워크로드 보안

Data Infrastructure Insights

NetApp
January 14, 2026

목차

워크로드 보안

스토리지 워크로드 보안에 관하여

Data Infrastructure Insights 스토리지 워크로드 보안(이전의 Cloud Secure)은 내부 위협에 대한 실행 가능한 인텔리전스를 통해 데이터를 보호하는 데 도움이 됩니다. 하이브리드 클라우드 환경 전반에서 모든 기업 데이터 액세스에 대한 중앙 집중식 가시성과 제어 기능을 제공하여 보안 및 규정 준수 목표가 충족되도록 보장합니다.

시계

온프레미스 또는 클라우드에 저장된 중요한 기업 데이터에 대한 사용자 액세스를 중앙에서 파악하고 제어하세요.

데이터 접근 및 제어에 대한 적시적절하고 정확한 가시성을 제공하지 못하는 도구와 수동 프로세스를 교체합니다. Workload Security는 클라우드와 온프레미스 스토리지 시스템 모두에서 고유하게 작동하여 악의적인 사용자 행동에 대한 실시간 알림을 제공합니다.

보호

고급 머신 러닝과 이상 감지를 통해 악의적이거나 손상된 사용자가 조직 데이터를 오용하는 것을 방지합니다.

고급 머신 러닝과 사용자 행동의 이상 감지를 통해 비정상적인 데이터 접근에 대한 경고를 제공합니다.

규정 준수

온프레미스 또는 클라우드에 저장된 중요한 회사 데이터에 대한 사용자 데이터 액세스를 감사하여 회사 규정 준수를 보장하세요.

시작하기

워크로드 보안 시작하기

워크로드 보안은 사용자 활동을 모니터링하고 스토리지 환경에서 잠재적인 보안 위협을 감지하는 데 도움이 됩니다. 모니터링을 시작하기 전에 에이전트, 데이터 수집기, 디렉터리 서비스를 구성하여 포괄적인 보안 모니터링의 기반을 마련해야 합니다.

워크로드 보안 시스템은 에이전트를 사용하여 스토리지 시스템에서 액세스 데이터를 수집하고 디렉토리 서비스 서버에서 사용자 정보를 수집합니다.

데이터 수집을 시작하려면 먼저 다음을 구성해야 합니다.

일	관련 정보
에이전트 구성	"에이전트 요구 사항" "에이전트 추가"

사용자 디렉토리 커넥터 구성	"사용자 디렉토리 커넥터 추가"
데이터 수집기 구성	*워크로드 보안 > 수집기*를 클릭합니다. 구성하려는 데이터 수집기를 클릭합니다. 수집기 정보는 설명서의 데이터 수집기 공급업체 참조 섹션을 참조하세요.
사용자 계정 생성	"사용자 계정 관리"

워크로드 보안은 다른 도구와도 통합될 수 있습니다. 예를 들어,"이 가이드를 참조하세요" Splunk와의 통합에 관하여.

워크로드 보안 에이전트 요구 사항

당신은해야합니다"Workload Security Agent 설치" 귀하의 데이터 수집자로부터 정보를 얻기 위해서입니다. 에이전트를 설치하기 전에 사용자 환경이 운영 체제, CPU, 메모리 및 디스크 공간 요구 사항을 충족하는지 확인하세요.

요소	리눅스 요구 사항
운영 체제	다음 중 하나의 라이선스 버전을 실행하는 컴퓨터: * AlmaLinux 9.4(64비트) ~ 9.5(64비트), 10(64비트), SELinux 포함 * CentOS Stream 9(64비트) * Debian 11(64비트), 12(64비트), SELinux 포함 * OpenSUSE Leap 15.3(64비트) ~ 15.6(64비트) * Oracle Linux 8.10(64비트), 9.1(64비트) ~ 9.6(64비트), SELinux 포함 * Red Hat Enterprise Linux 8.10(64비트), 9.1(64비트) ~ 9.6(64비트), 10(64비트), SELinux 포함 * Rocky 9.4(64비트) ~ 9.6(64비트), SELinux 포함 * SUSE Linux Enterprise Server 15 SP4(64비트) ~ 15 SP6(64비트), SELinux 포함 * Ubuntu 20.04 LTS(64비트), 22.04 LTS(64비트), 24.04 LTS(64비트) 이 컴퓨터에서는 다른 애플리케이션 수준 소프트웨어를 실행하면 안 됩니다. 전용 서버를 권장합니다.
명령	설치하려면 '압축 해제'가 필요합니다. 또한, 설치, 스크립트 실행, 제거에는 'sudo su –' 명령이 필요합니다.
CPU	4개의 CPU 코어
메모리	16GB 램
사용 가능한 디스크 공간	디스크 공간은 다음과 같은 방식으로 할당해야 합니다. /opt/netapp 36GB(파일 시스템 생성 후 최소 35GB의 여유 공간) 참고: 파일 시스템을 생성할 수 있도록 약간의 추가 디스크 공간을 할당하는 것이 좋습니다. 파일 시스템에 최소 35GB의 여유 공간이 있는지 확인하세요. /opt가 NAS 저장소에서 마운트된 폴더인 경우 로컬 사용자가 이 폴더에 액세스할 수 있는지 확인하세요. 로컬 사용자에게 이 폴더에 대한 권한이 없으면 에이전트 또는 데이터 수집기가 설치되지 않을 수 있습니다. 다음을 참조하세요."문제 해결" 자세한 내용은 섹션을 참조하세요.
회로망	100Mbps~1Gbps 이더넷 연결, 고정 IP 주소, 모든 장치에 대한 IP 연결, Workload Security 인스턴스에 필요한 포트(80 또는 443).

참고: Workload Security 에이전트는 Data Infrastructure Insights 수집 장치 및/또는 에이전트와 동일한 시스템에 설치할 수 있습니다. 하지만 이러한 장치를 별도의 컴퓨터에 설치하는 것이 가장 좋습니다. 동일한 컴퓨터에 설치된 경우 아래와 같이 디스크 공간을 할당하세요.

사용 가능한 디스크 공간	Linux의 경우 디스크 공간은 다음과 같은 방식으로 할당해야 합니다. /opt/netapp 25-30GB /var/log/netapp 25GB

추가 권장 사항

- ONTAP 시스템과 에이전트 머신 모두의 시간을 네트워크 시간 프로토콜**(NTP)** 또는 *단순 네트워크 시간 프로토콜(SNTP)*을 사용하여 동기화하는 것이 좋습니다.

클라우드 네트워크 액세스 규칙

미국 기반 워크로드 보안 환경의 경우:

규약	포트	원천	목적지	설명
TCP	443	워크로드 보안 에이전트	<사이트 이름>.cs01.cloudinsights.netapp.com <사이트 이름>.c01.cloudinsights.netapp.com <사이트 이름>.c02.cloudinsights.netapp.com	Data Infrastructure Insights 에 대한 액세스
TCP	443	워크로드 보안 에이전트	agentlogin.cs01.cloudinsights.netapp.com	인증 서비스 접근

유럽 기반 워크로드 보안 환경의 경우:

규약	포트	원천	목적지	설명
TCP	443	워크로드 보안 에이전트	<사이트 이름>.cs01-eu-1.cloudinsights.netapp.com <사이트 이름>.c01-eu-1.cloudinsights.netapp.com <사이트 이름>.c02-eu-1.cloudinsights.netapp.com	Data Infrastructure Insights 에 대한 액세스
TCP	443	워크로드 보안 에이전트	agentlogin.cs01-eu-1.cloudinsights.netapp.com	인증 서비스 접근

APAC 기반 워크로드 보안 환경의 경우:

규약	포트	원천	목적지	설명
TCP	443	워크로드 보안 에이전트	<사이트 이름>.cs01-ap-1.cloudinsights.netapp.com <사이트 이름>.c01-ap-1.cloudinsights.netapp.com <사이트 이름>.c02-ap-1.cloudinsights.netapp.com	Data Infrastructure Insights 에 대한 액세스
TCP	443	워크로드 보안 에이전트	agentlogin.cs01-ap-1.cloudinsights.netapp.com	인증 서비스 접근

네트워크 내 규칙

규약	포트	원천	목적지	설명
TCP	389(LDAP) 636(LDAP/start-tls)	워크로드 보안 에이전트	LDAP 서버 URL	LDAP에 연결
TCP	443	워크로드 보안 에이전트	클러스터 또는 SVM 관리 IP 주소(SVM 수집기 구성에 따라 다름)	ONTAP 과의 API 통신
TCP	35000 - 55000	SVM 데이터 LIF IP 주소	워크로드 보안 에이전트	Fpolicy 이벤트에 대한 ONTAP 에서 Workload Security Agent로의 통신입니다. ONTAP Workload Security Agent로 이벤트를 전송하려면 Workload Security Agent에 대한 이러한 포트가 열려 있어야 하며, 여기에는 Workload Security Agent 자체의 방화벽(있는 경우)도 포함됩니다. 모든 포트를 예약할 필요는 없지만, 예약하는 포트는 이 범위 내에 있어야 합니다. 처음에는 약 100개의 포트를 예약하고, 필요하다면 늘리는 것이 좋습니다.

규약	포트	원천	목적지	설명
TCP	35000-55000	클러스터 관리 IP	워크로드 보안 에이전트	*EMS 이벤트*에 대한 ONTAP 클러스터 관리 IP에서 워크로드 보안 에이전트로의 통신입니다. ONTAP 이 Workload Security Agent에 *EMS 이벤트*를 보낼 수 있도록 Workload Security Agent에 대한 이러한 포트가 열려 있어야 하며, 여기에는 Workload Security Agent 자체의 방화벽(있는 경우)도 포함됩니다. 모든 포트를 예약할 필요는 없지만, 예약하는 포트는 이 범위 내에 있어야 합니다. 처음에는 약 100개의 포트를 예약하고, 필요하다면 늘리는 것이 좋습니다.
SSH	22	워크로드 보안 에이전트	클러스터 관리	CIFS/SMB 사용자 차단에 필요합니다.

시스템 크기 조정

를 참조하십시오"이벤트 요금 확인기" 사이즈에 대한 정보는 설명서를 참조하세요.

워크로드 보안 에이전트 배포

워크로드 보안 에이전트는 스토리지 인프라 전반에서 사용자 활동을 모니터링하고 잠재적인 보안 위협을 탐지하는 데 필수적입니다. 이 가이드는 단계별 설치 지침, 에이전트 관리 모범 사례(일시 중지/재개 및 고정/고정 해제 기능 포함), 배포 후 구성 요구 사항을 제공합니다. 시작하기 전에 에이전트 서버가 다음 요구 사항을 충족하는지 확인하십시오. "시스템 요구 사항".

시작하기 전에

- 설치, 스크립트 실행, 설치 제거에는 sudo 권한이 필요합니다.
- 에이전트를 설치하는 동안 로컬 사용자 _cssys_와 로컬 그룹 _cssys_가 머신에 생성됩니다. 권한 설정에서 로컬 사용자 생성을 허용하지 않고 대신 Active Directory가 필요한 경우, 사용자 이름이 _cssys_인 사용자를 Active Directory 서버에 만들어야 합니다.
- Data Infrastructure Insights 보안에 대해 읽어보세요."여기" .

모범 사례

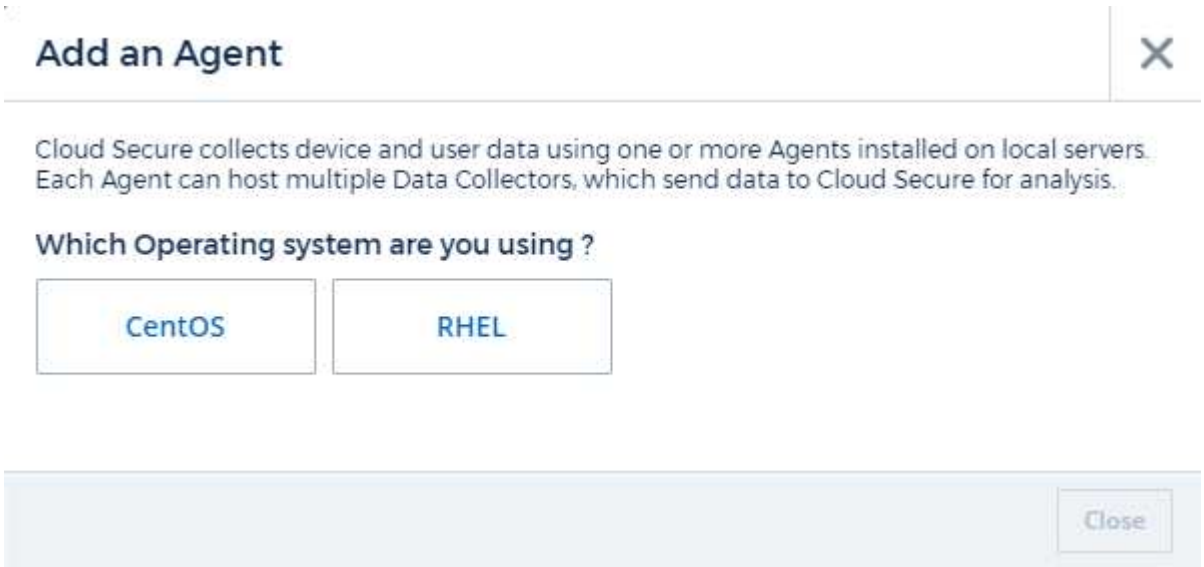
Workload Security 에이전트를 구성하기 전에 다음 사항을 염두에 두십시오.

일시 정지 및 재개	일시 중지: ONTAP 에서 fpolicies를 제거합니다. 일반적으로 고객이 에이전트 VM 재부팅이나 스토리지 교체 등 상당한 시간이 소요될 수 있는 확장된 유지 관리 활동을 수행할 때 사용됩니다. 재개: ONTAP 에 fpolicies를 다시 추가합니다.
고정 및 고정 해제	고정 해제는 최신 버전(사용 가능한 경우)을 즉시 가져오고 에이전트와 수집기를 업그레이드합니다. 이 업그레이드 중에 fpolicies의 연결이 끊어지고 다시 연결됩니다. 이 기능은 자동 업그레이드의 타이밍을 제어하려는 고객을 위해 설계되었습니다. 아래를 참조하세요고정/고정 해제 지침 .
권장 접근 방식	대규모 구성의 경우 수집기를 일시 중지하는 대신 고정 및 고정 해제를 사용하는 것이 좋습니다. 고정 및 고정 해제를 사용하는 동안 일시 정지 및 재개가 필요하지 않습니다. 고객은 에이전트와 수집가를 고정해 두고, 새 버전에 대한 이메일 알림을 받으면 30일 기간 내에 에이전트를 하나씩 선택적으로 업그레이드할 수 있습니다. 이 접근 방식은 fpolicies에 대한 지연 영향을 최소화하고 업그레이드 프로세스에 대한 더 큰 제어력을 제공합니다.

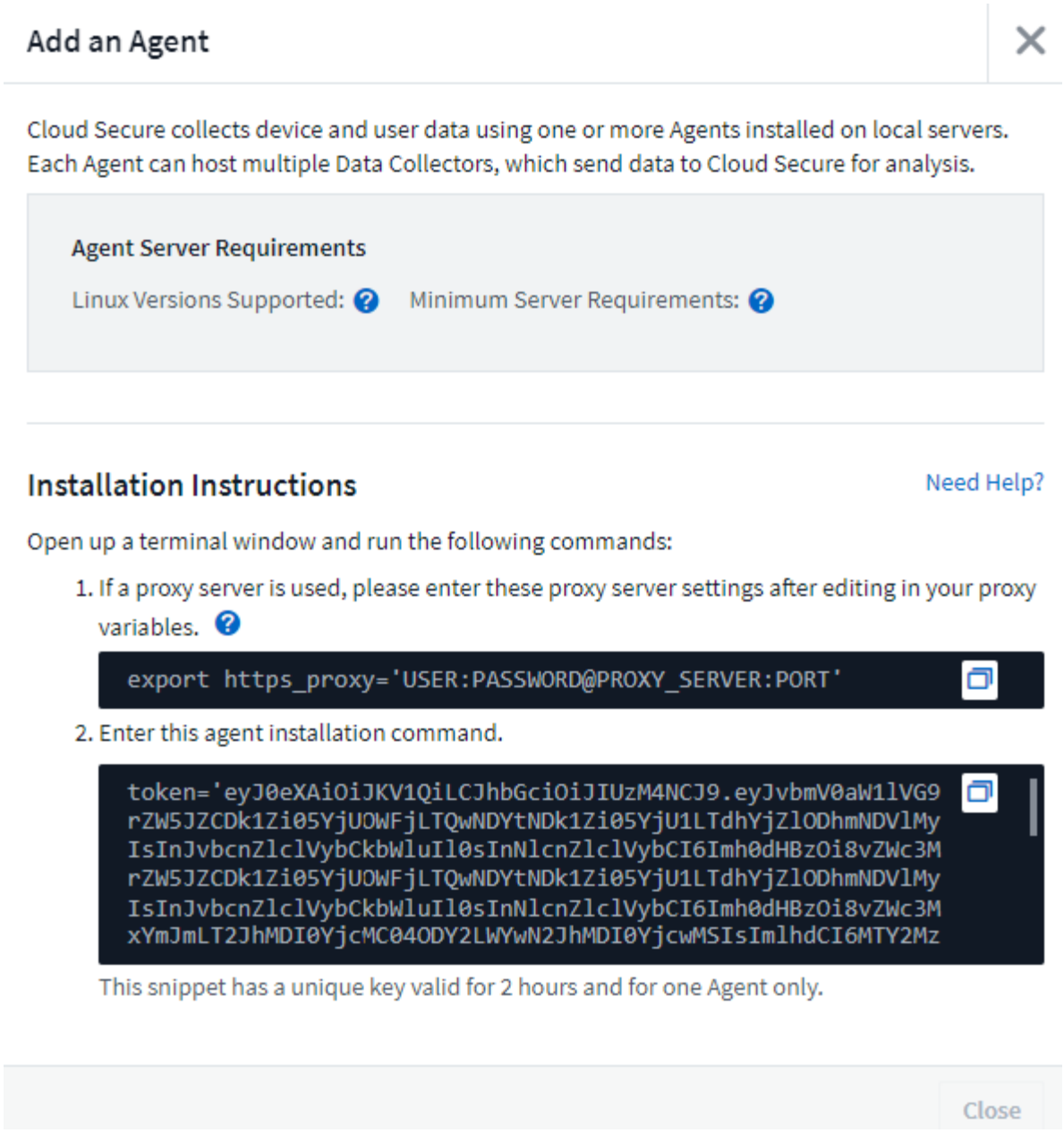
에이전트 설치 단계

1. 워크로드 보안 환경에 관리자 또는 계정 소유자로 로그인합니다.
2. *수집가 > 에이전트 > +에이전트*를 선택하세요.

   시스템에 에이전트 추가 페이지가 표시됩니다.



3. 에이전트 서버가 최소 시스템 요구 사항을 충족하는지 확인하세요.
4. 에이전트 서버가 지원되는 Linux 버전을 실행하고 있는지 확인하려면 _지원되는 버전(i)_을 클릭합니다.
5. 네트워크에서 프록시 서버를 사용하는 경우 프록시 섹션의 지침에 따라 프록시 서버 세부 정보를 설정하세요.



6. 클립보드에 복사 아이콘을 클릭하여 설치 명령을 복사합니다.
7. 터미널 창에서 설치 명령을 실행합니다.
8. 설치가 성공적으로 완료되면 시스템에 다음 메시지가 표시됩니다.

완료 후

1. 구성해야 합니다"사용자 디렉토리 수집기" .
2. 하나 이상의 데이터 수집기를 구성해야 합니다.

네트워크 구성

Workload Security에서 사용할 포트를 열려면 로컬 시스템에서 다음 명령을 실행하세요. 포트 범위와 관련하여 보안 문제가 있는 경우 _35000:35100_과 같이 더 작은 포트 범위를 사용할 수 있습니다. 각 SVM은 두 개의 포트를 사용합니다.

단계

1. `sudo firewall-cmd --permanent --zone=public --add-port=35000-55000/tcp`
2. `sudo firewall-cmd --reload`

플랫폼에 따라 다음 단계를 따르세요.

CentOS 7.x / RHEL 7.x:

1. `sudo iptables-save | grep 35000`

샘플 출력:

```
 -A IN_public_allow -p tcp -m tcp --dport 35000:55000 -m conntrack
-ctstate NEW,UNTRACKED -j ACCEPT
*CentOS 8.x / RHEL 8.x*:
```

1. `sudo firewall-cmd --zone=public --list-ports | grep 35000`(CentOS 8용)

샘플 출력:

```
35000-55000/tcp
```

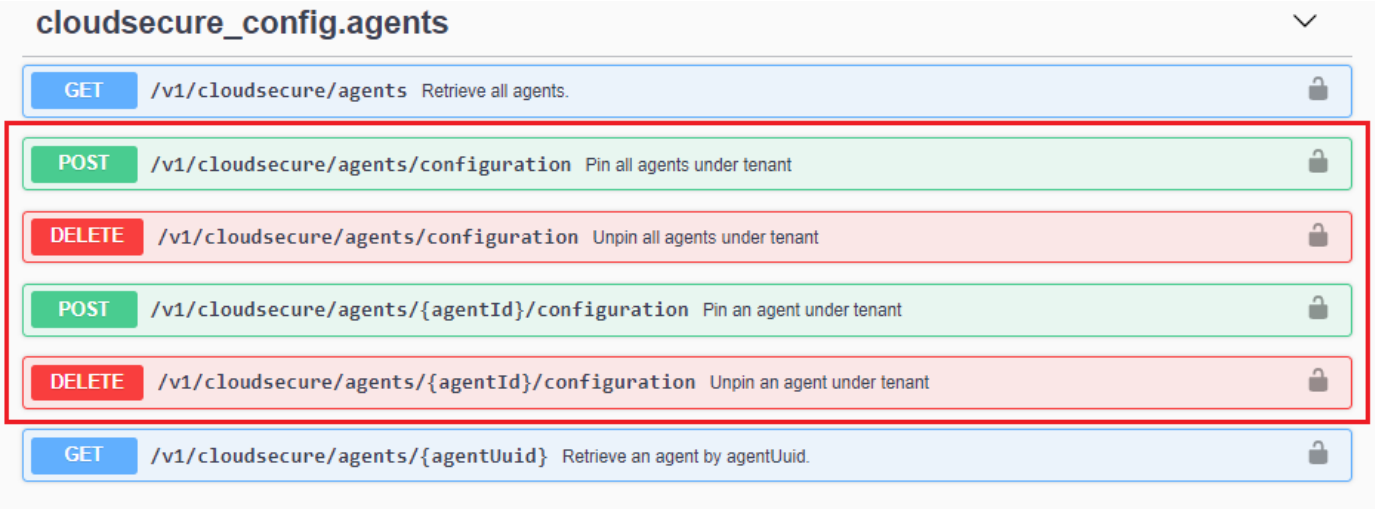
현재 버전에서 에이전트 **"고정"**

기본적으로 Data Infrastructure Insights Workload Security는 에이전트를 자동으로 업데이트합니다. 일부 고객은 자동 업데이트를 일시 중지하고 싶어할 수 있습니다. 이 경우 다음 중 하나가 발생할 때까지 에이전트가 현재 버전을 유지합니다.

- 고객이 자동 에이전트 업데이트를 재개합니다.
- 30일이 지났습니다. 30일은 에이전트가 일시 중지된 날이 아닌, 가장 최근의 에이전트 업데이트 날짜부터 시작됩니다.

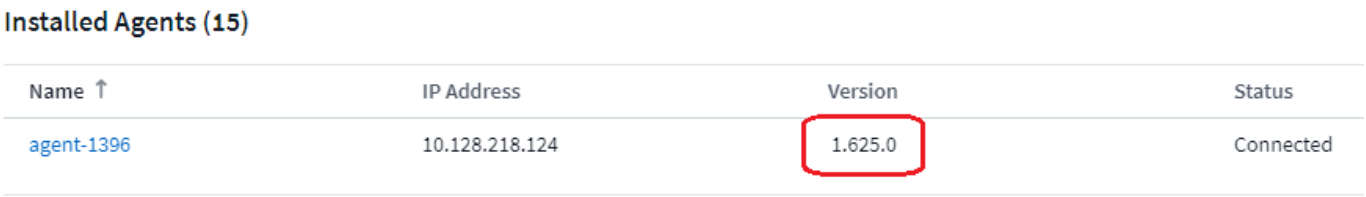
각각의 경우에서 에이전트는 다음 워크로드 보안 업데이트 시 업데이트됩니다.

자동 에이전트 업데이트를 일시 중지하거나 다시 시작하려면 *cloudsecure_config.agents* API를 사용하세요.



일시 중지 또는 재개 작업이 적용되려면 최대 5분이 걸릴 수 있습니다.

워크로드 보안 **>** 수집기 페이지의 에이전트 탭에서 현재 에이전트 버전을 볼 수 있습니다.



에이전트 오류 문제 해결

알려진 문제와 해결 방법은 다음 표에 설명되어 있습니다.

문제:	해결:
에이전트 설치 시 /opt/netapp/cloudsecure/agent/logs/agent.log 폴더가 생성되지 않고 install.log 파일에 관련 정보가 제공되지 않습니다.	이 오류는 에이전트 부트스트래핑 중에 발생합니다. 이 오류는 로거가 초기화되기 전에 발생하므로 로그 파일에 기록되지 않습니다. 오류는 표준 출력으로 리디렉션되고 서비스 로그에서 다음을 사용하여 볼 수 있습니다. `journalctl -u cloudsecure-agent.service` 명령. 이 명령은 문제를 추가로 해결하는 데 사용할 수 있습니다.
에이전트 설치가 '이 Linux 배포판은 지원되지 않습니다 .'라는 메시지와 함께 실패합니다. 설치를 종료합니다.	이 오류는 지원되지 않는 시스템에 에이전트를 설치하려고 할 때 나타납니다. 보다 "에이전트 요구 사항" .
에이전트 설치가 "-bash: unzip: 명령을 찾을 수 없습니다" 오류로 인해 실패했습니다.	unzip을 설치한 후 설치 명령을 다시 실행하세요. 컴퓨터에 Yum이 설치되어 있다면 "yum install unzip"을 실행하여 압축 해제 소프트웨어를 설치해 보세요. 그런 다음 에이전트 설치 UI에서 명령을 다시 복사하여 CLI에 붙여넣어 설치를 다시 실행합니다.

문제:	해결:

에이전트가 설치되어 실행 중입니다. 하지만 요원이 갑자기 멈췄습니다.	에이전트 머신에 SSH를 실행합니다. 에이전트 서비스 상태를 확인하세요. `sudo systemctl status cloudsecure-agent.service` . 1. 로그에 "Workload Security 데몬 서비스를 시작하지 못했습니다 "라는 메시지가 표시되는지 확인하세요. 2. 에이전트 머신에 cssys 사용자가 있는지 확인하세요. 루트 권한으로 다음 명령을 하나씩 실행하고 cssys 사용자와 그룹이 있는지 확인하세요.
	`sudo id cssys`
	`sudo groups cssys` 3. 해당 사항이 없다면 중앙 모니터링 정책으로 인해 cssys 사용자가 삭제되었을 수 있습니다. 4. 다음 명령을 실행하여 cssys 사용자와 그룹을 수동으로 생성합니다.
	`sudo useradd cssys`
	`sudo groupadd cssys` 5. 다음 명령을 실행하여 에이전트 서비스를 다시 시작합니다.
	`sudo systemctl restart cloudsecure-agent.service` 6. 그래도 실행되지 않으면 다른 문제 해결 옵션을 확인해 보세요.

