IBM Security QRadar

버전 7.3.0

문제점 해결 및 시스템 알림 안내서

IBM

참고

이 정보와 이 정보가 지원하는 제품을 사용하기 전에, 61 페이지의 『주의사항』에 있는 정보를 확인하십시오.

제품 정보

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

목차

이 책의 정보

이 정보는 IBM® Security QRadar®에서 사용하기 위한 것이며 QRadar SIEM 사용 시 표시될 수 있는 공통 시스템 알림과 오류에 대한 진단 및 해결 정보를 제공합니다.

IBM Security QRadar 문제점 해결 및 시스템 알림 안내서에서는 QRadar 콘솔에 표시되는 시스템 알림의 문제를 해결하는 방법에 대한 정보를 제공합니다. 콘솔에 표시되는 시스템 알림은 사용자 배치에 포함된 어플라이언스 또는 QRadar 제품에 적용할 수 있습니다.

달리 명시하지 않는 한 QRadar에 대한 모든 참조는 다음 제품을 말합니다.

- IBM Security QRadar SIEM
- IBM QRadar Log Manager

이 책의 사용자

문제를 해결할 책임이 있는 시스템 관리자는 IBM Security QRadar 및 네트워크 장치와 방화벽에 액세스할 관리 권한을 가지고 있어야 합니다. 시스템 관리자는 회사 네트워크 및 네트워킹 기술에 대한 지식을 가지고 있어야 합니다.

QRadar 시스템을 설치하고 구성할 책임이 있는 네트워크 관리자는 네트워크 보안 개념과 Linux 운영 체제에 익숙해야 합니다.

기술 문서

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

QRadar 제품 라이브러리에서 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 지원 및 기술 노트 다운로드 (http://www.ibm.com/support/docview.wss?uid=swg21616144)를 참조하십시오.

우수 보안 관리제도에 대한 설명

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

참고:

본 프로그램의 사용은 개인 정보, 정보 보호, 고용, 전기 통신 및 저장과 관련된 법률 또는 규정을 포함하여 다양한 법률 또는 규정과 연관될 수 있습니다. IBM Security QRadar는 합법적인 목적과 합법적인 방법으로만 사용될 수 있습니다. 고객은 적용되는 법률, 규정 또는 정책에 의거하여 본 프로그램을 사용하고, 적용되는 법률, 규정 또는 정책을 준수할 모든 책임이 있다는 것에 동의합니다. 라이센스 사용자는 IBM Security QRadar의 합법적인 사용이 가능하게 하기 위해 필요한 모든 동의, 허가 및 라이센스를 이미 취득했거나 취득할 것임을 진술하고 보증합니다.

제 1 장 문제점 해결

문제점 해결은 문제 해결을 위한 체계적인 접근 방식입니다. 문제점 해결의 목표는 일부 기능이 예상대로 작동하지 않는 이유 및 문제 해결 방법을 판별하는 것입니다. 문제점 해결 태스크에 도움이 될 수 있는 공통 기술이 있습니다.

문제점 해결 프로세스의 첫 번째 단계는 문제점을 완벽하게 서술하는 것입니다. 문제점 설명은 사용자 및 기술 지원 담당자가 문제의 원인을 어디에서 찾을 수 있는지를 파악하는 데 도움을 줍니다. 이 단계에서는 다음과 같은 기본적인 질문을 스스로에게 던져야 합니다.

- 문제의 증상은 어떻습니까?
- 문제가 어디에서 발생합니까?
- 문제가 언제 발생합니까?
- 어떠한 조건에서 문제가 발생합니까?
- 문제를 재현할 수 있습니까?

이러한 질문에 대답하면 문제를 잘 설명할 수 있으며 이를 통해 문제를 해결할 수 있습니다.

문제의 증상은 어떻습니까?

문제점 설명을 시작할 때 가장 명확한 질문은 "무슨 문제입니까?"입니다. 이 질문은 간단한 것 같지만 문제를 자세히 설명하기 위해 여러 주요한 문제로 나눌 수 있습니다. 다음과 같은 질문이 포함될 수 있습니다.

- 누가 또는 무엇이 문제를 보고합니까?
- 오류 코드와 메시지는 무엇입니까?
- 시스템이 어떻게 실패합니까? 예를 들어, 문제가 루프, 정지, 충돌, 성능 저하 또는 올바르지 않은 결과입니까?

문제가 어디에서 발생합니까?

문제가 어디에서 발생했는지 판별하는 것은 쉬운 일은 아니지만 문제를 해결하는 데 있어 가장 중요한 단계 중 하나입니다. 보고하는 구성요소와 실패한 구성요소 사이에 많은 기술 계층이 있을 수 있습니다. 네트워크, 디스크 및 드라이버는 문제를 조사할 때 고려할 몇 가지 구성요소일 뿐입니다.

다음 질문을 통해 문제 계층을 격리할 수 있습니다.

- 문제가 한 어플라이언스에만 해당합니까?

- 현재 환경과 구성이 지원됩니까?

한 계층에서 문제를 보고한다고 해서 해당 계층이 문제의 원인이라고 단정할 수는 없습니다. 문제가 발생되는 위치를 식별하는 것은 문제가 있는 환경을 이해하는 것입니다. 시간을 내어 운영 체제와 버전, 모든 소프트웨어와 버전, 하드웨어 등 문제점 환경을 자세히 설명하십시오. 지원되는 환경에서 실행 중인지 확인하십시오. 많은 문제는 함께 실행할 목적이 아니거나 함께 사용되도록 완전히 테스트되지 않은 호환되지 않는 레벨의 소프트웨어 때문에 발생하는 것으로 추적될 수 있습니다.

문제가 언제 발생합니까?

특히 일회성 문제의 경우 문제가 발생하게 되는 이벤트의 상세한 타임라인을 작성하십시오. 역순으로 작업하면 타임라인을 가장 쉽게 작성할 수 있습니다. 즉, 사용 가능한 로그와 정보를 통해 오류가 보고된 시간(가능한 한 밀리초 단위까지 정확하게)에서 시작하여 역순으로 작업하십시오. 일반적으로는 진단 로그에서 첫 번째로 의심스러운 이벤트까지만 살펴보면 됩니다.

이벤트의 세부 타임라인을 작성하려면 다음 질문에 응답하십시오.

- 문제가 주간 또는 야간의 특정 시간에만 발생합니까?
- 문제가 얼마나 자주 발생합니까?
- 문제가 보고되는 시점까지 이벤트가 어떤 순서로 발생합니까?
- 소프트웨어나 하드웨어의 설치 또는 업그레이드 등 환경이 변경된 이후 문제가 발생합니까?

어떠한 조건에서 문제가 발생합니까?

문제가 발생할 때 실행 중인 시스템 및 애플리케이션을 파악하는 일은 문제점 해결의 중요한 부분입니다. 이러한 환경에 대한 질문을 통해 문제의 원인을 식별할 수 있습니다.

- 동일한 태스크가 수행될 때 문제가 항상 발생합니까?
- 문제가 발생하려면 특정한 일련의 이벤트가 있어야 합니까?
- 다른 애플리케이션도 동시에 실패합니까?

이러한 질문에 응답하면 문제가 발생하는 환경을 설명하고 종속성을 연관시키는 데 도움이 됩니다. 여러 문제가 동시에 발생하는 경우 이러한 문제가 반드시 관련되어 있지는 않습니다.

문제를 재현할 수 있습니까?

재현할 수 있는 문제점은 쉽게 해결 가능한 경우가 많습니다. 그러나 문제점 재현에 따른 단점이 있을 수 있습니다. 문제가 비즈니스에 심각한 영향을 미치는 경

우 반복되지 않기를 원할 것입니다. 가능하면 테스트 또는 개발 환경에서 문제를 재현하십시오. 그러면 일반적으로 조사 중에 보다 유연성을 가지고 제어할 수 있습니다. 다음 질문에 답해보십시오.

- 테스트 시스템에서 문제를 재현할 수 있습니까?
- 여러 사용자에게 동일한 유형의 문제가 발생합니까?
- 단일 명령 또는 명령 세트를 실행하여 문제를 재현할 수 있습니까?

디스크 스토리지에 액세스 불가능 오류

IBM Security QRadar 배치의 각 호스트는 파티션의 가용성을 모니터합니다. 디스크 가용성은 파일을 열고 쓰고 삭제함으로써 매분마다 테스트됩니다.

디스크 가용성 테스트가 기본값 5초보다 오래 걸리는 경우 호스트 컨텍스트 프로세스가 QRadar 로그에 오류를 보고합니다. 또한 QRadar 시스템에 높은 부하가 발생하고 대량의 데이터가 기록되거나 검색되거나 제거되거나 다른 시스템에 복사되는 경우에도 오류가 발생할 수 있습니다.

오류는 다음 출력과 유사합니다.

```
Jun 24 07:22:41 127.0.0.1 [hostcontext.hostcontext]
[5b3acf9a-aa8a-437a-b059-01da87333f43/SequentialEventDispatcher]
com.q1labs.hostcontext.ds.DiskSpaceSentinel: [ERROR]
[NOT:0150062100][172.16.77.116/- -]
[-/- -]The storage partition(s) /store/backup on qradarfc (172.16.77.116)
are not currently accessible. Manual intervention may be required to
restore normal operation.
```

메시지가 반복적으로 표시되는 경우, 문제를 확인하십시오. 추가 정보는 『파티션 스토리지 문제 확인』의 내용을 참조하십시오.

파티션 스토리지 문제 확인

IBM Security QRadar Console 또는 관리 호스트에서 임시 파일을 작성하여 파티션 스토리지 문제를 확인합니다.

시작하기 전에

파티션 스토리지 문제가 느리거나 사용할 수 없는 외부 스토리지로 인해 발생하지 않았는지 확인하십시오.

프로시저

1. SSH를 사용하여 QRadar Console에 로그인하십시오.
2. 다음 명령을 입력하여 테스트를 작성하십시오.

```
touch /store/backup/testfile
```

```
ls -la /store/backup/testfile
```

3. 다음 메시지 2개 중 1개가 표시되면 파티션 테스트 제한시간을 늘리십시오.
   - `touch: cannot touch `/store/backup/testfile': Read-only file system`
   - `nfs server time out`
   a. **관리** 탭을 클릭하십시오.
   b. **시스템 구성** 메뉴에서 **시스템 설정** > **고급**을 클릭하십시오.
   c. **파티션 테스터 제한시간(초)** 목록 상자에 20을 선택하거나 입력하십시오.
   d. **저장**을 클릭하십시오.
4. 다음 옵션 중 하나를 선택하십시오.
   - iSCSI, 파이버 채널 또는 NFS(Network File System)와 같은 네트워크 파일 시스템을 사용하는 경우 스토리지 관리자에게 문의하여 파일 서버에 액세스할 수 있는지와 작동되는지 확인하십시오.
   - 로컬 파일 시스템을 사용하면 파일 시스템 문제 또는 실패한 디스크가 있을 수 있습니다.

프로토콜 업데이트 후 로그 소스 오류 해결

IBM Security QRadar, 디바이스 서비스 모듈(DSM), 프로토콜 또는 취약성 정보 서비스(VIS) 구성요소를 업그레이드한 후 로그 소스를 편집하려고 하면 오류 메시지가 표시될 수 있습니다. 캐시된 파일을 제거하려면 QRadar 웹 서비스를 다시 시작하고 브라우저 캐시에서 QRadar 파일을 지우십시오.

시작하기 전에

SSH 액세스 및 루트 계정 신임 정보가 있어야 합니다.

이 태스크 정보

다음 메시지는 QRadar가 업데이트된 후 웹 서버가 다시 시작되지 않았음을 표시합니다.

```
오류가 발생했습니다.
F5를 눌러 브라우저를 새로 고치고 조치를 다시 시도하십시오.
문제가 지속되면 고객 지원에 문의하여 도움을 받으십시오.
```

파일은 QRadar 웹 서비스 또는 데스크탑 브라우저에 의해 캐시될 수 있습니다. QRadar 웹 서비스를 다시 시작하고 데스크탑에서 캐시 파일을 제거해야 합니다.

프로시저

1. SSH를 사용하여 QRadar에 로그인하십시오.
2. 다음 명령을 입력하여 QRadar 웹 서비스를 다시 중지하십시오.

```
systemctl stop tomcat
```

3. 하나의 웹 브라우저 창을 열어 두십시오.
4. 브라우저 캐시를 지우려면 웹 브라우저의 환경 설정으로 이동하십시오.
5. 브라우저를 다시 시작하십시오.
6. 다음 명령을 입력하여 QRadar 웹 서비스를 다시 시작하십시오.

```
systemctl start tomcat
```

디스크 사용량 레벨 확인

디스크 용량이 100%에 도달해도 /var/log 파티션은 계속해서 작동합니다. 그러나 IBM Security QRadar 시작 프로세스와 구성요소에 영향을 줄 수 있는 로그 데이터가 디스크에 기록되지 않을 수 있습니다.

프로시저

1. SSH를 사용하여 QRadar 또는 관리 호스트에 로그인하십시오.
2. 디스크는 파티션 사용량을 검토하려면 다음 명령을 입력하십시오.

```
df -h
```

3. 파티션을 검토하여 해당 디스크 사용량 레벨을 확인하십시오.

다음에 수행할 작업

모니터되는 파티션이 95%에 도달하는 경우 『디스크 사용량 문제 해결』의 내용을 참조하십시오.

디스크 사용량 문제 해결

데이터 보존 기간 설정이 너무 높거나 사용 가능한 스토리지가 IBM Security QRadar가 데이터를 수신하는 비율에 충분하지 못한 경우 파일 시스템 파티션이 95%에 도달합니다. 보존 버킷 스토리지 설정을 다시 구성하면 전체 QRadar 배치의 저장소가 영향을 받습니다.

프로시저

1. / 파일 시스템에서 이전 디버그 또는 패치 파일을 식별하여 제거하십시오.
2. /store 파일 시스템의 디스크 사용량을 줄이십시오.
3. 다음 옵션 중 하나를 선택하십시오.
   - /store/ariel/events 파일 시스템에서 가장 오래된 데이터를 제거하십시오.

- 기본 보존 버킷 스토리지 설정을 조정하여 데이터 보존 기간을 줄이십시오. 자세한 정보는 *IBM Security QRadar* 관리 안내서의 내용을 참조하십시오.
- /store 파일이 가득 차면 짧은 기간 동안 보존할 수 있는 로그 소스를 식별하십시오. 보존 버킷을 사용하여 로그 소스를 관리하십시오. 자세한 정보는 *IBM Security QRadar* 관리 안내서의 내용을 참조하십시오.
- iSCSI 또는 파이버 채널과 같은 오프보드 스토리지 솔루션을 고려하십시오. 자세한 정보는 오프보드 스토리지 안내서의 내용을 참조하십시오.
- /var/log 파일 시스템이 100% 용량에 도달해도 QRadar가 종료되지 않습니다. 기타 문제로 인해 사용자 로그 파일이 예상보다 더 빨리 증가할 수 있습니다.

이벤트 처리 성능

IBM Security QRadar 구성이 이벤트 처리 파이프라인에 영향을 줄 수 있습니다.

이벤트 처리는 DSM 확장, 사용자 정의 특성, 룰 테스트 및 글로벌 보기의 영향을 받을 수 있습니다. 이벤트 구문 분석 및 사용자 정의 룰 엔진은 삭제된 이벤트를 자동으로 감지하고 자체 모니터링 진단을 실행하며 상태가 느린 DSM 확장, 룰 및 특성을 보고합니다.

최적화되지 않은 사용자 정의 특성

사용자 정의 특성은 검색 및 필터링을 위해 QRadar에 정기적으로 사용될 때 최적화됨으로 표시됩니다.

최적화되지 않은 사용자 정의 특성은 시스템에서 구문 분석하며, 이는 검색 속도 및 웹 브라우저의 로딩 비율에 영향을 줍니다.

성능에 영향을 주는 룰 테스트

이벤트 페이로드에서 정규식을 테스트하는 룰은 전체 페이로드는 검색하므로 QRadar 성능에 영향을 줍니다.

