattern" case-insensitive="true" xmlns="">
<![CDATA[(TCP|UDP|ICMP|GRE)]]></pattern>
```

(TCP|UDP|ICMP|GRE)는 정규식 패턴입니다.

사용자 정의 로그 소스 구성은 다음 섹션으로 구성됩니다.

패턴 특정 필드 이름과 연관시키는 정규식 패턴입니다. 패턴은 사용자 정의 로그 소스 파일 내에서 여러 차례 참조됩니다.

일치 그룹

구문 분석되는 일치 그룹 내의 엔티티(예: EventName)로, 구문 분석을 위해 적절한 패턴 및 그룹과 쌍을 이룹니다. 모든 일치 그룹이 확장 문서에 표시됩니다.

QRadar 포럼의 사용자 정의 로그 소스 예제

지원되는 DSM이 없는 로그 소스에 대해 사용자 정의 로그 소스(LSX)를 작성할 수 있습니다. 사용자 고유의 사용자 정의 로그 소스(DSM 확장이라고도 함)를 작성하려면 이전에 작성한 기존 확장을 수정하십시오.

사용자 정의 로그 소스 예제(https://www.ibm.com/developerworks/community/forums/html/topic?id=d15cac8d-b0fa-4461-bb1e-dc1b291de440&ps=25)에는 DSM 확장, 사용자 정의 특성 및 기타 REGEX 관

련 항목 포럼(https://www.ibm.com/developerworks/community/forums/html/forum?id=11111111-0000-0000-0000-000000003046&ps=25)을 통해 액세스할 수 있습니다.

IBM Security QRadar 포럼은 사용자와 주제 전문가가 정보를 수집하고 공유하는 온라인 토론 사이트입니다.

관련 개념:

40 페이지의 『사용자 정의 로그 소스 문서 작성』
지원되는 DSM이 없는 로그 소스에 대해서 또는 정보가 누락되었거나 올바르지 않은 이벤트를 수리하거나 연관된 DSM이 결과를 산출하지 못하는 경우 이벤트를 구문 분석하기 위해 사용자 정의 로그 소스(LSX)를 작성합니다.

사용자 정의 로그 소스 문서의 패턴

정규식을 특정 필드 이름에 바로 연관시키지 않고, 확장 문서의 맨 위에 패턴(patterns)이 개별적으로 선언됩니다. 이러한 정규식 패턴은 사용자 정의 로그 소스 파일 내에서 여러 차례 참조될 수 있습니다.

시작 태그 <pattern>과 끝 태그 </pattern> 사이의 모든 문자는 패턴의 일부로 간주됩니다. 패턴이나 <CDATA> 표현식의 내부 또는 주변에서는 추가 공간이나 강제 리턴을 사용하지 마십시오. 추가 문자나 공간이 있으면 DSM 확장이 의도한 패턴과 일치하지 않게 됩니다.

표 *32.* 패턴 매개변수 설명

패턴	유형	설명
id(필수)	String	확장 문서 내에서 고유한 정규 문자열입니다.
case-insensitive(선택사항)	Boolean	true인 경우 대소문자가 무시됩니다. 예를 들어, abc가 ABC와 동일합니다. 지정하지 않을 경우 이 매개변수의 기본값은 false입니다.
trim-whitespace(선택사항)	Boolean	true인 경우 캐리지 리턴이 무시됩니다. CDATA 섹션이 서로 다른 여러 행으로 나뉜 경우 추가 공간과 캐리지 리턴이 패턴의 파트로 해석되지 않습니다. 지정하지 않을 경우 이 매개변수의 기본값은 false입니다.

일치 그룹

일치 그룹(match-group)은 하나 이상의 이벤트 유형을 구문 분석하거나 수정하는 데 사용되는 패턴 세트입니다.

*matcher*는 구문 분석되는 일치 그룹 내의 엔티티(예: EventName)로, 구문 분석을 위해 적절한 패턴 및 그룹과 쌍을 이룹니다. 모든 일치 그룹이 확장 문서에 표시됩니다.

표 *33.* 일치 그룹 매개변수 설명

매개변수	설명
order(필수)	일치 그룹이 실행되는 순서를 정의하는 0보다 큰 정수입니다. 확장 문서 내에서 고유해야 합니다.
description(선택사항)	일치 그룹에 대한 설명 문자열입니다. 이 정보는 로그로 표시될 수 있습니다. 지정하지 않을 경우 이 매개변수의 기본값은 공백입니다.
device-type-id-override(선택사항)	QID를 겹쳐쓸 다른 디바이스 ID를 정의합니다. 특정 일치 그룹이 지정된 디바이스에서 이벤트 유형을 검색할 수 있도록 허용합니다. 정수로 표현된 올바른 로그 소스 유형 ID여야 합니다. 로그 소스 유형 ID 목록이 54 페이지의 표 40에 표시되어 있습니다. 지정하지 않을 경우 이 매개변수의 기본값은 확장이 연결된 로그 소스의 로그 소스 유형입니다.

일치 그룹은 다음과 같은 엔티티를 갖습니다.

- 『Matcher(matcher)』
- 36 페이지의 『Single-event modifier(event-match-single)』
- 36 페이지의 『Multi-event modifier(event-match-multiple)』

Matcher(matcher)

matcher 엔티티는 구문 분석되는 필드(예: EventName)로, 구문 분석을 위해 적절한 패턴 및 그룹과 쌍을 이룹니다.

matcher에는 순서가 연관되어 있습니다. 동일한 필드 이름에 여러 개의 matcher가 지정된 경우 성공적인 구문 분석을 찾거나 실패가 나타날 때까지 matcher는 제시된 순서대로 실행됩니다.

표 *34. matcher* 매개변수 설명

매개변수	설명
field(필수)	패턴을 적용하려는 필드(예: EventName 또는 SourceIp)입니다. 올바른 matcher 필드 이름 목록 테이블에 나열되는 모든 필드 이름을 사용할 수 있습니다.
pattern-id(필수)	페이로드로부터 필드를 구문 분석할 때 사용하려는 패턴입니다. 이 값은 이전에 패턴 ID 매개변수(30 페이지의 표 32)에서 정의한 패턴의 ID 매개변수와 (대소문자까지) 일치해야 합니다.
order(필수)	동일한 필드에 지정된 matcher 사이에서 이 패턴을 시도하려는 순서입니다. 두 개의 matcher가 EventName 필드에 지정된 경우 가장 낮은 순위의 matcher가 먼저 시도됩니다.
capture-group(선택사항)	정규식에서 소괄호()로 묶어 참조됩니다. 이러한 캡처는 1에서 인덱스가 시작되며 패턴의 왼쪽에서 오른쪽으로 처리됩니다. capture-group 필드는 패턴에 포함된 캡처 그룹 수 이하의 양의 정수여야 합니다. 기본값은 0이며 전체 일치를 의미합니다. 예를 들어, 소스 IP 주소와 포트에 대해 단일 패턴을 정의할 수 있습니다. 이 경우 SourceIp matcher가 캡처 그룹 1을 사용할 수 있고 SourcePort matcher가 캡처 그룹 2를 사용할 수 있지만 패턴은 하나만 정의해야 합니다. enable-substitutions 매개변수와 결합되는 경우 이 필드는 이중의 용도를 갖습니다. 예제를 보려면 확장 문서 예제를 검토하십시오.

표 *34. matcher* 매개변수 설명 *(*계속*)*

매개변수	설명
enable-substitutions(선택사항)	Boolean true로 설정하는 경우 직선 그룹 캡처를 사용하여 한 필드를 충분히 표시하지 못할 수 있습니다. 여러 그룹을 추가 텍스트와 결합하여 하나의 값을 형성할 수 있습니다. 이 매개변수는 capture-group 매개변수의 의미를 변경합니다. capture-group 매개변수는 새 값을 작성하고 \x를 사용하여 그룹 대체가 지정됩니다. 여기서 x는 그룹 번호 1 - 9입니다. 그룹을 여러 차례 사용할 수 있으며 자유 형식 텍스트를 값에 삽입할 수도 있습니다. 예를 들어, 그룹 1, 밑줄, 그룹 2, @, 다시 그룹 1로 값을 형성하려는 경우 적절한 캡처-그룹 구문은 다음 코드와 같습니다. capture-group="\1_\2@\1" 다른 예제에서, MAC 주소는 콜론으로 구분되지만 QRadar에서는 보통 하이픈으로 MAC 주소가 구분됩니다. 개별적인 부분을 구문 분석하고 캡처하는 구문은 다음 예제와 같습니다. capture-group="\1:\2:\3:\4:\5:\6" 대체가 사용될 때 캡처-그룹에 그룹을 지정하지 않으면 직접 텍스트 교체가 발생합니다. 기본값은 false입니다.
ext-data(선택사항)	matcher 필드가 확장에서 제공할 수 있는 형식화 또는 추가 필드 정보를 정의하는 추가 데이터 매개변수입니다. 이 매개변수를 사용하는 유일한 필드가 DeviceTime입니다. 예를 들어, 고유의 시간소인을 사용하여 이벤트를 전송하는 디바이스가 있지만 사용자는 이벤트를 표준 디바이스 시간으로 다시 형식화하고자 합니다. DeviceTime 필드에 포함된 추가 데이터 매개변수를 사용하여 이벤트의 날짜와 시간소인을 다시 형식화하십시오. 자세한 정보는 올바른 matcher 필드 이름 목록을 참조하십시오.

다음 표에서 올바른 matcher 필드 이름을 설명합니다.

표 *35.* 올바른 *matcher* 필드 이름 목록

필드 이름	설명
EventName(필수)	이벤트를 식별하기 위해 QID에서 검색하는 이벤트 이름입니다. **참고:** 이 매개변수는 **로그 보기** 탭에 필드로 표시되지 않습니다.
EventCategory	event-match-single 엔티티 또는 event-match-multiple 엔티티에 의해 처리되지 않는 카테고리의 이벤트에 대한 이벤트 카테고리입니다. EventName, EventCategory와 결합되어 QID의 이벤트를 검색하는 데 사용됩니다. 디바이스가 이미 QRadar에 알려진 경우 QIDmap 검색에 사용되는 필드에 겹쳐쓰기 플래그를 설정해야 하며 다음과 같습니다. `<event-match-single event-name= "Successfully logged in" force-qidmap-lookup-on-fixup="true" device-event-category="CiscoNAC" severity="4" send-identity= "OverrideAndNeverSend" />` `force-qidmap-lookup-on-fixup="true"`는 플래그 겹쳐쓰기입니다. **참고:** 이 매개변수는 **로그 보기** 탭에 필드로 표시되지 않습니다.
SourceIp	메시지에 대한 소스 IP 주소입니다.
SourcePort	메시지에 대한 소스 포트입니다.
SourceIpPreNAT	NAT(Network Address Translation)가 발생하기 전 메시지에 대한 소스 IP 주소입니다.
SourceIpPostNAT	NAT 발생 후 메시지에 대한 소스 IP 주소입니다.
SourceMAC	메시지에 대한 소스 MAC 주소입니다.
SourcePortPreNAT	NAT 발생 전 메시지에 대한 소스 포트입니다.
SourcePortPostNAT	NAT 발생 후 메시지에 대한 소스 포트입니다.
DestinationIp	메시지에 대한 대상 IP 주소입니다.
DestinationPort	메시지에 대한 대상 포트입니다.
DestinationIpPreNAT	NAT 발생 전 메시지에 대한 대상 IP 주소입니다.
DestinationIpPostNAT	NAT 발생 후 메시지에 대한 대상 IP 주소입니다.
DestinationPortPreNAT	NAT 발생 전 메시지에 대한 대상 포트입니다.
DestinationPortPostNAT	NAT 발생 후 메시지에 대한 대상 포트입니다.
DestinationMAC	메시지에 대한 대상 MAC 주소입니다.

표 35. 올바른 *matcher* 필드 이름 목록 (계속)

필드 이름	설명
DeviceTime	디바이스에서 사용하는 시간과 형식입니다. 이 날짜 및 시간소인은 이벤트가 전송된 시간을 디바이스에 맞게 표시합니다. 이 매개변수는 이벤트가 도착한 시간을 나타내지는 않습니다. DeviceTime 필드는 추가 데이터 Matcher 속성을 사용하여 이벤트에 대해 사용자 정의 날짜와 시간소인을 사용할 수 있는 기능을 지원합니다. 다음 목록에는 DeviceTime 필드에서 사용할 수 있는 날짜 및 시간소인 형식의 예제가 포함되어 있습니다. • ext-data="dd/MMM/YYYY:hh:mm:ss" 11/Mar/2015:05:26:00 • ext-data="MMM dd YYYY / hh:mm:ss" Mar 11 2015 / 05:26:00 • ext-data="hh:mm:ss:dd/MMM/YYYY" 05:26:00:11/Mar/2015 날짜 및 시간소인 형식에 사용 가능한 값에 대한 자세한 정보는 Joda-Time 웹 페이지 (http://www.joda.org/joda-time/key_format.html)의 내용을 참조하십시오. DeviceTime은 추가 데이터 선택사항 매개변수를 사용하는 유일한 이벤트 필드입니다.
프로토콜	이벤트와 연관된 프로토콜(예: TCP, UDP, ICMP)입니다.
UserName	이벤트와 연관된 사용자 이름입니다.
HostName	이벤트와 연관된 호스트 이름입니다. 일반적으로 이 필드는 ID 이벤트와 연관됩니다.
GroupName	이벤트와 연관된 그룹 이름입니다. 일반적으로 이 필드는 ID 이벤트와 연관됩니다.
NetBIOSName	이벤트와 연관된 NetBIOS 이름입니다. 일반적으로 이 필드는 ID 이벤트와 연관됩니다.
ExtraIdentityData	이벤트와 연관된 사용자 고유 데이터입니다. 일반적으로 이 필드는 ID 이벤트와 연관됩니다.
SourceIpv6	메시지에 대한 IPv6 소스 IP 주소입니다.
DestinationIpv6	메시지에 대한 IPv6 대상 IP 주소입니다.

Multi-event modifier(*event-match-multiple*)

Mmulti-event modifier(event-match-multiple)는 일치하는 일정 범위의 이벤트 유형을 찾은 다음 pattern-id 매개변수와 capture-group-index 매개변수가 지정한 대로 이를 수정합니다.

페이로드에 대해서는 이 일치가 수행되지 않지만 이전에 페이로드에서 구문 분석된 EventName matcher의 결과에 대해서는 수행됩니다.

이 엔티티에서는 디바이스 이벤트 카테고리, 심각도, 이벤트가 ID 이벤트 전송 시 사용하는 방법 등을 변경하여 성공한 이벤트의 변형이 가능합니다. capture-group-index는 정수 값이어야 하고(대체는 지원되지 않음) 패턴 ID는 기존의 패턴 엔티티를 참조해야 합니다. 다른 모든 특성은 single-event modifier의 해당 항목과 동일합니다.

Single-event modifier(*event-match-single*)

Single-event modifier(event-match-single)는 일치 항목을 찾은 다음, 대소문자를 구분하는 필수 EventName 매개변수가 지정하는 대로 정확히 한 가지 유형의 이벤트를 수정합니다.

이 엔티티에서는 디바이스 이벤트 카테고리, 심각도, ID 이벤트 전송 방법 등을 변경하여 성공한 이벤트의 변형이 가능합니다.

이 이벤트 이름과 일치하는 이벤트가 구문 분석될 때 디바이스 카테고리, 심각도 및 ID 특성이 결과로 얻어진 이벤트로 지정됩니다.

사용자가 event-name 속성을 설정해야 하며 이 속성 값은 **EventName** 필드의 값과 일치합니다. 또한 event-match-single 엔티티는 다음의 선택적 특성으로 구성됩니다.

표 *36. single-event* 매개변수 설명

매개변수	설명
device-event-category	이벤트의 OID를 검색하는 새 카테고리입니다. 일부 디바이스는 모든 이벤트에 대해 카테고리가 동일하므로 이 매개변수는 최적화 매개변수입니다.
severity	이벤트의 심각도입니다. 이 매개변수는 1 -10 사이의 정수 값이어야 합니다. 1 미만이거나 10을 초과하는 심각도를 지정하는 경우, 시스템 설정 기본값은 5입니다. 지정하지 않을 경우 QID의 값이 기본값입니다.

표 *36. single-event* 매개변수 설명 *(계속)*

매개변수	설명
send-identity	이벤트의 ID 변경 정보를 전송하도록 지정합니다. 다음 옵션 중 하나를 선택하십시오. • UseDSMResults DSM이 ID 이벤트를 리턴하는 경우 이벤트가 전달됩니다. DSM이 ID 이벤트를 리턴하지 않는 경우 확장은 ID 정보를 작성하거나 수정하지 않습니다. 값을 지정하지 않을 경우 이 옵션이 기본값입니다. • SendIfAbsent DSM이 ID 정보를 작성하는 경우 ID 이벤트는 영향을 받지 않고 전달됩니다. DSM이 ID 이벤트를 작성하지는 않지만 ID 이벤트 작성에 필요한 정보가 이벤트에 충분히 있는 경우 모든 관련 필드를 설정하여 이벤트가 작성됩니다. • OverrideAndAlwaysSend DSM이 리턴하는 모든 ID 이벤트를 무시하고 ID 이벤트를 새로 작성합니다(정보가 충분한 경우). • OverrideAndNeverSend DSM이 리턴하는 ID 정보를 금지합니다. 자산 업데이트로 이동시킬 이벤트를 처리하는 경우가 아니면 권장되는 옵션입니다.

확장 문서 템플리트

예제 확장 문서는 올바르지 않은 이벤트 이름을 사용하여 이벤트가 전송되지 않도록 Cisco FWSM의 특정 유형을 구문 분석하는 방법에 대한 정보를 제공합니다.

예를 들어, 이벤트 이름의 가운데에 임베드된 session이라는 단어를 분석하려는 경우 다음 코드를 사용하십시오.