에이전트에 50개 이상의 데이터 수집기를 추가할 수 없습니다.	에이전트에 추가할 수 있는 데이터 수집기는 최대 50개입니다. 여기에는 Active Directory, SVM 및 기타 수집기 등 모든 수집기 유형이 결합될 수 있습니다.
UI에서 에이전트가 NOT_CONNECTED 상태임을 표시합니다.	에이전트를 다시 시작하는 단계입니다. 1. 에이전트 머신에 SSH를 실행합니다. 2. 다음 명령을 실행하여 에이전트 서비스를 다시 시작합니다. `sudo systemctl restart cloudsecure-agent.service` 3. 에이전트 서비스 상태를 확인하세요. `sudo systemctl status cloudsecure-agent.service` . 4. 에이전트는 CONNECTED 상태로 전환되어야 합니다.
에이전트 VM이 Zscaler 프록시 뒤에 있어 에이전트 설치에 실패했습니다. Zscaler 프록시의 SSL 검사로 인해 워크로드 보안 인증서는 Zscaler CA에서 서명한 것처럼 표시되므로 에이전트는 통신을 신뢰하지 않습니다.	Zscaler 프록시에서 *.cloudinsights.netapp.com URL에 대한 SSL 검사를 비활성화합니다. Zscaler가 SSL 검사를 수행하고 인증서를 교체하는 경우 Workload Security는 작동하지 않습니다.
에이전트를 설치하는 동안 압축을 풀면 설치가 중단됩니다.	"chmod 755 -Rf" 명령이 실패합니다. 작업 디렉토리에 다른 사용자의 파일이 있고 해당 파일의 권한을 변경할 수 없는 루트가 아닌 sudo 사용자가 에이전트 설치 명령을 실행하면 명령이 실패합니다. chmod 명령이 실패하여 나머지 설치 과정이 실행되지 않습니다. 1. "cloudsecure"라는 이름의 새 디렉토리를 만듭니다. 2. 해당 디렉토리로 가세요. 3. 전체 “token=…… … ./cloudsecure-agent-install.sh” 설치 명령을 복사하여 붙여넣고 Enter를 누릅니다. 4. 설치가 진행될 것입니다.

문제:	해결:
에이전트가 여전히 SaaS에 연결할 수 없는 경우 NetApp 지원팀에 사례를 제출하세요. 사례를 열려면 Data Infrastructure Insights 일련번호를 제공하고, 기록된 대로 사례에 로그를 첨부하세요.	케이스에 로그를 부착하려면: 1. 루트 권한으로 다음 스크립트를 실행하고 출력 파일(cloudsecure-agent-symptoms.zip)을 공유합니다. a. /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh 2. 루트 권한으로 다음 명령을 하나씩 실행하고 출력을 공유하세요. a. id cssys b. groups cssys c. cat /etc/os-release
cloudsecure-agent-symptom-collector.sh 스크립트가 다음 오류로 인해 실패합니다. [root@machine tmp]# /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh 서비스 로그 수집 애플리케이션 로그 수집 에이전트 구성 수집 서비스 상태 스냅샷 생성 에이전트 디렉터리 구조 스냅샷 생성 ……. ……. /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh: 52번째 줄: zip: 명령을 찾을 수 없습니다. 오류: /tmp/cloudsecure-agent-symptoms.zip을 만들지 못했습니다.	Zip 도구가 설치되지 않았습니다. "yum install zip" 명령을 실행하여 zip 도구를 설치합니다. 그런 다음 cloudsecure-agent-symptom-collector.sh를 다시 실행합니다.
useradd로 에이전트 설치가 실패합니다. /home/cssys 디렉토리를 생성할 수 없습니다.	이 오류는 권한이 부족하여 사용자의 로그인 디렉토리를 /home 아래에 만들 수 없는 경우 발생할 수 있습니다. 해결 방법은 cssys 사용자를 만들고 다음 명령을 사용하여 로그인 디렉토리를 수동으로 추가하는 것입니다. *sudo useradd user_name -m -d HOME_DIR* -m : 사용자의 홈 디렉토리가 없으면 만듭니다. -d : 사용자 로그인 디렉토리의 값으로 HOME_DIR을 사용하여 새 사용자가 생성됩니다. 예를 들어, _sudo useradd cssys -m -d /cssys_는 사용자 _cssys_를 추가하고 루트 아래에 로그인 디렉토리를 만듭니다.
설치 후 에이전트가 실행되지 않습니다. _Systemctl status cloudsecure-agent.service_는 다음을 보여줍니다. [root@demo ~]# systemctl status cloudsecure-agent.service agent.service – Workload Security Agent Daemon Service 로드됨: 로드됨(/usr/lib/systemd/system/cloudsecure-agent.service; 활성화됨; 공급업체 사전 설정: 비활성화됨) 활성: 활성화 중(자동 재시작)(결과: 종료 코드) 2021-08-03 21:12:26 PDT 화요일부터; 2초 전 프로세스: 25889 ExecStart=/bin/bash /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent(코드=종료, 상태=126) 기본 PID: 25889(코드=종료, 상태=126), 8월 3일 21:12:26 데모 systemd[1]: cloudsecure-agent.service: 기본 프로세스가 종료되었습니다. 코드=종료, 상태=126/n/a 8월 3일 21:12:26 데모 systemd[1]: cloudsecure-agent.service 유닛이 실패 상태에 들어갔습니다. 08월 03일 21:12:26 데모 systemd[1]: cloudsecure-agent.service가 실패했습니다.	*cssys* 사용자에게 설치 권한이 없어서 실패할 수 있습니다. /opt/netapp이 NFS 마운트이고 *cssys* 사용자가 이 폴더에 액세스할 수 없는 경우 설치가 실패합니다. *cssys_*는 *Workload Security* 설치 프로그램에서 생성된 로컬 사용자로, 마운트된 공유에 액세스할 권한이 없을 수 있습니다. *_cssys* 사용자를 사용하여 /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent에 액세스를 시도하여 이를 확인할 수 있습니다. "권한 거부됨"이 반환되면 설치 권한이 없습니다. 마운트된 폴더 대신, 머신의 로컬 디렉토리에 설치하세요.

문제:	해결:
에이전트는 처음에 프록시 서버를 통해 연결되었으며, 프록시는 에이전트 설치 중에 설정되었습니다. 이제 프록시 서버가 변경되었습니다. 에이전트의 프록시 구성은 어떻게 변경할 수 있나요?	agent.properties를 편집하여 프록시 세부 정보를 추가할 수 있습니다. 다음 단계를 따르세요. 1. 속성 파일이 있는 폴더로 변경합니다: cd /opt/netapp/cloudsecure/conf 2. 좋아하는 텍스트 편집기를 사용하여 *agent.properties* 파일을 열어 편집합니다. 3. 다음 줄을 추가하거나 수정하세요: AGENT_PROXY_HOST=scspa1950329001.vm.netapp.com AGENT_PROXY_PORT=80 AGENT_PROXY_USER=pxuser AGENT_PROXY_PASSWORD=pass1234 4. 파일을 저장합니다. 5. 에이전트를 다시 시작합니다: sudo systemctl restart cloudsecure-agent.service

워크로드 보안 에이전트 삭제

Workload Security Agent를 삭제하면 먼저 해당 Agent와 연결된 모든 데이터 수집기를 삭제해야 합니다.

에이전트 삭제

에이전트를 삭제하면 해당 에이전트와 연결된 모든 데이터 수집기가 삭제됩니다. 다른 에이전트로 데이터 수집기를 구성하려는 경우 에이전트를 삭제하기 전에 데이터 수집기 구성의 백업을 만들어야 합니다.

시작하기 전에

1. 에이전트와 연결된 모든 데이터 수집기가 워크로드 보안 포털에서 삭제되었는지 확인하세요.

   참고: 연관된 모든 수집기가 STOPPED 상태인 경우 이 단계를 무시하세요.

에이전트를 삭제하는 단계:

1. 에이전트 VM에 SSH로 접속하여 다음 명령을 실행합니다. 메시지가 표시되면 "y"를 입력하여 계속하세요.

   ```
   sudo /opt/netapp/cloudsecure/agent/install/cloudsecure-agent-
   uninstall.sh
   Uninstall CloudSecure Agent? [y|N]:
   ```

2. *워크로드 보안 > 수집기 > 에이전트*를 클릭합니다.

   시스템은 구성된 에이전트 목록을 표시합니다.

3. 삭제할 에이전트의 옵션 메뉴를 클릭합니다.
4. *삭제*를 클릭하세요.

   시스템에 에이전트 삭제 페이지가 표시됩니다.

5. 삭제를 확인하려면 *삭제*를 클릭하세요.

Active Directory(AD) 사용자 디렉터리 수집기 구성

Workload Security는 Active Directory 서버에서 사용자 속성을 수집하도록 구성할 수 있습니다.

시작하기 전에

- 이 작업을 수행하려면 Data Infrastructure Insights 관리자 또는 계정 소유자여야 합니다.
- Active Directory 서버를 호스팅하는 서버의 IP 주소가 있어야 합니다.
- 사용자 디렉토리 커넥터를 구성하기 전에 에이전트를 구성해야 합니다.

사용자 디렉터리 수집기를 구성하는 단계

1. 작업 부하 보안 메뉴에서 *수집기 > 사용자 디렉터리 수집기 > + 사용자 디렉터리 수집기*를 클릭하고 *Active Directory*를 선택합니다.

   시스템에 사용자 디렉토리 추가 화면이 표시됩니다.

다음 표에 필요한 데이터를 입력하여 사용자 디렉토리 수집기를 구성합니다.

이름	설명
이름	사용자 디렉토리의 고유한 이름입니다. 예를 들어 *GlobalADCollector*
대리인	목록에서 구성된 에이전트를 선택하세요
서버 IP/도메인 이름	Active Directory를 호스팅하는 서버의 IP 주소 또는 FQDN(정규화된 도메인 이름)
숲 이름	디렉토리 구조의 포리스트 수준입니다. 포리스트 이름은 다음 두 가지 형식을 모두 허용합니다. *x.y.z* ⇒ SVM에 있는 것과 같은 직접 도메인 이름. [예: hq.companyname.com] *DC=x,DC=y,DC=z* ⇒ 상대적 고유 이름 [예: DC=hq,DC= companyname,DC=com] 또는 다음과 같이 지정할 수 있습니다. *OU=engineering,DC=hq,DC= companyname,DC=com* [특정 OU engineering으로 필터링] *CN=username,OU=engineering,DC=companyname, DC=netapp, DC=com* [OU <engineering>에서 <username>을 가진 특정 사용자만 가져오려면] *CN=Acrobat Users,CN=Users,DC=hq,DC=companyname,DC=com ,O= companyname,L=Boston,S=MA,C=US* [해당 조직의 사용자 내의 모든 Acrobat 사용자를 가져오려면] 신뢰할 수 있는 Active Directory 도메인도 지원됩니다.
DN 바인딩	사용자는 디렉토리를 검색할 수 있습니다. 예: *username@companyname.com* 또는 *username@domainname.com*. 또한 도메인 읽기 전용 권한이 필요합니다. 사용자는 보안 그룹 _읽기 전용 도메인 컨트롤러_의 구성원이어야 합니다.
BIND 비밀번호	디렉토리 서버 비밀번호(즉, Bind DN에 사용되는 사용자 이름에 대한 비밀번호)

규약	ldap, ldaps, ldap-start-tls
포트	포트 선택

Active Directory에서 기본 특성 이름이 수정된 경우 다음 디렉터리 서버 필수 특성을 입력하세요. 대부분의 경우 이러한 속성 이름은 Active Directory에서 수정되지 않습니다. 이 경우 기본 속성 이름을 그대로 사용하면 됩니다.

속성	디렉토리 서버의 속성 이름
표시 이름	이름
시드	객체 ID
사용자 이름	sAMAccountName

다음 속성을 추가하려면 '선택적 속성 포함'을 클릭하세요.

속성	디렉토리 서버의 속성 이름
이메일 주소	우편
전화번호	전화번호
역할	제목
국가	공동
상태	상태
부서	부서
사진	썸네일사진
매니저DN	관리자
여러 떼	멤버의

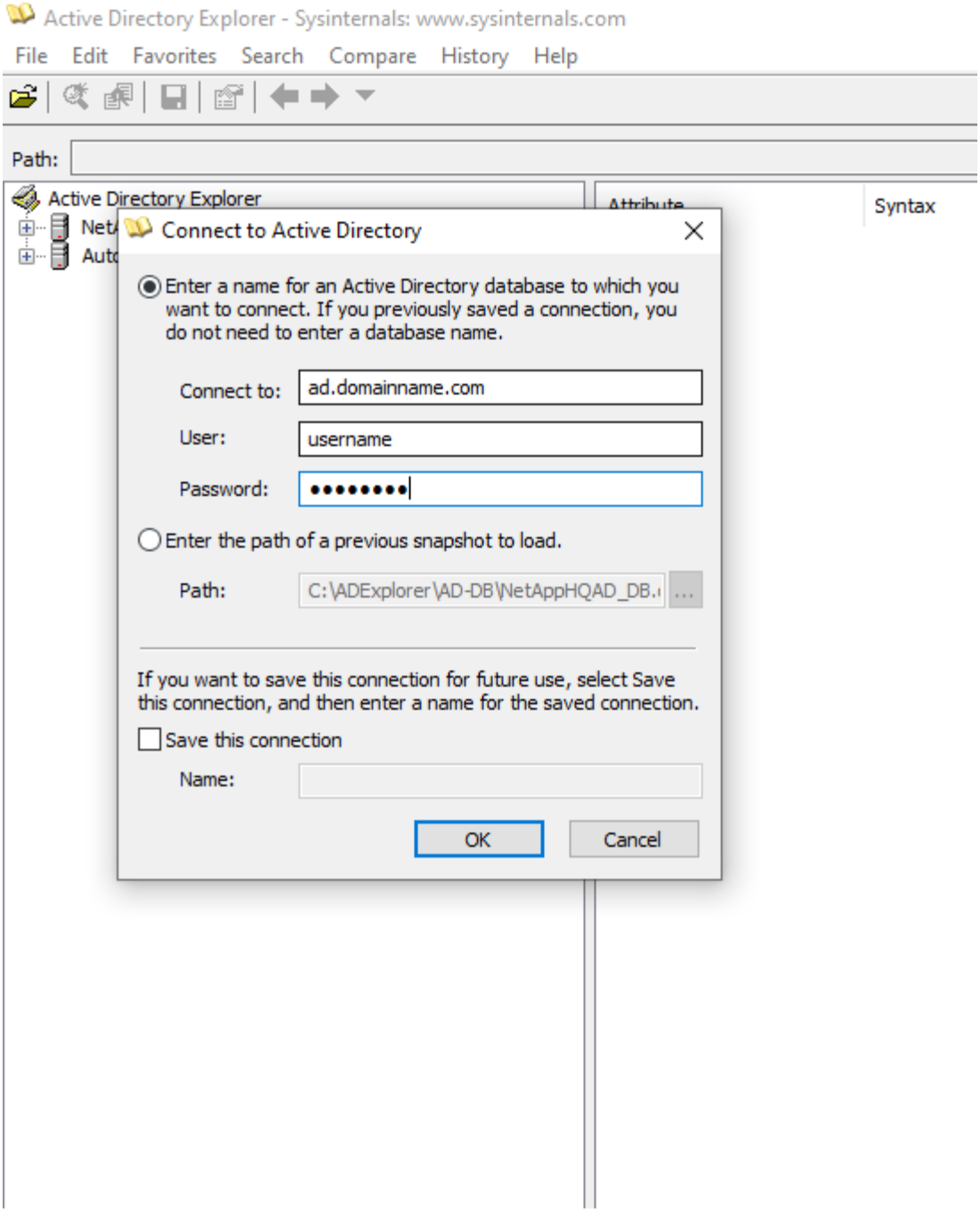
사용자 디렉토리 수집기 구성 테스트

다음 절차를 사용하여 LDAP 사용자 권한 및 속성 정의를 검증할 수 있습니다.

- 다음 명령을 사용하여 Workload Security LDAP 사용자 권한을 확인합니다.

```
ldapsearch -o ldif-wrap=no -LLL -x -b "dc=netapp,dc=com" -h 10.235.40.29 -p
389 -D Administrator@netapp.com -W
```

- AD Explorer를 사용하면 AD 데이터베이스를 탐색하고, 개체 속성 및 특성을 보고, 권한을 보고, 개체의 스키마를 보고, 저장하고 다시 실행할 수 있는 정교한 검색을 실행할 수 있습니다.
  - 설치하다"AD 탐색기" AD 서버에 연결할 수 있는 모든 Windows 컴퓨터에서.
  - AD 디렉토리 서버의 사용자 이름/비밀번호를 사용하여 AD 서버에 연결합니다.



사용자 디렉터리 수집기 구성 오류 문제 해결

다음 표에서는 수집기 구성 중 발생할 수 있는 알려진 문제와 해결 방법을 설명합니다.

문제:	해결:
사용자 디렉토리 커넥터를 추가하면 '오류' 상태가 발생합니다. 오류 메시지는 "LDAP 서버에 잘못된 자격 증명이 제공되었습니다"입니다.	잘못된 사용자 이름이나 비밀번호가 제공되었습니다. 사용자 이름과 비밀번호를 편집하여 올바른 정보를 입력하세요.
사용자 디렉토리 커넥터를 추가하면 '오류' 상태가 발생합니다. 오류 메시지는 "포리스트 이름으로 제공된 DN=DC=hq,DC=domainname,DC=com에 해당하는 개체를 가져오지 못했습니다."입니다.	잘못된 산림 이름이 제공되었습니다. 올바른 산림 이름을 편집하여 입력하세요.

문제:	해결:
도메인 사용자의 선택적 속성이 워크로드 보안 사용자 프로필 페이지에 나타나지 않습니다.	이는 CloudSecure에 추가된 선택적 특성 이름과 Active Directory의 실제 특성 이름이 일치하지 않기 때문일 수 있습니다. 올바른 선택적 속성 이름을 편집하여 제공하세요.
데이터 수집기가 "LDAP 사용자를 검색하지 못했습니다 ."라는 오류 상태에 있습니다. 실패 이유: 서버에 연결할 수 없습니다. 연결이 null입니다.	다시 시작 버튼을 클릭하여 수집기를 다시 시작합니다.
사용자 디렉토리 커넥터를 추가하면 '오류' 상태가 발생합니다.	필수 필드(서버, 포리스트 이름, 바인드 DN, 바인드 비밀번호)에 유효한 값을 제공했는지 확인하세요. bind-DN 입력은 항상 'Administrator@<domain_forest_name>' 또는 도메인 관리자 권한이 있는 사용자 계정으로 제공되어야 합니다.
사용자 디렉토리 커넥터를 추가하면 '재시도 중' 상태가 됩니다. "수집기 상태를 정의할 수 없습니다. 이유: Tcp 명령 [Connect(localhost:35012,None,List(),Some(,seconds) ,true)]이 java.net.ConnectionException:Connection refused로 인해 실패했습니다."라는 오류가 표시됩니다.	AD 서버에 잘못된 IP 또는 FQDN이 제공되었습니다. 올바른 IP 주소나 FQDN을 편집하여 제공하세요.
사용자 디렉토리 커넥터를 추가하면 '오류' 상태가 발생합니다. 오류 메시지는 "LDAP 연결을 설정하지 못했습니다"입니다.	AD 서버에 잘못된 IP 또는 FQDN이 제공되었습니다. 올바른 IP 주소나 FQDN을 편집하여 제공하세요.
사용자 디렉토리 커넥터를 추가하면 '오류' 상태가 발생합니다. 오류 메시지는 "설정을 로드하는 데 실패했습니다."입니다. 이유: 데이터 소스 구성에 오류가 있습니다. 구체적인 이유: /connector/conf/application.conf: 70: ldap.ldap-port에 NUMBER가 아닌 STRING 유형이 있습니다.	제공된 포트에 잘못된 값이 입력되었습니다. AD 서버에 기본 포트 값이나 올바른 포트 번호를 사용해 보세요.
필수 속성부터 시작했는데, 효과가 있었습니다. 선택 항목을 추가한 후, 선택 항목 속성 데이터가 AD에서 가져오지 않습니다.	이는 CloudSecure에 추가된 선택적 특성과 Active Directory의 실제 특성 이름이 일치하지 않기 때문일 수 있습니다. 필수 또는 선택 속성 이름을 편집하여 올바르게 입력하세요.
수집기를 다시 시작한 후 AD 동기화는 언제 발생합니까?	AD 동기화는 수집기가 다시 시작된 직후에 발생합니다. 약 30만 명의 사용자 데이터를 가져오는 데 약 15분이 걸리며, 12시간마다 자동으로 새로 고쳐집니다.
사용자 데이터는 AD에서 CloudSecure로 동기화됩니다. 데이터는 언제 삭제되나요?	새로고침이 없을 경우 사용자 데이터는 13개월 동안 보관됩니다. 세입자가 삭제되면 데이터도 삭제됩니다.
사용자 디렉토리 커넥터가 '오류' 상태를 초래합니다. "커넥터가 오류 상태입니다. 서비스 이름: usersLdap. 실패 이유: LDAP 사용자를 검색하지 못했습니다. 실패 이유: 80090308: LdapErr: DSID-0C090453, 주석: AcceptSecurityContext 오류, 데이터 52e, v3839	잘못된 산림 이름이 제공되었습니다. 올바른 산림 이름을 제공하는 방법은 위를 참조하세요.

문제:	해결:
사용자 프로필 페이지에 전화번호가 입력되지 않습니다.	이는 Active Directory의 속성 매핑 문제로 인해 발생할 가능성이 가장 높습니다. 1. Active Directory에서 사용자 정보를 가져오는 특정 Active Directory 수집기를 편집합니다. 2. 선택적 속성 아래에 Active Directory 속성 'telephonenumber'에 매핑된 필드 이름 "전화번호"가 있습니다. 4. 이제 위에서 설명한 대로 Active Directory Explorer 도구를 사용하여 Active Directory를 탐색하고 올바른 특성 이름을 확인하세요. 3. Active Directory에 사용자의 전화번호를 포함하는 'telephonenumber'라는 특성이 있는지 확인하세요. 5. Active Directory에서 '전화번호'로 수정되었다고 가정해 보겠습니다. 6. 그런 다음 CloudSecure 사용자 디렉터리 수집기를 편집합니다. 선택적인 속성 섹션에서 'telephonenumber'를 'phonenumber'로 바꾸세요. 7. Active Directory 수집기를 저장하면 수집기가 다시 시작되어 사용자의 전화번호를 가져와서 사용자 프로필 페이지에 표시합니다.
Active Directory(AD) 서버에서 암호화 인증서(SSL)가 활성화된 경우 Workload Security User Directory Collector가 AD 서버에 연결할 수 없습니다.	사용자 디렉터리 수집기를 구성하기 전에 AD 서버 암호화를 비활성화합니다. 사용자 세부 정보를 가져오면 13개월 동안 보관됩니다. 사용자 세부 정보를 가져온 후 AD 서버의 연결이 끊어지면 AD에 새로 추가된 사용자를 가져올 수 없습니다. 다시 가져오려면 사용자 디렉토리 수집기를 AD에 연결해야 합니다.
Active Directory의 데이터는 CloudInsights Security에 있습니다. CloudInsights에서 모든 사용자 정보를 삭제하고 싶습니다.	CloudInsights Security에서 Active Directory 사용자 정보만 삭제하는 것은 불가능합니다. 사용자를 삭제하려면 테넌트 전체를 삭제해야 합니다.

LDAP 디렉토리 서버 수집기 구성

LDAP 디렉터리 서버에서 사용자 속성을 수집하도록 Workload Security를 구성합니다.

시작하기 전에

- 이 작업을 수행하려면 Data Infrastructure Insights 관리자 또는 계정 소유자여야 합니다.
- LDAP 디렉토리 서버를 호스팅하는 서버의 IP 주소가 있어야 합니다.
- LDAP 디렉토리 커넥터를 구성하기 전에 에이전트를 구성해야 합니다.

사용자 디렉터리 수집기를 구성하는 단계

1. 작업 부하 보안 메뉴에서 *수집기 > 사용자 디렉터리 수집기 > + 사용자 디렉터리 수집기*를 클릭하고 *LDAP 디렉터리 서버*를 선택합니다.

   시스템에 사용자 디렉토리 추가 화면이 표시됩니다.

다음 표에 필요한 데이터를 입력하여 사용자 디렉토리 수집기를 구성합니다.

이름	설명
이름	사용자 디렉토리의 고유한 이름입니다. 예를 들어 *GlobalLDAPCollector*

대리인	목록에서 구성된 에이전트를 선택하세요
서버 IP/도메인 이름	LDAP 디렉토리 서버를 호스팅하는 서버의 IP 주소 또는 FQDN(정규화된 도메인 이름)
검색 기반	LDAP 서버의 검색 기반 검색 기반은 다음 두 가지 형식을 모두 허용합니다. *x.y.z* ⇒ SVM에 있는 것과 같은 직접 도메인 이름. [예: hq.companyname.com] *DC=x,DC=y,DC=z* ⇒ 상대적 고유 이름 [예: DC=hq,DC= companyname,DC=com] 또는 다음과 같이 지정할 수 있습니다.*OU=engineering,DC=hq,DC= companyname,DC=com* [특정 OU engineering으로 필터링] *CN=username,OU=engineering,DC=companyname, DC=netapp, DC=com* [OU <engineering>에서 <username>을 가진 특정 사용자만 가져오기] *CN=Acrobat Users,CN=Users,DC=hq,DC=companyname,DC=com ,O= companyname,L=Boston,S=MA,C=US* [해당 조직의 사용자 내의 모든 Acrobat 사용자를 가져오기]
DN 바인딩	사용자는 디렉토리를 검색할 수 있습니다. 예: uid=ldapuser, cn=users, cn=accounts, dc=domain, dc=companyname, dc=com uid=john, cn=users, cn=accounts, dc=dorp,dc=company, dc=com (사용자 john@dorp.company.com의 경우)
--계정	--사용자
--남자	--안나
BIND 비밀번호	디렉토리 서버 비밀번호(즉, Bind DN에 사용되는 사용자 이름에 대한 비밀번호)
규약	ldap, ldaps, ldap-start-tls
포트	포트 선택

LDAP 디렉토리 서버에서 기본 속성 이름이 수정된 경우 다음 디렉토리 서버 필수 속성을 입력하세요. 대부분의 경우 이러한 속성 이름은 LDAP 디렉토리 서버에서 수정되지 않습니다. 이 경우 기본 속성 이름을 그대로 사용하면 됩니다.

속성	디렉토리 서버의 속성 이름
표시 이름	이름
유닉스아이디	UID 번호
사용자 이름	액체

다음 속성을 추가하려면 '선택적 속성 포함'을 클릭하세요.