페이로드 테스트를 룰에 추가하기 전에 룰 필터를 사용하여 이벤트 수를 줄이십시오. 예를 들어 활성 디렉토리 로그에서 특정 메시지를 검색하는 경우 룰에 다음 필터를 적용하십시오.

- 로그 소스 유형 필터
- 로그 소스 그룹 또는 특정 로그 소스 필터
- 선택적 소스 IP 주소 필터

포트가 열린 호스트 테스트는 수동 및 활성 포트를 QRadar에서 받은 이벤트 및 플로우와 비교하므로 성능에 영향을 줍니다. 테스트를 사용하기 전에 호스트가 통신 요청에 응답하는지 확인하기 위해 양방향 검사를 수행하십시오.

글로벌 보기

여러 필드로 그룹화된 저장된 검색은 고유한 항목이 많이 있는 글로벌 보기를 생성합니다. 데이터 볼륨이 증가됨에 따라 디스크 사용량, 처리 시간 및 검색 성능이 영향을 받을 수 있습니다.

데이터 볼륨이 증가하지 않도록 하려면 필요한 필드에 대한 검색만 집계하십시오. 검색 기준에 필터를 추가하여 누산기에 대한 영향을 줄일 수 있습니다.

DSM 및 최적화된 사용자 정의 특성 문제 식별

성능 저하 문제를 해결하기 위해 최근에 설치한 DSM 확장 또는 최근에 사용 설정한 사용자 정의 특성에 대한 문제를 식별합니다.

이 태스크 정보

DSM 확장은 지원되지 않거나 완전하지 않은 로그 소스에서 이벤트 데이터를 추출하기 위해 정규 표현식 패턴 일치를 사용하여 사용자 정의 구분 분석 메소드를 작성합니다. 최적화된 사용자 정의 특성은 정규식 패턴을 사용하여 구문 분석할 때 이벤트에서 데이터를 추출합니다.

DSM 확장 또는 최적화된 사용자 정의 특성에 사용되는 정규 표현식 패턴은 IBM Security QRadar에서의 이벤트 처리에 영향을 줄 수 있습니다. 비효율적인 정규식을 사용하면 부적절하게 데이터를 스토리지로 직접 라우팅하고 QRadar 성능을 저하시키고 이벤트 처리에 영향을 줄 수 있습니다.

DSM 및 최적화된 사용자 정의 특성 문제로 인해 다음과 같은 시스템 알림이 발생할 수 있습니다.

이벤트 파이프라인에서 성능 저하가 발견되었습니다.
이벤트가 스토리지로 직접 라우팅되었습니다.

프로시저

1. 최근에 설치되거나 사용 설정된 DSM 확장 또는 사용자 정의 특성을 사용 안함으로 설정하십시오.
2. 다음 옵션 중 하나를 선택하십시오.
   - QRadar가 이벤트 삭제를 중지하고 시스템 알림을 수신하는 경우 DSM 확장 또는 사용자 정의 특성을 검토하여 비효율적인 정규 표현식 패턴을 식별하고 개선하십시오.

- QRadar가 이벤트를 삭제를 계속 진행하는 경우 다중 DSM 확장 또는 사용자 정의 특성으로 인해 이벤트 파이프라인에 문제가 발생할 수 있습니다.

3. SSH를 사용하여 이벤트를 삭제하는 QRadar 이벤트 프로세서에 로그인하고 다음 명령을 입력하십시오.

   ```
   /opt/qradar/support/threadTop.ssh –p 7777
   ```

   이 명령은 데이터 처리 엔진 활동을 표시합니다. 다음 표는 출력의 컬럼에 대해 설명합니다.

표 *1.* 데이터 처리 엔진 컬럼

컬럼	설명
서버	포트 또는 프로세스.
ID	프로세스 ID.
MSecs	CPU 시간.
이름	프로세스 이름.

4. 구문 분석기 스레드가 1500밀리초보다 길게 실행되는 경우 다음 명령을 입력하여 Java 스레드 스택을 검토하십시오.

   ```
   /opt/qradar/support/threadTop.sh -p 7777 -s -e ".*Event Parser.*" |
   less
   ```

다음에 수행할 작업

Java 스레드 스택에 `java.util.regex.Pattern$Curly.match`가 포함된 경우 비용 효율이 낮은 DSM 확장 또는 사용자 정의 특성으로 인해 성능 저하가 발생할 수 있습니다. 자세한 정보는 56 페이지의 『비용 효율이 낮은 DSM 확장 발견』 또는 54 페이지의 『비용 효율이 낮은 사용자 정의 특성 발견』의 내용을 참조하십시오.

Java 스레드 스택에 비용 효율이 낮은 정규식이 없으면 DSM 확장 또는 사용자 정의 특성으로 인해 구문 분석 문제가 발생할 수 있습니다. 자세한 정보는 *IBM Security QRadar* 로그 소스 사용자 안내서에서 구문 분석 문제 주제를 참조하십시오.

불완전한 보고서 결과

IBM Security QRadar 보고서를 구성하고 실행하면 예기치 않은 결과를 볼 수 있습니다. 보고서에 필요한 모든 데이터가 표시되지 않는 것처럼 보일 수 있습니다.

검색에 대한 데이터 누적은 검색이 스케줄된 보고서에 추가될 때만 시작됩니다. 예를 들어 수요일에 작성되고 매주 월요일에 실행되도록 스케줄된 보고서는 일주일 동안의 데이터를 표시하지 않습니다. 그러나 다음 보고서에는 일주일 동안의 데이터가 포함됩니다.

다음 솔루션 중 하나를 시도하십시오.

검색을 다시 실행하십시오.

네트워크, **활동** 또는 **로그 보기** 탭을 사용하여 검색을 다시 실행하십시오. 생성된 보고서와 결과를 비교할 수 있습니다.

보고서 탭에서 알림 메시지를 검토하십시오.

데이터가 완전하지 않으면 **보고서** 탭에 알림 메시지가 표시됩니다.

초기 기간의 원시 데이터에 대해 보고서를 실행하십시오.

초기 기간의 원시 데이터에 대해 보고서를 실행하여 모든 보고서 데이터를 캡처하는지 확인하십시오. 추가 정보는 *IBM Security QRadar* 사용자 안내서의 내용을 참조하십시오.

불완전한 보고서는 시스템이 60초 간격 이내에 데이터 집계를 누적할 수 없는 경우에도 발생합니다. QRadar는 매분 각 집계된 검색의 데이터 집계를 작성합니다. 검색 수 및 검색의 고유 값이 너무 큰 경우 집계를 처리하는 데 필요한 시간이 60초를 초과할 수 있습니다. 누적을 60초 이내에 완료할 수 없는 경우 누적 간격이 삭제됩니다. 문제가 발생하면 시계열 그래프 및 보고서에 기간에 대한 컬럼이 누락될 수 있습니다. 추가 정보는 28 페이지의 『누산기가 집계 데이터의 정의를 읽거나 볼 수 없음』의 내용을 참조하십시오.

관련 개념:

26 페이지의 『누산기 속도 감소』

38750099 - 누산기가 이 간격 동안의 모든 이벤트/플로우를 집계할 수 없습니다.

백업 파티션에 대한 디스크 공간 제한 문제 해결

대상 파일 시스템에서 디스크 공간이 제한되므로 시스템 알림이 표시됩니다. 디스크 공간이 충분하지 않아서 IBM Security QRadar가 백업을 완료할 수 없습니다.

다음 시스템 알림을 수신할 수 있습니다.

백업: 백업을 수행하기에 디스크 여유 공간이 부족합니다.

/store/backup/ 파티션의 디스크 공간이 마지막 백업 파일 크기의 두 배보다 작은 경우 제한된 디스크 공간에 대한 시스템 알림이 발생합니다. 데이터 볼륨 및

백업 보존 기간 설정으로 인해 디스크 공간이 제한됩니다. 자세한 정보는 *IBM Security QRadar* 관리 안내서의 내용을 참조하십시오.

보존 버킷 스토리지 설정을 구성하면 QRadar 배치의 스토리지 전체에 영향을 줍니다.

디스크 사용량 경고는 QRadar Console 또는 QRadar 배치의 관리 호스트에서 발생할 수 있습니다. 디스크 사용량을 확인하려면 QRadar Console 또는 관리 호스트에서 모니터되는 파티션을 검토하십시오.

프로시저

1. 백업 파티션 디스크 레벨을 확인하십시오.
   a. SSH를 사용하여 QRadar Console 또는 관리 호스트에 로그인하십시오.
   b. 다음 명령을 입력하십시오.

      ```
      df -PTh /store/backup
      ```
2. 백업 파티션을 검토하여 디스크 활용도 레벨을 확인하십시오.
   a. 백업 파티션이 마지막 백업 파일 크기의 두 배보다 큰 경우 백업 위치를 식별하십시오.
      - 백업이 `/store/ariel` 디렉토리와 같은 파일 시스템에 있는 경우 다른 스토리지 시스템으로 이동하십시오.
      - 외부 백업인 경우 사용량을 확인하여 백업 보존 기간에 사용 가능한 공간보다 더 많은 공간이 필요하지 않은지 확인하십시오.
   b. `/store` 파일 시스템의 디스크 사용량을 줄이십시오.
      - iSCSI 또는 파이버 채널 같은 오프보드 스토리지 솔루션을 사용하여 외부 스토리지 크기를 늘릴 것을 고려하십시오. 자세한 정보는 오프보드 스토리지 안내서의 내용을 참조하십시오.
      - QRadar 백업 파티션이 NFS 공유에 마운트된 경우 백업에 대한 보존 기간을 줄이십시오. 기본 백업 보존 기간은 2일입니다. 백업 보존 기간 구성에 대한 자세한 정보는 *IBM Security QRadar* 관리 안내서의 내용을 참조하십시오.

라이센스 시스템 알림

IBM Security QRadar 콘솔은 배치에 포함된 모든 라이센스를 관리합니다. 일별 시스템 알림은 라이센스가 만료되기 전과 후에 생성됩니다.

다음 표에서는 활성 라이센스에 종속되는 QRadar 구성요소를 표시합니다.

표 2. *QRadar* 만료 라이센스의 영향

만료된 라이센스 유형	결과
콘솔	QRadar Console 라이센스가 만료되면 콘솔에 직접 전달되는 이벤트 소스 또는 플로우 소스를 처리하거나 저장할 수 없습니다. 기존 데이터는 영향을 받지 않습니다. 콘솔 라이센스가 갱신될 때까지 배치에 유효한 라이센스가 있는 관리 호스트에 이벤트 소스를 연결하십시오.
관리 호스트	배치에서 관리 호스트 라이센스가 만료되면 해당 관리 호스트에서 호스트 컨텍스트를 사용하지 않습니다. 만료된 어플라이언스는 이벤트 또는 플로우 데이터를 처리하지 않습니다.
기능	X-Force®와 같은 기능 라이센스가 만료되면 해당 기능에서 데이터 업데이트 수신을 중지합니다. 이 기능은 X-Force에서 제공하는 최신 데이터 스트림에 따라 다릅니다.

시스템 알림이 반복되지 않도록 라이센스 제거

IBM Security QRadar 어플라이언스가 만료되면 해당 라이센스가 업데이트될 때까지 어플라이언스를 사용할 수 없습니다.

이 태스크 정보

X-Force와 같은 기능에 만료된 라이센스가 있는 경우 시스템 알림이 반복되지 않도록 라이센스를 삭제하십시오.

고가용성(HA) 어플라이언스가 있는 경우 보조 HA 호스트 라이센스를 삭제하십시오.

프로시저

1. QRadar Console에 로그인하십시오.
2. **관리** 탭을 클릭하십시오.
3. 탐색 메뉴에서 **시스템 구성**을 클릭하십시오.
4. **시스템 및 라이센스 관리** 아이콘을 클릭하십시오.
5. **표시** 목록 상자에서 **라이센스**를 선택하십시오.

6. 만료된 라이센스를 선택하십시오. **라이센스 정보 메시지**에서 만료된 라이센스를 나열합니다.
7. **조치** > **라이센스 삭제**를 클릭하십시오.
8. **확인**을 클릭하십시오.

다음에 수행할 작업

만료된 라이센스를 업데이트하십시오. 자세한 정보는 라이센스 키 업로드 (http://www.ibm.com/support/knowledgecenter/SS42VS_7.2.7/com.ibm.qradar.doc/t_qradar_adm_upload_license_key.html)를 참조하십시오.

Active Directory 계정을 사용하여 로그인 오류 해결

올바른 Active Directory 계정을 사용하여 IBM Security QRadar에 로그인할 때 오류가 발생하는 경우 시간 동기화 문제가 있는지 확인하십시오.

이 태스크 정보

올바른 Active Directory 계정이 QRadar Console과 동기화되지 않은 경우 다음과 유사한 로그인 오류가 발생할 수 있습니다.

제공한 사용자 이름과 비밀번호가 유효하지 않습니다. 다시 시도하십시오.

QRadar 서버 및 LDAP 인증 서버 간에 수동으로 데이터를 동기화할 수 있습니다.

사용자 속성 또는 그룹을 기반으로 한 권한을 사용하는 경우 LDAP 서버의 사용자 정보를 QRadar 콘솔로 자동으로 가져옵니다.

LDAP 서버에 구성된 각 그룹에는 QRadar 콘솔에 구성된 일치하는 user 역할 또는 보안 프로파일이 있어야 합니다. 일치하는 각 그룹에 대해, 사용자를 가져오고 이 사용자에게 해당 user 역할 또는 보안 프로파일을 기반으로 한 권한이 지정됩니다.

기본적으로 동기화는 24시간마다 수행됩니다. 동기화 시간 지정은 마지막 실행 시간을 기반으로 합니다. 예를 들어, 오후 11시 45분에 동기화를 수동으로 실행하고 동기화 간격을 8시간으로 설정하면 다음 동기화는 오전 7시 45분에 수행됩니다. 동기화될 때 로그인된 사용자의 액세스 권한이 변경되면 세션이 올바르지 않게 됩니다. 그러면 다음 요청 시에 사용자는 로그인 화면으로 경로 재지정됩니다.

다음 단계를 수행하십시오.

프로시저

1. Active Directory를 최근에 구성하지 않은 경우 SSH를 사용하여 root 사용자로 QRadar에 로그인하십시오.
2. 다음 명령을 입력하십시오.

   ```
   cat /opt/qradar/conf/login.conf
   ```

3. 서버가 Active Directory 인증을 위해 구성되었는지 확인하십시오. 예를 들어 인증된 서버는 다음 출력과 유사합니다.

   ```
   LDAPServerURL=ldaps://<server>:<port>
   ```

   <*server*> 옵션은 QRadar 인증을 받는 Active Directory 도메인 컨트롤러입니다. 389는 기본 Active Directory LDAP 포트입니다.
4. Active Directory 도메인 컨트롤러 IP 주소를 복사하십시오.
5. 다음 명령을 입력하고 <*server*> 옵션에 Active Directory 도메인 컨트롤러 IP 주소를 사용하십시오.

   ```
   ntpdate -q <server>
   ```

6. 오프셋 시간이 +/- 300초 이상인지 확인하십시오. 출력은 다음 예제와 유사할 수 있습니다.

   ```
   server 9.24.207.12, stratum 3, offset -10774.586000, delay 0.04221
   19 Nov 13:59:16 ntpdate[22011]: step time server 9.24.207.12 offset
   -10774.586000 sec
   ```

   오프셋 시간이 +/- 300초 이상인 경우 QRadar Console과 Active Directory 서버 간의 시간 간격으로 인해 인증 문제가 발생합니다.
7. 다음 명령을 입력하여 QRadar 웹 서비스를 다시 시작하십시오.

   ```
   systemctl restart tomcat
   ```

   QRadar 웹 서비스를 다시 시작하면 모든 사용자를 로그오프하고 이벤트 내보내기를 중지하며 보고서 생성을 중지합니다. 일부 보고서를 수동으로 다시 시작하거나 유지보수 창에서 이 프로시저가 완료될 때까지 기다려야 할 수 있습니다.
8. QRadar Console 시스템 시간과 Active Directory 서버 시스템 시간이 5분 이상 차이 나는 경우 다음 단계를 수행하십시오.
   a. **관리** 탭을 클릭하십시오.
   b. 탐색 메뉴에서 **시스템 구성**을 클릭하십시오.
   c. **인증**을 클릭하십시오.
   d. **인증 모듈** 목록에서 **LDAP**을 선택하십시오.

e. **동기화 관리** > **지금 동기화 실행**을 클릭하십시오.