```
Nov 17 09:28:26 129.15.126.6 %FWSM-session-0-302015:
Built UDP connection for faddr 38.116.157.195/80
gaddr 129.15.127.254/31696 laddr 10.194.2.196/2157
duration 0:00:00 bytes 57498 (TCP FINs)
```

이 조건은 DSM이 구문 분석되지 않았으며 일반 로그 프로그램과 연관된 모든 이벤트를 인식하지 않도록 합니다.

텍스트 문자열(302015)의 일부만이 QID 검색에 사용되어도 전체 텍스트 문자열(%FWSM-session-0-302015)이 Cisco FWSM에서 유입되는 이벤트를 식별합니다. 전체 텍스트 문자열이 올바르지 않으므로 DSM은 이벤트가 올바르지 않은 것으로 간주합니다.

한 이벤트 유형을 구문 분석하는 확장 문서 예제

FWSM 디바이스에는 다수의 이벤트 유형이 있고 이중 다수는 고유한 형식을 갖습니다. 다음의 확장 문서 예제는 한 이벤트 유형의 구문 분석 방식을 보여줍니다.

참고: 패턴 ID가 구문 분석 중인 필드 이름과 일치할 필요는 없습니다. 다음 예제에서는 패턴이 중복되지만 이 경우 SourceIp 필드와 SourceIpPreNAT 필드는 완전히 동일한 패턴을 사용할 수 있습니다. 이 상황이 모든 FWSM 이벤트에서 참인 것은 아닙니다.

```
<?xml version="1.0" encoding="UTF-8"?>
<device-extension xmlns="event_parsing/device_extension">
<pattern id="EventNameFWSM_Pattern" xmlns=""><![CDATA[%FWSM[a-zA-Z\-]*\d-(\d{1,6})]]></pattern>
<pattern id="SourceIp_Pattern" xmlns=""><![CDATA[gaddr (\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/([\d]{1,5})]]></pattern>
<pattern id="SourceIpPreNAT_Pattern" xmlns=""><![CDATA[gaddr (\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/([\d]{1,5})]]></pattern>
<pattern id="SourceIpPostNAT_Pattern" xmlns=""><![CDATA[laddr (\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/([\d]{1,5})]]></pattern>
<pattern id="DestinationIp_Pattern" xmlns=""><![CDATA[faddr (\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/([\d]{1,5})]]></pattern>
<pattern id="Protocol_Pattern" case-insensitive="true" xmlns=""><![CDATA[(tcp|udp|icmp|gre)]]></pattern>
<pattern id="Protocol_6_Pattern" case-insensitive="true" xmlns=""><![CDATA[protocol=6]]></pattern>
<pattern id="EventNameId_Pattern" xmlns=""><![CDATA[(\d{1,6})]]></pattern>
<match-group order="1" description="FWSM Test" device-type-id-override="6" xmlns="">
      <matcher field="EventName" order="1" pattern-id="EventNameFWSM_Pattern" capture-group="1"/>
      <matcher field="SourceIp" order="1" pattern-id="SourceIp_Pattern" capture-group="1" />
      <matcher field="SourcePort" order="1" pattern-id="SourcePort_Pattern" capture-group="2"/>
      <matcher field="SourceIpPreNAT" order="1" pattern-id="SourceIpPreNAT_Pattern" capture-group="1" />
      <matcher field="SourceIpPostNAT" order="1" pattern-id="SourceIpPostNAT_Pattern" capture-group="1" />
      <matcher field="SourcePortPreNAT" order="1" pattern-id="SourcePortPreNAT_Pattern" capture-group="2" />
      <matcher field="SourcePortPostNAT" order="1" pattern-id="SourcePortPostNAT_Pattern" capture-group="2" />
      <matcher field="DestinationIp" order="1" pattern-id="DestinationIp_Pattern" capture-group="1" />
      <matcher field="DestinationPort" order="1" pattern-id="DestinationIp_Pattern" capture-group="2" />
      <matcher field="Protocol" order="1" pattern-id="Protocol_Pattern" capture-group="1" />
      <matcher field="Protocol" order="2" pattern-id="Protocol_6_Pattern" capture-group="TCP" enable-substitutions=true/>
      <event-match-multiple pattern-id="EventNameId" capture-group-index="1" device-event-category="Cisco Firewall"/>
   </match-group>
</device-extension>