속성	디렉토리 서버의 속성 이름
이메일 주소	우편
전화번호	전화번호
역할	제목

국가	공동
상태	상태
부서	부서 번호
사진	사진
매니저DN	관리자
여러 떼	멤버의

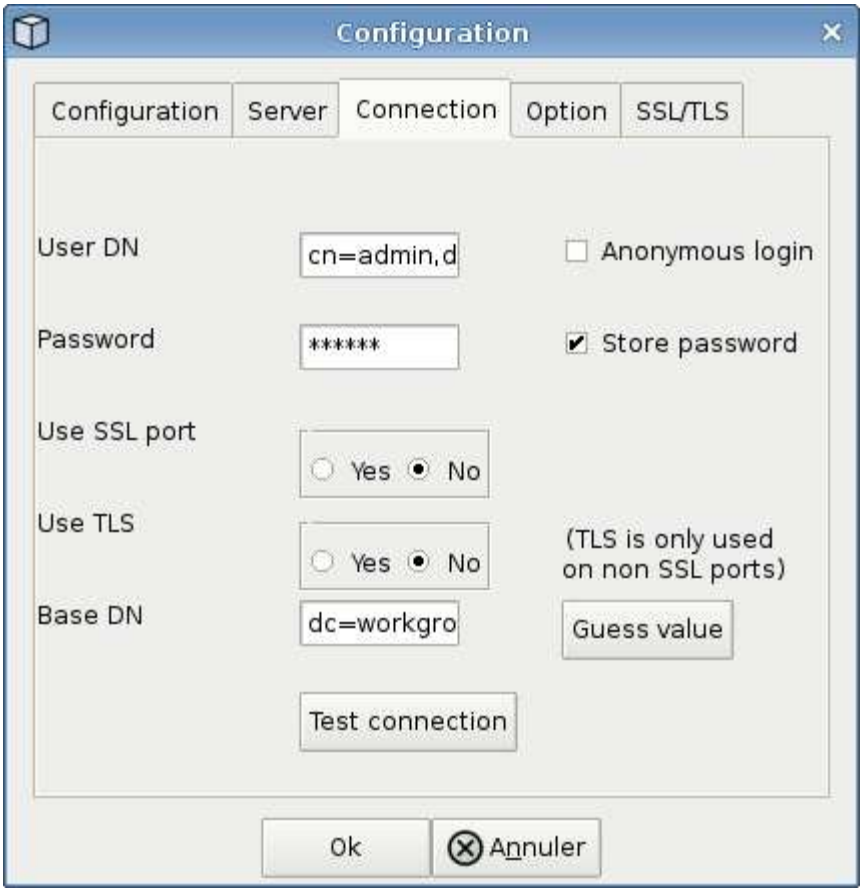
사용자 디렉토리 수집기 구성 테스트

다음 절차를 사용하여 LDAP 사용자 권한 및 속성 정의를 검증할 수 있습니다.

- 다음 명령을 사용하여 Workload Security LDAP 사용자 권한을 확인합니다.

```
 ldapsearch -D "uid=john
,cn=users,cn=accounts,dc=dorp,dc=company,dc=com" -W -x -LLL -o ldif-
wrap=no -b "cn=accounts,dc=dorp,dc=company,dc=com" -H
ldap://vmwipaapp08.dorp.company.com
* LDAP 탐색기를 사용하면 LDAP 데이터베이스를 탐색하고, 개체 속성 및 특성을 보고, 권한을 보고, 개체 스키마를 보고, 저장하고 다시 실행할 수 있는 정교한 검색을 실행할 수 있습니다.
```

  - LDAP 탐색기 설치(http://ldaptool.sourceforge.net/) 또는 Java LDAP 탐색기(http://jxplorer.org/) LDAP 서버에 연결할 수 있는 모든 Windows 컴퓨터에서.
  - LDAP 디렉토리 서버의 사용자 이름/비밀번호를 사용하여 LDAP 서버에 연결합니다.



LDAP 디렉터리 수집기 구성 오류 문제 해결

다음 표에서는 수집기 구성 중 발생할 수 있는 알려진 문제와 해결 방법을 설명합니다.

문제:	해결:
LDAP 디렉토리 커넥터를 추가하면 '오류' 상태가 발생합니다. 오류 메시지는 "LDAP 서버에 잘못된 자격 증명이 제공되었습니다"입니다.	잘못된 바인드 DN, 바인드 비밀번호 또는 검색 기반이 제공되었습니다. 편집하여 올바른 정보를 제공하세요.
LDAP 디렉토리 커넥터를 추가하면 '오류' 상태가 발생합니다. 오류 메시지는 "포리스트 이름으로 제공된 DN=DC=hq,DC=domainname,DC=com에 해당하는 개체를 가져오지 못했습니다."입니다.	잘못된 검색 기준이 제공되었습니다. 올바른 산림 이름을 편집하여 입력하세요.
도메인 사용자의 선택적 속성이 워크로드 보안 사용자 프로필 페이지에 나타나지 않습니다.	이는 CloudSecure에 추가된 선택적 특성 이름과 Active Directory의 실제 특성 이름이 일치하지 않기 때문일 수 있습니다. 필드는 대소문자를 구분합니다. 올바른 선택적 속성 이름을 편집하여 제공하세요.
데이터 수집기가 "LDAP 사용자를 검색하지 못했습니다 ."라는 오류 상태에 있습니다. 실패 이유: 서버에 연결할 수 없습니다. 연결이 null입니다.	다시 시작 버튼을 클릭하여 수집기를 다시 시작합니다.
LDAP 디렉토리 커넥터를 추가하면 '오류' 상태가 발생합니다.	필수 필드(서버, 포리스트 이름, 바인드 DN, 바인드 비밀번호)에 유효한 값을 제공했는지 확인하세요. bind-DN 입력은 항상 uid=ldapuser, cn=users, cn=accounts, dc=domain, dc=companyname, dc=com으로 제공되어야 합니다.

문제:	해결:
LDAP 디렉토리 커넥터를 추가하면 '재시도 중' 상태가 됩니다. "수집기 상태를 확인하지 못했으므로 다시 시도합니다"라는 오류가 표시됩니다.	올바른 서버 IP와 검색 기준이 제공되었는지 확인하세요.
LDAP 디렉토리를 추가하는 동안 다음 오류가 표시됩니다. "2번의 재시도 내에 수집기의 상태를 확인하지 못했습니다. 수집기를 다시 시작해 보세요(오류 코드: AGENT008)"	올바른 서버 IP와 검색 기준이 제공되었는지 확인하세요.
LDAP 디렉토리 커넥터를 추가하면 '재시도 중' 상태가 됩니다. "수집기 상태를 정의할 수 없습니다. 이유: Tcp 명령 [Connect(localhost:35012,None,List(),Some(,seconds),true)]이 java.net.ConnectionException:Connection refused로 인해 실패했습니다."라는 오류가 표시됩니다.	AD 서버에 잘못된 IP 또는 FQDN이 제공되었습니다. 올바른 IP 주소나 FQDN을 편집하여 제공하세요. ////
LDAP 디렉토리 커넥터를 추가하면 '오류' 상태가 발생합니다. 오류 메시지는 "LDAP 연결을 설정하지 못했습니다"입니다.	LDAP 서버에 잘못된 IP 또는 FQDN이 제공되었습니다. 올바른 IP 주소나 FQDN을 편집하여 제공하세요. 또는 제공된 포트에 잘못된 값이 있습니다. LDAP 서버에 기본 포트 값이나 올바른 포트 번호를 사용해 보세요.
LDAP 디렉토리 커넥터를 추가하면 '오류' 상태가 발생합니다. 오류 메시지는 "설정을 로드하는 데 실패했습니다."입니다. 이유: 데이터 소스 구성에 오류가 있습니다. 구체적인 이유: /connector/conf/application.conf: 70: ldap.ldap-port에 NUMBER가 아닌 STRING 유형이 있습니다.	제공된 포트에 잘못된 값이 입력되었습니다. AD 서버에 기본 포트 값이나 올바른 포트 번호를 사용해 보세요.
필수 속성부터 시작했는데, 효과가 있었습니다. 선택 항목을 추가한 후, 선택 항목 속성 데이터가 AD에서 가져오지 않습니다.	이는 CloudSecure에 추가된 선택적 특성과 Active Directory의 실제 특성 이름이 일치하지 않기 때문일 수 있습니다. 필수 또는 선택 속성 이름을 편집하여 올바르게 입력하세요.
수집기를 다시 시작한 후 LDAP 동기화는 언제 발생합니까?	LDAP 동기화는 수집기가 다시 시작된 직후에 수행됩니다. 약 30만 명의 사용자 데이터를 가져오는 데 약 15분이 걸리며, 12시간마다 자동으로 새로 고쳐집니다.
사용자 데이터는 LDAP에서 CloudSecure로 동기화됩니다. 데이터는 언제 삭제되나요?	새로고침이 없을 경우 사용자 데이터는 13개월 동안 보관됩니다. 세입자가 삭제되면 데이터도 삭제됩니다.
LDAP 디렉토리 커넥터가 '오류' 상태를 초래합니다. "커넥터가 오류 상태입니다. 서비스 이름: usersLdap. 실패 이유: LDAP 사용자를 검색하지 못했습니다. 실패 이유: 80090308: LdapErr: DSID-0C090453, 주석: AcceptSecurityContext 오류, 데이터 52e, v3839	잘못된 산림 이름이 제공되었습니다. 올바른 산림 이름을 제공하는 방법은 위를 참조하세요.

문제:	해결:
사용자 프로필 페이지에 전화번호가 입력되지 않습니다.	이는 Active Directory의 속성 매핑 문제로 인해 발생할 가능성이 가장 높습니다. 1. Active Directory에서 사용자 정보를 가져오는 특정 Active Directory 수집기를 편집합니다. 2. 선택적 속성 아래에 Active Directory 속성 'telephonenumber'에 매핑된 필드 이름 "전화번호"가 있습니다. 4. 이제 위에서 설명한 대로 Active Directory Explorer 도구를 사용하여 LDAP 디렉터리 서버를 탐색하고 올바른 속성 이름을 확인하세요. 3. LDAP 디렉토리에 사용자의 전화번호를 포함하는 '전화번호'라는 속성이 있는지 확인하세요. 5. LDAP 디렉토리에서 '전화번호'로 수정되었다고 가정해 보겠습니다. 6. 그런 다음 CloudSecure 사용자 디렉터리 수집기를 편집합니다. 선택적인 속성 섹션에서 'telephonenumber'를 'phonenumber'로 바꾸세요. 7. Active Directory 수집기를 저장하면 수집기가 다시 시작되어 사용자의 전화번호를 가져와서 사용자 프로필 페이지에 표시합니다.
Active Directory(AD) 서버에서 암호화 인증서(SSL)가 활성화된 경우 Workload Security User Directory Collector가 AD 서버에 연결할 수 없습니다.	사용자 디렉터리 수집기를 구성하기 전에 AD 서버 암호화를 비활성화합니다. 사용자 세부 정보를 가져오면 13개월 동안 보관됩니다. 사용자 세부 정보를 가져온 후 AD 서버의 연결이 끊어지면 AD에 새로 추가된 사용자를 가져올 수 없습니다. 다시 사용자 디렉토리 수집기를 가져오려면 AD에 연결해야 합니다.

ONTAP SVM 데이터 수집기 구성

ONTAP SVM 데이터 수집기를 사용하면 Workload Security에서 NetApp ONTAP 스토리지 가상 머신(SVM)의 파일 및 사용자 액세스 활동을 모니터링할 수 있습니다. 이 가이드에서는 ONTAP 환경에 대한 포괄적인 보안 모니터링을 제공하기 위해 SVM 데이터 수집기의 구성과 관리 방법을 안내합니다.

시작하기 전에

- 이 데이터 수집기는 다음과 같은 기능을 지원합니다.
  - Data ONTAP 9.2 및 이후 버전. 최상의 성능을 얻으려면 9.13.1 이상의 Data ONTAP 버전을 사용하세요.
  - SMB 프로토콜 버전 3.1 및 이전 버전.
  - NFS 4.1 이하 NFS 버전(NFS 4.1은 ONTAP 9.15 이상에서 지원됨).
  - Flexgroup은 ONTAP 9.4 이상 버전에서 지원됩니다.
  - FlexCache 는 ONTAP 9.7 이상 버전의 NFS에서 지원됩니다.
  - FlexCache 는 ONTAP 9.14.1 이상 버전의 SMB에서 지원됩니다.
  - ONTAP Select 지원됩니다
- SVM 데이터 유형만 지원됩니다. 무한 볼륨을 가진 SVM은 지원되지 않습니다.
- SVM에는 여러 하위 유형이 있습니다. 이 중에서 *default*, *sync_source*, _sync_destination_만 지원됩니다.
- 에이전트"구성되어야 합니다" 데이터 수집기를 구성하기 전에.

- 사용자 디렉터리 커넥터가 제대로 구성되어 있는지 확인하세요. 그렇지 않으면 이벤트에서 "활동 포렌식" 페이지에 실제 사용자 이름(Active Directory에 저장된 이름)이 아닌 인코딩된 사용자 이름이 표시됩니다.
- ONTAP 영구 저장소는 9.14.1 버전부터 지원됩니다.
- 최적의 성능을 위해서는 FPolicy 서버를 스토리지 시스템과 동일한 서브넷에 구성해야 합니다.
- 워크로드 보안 FPolicy 구성에 대한 포괄적인 모범 사례 및 권장 사항은 다음을 참조하십시오."KB 정책 모범 사례 관련 문서" .
- 다음 두 가지 방법 중 하나를 사용하여 SVM을 추가해야 합니다.
  - 클러스터 IP, SVM 이름, 클러스터 관리 사용자 이름과 비밀번호를 사용합니다. 추천하는 방법입니다.
    - SVM 이름은 ONTAP 에 표시된 대로 정확히 지정해야 하며 대소문자를 구분합니다.
  - SVM Vserver 관리 IP, 사용자 이름 및 비밀번호를 사용하여
  - 전체 관리자 클러스터/SVM 관리 사용자 이름 및 비밀번호를 사용할 수 없거나 사용할 의향이 없는 경우 다음에서 언급한 대로 권한이 낮은 사용자 지정 사용자를 만들 수 있습니다.“권한에 대한 참고 사항” 아래 섹션을 참조하세요. 이 사용자 지정 사용자는 SVM 또는 클러스터 액세스를 위해 생성될 수 있습니다.
    - 아래 "권한에 대한 참고 사항" 섹션에 언급된 것처럼 최소한 csrole 권한을 가진 역할이 있는 AD 사용자를 사용할 수도 있습니다. 또한 다음을 참조하십시오."ONTAP 문서" .
- 다음 명령을 실행하여 SVM에 올바른 애플리케이션이 설정되었는지 확인하세요.

```
clustershell:> security login show -vserver <vservername> -user-or-group
-name <username>
```

출력 예

```
Vserver: svmname
                                                                 Second
User/Group                 Authentication                 Acct   Authentication
Name           Application Method        Role Name        Locked Method
-------------- ----------- ------------- ---------------- ------ --------------
vsadmin        http        password      vsadmin          no     none
vsadmin        ontapi      password      vsadmin          no     none
vsadmin        ssh         password      vsadmin          no     none
3 entries were displayed.
```

- SVM에 CIFS 서버가 구성되어 있는지 확인하세요: clustershell:> `vserver cifs show`

  시스템은 Vserver 이름, CIFS 서버 이름 및 추가 필드를 반환합니다.

- SVM vsadmin 사용자의 비밀번호를 설정합니다. 사용자 정의 사용자 또는 클러스터 관리자 사용자를 사용하는 경우 이 단계를 건너뜁니다. clustershell:> `security login password -username vsadmin -vserver svmname`
- 외부 액세스를 위해 SVM vsadmin 사용자의 잠금을 해제합니다. 사용자 정의 사용자 또는 클러스터 관리자 사용자를 사용하는 경우 이 단계를 건너뜁니다. clustershell:> `security login unlock -username vsadmin -vserver svmname`
- 데이터 LIF의 방화벽 정책이 'mgmt'('data'가 아님)로 설정되어 있는지 확인하세요. 전용 관리 lif를 사용하여 SVM을 추가하는 경우 이 단계를 건너뜁니다. clustershell:> `network interface modify -lif`

```
<SVM_data_LIF_name> -firewall-policy mgmt
```

- 방화벽이 활성화된 경우 Data ONTAP 데이터 수집기를 사용하여 해당 포트에 대한 TCP 트래픽을 허용하기 위한 예외를 정의해야 합니다.

  보다"에이전트 요구 사항" 구성 정보. 이는 온프레미스 에이전트와 클라우드에 설치된 에이전트에 적용됩니다.

- Cloud ONTAP SVM을 모니터링하기 위해 AWS EC2 인스턴스에 에이전트를 설치하는 경우, 에이전트와 스토리지는 동일한 VPC에 있어야 합니다. 서로 다른 VPC에 있는 경우 VPC 간에 유효한 경로가 있어야 합니다.

데이터 수집기를 위한 테스트 연결

테스트 연결 기능(2025년 3월 도입)은 최종 사용자가 Data Infrastructure Insights (DII) 워크로드 보안에서 데이터 수집기를 설정할 때 오류의 구체적인 원인을 식별하는 데 도움을 주는 것을 목표로 합니다. 이를 통해 사용자는 네트워크 통신이나 누락된 역할과 관련된 문제를 스스로 수정할 수 있습니다.

이 기능은 사용자가 데이터 수집기를 설정하기 전에 네트워크 관련 검사가 모두 제대로 수행되었는지 확인하는 데 도움이 됩니다. 또한 ONTAP 버전, 역할 및 ONTAP 에서 할당된 권한에 따라 액세스할 수 있는 기능에 대해 사용자에게 알려줍니다.

ⓘ 사용자 디렉토리 수집기에서는 테스트 연결이 지원되지 않습니다.

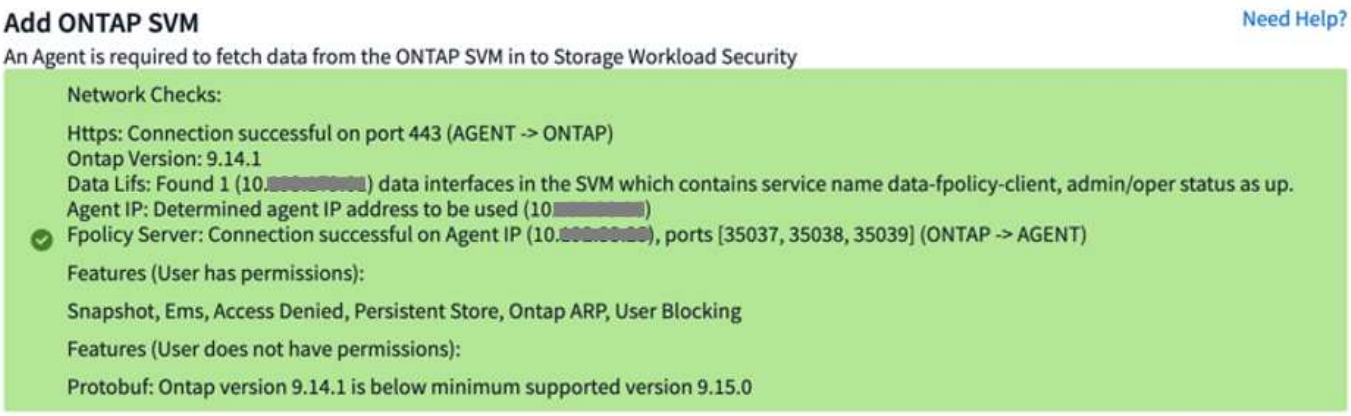
연결 테스트를 위한 전제 조건

- 이 기능을 완벽하게 작동하려면 클러스터 수준 자격 증명이 필요합니다.
- SVM 모드에서는 기능 액세스 검사가 지원되지 않습니다.
- 클러스터 관리 자격 증명을 사용하는 경우 새로운 권한이 필요하지 않습니다.
- 사용자 지정 사용자(예: *csuser*)를 사용하는 경우, 사용하려는 기능에 대한 필수 권한과 기능별 권한을 제공하세요.

반드시 검토하세요권한 아래 섹션도 참조하세요.

연결 테스트

사용자는 수집기 추가/편집 페이지로 이동하여 클러스터 수준 세부 정보(클러스터 모드) 또는 SVM 수준 세부 정보(SVM 모드)를 입력하고 연결 테스트 버튼을 클릭할 수 있습니다. 그러면 Workload Security가 요청을 처리하고 적절한 성공 또는 실패 메시지를 표시합니다.



사용자 액세스 차단을 위한 전제 조건

다음 사항을 염두에 두십시오."사용자 접근 차단" :

이 기능을 사용하려면 클러스터 수준 자격 증명이 필요합니다.

클러스터 관리 자격 증명을 사용하는 경우 새로운 권한이 필요하지 않습니다.

사용자에게 권한이 부여된 사용자 지정 사용자(예: *csuser*)를 사용하는 경우 다음 단계를 따르세요."사용자 접근 차단" Workload Security에 사용자 차단 권한을 부여합니다.

권한에 대한 참고 사항

*클러스터 관리 **IP**를 통해 추가할 때의 권한:

클러스터 관리 관리자 사용자를 사용하여 Workload Security가 ONTAP SVM 데이터 수집기에 액세스하도록 허용할 수 없는 경우 아래 명령에 표시된 역할을 가진 "csuser"라는 새 사용자를 만들 수 있습니다. 워크로드 보안 데이터 수집기를 클러스터 관리 IP를 사용하도록 구성할 때 사용자 이름 "csuser"와 비밀번호 "csuser"를 사용합니다.

참고: 사용자 지정 사용자의 모든 기능 권한에 사용할 단일 역할을 만들 수 있습니다. 기존 사용자가 있는 경우 다음 명령을 사용하여 기존 사용자와 역할을 먼저 삭제합니다.

```
security login delete -user-or-group-name csuser -application *
security login role delete -role csrole -cmddirname *
security login rest-role delete -role csrestrole -api *
security login rest-role delete -role arwrole -api *
```

새로운 사용자를 생성하려면 클러스터 관리 관리자 사용자 이름/비밀번호로 ONTAP 에 로그인하고 ONTAP 서버에서 다음 명령을 실행합니다.

```
security login role create -role csrole -cmddirname DEFAULT -access
readonly
```

```
security login role create -role csrole -cmddirname "vserver fpolicy"
-access all
security login role create -role csrole -cmddirname "volume snapshot"
-access all -query "-snapshot cloudsecure_*"
security login role create -role csrole -cmddirname "event catalog"
-access all
security login role create -role csrole -cmddirname "event filter" -access
all
security login role create -role csrole -cmddirname "event notification
destination" -access all
security login role create -role csrole -cmddirname "event notification"
-access all
security login role create -role csrole -cmddirname "security certificate"
-access all
security login role create -role csrole -cmddirname "cluster application-
record" -access all
security login create -user-or-group-name csuser -application ontapi
-authmethod password -role csrole
security login create -user-or-group-name csuser -application ssh
-authmethod password -role csrole
security login create -user-or-group-name csuser -application http
-authmethod password -role csrole
```

Vserver** 관리 **IP를 통해 추가할 때의 권한**:**

클러스터 관리 관리자 사용자를 사용하여 Workload Security가 ONTAP SVM 데이터 수집기에 액세스하도록 허용할 수 없는 경우 아래 명령에 표시된 역할을 가진 "csuser"라는 새 사용자를 만들 수 있습니다. Workload Security 데이터 수집기를 Vserver 관리 IP를 사용하도록 구성할 때 사용자 이름 "csuser"와 비밀번호 "csuser"를 사용합니다.

참고: 사용자 지정 사용자의 모든 기능 권한에 사용할 단일 역할을 만들 수 있습니다. 기존 사용자가 있는 경우 다음 명령을 사용하여 기존 사용자와 역할을 먼저 삭제합니다.

```
security login delete -user-or-group-name csuser -application * -vserver
<vservername>
security login role delete -role csrole -cmddirname * -vserver
<vservername>
security login rest-role delete -role csrestrole -api * -vserver
<vservername>
```

새로운 사용자를 생성하려면 클러스터 관리 관리자 사용자 이름/비밀번호로 ONTAP 에 로그인하고 ONTAP 서버에서 다음 명령을 실행합니다. 편의를 위해 다음 명령을 텍스트 편집기에 복사하고 ONTAP 에서 다음 명령을 실행하기 전에 <vservername>을 Vserver 이름으로 바꾸세요.

```
security login role create -vserver <vservername> -role csrole -cmddirname
DEFAULT -access none
```

```
security login role create -vserver <vservername> -role csrole -cmddirname
"network interface" -access readonly
security login role create -vserver <vservername> -role csrole -cmddirname
version -access readonly
security login role create -vserver <vservername> -role csrole -cmddirname
volume -access readonly
security login role create -vserver <vservername> -role csrole -cmddirname
vserver -access readonly
```

```
security login role create -vserver <vservername> -role csrole -cmddirname
"vserver fpolicy" -access all
security login role create -vserver <vservername> -role csrole -cmddirname
"volume snapshot" -access all
```

```
security login create -user-or-group-name csuser -application ontapi
-authmethod password -role csrole -vserver <vservername>
security login create -user-or-group-name csuser -application http
-authmethod password -role csrole -vserver <vservername>
```

프로토콜 버퍼 모드

수집기의 고급 구성 설정에서 이 옵션이 활성화된 경우 Workload Security는 FPolicy 엔진을 protobuf 모드로 구성합니다. Protobuf 모드는 ONTAP 버전 9.15 이상에서 지원됩니다.

이 기능에 대한 자세한 내용은 다음에서 확인할 수 있습니다."ONTAP 문서" .

protobuf에는 특정 권한이 필요합니다(이 중 일부 또는 전부가 이미 존재할 수 있음):

클러스터 모드:

```
 security login role create -role csrole -cmddirname "vserver fpolicy"
-access all
Vserver 모드:
```

```
security login role create -vserver <vservername> -role csrole -cmddirname
"vserver fpolicy" -access all
```

ONTAP 자율 랜섬웨어 보호 및 **ONTAP** 액세스에 대한 권한이 거부되었습니다.

클러스터 관리 자격 증명을 사용하는 경우 새로운 권한이 필요하지 않습니다.

사용자 지정 사용자(예: *csuser*)에게 권한이 부여된 경우 아래 단계에 따라 Workload Security에 ONTAP 에서 ARP 관련 정보를 수집할 수 있는 권한을 부여하세요.

자세한 내용은 다음을 읽어보세요."ONTAP 액세스와의 통합이 거부되었습니다."

그리고"ONTAP 자율형 랜섬웨어 보호와 통합"

데이터 수집기 구성

구성 단계

1. Data Infrastructure Insights 환경에 관리자 또는 계정 소유자로 로그인합니다.
2. *워크로드 보안 > 수집기 > +데이터 수집기*를 클릭합니다.

   시스템은 사용 가능한 데이터 수집기를 표시합니다.

3. * NetApp SVM 타일 위에 마우스를 올려놓고 *+모니터*를 클릭합니다.

   시스템에 ONTAP SVM 구성 페이지가 표시됩니다. 각 필드에 필요한 데이터를 입력하세요.

필드	설명
이름	데이터 수집기의 고유 이름
대리인	목록에서 구성된 에이전트를 선택합니다.
관리 IP를 통해 연결:	클러스터 IP 또는 SVM 관리 IP를 선택하세요
클러스터/SVM 관리 IP 주소	위에서 선택한 내용에 따라 클러스터 또는 SVM의 IP 주소가 결정됩니다.
SVM 이름	SVM의 이름(클러스터 IP를 통해 연결할 때 이 필드가 필요합니다)
사용자 이름	SVM/클러스터에 액세스하기 위한 사용자 이름 클러스터 IP를 통해 추가하는 경우 옵션은 다음과 같습니다. 1. 클러스터 관리자 2. 'csuser' 3. AD 사용자는 csuser와 비슷한 역할을 합니다. SVM IP를 통해 추가할 때 옵션은 다음과 같습니다. 4. vsadmin 5. 'csuser' 6. csuser와 비슷한 역할을 하는 AD 사용자 이름입니다.
비밀번호	위 사용자 이름에 대한 비밀번호
공유/볼륨 필터링	이벤트 수집에서 공유/볼륨을 포함할지 또는 제외할지 선택하세요.
제외/포함할 전체 공유 이름을 입력하세요.	이벤트 수집에서 제외하거나 포함할(해당되는 경우) 공유의 쉼표로 구분된 목록
제외/포함할 전체 볼륨 이름을 입력하세요.	이벤트 수집에서 제외하거나 포함할 볼륨의 쉼표로 구분된 목록(해당되는 경우)

폴더 액세스 모니터링	이 옵션을 선택하면 폴더 액세스 모니터링 이벤트가 활성화됩니다. 이 옵션을 선택하지 않아도 폴더 생성/이름 변경 및 삭제가 모니터링됩니다. 이 기능을 활성화하면 모니터링되는 이벤트 수가 늘어납니다.
ONTAP 전송 버퍼 크기 설정	ONTAP Fpolicy 전송 버퍼 크기를 설정합니다. 9.8p7 이전의 ONTAP 버전을 사용하고 성능 문제가 발생하는 경우 ONTAP 전송 버퍼 크기를 변경하여 ONTAP 성능을 향상시킬 수 있습니다. 이 옵션이 보이지 않고 이에 대해 알아보고 싶다면 NetApp 지원팀에 문의하세요.