QRadar의 syslog 이벤트 수신 확인

IBM Security QRadar가 이벤트를 수신하는지 확인하려면 원격 syslog 소스 이벤트에 대한 전체 syslog 헤더를 검토하십시오. 방화벽이 통신을 차단했거나 디바이스가 이벤트를 보내지 않아서 QRadar가 syslog 이벤트를 받지 못할 수 있습니다.

시작하기 전에

syslog 이벤트를 보내는 이벤트 소스를 검토하고 IP 주소를 확인하십시오.

프로시저

1. SSH를 사용하여 QRadar에 root 사용자로 로그인하십시오.
2. syslog 대상이 이벤트 콜렉터와 같은 다른 어플라이언스에 있는 경우 SSH를 사용하여 이벤트 콜렉터에 로그인하십시오.
3. 다음 옵션 중 하나를 선택하십시오.
   - TCP syslog의 경우 다음 명령을 입력하십시오.

     ```
     tcpdump -s 0 -A host Device_Address and port 514
     ```
   - UDP syslog의 경우 다음 명령을 입력하십시오.

     ```
     tcpdump -s 0 -A host Device_Address and udp port 514
     ```

   *Device_Address*는 IPv4 주소 또는 호스트 이름이어야 합니다. **tcpdump** 명령은 디바이스에서 이벤트를 받는 QRadar 어플라이언스에서 실행해야 합니다. 기본적으로 QRadar 어플라이언스는 TCP 또는 UDP 및 포트 514를 사용하여 syslog 이벤트를 수신하도록 구성되어 있습니다. QRadar 방화벽을 구성하지 마십시오.
4. **tcpdump** 명령이 이벤트를 표시하지 않는 경우 QRadar Console로 syslog 이벤트를 보낼 수 없습니다.
   a. 방화벽 관리자 또는 운영 그룹에 문의하여 QRadar 어플라이언스와 디바이스 간 통신을 차단하는 방화벽을 확인하십시오.
   b. QRadar에서 다음 명령을 입력하여 TCP 포트가 Telnet에 열려 있는지 확인하십시오.

      ```
      telnet Device_IPAddress 514
      ```
   c. 원격 장치의 syslog 구성을 검토하여 이벤트가 적절한 어플라이언스로 전송되는지 확인하십시오.

수신되지 않는 syslog 이벤트 문제 해결

tcpdump 명령이 이벤트를 나열하지만 로그 보기에 이벤트가 표시되지 않는 경우 IBM Security QRadar Console이 syslog 이벤트를 수신하지 못합니다.

프로시저

1. 시스템 알림을 검토하십시오.
2. 시스템 알림에 로그 소스의 잘못된 소스 주소가 표시되면 다음 옵션 중 하나를 선택하십시오.
   - 로그 소스를 수동으로 다시 작성하십시오.
   - 올바른 호스트 이름 또는 IP 주소를 사용하여 **로그 소스 ID** 필드를 업데이트하십시오.
3. 디바이스가 QRadar 자동 감지를 지원하는지 확인하십시오. *IBM Security QRadar DSM* 구성 안내서 부록에서는 자동 로그 소스 작성을 지원하는 디바이스 지원 모듈(DSM)을 나열합니다.
4. QRadar의 로그 소스가 tcpdump 결과와 일치하는지 확인하십시오.
   a. tcpdump 결과에서 로그 소스의 호스트 이름 또는 패킷 IP 주소를 검색하십시오.
   b. **관리** 탭을 클릭하십시오.
   c. 탐색 메뉴에서 **데이터 소스**를 클릭하십시오.
   d. 이벤트 분할창에서 **로그 소스**를 클릭하십시오.
   e. 로그 소스의 호스트 이름 또는 패킷 IP 주소를 검색하십시오.

   QRadar 호스트 이름 또는 패킷 IP 주소가 tcpdump 결과와 일치하지 않으면 로그 소스가 올바르지 않은 주소로 작성될 수 있습니다. 일부 디바이스의 경우, 이벤트 소스가 여러 디바이스의 이벤트를 처리할 때 syslog 헤더에 예기치 않은 값이 발생합니다. syslog 이벤트를 보내기 전에 디바이스가 원래 이벤트 IP 주소를 보존할 수 있습니다.
5. QRadar에서 고유한 페이로드 값을 검색하십시오.
   a. tcpdump 원시 페이 로드를 검토하십시오.
   b. 이벤트 소스에 고유한 ID를 선택하십시오.
   c. **로그 보기** 탭을 클릭하십시오.
   d. 도구 모음에서 **필터 추가**를 클릭하십시오.
   e. **매개변수** 메뉴에서 **페이로드 포함**을 선택하십시오.
   f. **값** 필드에 고유한 ID를 입력하십시오.
   g. 검색 결과를 검토하십시오.

다음에 수행할 작업

결과를 다른 로그 소스를 리턴하는 경우 자동 감지 False Positive 오류가 발생했습니다. 잘못 발견된 로그 소스를 삭제하십시오.

로그 소스가 잘못 발견된 경우 QRadar Console이 최신 DSM 버전으로 설치되었는지 확인하십시오. 로그 소스를 재발견하십시오.

제 2 장 QRadar 시스템 알림

IBM Security QRadar에서 생성되는 시스템 알림을 사용하여 시스템의 상태를 모니터합니다. 소프트웨어 및 하드웨어 도구와 프로세스는 QRadar 어플라이언스를 지속적으로 모니터하여 정보, 경고 및 오류 메시지를 사용자와 관리자에게 전달합니다.

에상치 못한 시스템 동작이 발생하면 시스템 알림이 QRadar 대시보드 또는 알림 창에 표시됩니다. 가장 일반적인 QRadar 알림을 해결할 수 있습니다.

디스크 사용량 시스템 알림

IBM Security QRadar 디스크 센트리는 파티션이 사전정의된 사용량 임계값에 도달하기 전에 /, /store, /storetmp, /transient 및 /var/log 파티션을 모니터합니다.

다음 표에서는 모니터되는 각 파티션의 디스크 사용량에 따른 호스트 컨텍스트 시스템 알림을 표시합니다.

표 3. 디스크 사용량 알림

알림	설명	제안 조치
디스크 센트리: 디스크 사용량이 경고 임계값을 초과했습니다.	디스크 사용량이 모니터되는 파티션의 90%입니다. 파티션이 이 임계값에 도달하면 QRadar는 영향을 받지 않습니다. 파티션 레벨을 계속 모니터하십시오.	18 페이지의 『디스크 사용량이 임계값을 초과함』을 참조하십시오.
디스크 센트리: 디스크 사용량이 최대 임계값을 초과했습니다.	디스크 사용량이 모니터되는 파티션의 95%입니다. 파일 시스템이 100%에 도달하지 않도록 QRadar 데이터 콜렉션 및 검색 프로세스가 종료됩니다.	43 페이지의 『디스크 사용량 경고』을 참조하십시오.
디스크 센트리: 시스템 디스크 사용량이 다시 정상 레벨이 되었습니다.	디스크 사용량이 95%의 임계값에 도달하면 QRadar가 데이터 콜렉션 및 검색 프로세스를 자동으로 다시 시작하기 전에 92%로 돌아가야 합니다.	디스크 사용량 임계값을 낮추려면 영향받는 파티션에서 데이터를 수동으로 제거하십시오. 58 페이지의 『디스크 사용량이 정상으로 돌아옴』을 참조하십시오.

QRadar 어플라이언스에 대한 오류 알림

IBM Security QRadar 제품의 오류 알림에는 사용자 또는 관리자 응답이 필요합니다.

메모리 부족 오류

38750004 - 애플리케이션에 메모리가 부족합니다.

설명

IBM Security QRadar 구성요소가 할당된 양 이상의 메모리를 사용하려고 시도하면 애플리케이션 또는 서비스가 작업을 중지할 수 있습니다. 메모리 부족 문제는 사용 가능한 메모리가 부족한 소프트웨어 또는 사용자 정의 조회 및 조작으로 인해 발생합니다.

사용자 응답

다음 해결 방법을 검토하십시오.

- 실패한 구성요소를 판별하려면 /var/log/qradar.log 파일에 작성된 오류 메시지를 검토하십시오.
- Ariel 프록시 서버가 많은 양의 데이터를 검색하거나 검색 결과에서 고유 값을 생성하는 그룹화 옵션을 사용하는 경우 고유 값의 수를 줄이거나 검색 시간 프레임을 줄이십시오.
- 누산기가 많은 고유 값이 집계된 시계열 그래프를 생성하는 경우, 조회 크기를 줄이십시오.
- 프로토콜 기반 로그 소스가 최근에 사용 가능하도록 설정된 경우, 조회되는 데이터를 줄이기 위해 폴링 기간을 줄이십시오. 다중 프로토콜 기반 로그 소스가 동시에 실행 중인 경우 시작 시간을 엇갈리게 배치하십시오.
- 룰이 최근에 장기간에 걸쳐 고유 특성을 추적하도록 변경된 경우, 시간 프레임을 절반으로 줄이거나 다른 필터를 추가하여 일치하는 이벤트 수를 줄이십시오.

디스크 사용량이 임계값을 초과함

38750038 - 디스크 센트리: 디스크 사용량이 최대 임계값을 초과했습니다.

설명

시스템에서 하나 이상의 디스크가 95% 찼습니다.

시스템의 데이터 손상을 방지하도록 프로세스가 종료되었습니다.

사용자 응답

가득 찬 파티션을 식별하십시오. 예를 들어, / 및 /store 파일 시스템입니다. 필요 없는 파일을 삭제하여 디스크 여유 공간을 만드십시오. 예를 들어, / 파일 시스템에서 디버그 출력 및 패치 파일을 제거하십시오. /store 파일 시스템이 용량에 근접하면 이벤트 및 플로우에 대한 보존 설정을 줄이십시오.

또한 /store/ariel/ 디렉토리에서 이전 데이터를 수동으로 삭제할 수 있습니다. 충분한 디스크 여유 공간을 확보하여 92% 용량 임계값 아래로 떨어지면 시스템이 자동으로 프로세스를 다시 시작합니다.

프로세스 모니터 애플리케이션의 시작이 여러 번 실패함

38750043 - 프로세스 모니터: 애플리케이션 시작이 여러 번 실패했습니다.

설명

시스템의 애플리케이션 또는 프로세스를 시작할 수 없습니다.

사용자 응답

실패한 구성요소를 검토하십시오. 예를 들어, 플로우 소스가 지정되지 않은 경우에는 IBM Security QRadar QFlow Collector 시작이 실패합니다. 배치 조치를 사용하여 해당 QFlow 구성요소를 제거하십시오.

프로세스 모니터가 디스크 사용량을 줄여야 함

38750045 - 프로세스 모니터: 디스크 사용량을 줄여야 합니다.

설명

시스템 자원이 부족하여 프로세스 모니터가 프로세스를 시작할 수 없습니다. 시스템의 스토리지 파티션이 95% 이상 사용 중입니다.

사용자 응답

파일을 수동으로 삭제하거나 이벤트 또는 플로우 데이터 보존 정책을 변경하여 디스크 여유 공간을 확보하십시오. 사용된 디스크 공간이 92% 용량 임계값 아래로 떨어지면 시스템이 자동으로 시스템 프로세스를 다시 시작합니다.

이벤트 파이프라인의 이벤트 제거

38750060 - 이벤트 파이프라인에서 이벤트/플로우를 제거했습니다.

설명

이벤트 파이프라인에 문제가 있거나 라이센스 한계를 초과한 경우, 이벤트나 플로우가 제거될 수 있습니다.

제거된 이벤트와 플로우는 복구할 수 없습니다.

사용자 응답

다음 옵션을 검토하십시오.

- 시스템의 수신 이벤트와 플로우 비율을 검증하십시오. 라이센스가 초과되어 이벤트 파이프라인이 이벤트를 제거하고 있는 경우, 더 많은 데이터를 처리하도록 라이센스를 확장하십시오.
- 룰 또는 사용자 정의 특성에 대한 최신 변경사항을 검토하십시오. 룰이나 사용자 정의 특성을 변경하면 이벤트나 플로우 비율이 변경되어 시스템 성능에 영향을 줄 수 있습니다.
- 문제가 SAR 알림에 연관되어 있는지 판별하십시오. SAR 알림이 큐에 대기된 이벤트 및 플로우가 이벤트 파이프라인에 있음을 표시할 수 있습니다. 시스템은 일반적으로 이벤트를 제거하는 대신 이벤트를 스토리지로 라우팅합니다.
- 시스템을 튜닝하여 이벤트 파이프라인에 들어가는 이벤트 및 플로우 볼륨을 줄이십시오.

이벤트 파이프라인의 연결 제거

38750061 - 이벤트 파이프라인에 의해 연결이 끊어졌습니다.

설명

TCP 기반 프로토콜이 시스템에 설정된 연결을 제거했습니다.

연결을 설정하고 이벤트를 전달할 수 있도록 TCP 기반 프로토콜에서 설정할 수 있는 연결 수가 제한됩니다. 이벤트 콜렉션 서비스(ECS)를 사용하면 최대 15,000 개의 파일 핸들이 허용되며 각 TCP 연결은 세 개의 파일 핸들을 사용합니다.

연결 제거 알림을 제공하는 TCP 프로토콜에는 다음 프로토콜이 포함됩니다.

- TCP syslog 프로토콜
- TLS syslog 프로토콜
- TCP 다중 행 프로토콜

사용자 응답

다음 옵션을 검토하십시오.

- 이벤트를 추가 어플라이언스에 분배하십시오. 다른 이벤트 및 플로우 프로세서에 대한 연결이 콘솔의 워크로드를 분배합니다.
- UDP 네트워크 프로토콜을 사용하도록 낮은 우선순위의 TCP 로그 소스 이벤트를 구성하십시오.
- 시스템을 튜닝하여 이벤트 파이프라인에 들어가는 이벤트 및 플로우 볼륨을 줄이십시오.

자동 업데이트 오류

38750066 - 자동 업데이트가 설치를 완료할 수 없습니다. 자세한 정보는 자동 업데이트 로그를 참조하십시오.

설명

업데이트 프로세스에서 오류가 발생했거나 업데이트 서버에 연결할 수 없습니다. 시스템이 업데이트되지 않습니다.

사용자 응답

다음 옵션 중 하나를 선택하십시오.

- 자동 업데이트 히스토리를 검증하여 설치 오류의 원인을 판별하십시오.

  관리 탭에서 **자동 업데이트** 아이콘을 클릭하여 **로그 보기**를 선택하십시오.
- 콘솔이 업데이트 서버에 연결할 수 있는지 확인하십시오.

  업데이트 창에서 **설정 변경**을 선택하고 **고급** 탭을 클릭하여 자동 업데이트 구성을 확인하십시오. **웹 서버** 필드의 주소를 검증하여 자동 업데이트 서버에 액세스할 수 있는지 확인하십시오.

자동 업데이트 설치 시 오류 발생

38750067 - 자동 업데이트가 설치되었지만 오류가 있습니다. 자세한 정보는 자동 업데이트 로그를 참조하십시오.

설명

가장 일반적인 자동 업데이트 오류 원인은 DSM, 프로토콜 또는 스캐너 업데이트에 대한 소프트웨어 종속성이 누락된 경우입니다.

사용자 응답

다음 옵션 중 하나를 선택하십시오.

- **관리** 탭에서 **자동 업데이트** 아이콘을 클릭하고 **업데이트 히스토리 보기**를 선택하여 설치 오류의 원인을 판별할 수 있습니다. 실패한 RPM을 보고 선택한 다음 다시 설치할 수 있습니다.
- 자동 업데이트가 사용자 인터페이스를 통해 재설치할 수 없는 경우 콘솔에서 누락된 종속성을 수동으로 다운로드하여 설치하십시오. 콘솔이 설치된 파일을 모든 관리 호스트로 복제합니다.

스탠바이 고가용성(HA) 시스템 실패

38750080 - 스탠바이 HA 시스템 실패입니다.