<?xml version="1.0" encoding="UTF-8"?>
<device-extension xmlns="event_parsing/device_extension">
<!-- Do not remove the "allEventNames" value -->
<pattern id="EventName-Fakeware_Pattern" xmlns=""><![CDATA[]]></pattern>
<pattern id="SourceIp-Fakeware_Pattern" xmlns=""><![CDATA[]]</pattern>
<pattern id="SourcePort-Fakeware_Pattern" xmlns=""><![CDATA[]]></pattern>
<pattern id="SourceMAC-Fakeware_Pattern" xmlns=""><![CDATA[]]></pattern>
<pattern id="DestinationIp-Fakeware_Pattern" xmlns=""><![CDATA[]]></pattern>
<pattern id="DestinationPort-Fakeware_Pattern" case-insensitive="true" xmlns=""><![CDATA[]]></pattern>
<pattern id="Protocol-Fakeware_Pattern" case-insensitive="true" xmlns=""><![CDATA[]]></pattern>
<match-group order="1" description="FWSM Test" device-type-id-override="6" xmlns="">
   <matcher field="EventName" order="1" pattern-id="EventName-Fakeware_Pattern" capture-group="1"/>
   <matcher field="SourceIp" order="1" pattern-id="SourceIp-Fakeware_Pattern" capture-group="1" />
   <matcher field="SourcePort" order="1" pattern-id="SourcePort-Fakeware_Pattern" capture-group="1"/>
   <matcher field="SourceMAC" order="1" pattern-id="SourceMAC-Fakeware_Pattern" capture-group="1" />
   <matcher field="DestinationIp" order="1" pattern-id="DestinationIp-Fakeware_Pattern" capture-group="1" />
   <matcher field="DestinationPort" order="1" pattern-id="SDestinationPort-Fakeware_Pattern" capture-group="1" />
   <matcher field="Protocol" order="1" pattern-id="Protocol-Fakeware_Pattern" capture-group="1" />
   <event-match-multiple pattern-id="EventNameId" capture-group-index="1" device-event-category="Cisco Firewall"/>
</match-group>
</device-extension>
```

기본 구문 분석

이전의 확장 문서 예제는 구문 분석의 기본적인 부분을 보여줍니다.

- IP 주소
- 포트
- 프로토콜

- 다른 그룹에서 동일한 패턴을 사용하는 여러 필드

다음 예제는 지정된 패턴을 따르는 모든 FWSM 이벤트를 구문 분석합니다. 이 벤트에 다른 컨텐츠가 포함된 경우 구문 분석된 필드가 이들 이벤트에 표시되지 않을 수 있습니다.

이벤트를 통해 제공되지는 않지만 이 구성을 작성하는 데 필요한 정보는 다음과 같습니다.

- 이벤트 이름은 이벤트의 %FWSM-session-0-302015 부분 중 마지막 6자리 (302015) 뿐입니다.
- FWSM은 Cisco Firewall의 하드 코딩된 디바이스 이벤트 카테고리를 갖습니다.
- FWSM DSM은 Cisco Pix QIDmap을 사용하므로 일치 그룹에 device-type-id-override="6" 매개변수가 포함됩니다. Pix firewall 로그 소스 유형 ID는 6입니다. 자세한 정보는 54 페이지의 『로그 소스 유형 ID』의 내용을 참조하십시오.

참고: QID 정보를 지정하지 않거나 사용 불가능한 경우, 이벤트 맵핑을 수정할 수 있습니다. 자세한 정보는 *IBM Security QRadar SIEM* 사용자 안내서의 이벤트 맵핑 수정 섹션을 참조하십시오.

이벤트 이름 및 디바이스 이벤트 카테고리

QIDmap이 검색되면 이벤트 이름과 디바이스 이벤트 카테고리가 필요합니다. 이 디바이스 이벤트 카테고리는 데이터베이스 내의 그룹화 매개변수로, 디바이스 내의 유사 이벤트를 정의할 때 도움이 됩니다. 일치 그룹 끝의 event-match-multiple에는 하드 코딩된 카테고리가 포함되어 있습니다. event-match-multiple는 구문 분석된 이벤트 이름에 EventNameId 패턴을 사용하여 최대 6 자리를 일치시킵니다. 이 패턴은 전체 페이로드에 대해서는 실행되지 않으며 EventName 필드로 구문 분석되는 부분에 대해서만 실행됩니다.

EventName 패턴은 이벤트의 %FWSM 부분을 참조합니다. 모든 Cisco FWSM 이벤트에는 %FWSM 부분이 포함되어 있습니다. 예제의 패턴은 0 이상의 숫자와 대시가 후속되는 %FWSM을 찾습니다. 이 패턴 일치는 제거해야 하며 이벤트 이름의 가운데에 임베드된 session이라는 단어를 찾습니다. 이벤트 심각도(Cisco 기준)에는 대시와 QRadar에 요구되는 이벤트 이름이 후속합니다. (\d{6}) 문자열이 캡처 그룹을 갖는 EventNameFWSM 패턴 내의 유일한 문자열입니다.

이벤트의 IP 주소와 포트는 모두 IP 주소, 콜론, 포트 번호 순의 동일한 기본 패턴을 따릅니다. 이 패턴은 데이터의 두 부분(IP 주소와 포트)을 구문 분석하고 matcher 섹션에서 서로 다른 캡처 그룹을 지정합니다.