당신이 완료한 후

- 설치된 데이터 수집기 페이지에서 각 수집기의 오른쪽에 있는 옵션 메뉴를 사용하여 데이터 수집기를 편집합니다. 데이터 수집기를 다시 시작하거나 데이터 수집기 구성 속성을 편집할 수 있습니다.

MetroCluster 에 권장되는 구성

MetroCluster 에 권장되는 사항은 다음과 같습니다.

1. 두 개의 데이터 수집기를 연결합니다. 하나는 소스 SVM에, 다른 하나는 대상 SVM에 연결합니다.
2. 데이터 수집기는 _클러스터 IP_를 통해 연결되어야 합니다.
3. 언제든지 현재 '실행 중인' SVM의 데이터 수집기는 _실행 중_으로 표시됩니다. 현재 '중지된' SVM의 데이터 수집기는 _중지됨_으로 표시됩니다.
4. 전환이 있을 때마다 데이터 수집기의 상태는 _실행 중_에서 _중지됨_으로 변경되고 그 반대의 경우도 마찬가지입니다.
5. 데이터 수집기가 중지 상태에서 실행 상태로 전환하는 데 최대 2분이 걸립니다.

서비스 정책

ONTAP 버전 9.9.1 이상에서 서비스 정책을 사용하는 경우 데이터 소스 수집기에 연결하려면 *data-nfs* 및/또는 *data-cifs* 데이터 서비스와 함께 *data-fpolicy-client* 서비스가 필요합니다.

예:

```
Testcluster-1:*> net int service-policy create -policy only_data_fpolicy
-allowed-addresses 0.0.0.0/0 -vserver aniket_svm
-services data-cifs,data-nfs,data,-core,data-fpolicy-client
(network interface service-policy create)
```

ONTAP 9.9.1 이전 버전에서는 _data-fpolicy-client_를 설정할 필요가 없습니다.

재생**-**일시 정지 데이터 수집기

데이터 수집기가 실행 상태인 경우 수집을 일시 중지할 수 있습니다. 수집기의 "세 개의 점" 메뉴를 열고 일시 중지를 선택합니다. 수집기가 일시 중지된 동안에는 ONTAP 에서 데이터가 수집되지 않고, 수집기에서 ONTAP 으로 데이터가 전송되지 않습니다. 즉, ONTAP 에서 데이터 수집기로 Fpolicy 이벤트가 흐르지 않으며, 거기에서 Data Infrastructure Insights 로 흐르지 않습니다.

수집기가 일시 중지된 동안 ONTAP 에 새로운 볼륨 등이 생성되면 Workload Security가 데이터를 수집하지 않으며 해당 볼륨 등은 대시보드나 표에 반영되지 않습니다.

제한된 사용자가 있는 경우 수집기를 일시 중지할 수 없습니다. 수집기를 일시 중지하기 전에 사용자 액세스를 복원하세요.

다음 사항을 명심하세요.

- 일시 중지된 수집기에 구성된 설정에 따라 스냅샷 정리가 수행되지 않습니다.
- 일시 중지된 수집기에서는 EMS 이벤트(ONTAP ARP 등)가 처리되지 않습니다. 즉, ONTAP 랜섬웨어 공격을 식별하더라도 Data Infrastructure Insights Workload Security는 해당 이벤트를 수집할 수 없습니다.
- 일시 중지된 수집자에게는 건강 알림 이메일이 전송되지 않습니다.
- 일시 중지된 수집기에서는 수동 또는 자동 작업(스냅샷이나 사용자 차단 등)이 지원되지 않습니다.
- 에이전트 또는 수집기 업그레이드, 에이전트 VM 재시작/재부팅 또는 에이전트 서비스 재시작 시 일시 중지된 수집기는 일시 중지 상태로 유지됩니다.
- 데이터 수집기가 *Error* 상태인 경우 수집기를 *Paused* 상태로 변경할 수 없습니다. 일시 중지 버튼은 수집기 상태가 _실행 중_인 경우에만 활성화됩니다.
- 에이전트가 연결이 끊어지면 수집기를 일시 중지 상태로 변경할 수 없습니다. 수집기는 중지 상태로 전환되고 일시 중지 버튼이 비활성화됩니다.

영구 저장소

영구 저장소는 ONTAP 9.14.1 이상에서 지원됩니다. 볼륨 이름 지침은 ONTAP 9.14에서 9.15로 다릅니다.

영구 저장소는 수집기 편집/추가 페이지에서 확인란을 선택하여 활성화할 수 있습니다. 체크박스를 선택하면 볼륨 이름을 입력할 수 있는 텍스트 필드가 표시됩니다. 볼륨 이름은 영구 저장소를 활성화하는 데 필요한 필수 필드입니다.

- ONTAP 9.14.1의 경우 기능을 활성화하기 전에 볼륨을 생성하고 볼륨 이름 필드에 동일한 이름을 제공해야 합니다. 권장되는 볼륨 크기는 16GB입니다.
- ONTAP 9.15.1의 경우 볼륨은 볼륨 이름 필드에 제공된 이름을 사용하여 수집기에 의해 16GB 크기로 자동 생성됩니다.

영구 저장소에는 특정 권한이 필요합니다(이 중 일부 또는 전부가 이미 존재할 수 있음):

클러스터 모드:

```
security login role create -role csrole -cmddirname "vserver fpolicy"
-access all
security login role create -role csrole -cmddirname "job show" -access
readonly
```

Vserver 모드:

```
security login role create -vserver <vservername> -role csrole -cmddirname
"vserver fpolicy" -access all
security login role create -vserver <vservername> -role csrole -cmddirname
"job show" -access readonly
```

수집기 마이그레이션

한 에이전트에서 다른 에이전트로 Workload Security 수집기를 쉽게 마이그레이션하여 에이전트 간에 수집기의 부하를 효율적으로 분산할 수 있습니다.

필수 조건

- 소스 에이전트는 연결 상태여야 합니다.
- 마이그레이션할 수집기는 실행 상태여야 합니다.

메모:

- 마이그레이션은 데이터 및 사용자 디렉토리 수집기 모두에서 지원됩니다.
- 수동으로 관리되는 테넌트의 경우 수집기 마이그레이션이 지원되지 않습니다.

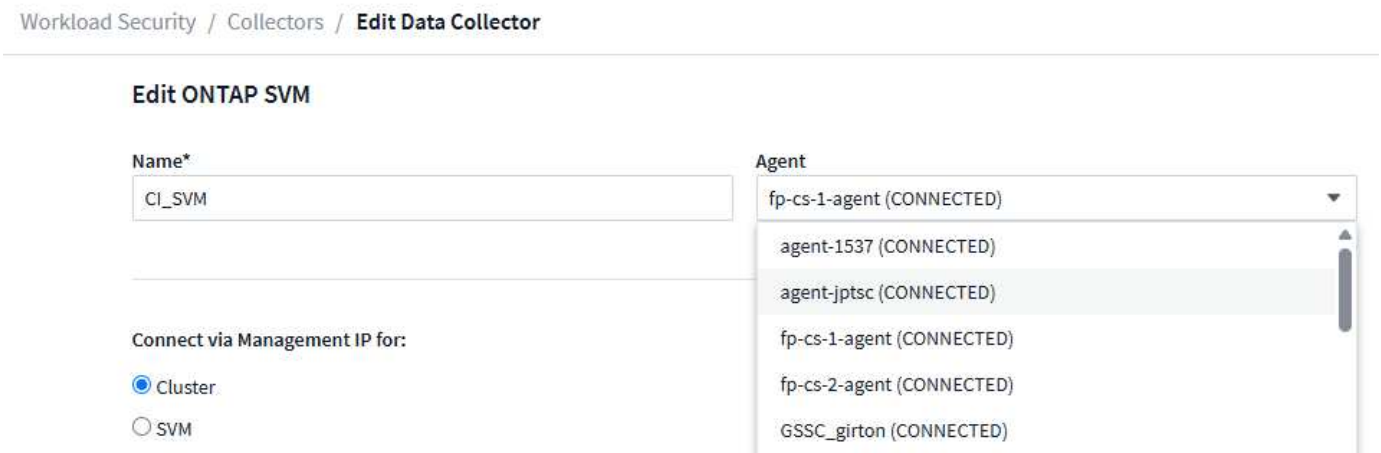
수집기 마이그레이션

수집기를 마이그레이션하려면 다음 단계를 따르세요.

1. "수집기 편집" 페이지로 이동합니다.
2. 에이전트 드롭다운에서 목적지 에이전트를 선택하세요.
3. "수집기 저장" 버튼을 클릭하세요.

워크로드 보안이 요청을 처리합니다. 마이그레이션이 성공적으로 완료되면 사용자는 수집자 목록 페이지로 리디렉션됩니다. 실패할 경우, 편집 페이지에 해당 메시지가 표시됩니다.

참고: 이전에 "수집기 편집" 페이지에서 변경한 모든 구성 내용은 수집기가 대상 에이전트로 성공적으로 마이그레이션되면 그대로 적용됩니다.



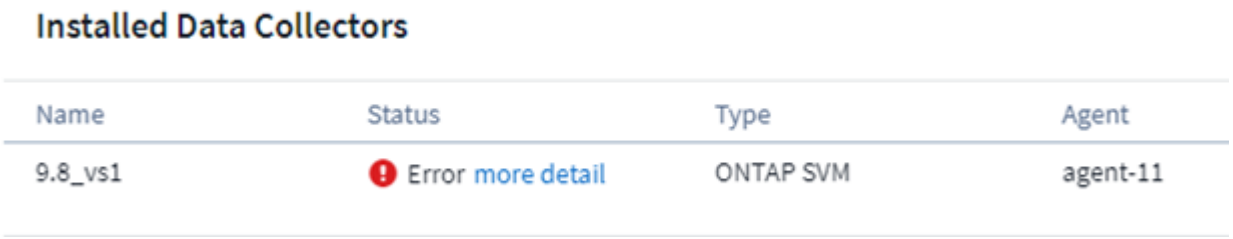
를 참조하십시오"SVM 수집기 문제 해결" 문제 해결 팁을 보려면 여기를 클릭하세요.

ONTAP SVM 데이터 수집기 문제 해결

워크로드 보안은 데이터 수집기를 사용하여 장치에서 파일 및 사용자 액세스 데이터를 수집합니다. 여기에서는 이 수집기와 관련된 문제를 해결하기 위한 팁을 찾을 수 있습니다.

를 참조하십시오"SVM 수집기 구성" 이 수집기를 구성하는 방법에 대한 지침은 페이지를 참조하세요.

오류가 발생한 경우, 설치된 데이터 수집기 페이지의 상태 열에서 _자세한 내용_을 클릭하면 오류에 대한 자세한 내용을 볼 수 있습니다.



알려진 문제와 해결 방법은 아래와 같습니다.

문제: 데이터 수집기가 잠시 실행되다가 임의의 시간 후에 중지되고 "오류 메시지: 커넥터가 오류 상태입니다."라는 오류 메시지가 나타납니다. 서비스 이름: 감사. 실패 이유: 외부 fpolicy 서버가 과부하되었습니다. 다음을 시도해 보세요. ONTAP 의 이벤트 비율은 에이전트 상자가 처리할 수 있는 것보다 훨씬 높았습니다. 그래서 연결이 종료되었습니다.

연결이 끊어졌을 때 CloudSecure에서 최대 트래픽을 확인하세요. **CloudSecure >** 활동 포렌식 **>** 모든 활동 페이지에서 확인할 수 있습니다.

최대 집계 트래픽이 Agent Box에서 처리할 수 있는 것보다 높은 경우 Agent Box에서 Collector 배포 크기를 조정하는 방법에 대한 이벤트 속도 검사기 페이지를 참조하세요.

2021년 3월 4일 이전에 에이전트가 에이전트 상자에 설치된 경우 에이전트 상자에서 다음 명령을 실행하세요.

```
echo 'net.core.rmem_max=8388608' >> /etc/sysctl.conf
echo 'net.ipv4.tcp_rmem = 4096 2097152 8388608' >> /etc/sysctl.conf
sysctl -p
```

크기를 조정한 후 UI에서 수집기를 다시 시작합니다.

{비어 있는}

문제: 수집기에서 "SVM의 데이터 인터페이스에 도달할 수 있는 커넥터에서 로컬 IP 주소를 찾을 수 없습니다"라는 오류 메시지가 보고됩니다. 다음을 시도해 보세요: 이는 ONTAP 측의 네트워킹 문제로 인해 발생할 가능성이 가장 높습니다.

다음 단계를 따르세요.

1. SVM 데이터 영역이나 관리 영역에 SVM의 연결을 차단하는 방화벽이 없는지 확인하세요.
2. 클러스터 관리 IP를 통해 SVM을 추가하는 경우 에이전트 VM에서 SVM의 데이터 레벨과 관리 레벨에 ping을 보낼 수 있는지 확인하세요. 문제가 발생한 경우, 해당 게이트웨이, 넷마스크, 경로를 확인하세요.

   클러스터 관리 IP를 사용하여 ssh를 통해 클러스터에 로그인하고 에이전트 IP를 ping해 볼 수도 있습니다. 에이전트 IP가 ping 가능한지 확인하세요.

   ```
   network ping -vserver <vserver name> -destination <Agent IP> -lif <Lif Name> -show-detail
   ```

   ping을 사용할 수 없는 경우 ONTAP 의 네트워크 설정이 올바른지 확인하여 Agent 머신이 ping을 사용할 수 있도록 하세요.

3. 클러스터 IP를 통해 연결을 시도했지만 작동하지 않는 경우 SVM IP를 통해 직접 연결을 시도하세요. SVM IP를 통해 연결하는 단계는 위를 참조하세요.
4. SVM IP 및 vsadmin 자격 증명을 통해 수집기를 추가하는 동안 SVM Lif에 데이터 및 관리 역할이 활성화되어 있는지 확인하세요. 이 경우 SVM Lif에 대한 ping은 작동하지만 SVM Lif에 대한 SSH는 작동하지 않습니다. 그렇다면 SVM 관리 전용 Lif를 만들고 이 SVM 관리 전용 Lif를 통해 연결을 시도하세요.
5. 그래도 작동하지 않는다면 새로운 SVM Lif를 생성하고 해당 Lif를 통해 연결을 시도해보세요. 서브넷 마스크가 올바르게 설정되었는지 확인하세요.
6. 고급 디버깅:
   a. ONTAP 에서 패킷 추적을 시작합니다.
   b. CloudSecure UI에서 SVM에 데이터 수집기를 연결해 보세요.
   c. 오류가 나타날 때까지 기다리세요. ONTAP 에서 패킷 추적을 중지합니다.
   d. ONTAP 에서 패킷 추적을 엽니다. 이 위치에서 사용 가능합니다

      ```
      https://<cluster_mgmt_ip>/spi/<clustername>/etc/log/packet_traces/
      .. ONTAP 에서 Agent 상자로 SYN이 있는지 확인하세요.
      .. ONTAP 에서 SYN이 없으면 ONTAP 의 방화벽에 문제가 있습니다.
      .. ONTAP 에서 방화벽을 열어 ONTAP 에이전트 상자에 연결할 수 있도록 합니다.
      ```

7. 그래도 작동하지 않으면 네트워킹 팀에 문의하여 외부 방화벽이 ONTAP 에서 Agent 상자로의 연결을 차단하고 있지 않은지 확인하세요.
8. 위의 방법으로도 문제가 해결되지 않으면 사례를 열어주세요."넷앱 지원" 추가 지원이 필요하면.

{비어 있는}

문제**:** 메시지: "[호스트 이름: <IP 주소>에 대한 ONTAP 유형을 확인하지 못했습니다. 이유: 스토리지 시스템 <IP 주소>에 대한 연결 오류: 호스트에 접근할 수 없습니다(Host unreachable)" 다음을 시도해 보세요**:**

---

1. 올바른 SVM IP 관리 주소 또는 클러스터 관리 IP가 제공되었는지 확인하세요.
2. 연결하려는 SVM이나 클러스터에 SSH를 실행합니다. 연결되면 SVM 또는 클러스터 이름이 올바른지 확인하세요.

{비어 있는}

문제**:** 오류 메시지: "커넥터가 오류 상태입니다. 서비스 이름: 감사. 실패 이유: 외부 fpolicy 서버가 종료되었습니다. 이걸 시도해보세요**:**

1. 방화벽이 에이전트 머신의 필수 포트를 차단하고 있을 가능성이 큽니다. 에이전트 머신이 SVM에서 연결할 수 있도록 포트 범위 35000-55000/tcp가 열려 있는지 확인하세요. 또한 ONTAP 측에서 에이전트 머신과의 통신을 차단하는 방화벽이 활성화되어 있지 않은지 확인하세요.
2. 에이전트 상자에 다음 명령을 입력하고 포트 범위가 열려 있는지 확인하세요.

   ```
   sudo iptables-save | grep 3500*
   ```

   샘플 출력은 다음과 같습니다.

   ```
    -A IN_public_allow -p tcp -m tcp --dport 35000 -m conntrack -ctstate
   NEW -j ACCEPT
   . SVM에 로그인하고 다음 명령을 입력한 후 ONTAP 과의 통신을 차단하는 방화벽이 설정되어 있지 않은지 확인합니다.
   ```

   ```
   system services firewall show
   system services firewall policy show
   ```

   "방화벽 명령 확인"ONTAP 측에서.

3. 모니터링하려는 SVM/클러스터에 SSH를 실행합니다. SVM 데이터 lif(CIFS, NFS 프로토콜 지원)에서 Agent 상자에 ping을 보내고 ping이 작동하는지 확인합니다.

   ```
   network ping -vserver <vserver name> -destination <Agent IP> -lif <Lif
   Name> -show-detail
   ```

   ping을 사용할 수 없는 경우 ONTAP 의 네트워크 설정이 올바른지 확인하여 Agent 머신이 ping을 사용할 수 있도록 하세요.

4. 2개의 데이터 수집기를 통해 하나의 SVM이 테넌트에 두 번 추가되면 이 오류가 표시됩니다. UI를 통해 데이터 수집기 중 하나를 삭제합니다. 그런 다음 UI를 통해 다른 데이터 수집기를 다시 시작합니다. 그러면 데이터 수집기가 "실행 중" 상태를 표시하고 SVM에서 이벤트를 수신하기 시작합니다.

   기본적으로 테넌트에서는 1개의 SVM이 1개의 데이터 수집기를 통해 한 번만 추가되어야 합니다. 1 SVM은 2개의 데이터 수집기를 통해 두 번 추가되어서는 안 됩니다.

5. 두 개의 서로 다른 워크로드 보안 환경(테넌트)에 동일한 SVM이 추가된 경우, 항상 마지막에 추가된 SVM이 성공합니다. 두 번째 수집기는 자체 IP 주소로 fpolicy를 구성하고 첫 번째 수집기를 제거합니다. 따라서 첫 번째 수집기는 이벤트 수신을 중단하고 해당 "감사" 서비스는 오류 상태로 전환됩니다. 이를 방지하려면 각 SVM을 단일 환경에 구성하세요.
6. 서비스 정책이 올바르게 구성되지 않은 경우에도 이 오류가 발생할 수 있습니다. ONTAP 9.8 이상에서 데이터 소스 수집기에 연결하려면 data-nfs 및/또는 data-cifs 데이터 서비스와 함께 data-fpolicy-client 서비스가 필요합니다. 또한, data-fpolicy-client 서비스는 모니터링되는 SVM의 데이터 라이프와 연결되어야 합니다.

{비어 있는}

문제: 활동 페이지에서 이벤트가 보이지 않습니다. 이걸 시도해보세요:

1. ONTAP 수집기가 "실행 중" 상태인지 확인하세요. 그렇다면 일부 파일을 열어서 cifs 클라이언트 VM에서 일부 cifs 이벤트가 생성되는지 확인하세요.
2. 활동이 보이지 않으면 SVM에 로그인하여 다음 명령을 입력하세요.

   ```
   <SVM>event log show -source fpolicy
   ```

   fpolicy와 관련된 오류가 없는지 확인하세요.

3. 활동이 보이지 않으면 SVM에 로그인하세요. 다음 명령을 입력하세요:

   ```
   <SVM>fpolicy show
   ```

   "cloudsecure_" 접두사가 붙은 fpolicy 정책이 설정되었고 상태가 "on"인지 확인하세요. 설정하지 않으면 에이전트가 SVM에서 명령을 실행할 수 없을 가능성이 큽니다. 이 페이지의 시작 부분에 설명된 모든 전제 조건이 충족되었는지 확인하세요.

{비어 있는}

문제: SVM 데이터 수집기가 오류 상태이며 오류 메시지는 "에이전트가 수집기에 연결하지 못했습니다"입니다. 다음을 시도해 보세요.

1. 에이전트가 과부하되어 데이터 소스 수집기에 연결할 수 없는 것 같습니다.
2. 에이전트에 연결된 데이터 소스 수집기의 수를 확인합니다.
3. 또한 UI의 "모든 활동" 페이지에서 데이터 흐름 속도를 확인하세요.
4. 초당 활동 수가 상당히 높은 경우 다른 에이전트를 설치하고 일부 데이터 소스 수집기를 새 에이전트로 이동합니다.

{비어 있는}

문제: SVM 데이터 수집기가 "fpolicy.server.connectError: 노드가 FPolicy 서버 "12.195.15.146"과 연결을 설정하지

못했습니다(이유: "선택 시간 초과")"라는 오류 메시지를 표시합니다. 다음을 시도해 보세요**:** SVM/클러스터에서 방화벽이 활성화되어 있습니다. 따라서 fpolicy 엔진이 fpolicy 서버에 연결할 수 없습니다. 더 많은 정보를 얻는 데 사용할 수 있는 ONTAP 의 CLI는 다음과 같습니다.

```
event log show -source fpolicy which shows the error
event log show -source fpolicy -fields event,action,description which
shows more details.
```

"방화벽 명령 확인"ONTAP 측에서.

{비어 있는}

문제**:** 오류 메시지: "커넥터가 오류 상태입니다. 서비스 이름: 감사. 실패 이유: SVM에서 유효한 데이터 인터페이스(역할: 데이터, 데이터 프로토콜: NFS 또는 CIFS 또는 둘 다, 상태: 작동)를 찾을 수 없습니다. 다음을 시도해 보세요**.** CIFS/NFS로서 데이터 역할과 데이터 프로토콜을 갖는 운영 인터페이스가 있는지 확인하세요.

{비어 있는}

문제**:** 데이터 수집기가 오류 상태로 전환된 후 얼마 후 실행 상태로 전환되고 다시 오류 상태로 돌아갑니다. 이런 순환이 반복됩니다. 다음을 시도해 보세요**:** 이는 일반적으로 다음 시나리오에서 발생합니다.

1. 여러 개의 데이터 수집기가 추가되었습니다.
2. 이런 종류의 행동을 보이는 데이터 수집기에는 해당 데이터 수집기에 1개의 SVM이 추가됩니다. 즉, 2개 이상의 데이터 수집기가 1개의 SVM에 연결되어 있습니다.
3. 1개의 데이터 수집기가 1개의 SVM에만 연결되도록 하세요.
4. 동일한 SVM에 연결된 다른 데이터 수집기를 삭제합니다.

{비어 있는}

문제**:** 커넥터가 오류 상태입니다. 서비스 이름: 감사. 실패 이유: (SVM svmname에 대한 정책을 구성하지 못했습니다.) 이유: 'fpolicy.policy.scope-modify: "Federal" 내의 'shares-to-include' 요소에 잘못된 값이 지정되었습니다. 다음을 시도해 보세요**.** *공유 이름은 따옴표 없이 지정해야 합니다. ONTAP SVM DSC 구성을 편집하여 공유 이름을 수정합니다.

_주식 포함 및 제외_는 긴 주식 이름 목록에는 적용되지 않습니다. 포함하거나 제외할 주식 수가 많은 경우 대신 거래량별 필터링을 사용하세요.

{비어 있는}

문제**:** 클러스터에 사용되지 않는 기존 fpolicies가 있습니다. Workload Security를 설치하기 전에 무엇을 해야 합니까? 다음을 시도해 보세요**.** 연결이 끊긴 상태라도 기존의 사용되지 않는 모든 fpolicy 설정을 삭제하는 것이 좋습니다. Workload Security는 "cloudsecure_" 접두사로 fpolicy를 생성합니다. 나머지 사용되지 않는 fpolicy 구성은 모두

삭제할 수 있습니다.

fpolicy 목록을 표시하는 CLI 명령:

```
 fpolicy show
fpolicy 구성을 삭제하는 단계:
```

```
fpolicy disable -vserver <svmname> -policy-name <policy_name>
fpolicy policy scope delete -vserver <svmname> -policy-name <policy_name>
fpolicy policy delete -vserver <svmname> -policy-name <policy_name>
fpolicy policy event delete -vserver <svmname> -event-name <event_list>
fpolicy policy external-engine delete -vserver <svmname> -engine-name
<engine_name>
```

{비어 있는}

문제점: 워크로드 보안을 활성화한 후 ONTAP 성능에 문제가 발생합니다. 지연 시간이 간헐적으로 높아지고, IOP가 간헐적으로 낮아집니다. 다음과 같이 시도해 보세요: ONTAP 워크로드 보안과 함께 사용할 때 ONTAP 에서 지연 문제가 발생할 수 있습니다. 다음과 같이 몇 가지 가능한 이유가 있습니다."1372994" , "1415152" , "1438207" , "1479704" , "1354659" . 이러한 문제는 모두 ONTAP 9.13.1 이상에서 해결되었습니다. 이후 버전 중 하나를 사용하는 것이 좋습니다.

{비어 있는}

문제: 데이터 수집기에서 다음 오류 메시지가 표시됩니다. "오류: 2번의 재시도 내에 수집기의 상태를 확인하지 못했습니다. 수집기를 다시 시작해 보세요(오류 코드: AGENT008)". 이걸 시도해보세요:

1. 데이터 수집기 페이지에서 오류가 발생한 데이터 수집기의 오른쪽으로 스크롤하여 3개 점 메뉴를 클릭합니다. 편집 _을 선택하세요. 데이터 수집기의 비밀번호를 다시 입력하세요. _저장 버튼을 눌러 데이터 수집기를 저장합니다. 데이터 수집기가 다시 시작되면 오류가 해결될 것입니다.
2. 에이전트 머신에는 CPU나 RAM 여유 공간이 충분하지 않아 DSC가 실패하는 것입니다. 머신의 에이전트에 추가된 데이터 수집기의 수를 확인하세요. 20이 넘을 경우, Agent 머신의 CPU와 RAM 용량을 늘려주세요. CPU와 RAM이 늘어나면 DSC는 초기화 상태로 전환되고, 그다음에는 자동으로 실행 상태로 전환됩니다. 사이즈 가이드를 살펴보세요"이 페이지" .

{비어 있는}

문제: SVM 모드를 선택하면 데이터 수집기에서 오류가 발생합니다. 다음을 시도해 보세요. SVM 모드에서 연결하는 동안 SVM 관리 IP 대신 클러스터 관리 IP를 사용하여 연결하면 연결 오류가 발생합니다. 올바른 SVM IP가 사용되었는지 확인하세요.