설명

보조 어플라이언스의 상태가 실패로 전환되고 시스템에 HA 보호가 실행되지 않습니다.

사용자 응답

다음 해결 방법을 검토하십시오.

- 보조 시스템을 복원하십시오.

  관리 탭을 클릭하고 **시스템 및 라이센스 관리**를 클릭한 다음 **시스템 복원**을 클릭하십시오.
- 보조 HA 어플라이언스를 검사하여 전원이 꺼져있는지 또는 하드웨어 장애가 있는지 판별하십시오.
- **ping** 명령을 사용하여 기본 시스템과 스탠바이 시스템 사이의 통신을 검사하십시오.
- 기본 및 보조 HA 어플라이언스를 연결하는 스위치를 검사하십시오.

  기본 및 보조 어플라이언스의 IPtables를 검증하십시오.
- 스탠바이 어플라이언스의 /var/log/qradar.log 파일을 검토하여 실패의 원인을 판별하십시오.

활성 고가용성(HA) 시스템 실패

38750081 - 활성 HA 시스템 실패입니다.

설명

활성 시스템이 응답하지 않거나 실패하여 스탠바이 시스템과 통신할 수 없습니다. 스탠바이 시스템은 실패한 활성 시스템에서 조작을 이어 받습니다.

사용자 응답

다음 해결 방법을 검토하십시오.

- 활성 HA 어플라이언스를 검사하여 전원이 꺼져있는지 또는 하드웨어 장애가 있는지 판별하십시오.
- 활성 시스템이 기본 HA인 경우 활성 시스템을 복원하십시오.

  관리 탭을 클릭하고 **시스템 및 라이센스 관리**를 클릭하십시오. **고가용성** 메뉴에서 **시스템 복원** 옵션을 선택하십시오.
- 스탠바이 어플라이언스의 /var/log/qradar.log 파일을 검토하여 실패의 원인을 판별하십시오.

- **ping** 명령을 사용하여 활성 시스템과 스탠바이 시스템 사이의 통신을 검사하십시오.
- 활성 및 스탠바이 HA 어플라이언스를 연결하는 스위치를 검사하십시오.

  활성 및 스탠바이 어플라이언스의 IPtables를 검증하십시오.

고가용성 설치 실패

38750086 - 클러스터의 고가용성 설치 시 문제가 발생했습니다.

설명

고가용성(HA) 어플라이언스를 설치할 때 설치 프로세스가 기본 및 보조 어플라이언스를 연결합니다. 구성 및 설치 프로세스에는 설치 시 주의가 필요한 시점을 판별하는 시간 간격이 포함되어 있습니다. 고가용성 설치가 6시간 제한을 초과했습니다.

문제가 해결될 때까지 HA 보호를 사용할 수 없습니다.

사용자 응답

고객 지원에 문의하십시오.

고가용성(HA) 어플라이언스 설치 제거 실패

OT38750087 - 클러스터의 고가용성을 제거하는 동안 문제가 발생했습니다.

설명

HA 어플라이언스를 제거할 때 설치 프로세스가 기본 및 보조 어플라이언스 간의 연결과 데이터 복제를 제거합니다. 설치 프로세스가 클러스터에서 HA 어플라이언스를 제거할 수 없는 경우, 기본 시스템이 계속 정상적으로 작동합니다.

사용자 응답

고가용성 어플라이언스를 두 번째로 제거해 보십시오.

스캐너 초기화 오류

38750089 - 스캐너를 초기화하는 데 실패했습니다.

설명

스케줄된 취약성 스캔이 외부 스캐너에 연결하여 스캔 가져오기 프로세스를 시작할 수 없습니다.

스캔 초기화 문제는 일반적으로 원격 스캐너에 대한 연결이나 신임 정보에 문제가 있어서 발생합니다. 스캐너의 초기화에 실패하면 실패한 상태의 스케줄된 스

캔에서 풍선 텍스트로 자세한 오류 메시지가 표시됩니다.

사용자 응답

다음 단계를 수행하십시오.

1. **관리** 탭을 클릭하십시오.
2. 탐색 메뉴에서 **데이터 소스**를 클릭하십시오.
3. **VA 스캐너 스케줄** 아이콘을 클릭하십시오.
4. 스캐너 목록에서 스캐너의 **상태** 컬럼에 마우스 커서를 놓아서 자세한 성공 또는 실패 메시지를 표시하십시오.

스캔 실패 오류

38750090 - 스캐너가 실패했습니다.

설명

스케줄된 취약성 스캔에서 취약성 데이터를 가져오는 데 실패했습니다. 스캔 실패의 원인은 일반적으로 가져오는 데이터의 볼륨이 커서 초래되는 구성 또는 성능 문제입니다. 스캔 실패는 시스템에서 다운로드한 스캔 보고서가 읽을 수 없는 형식인 경우에도 발생합니다.

사용자 응답

다음 단계를 수행하십시오.

1. **관리** 탭을 클릭하십시오.
2. 탐색 메뉴에서 **데이터 소스**를 클릭하십시오.
3. **VA 스캐너 스케줄**을 클릭하십시오.
4. 스캐너 목록에서 스캐너의 **상태** 컬럼에 마우스 커서를 놓아서 자세한 성공 또는 실패 메시지를 표시하십시오.

필터 초기화 실패

38750091 - 트래픽 분석 필터를 초기화하는 데 실패했습니다.

설명

구성이 올바르게 저장되지 않았거나 구성 파일이 손상된 경우, 이벤트 콜렉션 서비스(ECS)의 초기화가 실패할 수 있습니다. 트래픽 분석 프로세스가 시작되지 않은 경우, 새 로그 소스가 자동으로 감지됩니다.

사용자 응답

다음 옵션 중 하나를 선택하십시오.

- 새로운 어플라이언스 또는 이벤트 소스에 대해 로그 소스를 수동으로 작성하십시오. 트래픽 분석 프로세스가 작동하기 시작할 때까지 이를 수동으로 작성하십시오.

  모든 새 이벤트 소스는 로그 소스에 맵핑될 때까지 SIM Generic으로 분류됩니다.
- 자동 업데이트 오류를 수신한 경우, 자동 업데이트 로그를 검토하여 DSM을 설치할 때 오류가 발생했는지 프로토콜을 설치할 때 오류가 발생했는지 판별하십시오.

디스크 스토리지 사용 불가능

38750092 - 디스크 센트리가 하나 이상의 스토리지 파티션에 액세스할 수 없음을 발견했습니다.

설명

디스크 센트리가 30초 내에 응답을 수신하지 못했습니다. 스토리지 파티션에 문제가 있거나 시스템 로드가 너무 많아서 30초 임계값 내에 응답을 수신하지 못한 것일 수 있습니다.

사용자 응답

다음 옵션 중 하나를 선택하십시오.

- **touch** 명령을 사용하여 /store 파티션의 상태를 검증하십시오.

시스템이 **touch** 명령에 응답하면 시스템 로드 문제가 있어 디스크 스토리지를 사용할 수 없는 경우입니다.

- 알림이 삭제된 이벤트에 해당하는지 확인하십시오.

IBM Security QRadar에서는 이벤트를 디스크에 쓸 수 없는 경우 이벤트를 삭제합니다. 스토리지 파티션의 상태를 확인하십시오.

관련 개념:

58 페이지의 『디스크 스토리지 사용 가능』

38750093 - 이전에 액세스 불가능한 하나 이상의 스토리지 파티션이 현재 액세스 가능합니다.

디스크 공간이 부족하여 데이터를 내보낼 수 없음

38750096 - 데이터 내보내기 요청을 완료하기에 디스크 공간이 충분하지 않습니다.

설명

내보내기 디렉토리에 공간이 부족한 경우 이벤트, 플로우 및 오펜스 데이터의 내보내기가 취소됩니다.

사용자 응답

다음 옵션 중 하나를 선택하십시오.

- /store/exports 디렉토리에서 여유 디스크 공간을 확보하십시오.
- 시스템 설정 창의 **내보내기 디렉토리** 특성을 구성하여 충분한 디스크 공간이 있는 파티션을 사용하십시오.
- 오프보드 스토리지 디바이스를 구성하십시오.

누산기 속도 감소

38750099 - 누산기가 이 간격 동안의 모든 이벤트/플로우를 집계할 수 없습니다.

설명

이 메시지는 시스템이 60초 간격 이내에 데이터 집계를 누적할 수 없는 경우에 표시됩니다.

QRadar는 매분 각 집계된 검색의 데이터 집계를 작성합니다. 데이터 집계는 시계열 그래프와 보고서에 사용되며 60초 간격 이내에 완료되어야 합니다. 검색 수 및 검색의 고유 값이 너무 큰 경우 집계를 처리하는 데 필요한 시간이 60초를 초과할 수 있습니다. 문제가 발생하면 시계열 그래프 및 보고서에 기간에 대한 컬럼이 누락될 수 있습니다.

이 문제가 발생할 때 데이터가 유실되지 않습니다. 모든 원시 데이터와 이벤트 및 플로우가 계속 디스크에 쓰여집니다. 저장된 데이터에서 생성되는 데이터 세트인 누적의 경우에만 완료되지 않습니다.

사용자 응답

다음과 같은 요인으로 인해 워크로드가 증가하여 누산기가 지체될 수 있습니다.

완료되지 않은 누적 빈도

누적이 하루에 한 번 또는 두 번만 실패하는 경우 대량 검색, 데이터 압축 주기 또는 데이터 백업에 따른 시스템 로드의 증가로 인해 삭제가 발생할 수 있습니다.

빈번하지 않게 실패하는 경우는 무시할 수 있습니다. 하루의 모든 시간 중에 여러 번 실패가 발생하는 경우 더 조사할 수 있습니다.

높은 시스템 로드

다른 프로세스에서 여러 시스템 자원을 사용하는 경우 증가된 시스템 로

드로 인해 집계 속도가 느려질 수 있습니다. 증가된 시스템 로드의 원인을 검토하고 가능하면 원인을 해결하십시오.

예를 들어, 완료하는 데 시간이 오래 걸리는 대량 데이터 검색을 수행하는 동안 집계 실패가 발생하는 경우 저장된 검색의 크기를 줄여 누산기 삭제를 방지할 수 있습니다.

대량 누산기 요구

누산기 간격이 규칙적으로 삭제되는 경우 워크로드를 줄일 필요가 있습니다.

누산기의 워크로드는 집계 수 및 해당 집계의 고유 오브젝트 수에 따라 좌우됩니다. 집계에 포함된 고유 오브젝트 수는 검색에 적용된 필터 및 그룹별 매개변수에 따라 달라집니다.

예를 들어 서비스를 집계하는 검색은 DMZ 영역과 같은 로컬 네트워크 계층 구조 항목을 사용하여 데이터를 필터링합니다. IP 주소별 그룹화 결과는 고유 오브젝트를 200개까지 포함할 수 있습니다. 검색에 대상 포트를 추가하고 각 서버가 서로 다른 포트에서 5 - 10개의 서비스를 호스팅하는 경우, `destination.ip + destination.port`의 새 집계는 고유 오브젝트 수를 2000으로 증가시킬 수 있습니다. 집계에 소스 IP 주소를 추가하고 각 서비스를 히트하는 원격 IP 주소가 수천 개인 경우 집계된 보기에는 수십만 개의 고유 값이 포함될 수 있습니다. 이러한 검색은 누산기에 과중한 요구를 생성할 수 있습니다.

누산기에 과중한 요구를 부과하는 집계된 보기를 검토하려면 다음을 수행하십시오.

1. **관리** 탭에서 **집계된 데이터 관리**를 클릭하십시오.
2. 데이터를 내림차순으로 정렬하고 최대 보기를 표시하려면 **작성한 데이터** 컬럼을 클릭하십시오.
3. 계속 필요한지 여부를 보려면 각 최대 집계에 대한 비즈니스 케이스를 검토하십시오.

관련 개념:

8 페이지의 『불완전한 보고서 결과』

IBM Security QRadar 보고서를 구성하고 실행하면 예기치 않은 결과를 볼 수 있습니다. 보고서에 필요한 모든 데이터가 표시되지 않는 것처럼 보일 수 있습니다.

CRE가 룰 읽기에 실패함

38750107 - 룰에서 마지막 읽기 시도가 실패했습니다(일반적으로 룰 변경으로 인해). 이를 해결하는 방법에 대한 정보는 메시지 세부사항과 오류 로그를 참조하십시오.

설명

이벤트 프로세서의 사용자 정의 룰 엔진(CRE)이 룰을 읽어서 수신 이벤트를 연관시키는 룰을 읽을 수 없습니다. 알림에는 다음 메시지 중 하나가 포함될 수 있습니다.

- CRE가 단일 룰을 읽을 수 없는 경우, 대부분은 최근에 룰을 변경한 것이 원인입니다. 알림 메시지의 페이로드는 책임이 있는 룰 또는 룰의 룰 체인을 표시합니다.
- 드문 경우, 데이터가 손상되어 룰 세트가 완전히 실패할 수 있습니다. 애플리케이션 오류가 표시되며 룰 편집기 인터페이스가 응답하지 않거나 오류가 추가로 발생할 수 있습니다.

사용자 응답

단일 룰 읽기 오류의 경우, 다음 옵션을 검토하십시오.

- 알림이 발생한 원인이 되는 룰을 찾으려면 룰을 임시로 사용하지 않도록 설정하십시오.
- 룰을 편집하여 최근 변경사항을 되돌리십시오.
- 오류를 발생시킨 룰을 삭제하고 다시 작성하십시오.

CRE가 룰을 읽는 데 실패한 애플리케이션 오류의 경우 고객 지원에 문의하십시오.

누산기가 집계 데이터의 정의를 읽거나 볼 수 없음

38750108 - 누산기: 집계된 데이터 보기 정의를 읽을 수 없어서 동기화 문제를 예방할 수 없습니다. 더 이상 집계된 데이터 보기를 작성하거나 로드할 수 없습니다. 시계열 그래프가 작동하지 않으며 보고하지 않습니다.

설명

동기화 문제가 발생했습니다. 메모리에 있는 데이터 집계 보기 구성이 잘못된 데이터를 데이터베이스에 작성했습니다.

데이터 손상을 방지하기 위해 시스템은 집계 데이터 보기를 사용하지 않습니다. 집계 데이터 보기를 사용하지 않으면 시계열 그래프, 저장된 검색 및 스케줄된 보고서가 비어 있는 그래프를 표시합니다.

사용자 응답

고객 지원에 문의하십시오.

저장 및 전달 스케줄에서 모든 이벤트를 전달하지 않음

38750109 - 디스크에 이벤트가 남아 있는 동안 저장 및 전달 스케줄이 완료되었습니다. 이러한 이벤트는 다음 전달 세션이 시작될 때까지 로컬 이벤트 콜렉터에 저장됩니다.

설명

스케줄에 짧은 시작 및 종료 시간이 포함되어 있거나 전달할 이벤트가 많은 경우 이벤트 콜렉터에 큐 대기된 이벤트를 전송할 시간이 충분하지 않을 수 있습니다. 이벤트는 다음에 이벤트를 전달할 때까지 저장됩니다. 다음 저장 및 전달 간격이 발생하는 경우 이벤트 프로세서에 이벤트가 전달됩니다.

사용자 응답

이벤트 콜렉터에서 이벤트 전달률을 늘리거나 이벤트 전달에 대해 구성되는 시간 간격을 늘리십시오.

디스크 실패

38750110 - 디스크 실패: 하드웨어 모니터링에서 디스크가 실패 상태에 있음을 확인했습니다.

설명

온보드 시스템 도구가 실패한 디스크를 발견했습니다. 알림 메시지는 실패한 디스크 및 장애가 있는 슬롯 또는 베이 위치에 대한 정보를 제공합니다.

사용자 응답

알림이 지속되면 고객 지원에 문의하거나 부품을 교체하십시오.

예측 디스크 실패

38750111 - 예측 디스크 실패: 하드웨어 모니터링에서 디스크가 예측 실패 상태에 있음을 확인했습니다.

설명

시스템이 시간별로 하드웨어 상태를 모니터하여 언제 어플라이언스에서 하드웨어 지원이 필요한지 판별합니다.