```
<device-extension>
<pattern id="EventName1">(logger):</pattern>
<pattern id="DeviceTime1">time=\[(\d{2}/\w{3}/\d{4}:\d{2}:\d{2}:\d{2})\] </pattern>
<pattern id="Username">(TLSv1)</pattern>
<match-group order="1" description="Full Test">
   <matcher field="EventName" order="1" pattern-id="EventName1" capture-group="1"/>
   <matcher field="DeviceTime" order="1" pattern-id="DeviceTime1"
       capture-group="1" ext-data="dd/MMM/YYYY:hh:mm:ss"/>
   <matcher field="UserName" order="1" pattern-id="Username" capture-group="1"/>
</match-group>
</device-extension>
```

IP 주소 및 포트 패턴

IP 주소와 포트 패턴은 마침표, 콜론, 포트 번호로 구분되는 네 세트의 1 ~ 3 자리 수입니다. IP 주소 섹션은 그룹에 있으며 포트 번호이지만 콜론은 없습니다. 이러한 필드의 matcher 섹션은 동일한 패턴 이름을 참조하지만 캡처 그룹은 다르게 참조합니다(IP 주소는 그룹 1이고 포트는 그룹 2입니다).

프로토콜은 페이로드에서 TCP, UDP, ICMP 또는 GRE의 첫 번째 인스턴스를 검색하는 공통 패턴입니다. 패턴은 일치 항목이 찾아지도록 대소문자를 구분하지 않는 매개변수를 사용하여 표시됩니다.

두 번째 프로토콜 패턴은 예제에 사용된 이벤트에서 나타나 않지만 순서 2로 정의된 두 번째 프로토콜 패턴은 있습니다. 가장 낮은 순위의 프로토콜 패턴을 찾지 못하는 경우 그 다음 패턴을 찾습니다. 두 번째 프로토콜 패턴도 직접 대체를 보여줍니다. 패턴에 일치 그룹이 없지만 대체 사용 매개변수를 사용하면 다음 TCP가 protocol=6 대신 사용됩니다.

사용자 정의 로그 소스 문서 작성

지원되는 DSM이 없는 로그 소스에 대해서 또는 정보가 누락되었거나 올바르지 않은 이벤트를 수리하거나 연관된 DSM이 결과를 산출하지 못하는 경우 이벤트를 구문 분석하기 위해 사용자 정의 로그 소스(LSX)를 작성합니다.

공식 DSM이 없는 로그 소스의 경우 범용 DSM 또는 UDSM을 사용하여 로그 소스를 통합하십시오. 그러면 사용자 정의 로그 소스(디바이스 확장이라고도 함)가 UDSM에 적용되어 로그의 구문 분석을 위한 로직을 제공합니다. LSX는 Java 정규식에 기반하며 모든 로그 프로토콜(예: syslog, JDBC, LFPS)에 대해 사용할 수 있습니다. 로그에서 값을 추출하여 QRadar 내의 모든 공통 필드에 맵핑할 수 있습니다.

사용자 정의 로그 소스를 사용하여 누락되거나 올바르지 않은 컨텐츠를 수리하는 경우 사용자 정의 로그 소스에 의해 작성되는 모든 새 이벤트는 원래 페이로드를 구문 분석하는 데 실패한 로그 소스와 연관됩니다. 확장을 작성하면 알 수 없거나 분류되지 않은 이벤트가 IBM Security QRadar에서 알 수 없으므로 저장되지 않습니다.

사용자 정의 로그 소스를 작성하려면 다음 단계를 수행하십시오.

1. QRadar에 로그 소스가 작성되었는지 확인하십시오.

   목록에 없는 항목을 처리하려면 범용 DSM(UDSM)을 로그 소스 유형으로 사용하십시오. 또한 로그가 자동으로 분류되는 것을 막기 위해 로그 소스를 수동으로 작성할 수도 있습니다.
2. 사용 가능한 필드를 판별하려면 **로그 보기** 탭을 사용하여 평가할 로그를 내보내십시오.
3. 확장 문서 예제 템플리트를 사용하여 사용 가능한 필드를 판별하십시오. (37 페이지의 『확장 문서 템플리트』).

   템플리트의 모든 필드를 사용할 필요는 없습니다. 확장 문서 템플리트의 필드에 맵핑할 수 있는 로그 소스의 값을 판별하십시오. 자세한 정보는 37 페이지의 『확장 문서 템플리트』의 내용을 참조하십시오.
4. 사용하지 않은 필드와 해당 패턴 ID를 사용자 정의 로그 소스 문서에서 제거하십시오.
5. 확장 문서를 업로드하고 로그 소스에 확장을 적용하십시오.
6. 이벤트를 QIDmap의 해당 항목에 맵핑하십시오.

   로그 보기 탭의 이 수동 조치는 알 수 없는 로그 소스 이벤트를 알려진 QRadar 이벤트에 맵핑하여 이들 이벤트를 분류하고 처리할 수 있게 합니다.

관련 개념:

29 페이지의 『QRadar 포럼의 사용자 정의 로그 소스 예제』
지원되는 DSM이 없는 로그 소스에 대해 사용자 정의 로그 소스(LSX)를 작성할 수 있습니다. 사용자 고유의 사용자 정의 로그 소스(DSM 확장이라고도 함)를 작성하려면 이전에 작성한 기존 확장을 수정하십시오.

범용 DSM 빌드

범용 DSM 빌드의 첫 번째 단계는 IBM Security QRadar에서 로그 소스를 작성하는 것입니다. 로그 소스를 작성할 때, 로그가 자동 분류되지 않으며 검토를 위해 로그를 내보낼 수 있습니다.

프로시저

1. **관리** 탭에서 **로그 소스** 아이콘을 클릭하여 소스를 새로 작성하십시오.
2. **추가**를 클릭하십시오.
3. **로그 소스 이름** 필드에 이름을 지정하십시오.
4. **로그 소스 유형** 목록에서 **범용 DSM**을 선택하십시오.

   아직 QRadar Console에 로그 소스 확장을 적용하지 않은 경우 **로그 소스 확장**이 표시되지 않을 수 있습니다.

5. **프로토콜 구성** 목록에서 사용할 프로토콜을 지정하십시오.

   이 방법은 QRadar가 지원되지 않는 로그 소스에서 로그를 가져올 때 사용합니다.
6. **로그 소스 ID**에 지원되지 않는 로그 소스의 호스트 이름 또는 IP 주소를 입력하십시오.
7. **저장**을 클릭하여 새 로그 소스를 저장하고 창을 닫으십시오.
8. **관리** 탭에서 **변경사항 배치**를 클릭하십시오.

다음에 수행할 작업

『로그 내보내기』

로그 내보내기

범용 DSM을 빌드한 후 작성된 로그를 내보냅니다.

이 태스크 정보

일반적으로, 검토를 위해 상당수의 로그가 필요합니다. 지원되지 않는 로그 소스의 EPS 비율에 따라 종합적인 로그 샘플을 획득하는 데 몇 시간이 걸릴 수도 있습니다.

QRadar가 로그 소스 유형을 발견하지 못하면 이벤트는 수집되지만 구문 분석되지 않습니다. 이러한 구문 분석되지 않은 이벤트를 필터링한 다음 수신된 마지막 시스템 알림을 검토할 수 있습니다. 시스템 알림을 모두 검토한 후 시간 프레임에 따라 검색을 작성할 수 있습니다.

프로시저

1. 구문 분석되지 않은 이벤트만 보려면 로그를 필터링하십시오.
   a. **로그 보기** 탭을 클릭하십시오.
   b. **필터 추가**를 클릭하십시오.
   c. **이벤트가 구문 분석되지 않음**을 선택하십시오.

      팁: 이벤트가 구문 분석되지 않음 항목을 보려면 **매개변수** 텍스트 내에 입력하십시오.
   d. 시간 프레임을 선택하십시오.
   e. 시스템 알림의 **정보** 이벤트를 보려면 마우스 오른쪽 단추를 클릭하여 정보 이벤트를 필터링하십시오.
   f. **소스 IP** 컬럼을 검토하여 이벤트를 보내고 있는 디바이스를 판별하십시오.

원시 이벤트 페이로드를 볼 수 있습니다. 일반적으로 제조사는 식별 가능한 제품 이름을 헤더에 두므로, 검색을 **표시: 원시 이벤트**로 설정하면 각 이벤트를 직접 열지 않고도 페이로드를 표시할 수 있습니다. 네트워크를 기준으로 정렬하면 이벤트가 시작된 특정 디바이스를 찾는 데 도움이 될 수 있습니다.

2. 로그를 내보내기 위한 검색을 작성하십시오.
   a. **로그 보기** 탭에서 **검색** > **검색 편집**을 선택하십시오.
   b. **시간 범위**에 로그 소스를 작성하기에 충분한 시간(예: 6시간)을 지정하십시오.
   c. **매개변수** 목록의 **검색 매개변수**에서 **로그 소스(색인화됨)**를 선택하고 **연산자** 목록에서 **등호**를 선택하고 **로그 소스 그룹** 목록에서 **기타**를 선택하고, 범용 DSM 빌드 시 작성된 로그 소스를 지정하십시오.

   참고: 설정에 따라, **로그 소스(색인화됨)**가 아닌 **매개변수** 목록에 **로그 소스**가 표시될 수 있습니다.
   d. **검색**을 클릭하여 결과를 보십시오.
3. 콘솔의 결과를 검토하여 페이로드를 확인하십시오.
4. 선택적으로 **조치** > **XML로 내보내기** > **전체 내보내기(모든 컬럼)**을 클릭하여 결과를 내보낼 수 있습니다.

   페이로드가 여러 컬럼으로 분할되어 페이로드를 찾기 어렵게 될 수 있으므로 **CSV로 내보내기**는 선택하지 마십시오. 이벤트 검토에는 XML이 권장되는 형식입니다.
   a. 압축 파일을 다운로드하도록 프롬프트가 표시됩니다. 압축 파일을 열고 결과 파일을 여십시오.
   b. 로그를 검토하십시오.

      다음 태그 사이에 이벤트 페이로드가 있습니다.

```
<payloadAsUTF>
...
</payloadAsUTF>
```

      다음 코드는 예제 페이로드입니다.

```
<payloadAsUTF>ecs-ep (pid 4162 4163 4164) is running... </payloadAsUTF>
```

범용 DSM 작성의 중요 단계가 사용성 로그를 검토하는 것입니다. 로그에는 최소한 이벤트 이름에 맵핑할 수 있는 값이 있어야 합니다. 이벤트 이름은 다양한 로그 유형을 구별할 수 있는 고유 값이어야 합니다.

다음 코드는 사용 가능한 예제 로그입니다.

```
May 20 17:16:14 dropbear[22331]: bad password attempt for 'root'
from 192.168.50.80:3364
May 20 17:16:26 dropbear[22331]: password auth succeeded for
'root' from 192.168.50.80:3364
May 20 16:42:19 kernel: DROP IN=vlan2 OUT=
MAC=00:01:5c:31:39:c2:08:00 SRC=172.29.255.121
DST=255.255.255.255 PROTO=UDP SPT=67 DPT=68
```

다음 예제 코드는 사용성이 다소 떨어지는 로그입니다.

```
Oct 26 08:12:08 loopback 1256559128 autotrace[215824]: W: trace:
no map for prod 49420003, idf 010029a2, lal 00af0008
Oct 26 16:35:00 sxpgbd0081 last message repeated 7 times
Nov 24 01:30:00 sxpgbd0081 /usr/local/monitor-rrd/sxpgbd0081/.rrd
(rc=-1, opening '/usr/local/monitor-rrd/sxpgbd0081/.rrd':
No such file or directory)
```

공통 정규식

정규식을 사용하여 로그 소스 파일에서 일치하는 텍스트 패턴을 찾을 수 있습니다. 메시지를 스캔하여 문자, 숫자 또는 문자와 숫자의 조합 패턴을 찾을 수 있습니다. 예를 들어, 일치하는 소스와 대상 IP 주소, 포트, MAC 주소 등을 찾는 정규식을 작성할 수 있습니다.

다음 코드는 몇 가지 공통 정규식을 보여줍니다.

```
\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3} \d{1,5}
(?:[0-9a-fA-F]{2}\:){5}[0-9a-fA-F]{2} (TCP|UDP|ICMP|GRE)
\w{3}\s\d{2}\s\d{2}:\d{2}:\d{2}
\s \t .*?
```

이스케이프 문자 또는 "\"는 리터럴 문자를 표시하는 데 사용됩니다. 예를 들어, "." 문자는 "단일 문자"를 의미하며 A, B, 1, X 등에 해당합니다. 일치하는 "." 문자(리터럴 일치)를 찾으려면 "\"를 사용해야 합니다.

표 *37.* 공통 *regex* 표현식

유형	표현식
유형	\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}
IP 주소	\d{1,5}
포트 번호	(?:[0-9a-fA-F]{2}\:){5}[0-9a-fA-F]{2}
프로토콜	(TCP|UDP|ICMP|GRE)
디바이스 시간	\w{3}\s\d{2}\s\d{2}:\d{2}:\d{2}
공백	\s
탭	\t

표 37. 공통 *regex* 표현식 (계속)

유형	표현식
모든 일치 항목	.*?

팁: 우연히라도 다른 문자와 일치하지 않게 하려면 숫자가 아니거나 알파벳이 아닌 문자를 이스케이프 처리하십시오.

정규식 패턴 빌드

범용 DSM을 작성하려면 정규식(regex)을 사용하여, 지원되지 않는 로그 소스에서 일치하는 텍스트 문자열을 찾으십시오.

이 태스크 정보

다음 예제는 단계에서 참조되는 로그 항목을 보여줍니다.