{비어 있는}

문제**:** 액세스 거부 기능이 활성화된 경우 데이터 수집기에서 "커넥터가 오류 상태입니다."라는 오류 메시지가 표시됩니다. 서비스 이름: 감사. 실패 이유: SVM test_svm에서 fpolicy를 구성하지 못했습니다. 사유: 사용자에게 권한이 없습니다. 다음을 시도해 보세요**.** 사용자에게 액세스 거부 기능에 필요한 REST 권한이 없을 수 있습니다. 다음 지침을 따르십시오."이 페이지" 권한을 설정하려면.

권한이 설정되면 수집기를 다시 시작합니다.

{비어 있는}

문제**:** 컬렉터가 "커넥터가 오류 상태입니다"라는 메시지와 함께 오류 상태에 있습니다. 실패 원인: SVM <SVM 이름>에 영구 저장소를 구성하는 데 실패했습니다. 이유: SVM "<SVM 이름>"에서 볼륨 "<볼륨 이름>"에 적합한 집계를 찾을 수 없습니다. 이유: 현재 집계 "<aggregateName>"에 대한 성능 정보를 사용할 수 없습니다. 몇 분 기다렸다가 명령어를 다시 시도해 보세요. 서비스 이름: 감사. 실패 이유: SVM에서 영구 저장소를 구성하지 못했습니다 <svm name="">.</svm> 이유: <volumename>SVM "<svm name="">"</svm>에서</volumename> 볼륨 ""에 적합한 애그리게이트를 찾을 수 없습니다. 이유: 애그리게이트 ""에 대한 성능 정보를 <aggregatename>현재 사용할 수 없습니다.</aggregatename> 몇 분 정도 기다렸다가 명령을 다시 시도하십시오.

다음 방법을 시도해 보세요**:** 몇 분 정도 기다린 후 수집기를 다시 시작하세요.

{비어 있는}

여전히 문제가 발생하는 경우, 도움말 **>** 지원 페이지에 언급된 지원 링크로 문의하세요.

Amazon FSx for NetApp ONTAP Cloud Volumes ONTAP 및 Amazon FSx 구성

Cloud Volumes ONTAP 및 Amazon FSx for NetApp ONTAP 용 워크로드 보안 데이터 수집기를 구성하여 클라우드 스토리지 인프라 전반의 파일 및 사용자 액세스를 모니터링하세요. 이 가이드는 AWS에 에이전트를 배포하고 클라우드 스토리지 인스턴스에 연결하는 방법에 대한 단계별 지침을 제공합니다.

Cloud Volumes ONTAP 스토리지 구성

Workload Security Agent를 호스팅하기 위해 단일 노드/HA AWS 인스턴스를 구성하려면 OnCommand Cloud Volumes ONTAP 설명서를 참조하세요.https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/index.html[]

구성이 완료되면 다음 단계에 따라 SVM을 설정하세요.https://docs.netapp.com/us-en/cloudinsights/task_add_collector_svm.html[]

지원 플랫폼

- Cloud Volumes ONTAP 사용 가능한 모든 클라우드 서비스 제공업체에서 지원됩니다. 예를 들어: Amazon, Azure, Google Cloud.
- ONTAP Amazon FSx

에이전트 머신 구성

에이전트 머신은 클라우드 서비스 공급자의 해당 서브넷에 구성되어야 합니다. [에이전트 요구 사항]에서 네트워크 액세스에 대한 자세한 내용을 읽어보세요.

AWS에 에이전트를 설치하는 단계는 다음과 같습니다. 클라우드 서비스 제공업체에 적용되는 동등한 단계는 Azure 또는 Google Cloud에서 설치를 위해 따를 수 있습니다.

AWS에서 다음 단계에 따라 워크로드 보안 에이전트로 사용할 머신을 구성합니다.

다음 단계에 따라 워크로드 보안 에이전트로 사용할 머신을 구성하세요.

단계

1. AWS 콘솔에 로그인하고 EC2-Instances 페이지로 이동하여 _인스턴스 시작_을 선택합니다.
2. 이 페이지에 언급된 대로 적절한 버전의 RHEL 또는 CentOS AMI를 선택하세요:https://docs.netapp.com/us-en/cloudinsights/concept_cs_agent_requirements.html[]
3. Cloud ONTAP 인스턴스가 있는 VPC와 서브넷을 선택합니다.
4. 할당된 리소스로 *t2.xlarge* (4개의 vcpus와 16GB RAM)를 선택합니다.
    a. EC2 인스턴스를 생성합니다.
5. YUM 패키지 관리자를 사용하여 필요한 Linux 패키지를 설치합니다.
    a. *wget*_과 _*unzip* 네이티브 Linux 패키지를 설치합니다.

Workload Security Agent 설치

1. Data Infrastructure Insights 환경에 관리자 또는 계정 소유자로 로그인합니다.
2. 워크로드 보안 수집기*로 이동하여 *에이전트 탭을 클릭합니다.
3. *+에이전트*를 클릭하고 대상 플랫폼으로 RHEL을 지정합니다.
4. 에이전트 설치 명령을 복사합니다.
5. 로그인한 RHEL EC2 인스턴스에 에이전트 설치 명령을 붙여넣습니다. 이렇게 하면 Workload Security 에이전트가 설치되고 모든 것이 제공됩니다."에이전트 전제 조건" 충족됩니다.

자세한 단계는 다음 링크를 참조하세요: https://docs.netapp.com/us-en/cloudinsights/task_cs_add_agent.html#steps-to-install-agent

문제 해결

알려진 문제와 해결 방법은 다음 표에 설명되어 있습니다.

문제	해결

데이터 수집기에서 "워크로드 보안: Amazon FxSN 데이터 수집기의 ONTAP 유형을 확인하지 못했습니다" 오류가 표시됩니다. 고객이 Workload Security에 새로운 Amazon FSxN 데이터 수집기를 추가할 수 없습니다. 에이전트에서 포트 443을 통해 FSxN 클러스터에 연결하는 데 시간이 초과되었습니다. 방화벽과 AWS 보안 그룹에는 통신을 허용하는 데 필요한 규칙이 활성화되어 있습니다. 에이전트가 이미 배포되어 있으며 동일한 AWS 계정에 있습니다. 동일한 에이전트는 나머지 NetApp 장치를 연결하고 모니터링하는 데 사용됩니다(그리고 이들 모두 작동 중입니다).	에이전트의 보안 규칙에 fsxadmin LIF 네트워크 세그먼트를 추가하여 이 문제를 해결하세요. 포트에 대해 확실하지 않으면 모든 포트를 허용합니다.

사용자 관리

워크로드 보안 사용자 계정은 Data Infrastructure Insights 통해 관리됩니다.

Data Infrastructure Insights 계정 소유자, 관리자, 사용자, 게스트의 네 가지 사용자 계정 수준을 제공합니다. 각 계정에는 특정 권한 수준이 지정됩니다. 관리자 권한이 있는 사용자 계정은 사용자를 생성하거나 수정할 수 있으며, 각 사용자에게 다음 워크로드 보안 역할 중 하나를 할당할 수 있습니다.

역할	워크로드 보안 액세스
관리자	알림, 포렌식, 데이터 수집기, 자동 응답 정책, 워크로드 보안 API 등 모든 워크로드 보안 기능을 수행할 수 있습니다. 관리자는 다른 사용자를 초대할 수도 있지만 워크로드 보안 역할만 할당할 수 있습니다.
사용자	알림을 보고 관리하고 포렌식을 볼 수 있습니다. 사용자 역할은 알림 상태를 변경하고, 메모를 추가하고, 수동으로 스냅샷을 찍고, 사용자 액세스를 제한할 수 있습니다.
손님	알림과 포렌식을 볼 수 있습니다. 게스트 역할은 알림 상태를 변경하거나, 메모를 추가하거나, 수동으로 스냅샷을 찍거나, 사용자 액세스를 제한할 수 없습니다.

단계

1. Workload Security에 로그인하세요
2. 메뉴에서 *관리자 > 사용자 관리*를 클릭하세요.

   Data Infrastructure Insights의 사용자 관리 페이지로 이동하게 됩니다.

3. 각 사용자별로 원하는 역할을 선택하세요.

새로운 사용자를 추가할 때 원하는 역할(일반적으로 사용자 또는 게스트)을 선택하기만 하면 됩니다.

사용자 계정 및 역할에 대한 자세한 내용은 Data Infrastructure Insights 에서 확인할 수 있습니다."사용자 역할" 선적 서류 비치.

SVM 이벤트 비율 검사기(에이전트 크기 조정 가이드)

이벤트 비율 검사기는 ONTAP SVM 데이터 수집기를 설치하기 전에 SVM에서 NFS/SMB 결합

이벤트 비율을 검사하여 하나의 에이전트 머신이 모니터링할 수 있는 SVM의 수를 확인하는 데 사용됩니다. 이벤트 비율 검사기를 크기 조정 가이드로 사용하여 보안 환경을 계획하세요.

에이전트는 최대 50개의 데이터 수집기를 지원할 수 있습니다.

요구 사항**:**

- 클러스터 IP
- 클러스터 관리자 사용자 이름 및 비밀번호

이 스크립트를 실행할 때 이벤트 비율을 결정하는 SVM에 대해 ONTAP SVM 데이터 수집기가 실행되어서는 안 됩니다.

단계:

1. CloudSecure의 지침에 따라 에이전트를 설치하세요.
2. 에이전트가 설치되면 sudo 사용자로 *server_data_rate_checker.sh* 스크립트를 실행합니다.

```
 /opt/netapp/cloudsecure/agent/install/svm_event_rate_checker.sh
. 이 스크립트를 사용하려면 Linux 시스템에 _sshpass_가 설치되어 있어야 합니다.
설치하는 방법은 두 가지가 있습니다.
```

   a. 다음 명령을 실행하세요.

```
 linux_prompt> yum install sshpass
.. 그래도 작동하지 않으면 웹에서 Linux 머신에 _sshpass_를 다운로드하고 다음 명령을
실행하세요.
```

```
linux_prompt> rpm -i sshpass
```

3. 메시지가 표시되면 올바른 값을 입력하세요. 아래 예를 참조하세요.
4. 스크립트를 실행하는 데 약 5분이 걸립니다.
5. 실행이 완료되면 스크립트는 SVM에서 이벤트 비율을 인쇄합니다. 콘솔 출력에서 SVM당 이벤트 비율을 확인할 수 있습니다.

```
“Svm svm_rate is generating 100 events/sec”.
```

각 Ontap SVM 데이터 수집기는 단일 SVM과 연결될 수 있습니다. 즉, 각 데이터 수집기는 단일 SVM이 생성하는 이벤트 수만큼 수신할 수 있습니다.

다음 사항을 명심하세요.

A) 이 표를 일반적인 사이즈 가이드로 활용하세요. 최대 50개까지 지원되는 데이터 수집기 수를 늘리려면 코어 수 및 /또는 메모리 수를 늘릴 수 있습니다.

에이전트 머신 구성	SVM 데이터 수집기 수	에이전트 머신이 처리할 수 있는 최대 이벤트 속도
4코어, 16GB	10명의 데이터 수집가	20K 이벤트/초
4코어, 32GB	20명의 데이터 수집가	20K 이벤트/초

B) 총 이벤트를 계산하려면 해당 에이전트의 모든 SVM에 대해 생성된 이벤트를 추가합니다.

C) 스크립트가 최대 사용량 시간대에 실행되지 않거나 최대 사용량 트래픽을 예측하기 어려운 경우 이벤트 비율 버퍼를 30%로 유지합니다.

B + C는 A보다 작아야 합니다. 그렇지 않으면 에이전트 머신이 모니터링에 실패합니다.

즉, 단일 에이전트 머신에 추가할 수 있는 데이터 수집기의 수는 아래 공식을 따라야 합니다.

```
 Sum of all Event rate of all Data Source Collectors + Buffer Event rate
of 30% < 20000 events/second
```

를 참조하십시오link:concept_cs_agent_requirements.html["에이전트 요구 사항"] 추가 전제 조건 및 요구 사항은 페이지를 참조하세요.

예

각각 초당 100, 200, 300개의 이벤트를 생성하는 3개의 SVMS가 있다고 가정해 보겠습니다.

우리는 다음 공식을 적용합니다:

```
 (100+200+300) + [(100+200+300)*30%] = 600+180 = 780events/sec
780 events/second is < 20000 events/second, so the 3 SVMs can be monitored
via one agent box.
```

콘솔 출력은 현재 작업 디렉토리의 *fpolicy_stat_<SVM* 이름*>.log* 파일 이름으로 에이전트 머신에서 사용할 수 있습니다.

다음과 같은 경우 스크립트가 잘못된 결과를 제공할 수 있습니다.

- 잘못된 자격 증명, IP 또는 SVM 이름이 제공되었습니다.
- 동일한 이름, 시퀀스 번호 등을 가진 이미 존재하는 fpolicy가 있으면 오류가 발생합니다.
- 스크립트가 실행 중에 갑자기 중단됩니다.

스크립트 실행 예는 아래와 같습니다.

```
[root@ci-cs-data agent]#
/opt/netapp/cloudsecure/agent/install/svm_event_rate_checker.sh
```

```
Enter the cluster ip: 10.192.139.166
Enter the username to SSH: admin
Enter the password:
Getting event rate for NFS and SMB events.
Available SVMs in the Cluster
------------------------------
QA_SVM
Stage_SVM
Qa-fas8020
Qa-fas8020-01
Qa-fas8020-02
audit_svm
svm_rate
vs_new
vs_new2
```

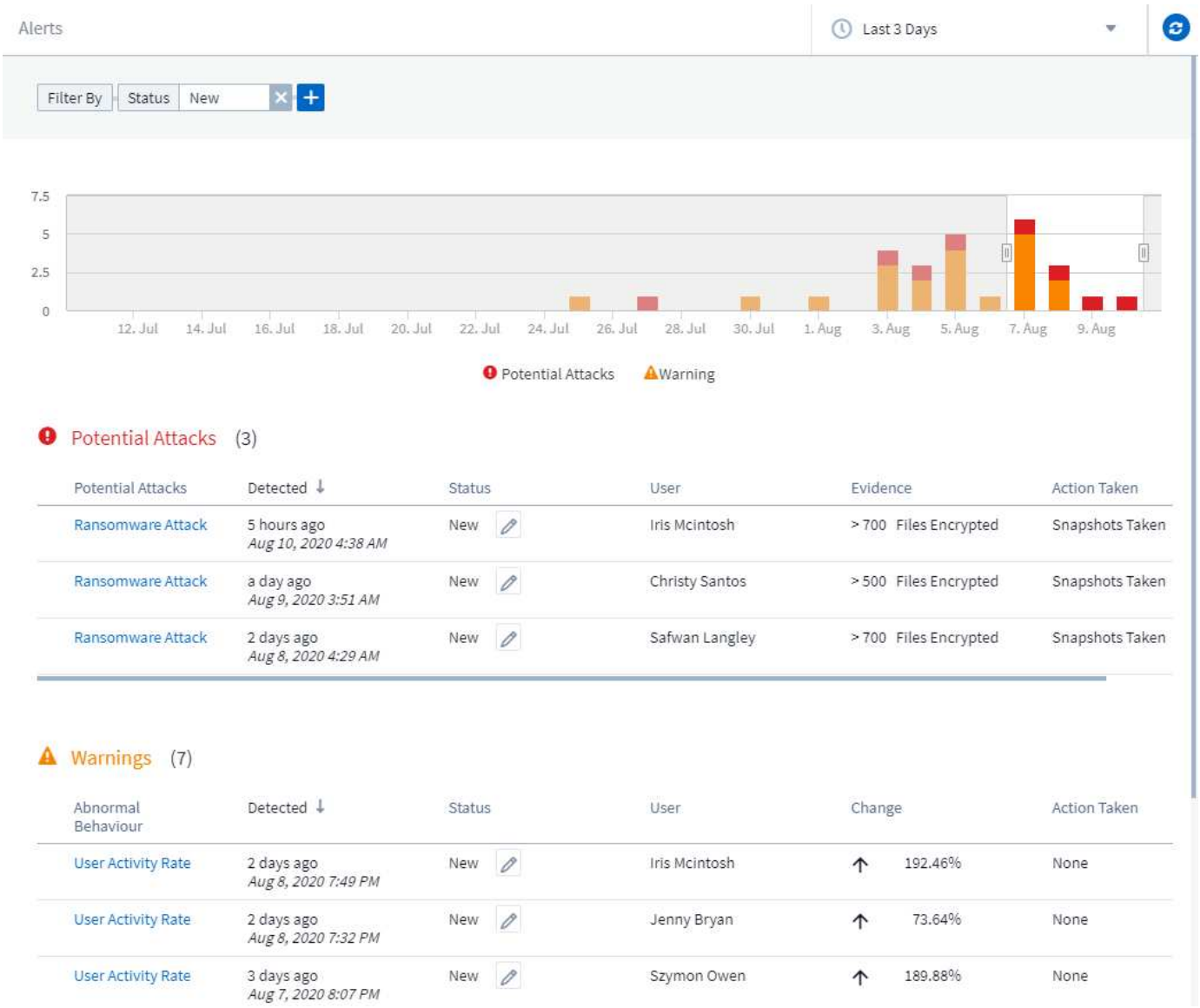
```
------------------------------
Enter [1/5] SVM name to check (press enter to skip): svm_rate
Enter [2/5] SVM name to check (press enter to skip): audit_svm
Enter [3/5] SVM name to check (press enter to skip):
Enter [4/5] SVM name to check (press enter to skip):
Enter [5/5] SVM name to check (press enter to skip):
Running check for svm svm_rate...
Running check for svm audit_svm...
Waiting 5 minutes for stat collection
Stopping sample svm_rate_sample
Stopping sample audit_svm_sample
fpolicy stats of svm svm_rate is saved in fpolicy_stat_svm_rate.log
Svm svm_rate is generating 100 SMB events/sec and 100 NFS events/sec
Overall svm svm_rate is generating 200 events/sec
fpolicy stats of svm audit_svm is saved in fpolicy_stat_audit_svm.log
Svm audit_svm is generating 200 SMB events/sec and 100 NFS events/sec
Overall svm audit_svm is generating 300 events/sec
```

```
[root@ci-cs-data agent]#
```

질문	답변
Workload Security에 대해 이미 구성된 SVM에서 이 스크립트를 실행하면 SVM의 기존 fpolicy 구성을 그대로 사용하나요? 아니면 임시 구성을 설정하고 프로세스를 실행하나요?	이벤트 비율 검사기는 워크로드 보안을 위해 이미 구성된 SVM에서도 정상적으로 실행될 수 있습니다. 아무런 영향이 없어야 합니다.
스크립트를 실행할 수 있는 SVM의 수를 늘릴 수 있나요?	네. 스크립트를 편집하여 SVM의 최대 개수를 5개에서 원하는 개수로 변경하기만 하면 됩니다.
SVM의 수를 늘리면 스크립트 실행 시간이 늘어나나요?	아니요. SVM 수가 늘어나더라도 스크립트는 최대 5분 동안 실행됩니다.
스크립트를 실행할 수 있는 SVM의 수를 늘릴 수 있나요?	네. 스크립트를 편집하여 SVM의 최대 수를 5에서 원하는 수로 변경해야 합니다.
SVM의 수를 늘리면 스크립트 실행 시간이 늘어나나요?	아니요. SVM 수가 늘어나도 스크립트는 최대 5분 동안만 실행됩니다.
기존 에이전트로 이벤트 비율 검사기를 실행하면 어떻게 되나요?	이미 존재하는 에이전트에 대해 이벤트 비율 검사기를 실행하면 SVM에서 지연 시간이 증가할 수 있습니다. 이벤트 요금 검사가 실행되는 동안 이러한 증가는 일시적인 성격을 갖습니다.

알림

워크로드 보안 경고 페이지는 탐지된 위협 및 경고에 대한 포괄적인 타임라인과 자세한 조사 도구를 제공합니다. 보안 사고를 효율적으로 조사하고 대응하기 위해 알림 세부 정보를 확인하고, 상태 업데이트를 관리하고, 기준별로 필터링하고, 사용자 활동을 추적할 수 있습니다.



알리다

경고 목록에는 선택한 시간 범위 내에 발생한 잠재적 공격 및/또는 경고의 총 수를 보여주는 그래프가 표시되고, 그 뒤에 해당 시간 범위 내에 발생한 공격 및/또는 경고 목록이 표시됩니다. 그래프에서 시작 시간과 종료 시간 슬라이더를 조정하여 시간 범위를 변경할 수 있습니다.

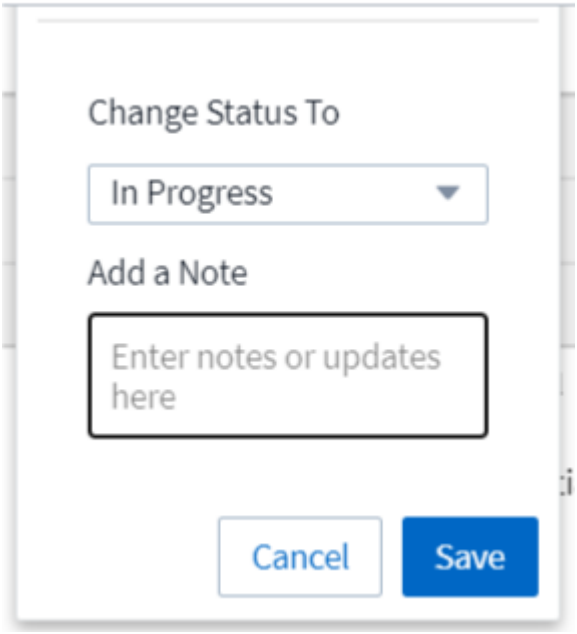
각 알림에 대해 다음 사항이 표시됩니다.

잠재적 공격:

- 잠재적 공격 유형(예: 파일 변조 또는 시스템 파괴 행위)
- 잠재적 공격이 감지된 날짜 및 시간
- 경고의 상태:
  - 새로 만들기: 이는 새 알림의 기본값입니다.
  - 진행 중: 팀원이 알림을 조사 중입니다.
  - 해결됨: 팀원이 알림을 해결한 것으로 표시했습니다.

◦ 거부됨: 경고가 거짓 양성 또는 예상된 동작으로 간주되어 거부되었습니다.

관리자는 알림 상태를 변경하고 조사에 도움이 되는 메모를 추가할 수 있습니다.



- 경고를 유발한 동작을 하는 사용자
- 공격의 증거(예: 많은 수의 파일이 암호화됨)
- 수행된 작업 (예: 스냅샷이 촬영됨)

경고:

- 경고를 유발한 비정상적인 동작
- 동작이 감지된 날짜와 시간
- 알림의 상태(신규, 진행 중 등)
- 경고를 유발한 동작을 하는 사용자
- _변경_에 대한 설명(예: 파일 액세스의 비정상적인 증가)
- 취해진 조치

필터 옵션

다음 기준으로 알림을 필터링할 수 있습니다.

- 경고의 상태
- _Note_의 특정 텍스트
- _공격/경고_의 유형
- 경고/알림을 트리거한 작업을 수행한 사용자

알림 세부 정보 페이지

알림 목록 페이지에서 알림 링크를 클릭하면 해당 알림에 대한 상세 페이지를 열 수 있습니다. 경고 세부 정보는 공격 또는 경고 유형에 따라 다를 수 있습니다. 예를 들어, 파일 변조 공격 상세 정보 페이지에는 다음과 같은 정보가 표시될 수 있습니다.

요약 섹션:

- 공격 유형(파일 변조, 파괴 행위) 및 경고 ID(워크로드 보안에서 할당)
- 공격이 감지된 날짜 및 시간
- 수행된 작업(예: 자동 스냅샷이 생성됨) 스냅샷 시간은 요약 섹션 바로 아래에 표시됩니다.))
- 상태(신규, 진행 중 등)

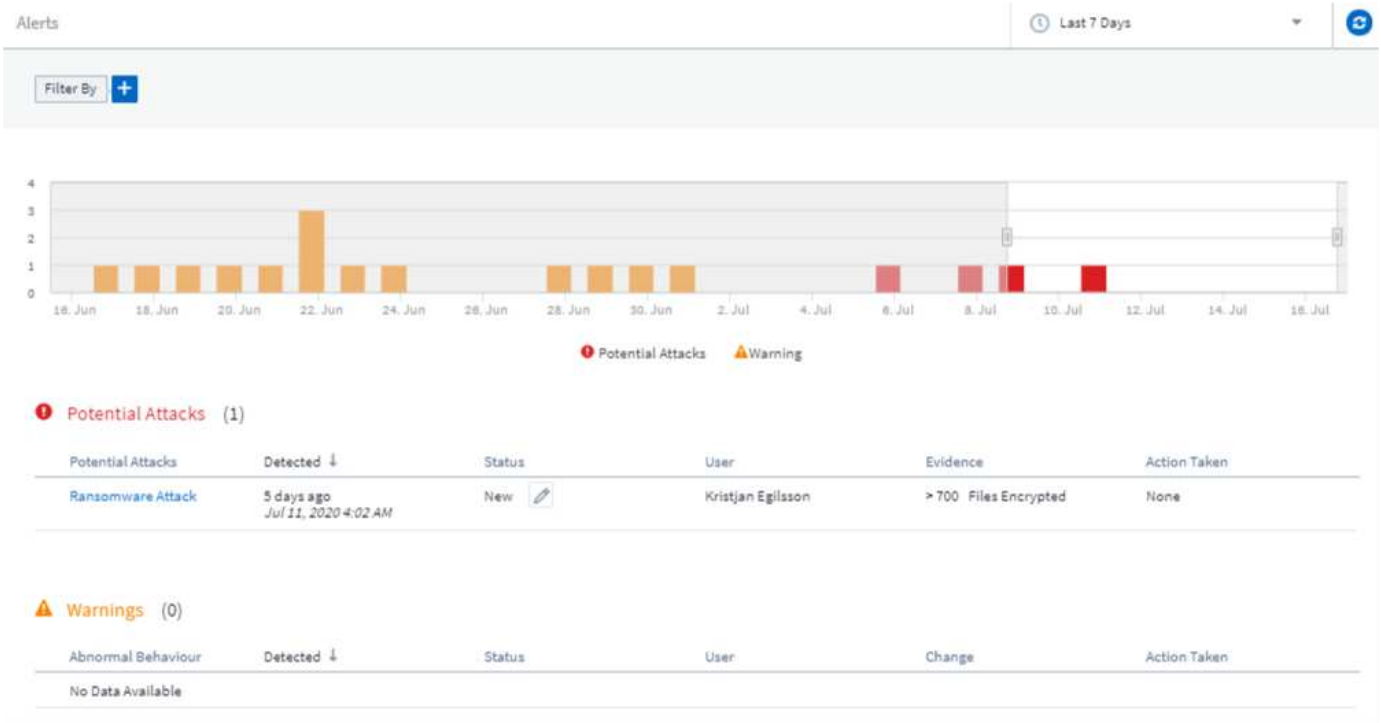
공격 결과 섹션:

- 영향을 받은 볼륨 및 파일 수
- 탐지에 대한 첨부 요약
- 공격 중 파일 활동을 보여주는 그래프

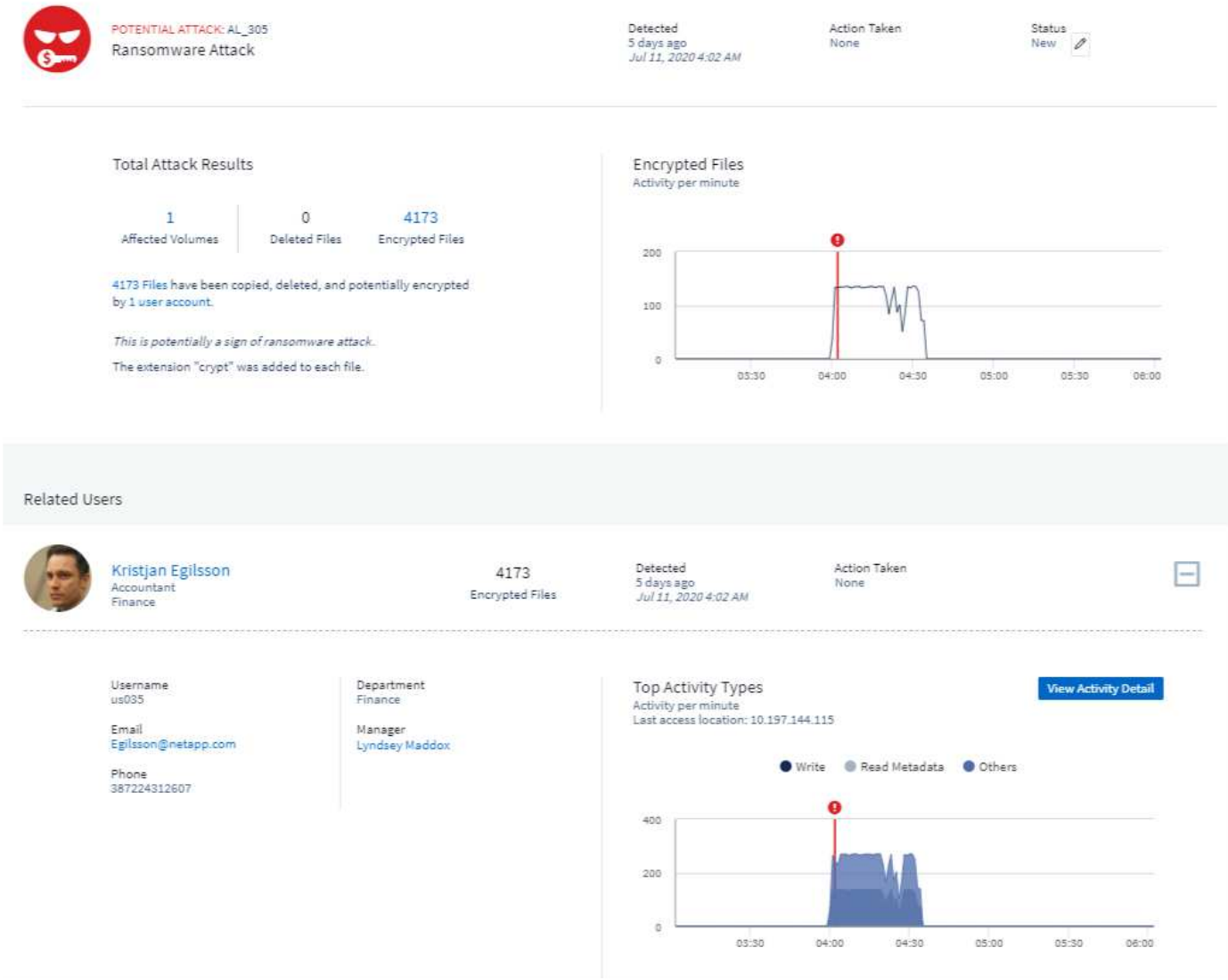
관련 사용자 섹션:

이 섹션에서는 사용자의 주요 활동 그래프를 포함하여 잠재적인 공격에 연루된 사용자에 대한 세부 정보를 보여줍니다.