온보드 시스템 도구가 디스크 장애나 수명 종료 위험이 있음을 발견했습니다. 실패한 슬롯 또는 베이 위치가 식별되었습니다.

사용자 응답

예측 실패 상태인 디스크의 유지보수를 스케줄하십시오.

스캔 도구 실패

38750118 - 스캔이 예기치 않게 중지되었으며 이로 인해 스캔이 중지될 수 있습니다.

설명

시스템이 취약성 스캔을 초기화할 수 없으며 외부 스캐너에서 자산 스캔 결과를 가져올 수 없습니다. 스캔 도구가 예기치 않게 종료되는 경우, 시스템이 외부 스캐너와 통신할 수 없습니다. 시스템이 30초 간격으로 5번 외부 스캐너에 연결을 시도합니다.

드문 경우, 감지 도구에 테스트되지 않은 호스트 또는 네트워크 구성이 발생할 수 있습니다.

사용자 응답

다음 옵션 중 하나를 선택하십시오.

- 배치 편집기의 외부 스캐너에 대한 구성을 검토하여 게이트웨이 IP 주소가 올바른지 확인하십시오.
- 외부 스캐너가 구성된 IP 주소를 통해 통신할 수 있는지 확인하십시오.
- DMZ에 대한 방화벽 룰이 어플라이언스와 스캔하려는 자산 간의 통신을 차단하고 있지는 않는지 확인하십시오.

외부 스캔 게이트웨이 실패

38750119 - 유효하지 않거나 알 수 없는 게이트웨이 IP 주소가 외부 호스트 스캐너에 제공되어 스캔이 중지되었습니다.

설명

외부 스캐너가 추가된 경우, 게이트웨이 IP 주소가 필요합니다. 배치 편집기에서 스캐너에 대해 구성된 주소가 올바르지 않은 경우, 스캐너가 외부 네트워크에 액세스할 수 없습니다.

사용자 응답

다음 옵션 중 하나를 선택하십시오.

- 배치 편집기에 구성된 외부 스캐너에 대한 구성을 검토하여 게이트웨이 IP 주소가 올바른지 확인하십시오.
- 외부 스캐너가 구성된 IP 주소를 통해 통신할 수 있는지 확인하십시오.
- DMZ에 대한 방화벽 룰이 어플라이언스와 스캔하려는 자산 간의 통신을 차단하고 있지는 않는지 확인하십시오.

자동 업데이트에 대해 사용자 인증 실패

38750127 - 자동 업데이트 사용자 인증에 실패했습니다. 유효한 개인 IBM ID가 필요합니다.

설명

업데이트 서버에서 자동 다운로드 권한을 부여하려면 유효한 신임 정보가 필요합니다.

사용자 응답

다음 옵션 중 하나를 선택하십시오.

- 관리자는 IBM 지원 센터 웹 사이트(http://www.ibm.com/support/)에서 계정을 등록해야 합니다.
- 자동 업데이트 설정을 보려면 **관리** 탭에서 **자동 업데이트** 아이콘을 클릭하고 **설정 변경** > **고급**을 선택하십시오. 관리자는 설정 창의 사용자 이름 및 비밀번호가 올바른지 확인할 수 있습니다.

집계된 데이터 한계에 도달함

38750130 - 집계 한계로 인해 집계된 데이터 보기를 작성할 수 없었습니다.

설명

누산기는 검색, 차트 표시 및 성능 보고를 지원하기 위해 데이터 누적에서 이벤트 및 플로우를 계수하고 준비하는 QRadar 프로세스입니다. 누산기 프로세스는 데이터 집계 보기를 작성하기 위해 사전정의된 시간 범위 내에서 데이터를 집계하는 프로세스입니다. 데이터 집계 보기는 시계열 그래프를 그리거나 스케줄된 보고서를 작성하거나 비정상 발견 룰을 트리거하는 데 사용되는 데이터 세트입니다.

콘솔은 130개의 활성 데이터 집계 보기로 제한됩니다.

다음 사용자 조치는 새 데이터 집계 보기를 작성할 수 있습니다.

- 새 비정상 발견 룰.
- 새 보고서.
- 시계열 데이터를 사용하는 새로 저장된 검색.

데이터 집계 보기 제한에 도달하면 알림이 생성됩니다. 사용자가 새 비정상 룰을 작성하거나 검색을 저장하려고 시도하면 사용자 인터페이스에 시스템이 한계에 도달했음이 프롬프트됩니다.

사용자 응답

이 문제를 해결하기 위해 관리자가 **집계된 데이터 관리** 창의 **관리** 탭에서 활성 데이터 집계 보기를 검토할 수 있습니다. 집계된 데이터 관리 기능은 각 데이터 집계 보기에서 사용되는 보고서, 검색 및 비정상 발견 룰에 대한 정보를 제공합니다. 관리자는 데이터 집계 보기의 목록을 검토하여 사용자에게 가장 중요한 정보를 판별할 수 있습니다. 사용자가 데이터 집계 보기가 필요한 새 룰, 보고서 또는 저장된 검색을 작성할 수 있도록 허용하기 위해 데이터 집계 보기를 사용하지 않도록 설정할 수 있습니다.

관리자가 데이터 집계 보기를 삭제하기로 판단하면 요약에서 영향을 받는 검색, 룰, 보고서에 대한 아웃라인이 제공됩니다. 관리자는 검색, 비정상 룰 또는 보고서를 다시 사용으로 설정하거나 다시 작성하기만 하면 삭제된 데이터 집계 보기를 다시 작성할 수 있습니다. 시스템이 필요한 데이터를 기반으로 하여 데이터 집계 보기를 자동으로 작성합니다.

치안 판사가 오펜스 업데이트를 지속할 수 없음

38750147 - 치안 판사에 오펜스 업데이트를 방해할 수 있는 심각한 오류가 발생했습니다.

설명

데이터베이스에 오펜스 업데이트를 작성할 때 시스템에서 예외를 발견했습니다.

이벤트가 처리되어 저장되지만 오펜스를 수행할 수 없습니다.

사용자 응답

오펜스 비활성화를 선택하지 않은 상태로 SIM 데이터 모델의 소프트 정리를 수행하십시오.

1. **관리** 탭을 클릭하십시오.
2. 도구 모음에서 **고급** > **SIM 모델 정리**를 클릭하십시오.
3. **소프트 정리**를 클릭하여 오펜스를 비활성으로 설정하십시오.
4. **오펜스 비활성화**가 선택되지 않았는지 확인하십시오.
5. **데이터 모델을 재설정하시겠습니까?** 선택란을 클릭하고 **계속**을 클릭하십시오.

SIM 모델을 정리하면 기존 오펜스가 모두 닫힙니다. SIM 모델 정리는 기존 이벤트와 플로우에 영향을 미치지 않습니다.

QRadar 어플라이언스에 대한 경고 알림

IBM Security QRadar 시스템 상태 알림은 실제 또는 임박한 소프트웨어 또는 하드웨어 장애에 대한 사전 예방적 메시지입니다.

최대 센서 디바이스 수 모니터

38750006 - 트래픽 분석이 최대 로그 소스 수를 모니터하고 있습니다.

설명

시스템에 트래픽 분석에서 자동 감지하도록 큐에 대기할 수 있는 로그 소스 수에 대한 한계가 있습니다. 큐에 허용되는 최대 로그 소스 개수에 도달한 경우, 새 로그 소스를 추가할 수 없습니다.

로그 소스에 대한 이벤트는 SIM Generic으로 분류되며 알 수 없는 이벤트 로그로 레이블이 지정됩니다.

사용자 응답

다음 옵션 중 하나를 선택하십시오.

- **로그 보기** 탭에서 SIM Generic 로그 소스를 검토하여 이벤트 페이로드의 어플라이언스 유형을 판별하십시오.
- 자동 업데이트가 최신 DSM 업데이트를 다운로드하여 로그 소스 이벤트를 올바르게 식별하고 구문 분석할 수 있는지 확인하십시오.
- 로그 소스가 공식적으로 지원되는지 검증하십시오.

  어플라이언스가 지원되는 경우, 자동으로 감지되지 않은 이벤트의 로그 소스를 수동으로 작성하십시오.
- 어플라이언스가 공식적으로 지원되지 않는 경우, Universal DSM을 작성하여 이벤트를 식별하고 분류하십시오.
- 디바이스가 1,000개의 이벤트를 제공할 때까지 대기하십시오.

  1,000개의 이벤트 이후에 시스템이 로그 소스를 자동으로 감지할 수 없는 경우, 트래픽 분석 큐에서 제거된 것입니다. 다른 로그 소스가 자동으로 감지될 수 있도록 공간이 제공됩니다.

연관된 로그 소스를 판별할 수 없음

38750007 - IP 주소 <*IP* 주소>의 연관된 로그 소스를 자동으로 발견할 수 없습니다. IP 주소의 연관된 로그 소스를 자동으로 발견할 수 없습니다.

설명

이벤트가 감지되지 않거나 인식되지 않는 디바이스로부터 전송되는 경우 트래픽 분석 구성요소는 로그 소스를 식별하기 위해 최소 25개의 이벤트가 필요합니다.

1,000개의 이벤트 후에 로그 소스가 식별되지 않는 경우 시스템은 자동 감지 프로세스를 포기하고 시스템 알림을 생성합니다. 그런 다음 시스템은 로그 소스를 SIM Generic으로 분류하고 이벤트 레이블을 알 수 없는 이벤트 로그로 지정합니다.

사용자 응답

다음 옵션을 검토하십시오.

- 시스템 알림에서 IP 주소를 검토하여 로그 소스를 식별하십시오.
- **로그 보기** 탭을 검토하여 알림 메시지의 IP 주소에서 애플리케이션 유형을 판별한 다음 로그 소스를 수동으로 작성하십시오.

  로그 소스 ID 필드가 원래 페이로드 syslog 헤더의 호스트 이름과 일치하는지 확인하십시오. 변경사항을 배치하고 수동으로 작성된 로그 소스에서 검색하여 이벤트가 디바이스에 표시되는지 확인하십시오.
- 낮은 이벤트 비율로 전달하는 로그 소스를 모두 검토하십시오. 이 알림은 일반적으로 이벤트 비율이 낮은 로그 소스로 인해 발생됩니다.
- 시스템의 이벤트를 적절히 구문 분석하려면 자동 업데이트가 최신 DMS를 다운로드해야 합니다.
- 중앙 로그 서버를 통해 이벤트를 제공하는 로그 소스를 검토하십시오. 중앙 로그 서버 또는 관리 콘솔에서 제공하는 로그 소스의 경우 해당 로그 소스를 수동으로 작성해야 합니다.
- 로그 소스가 공식적으로 지원되는지 검증하십시오. 어플라이언스가 지원되는 경우 이벤트의 로그 소스를 수동으로 작성하고 로그 소스 확장을 추가하십시오.
- 어플라이언스가 공식적으로 지원되지 않는 경우, Universal DSM을 작성하여 이벤트를 식별하고 분류하십시오.

최대 이벤트 수 또는 플로우 수 도달

38750008 - 어플라이언스가 지난 한 시간 내에 EPS 또는 FPM 할당을 초과했습니다.

설명

각 어플라이언스에는 라이센스 풀의 플로우 데이터와 특정 이벤트 볼륨이 할당됩니다. 지난 한 시간 내에 어플라이언스가 할당된 EPS 또는 FPM을 초과했습니다.

어플라이언스가 할당된 용량을 계속 초과하면 시스템은 이벤트와 플로우를 큐에 넣거나 백업 큐가 가득 찬 경우 데이터를 삭제할 수도 있습니다.

사용자 응답

- 라이센스 풀 할당을 조정하여 어플라이언스의 EPS 및 FPM 용량을 늘리십시오.
- 시스템을 튜닝하여 이벤트 파이프라인에 들어가는 이벤트 및 플로우 볼륨을 줄이십시오.

플로우 콜렉터가 초기 시간 동기화를 설정할 수 없음

38750009 - 플로우 콜렉터가 초기 시간 동기화를 설정할 수 없습니다.

설명

IBM Security QRadar QFlow Collector 프로세스에는 시간 동기화용 서버 IP 주소를 구성하는 데 필요한 고급 기능이 포함되어 있습니다. 대부분은 값을 구성하지 않습니다. 구성하는 경우, QFlow 프로세스가 IP 주소 시간 서버를 사용하여 매시간 시간을 동기화합니다.

사용자 응답

배치 조치에서 QFlow 프로세스를 선택하십시오. **조치** > **구성**을 클릭하고 **고급**을 클릭하십시오. **시간 동기화 서버 IP 주소** 필드에서 값을 지우고 **저장**을 클릭하십시오.

백업이 요청을 완료할 수 없음

38750033 - 백업: 백업을 수행하기에 디스크 여유 공간이 부족합니다.

설명

디스크 센트리는 시스템 디스크 및 스토리지 문제의 모니터링을 담당합니다. 백업이 시작되기 전에 디스크 센트리는 사용 가능한 디스크 공간을 확인하여 백업이 제대로 완료될 수 있는지를 판별합니다. 디스크 여유 공간이 마지막 백업 크기의 두 배보다 작은 경우 백업이 취소됩니다. 기본적으로 백업은 /store/backup에 저장됩니다.

사용자 응답

이 문제를 해결하려면 다음 옵션 중 하나를 선택하십시오.

- 어플라이언스의 디스크 여유 공간을 확보하여 /store/backup에서 백업을 완료할 공간을 충분히 허용하십시오.
- 디스크 여유 공간이 있는 파티션을 사용하도록 기존 백업을 구성하십시오.

- 어플라이언스에 대해 추가 스토리지를 구성하십시오. 자세한 정보는 오프보드 스토리지 안내서를 참조하십시오.

백업 요청을 실행할 수 없음

38750035 - 백업: 백업 요청을 수행할 수 없습니다.

설명

다음 이유 중 하나로 인해 백업을 시작하거나 완료할 수 없습니다.

- 시스템이 백업 복제 동기화 테이블을 정리할 수 없습니다.
- 시스템이 삭제 요청을 실행할 수 없습니다.
- 시스템이 디스크에 있는 파일을 사용하여 백업을 동기화할 수 없습니다.
- NFS 마운트 백업 디렉토리를 사용할 수 없거나 올바르지 않은 NFS 내보내기 옵션(no_root_squash)이 있습니다.
- 시스템이 On Demand 백업을 초기화할 수 없습니다.
- 시스템이 선택한 백업 유형의 구성을 검색할 수 없습니다.
- 스케줄된 백업을 초기화할 수 없습니다.

사용자 응답

백업을 수동으로 시작하여 실패가 다시 발생하는지 확인하십시오. 백업 시작 실패가 여러 번 발생하면 고객 지원에 문의하십시오.

프로세스 모니터 라이센스가 만료되었거나 올바르지 않음

38750044 - 프로세스 모니터: 프로세스를 시작할 수 없음: 라이센스가 만료되었거나 올바르지 않습니다.

설명

관리 호스트에 대한 라이센스가 만료되었습니다. 어플라이언스에서 모든 데이터 콜렉션 프로세스가 중지되었습니다.

사용자 응답

영업 담당자에게 문의하여 라이센스를 갱신하십시오.

긴 트랜잭션을 발생시키는 관리되지 않는 프로세스 발견

38750048 - 트랜잭션 센트리: 긴 트랜잭션을 발생시켜 시스템 안정성을 낮추는 관리되지 않는 프로세스를 발견했습니다.

설명

트랜잭션 센트리가 외부 프로세스(예: 데이터베이스 복제 실행, 유지보수 스크립트, 자동 업데이트, 명령행 프로세스) 또는 트랜잭션이 데이터베이스 잠금을 발생시키는 것을 판별했습니다. 대부분의 프로세스가 한 시간 넘게 실행될 수 없습니다. 동일한 프로세스가 반복하여 발생하는 경우 조사가 필요합니다.

사용자 응답

다음 옵션 중 하나를 선택하십시오.

- /var/log/qradar.log 파일에서 단어 TxSentry를 검토하여 트랜잭션 문제의 원인이 되는 프로세스 ID를 판별하십시오.
- 대기하여 프로세스가 트랜잭션을 완료하고 데이터베이스 잠금을 해제하는지 검토하십시오.
- 프로세스 ID를 다시 시작하여 수동으로 데이터베이스 잠금을 해제하십시오.