```
May 20 17:24:59 kernel: DROP MAC=5c:31:39:c2:08:00
SRC=172.29.255.121 DST=10.43.2.10 LEN=351 TOS=0x00 PREC=0x00 TTL=64 ID=9582
PROTO=UDP SPT=67 DPT=68 LEN=331
May 20 17:24:59 kernel: PASS MAC=5c:14:ab:c4:12:59
SRC=192.168.50.10 DST=192.168.10.25 LEN=351 TOS=0x00 PREC=0x00 TTL=64
ID=9583 PROTO=TCP SPT=1057 DPT=80 LEN=331
May 20 17:24:59 kernel: REJECT
MAC=5c:ad:3c:54:11:07 SRC=10.10.10.5 DST=192.168.100.25 LEN=351
TOS=0x00 PREC=0x00 TTL=64 ID=9584 PROTO=TCP SPT=25212 DPT=6881 LEN=331
```

프로시저

1. 지원되는 로그 소스를 분석하여 가시적으로 고유 패턴을 식별하십시오.

   이러한 패턴은 차후에 정규식으로 변환됩니다.

2. 일치하는 텍스트 문자열을 찾으십시오.

   팁: 기본 오류 점검을 제공하려면 유사한 값이 잘못 찾아지지 않도록 값의 전후에 문자를 포함시키십시오. 나중에 이러한 추가 문자와 실제 값을 격리시킬 수 있습니다.

3. 일치하는 패턴을 찾기 위한 의사 코드를 개발하고 패턴의 시작과 끝을 표시하는 공백 문자를 포함시키십시오.

   따옴표는 무시해도 됩니다. 예제 로그 항목에서 이벤트 이름은 DROP, PASS 및 REJECT입니다. 다음 목록은 사용 가능한 이벤트 필드를 보여줍니다.

   - EventName: " kernel: VALUE "
   - SourceMAC: " MAC=VALUE "
   - SourceIp: " SRC=VALUE "
   - DestinationIp: " DST=VALUE "
   - Protocol: " PROTO=VALUE "

- SourcePort: " SPT=VALUE "
- DestinationPort: " DPT=VALUE "

4. 공백을 \s 정규식으로 대체하십시오.

   숫자가 아니거나 알파벳이 아닌 문자에는 이스케이프 문자를 사용해야 합니다. 예를 들어, =는 \=이 되고 :는 \:이 됩니다.

5. 의사 코드를 정규식으로 변환하십시오.

표 *38.* 의사 코드를 정규식으로 변환

필드	의사 코드	정규식
EventName	" kernel: VALUE "	\skernel\:\s.*?\s
SourceMAC	" MAC=VALUE "	\sMAC\=(?:[0-9a-fA-F]{2}\:){5}[0-9a-fA-F]{2}\s
SourceIP	" SRC=VALUE "	\sSRC\=\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\s
DestinationIp	" DST=VALUE "	\sDST\=\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\s
프로토콜	" PROTO=VALUE "	\ s P R O T O \ = (TCP|UDP|ICMP|GRE)\s
SourcePort	" SPT=VALUE "	\sSPT\=\d{1,5}\s
DestinationPort	" DPT=VALUE "	\sDPT\=\d{1,5}\s

6. 캡처 그룹을 지정하십시오.

   캡처 그룹은 정규식에서 특정 값을 격리시킵니다.

   예를 들어, 이전 예제의 SourcePort 패턴에서는 공백과 SRC=<code>가 포함되어 있으므로 전체 값을 전달할 수 없습니다. 대신 캡처 그룹을 사용하여 포트 번호만 지정하십시오. 캡처 그룹의 값이 IBM Security QRadar의 관련 필드에 전달되는 값입니다.

   캡처하려는 값 주위에 소괄호를 삽입하십시오.

표 *39.* 정규식을 맵핑하여 이벤트 필드 그룹 캡처

필드	정규식	캡처 그룹
EventName	\skernel\:\s.*?\s	\skernel\:\s(.*?)\s
SourceMAC	\sMAC\=(?:[0-9a-fA- F]{2}\:){5}[0-9a-fA-F]{2}\s	\sMAC\=((?:[0-9a-fA- F]{2}\:){5}[0-9a-fA-F]{2})\s
SourceIP	\sSRC\=\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\s	\sSRC\=(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})\s
Destination IP	\sDST\=\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\s	\sDST\=(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})\s
Protocol	\ s P R O T O \ = (TCP|UDP|ICMP|GRE)\s	\ s P R O T O \ = ((TCP|UDP|ICMP|GRE))\s
SourcePort	\sSPT\=\d{1,5}\s	\sSPT\=(\d{1,5})\s
DestinationPort	\sDPT\=\d{1,5}\s	\sDPT\=(\d{1,5})\s

7. 패턴과 캡처 그룹을 사용자 정의 로그 소스 문서로 마이그레이션하십시오.

   다음 코드 스니팻은 사용자가 사용하는 문서의 일부분입니다.

```
<device-extension xmlns="event_parsing/device_extension">
<pattern id="EventNameFWSM_Pattern" xmlns=""><![CDATA[%FWSM[a-zA-Z\-]*\d-(\d{1,6})]]></pattern>
<pattern id="SourceIp_Pattern" xmlns=""><![CDATA[gaddr (\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/([\d]{1,5})]]></pattern>
<pattern id="SourceIpPreNAT_Pattern" xmlns=""><![CDATA[gaddr (\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/([\d]{1,5})]]></pattern>
<pattern id="SourceIpPostNAT_Pattern" xmlns=""><![CDATA[laddr (\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/([\d]{1,5})]]></pattern>
<pattern id="DestinationIp_Pattern" xmlns=""><![CDATA[faddr (\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/([\d]{1,5})]]></pattern>
<pattern id="Protocol_Pattern" case-insensitive="true" xmlns=""><![CDATA[(TCP|UDP|ICMP|GRE)]]></pattern>
<pattern id="Protocol_6_Pattern" case-insensitive="true" xmlns=""><![CDATA[protocol=6]]></pattern>
<pattern id="EventNameId_Pattern" xmlns=""><![CDATA[(\d{1,6})]]></pattern>
```

QRadar에 확장 문서 업로드

여러 개의 확장 문서를 작성한 다음 이를 업로드하고 다양한 로그 소스 유형에 이를 연관시킬 수 있습니다. 지원되지 않는 로그 소스의 로그를 구문 분석하는 데에는 사용자 정의 로그 소스(LSX)의 로직이 사용됩니다.

IBM Security QRadar에 업로드하기 전에 임의의 위치에 확장 문서를 저장할 수 있습니다.

프로시저

1. **관리** 탭에서 **데이터 소스** > **사용자 정의 로그 소스**를 클릭하십시오.
2. 사용자 정의 로그 소스 추가 창에서 **추가**를 클릭하십시오.
3. 이름을 지정하십시오.
4. 범용 DSM(UDSM)을 사용하는 경우 확장 문서를 **로그 소스 유형**의 기본값으로 선택하지 마십시오.

   범용 DSM을 기본값으로 선택하면 연관된 모든 로그 소스에 영향이 미칩니다. 범용 DSM을 사용하여 여러 개의 사용자 정의 이벤트 소스와 지원되지 않는 이벤트 소스에 대한 구문 분석 로직을 정의할 수 있습니다.
5. 옵션: 이 사용자 정의 로그 소스를 둘 이상의 로그 소스 유형 인스턴스에 적용하려는 경우 사용 가능한 **로그 소스 유형** 목록에서 로그 소스 유형을 선택하고 추가 화살표를 클릭하여 이를 기본값으로 설정하십시오.

   기본 로그 소스를 설정하면 자동으로 발견된 로그 소스를 비롯하여 로그 소스 유형의 모든 이벤트에 사용자 정의 로그 소스가 적용됩니다.

   먼저 로그 소스 유형의 확장을 테스트하여 이벤트가 올바로 구문 분석되는지 확인하십시오.
6. **찾아보기**를 클릭하여 저장한 LSX를 찾은 다음 **업로드**를 클릭하십시오.

   QRadar는 내부 XSD에 견주어 문서의 유효성을 검증하고 확장 문서가 시스템에 업로드되기 전에 문서의 유효성을 검증합니다.
7. **저장**을 클릭하고 창을 닫으십시오.
8. 사용자 정의 로그 소스를 로그 소스에 연관시키십시오.

a. **관리** 탭에서 **데이터 소스** > **로그 소스**를 클릭하십시오.

b. 해당 확장 문서를 작성한 로그 소스 유형을 두 번 클릭하십시오.

c. **사용자 정의 로그 소스** 목록에서, 사용자가 작성한 문서를 선택하십시오.

d. **저장**을 클릭하고 창을 닫으십시오.

알 수 없는 이벤트 맵핑

처음에는 범용 DSM의 모든 이벤트가 QRadar의 **로그 보기** 탭에 알 수 없음으로 표시됩니다. 모든 알 수 없는 이벤트를 QID 맵의 관련 항목에 직접 맵핑해야 합니다.

로그 파일의 이벤트 이름(예: DROP, DENY 및 ACCEPT)이 이해 가능한 값이어도 QRadar가 이들 값의 의미를 이해하지 못합니다. QRadar에게 이들 값은 알려진 값에는 맵핑되지 않는 텍스트 문자열입니다. 값은 예상대로 표시되어 직접 맵핑할 때까지 정상화된 이벤트로 취급됩니다.

IDS(Intrusion Detection System) 또는 IDP(Intrusion Detection and Prevention System)과 같은 일부 인스턴스에는 수천 개의 이벤트가 존재하여 맵핑이 필요합니다. 이런 경우 카테고리를 이벤트 이름으로 맵핑하십시오. 예를 들어, 다음 예제에서 맵핑 수를 줄이려면 이벤트 이름에 이름 필드를 사용하지 말고 카테고리 필드를 대신 사용하십시오. 다음과 같이 사용자 정의 특성을 사용하여 이벤트 이름(Code Red v412)을 표시할 수 있습니다.

```
date: "Feb 25 2010 00:43:26"; name: "SQL Slammer v312"; category: "Worm
Activity"; source ip: "100.100.200.200"; date:
"Feb 25 2015 00:43:26"; name: "Code Red v412"; category: "Worm Activity";
source ip: "100.100.200.200"; date: "Feb 25 2015 00:43:26"; name:
"Annoying Toolbar"; category: "Malware"; source ip: "100.100.200.200";
```

이벤트 이름에 이름 필드를 사용하지 말고 카테고리 필드를 대신 사용하십시오. 실제 이벤트 이름(즉, Code Red v412)은 사용자 정의 특성을 사용하여 표시할 수 있습니다.

시작하기 전에

사용자 정의 로그 소스 문서를 업로드하여 범용 DSM에 적용했는지 확인하십시오. 자세한 정보는 47 페이지의 『QRadar에 확장 문서 업로드』의 내용을 참조하십시오.

프로시저

1. **로그 보기** 탭에서 **검색** > **검색 편집**을 클릭하십시오.
2. **시간 범위** 옵션에서 사용자 정의 로그 소스를 범용 DSM에 적용하기에 충분한 시간(약 15분)을 선택하십시오.

3. **검색 매개변수**의 **매개변수** 목록에서 **로그 소스[색인]**를 선택하고 **연산자** 목록에서 **등호**를 선택한 다음 **로그 소스 그룹**과 **로그 소스 목록**에서 사용자가 작성한 로그 소스를 선택하십시오.
4. **검색**을 클릭하여 결과를 보십시오.

   모든 이벤트가 알 수 없음으로 표시됩니다.
5. 알 수 없음 항목을 두 번 클릭하여 이벤트 세부사항을 보십시오.
6. 도구 모음의 **이벤트 맵핑**을 클릭하십시오.

   사용자 정의 로그 소스의 **EventName 값**(예: DROP, DENY 또는 ACCEPT)이 **로그 소스 이벤트 ID** 값에 표시됩니다. 값이 공백이면 안 됩니다. 공백 값은 사용자 정의 로그 소스 문서에 오류가 있음을 나타냅니다.
7. **로그 소스 이벤트 ID**로 표시되는 값을 해당 QID에 맵핑하십시오.

   카테고리별로 찾아보기, **QID 검색** 또는 둘 다를 사용하여 **로그 소스 이벤트 ID** 값에 가장 잘 맞는 값을 찾으십시오. 예를 들어, DROP 값은 **QID Firewall Deny - Event CRE**에 맵핑할 수 있습니다.

   이름에는 QID와 이벤트 CRE를 함께 사용하십시오. 대부분의 이벤트는 특정 로그 소스 유형에 고유합니다. 예를 들어, 무작위 방화벽에 맵핑하는 경우 **Deny QID**는 범용 DSM을 다른 로그 소스 유형의 이벤트에 맵핑하는 것과 유사합니다. 이름 Event CRE를 포함하는 QID 항목은 일반용이며 특정 로그 소스 유형에 연결되지 않습니다.
8. 알 수 없음 이벤트가 모두 정상적으로 맵핑될 때까지 이들 단계를 반복하십시오.

   이 시점에서 특정 로그 소스 이벤트 ID를 포함하는 범용 DSM의 추가 이벤트는 지정된 QID로 표시됩니다. QID 맵핑 이전에 도착한 이벤트는 계속 알 수 없음으로 유지됩니다. 이전 이벤트를 현재 QID에 맵핑하기 위한 방법은 없습니다. 모든 알 수 없음 이벤트가 정상적으로 QID에 맵핑될 때까지 이 프로세스를 반복해야 합니다.

구문 분석 문제 및 예제

사용자 정의 로그 소스를 작성할 때 구문 분석 문제점이 발생할 수 있습니다. 다음의 XML 예제를 사용하여 특정의 구문 분석 문제점을 해결할 수 있습니다.

프로토콜 변환

다음 예제는 페이로드에서 TCP, UDP, ICMP 또는 GRE를 검색하는 일반적인 프로토콜 변환을 보여줍니다. 검색 패턴은 단어 경계(예: 탭, 공백 또는 행의 끝)로 묶여 있습니다. 또한 대소문자는 무시됩니다.