경고 페이지(이 예시는 파일 변조 공격 가능성을 보여줍니다):



상세 페이지 (이 예시는 파일 변조 공격 가능성을 보여줍니다):

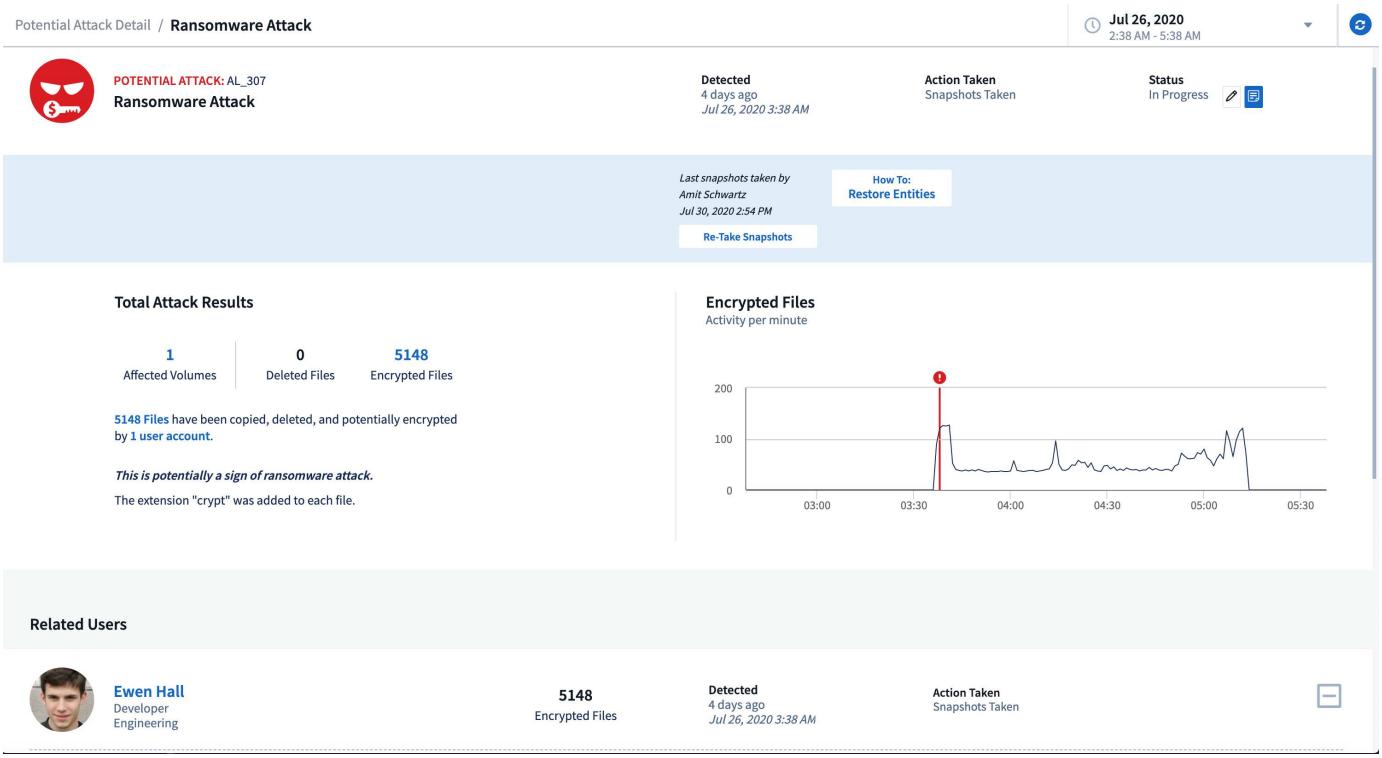


스냅샷 찍기 작업

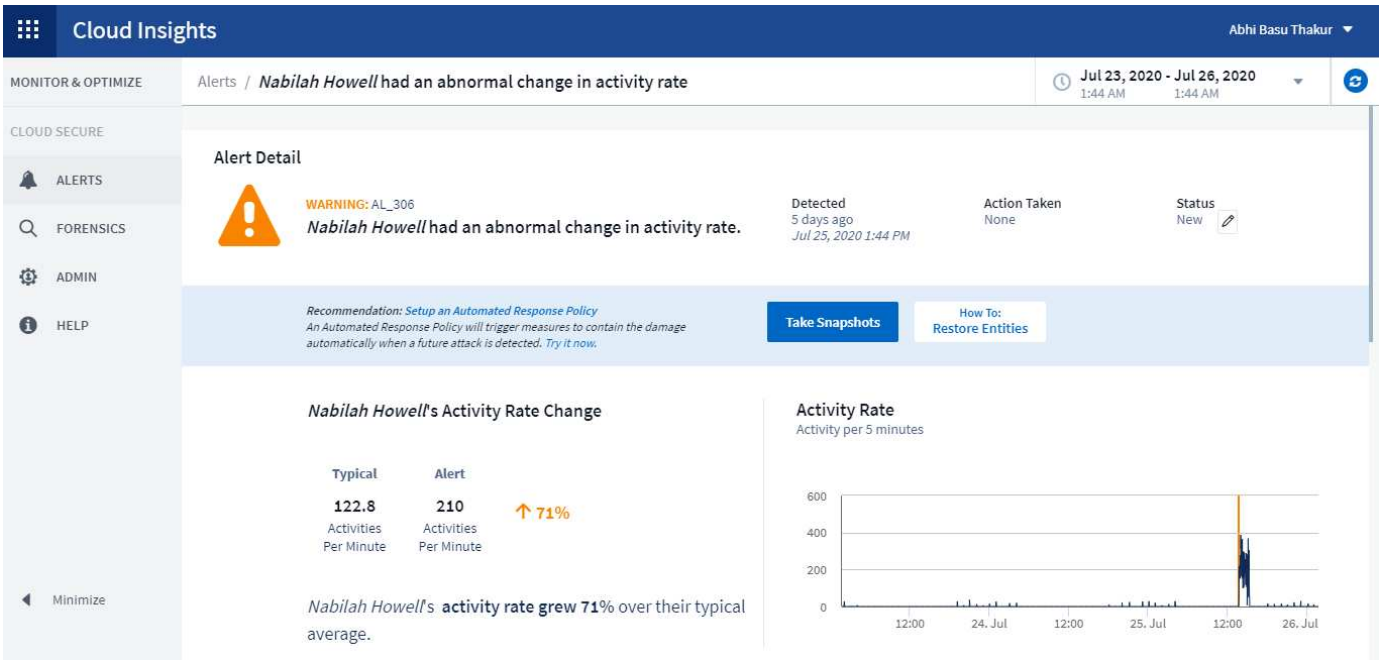
Workload Security는 악성 활동이 감지되면 자동으로 스냅샷을 찍어 데이터를 보호하고 데이터가 안전하게 백업되도록 보장합니다.

정의할 수 있습니다 "자동 응답 정책" 파일 변조 공격이나 기타 비정상적인 사용자 활동이 감지될 때 스냅샷을 찍는 기능입니다. 알림 페이지에서 수동으로 스냅샷을 찍을 수도 있습니다.

자동 스냅샷 촬영
:



수동 스냅샷
:



알림 알림

알림에 대한 모든 작업에 대해 알림 이메일 알림이 알림 수신자 목록으로 전송됩니다. 알림 수신자를 구성하려면 *관리자 > 알림*을 클릭하고 각 수신자의 이메일 주소를 입력하세요.

보존 정책

알림과 경고는 13개월 동안 보관됩니다. 13개월이 지난 알림과 경고는 삭제됩니다. 워크로드 보안 환경이 삭제되면 해당

환경과 관련된 모든 데이터도 삭제됩니다.

문제 해결

문제:	이것을 시도해보세요:
ONTAP 이 하루에 매시간 스냅샷을 찍는 상황이 있습니다. 워크로드 보안(WS) 스냅샷이 이에 영향을 미칠까요? WS 스냅샷이 시간별 스냅샷을 대체할 수 있을까요? 기본 시간별 스냅샷이 중지되나요?	워크로드 보안 스냅샷은 시간별 스냅샷에 영향을 미치지 않습니다. WS 스냅샷은 시간당 스냅샷 공간을 차지하지 않으며 이는 이전과 동일하게 유지됩니다. 기본 시간별 스냅샷은 중지되지 않습니다.
ONTAP 에서 최대 스냅샷 수에 도달하면 어떻게 되나요?	최대 스냅샷 수에 도달하면 후속 스냅샷 생성이 실패하고 Workload Security에서 스냅샷이 가득 찼다는 오류 메시지가 표시됩니다. 사용자는 가장 오래된 스냅샷을 삭제하기 위해 스냅샷 정책을 정의해야 합니다. 그렇지 않으면 스냅샷이 생성되지 않습니다. ONTAP 9.3 이하 버전에서는 볼륨에 최대 255개의 스냅샷 복사본이 포함될 수 있습니다. ONTAP 9.4 이상에서는 볼륨에 최대 1023개의 스냅샷 복사본을 포함할 수 있습니다. 자세한 내용은 ONTAP 문서를 참조하세요."스냅샷 삭제 정책 설정" .
Workload Security는 스냅샷을 전혀 찍을 수 없습니다.	스냅샷을 생성하는 데 사용되는 역할에 링크가 있는지 확인하세요: https://docs.netapp.com/us-en/cloudinsights/task_add_collector_svm.html#a-note-about-permissions [적절한 권한이 할당됨]. 스냅샷을 찍기 위한 적절한 액세스 권한으로 _csrole_이 생성되었는지 확인하세요: security login role create -vserver <vservername> -role csrole -cmddirname "volume snapshot" -access all
Workload Security에서 제거된 후 다시 추가된 SVM의 이전 알림에 대한 스냅샷이 실패합니다. SVM이 다시 추가된 후 발생하는 새로운 알림의 경우 스냅샷이 생성됩니다.	이는 드문 경우입니다. 이런 문제가 발생하는 경우 ONTAP에 로그인하여 이전 알림에 대한 스냅샷을 수동으로 찍으세요.
알림 세부 정보 페이지에서 스냅샷 찍기 버튼 아래에 "마지막 시도가 실패했습니다" 오류 메시지가 표시됩니다. 오류 위에 마우스를 올리면 "ID가 있는 데이터 수집기에 대한 API 명령 호출 시간이 초과되었습니다."라는 메시지가 표시됩니다.	ONTAP 에서 SVM의 LIF가 비활성화 상태인 경우 SVM 관리 IP를 통해 워크로드 보안에 데이터 수집기가 추가되면 이런 일이 발생할 수 있습니다. ONTAP 에서 특정 LIF를 활성화하고 Workload Security에서 _스냅샷 수동 촬영 _을 트리거합니다. 그러면 스냅샷 작업이 성공합니다.

법의학

법의학 - 모든 활동

모든 활동 페이지는 워크로드 보안 환경에서 엔터티에 수행된 작업을 이해하는 데 도움이 됩니다.

모든 활동 데이터 검토

과학 수사 > 활동 과학 수사*를 클릭하고 *모든 활동 탭을 클릭하여 모든 활동 페이지에 액세스합니다. 이 페이지에서는 세입자의 활동에 대한 개요를 제공하며 다음 정보를 강조합니다.

- _활동 내역_을 보여주는 그래프(선택된 글로벌 시간 범위 기반)

  그래프에서 사각형을 끌어서 그래프를 확대/축소할 수 있습니다. 확대된 기간 범위를 표시하기 위해 전체 페이지가 로드됩니다. 확대하면 사용자가 확대 축소할 수 있는 버튼이 표시됩니다.

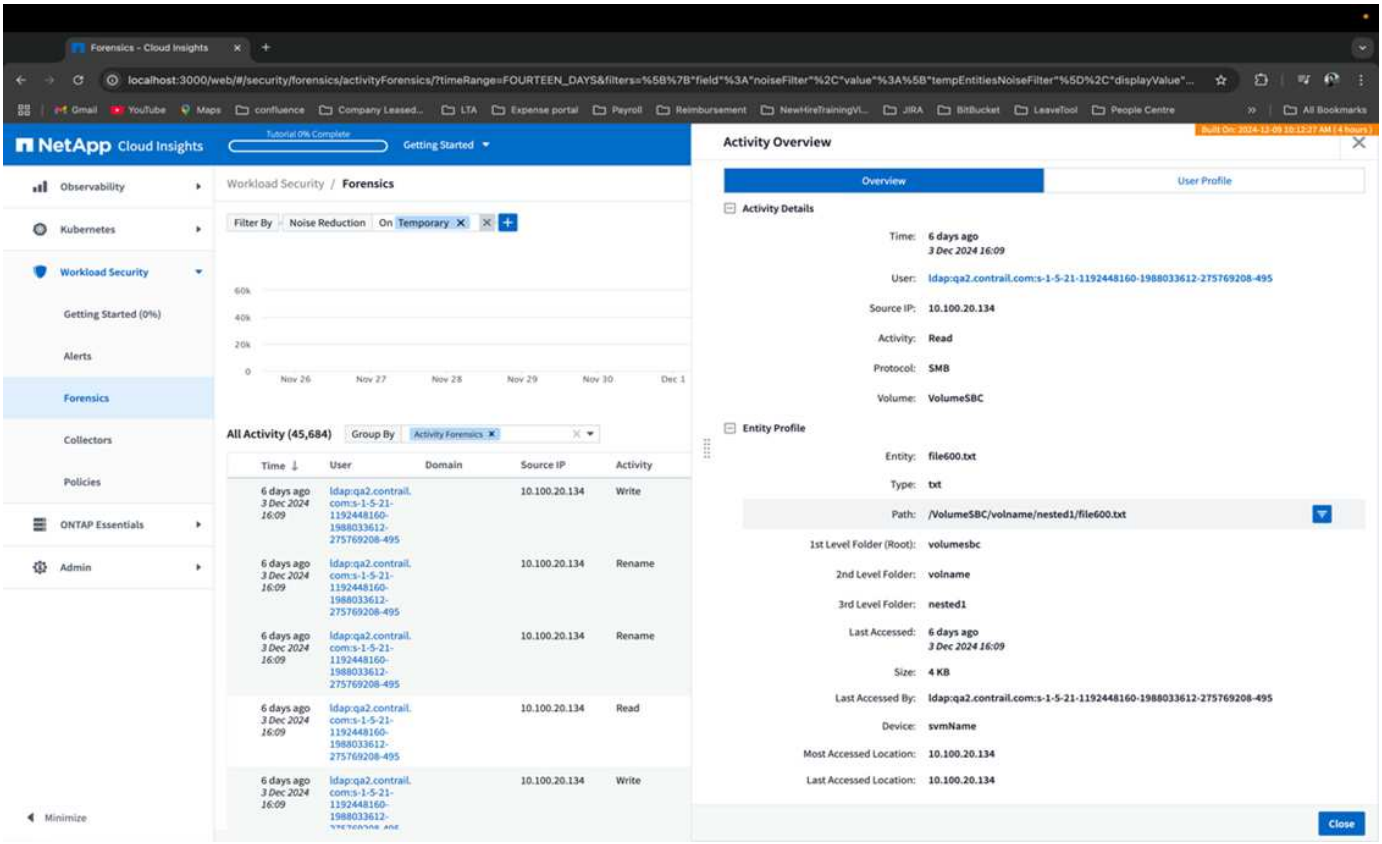
- 모든 활동 데이터 목록입니다.
- 드롭다운으로 그룹화하면 사용자, 폴더, 엔터티 유형 등으로 활동을 그룹화할 수 있는 옵션이 제공됩니다.
- 테이블 위에 있는 일반 경로 버튼을 클릭하면 엔터티 경로 세부 정보가 있는 슬라이드 아웃 패널을 볼 수 있습니다.

모든 활동 표에는 다음 정보가 표시됩니다. 이러한 열 중 일부가 기본적으로 표시되는 것은 아닙니다. "기어" 아이콘을 클릭하면 표시할 열을 선택할 수 있습니다.

- 엔터티에 접근한 *시간*에는 마지막 접근 시점의 연도, 월, 일, 시간이 포함됩니다.
- 링크를 통해 엔터티에 액세스한 *사용자*"사용자 정보" 슬라이드 아웃 패널로.
- 사용자가 수행한 활동 지원되는 유형은 다음과 같습니다.
  - 그룹 소유권 변경 - 파일이나 폴더의 그룹 소유권이 변경되었습니다. 그룹 소유권에 대한 자세한 내용은 다음을 참조하세요."이 링크."
  - 소유자 변경 - 파일이나 폴더의 소유권이 다른 사용자로 변경됩니다.
  - 권한 변경 - 파일이나 폴더의 권한이 변경되었습니다.
  - 만들기 - 파일이나 폴더를 만듭니다.
  - 삭제 - 파일이나 폴더를 삭제합니다. 폴더가 삭제되면 해당 폴더와 하위 폴더의 모든 파일에 대한 삭제 이벤트가 생성됩니다.
  - 읽기 - 파일을 읽었습니다.
  - 메타데이터 읽기 - 폴더 모니터링 옵션을 활성화한 경우에만 해당. Windows에서 폴더를 열거나 Linux에서 폴더 내에서 "ls"를 실행하면 생성됩니다.
  - 이름 바꾸기 - 파일이나 폴더의 이름을 바꿉니다.
  - 쓰기 - 데이터가 파일에 기록됩니다.
  - 메타데이터 쓰기 - 파일 메타데이터가 기록됩니다(예: 권한 변경).
  - 기타 변경 사항 - 위에 설명되지 않은 기타 이벤트. 매핑되지 않은 모든 이벤트는 "기타 변경" 활동 유형에 매핑됩니다. 파일과 폴더에 적용됩니다.
- 경로*는 엔터티 경로입니다. 이는 정확한 엔터티 경로(예: "***/home/userX/nested1/nested2/abc.txt***")이거나 재귀 검색을 위한 경로의 디렉토리 부분(예: "***/home/userX/nested1/nested2/***")이어야 합니다. 참고: 정규식 경로 패턴(예: *중첩)은 여기서 허용되지 않습니다. 또는 아래에 언급된 대로 개별 경로 폴더 수준 필터를 경로 필터링에 지정할 수도 있습니다.
- *1차 폴더(루트)*는 소문자로 된 엔티티 경로의 루트 디렉토리입니다.
- *2차 폴더*는 소문자로 된 엔티티 경로의 2차 디렉토리입니다.
- *3차 폴더*는 소문자로 된 엔티티 경로의 3차 디렉토리입니다.
- *4단계 폴더*는 소문자로 된 엔티티 경로의 4단계 디렉토리입니다.
- *엔터티 유형*에는 엔터티(즉, 파일) 확장자(.doc, .docx, .tmp 등)가 포함됩니다.
- 엔티티가 있는 *장치*입니다.

- 이벤트를 가져오는 데 사용되는 *프로토콜*입니다.
- 원본 파일의 이름이 변경되었을 때 이벤트 이름을 바꾸는 데 사용되는 *원래 경로*입니다. 이 열은 기본적으로 표에 표시되지 않습니다. 열 선택기를 사용하여 이 열을 표에 추가합니다.
- 엔티티가 있는 *볼륨*입니다. 이 열은 기본적으로 표에 표시되지 않습니다. 열 선택기를 사용하여 이 열을 표에 추가합니다.
- *엔터티 이름*은 엔터티 경로의 마지막 구성 요소입니다. 엔터티 유형이 파일인 경우 파일 이름입니다.

테이블 행을 선택하면 사용자 프로필이 있는 탭과 활동 및 엔터티 개요가 있는 다른 탭이 있는 슬라이드 아웃 패널이 열립니다.



기본 그룹화 방법은 활동 포렌식_입니다. 다른 _그룹화 방법(예: 엔터티 유형)을 선택하면 엔터티 그룹화 테이블이 표시됩니다. 선택하지 않으면 그룹화 *모두*가 표시됩니다.

- 활동 수는 하이퍼링크로 표시됩니다. 이를 선택하면 선택한 그룹이 필터로 추가됩니다. 해당 필터에 따라 활동 표가 업데이트됩니다.
- 필터를 변경하거나, 시간 범위를 변경하거나, 화면을 새로 고침하는 경우 필터를 다시 설정하지 않으면 필터링된 결과로 돌아갈 수 없습니다.
- 엔티티 이름을 필터로 선택하면 그룹화 기준 드롭다운이 비활성화됩니다. 또한, 사용자가 이미 그룹화 기준 화면에 있는 경우 엔티티 이름을 필터로 사용하는 기능이 비활성화됩니다.

법의학 활동 내역 데이터 필터링

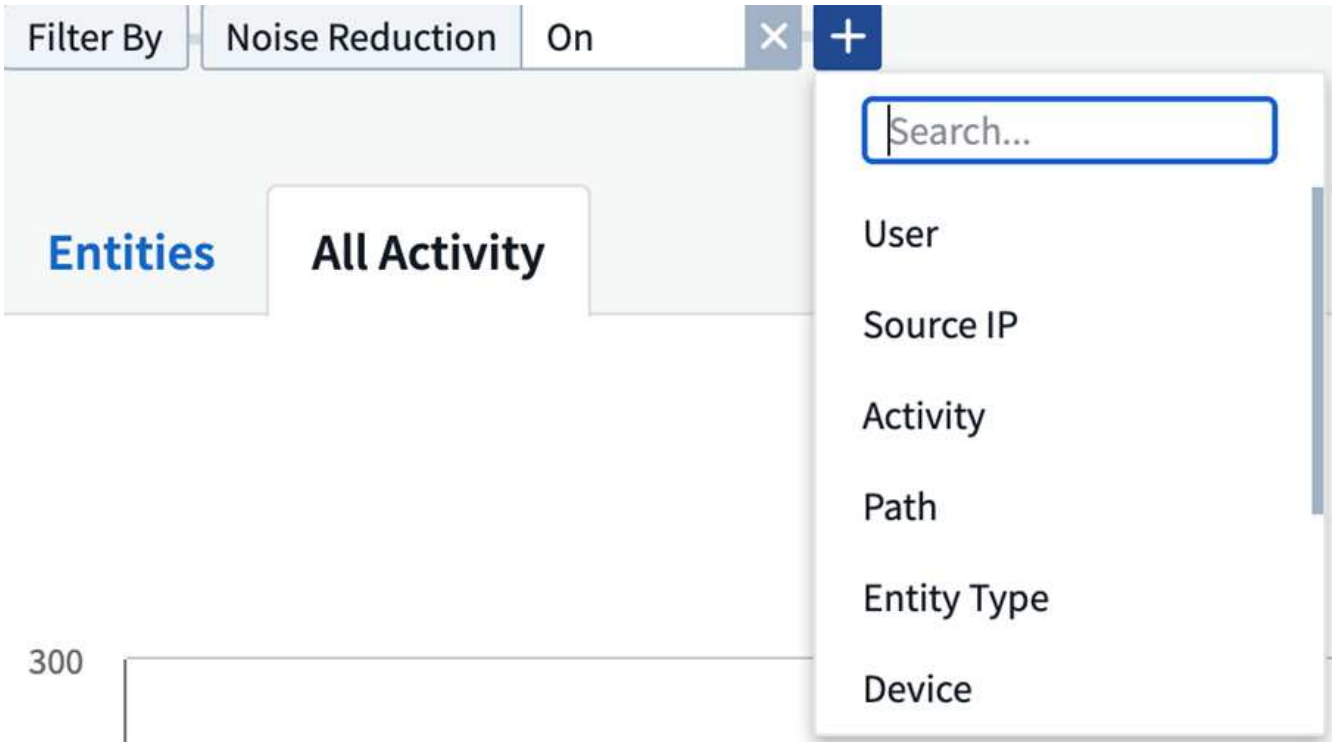
데이터를 필터링하는 데 사용할 수 있는 방법은 두 가지가 있습니다.

- 필터는 슬라이드 아웃 패널에서 추가할 수 있습니다. 해당 값은 상단의 필터 기준 목록에 있는 적절한 필터에

추가됩니다.

- 필터 기준 필드에 입력하여 데이터를 필터링합니다.

  [+] 버튼을 클릭하여 상단의 '필터 기준' 위젯에서 적절한 필터를 선택하세요.



  검색어를 입력하세요

  필터를 적용하려면 Enter 키를 누르거나 필터 상자 밖을 클릭하세요.

다음 필드를 기준으로 포렌식 활동 데이터를 필터링할 수 있습니다.