정지된 트랜잭션을 취소하여 시스템 상태 복원

38750049 - 트랜잭션 센트리: 정지된 트랜잭션 또는 교착 상태를 취소하여 시스템 상태를 복원했습니다.

설명

트랜잭션 센트리가 일시중단된 데이터베이스 트랜잭션을 취소하거나 데이터베이스 잠금을 제거하여 시스템 상태를 정상으로 복원했습니다. 오류의 원인이 된 프로세스를 판별하려면 qradar.log 파일에서 단어 TxSentry를 검토하십시오.

사용자 응답

조치가 필요하지 않습니다.

최대 활성 오펜스 도달

38750050 - MPC: 새 오펜스를 작성할 수 없습니다. 최대 활성 오펜스 수에 도달했습니다.

설명

시스템이 오펜스를 작성할 수 없거나 유휴 오펜스를 활성 오펜스로 변경할 수 없습니다. 시스템에서 열릴 수 있는 활성 오펜스의 기본 수는 2500으로 제한됩니다. 활성 오펜스는 지난 5일 또는 그 미만의 기간 동안 업데이트된 이벤트 수를 계속 수신하는 모든 오펜스입니다.

사용자 응답

다음 옵션 중 하나를 선택하십시오.

- 낮은 수준의 보안 오펜스를 열림 또는 활성에서 닫힘 또는 닫힘 및 보호로 변경하십시오.
- 시스템을 튜닝하여 오펜스를 생성하는 이벤트의 개수를 줄이십시오.

  폐쇄된 오펜스를 보호하여 데이터 보존 정책이 폐쇄된 오펜스를 제거하지 않도록 방지할 수 있습니다.

최대 오펜스 총계 도달

38750051 - MPC: 오펜스를 처리할 수 없습니다. 최대 오펜스 수에 도달했습니다.

설명

기본적으로 프로세스 한계는 2500개의 활성 오펜스 및 100,000개의 전체 오펜스입니다.

활성 오펜스가 30분 내에 이벤트 업데이트를 수신하지 않으면 오펜스 상태가 유휴 상태로 변경됩니다. 이벤트 업데이트가 발생하면 유휴 오펜스가 활성으로 변경될 수 있습니다. 유휴 오펜스가 5일 동안 이벤트 업데이트를 수신하지 않으면 비활성 상태로 변경됩니다.

사용자 응답

다음 옵션 중 하나를 선택하십시오.

- 시스템을 튜닝하여 오펜스를 생성하는 이벤트의 개수를 줄이십시오.
- 오펜스 보존 정책을 데이터 보존이 비활성 오펜스를 제거할 수 있는 간격으로 조정하십시오.

  폐쇄된 오펜스를 보호하여 데이터 보존 정책이 폐쇄된 오펜스를 제거하지 않도록 방지할 수 있습니다.
- 오펜스를 활성에서 유휴로 변경하여 중요한 활성 오펜스를 위해 디스크 여유 공간을 확보하십시오.

장기 실행 보고서가 중지됨

38750054 - 구성된 최대 임계값을 초과하여 실행되는 보고서를 발견하면 해당 보고서를 중지합니다.

설명

시스템이 시간 제한을 초과한 보고서를 취소합니다. 다음 기본 시간 제한을 초과하여 실행되는 보고서를 취소합니다.

표 4. 보고서 빈도에 따른 기본 시간 제한

보고서 빈도	기본 시간 제한(시간)
시간별	2
일별	12
수동	12
주별	24
월별	24

사용자 응답

다음 옵션 중 하나를 선택하십시오.

- 보고서의 기간을 줄이고 대신 보고서가 더 자주 실행되도록 스케줄하십시오.
- 스케줄에 따라 생성되도록 수동 보고서를 편집하십시오.

  수동 보고서는 원시 데이터를 사용하지만 누적된 데이터에 액세스할 수는 없습니다. 수동 보고서를 편집하고 보고서를 변경하여 시간별, 일별, 월별 또는 주별 스케줄을 사용하도록 설정하십시오.

메모리 부족 오류 및 잘못된 애플리케이션 재시작

38750055 - 메모리 부족: 시스템이 복원되었으며 잘못된 애플리케이션이 다시 시작되었습니다.

설명

애플리케이션 또는 서비스의 메모리가 부족하며 다시 시작되었습니다. 메모리 부족 문제는 일반적으로 소프트웨어 문제 또는 사용자 정의 조회로 인해 발생합니다.

사용자 응답

다음 해결 방법을 검토하십시오.

- 실패한 구성요소를 판별하려면 /var/log/qradar.log 파일에 작성된 오류 메시지를 검토하십시오.
- Ariel 프록시 서버가 많은 양의 데이터를 검색하거나 검색 결과에서 고유 값을 생성하는 그룹화 옵션을 사용하는 경우 고유 값의 수를 줄이거나 검색 시간 프레임을 줄이십시오.
- 누산기가 많은 고유 값이 집계된 시계열 그래프를 생성하는 경우, 조회 크기를 줄이십시오.
- 프로토콜 기반 로그 소스가 최근에 사용 가능하도록 설정된 경우, 조회되는 데이터를 줄이기 위해 폴링 기간을 줄이십시오. 다중 프로토콜 기반 로그 소스가 동시에 실행 중인 경우 시작 시간을 엇갈리게 배치하십시오.

- 룰이 최근에 장기간에 걸쳐 고유 특성을 추적하도록 변경된 경우, 시간 프레임을 절반으로 줄이거나 다른 필터를 추가하여 일치하는 이벤트 수를 줄이십시오.

관리 프로세스에 대한 긴 트랜잭션

38750056 - 트랜잭션 센트리: 긴 트랜잭션을 발생시켜 시스템 안정성을 낮추는 관리 프로세스를 발견했습니다.

설명

트랜잭션 센트리에서 관리 프로세스(예: Tomcat 또는 이벤트 콜렉션 서비스(ECS))가 데이터 잠금의 원인인 것을 발견했습니다.

관리 프로세스가 강제로 재시작됩니다.

사용자 응답

오류의 원인이 된 프로세스를 판별하려면 qradar.log에서 단어 TxSentry를 검토하십시오.

프로토콜 소스 구성이 올바르지 않음

38750057 - 프로토콜 소스 구성이 이벤트 수집을 중지합니다.

설명

시스템이 로그 소스에 대해 올바르지 않은 프로토콜 구성을 발견했습니다. 프로토콜을 사용하여 원격 소스에서 이벤트를 검색하는 로그 소스는 프로토콜의 구성 문제를 발견하면 초기화 오류를 생성합니다.

사용자 응답

다음 단계에 따라 프로토콜 구성 문제를 해결하십시오.

- 로그 소스를 검토하여 프로토콜 구성이 올바른지 확인하십시오.

  JDBC의 인증 필드, 파일 경로, 데이터베이스 이름을 검증하고 시스템이 원격 서버와 통신할 수 있는지 확인하십시오. 마우스 포인터를 로그 소스 위에 놓아서 자세한 오류 정보를 보십시오.
- /var/log/qradar.log 파일을 검토하여 프로토콜 구성 오류에 대한 정보를 확인하십시오.

MPC: 프로세스가 완전히 종료되지 않음

38750058 - MPC: 서버가 완전히 종료되지 않았습니다. 다시 동기화하고 시스템 안정성을 높이기 위해 오펜스를 닫습니다.

설명

치안 판사 프로세스에서 오류가 발생했습니다. 활성 오펜스가 닫히고 서비스가 다시 시작되며 데이터베이스 테이블이 검증되고 필요한 경우 다시 빌드됩니다.

데이터 손상을 방지하기 위해 시스템이 동기화됩니다. 치안 판사 구성요소가 손상된 상태를 발견하는 경우, 데이터베이스 테이블 및 파일이 다시 빌드됩니다.

사용자 응답

치안 판사 구성요소가 자체 복구됩니다. 오류가 계속 발생하면 고객 지원에 문의하십시오.

마지막 백업이 허용되는 시간 한계를 초과함

38750059 - 백업: 마지막으로 스케줄된 백업이 실행 임계값을 초과했습니다.

설명

시간 한계는 구성 중에 지정한 백업 우선순위에 따라서 결정됩니다.

사용자 응답

다음 옵션 중 하나를 선택하십시오.

- 백업 구성을 편집하여 백업 완료에 구성된 시간 한계를 확장하십시오. 24시간을 초과하도록 확장하지 마십시오.
- 실패한 백업을 편집하고 우선순위 레벨을 더 높은 우선순위로 변경하십시오. 우선순위 레벨이 높으면 백업 완료에 더 많은 시스템 자원을 할당합니다.

자동 업데이트 배치

38750069 - 자동 업데이트가 설치되었습니다. 관리 탭에서 변경사항 배치를 클릭하십시오.

설명

자동 업데이트(예: RPM 업데이트)를 다운로드했으며 사용자가 변경사항을 배치하여 설치 프로세스를 완료해야 합니다.

사용자 응답

관리 탭에서 **변경사항 배치**를 클릭하십시오.

사용 안함 상태에서 작성된 로그 소스

38750071 - 라이센스 한계로 인해 사용 안함 상태에서 로그 소스가 작성되었습니다.

설명

트래픽 분석은 이벤트에서 로그 소스를 자동으로 발견하여 작성하는 프로세스입니다. 현재 로그 소스 라이센스 한계에 도달한 경우, 트래픽 분석 프로세스가 사용 안함 상태에서 로그 소스를 작성할 수 있습니다. 사용 안함으로 설정된 로그 소스는 이벤트를 수집하지 않으며 로그 소스 한계에 포함되지 않습니다.

사용자 응답

다음 옵션을 검토하십시오.

- **관리** 탭에서 **로그 소스** 아이콘을 클릭하고 우선순위가 낮은 로그 소스를 사용 안함으로 설정하거나 삭제하십시오. 사용 안함으로 설정된 로그 소스는 로그 소스 라이센스로 계수하지 않습니다.
- 삭제된 로그 소스가 자동으로 재발견하지 않는지 확인하십시오. 로그 소스를 사용 안함으로 설정하여 자동 감지를 방지할 수 있습니다.
- 동시에 다수의 로그 소스를 추가할 때 라이센스 한계를 초과하지 않아야 합니다.
- 라이센스를 연장하여 로그 소스를 추가로 포함하려는 경우, 영업 담당자에게 문의하십시오.

SAR Sentinel 임계값 초과

38750073 - SAR Sentinel: 임계값을 초과했습니다.

설명

SAR(system activity reporter) 유틸리티가 시스템 로드가 임계값을 초과한 것을 발견했습니다. 시스템의 성능이 저하될 수 있습니다.

사용자 응답

다음 옵션을 검토하십시오.

- 대부분 해결 방법이 필요하지 않습니다.

  예를 들어, CPU 사용량이 90%를 넘는 경우 시스템이 자동으로 정상 조작으로 돌아가려고 합니다.
- 이 알림이 반복되는 경우, SAR Sentinel의 기본값을 증가시키십시오.

  관리 탭을 클릭한 다음 **글로벌 시스템 알림**을 클릭하십시오. 알림 임계값을 증가시키십시오.
- 시스템 로드 알림의 경우 동시에 실행되는 프로세스 수를 줄이십시오.

로그 소스에 대한 보고서, 취약성 스캔 또는 데이터 가져오기의 시작 시간을 엇갈리게 배치하십시오. 백업 및 시스템 프로세스의 백업을 서로 다른 시간에 시작하도록 스케줄하여 시스템 로드를 줄이십시오.

사용자가 없거나 정의되지 않음

38750075 - 사용자가 없거나 사용자에게 정의된 역할이 없습니다.

설명

시스템이 더 많은 권한이 있는 사용자 계정으로 업데이트하려고 했으나 사용자 계정 또는 사용자 역할이 존재하지 않습니다.

사용자 응답

관리 탭에서 **변경사항 배치**를 클릭하십시오. 사용자 계정 또는 역할에 대한 업데이트를 수행하려면 변경사항을 배치해야 합니다.

디스크 사용량 경고

38750076 - 디스크 센트리: 디스크 사용량이 경고 임계값을 초과했습니다.

설명

디스크 센트리가 시스템의 디스크 사용량이 90%를 초과한 것을 발견했습니다.

시스템의 디스크 공간 사용이 95%에 도달하면 시스템이 데이터 손상을 방지하기 위해 프로세스를 사용하지 않습니다.

사용자 응답

파일을 삭제하거나 데이터 보존 정책을 변경하여 여유 디스크 공간을 확보해야 합니다. 디스크 공간 사용량이 92% 용량 임계값 아래로 떨어지면 시스템이 자동으로 프로세스를 다시 시작할 수 있습니다.

인프라 구성요소가 손상되었거나 시작되지 않음

38750083 - 인프라 구성요소가 손상되었습니다.

설명

메시지 서비스(IMQ) 또는 PostgreSQL 데이터베이스를 시작할 수 없거나 재빌드할 수 없는 경우, 관리 호스트가 올바르게 작동할 수 없거나 콘솔과 통신할 수 없습니다.

사용자 응답

고객 지원에 문의하십시오.

데이터 복제 문제점

38750085 - 데이터 복제에 문제점이 있습니다.

설명

데이터 복제는 콘솔이 사용 불가능한 경우 관리 호스트에서 계속 데이터를 수집할 수 있도록 합니다.

관리 호스트가 데이터를 다운로드하는 데 문제점이 발생했습니다. 관리 호스트가 반복해서 데이터 다운로드에 실패하는 경우 시스템에 성능 또는 통신 문제가 발생할 수 있습니다.

사용자 응답

관리 호스트에서 자체적으로 복제 문제가 해결되지 않는 경우 고객 지원에 문의하십시오.

스토리지에 직접 라우팅된 이벤트

38750088 - 이벤트 파이프라인에서 성능 저하가 발견되었습니다. 이벤트가 스토리지로 직접 라우팅되었습니다.

설명

큐를 채우지 않고 시스템이 이벤트를 제거하지 않도록 하기 위해 이벤트 콜렉션 서버(ECS)가 데이터를 스토리지에 라우팅합니다. 수신되는 이벤트와 플로우를 분류하지 않습니다. 그러나 원시 이벤트와 플로우 데이터가 수집되고 검색 가능해집니다.

사용자 응답

다음 옵션을 검토하십시오.

- 수신 이벤트와 플로우 비율을 확인하십시오. 이벤트 파이프라인이 이벤트를 큐에 대기시키고 있는 경우, 라이센스를 확장하여 더 많은 데이터를 저장하십시오.
- 룰 또는 사용자 정의 특성에 대한 최신 변경사항을 검토하십시오. 룰이나 사용자 정의 특성 변경으로 인해 이벤트나 플로우 비율이 갑자기 변경될 수 있습니다. 변경사항으로 인해 성능이 저하되거나 시스템이 이벤트를 스토리지에 라우팅할 수 있습니다.
- DSM 구문 분석 문제가 발생하면 이벤트 데이터를 스토리지에 라우팅할 수 있습니다. 로그 소스가 공식적으로 지원되는지 검증하십시오.
- SAR 알림이 큐에 대기된 이벤트 및 플로우가 이벤트 파이프라인에 있음을 표시할 수 있습니다.

- 시스템을 튜닝하여 이벤트 파이프라인에 들어가는 이벤트 및 플로우 볼륨을 줄이십시오.

사용자 정의 특성 사용 안함

38750097 - 사용자 정의 특성을 사용하지 않습니다.

설명

사용자 정의 특성을 처리하는 중에 문제가 발생하여 사용자 정의 특성을 사용하지 않습니다. 사용하지 않도록 설정된 사용자 정의 특성을 사용하는 룰, 보고서 또는 검색은 올바르게 작동하지 않습니다.

사용자 응답

다음 옵션 중 하나를 선택하십시오.

- 사용하지 않는 사용자 정의 특성을 검토하여 정규 표현식 패턴을 정정하십시오. 사용하지 않는 사용자 정의 특성을 다시 사용하도록 설정하기 전에 먼저 정규 표현식 패턴 또는 계산을 검토하고 최적화해야 합니다.
- 사용자 정의 특성이 사용자 정의 룰 또는 보고서에서 사용되는 경우, **룰, 보고서 및 검색의 구문 분석 최적화** 선택란을 선택했는지 확인하십시오.