```
<pattern id="Protocol" case-insensitive="true" xmlns="">
<![CDATA[\b(TCP|UDP|ICMP|GRE)\b]]>
</pattern>
<matcher field="Protocol" order="1" pattern-id="Protocol" capture-group="1" />
```

단일 대체 작성

다음 예제는 소스 IP 주소를 구문 분석하여 결과를 대체하고 IP 주소를 100.100.100.100으로 설정하는(페이로드의 IP 주소는 무시함) 대체를 보여줍니다.

다음 예에서는 소스 IP 주소가 쉼표가 후속하는 SrcAddress=10.3.111.33과 유사한 것으로 가정합니다.

```
<pattern id="SourceIp_AuthenOK" xmlns="">
<![CDATA[SrcAddress=(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}),]]>
</pattern>

<matcher field="SourceIp" order="1" pattern-id="SourceIp_AuthenOK"
capture-group="100.100.100.100" enable-substitutions="true"/>
```

콜론으로 구분되는 MAC 주소 생성

QRadar는 콜론으로 구분된 양식의 MAC 주소를 발견합니다. 모든 디바이스가 이 양식을 사용하지는 않으므로 다음 예제는 해당 상황을 정정하는 방법을 보여줍니다.

```
<pattern id="SourceMACWithDashes" xmlns="">
    <![CDATA[SourceMAC=([0-9a-fA-F]{2})-([0-9a-fA-F]{2})-([0-9a-fA-F]{2})-
    ([0-9a-fA-F]{2})-([0-9a-fA-F]{2})-([0-9a-fA-F]{2})]]>
</pattern>
 <matcher field="SourceMAC" order="1" pattern-id="
    SourceMACWithDashes" capture-group="\1:\2:\3:\4:\5:\6" />
```

이전 예제에서는 SourceMAC=12-34-56-78-90-AB가 12:34:56:78:90:AB의 MAC 주소로 변환되었습니다.

패턴에서 대시가 제거되면 패턴은 MAC 주소로 변환되고 구분 기호를 갖지 않습니다. 공백이 삽입되면 패턴은 공백으로 구분되는 MAC 주소로 변환됩니다.

IP 주소와 포트 결합

일반적으로 IP 주소와 포트는 콜론으로 구분되어 한 필드에 결합됩니다.

다음 예제는 한 패턴에서 여러 개의 캡처 그룹을 사용합니다.

```
pattern id="SourceIPColonPort" xmlns="">
<! [CDATA[Source=(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}):([\d]{1,5})]]>
</pattern>

<matcher field="SourceIp" order="1" pattern-id="SourceIPColonPort" capture-group="1" />
<matcher field="SourcePort" order="1" pattern-id="SourceIPColonPort" capture-group="2" />
```

이벤트 카테고리 수정

디바이스 이벤트 카테고리를 하드 코딩하거나 심각도를 조정할 수 있습니다.

다음 예제는 단일 이벤트 유형의 심각도를 조정합니다.

```
<event-match-single event-name="TheEvent" device-event-
category="Actual Category" severity="6" send-identity="UseDSMResults"
/>
```

ID 변경 이벤트 금지

DSM은 불필요하게 ID 변경 이벤트를 전송할 수 있습니다.

다음 예제는 단일 이벤트 유형이나 이벤트 그룹에서 ID 변경 이벤트가 전송되지 않게 하는 방법을 보여줍니다.

```
// Never send identity for the event with an EventName of Authen OK
<event-match-single event-name="Authen OK" device-event-category="ACS"
severity="6" send-identity="OverrideAndNeverSend" />

// Never send any identity for an event with an event name starting with 7,
followed by one to five other digits:
<pattern id="EventNameId" xmlns=""><![CDATA[(7\d{1,5})]]>
</pattern>

<event-match-multiple pattern-id="EventNameId" capture-group-index="1"
device-event-category="Cisco Firewall" severity="7"
send-identity="OverrideAndNeverSend"/>
```

인코딩 로그

다음의 인코딩 형식이 지원됩니다.

- US-ASCII
- UTF-8

US-ASCII 또는 UTF-8 형식과 일치하지 않는 인코딩으로 시스템에 로그를 전달할 수 있습니다. 입력이 구문 분석과 저장 용도로 다시 UTF-8로 인코딩될 수 있도록 고급 플래그를 구성할 수 있습니다.

예를 들어, SHIFT-JIS(ANSI/OEM Japanese) 인코딩으로 소스 로그가 도달하는 경우 다음 코드를 입력하십시오.

```
<device-extension source-encoding=SHIFT-JIS xmlns=event_parsing/device_extension>
```

로그는 UTF-8 형식으로 인코딩됩니다.

형식화 이벤트 날짜 및 시간소인

사용자 정의 로그 소스는 이벤트에서 여러 개의 서로 다른 날짜 및 시간소인 형식을 발견할 수 있습니다.

디바이스 제조업체들이 표준 날짜 및 시간소인 형식을 따르지 않으므로 DeviceTime을 다시 형식화할 수 있도록 추가 데이터 선택 매개변수가 사용자 정의 로그 소스에 포함되어 있습니다. 다음 예제는 날짜 및 시간소인 형식을 정정하기 위해 이벤트를 다시 형식화하는 방법을 보여줍니다.

```
<device-extension>
<pattern id="EventName1">(logger):</pattern>
<pattern id="DeviceTime1">time=\[(\d{2}/\w{3}/\d{4}:\d{2}:\d{2}:\d{2})\]</pattern>
<pattern id="Username">(TLSv1)</pattern>

<match-group order="1" description="Full Test">
   <matcher field="EventName" order="1" pattern-id="EventName1_Pattern" capture-group="1"/>
   <matcher field="DeviceTime" order="1" pattern-id="DeviceTime1_Pattern"
   capture-group="1" ext-data="dd/MMM/YYYY:hh:mm:ss"/>
   <matcher field="UserName" order="1" pattern-id="Username_Pattern" capture-group="1"/>
</match-group>
</device-extension>
```

단일 로그 소스의 다중 로그 형식

다중 로그 형식이 단일 로그 소스에 포함되는 경우가 종종 있습니다.

```
May 20 17:15:50 kernel: DROP IN=vlan2 OUT= MAC= SRC=67.149.62.133
DST=239.255.255.250 PROTO=UDP SPT=1900 DPT=1900
May 20 17:16:26 dropbear[22331]: password auth succeeded for 'root' from 192.168.50.80:3364
May 20 17:16:28 dropbear[22331]: exit after auth (root): Exited normally </br>
May 20 17:16:14 dropbear[22331]: bad password attempt for 'root' from 192.168.50.80:3364
```

예를 들어, 방화벽 이벤트용과 인증 이벤트용으로 하나씩 두 개의 로그 형식이 있습니다. 이벤트를 구문 분석하려면 여러 개의 패턴을 작성해야 합니다. 구문 분석 순서를 지정할 수 있습니다. 일반적으로 빈도가 낮은 이벤트 보다 빈도가 높은 이벤트를 먼저 구문 분석합니다. 모든 이벤트를 구문 분석하기 위해 필요한 만큼 패턴을 사용할 수 있습니다. 순서 변수는 일치하는 패턴을 찾는 순서를 판별합니다.

다음 예제는 EventName 및 UserName 필드에 대한 여러 가지 형식을 보여줍니다.

고유한 각 로그 유형을 구문 분석하기 위해 별도의 패턴이 작성됩니다. 정규화된 필드에 값을 지정할 때 두 패턴이 모두 참조됩니다.

```
<pattern id="EventName-DDWRT-FW_Pattern" xmlns=""><![CDATA[kernel\:\s(.*?)\s]]></pattern>
<pattern id="EventName-DDWRT-Auth_Pattern" xmlns=""><![CDATA[sdrophear\[\d{1,5}\]|:\s(.*?\s.*?)\s]]>
</pattern>

<pattern id="UserName_DDWRT-Auth1__Pattern" xmlns=""><![CDATA[\sfor\s\'(.*?)\'s]]></pattern>
<pattern id="UserName_DDWRT-Auth2__Pattern" xmlns=""><![CDATA[\safter\sauth\s\((.*?)\)\:]]></pattern>

<match-group order="1" description="DD-WRT Device Extensions xmlns="">
   <matcher field="EventName" order="1" pattern-id="EventName-DDWRT-FW_Pattern" capture-group="1"/>
   <matcher field="EventName" order="2" pattern-id="EventName-DDWRT-Auth_Pattern" capture-group="1"/>

   <matcher field="UserName" order="1" pattern-id="UserName-DDWRT-Auth1_Pattern" capture-group="1"/>
   <matcher field="UserName" order="2" pattern-id="UserName-DDWRT-Auth2_Pattern" capture-group="1"/>
```

CSV 로그 형식 구문 분석

CSV 형식 로그 파일은 여러 개의 캡처 그룹이 있는 단일 구문 분석기를 사용할 수 있습니다. 이 로그 유형을 구문 분석할 때에는 패턴 ID를 반드시 여러 개 작성해야 하는 것은 아닙니다.

이 태스크 정보

다음 로그 로그 샘플이 사용됩니다.