- 활동 유형.
- 프로토콜 프로토콜별 활동을 가져옵니다.
- 활동을 수행하는 사용자의 사용자 이름*입니다. 필터링하려면 정확한 사용자 이름을 제공해야 합니다. 사용자 이름의 일부 또는 일부 사용자 이름에 " 접두사나 접미사를 붙여 검색하면 작동하지 않습니다.
- *노이즈 감소*는 사용자가 지난 2시간 동안 만든 파일을 필터링하는 기능입니다. 또한 사용자가 액세스하는 임시 파일(예: .tmp 파일)을 필터링하는 데 사용됩니다.
- 활동을 수행하는 사용자의 도메인*입니다. 필터링하려면 *정확한 도메인*을 제공해야 합니다. 부분 도메인이나 와일드카드()로 접두사나 접미사가 붙은 부분 도메인을 검색하는 것은 작동하지 않습니다. _None_을 지정하면 누락된 도메인을 검색할 수 있습니다.

다음 필드에는 특별 필터링 규칙이 적용됩니다.

- 엔터티 유형, 엔터티(파일) 확장자를 사용합니다. 따옴표 안에 정확한 엔터티 유형을 지정하는 것이 좋습니다. 예를 들어 *"txt"*.
- 엔티티의 경로 - 이는 정확한 엔티티 경로(예: "*/home/userX/nested1/nested2/abc.txt*")이거나 재귀 검색을 위한 경로의 디렉토리 부분(예: "*/home/userX/nested1/nested2/*")이어야 합니다. 참고: 정규식 경로 패턴(예: *중첩*)은

여기서 허용되지 않습니다. 더 빠른 결과를 얻으려면 최대 4개 디렉토리까지 디렉토리 경로 필터(경로 문자열이 /로 끝남)를 사용하는 것이 좋습니다. 예를 들어, "*/home/userX/nested1/nested2/*". 자세한 내용은 아래 표를 참조하세요.

- 1단계 폴더(루트) - 필터로서의 엔티티 경로의 루트 디렉토리. 예를 들어, 엔티티 경로가 /home/userX/nested1/nested2/인 경우 home 또는 "home"을 사용할 수 있습니다.
- 2차 폴더 - 엔터티 경로 필터의 2차 디렉토리입니다. 예를 들어, 엔티티 경로가 /home/userX/nested1/nested2/인 경우 userX 또는 "userX"를 사용할 수 있습니다.
- 3차 폴더 – 엔터티 경로 필터의 3차 디렉토리입니다.
- 예를 들어, 엔티티 경로가 /home/userX/nested1/nested2/인 경우 nested1 또는 "nested1"을 사용할 수 있습니다.
- 4단계 폴더 - 디렉토리 엔터티 경로 필터의 4단계 디렉토리입니다. 예를 들어, 엔티티 경로가 /home/userX/nested1/nested2/인 경우 nested2 또는 "nested2"를 사용할 수 있습니다.
- 활동을 수행하는 사용자 - 따옴표로 정확한 사용자를 지정하는 것이 좋습니다. 예를 들어, *"관리자"*.
- 장치 (SVM) 엔티티가 상주하는 곳
- 볼륨 엔터티가 있는 곳
- 원본 파일의 이름이 변경되었을 때 이벤트 이름을 바꾸는 데 사용되는 *원래 경로*입니다.
- *엔터티에 접근한 소스 IP*입니다.
  - 와일드카드 * 및 ?를 사용할 수 있습니다. 예: 10.0.0.**, 10.0?.0.10, 10.10**
  - 정확한 일치가 필요한 경우 유효한 소스 IP 주소를 큰따옴표로 묶어 제공해야 합니다(예: "10.1.1.1."). "10.1.1.", "10.1..*" 등과 같이 큰따옴표가 포함된 불완전한 IP는 작동하지 않습니다.
- 엔터티 이름 - 필터로서의 엔터티 경로의 파일 이름입니다. 예를 들어, 엔티티 경로가 /home/userX/nested1/testfile.txt이면 엔티티 이름은 testfile.txt입니다. 정확한 파일 이름을 따옴표로 묶어 지정하는 것이 좋습니다. 와일드카드 검색은 피하세요. 예를 들어, "testfile.txt". 또한, 이 엔터티 이름 필터는 짧은 시간 범위(최대 3일)에 권장됩니다.

필터링 시 이전 필드는 다음 사항에 따라 달라집니다.

- 정확한 값은 따옴표 안에 있어야 합니다. 예: "searchtext"
- 와일드카드 문자열에는 따옴표가 포함될 수 없습니다. 예: searchtext, *searchtext*는 'searchtext'를 포함하는 모든 문자열을 필터링합니다.
- 접두사가 있는 문자열(예: searchtext*)은 'searchtext'로 시작하는 모든 문자열을 검색합니다.

모든 필터 필드는 대소문자를 구분하여 검색합니다. 예를 들어, 적용된 필터가 'searchtext' 값을 갖는 엔터티 유형인 경우 엔터티 유형이 'searchtext', 'SearchText', 'SEARCHTEXT'인 결과가 반환됩니다.

활동 포렌식 필터 예**:**

사용자가 적용한 필터 표현식	예상 결과	성과 평가	논평
경로 = "/home/userX/nested1/nested2/"	지정된 디렉토리 아래의 모든 파일 및 폴더에 대한 재귀적 조회	빠른	최대 4개의 디렉토리를 검색하면 빠르게 검색됩니다.

사용자가 적용한 필터 표현식	예상 결과	성과 평가	논평
경로 = "/home/userX/nested1/"	지정된 디렉토리 아래의 모든 파일 및 폴더에 대한 재귀적 조회	빠른	최대 4개의 디렉토리를 검색하면 빠르게 검색됩니다.
경로 = "/home/userX/nested1/test"	경로 값이 /home/userX/nested1/test와 일치하는 정확한 일치	더 느리게	정확한 검색은 디렉토리 검색에 비해 검색 속도가 느립니다.
경로 = "/home/userX/nested1/nested2/nested3/"	지정된 디렉토리 아래의 모든 파일 및 폴더에 대한 재귀적 조회	더 느리게	4개 이상의 디렉토리에서 검색하면 검색 속도가 느려집니다.
기타 경로 기반이 아닌 필터. 사용자 및 엔터티 유형 필터는 따옴표로 묶는 것이 좋습니다(예: User="Administrator" 엔터티 유형="txt").		빠른	
엔티티 이름 = "test.log"	파일 이름이 test.log인 정확한 일치	빠른	정확히 일치하므로
엔티티 이름 = *test.log	test.log로 끝나는 파일 이름	느린	와일드 카드로 인해 느릴 수 있습니다.
엔티티 이름 = test*.log	test로 시작하고 .log로 끝나는 파일 이름	느린	와일드 카드로 인해 느릴 수 있습니다.
엔티티 이름 = test.lo	test.lo로 시작하는 파일 이름 예: test.log, test.log.1, test.log1과 일치합니다.	더 느리게	끝에 와일드카드가 있어서 느릴 수 있습니다.
엔티티 이름 = 테스트	test로 시작하는 파일 이름	가장 느림	끝에 와일드카드가 있고 보다 일반적인 값이 사용되기 때문에 가장 느릴 수 있습니다.

메모:

1. 모든 활동 아이콘 옆에 표시되는 활동 수는 선택한 시간 범위가 3일을 초과하는 경우 30분으로 반올림됩니다. 예를 들어, _9월 1일 오전 10시 15분 ~ 9월 7일 오전 10시 15분_의 시간 범위는 9월 1일 오전 10시부터 9월 7일 오전 10시 30분까지의 활동 수를 표시합니다.
2. 마찬가지로, 선택한 시간 범위가 3일을 넘을 경우 활동 내역 그래프에 표시되는 카운트 지표는 30분으로 반올림됩니다.

법의학 활동 내역 데이터 정렬

활동 내역 데이터를 시간, 사용자, 소스 *IP,* 활동, 엔터티 유형, 1차 폴더(루트), 2차 폴더, 3차 폴더, 4차 폴더별로 정렬할 수 있습니다. 기본적으로 표는 시간 순으로 내림차순으로 정렬됩니다. 즉, 최신 데이터가 먼저 표시됩니다. *Device* 및 *Protocol* 필드에 대한 정렬이 비활성화되었습니다.

비동기 내보내기 사용자 가이드

개요

Storage Workload Security의 비동기 내보내기 기능은 대용량 데이터 내보내기를 처리하도록 설계되었습니다.

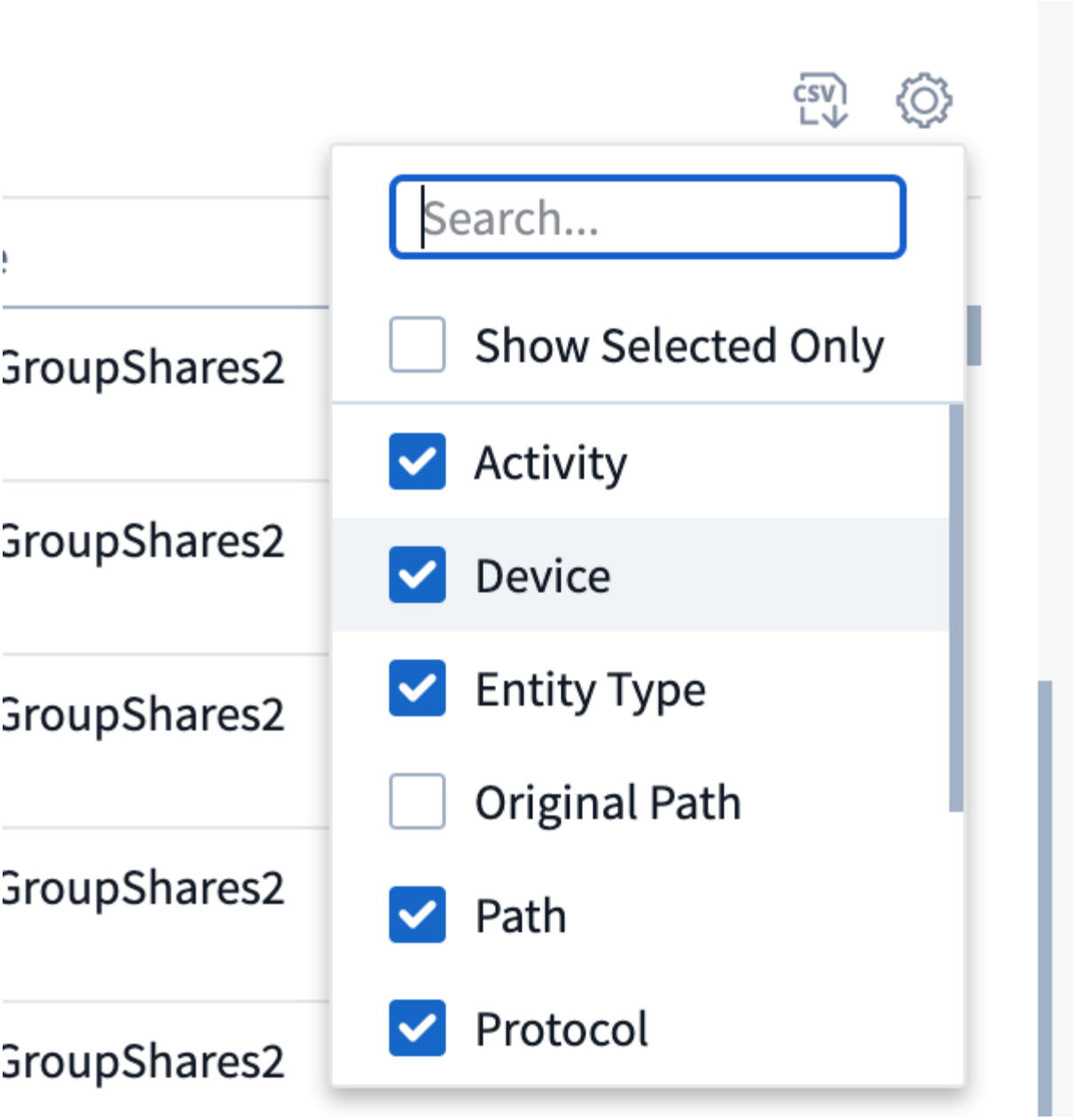
단계별 가이드: 비동기 내보내기를 통한 데이터 내보내기

1. 내보내기 시작: 내보내기에 필요한 기간과 필터를 선택하고 내보내기 버튼을 클릭합니다.
2. 내보내기가 완료될 때까지 기다리세요: 처리 시간은 몇 분에서 몇 시간까지 걸릴 수 있습니다. 법의학 페이지를 여러 번 새로 고쳐야 할 수도 있습니다. 내보내기 작업이 완료되면 "마지막으로 내보낸 CSV 파일 다운로드" 버튼이 활성화됩니다.
3. 다운로드: "마지막으로 생성된 내보내기 파일 다운로드" 버튼을 클릭하면 내보낸 데이터를 .zip 형식으로 받을 수 있습니다. 이 데이터는 사용자가 다른 비동기 내보내기를 시작하거나 3일이 경과할 때까지 다운로드할 수 있습니다. 어느 쪽이 먼저 발생하는지에 따라 달라집니다. 다른 비동기 내보내기가 시작될 때까지 버튼은 활성화된 상태로 유지됩니다.
4. 제한 사항:
    - 비동기 다운로드 수는 현재 각 활동 및 활동 분석 테이블의 경우 사용자당 1개, 테넌트당 3개로 제한되어 있습니다.
    - 활동 표의 경우 내보낼 수 있는 데이터는 최대 100만 개의 레코드로 제한되고, 그룹화 기준의 경우 레코드 수는 50만 개로 제한됩니다.

API를 통해 포렌식 데이터를 추출하는 샘플 스크립트는 에이전트의 _/opt/netapp/cloudsecure/agent/export-script/_에 있습니다. 스크립트에 대한 자세한 내용은 이 위치의 readme를 참조하세요.

모든 활동에 대한 열 선택

모든 활동 표에는 기본적으로 선택된 열이 표시됩니다. 열을 추가, 제거 또는 변경하려면 표 오른쪽에 있는 기어 아이콘을 클릭하고 사용 가능한 열 목록에서 선택하세요.



활동 내역 보존

활성 워크로드 보안 환경의 활동 내역은 13개월 동안 보관됩니다.

포렌식 페이지에서 필터 적용 가능성

필터	그것이 하는 일	예	다음 필터에 적용 가능	이 필터에는 적용되지 않습니다.	결과
* (별표)	모든 것을 검색할 수 있습니다	Auto*03172022 검색 텍스트에 하이픈이나 밑줄이 포함된 경우 괄호 안에 표현식을 입력합니다. 예: svm-123을 검색하는 경우 (svm*)	사용자, 엔터티 유형, 장치, 볼륨, 원래 경로, 1차 폴더, 2차 폴더, 3차 폴더, 4차 폴더, 엔터티 이름, 소스 IP		"Auto"로 시작하고 "03172022"로 끝나는 모든 리소스를 반환합니다.
? (물음표)	특정 수의 문자를 검색할 수 있습니다	AutoSabotageUser1_03172022?	사용자, 엔터티 유형, 장치, 볼륨, 1차 폴더, 2차 폴더, 3차 폴더, 4차 폴더, 엔터티 이름, 소스 IP		AutoSabotageUser1_03172022A, AutoSabotageUser1_03172022B, AutoSabotageUser1_031720225 등을 반환합니다.
또는	여러 엔터티를 지정할 수 있습니다.	AutoSabotageUser1_03172022 또는 AutoRansomUser4_03162022	사용자, 도메인, 엔터티 유형, 원래 경로, 엔터티 이름, 소스 IP		AutoSabotageUser1_03172022 또는 AutoRansomUser4_03162022 중 하나를 반환합니다.
아니다	검색 결과에서 텍스트를 제외할 수 있습니다.	NOT AutoRansomUser4_03162022	사용자, 도메인, 엔터티 유형, 원래 경로, 1차 폴더, 2차 폴더, 3차 폴더, 4차 폴더, 엔터티 이름, 소스 IP	장치	"AutoRansomUser4_03162022"로 시작하지 않는 모든 항목을 반환합니다.
None	모든 필드에서 NULL 값을 검색합니다.	None	도메인		대상 필드가 비어 있는 결과를 반환합니다.

경로 검색

/가 있는 경우와 없는 경우의 검색 결과가 다릅니다.

"/자동 디렉토리1/자동 파일03242022"	정확한 검색만 작동합니다. /AutoDir1/AutoFile03242022(대소문자 구분 없이)와 같은 정확한 경로를 가진 모든 활동을 반환합니다.
"/자동 디렉토리1/ "	작동합니다. AutoDir1과 일치하는 1차 디렉토리가 있는 모든 활동을 반환합니다(대소문자 구분 없음).
"/자동 디렉토리1/자동 파일03242022/"	작동합니다. 1차 디렉토리가 AutoDir1과 일치하고 2차 디렉토리가 AutoFile03242022와 일치하는 모든 활동을 반환합니다(대소문자 구분 없음).

/AutoDir1/AutoFile03242022 또는 /AutoDir1/AutoFile03242022	작동하지 않습니다
/AutoDir1/AutoFile03242022가 아닙니다	작동하지 않습니다
/AutoDir1이 아닙니다	작동하지 않습니다
아니요 /AutoFile03242022	작동하지 않습니다
*	작동하지 않습니다

로컬 루트 **SVM** 사용자 활동 변경

로컬 루트 SVM 사용자가 어떤 활동을 수행하는 경우, NFS 공유가 마운트된 클라이언트의 IP가 이제 사용자 이름에 고려되며, 이는 포렌식 활동 및 사용자 활동 페이지 모두에서 root@<클라이언트의 IP 주소>로 표시됩니다.

예를 들어:

- SVM-1이 Workload Security에서 모니터링되고 해당 SVM의 루트 사용자가 IP 주소 10.197.12.40의 클라이언트에 공유를 마운트하는 경우, 포렌식 활동 페이지에 표시되는 사용자 이름은 _root@10.197.12.40_입니다.
- 동일한 SVM-1이 IP 주소 10.197.12.41의 다른 클라이언트에 마운트되면 포렌식 활동 페이지에 표시되는 사용자 이름은 _root@10.197.12.41_이 됩니다.

*• 이는 IP 주소별로 NFS 루트 사용자 활동을 분리하기 위해 수행됩니다. 이전에는 모든 활동이 IP 구분 없이 *root* 사용자에 의해서만 수행되는 것으로 간주되었습니다.

문제 해결

문제	이것을 시도해보세요
"모든 활동" 테이블의 "사용자" 열에서 사용자 이름은 "ldap:HQ.COMPANYNAME.COM:S-1-5-21-3577637-1906459482-1437260136-1831817" 또는 "ldap:default:80038003"으로 표시됩니다.	가능한 이유는 다음과 같습니다. 1. 아직 사용자 디렉토리 수집기가 구성되지 않았습니다. 하나를 추가하려면 *워크로드 보안 > 수집기 > 사용자 디렉터리 수집기*로 이동하여 *+사용자 디렉터리 수집기*를 클릭합니다. *Active Directory* 또는 _LDAP 디렉터리 서버_를 선택하세요. 2. 사용자 디렉토리 수집기가 구성되었지만 중지되었거나 오류 상태입니다. *수집기 > 사용자 디렉토리 수집기*로 가서 상태를 확인하세요. 를 참조하세요"사용자 디렉토리 수집기 문제 해결" 문제 해결 팁에 대한 설명서 섹션입니다. 올바르게 구성하면 이름은 24시간 이내에 자동으로 확인됩니다. 그래도 문제가 해결되지 않으면 올바른 사용자 데이터 수집기를 추가했는지 확인하세요. 사용자가 실제로 추가된 Active Directory/LDAP 디렉터리 서버에 속해 있는지 확인하세요.

일부 NFS 이벤트는 UI에서 볼 수 없습니다.	다음 사항을 확인하세요. 1. POSIX 속성이 설정된 AD 서버용 사용자 디렉터리 수집기는 UI에서 unixid 속성을 활성화하여 실행해야 합니다. 2. UI 3의 사용자 페이지에서 검색하면 NFS 액세스를 수행하는 모든 사용자가 표시되어야 합니다. 원시 이벤트(사용자가 아직 검색되지 않은 이벤트)는 NFS 4에서 지원되지 않습니다. NFS 내보내기에 대한 익명 액세스는 모니터링되지 않습니다. 5. 사용하는 NFS 버전이 4.1 이하인지 확인하세요. (NFS 4.1은 ONTAP 9.15 이상에서 지원됩니다.)
포렌식 모든 활동 또는 엔터티 페이지의 필터에 별표(*)와 같은 와일드카드 문자가 포함된 몇 글자를 입력한 후 페이지가 매우 느리게 로드됩니다.	검색 문자열에 별표(*)를 넣으면 모든 것을 검색합니다. 하지만 *<*searchTerm*> 또는 *<*searchTerm*>*_와 같은 와일드카드 문자열을 앞에 붙이면 쿼리 속도가 느려집니다. 더 나은 성능을 얻으려면 대신 접두사 문자열을 사용하세요. 형식은 _<*searchTerm*>*_입니다. (즉, 검색어 _뒤에 별표(*)를 추가하세요.) 예: *testvolume* 또는 *test*volume* 대신 *testvolume** 문자열을 사용하세요. 디렉토리 검색을 사용하여 지정된 폴더 아래에 있는 모든 활동을 재귀적으로 확인합니다(계층적 검색). 예를 들어, "/path1/path2/path3/"은 /path1/path2/path3 아래에 있는 모든 활동을 재귀적으로 나열합니다. 또는 모든 활동 탭 아래의 "필터에 추가" 옵션을 사용하세요.
경로 필터를 사용할 때 "요청이 상태 코드 500/503으로 실패했습니다" 오류가 발생합니다.	레코드 필터링에 더 작은 날짜 범위를 사용해 보세요.
path 필터를 사용하면 포렌식 UI에서 데이터 로드 속도가 느려집니다.	더 빠른 결과를 얻으려면 최대 4개 디렉토리까지 디렉토리 경로 필터(경로 문자열이 /로 끝남)를 사용하는 것이 좋습니다. 예를 들어 디렉토리 경로가 /Aaa/Bbb/Ccc/Ddd인 경우 "/Aaa/Bbb/Ccc/Ddd/"를 검색하여 데이터를 더 빨리 로드해 보세요.
포렌식 UI가 데이터를 느리게 로드하고 엔터티 이름 필터를 사용할 때 오류가 발생합니다.	더 작은 시간 범위와 큰따옴표로 묶인 정확한 값으로 검색을 시도해 보세요. 예를 들어, entityPath가 "/home/userX/nested1/nested2/nested3/testfile.txt"인 경우 엔티티 이름 필터로 "testfile.txt"를 사용해 보세요.

포렌식 사용자 개요

각 사용자에 대한 정보는 사용자 개요에서 제공됩니다. 이러한 보기를 사용하면 사용자 특성, 관련 엔터티, 최근 활동을 파악할 수 있습니다.

사용자 프로필

사용자 프로필 정보에는 사용자의 연락처 정보와 위치가 포함됩니다. 프로필에는 다음과 같은 정보가 제공됩니다.

- 사용자 이름
- 사용자의 이메일 주소
- 사용자 관리자
- 사용자를 위한 전화 연락처
- 사용자의 위치

사용자 행동

사용자 행동 정보는 사용자가 최근에 수행한 활동과 작업을 식별합니다. 이 정보에는 다음이 포함됩니다.

- 최근 활동
  - 마지막 접속 위치
  - 활동 그래프
  - 알림
- 지난 7일간의 작업
  - 작업 수

새로 고침 간격

사용자 목록은 12시간마다 새로 고쳐집니다.

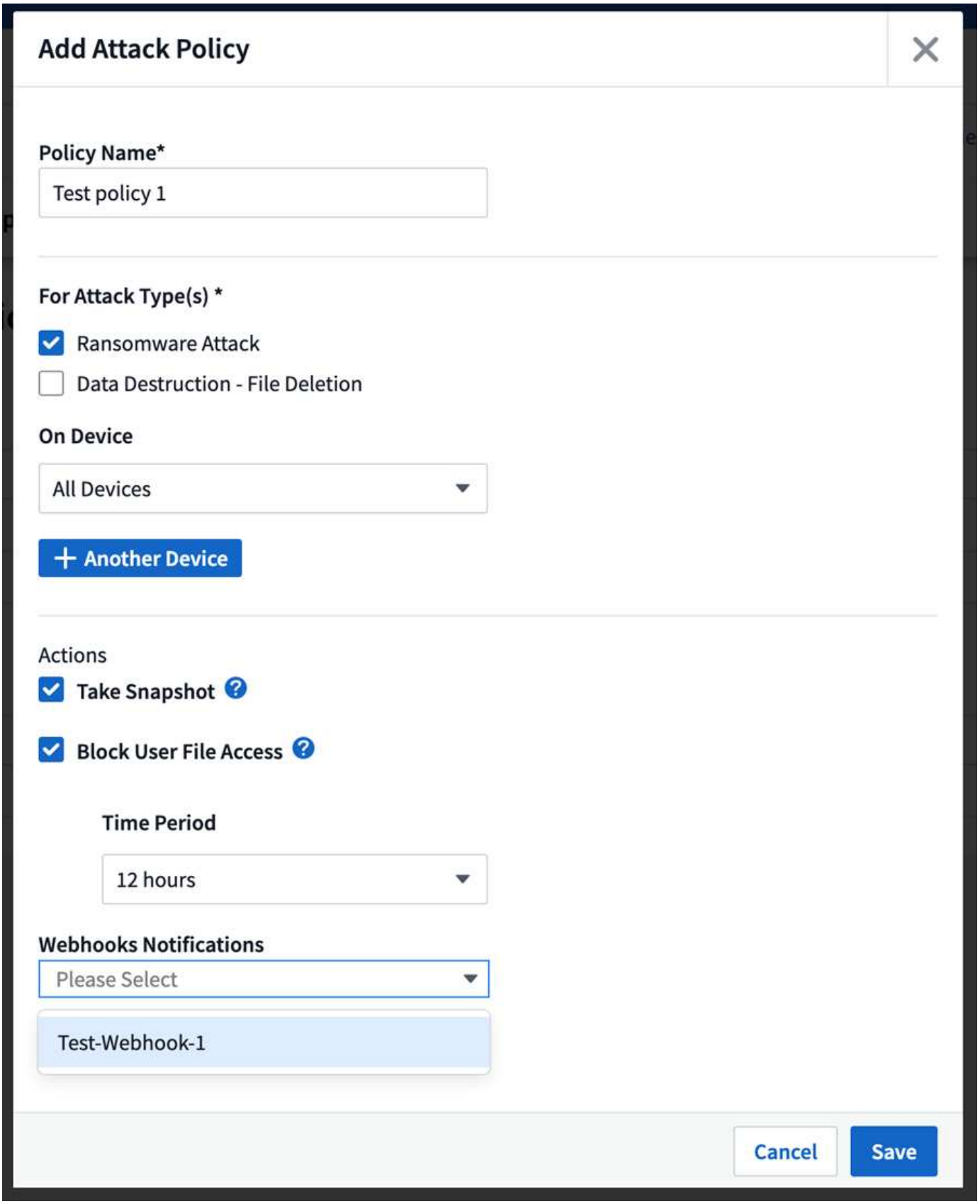
보존 정책

새로고침하지 않으면 사용자 목록은 13개월 동안 보관됩니다. 13개월 후에 데이터가 삭제됩니다. 워크로드 보안 환경이 삭제되면 해당 환경과 관련된 모든 데이터가 삭제됩니다.

자동 응답 정책

대응 정책은 공격이나 비정상적인 사용자 동작이 발생할 경우 스냅샷을 찍거나 사용자 액세스를 제한하는 등의 작업을 실행합니다.

특정 기기나 모든 기기에 정책을 설정할 수 있습니다. 응답 정책을 설정하려면 관리 **>** 자동 응답 정책*을 선택하고 해당 *+정책 버튼을 클릭합니다. 공격이나 경고에 대한 정책을 만들 수 있습니다.



정책을 고유한 이름으로 저장해야 합니다.