디바이스 백업 실패

38750098 - 디바이스를 백업하려고 시도하는 중 실패가 발생했거나 백업이 취소되었습니다.

설명

이 오류는 일반적으로 구성 소스 관리(CSM)에 구성 오류가 있거나 사용자가 백업을 취소한 경우 발생합니다.

사용자 응답

다음 옵션 중 하나를 선택하십시오.

- CSM의 신임 정보와 주소 세트를 검토하여 어플라이언스가 로그인할 수 있는지 확인하십시오.
- 네트워크 디바이스에 연결하도록 구성된 프로토콜이 유효한지 확인하십시오.
- 네트워크 디바이스 및 버전이 지원되는지 확인하십시오.
- 네트워크 디바이스가 어플라이언스에 연결되어 있는지 확인하십시오.
- 가장 최신 어댑터를 설치했는지 확인하십시오.

색인화되지 않은 이벤트 또는 플로우

38750101 - 간격 동안 이벤트/플로우 데이터가 색인화되지 않았습니다.

설명

너무 많은 색인을 사용하거나 시스템이 과도하게 사용되는 경우, 시스템이 색인 부분에서 이벤트나 플로우를 제거할 수 있습니다.

사용자 응답

다음 옵션 중 하나를 선택하십시오.

- 제거된 색인 간격이 SAR Sentinel 알림 시 발생하는 경우 시스템 로드 관련 문제이거나 디스크 공간이 적은 경우일 수 있습니다.
- 시스템 로드를 줄이기 위해 일부 색인을 임시로 사용하지 않으려면 **관리** 탭에서 **인덱스 관리** 아이콘을 클릭하십시오.

응답 조치에 대한 임계값 도달

38750102 - 응답 조치: 임계값에 도달했습니다.

설명

응답 임계값에 도달하여 사용자 정의 룰 엔진(CRE)이 룰에 응답할 수 없습니다.

튜닝된 시스템 또는 일반 룰은 여러 응답 조치, 특히 **IF-MAP** 옵션을 사용하는 시스템을 생성할 수 있습니다. 응답 조치가 큐에 대기되었습니다. 이벤트 콜렉션 시스템(ECS)에서 큐에 2000개를 초과하는 항목이 있거나 Tomcat에 1000개를 초과하는 응답 조치가 있는 경우 응답 조치가 제거될 수 있습니다.

사용자 응답

- **IF-MAP** 옵션을 사용하는 경우 **IF-MAP** 서버에 대한 연결이 있는지 Tomcat에 룰 응답을 큐에 대기시키는 대역폭 문제가 있는지 확인하십시오.
- 시스템을 튜닝하여 트리거되는 룰 개수를 줄이십시오.

디스크 복제 속도 감소

38750103 - DRBD Sentinel: 디스크 복제 속도가 감소됩니다. 자세한 내용은 로그를 참조하십시오.

설명

기본 어플라이언스의 복제 큐가 채워지면, 모든 인스턴스에 대한 기본 어플라이언스가 증가할 수 있습니다. 복제 문제는 일반적으로 기본 시스템에 성능 문제가 있거나 보조 시스템에 스토리지 문제가 있거나 어플라이언스 간 대역폭 문제가 있는 경우 발생합니다.

사용자 응답

다음 옵션 중 하나를 선택하십시오.

- **로그 보기** 탭에서 저장된 검색 **MGMT: Bandwidth Manager**를 로드하여 대역폭 활동을 검토하십시오. 이 검색을 수행하면 콘솔과 호스트 간 대역폭 사용량이 표시됩니다.
- 기본 어플라이언스에서 SAR Sentinel 알림이 반복되는 경우, 기본 시스템에서 Distributed Replicated Block Device 큐가 가득 찰 수 있습니다.
- SSH 및 `cat /proc/drbd` 명령을 사용하여 기본 또는 보조 호스트의 Distributed Replicated Block Device 상태를 모니터하십시오.

자산 변경 버림

38750106 - 자산 변경이 중단되었습니다.

설명

자산 변경이 변경 임계값을 초과하여 자산 프로파일 관리자가 자산 변경 요청을 무시합니다.

자산 프로파일 관리자에는 자산의 프로파일 정보를 업데이트하는 자산 지속성 프로세스가 포함됩니다. 프로세스는 자산 모델을 업데이트하기 전에 새 자산 데이터를 수집한 다음 정보를 큐에 대기시킵니다. 사용자가 자산을 추가하거나 편집할 때 데이터가 임시 스토리지에 저장되며 변경 큐의 끝에 추가됩니다. 변경 큐가 크면 자산 변경의 제한시간이 초과되어 임시 스토리지가 삭제될 수 있습니다.

사용자 응답

다음 옵션 중 하나를 선택하십시오.

- 자산을 두 번째로 추가 또는 편집하십시오.
- 취약성 스캔의 시작 시간을 조정하거나 엇갈리게 배치할 수 있으며 스캔 크기를 줄일 수 있습니다.

자산 지속성 큐 디스크 공간 없음

38750113 - 자산 지속성 큐 디스크 공간이 없습니다.

설명

시스템이 자산 지속성 큐에 지정된 스필오버 디스크 공간이 부족하다는 것을 발견했습니다. 디스크 공간을 사용할 수 있을 때까지 자산 지속성 업데이트가 차단됩니다. 정보가 제거되지 않습니다.

사용자 응답

스캔 크기를 줄이십시오. 스캔 크기를 줄이면 자산 지속성 큐의 오버플로우를 예방할 수 있습니다.

자산 업데이트 분석기 큐 디스크 공간 없음

38750115 - 자산 업데이트 분석기 큐 디스크 공간이 없습니다.

설명

시스템이 자산 분석기 큐에 지정된 스필오버 디스크 공간이 부족하다는 것을 발견했습니다.

시스템이 계속해서 디스크에 데이터를 작성하여 데이터 유실을 방지합니다. 그러나 시스템에 디스크 공간이 없으면 스캔 데이터를 제거합니다. 디스크 공간이 확보될 때까지 수신되는 자산 스캔 데이터를 처리할 수 없습니다.

사용자 응답

다음 옵션을 검토하십시오.

- 시스템에 여유 디스크 공간이 있는지 확인하십시오. 알림에는 잠재적 디스크 공간 문제를 알리기 위한 SAR Sentinel 알림이 포함될 수 있습니다.
- 스캔 크기를 줄이십시오.
- 스캔 빈도를 줄이십시오.

자산 변경 큐의 디스크 공간 없음

38750117 - 자산 변경 리스너 큐 디스크 공간이 없습니다.

설명

자산 프로파일 관리자에는 통계를 계산하여 자산의 CVSS 코어를 업데이트하는 변경 리스너 프로세스가 포함됩니다. 시스템은 디스크에 데이터를 작성하여 보류 중인 자산 통계의 데이터 손실을 예방합니다. 그러나 디스크 공간이 없으면 시스템이 스캔 데이터를 제거합니다.

디스크 공간이 확보될 때까지 수신되는 자산 스캔 데이터를 처리할 수 없습니다.

사용자 응답

다음 옵션 중 하나를 선택하십시오.

- 시스템에 충분한 여유 디스크 공간이 있는지 확인하십시오.
- 스캔 크기를 줄이십시오.
- 스캔 빈도를 줄이십시오.

비용 효율이 낮은 사용자 정의 룰 발견

38750120 - 비용 효율이 낮은 사용자 정의 룰을 CRE에서 발견했습니다. 이벤트 파이프라인에서 성능 저하가 발견되었습니다. 비용 효율이 낮은 사용자 정의 룰이 CRE에서 발견되었습니다.

설명

사용자 정의 룰 엔진(CRE)은 이벤트가 룰 세트에 일치하는지 유효성을 검증하고 경보, 오펜스 또는 알림을 트리거하는 프로세스입니다.

사용자는 넓은 범위를 사용하거나 효율적이지 않은 정규 표현식 패턴을 사용하거나 **페이로드 포함** 테스트를 포함하거나 또는 정규식에 룰을 결합하는 사용자 정의 룰을 작성할 수 있습니다. 이 사용자 정의 룰을 사용하면 성능에 부정적인 영향을 끼쳐 이벤트가 부적절하게 스토리지로 직접 라우팅될 수 있습니다. 이벤트가 인덱싱되고 정규화되지만 경보 또는 오펜스를 트리거하지 않습니다.

비용 효율이 낮거나 비효율적이거나 여러 룰 테스트를 사용하면 최대 이벤트 처리량이 감소되어 이벤트 백로그가 룰 엔진을 거치하도록 할 수 있습니다. 이벤트가 스토리지로 직접 라우팅될 수 있으며 이 경고가 표시됩니다.

사용자 응답

다음 옵션을 검토하십시오.

- 알림의 페이로드를 검토하여 파이프라인에서 비용 효율이 낮은 룰이 성능에 영향을 미치는지 판별하십시오.

  예를 들어 다음 페이로드는 파이프라인에서 테스트 "Payload Verification" 룰을 보고하고 보고된 EPS 비율은 초당 787개의 이벤트이며, 잠재적으로 최대 룰 엔진 처리량을 줄입니다.

  ```
  Feb 23 15:56:58 ::ffff:10.1.2.4 [ecs-ep]
  [Timer-27]com.q1labs.semsources.cre.CRE:
  [WARN] [NOT:0040004101][10.1.2.4/-  -]
  [-/--]Expensive Custom Rules Based On Average Throughput in the last 60 seconds:
  Test: Payload Verification=787.98045190917eps,
  Monitoring: Suspect IPs seen with successful logins=899.02679830748eps
  ```

- **오펜스** 탭에서 **룰**을 클릭하고 검색 창을 사용하여 검색해서 비용 효율이 낮은 룰을 편집하거나 사용 안함으로 설정하십시오. 룰을 편집해서 로그 소스 또는 IP 주소 범위 필터를 적용하여 룰을 거치는 데이터 양을 줄일 수 있습니다. 비용 효율이 낮은 테스트(예: 페이로드 포함)도 필요하지 않은 경우 줄이거나 제거할 수 있습니다. 참조 세트 테스트는 대량 참조 세트를 조회하지 않도록 하기 위해 검토해야 합니다.
- SSH를 사용하여 이벤트 프로세서에 로그인하고 다음 명령을 사용하여 구문 분석기 스레드가 EPS 로드에 대해 1500밀리초 넘게 실행되는지 확인하십시오.

  ```
  /opt/qradar/support/threadTop.ssh –p 7799
  ```

다음 명령을 사용하여 regex.Pattern.Curly, referenceSet, assets, host profile 및 port profile에 대한 Java 스레드 스택을 검색하십시오.

```
/opt/qradar/support/threadTop.sh -p 7799 -s -e ".*CRE Processor.*"
```

- 출력에 regex.Pattern.Curly가 포함되어 있는 경우 **페이로드 포함** 테스트 문제가 가능합니다.
- 출력에 referenceSet가 포함되어 있는 경우 대형 참조 세트에 대한 테스트 문제가 발생할 수 있습니다.
- 출력에 assets, host profile 및 port profile이 포함되어 있는 경우 **포트가 열린 호스트** 테스트 또는 자산 테스트 문제가 발생할 수 있습니다.

룰이 문제가 되지 않을 수 있음

이 알림은 이벤트가 룰 엔진을 중심으로 스토리지에 라우팅할 때 트리거할 수 있습니다. 이 알림을 조사할 때 알림의 "EPS" 비율이 ~20,000EPS보다 높은 경우 이는 문제가 다른 곳에 있을 수 있음을 표시합니다. 20,000EPS 이상의 이벤트를 처리할 수 있는 룰은 상당히 최적화되어 있습니다. '스토리지에 라우팅된 이벤트'를 트리거한 상황은 룰이 아닌 다른 상황일 수 있습니다. 고려해야 할 다른 항목이 다음과 같이 나열됩니다.

- 장기 데이터 검색과 같이 다른 이유로 시스템에서 로드가 많습니까?
- 디스크 활용도가 85% 이상 "on/store"이며 데이터 압축이 스토리지 성능에 잠재적으로 영향을 끼칩니까?
- HA가 사용 중인 경우 이벤트 비율이 10,000EPS보다 높으면 충분한 대역폭이 두 HA 노드 간에 있는지 확인하십시오. 예를 들어, 하나의 1Gbps 연결은 전용 교차 연결이라도 스토리지 성능을 제한할 수 있습니다.
- 별도의 "/transient/" 파티션이 있습니까? 그렇지 않으면 임시 데이터 압축 해제에서도 스토리지 자원을 사용하여 스토리지 요청이 높아지는 데 기여할 수 있습니다.

비정상 발견 엔진에 대해 누적을 사용하지 않음

38750121 - 비정상 발견 엔진에 대해 누적이 사용 안함으로 설정되었습니다.

설명

집계 데이터 보기를 사용하지 않거나 사용할 수 없으므로 새 룰에 사용할 수 없는 데이터가 필요합니다.

제거된 누적이 유실된 비정상 데이터를 표시하지 않습니다. 누적이 저장된 데이터에서 생성된 데이터 세트이므로 원래 비정상 데이터가 유지됩니다. 알림에서 제거된 누적 간격에 대한 세부사항을 추가로 제공합니다.

비정상 발견 엔진이 누적의 비정상 데이터에 대한 간격을 검토할 수 없습니다.

사용자 응답

비정상 룰을 업데이트하여 더 작은 데이터 세트를 사용하십시오.

알림이 반복 SAR Sentinel 오류인 경우 시스템 성능이 문제의 원인일 수 있습니다.

프로세스가 허용되는 실행 시간을 초과함

38750122 - 프로세스 실행 시간이 너무 깁니다. 최대 기본 시간은 3600초입니다.

설명

태스크 완료를 위해 개별 프로세스에 허용되는 기본 시간 한계인 1시간을 초과했습니다.

사용자 응답

실행 프로세스를 검토하여 태스크가 계속 실행할 수 있는 프로세스인지 중지해야 하는 프로세스인지 판별하십시오.

라이센스가 만료됨

38750123 - 할당된 라이센스가 만료되었으며 더 이상 유효하지 않습니다.

설명

콘솔에서 라이센스가 만료되면 새 라이센스를 적용해야 합니다. 관리 호스트에서 라이센스가 만료되면 어플라이언스가 공유 라이센스 풀에서 할당된 비율까지 이벤트 및 플로우를 계속해서 처리합니다.

라이센스가 EPS 및 FPM 용량을 공유 라이센스 풀에 제공하는 경우 만료로 인해 공유 라이센스 풀이 배치의 요구사항을 충족할 만큼 충분한 용량을 갖지 못한 부족 상태가 될 수 있습니다. 부족 상태에서는 QRadar가 **네트워크 보기** 및 **로그 보기** 탭의 용량에 대한 액세스를 차단합니다.

사용자 응답

1. 만료된 라이센스를 가진 어플라이언스를 판별하십시오.
   a. **관리** 탭에서 **시스템 및 라이센스 관리**를 클릭하십시오.
   b. **표시** 상자에서 **라이센스**를 선택하십시오.

      만료된 라이센스가 **라이센스 정보 메시지** 섹션에 표시됩니다.
2. 콘솔에 만료된 라이센스가 있으면 이를 바꾸십시오.

3. 관리 호스트에 만료된 라이센스가 있으면 공유 라이센스 풀을 검토하여 시스템에 EPS 및 FPM 용량이 충분한지 확인하십시오.
   a. 공유 라이센스 풀이 초과 할당된 경우 만료된 라이센스를 시스템 용량 요구사항을 충족하기에 충분한 EPS 및 FPM이 있는 새 라이센스로 바꾸십시오.
   b. 라이센스 풀의 용량이 충분한 경우 만료된 라이센스를 삭제하십시오. **라이센스** 테이블에서 만료된 라이센스의 행(관리 호스트 요약 행에 중첩되어 표시됨)을 선택하고 **조치** > **라이센스 삭제**를 선택하십시오.

권한없는 IP 주소 또는 범위의 외부 스캔

38750126 - 외부 스캔 실행이 권한없는 IP 주소 또는 주소 범위를 스캔하려고 했습니다.