```
Event,User,Source IP,Source Port,Destination IP,Destination Port
Failed Login,bjones,192.168.50.100,1024,10.100.24.25,22
Successful Login,nlabadie,192.168.64.76,1743,10.100.24.25,110
Privilege Escalation,bjones,192.168.50.100,1028,10.100.1.100,23
```

프로시저

1. 이전 패턴을 사용하여 관련 값을 모두 찾아내는 구문 분석기를 작성하십시오.

   ```
   .*?\,.*?\,\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}
   \,\d{1,5}\,\d{1,3}\.\d{1,3} \.\d{1,3}\.\d{1,3}\,\d{1,5}
   ```

2. 각 값 주위에 캡처 그룹을 배치하십시오.

   ```
   (.*?)\,(.*?)\,(\d{1,3}\.\d{1,3}\.\d{1,3}\.
   \d{1,3})\,(\d{1,5})\,(\d{1,3} \.\d{1,3}\.\d{1,3}\.\d{1,3})\,(\d{1,5})
   ```

3. 이동 시마다 값을 증가시키면서 각 캡처 그룹이 맵핑된 필드를 맵핑하십시오.

   ```
   1 = Event, 2 = User, 3 = Source IP,
   4 = Source Port, 5 = Destination IP, 6 = Destination Port
   ```

4. 캡처 그룹을 관련 이벤트에 맵핑하여 사용자 정의 로그 소스에 값을 포함시키십시오.

   다음 코드는 캡처 그룹을 관련 이벤트에 맵핑하는 예제의 일부입니다.

   ```
   <pattern id="CSV-Parser_Pattern" xmlns=""><![CDATA 9.*?)\,(.*?)\,(\d{1,3}\.\{1,3}\.{1,3}]]></pattern>
   <match-group order="1" description="Log Source Extension xmlns="">
      <matcher field="EventName" order="1" pattern-id="CSV-Parser_Pattern" capture-group="1"/>
      <matcher field="SourceIP" order="1" pattern-id="CSV-Parser_Pattern" capture-group="3"/>
      <matcher field="SourcePort" order="1" pattern-id="CSV-Parser_Pattern" capture-group="4"/>
      <matcher field="DestinationIP" order="1" pattern-id="CSV-Parser_Pattern" capture-group="5"/>
      <matcher field="DestinationPort" order="1" pattern-id="CSV-Parser_Pattern" capture-group="6"/>
      <matcher field="UserName" order="1" pattern-id="CSV-Parser_Pattern" capture-group="2"/>
   ```

5. 사용자 정의 로그 소스를 업로드하십시오.

6. 이벤트를 맵핑하십시오.

관련 태스크:

48 페이지의 『알 수 없는 이벤트 맵핑』

처음에는 범용 DSM의 모든 이벤트가 QRadar의 **로그 보기** 탭에 알 수 없음으로 표시됩니다. 모든 알 수 없는 이벤트를 QID 맵의 관련 항목에 직접 맵핑해야 합니다.

로그 소스 유형 ID

IBM Security QRadar는 다수의 로그 소스를 지원하며 각 로그 소스는 ID를 갖습니다. `match-group`문에서 로그 소스 유형 ID를 사용합니다.

다음 표에 지원되는 로그 소스 유형과 해당 ID가 나열되어 있습니다.

표 *40.* 로그 소스 유형 *ID*

ID	로그 소스 유형
2	Snort Open Source IDS
3	Check Point Firewall-1
4	구성 가능한 방화벽 필터
5	Juniper Networks Firewall 및 VPN
6	Cisco PIX Firewall
7	구성 가능한 인증 메시지 필터
9	Enterasys Dragon Network IPS
10	Apache HTTP Server
11	Linux OS
12	Microsoft Windows 보안 이벤트 로그
13	Windows IIS
14	Linux iptables Firewall
15	IBM Proventia Network Intrusion Prevention System(IPS)
17	Juniper Networks Intrusion Detection and Prevention(IDP)
19	TippingPoint Intrusion Prevention System(IPS)
20	Cisco IOS
21	Nortel Contivity VPN Switch
22	Nortel Multiprotocol Router
23	Cisco VPN 3000 Series Cntrator
24	Solaris 운영 체제 인증 메시지
25	McAfee IntruShield Network IPS Appliance
26	Cisco CSA
28	Enterasys Matrix E1 Switch
29	Solaris 운영 체제 메일 발송 로그
30	Cisco Intrusion Prevention System(IDS)
31	Cisco Firewall Services Module(FWSM)
33	IBM Proventia Management SiteProtector
35	Cyberguard FW/VPN KS Family
36	Juniper Networks Secure Access(SA) SSL VPN
37	Nortel Contivity VPN Switch
38	Top Layer Intrusion Prevention System(IPS)

표 *40.* 로그 소스 유형 *ID (*계속*)*

ID	로그 소스 유형
39	Universal DSM
40	Tripwire Enterprise
41	Cisco Adaptive Security Appliance(ASA)
42	Niksun 2005 v3.5
45	Juniper Networks Network and Security Manager(NSM)
46	Squid Web Proxy
47	Ambiron TrustWave ipAngel Intrusion Prevention System(IPS)
48	Oracle RDBMS 감사 보고서
49	F5 Networks BIG-IP LTM
50	Solaris 운영 체제 DHCP 로그
55	Array Networks SSL VPN Access Gateway
56	Cisco CatOS for Catalyst Switches
57	ProFTPD Server
58	Linux DHCP Server
59	Juniper Networks Infranet Controller
64	Juniper JunOS Platform
68	Enterasys Matrix K/N/S Series Switch
70	Extreme Networks ExtremeWare Operating System(OS)
71	Sidewinder G2 Security Appliance
73	Fortinet FortiGate Security Gateway
78	SonicWall UTM/Firewall/VPN device
79	Vericept Content 360
82	Symantec Gateway Security(SGS) Appliance
83	Juniper Steel Belted Radius
85	IBM AIX Server
86	Metainfo MetaIP
87	SymantecSystemCenter
90	Cisco ACS
92	Forescout CounterACT
93	McAfee ePolicy Orchestrator
95	CiscoNAC Appliance
96	TippingPoint X Series Appliances
97	Microsoft DHCP Server
98	Microsoft IAS Server
99	Microsoft Exchange Server
100	Trend Interscan VirusWall
101	Microsoft SQL Server

표 *40.* 로그 소스 유형 *ID (*계속*)*

ID	로그 소스 유형
102	MAC OS X
103	Bluecoat SG Appliance
104	Nortel Switched Firewall 6000
106	3Com 8800 Series Switch
107	Nortel VPN Gateway
108	Nortel Threat Protection System(TPS) Intrusion Sensor
110	Nortel Application Switch
111	Juniper DX Application Acceleration Platform
112	SNARE Reflector Server
113	Cisco 12000 Series Routers
114	Cisco 6500 Series Switches
115	Cisco 7600 Series Routers
116	Cisco Carrier Routing System
117	Cisco Integrated Services Router
118	Juniper M-Series Multiservice Edge Routing
120	Nortel Switched Firewall 5100
122	Juniper MX-Series Ethernet Services Router
123	Juniper T-Series Core Platform
134	Nortel Ethernet Routing Switch 8300/8600
135	Nortel Ethernet Routing Switch 2500/4500/5500
136	Nortel Secure Router
138	OpenBSD OS
139	Juniper Ex-Series Ethernet Switch
140	Sysmark Power Broker
141	Oracle Database Listener
142	Samhain HIDS
143	Bridgewater Systems AAA Service Controller
144	이름 값 쌍
145	Nortel Secure Network Access Switch(SNAS)
146	Starent Networks Home Agent(HA)
148	IBM AS/400 iSeries
149	Foundry Fastiron
150	Juniper SRX Series Services Gateway
153	CRYPTOCard CRYPTOShield
154	Imperva Securesphere
155	Aruba Mobility Controller
156	Enterasys NetsightASM
157	Enterasys HiGuard

표 *40.* 로그 소스 유형 *ID (*계속*)*

ID	로그 소스 유형
158	Motorola SymbolAP
159	Enterasys HiPath
160	Symantec Endpoint Protection
161	IBM RACF
163	RSA Authentication Manager
164	Redback ASE
165	Trend Micro Office Scan
166	Enterasys XSR Security Routers
167	Enterasys Stackable and Standalone Switches
168	Juniper Networks AVT
169	OS Services Qidmap
170	Enterasys A-Series
171	Enterasys B2-Series
172	Enterasys B3-Series
173	Enterasys C2-Series
174	Enterasys C3-Series
175	Enterasys D-Series
176	Enterasys G-Series
177	Enterasys I-Series
178	Trend Micro Control Manager
179	Cisco IronPort
180	Hewlett Packard UniX
182	Cisco Aironet
183	Cisco Wireless Services Module(WiSM)
185	ISC BIND
186	IBM Lotus Domino
187	HP Tandem
188	Sentrigo Hedgehog
189	Sybase ASE
191	Microsoft ISA
192	Juniper SRC
193	Radware DefensePro
194	Cisco ACE Firewall
195	IBM DB2
196	Oracle Audit Vault
197	Sourcefire Defense Center
198	Websense V Series
199	Oracle RDBMS OS 감사 보고서
206	Palo Alto PA Series
208	HP ProCurve

표 *40.* 로그 소스 유형 *ID (*계속*)*

ID	로그 소스 유형
209	Microsoft Operations Manager
210	EMC VMWare
211	IBM WebSphere Application Server
213	F5 Networks BIG-IP ASM
214	FireEye
215	Fair Warning
216	IBM Informix
217	CA Top Secret
218	Enterasys NAC
219	System Center Operations Manager
220	McAfee Web Gateway
221	CA Access Control Facility(ACF2)
222	McAfee 애플리케이션 / 변경 제어
223	Lieberman Random Password Manager
224	Sophos Enterprise Console
225	NetApp Data ONTAP
226	Sophos PureMessage
227	Cyber-Ark Vault
228	Itron Smart Meter
230	Bit9 Parity
231	IBM IMS
232	F5 Networks FirePass
233	Citrix NetScaler
234	F5 Networks BIG-IP APM
235	Juniper Networks vGW
239	Oracle BEA WebLogic
240	Sophos Web Security Appliance
241	Sophos Astaro Security Gateway
243	Infoblox NIOS
244	Tropos Control
245	Novell eDirectory
249	IBM Guardium
251	Stonesoft Management Center
252	SolarWinds Orion
254	Great Bay Beacon
255	Damballa Failsafe
258	CA SiteMinder
259	IBM z/OS
260	Microsoft SharePoint
261	iT-CUBE agileSI

표 *40.* 로그 소스 유형 *ID (*계속*)*

ID	로그 소스 유형
263	Digital China Networks DCS and DCRS Series switch
264	Juniper Security Binary Log Collector
265	Trend Micro Deep Discovery
266	Tivoli Access Manager for e-business
268	Verdasys Digital Guardian
269	Hauwei S Series Switch
271	HBGary Active Defense
272	APC UPS
272	Cisco Wireless LAN Controller
276	IBM Customer Information Control System(CICS)
278	Barracuda Spam & Virus Firewall
279	Open LDAP
280	Application Security DbProtect
281	Barracuda Web Application Firewall
283	Huawei AR Series Router
286	IBM AIX Audit
289	IBM Tivoli Endpoint Manager
290	Juniper Junos WebApp Secure
291	Nominum Vantio
292	Enterasys 800-Series Switch
293	IBM zSecure Alert
294	IBM Security Network Protection(XGS)
295	IBM Security Identity Manager
296	F5 Networks BIG-IP AFM
297	IBM Security Network IPS(GX)
298	Fidelis XPS
299	Arpeggio SIFT-IT
300	Barracuda Web Filter
302	Brocade FabricOS
303	ThreatGRID Malware Threat Intelligence Platform
304	IBM Security Access Manager for Enterprise Single Sign-On
306	Venustech Venusense Unified Threat Management
307	Venustech Venusense Firewall
308	Venustech Venusense Network Intrusion Prevention System
309	ObserveIT

표 *40.* 로그 소스 유형 *ID (*계속*)*

ID	로그 소스 유형
311	Pirean Access: One
312	Venustech Venusense Security Platform
313	PostFix MailTransferAgent
314	Oracle Fine Grained Auditing
315	VMware vCenter
316	Cisco Identity Services Engine
318	Honeycomb Lexicon File Integrity Monitor
319	Oracle Acme Packet SBC
320	Juniper WirelessLAN
330	Arbor Networks Peakflow SP
331	Zscaler Nss
332	Proofpoint Enterprise Protection/Enterprise Privacy
338	Microsoft Hyper-V
339	Cilasoft QJRN/400
340	Vormetric Data Security
341	SafeNet DataSecure/KeySecure
343	STEALTHbits StealthINTERCEPT
344	Juniper DDoS Secure
345	Arbor Networks Pravail
346	Trusteer Apex
348	IBM Security Directory Server
349	Enterasys A4-Series
350	Enterasys B5-Series
351	Enterasys C5-Series
354	Avaya VPN Gateway
356	DG Technology MEAS
358	CloudPassage Halo
359	CorreLog Agent for IBM zOS
360	WatchGuard Fireware OS
361	IBM Fiberlink MaaS360
362	Trend Micro Deep Discovery Analyzer
363	AccessData InSight
364	BM Privileged Session Recorder
367	Universal CEF
369	FreeRADIUS
370	Riverbed SteelCentral NetProfiler
372	SSH CryptoAuditor
373	IBM WebSphere DataPower
374	Symantec Critical System Protection

표 *40.* 로그 소스 유형 *ID (*계속*)*

ID	로그 소스 유형
375	Kisco Information Systems SafeNet/i
376	IBM Federated Directory Server
378	Lastline Enterprise
379	genua genugate
383	Oracle Enterprise Manager

제 3 장 사용자 정의 로그 소스 관리

사용자 정의 로그 소스를 작성하여 특정 디바이스의 구문 분석 루틴을 확장하거나 수정할 수 있습니다.

사용자 정의 로그 소스는 이벤트 페이로드에서 수신된 이벤트를 식별하고 분류하는 데 필요한 모든 정규식 패턴을 포함하는 XML 파일입니다. 구문 분석 문제를 정정하거나 DSM의 이벤트에 대한 기본 구문 분석을 겹쳐써야 할 때 이벤트를 구문 분석하는 데 확장 파일을 사용할 수 있습니다. 네트워크에 있는 어플라이언스 또는 보안 디바이스의 이벤트를 구문 분석하는 DSM이 없는 경우, 확장에서 이벤트 지원을 제공할 수 있습니다. **로그 보기** 탭은 다음과 같은 기본 유형으로 로그 소스 이벤트를 식별합니다.

- 이벤트를 적절히 구문 분석하는 로그 소스. 적절히 구문 분석된 이벤트는 올바른 로그 소스 유형 및 카테고리에 지정됩니다. 이 경우에는 개입이나 확장이 필요하지 않습니다.
- 이벤트를 구문 분석하지만 **로그 소스** 매개변수에 **알 수 없음** 값을 갖는 로그 소스. 알 수 없는 이벤트는 로그 소스 유형은 식별되지만 DSM에서 해당 페이로드 정보를 이해할 수 없는 로그 소스 이벤트입니다. 시스템은 사용 가능 정보에서 이벤트를 적절히 분류하는 데 필요한 이벤트 ID를 판별할 수 없습니다. 이 경우에는 이벤트를 임의 카테고리로 맵핑하거나 알 수 없는 이벤트에 대한 이벤트 구문 분석을 수리하는 사용자 정의 로그 소스를 작성할 수 있습니다.
- 로그 소스 유형을 식별할 수 없고 **로그 소스** 매개변수에 **저장됨** 이벤트 값을 갖는 로그 소스. 저장된 이벤트를 적절히 구문 분석하려면 DSM 파일을 업데이트하거나 사용자 정의 로그 소스를 작성해야 합니다. 이벤트 구문 분석 후 이벤트를 맵핑할 수 있습니다.

사용자 정의 로그 소스를 추가하려면 먼저 확장 문서를 작성해야 합니다. 확장 문서는 일반 문서 처리 또는 텍스트 편집 애플리케이션으로 작성할 수 있는 XML 문서입니다. 여러 확장 문서를 작성하고 업로드하며 다양한 로그 소스 유형과 연관시킬 수 있습니다. 확장 문서의 형식은 표준 XML 스키마 문서(XSD)를 준수해야 합니다. 확장 문서를 개발하려면 XML 코딩 지식과 경험이 필요합니다.

사용자 정의 로그 소스 추가

사용자 정의 로그 소스를 추가하여 특정 디바이스의 구문 분석 루틴을 확장하거나 수정할 수 있습니다.

프로시저

1. **관리** 탭을 클릭하십시오.
2. **사용자 정의 로그 소스** 아이콘을 클릭하십시오.
3. **추가**를 클릭하십시오.
4. **로그 소스 유형** 목록에서 다음 옵션 중 하나를 선택하십시오.

옵션	설명
사용 가능	디바이스 지원 모듈(DSM)이 로그 소스의 대부분의 필드를 올바르게 구문 분석할 때 이 옵션을 선택하십시오. 올바르지 않게 구문 분석된 필드 값은 새 XML 값으로 개선됩니다.
기본값으로 설정	확장 구문 분석에 추가하거나 제거할 로그 소스를 선택하십시오. 로그 소스에 확장을 추가하거나 제거할 수 있습니다. 사용자 정의 로그 소스를 로그 소스의 **기본값으로 설정**하는 경우, **로그 소스 유형**이 동일한 새 로그 소스는 지정된 사용자 정의 로그 소스를 사용합니다.

5. **찾아보기**를 클릭하여 사용자 정의 로그 소스 XML 문서를 찾으십시오.
6. **업로드**를 클릭하십시오. 올바른 확장 파일이 업로드되었는지 확인할 수 있도록 사용자 정의 로그 소스의 컨텐츠가 표시됩니다. 확장 파일을 업로드할 때 XSD에 대해 파일을 평가하여 오류가 있는지 확인합니다.
7. **저장**을 클릭하십시오.

결과

확장 파일에 오류가 없으면 새 사용자 정의 로그 소스가 작성되고 사용됩니다. 로그 소스에 사용자 정의 로그 소스를 적용하지 않고 사용자 정의 로그 소스를 업로드할 수 있습니다. 확장의 상태에 대한 변경은 즉시 적용되며 관리 호스트 또는 콘솔은 사용자 정의 로그 소스에서 새 이벤트 구문 분석 매개변수를 적용합니다.

다음에 수행할 작업

로그 보기 탭에서 이벤트에 대한 구문 분석 패턴이 올바르게 적용되는지 검증하십시오. 로그 소스가 이벤트를 **저장됨**으로 분류하는 경우, 사용자 정의 로그 소스의 구문 분석 패턴을 조정해야 합니다. 로그 소스 이벤트에 대해 확장 파일을 검토하여 이벤트 구문 분석 문제를 찾을 수 있습니다.

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.

150-945
서울특별시 영등포구
국제금융로 10, 3IFC
한국 아이.비.엠 주식회사
대표전화서비스: 02-3781-7114

2바이트(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

다음 단락은 현지법과 상충하는 영국이나 기타 국가에서는 적용되지 않습니다.

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 비IBM의 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.

150-945
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 있는 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.

본 문서에 포함된 모든 성능 데이터는 제한된 환경에서 산출된 것입니다. 따라서 다른 운영 환경에서 얻어진 결과는 상당히 다를 수 있습니다. 일부 성능은 개발 단계의 시스템에서 측정되었을 수 있으므로 이러한 측정치가 일반적으로 사용되고 있는 시스템에서도 동일하게 나타날 것이라고는 보증할 수 없습니다. 또한 일부 성능은 추정을 통해 추측되었을 수도 있으므로 실제 결과는 다를 수 있습니다. 이 책의 사용자는 해당 데이터를 본인의 특정 환경에서 검증해야 합니다.

비IBM 제품에 관한 정보는 해당 제품의 공급업체, 공개 자료 또는 기타 범용 소스로부터 얻은 것입니다. IBM에서는 이러한 비IBM 제품을 반드시 테스트하지 않았으므로, 이들 제품과 관련된 성능의 정확성, 호환성 또는 기타 주장에 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 기업의 이름 및 주소와 유사하더라도 이는 전적으로 우연입니다.

이 정보를 소프트카피로 확인하는 경우에는 사진과 컬러 삽화가 제대로 나타나지 않을 수도 있습니다.

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.

Linux는 미국 또는 기타 국가에서 사용되는 Linus Torvalds의 등록상표입니다.

UNIX는 미국 또는 기타 국가에서 사용되는 The Open Group의 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.

상표

IBM, IBM 로고 및 ibm.com은 미국 또는 기타 국가에서 사용되는 International Business Machines Corporation의 상표 또는 등록상표입니다. 이와 함께 기타 IBM 상표가 기재된 용어가 상표 기호(® 또는 ™)와 함께 이 정보에 처음 표시된 경우, 이와 같은 기호는 이 정보를 발행할 때 미국에서 IBM이 소유한 등록상표 또는 일반 법적 상표입니다. 또한 이러한 상표는 기타 국가에서 등록상표 또는 일반 법적 상표입니다. 현재 IBM 상표 목록은 다음 사이트에서 확인할 수 있습니다. 저작권 및 상표 정보(www.ibm.com/legal/copytrade.shtml)

다음 용어는 각 회사의 상표 또는 등록상표입니다.

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

Linux는 미국 또는 기타 국가에서 사용되는 Linus Torvalds의 등록상표입니다.

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

UNIX는 미국 또는 기타 국가에서 사용되는 The Open Group의 등록상표입니다.

기타 회사, 제품 및 서비스 이름은 타사의 상표 또는 서비스표입니다.

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.

배치된 구성에 따라 이 소프트웨어 오퍼링은 세션 관리 및 인증을 위해 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/) 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.

색인

[가]

[나]

[라]

[바]

[사]

[자]

[하]

C

E

I

J

M

O

P

S

T

U

V

X