설명

스캔 프로파일에 정의된 자산 목록 외부의 CIDR 범위 또는 IP 주소가 포함된 경우, 스캔이 계속됩니다. 하지만 외부 스캐너 목록에 없는 자산의 CIDR 범위 또는 IP 주소는 무시됩니다.

사용자 응답

외부 스캐너에서 스캔하는 자산의 권한없는 CIDR 범위 또는 IP 주소 목록을 업데이트하십시오. 스캔 프로파일을 검토하여 외부 네트워크 목록에 포함된 자산에 대해 스캔이 구성되어 있는지 확인하십시오.

시간 동기화 실패

38750129 - 기본 어플라이언스 또는 콘솔에 대한 시간 동기화가 실패했습니다.

설명

관리 호스트는 콘솔과 동기화할 수 없으며 보조 HA 어플라이언스는 기본 어플라이언스와 동기화할 수 없습니다.

관리자는 포트 123에서 **ntpdate** 통신을 허용해야 합니다. 시간 동기화가 정확하지 않은 경우, 데이터가 콘솔에 올바르게 보고되지 않습니다. 시스템에서 동기화를 수행하지 않는 시간이 길어질수록 데이터, 보고서 또는 오펜스에 대한 검색에서 정확하지 않은 결과를 리턴할 확률이 높아집니다. 시간 동기화는 관리 호스트 및 어플라이언스에서 요청을 수행하는 데 매우 중요한 요소입니다.

사용자 응답

고객 지원에 문의하십시오.

순환 사용자 정의 룰 종속성 체인이 발견됨

38750131 - 사용자 정의 룰 순환 종속성 체인을 발견했습니다.

설명

단일 룰이 직접 자체 참조하거나 다른 룰이나 구성 요소를 통해 자체 참조했습니다. 전체 구성을 배치할 때 오류가 발생합니다. 룰 세트가 로드되지 않습니다.

사용자 응답

순환 종속성을 작성한 룰을 편집하십시오. 시스템 알림이 반복해서 발생하지 않도록 하려면 룰 체인을 중단해야 합니다. 룰 체인을 수정한 후에는 저장사항이 자동으로 룰을 다시 로드하고 문제를 해결합니다.

블랙리스트 알림

38750136 - 자산 조정 제외 룰에서 자산 블랙리스트에 새 자산 데이터를 추가했습니다.

설명

자산 데이터 조각(예: IP 주소, 호스트 이름 또는 MAC 주소)에서 자산 증가 편차와 일치하는 행동을 표시합니다.

자산 블랙리스트는 자산 조정 제외 사용자 정의 엔진 룰에서 신뢰할 수 없는 것으로 고려되는 자산 데이터 콜렉션입니다. 해당 룰은 자산 데이터의 일관성 및 무결성을 모니터합니다. 자산 데이터 조각이 2시간 이내에 두 번 이상 의심스러운 행동을 표시하는 경우 해당 데이터 조각은 자산 블랙리스트에 추가됩니다. 블랙리스트의 자산 데이터가 포함된 후속 업데이트는 자산 데이터베이스에 적용되지 않습니다.

사용자 응답

- 알림 설명에서 **자산 조정 제외 룰**을 클릭하여 자산 데이터를 모니터하는 데 사용되는 룰을 보십시오.
- 알림 설명에서 **로그 소스별 자산 편차**를 클릭하여 최근 24시간 동안 발생한 자산 편차 보고서를 보십시오.
- 블랙리스트가 너무 급격하게 채워지는 경우 이를 채우는 자산 조정 제외 룰을 튜닝할 수 있습니다.
- 자산 데이터베이스에 자산 데이터를 추가하려는 경우 블랙리스트에서 자산 데이터를 제거하고 해당 자산 화이트리스트에 이를 추가하십시오. 화이트리스트에 자산 데이터를 추가하면 이 자산 데이터가 블랙리스트에 실수로 다시 표시되는 것을 방지할 수 있습니다.

- 자산 데이터에 대한 업데이트(http://www.ibm.com/support/knowledgecenter/SS42VS_7.3.0/com.ibm.qradar.doc/c_qradar_ug_asset_reconciliation.html)를 검토하십시오.

자산 증가 편차 발견

38750137 - 시스템에서 정상 크기 임계값을 초과하는 자산 프로파일을 발견했습니다.

설명

시스템이 자산 데이터베이스에서 일탈 또는 비정상적인 증가를 표시하는 자산 프로파일을 하나 이상 발견했습니다. 단일 자산이 시스템 임계값에서 허용하는 것보다 더 많은 IP 주소, DNS 호스트 이름, NetBIOS 이름 또는 MAC 주소를 누적하는 경우 일탈성 증가가 발생합니다. 증가 편차가 발견되는 경우 시스템은 이러한 자산 프로파일에 대한 모든 후속 수신 업데이트를 일시중단합니다.

사용자 응답

자산 증가 편차의 원인을 판별하십시오.

- 알림 설명 위로 마우스를 이동하여 알림 페이로드를 검토하십시오. 페이로드는 가장 자주 편차가 발생하는 상위 5개의 자산 목록을 표시합니다. 이는 또한 시스템에서 각 자산을 증가 편차로 표시한 이유 및 자산이 자산 크기 임계값을 초과하여 증가하려고 한 횟수에 대한 정보를 제공합니다.
- 알림 설명에서 **이 자산의 보고서 검토**를 클릭하여 최근 24시간의 자산 증가 편차에 대한 전체 보고서를 보십시오.
- 자산 데이터에 대한 업데이트(http://www.ibm.com/support/knowledgecenter/SS42VS_7.3.0/com.ibm.qradar.doc/c_qradar_ug_asset_reconciliation.html)를 검토하십시오.

비용 효율이 낮은 사용자 정의 특성 발견

38750138 - 이벤트 파이프라인에서 성능 저하가 발견되었습니다. 비용 효율이 낮은 사용자 정의 특성을 발견했습니다.

설명

정상 처리 중에 최적화된 것으로 표시된 사용자 정의 이벤트와 사용자 정의 플로우 특성이 파이프라인에서 추출되었습니다. 이 값은 사용자 정의 룰 엔진(CRE)에 사용되며 인덱스를 검색합니다.

부적절한 양식의 정규식인 정규 표현식 명령문으로 인해 이벤트가 부적절하게 스토리지로 직접 라우팅될 수 있습니다.

사용자 응답

다음 옵션 중 하나를 선택하십시오.

- 최근에 설치한 사용자 정의 특성을 사용 안함으로 설정하십시오.
- 알림의 페이로드를 검토하십시오. 가능한 경우 사용자 정의 특성과 연관된 정규 표현식 명령문을 개선하십시오.

  예를 들어, 다음 페이로드는 다음 정규 표현식 패턴을 보고합니다.

  ```
  Feb 23 11:44:43 ::ffff:10.1.12.12 [ecs-ec]
  [Timer-60] com.q1labs.semsources.filters.normalize.DSMFilter:
  [WARN] [NOT:0080004105][10.130.126.12/- -]
  [-/- -]Expensive Custom  Properties Based On Average
  Throughput in the last 60 seconds (most to  least expensive)
  - (\w+) /\S+=1136.0eps
  ```

- 사용자 정의 특성 정의를 수정하여 특성을 일치시키고자 하는 카테고리의 범위를 축소하십시오.
- 불필요하게 이벤트를 구문 분석하려는 시도를 피하기 위해 사용자 정의 특성 정의에서 하나의 이벤트 이름을 지정하십시오.
- 가장 많이 전송된 이벤트의 로그 소스부터 가장 적게 전송된 로그 소스까지 로그 소스 구문 분석기를 순서화하고 사용하지 않는 구문 분석기를 사용 안함으로 설정하십시오.

RAID 컨트롤러의 잘못된 구성

38750140 - RAID 컨트롤러의 잘못된 구성: 하드웨어 모니터링에서 가상 드라이브가 잘못 구성되어 있음을 확인했습니다.

설명

최고의 성능을 위해 RAID 컨트롤러 캐시와 배터리 백업 유닛(BBU)은 라이트 백(write-back) 캐시 정책을 사용하도록 구성되어야 합니다. 라이트 쓰루(write-through) 캐시 정책을 사용하면 스토리지 성능이 저하되고 시스템 불안정의 원인이 될 수 있습니다.

사용자 응답

배터리 백업 유닛의 성능 상태를 검토하십시오. 배터리 백업 유닛이 제대로 작동하면 캐시 정책을 라이트 백(write-back)으로 변경하십시오.

로그 파일 수집 중에 오류가 발생함

38750141 - 필수 지원 로그 콜렉션이 오류와 함께 실패했습니다. 시스템 및 라이센스 관리자를 참조하십시오.

설명

로그 파일이 수집되는 중에 오류가 발생했습니다. 로그 파일 콜렉션에 실패했습니다.

사용자 응답

콜렉션 실패 원인에 대한 정보를 보려면 다음 단계를 수행하십시오.

1. 알림 메시지에서 **시스템 및 라이센스 관리자**를 클릭하십시오.
2. **시스템 지원 활동 메시지**를 펼치십시오.
3. 로그 파일 콜렉션 실패 원인에 대한 추가 정보를 보십시오.

비용 효율이 낮은 DSM 확장 발견

38750143 - 이벤트 파이프라인에서 성능 저하가 발견되었습니다. 비용 효율이 낮은 DSM 확장을 발견했습니다.

설명

로그 소스 확장은 이벤트 페이로드에서 온 이벤트를 식별하고 분류하는 데 필요한 모든 정규식 패턴을 포함하는 XML 파일입니다. 로그 소스 확장은 오류 로그 및 일부 시스템 알림에서 디바이스 확장이라고도 합니다.

정상 처리 중에 로그 소스 확장은 이벤트 파이프라인에서 실행됩니다. 이 값은 사용자 정의 룰 엔진(CRE)에 즉시 사용 가능하며 디스크에 저장됩니다.

정규식(regex) 양식이 올바르지 않은 경우 이벤트는 스토리지로 직접 라우팅될 수 있습니다.

사용자 응답

다음 옵션 중 하나를 선택하십시오.

- 최근에 설치한 DSM 확장을 사용 안함으로 설정하십시오.
- 알림의 페이로드를 검토하여 파이프라인에서 비용 효율이 낮은 DSM 확장이 성능에 영향을 미치는지 판별하십시오. 가능한 경우 디바이스 확장과 연관된 정규 표현식 명령문을 개선하십시오.

  예를 들어, 다음 페이로드는 파이프라인이 체크포인트 DSM에 의해 차단됨을 보고합니다.

  ```
  Oct 23 12:32:53 ::ffff:10.1.2.4 [ecs-ec]
  [Timer-57] com.q1labs.semsources.filters.normalize.DSMFilter: [WARN]
  [NOT:0080014100][10.1.2.4/- -][-/- -]Expensive Log Source or Log Source
  Extensions Based On Average Throughput in the last 60 seconds
  (most to least expensive) - Checkpoint=0.0eps, CatOS=86.0eps, Apache=2500.0eps,
  Endpointprotection=2905.0eps
  ```

- 로그 소스 확장이 올바른 로그 소스에만 적용되는지 확인하십시오.

관리 탭에서 **시스템 구성** > **데이터 소스** > **로그 소스**를 클릭하십시오. 각 로그 소스를 선택하고 **편집**을 클릭하여 로그 소스 세부사항을 확인하십시오.

- 프로토콜 기반 로그 소스를 사용하여 작업 중인 경우 이벤트가 디스크를 버퍼링하지 않도록 이벤트 제한을 줄이십시오. 이벤트 제한 설정은 로그 소스에 대한 프로토콜 구성의 일부입니다.
- 가장 많이 전송된 이벤트의 로그 소스부터 가장 적게 전송된 로그 소스까지 로그 소스 구문 분석기를 순서화하고 사용하지 않는 구문 분석기를 사용 안함으로 설정하십시오.
- 콘솔이 최신 DSM 버전으로 설치되었는지 확인하십시오.
- 로그 소스가 환경에 없는 디바이스에 대해 작성된 경우 다음 명령을 사용하여 로그 소스를 제거하십시오.

  ```
  /opt/qradar/bin/tatoggle.pl
  ```

  여러 이벤트 프로세서가 있는 경우 `/opt/qradar/conf/TrafficAnalysisConfig.xml` 파일을 `/store/configservices/staging/globalconfig/` 디렉토리에 복사하십시오. **관리** 탭에서 모든 관리 호스트에 대해 **전체 구성 배치**를 클릭하여 구성 파일을 가져오십시오.

QRadar 어플라이언스에 대한 정보 알림

IBM Security QRadar는 프로세스 또는 조치의 상태나 결과에 대한 정보 메시지를 제공합니다.

자동 업데이트 다운로드 완료

38750068 - 자동 업데이트가 다운로드되었습니다. 자세한 정보는 자동 업데이트 로그를 참조하십시오.

설명

소프트웨어 업데이트가 자동으로 다운로드되었습니다.

사용자 응답

알림의 링크를 클릭하여 다운로드된 업데이트를 설치해야 하는지 판별하십시오.

자동 업데이트 완료

38750070 - 자동 업데이트가 완료되었습니다.

설명

자동 소프트웨어 업데이트를 다운로드하여 설치했습니다.

사용자 응답

조치가 필요하지 않습니다.

SAR Sentinel 조작 복원

38750072 - SAR Sentinel: 정상 조작이 복원되었습니다.

설명

SAR(system activity reporter) 유틸리티가 시스템 로드가 허용 가능한 수준으로 돌아간 것을 발견했습니다.

사용자 응답

조치가 필요하지 않습니다.

디스크 사용량이 정상으로 돌아옴

38750077 - 디스크 센트리: 시스템 디스크 사용량이 정상 수준으로 돌아왔습니다.

설명

디스크 센트리가 디스크 사용량이 전체 용량의 90% 미만으로 떨어진 것을 발견했습니다.

사용자 응답

조치가 필요하지 않습니다.

인프라 구성요소가 복구됨

38750084 - 손상된 인프라 구성요소가 복구되었습니다.

설명

관리 호스트의 호스트 서비스를 담당하는 손상된 구성요소가 복구되었습니다.

사용자 응답

조치가 필요하지 않습니다.

디스크 스토리지 사용 가능

38750093 - 이전에 액세스 불가능한 하나 이상의 스토리지 파티션이 현재 액세스 가능합니다.

설명

25 페이지의 『디스크 스토리지 사용 불가능』에서 알림이 표시된 후에 디스크 센트리가 스토리지 파티션이 사용 가능한 것을 발견했습니다. 디스크 사용 불가능이 해결되었습니다.

사용자 응답

조치가 필요하지 않습니다.

관련 개념:

25 페이지의 『디스크 스토리지 사용 불가능』

38750092 - 디스크 센트리가 하나 이상의 스토리지 파티션에 액세스할 수 없음을 발견했습니다.

라이센스 만료 예정

38750124 - 라이센스가 만료될 예정입니다. 곧 라이센스를 대체해야 합니다.

설명

시스템에서 어플라이언스의 라이센스가 35일 내에 만료됨을 발견했습니다.

사용자 응답

조치가 필요하지 않습니다.

로그 파일이 수집됨

38750142 - 필수 지원 로그가 수집되었습니다. 시스템 및 라이센스 관리자를 참조하십시오.

설명

로그 파일이 수집되었습니다.

사용자 응답

로그 파일 콜렉션을 다운로드하려면 다음 단계를 수행하십시오.

1. 알림 메시지에서 **시스템 및 라이센스 관리자**를 클릭하십시오.
2. **시스템 지원 활동 메시지**를 펼치십시오.
3. **파일을 다운로드하려면 여기를 클릭하십시오**를 클릭하십시오.

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 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.

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

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

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

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

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

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

상표

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

Linux는 미국 또는 기타 국가에서 사용되는 Linus Torvalds의 등록상표입니다.

제품 문서의 이용 약관

다음 이용 약관에 따라 이 책을 사용할 수 있습니다.

적용성

본 이용 약관은 IBM 웹 사이트의 모든 이용 약관에 추가됩니다.

개인적 사용

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

상업적 사용

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

권한

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

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

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

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

IBM 온라인 개인정보 보호정책

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

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

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

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

색인