자동 응답 작업(예: 스냅샷 찍기)을 비활성화하려면 해당 작업의 선택을 취소하고 정책을 저장하기만 하면 됩니다.

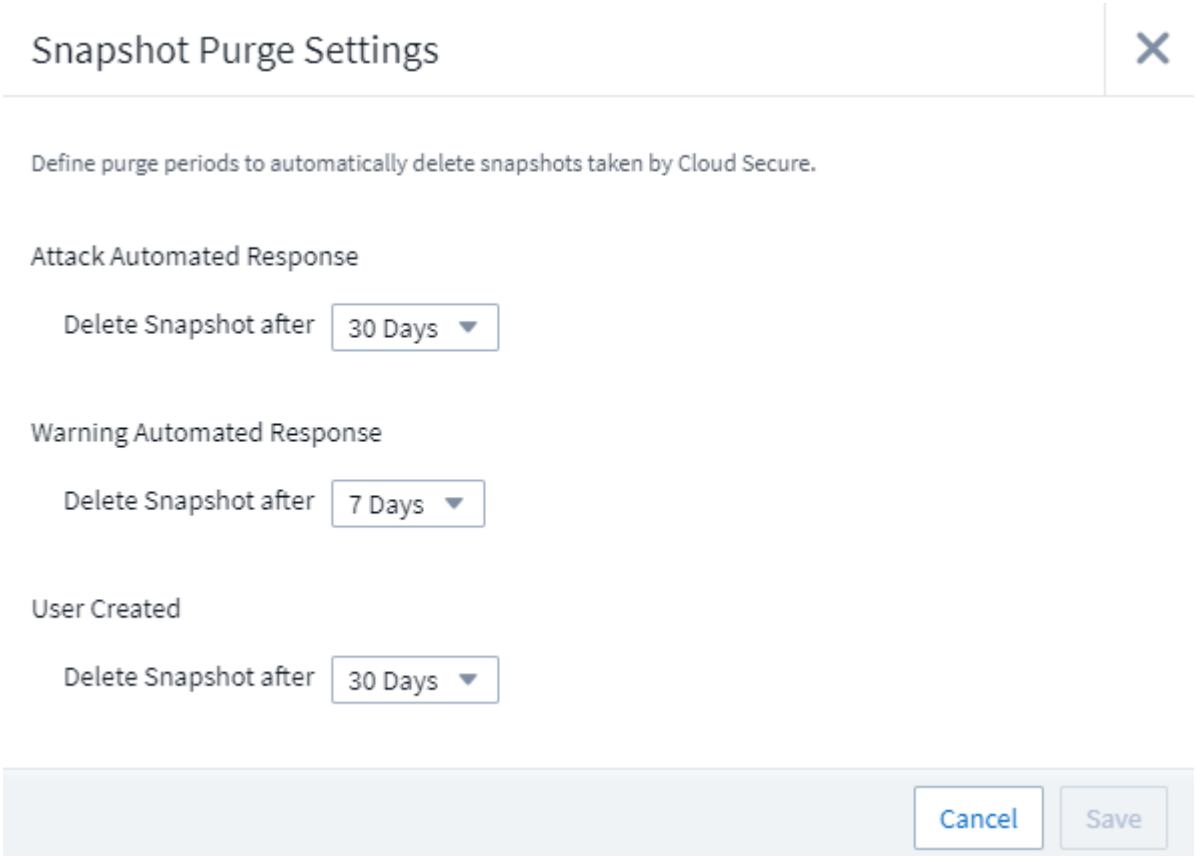
지정된 장치(또는 선택한 경우 모든 장치)에 대한 알림이 발생하면 자동 응답 정책이 데이터 스냅샷을 만듭니다. 스냅샷 상태는 다음에서 확인할 수 있습니다."알림 세부 정보 페이지" .

를 참조하십시오"사용자 액세스 제한" IP를 기준으로 사용자 접근을 제한하는 방법에 대한 자세한 내용은 해당 페이지를 참조하세요.

알림이 생성되고 작업이 수행될 때 알림을 받으려면 정책에 하나 이상의 웹후크를 첨부할 수 있습니다. 정책에 웹훅을 10개 이하로 추가하는 것이 좋습니다. 정책이 일시 중지되면 웹훅 알림이 트리거되지 않는다는 점을 명심하세요.

정책의 드롭다운 메뉴에서 옵션을 선택하여 자동 응답 정책을 수정하거나 일시 중지할 수 있습니다.

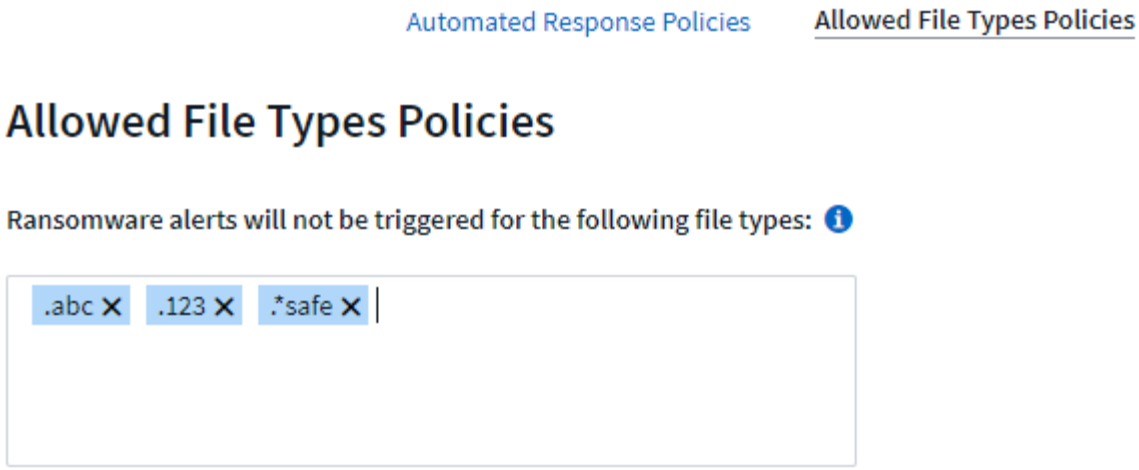
Workload Security는 스냅샷 정리 설정에 따라 하루에 한 번 스냅샷을 자동으로 삭제합니다.



허용된 파일 유형 정책

알려진 파일 확장자에 대한 파일 변조 공격이 감지되어 경고 화면에 경고가 생성되는 경우, 불필요한 경고를 방지하기 위해 해당 파일 확장자를 허용된 파일 형식 목록에 추가할 수 있습니다.

*작업 부하 보안 > 정책*으로 이동하여 허용되는 파일 유형 정책 탭으로 이동합니다.



허용된 파일 형식 목록에 추가되면 해당 파일 형식에 대해서는 파일 변조 공격 경고가 생성되지 않습니다. 허용 파일 형식 정책은 파일 변조 감지에만 적용된다는 점에 유의하십시오.

예를 들어, *test.txt*_라는 파일의 이름이 _*test.txt.abc*_로 변경되었는데 워크로드 보안에서 _*.abc* 확장자 때문에 파일 변조 공격으로 감지하는 경우, *.abc* 확장자를 허용된 파일 형식 목록에 추가할 수 있습니다. 해당 목록에 추가된 후에는 *.abc* 확장자를 가진 파일에 대해 더 이상 파일 변조 공격이 발생하지 않습니다.

허용되는 파일 유형은 정확한 일치(예: ".abc") 또는 표현식(예: "**.type", ".type**" 또는 "**type**")일 수 있습니다. “.a*c”, “.p*f” 유형의 표현식은 지원되지 않습니다.

ONTAP 자율형 랜섬웨어 보호와 통합

ONTAP 자율 보호 기능은 NAS(NFS 및 SMB) 환경에서 워크로드 분석을 사용하여 악의적인 공격이나 무단 데이터 수정을 나타낼 수 있는 파일 내 비정상적인 활동을 사전에 감지하고 경고합니다.

ARP에 대한 추가 세부 정보 및 라이센스 요구 사항은 다음과 같습니다."여기" .

Workload Security는 ONTAP 과 통합되어 ARP 이벤트를 수신하고 추가적인 분석 및 자동 응답 계층을 제공합니다.

Workload Security는 ONTAP 에서 ARP 이벤트를 수신하고 다음 작업을 수행합니다.

1. 볼륨 암호화 이벤트와 사용자 활동을 연관시켜 피해를 일으키는 사람을 파악합니다.
2. 자동 응답 정책을 구현합니다(정의된 경우)
3. 포렌식 기능을 제공합니다:
    - 고객이 데이터 침해에 대한 조사를 수행할 수 있도록 허용합니다.
    - 영향을 받은 파일을 식별하여 더 빠른 복구와 데이터 침해 조사 수행에 도움이 됩니다.

필수 조건

1. 최소 ONTAP 버전: 9.11.1
2. ARP가 활성화된 볼륨. ARP 활성화에 대한 자세한 내용은 다음을 참조하세요."여기" . ARP는 OnCommand System Manager 통해 활성화되어야 합니다. 워크로드 보안은 ARP를 활성화할 수 없습니다.

3. 워크로드 보안 수집기는 클러스터 IP를 통해 추가해야 합니다.
4. 이 기능을 사용하려면 클러스터 수준 자격 증명이 필요합니다. 즉, SVM을 추가할 때는 클러스터 수준 자격 증명을 사용해야 합니다.

사용자 권한이 필요합니다

클러스터 관리 자격 증명을 사용하는 경우 새로운 권한이 필요하지 않습니다.

사용자 지정 사용자(예: *csuser*)에게 권한이 부여된 경우 아래 단계에 따라 Workload Security에 ONTAP 에서 ARP 관련 정보를 수집할 수 있는 권한을 부여하세요.

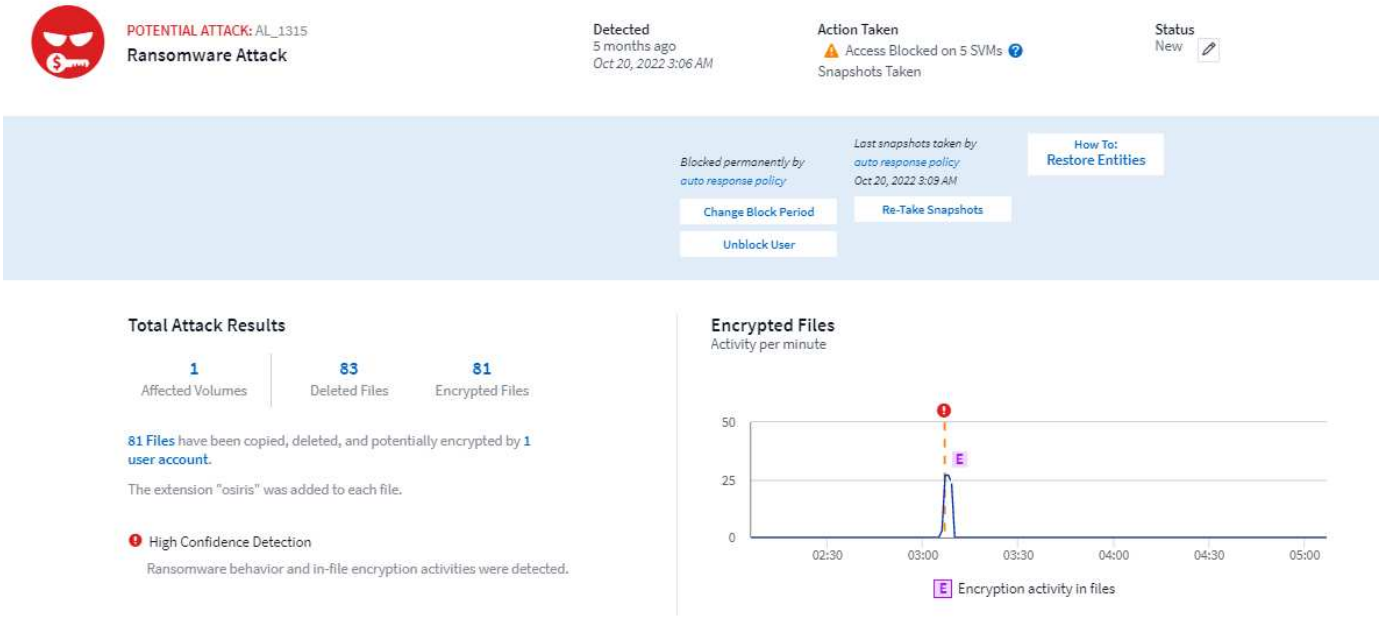
클러스터 자격 증명이 있는 _csuser_의 경우 ONTAP 명령줄에서 다음을 수행합니다.

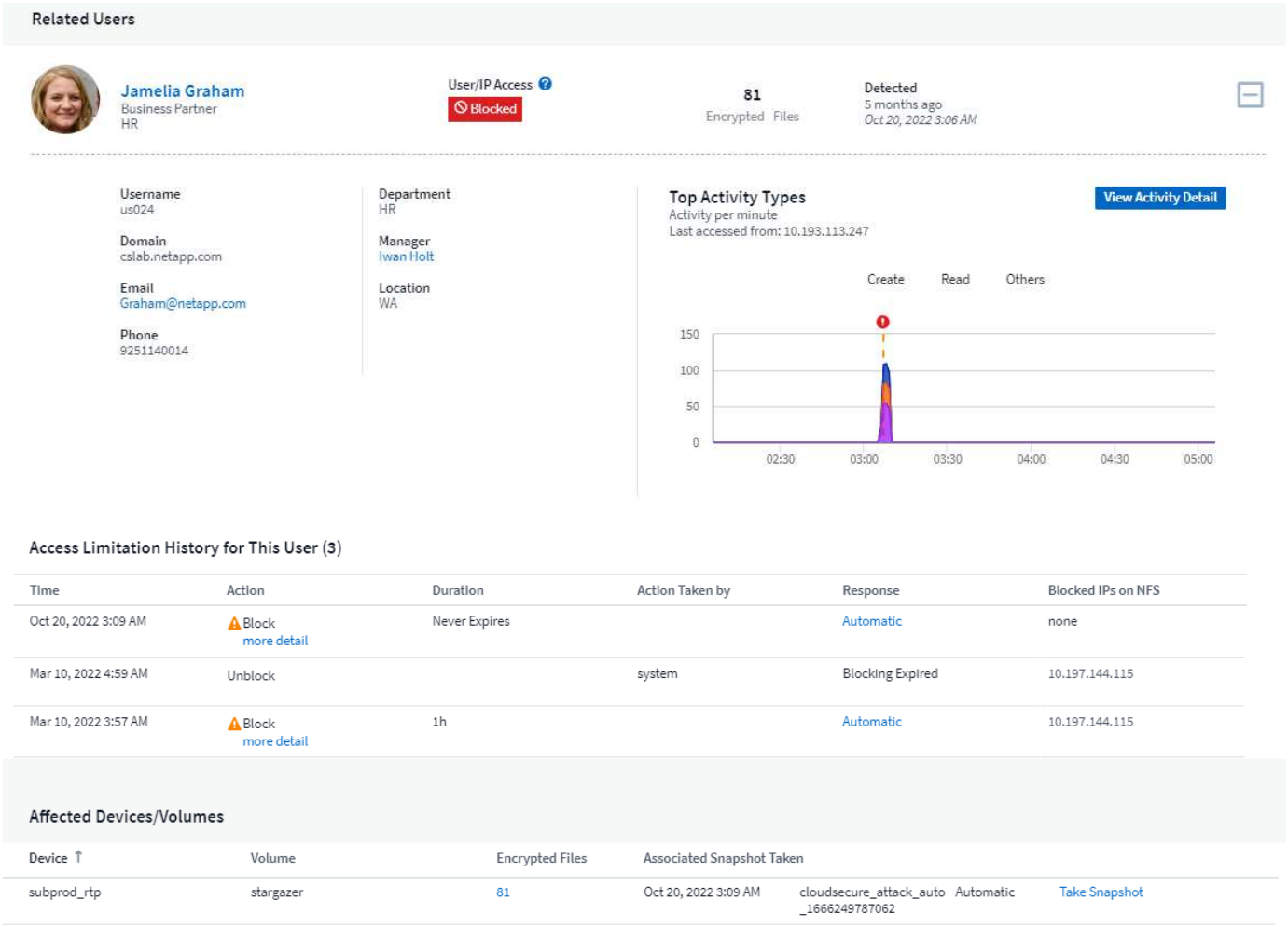
```
security login role create -role csrole -cmddirname "volume" -access
readonly
security login role create -role csrole -cmddirname "security anti-
ransomware volume" -access readonly
```

다른 구성에 대해 자세히 알아보세요"ONTAP 권한" .

샘플 알림

ARP 이벤트로 인해 생성된 경고 샘플은 아래와 같습니다.





높은 신뢰도 배너는 해당 공격이 파일 암호화 활동과 함께 파일 변조 행위를 보였음을 나타냅니다. 암호화된 파일 그래프는 ARP 솔루션이 볼륨 암호화 활동을 감지한 시점을 타임스탬프로 나타냅니다.

제한 사항

Workload Security에서 SVM을 모니터링하지 않지만 ONTAP 에서 ARP 이벤트를 생성한 경우 Workload Security에서 해당 이벤트를 계속 수신하여 표시합니다. 하지만 알림과 관련된 법의학적 정보와 사용자 매핑은 캡처되거나 표시되지 않습니다.

문제 해결

알려진 문제와 해결 방법은 다음 표에 설명되어 있습니다.

문제:	해결:
공격이 감지된 후 24시간 이내에 이메일 알림이 전송됩니다. UI에서는 Data Infrastructure Insights Workload Security에서 이메일을 수신하기 24시간 전에 알림이 표시됩니다.	ONTAP 에서 랜섬웨어 감지 이벤트를 Data Infrastructure Insights Workload Security(즉, Workload Security)로 보내면 이메일이 전송됩니다. 이벤트에는 공격 목록과 타임스탬프가 포함되어 있습니다. 워크로드 보안 UI는 공격을 받은 첫 번째 파일의 경고 타임스탬프를 표시합니다. 특정 수의 파일이 인코딩되면 ONTAP 랜섬웨어 감지 이벤트를 Data Infrastructure Insights 로 보냅니다. 따라서 UI에 알림이 표시되는 시간과 이메일이 전송되는 시간 사이에 차이가 있을 수 있습니다.

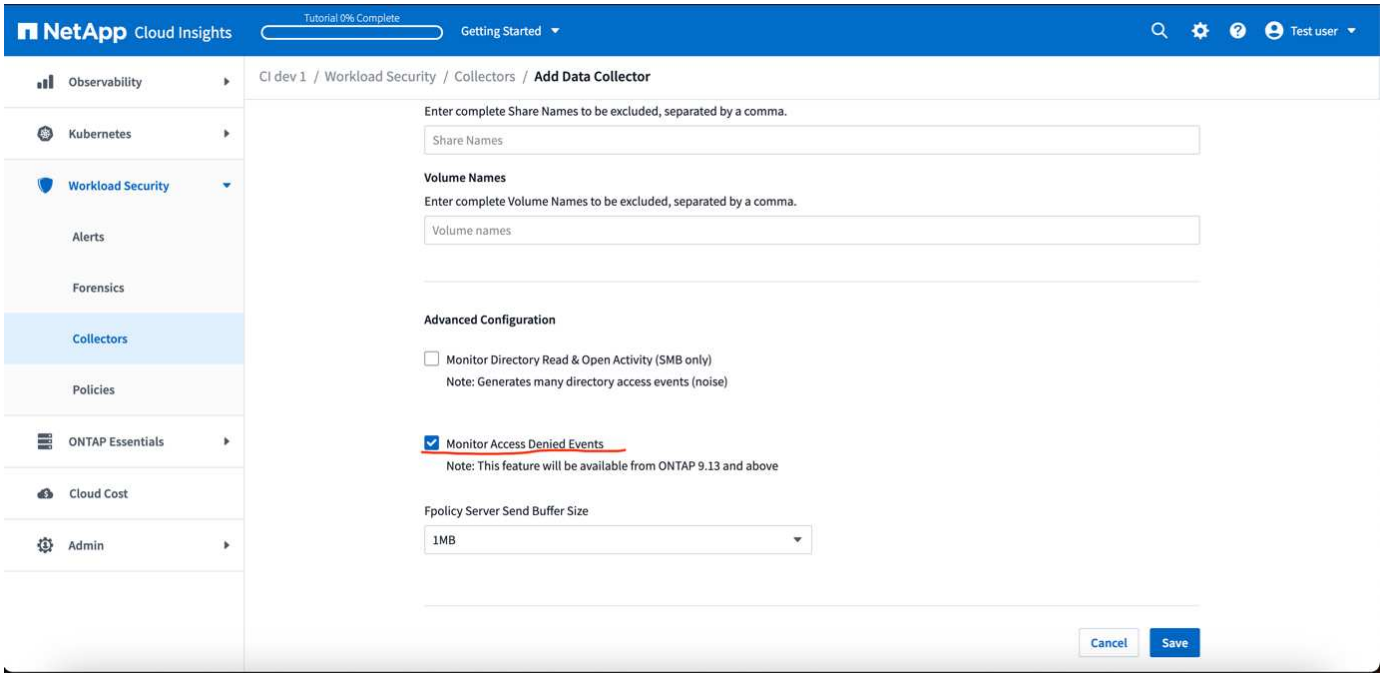
ONTAP 액세스와의 통합이 거부되었습니다.

ONTAP 액세스 거부 기능은 NAS 환경(NFS 및 SMB)에서 작업 부하 분석을 사용하여 실패한 파일 작업(즉, 사용자가 권한이 없는 작업을 수행하려는 경우)을 사전에 감지하고 경고합니다. 이러한 실패한 파일 작업 알림은(특히 보안 관련 실패의 경우) 초기 단계에서 내부자 공격을 차단하는 데 더욱 도움이 됩니다.

Data Infrastructure Insights Workload Security는 ONTAP 과 통합되어 액세스 거부 이벤트를 수신하고 추가적인 분석 및 자동 대응 계층을 제공합니다.

필수 조건

- 최소 ONTAP 버전: 9.13.0.
- 워크로드 보안 관리자는 새로운 수집기를 추가하거나 기존 수집기를 편집하는 동안 고급 구성에서 액세스 거부 이벤트 모니터링 확인란을 선택하여 액세스 거부 기능을 활성화해야 합니다.



사용자 권한이 필요합니다

클러스터 관리 자격 증명을 사용하여 데이터 수집기를 추가한 경우 새로운 권한이 필요하지 않습니다.

사용자 지정 사용자(예: *csuser*)를 사용하여 Collector를 추가하고 해당 사용자에게 권한이 부여된 경우 아래 단계에 따라 Workload Security에 ONTAP 에서 액세스 거부 이벤트에 등록하는 데 필요한 권한을 부여합니다.

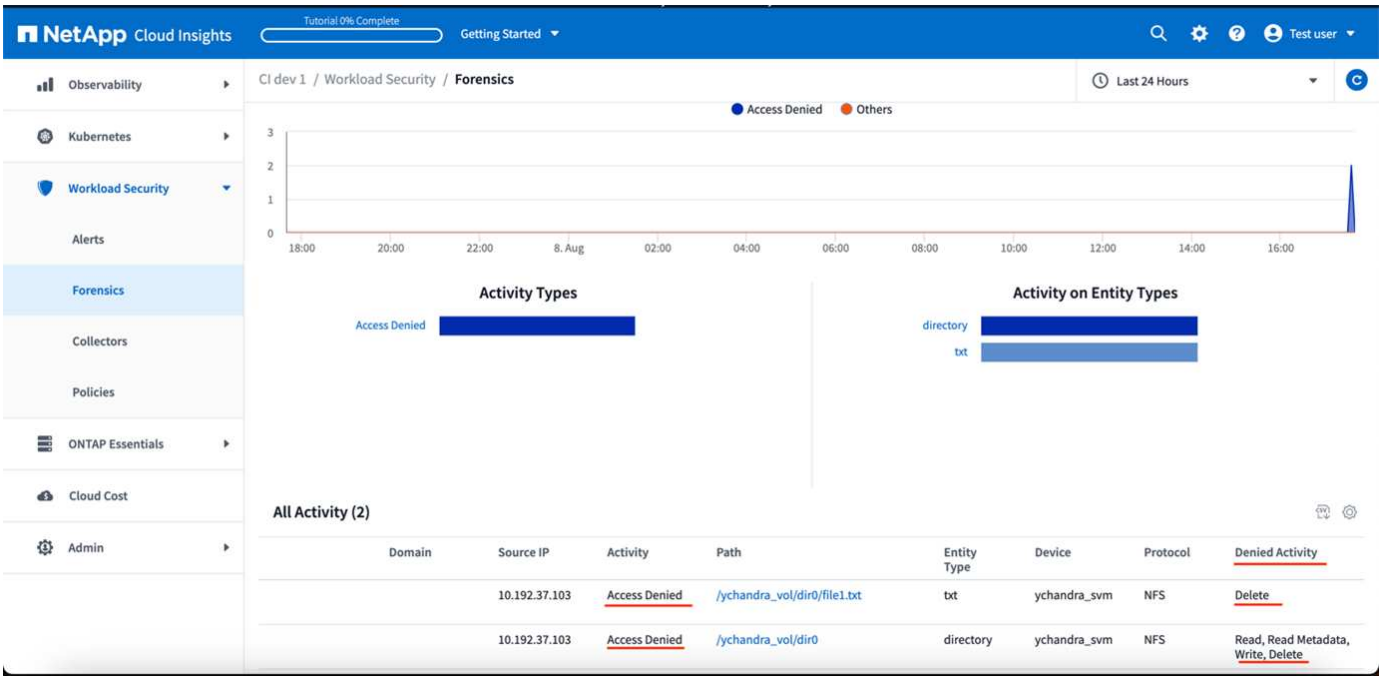
cluster 자격 증명이 있는 csuser의 경우 ONTAP 명령줄에서 다음 명령을 실행합니다. 이 권한이 이미 존재할 수도 있습니다.

```
 security login role create -role csrole -cmddirname "vserver fpolicy"
-access all
_SVM_ 자격 증명을 사용하는 csuser의 경우 ONTAP 명령줄에서 다음 명령을 실행합니다.  이 권한이 이미 존재할 수도 있습니다.
```

```
 security login role create -vserver <vservername> -role csrole
-cmddirname "vserver fpolicy" -access all
다른 구성에 대해 자세히 알아보세요link:task_add_collector_svm.html["ONTAP 권한"] .
```

액세스 거부 이벤트

ONTAP 시스템에서 이벤트를 수집하면 워크로드 보안 포렌식 페이지에 액세스 거부 이벤트가 표시됩니다. 표시된 정보 외에도 기어 아이콘에서 표에 원하는 활동 열을 추가하여 특정 작업에 대해 누락된 사용자 권한을 볼 수 있습니다.



공격 방지를 위해 사용자 접근을 차단합니다.

탐지된 공격은 즉시 차단해야 합니다. 손상된 사용자의 접근을 차단하여 추가적인 데이터

손상이나 유출을 방지하십시오. 워크로드 보안은 자동 대응 정책을 통한 자동 차단과 경고 또는 사용자 세부 정보 페이지에서의 수동 개입을 모두 지원하여 보안 대응을 유연하게 제어할 수 있도록 합니다. 접근 제한은 모니터링되는 모든 스토리지 볼륨에 자동으로 적용되며, 자동 복원을 위한 시간 제한이 있습니다.

사용자는 SMB에 대해 직접 차단되고, 공격을 일으키는 호스트 머신의 IP 주소는 NFS에 대해 차단됩니다. 해당 머신 IP 주소는 Workload Security에서 모니터링하는 스토리지 가상 머신(SVM)에 액세스하는 것이 차단됩니다.

예를 들어, Workload Security가 10개의 SVM을 관리하고 그 중 4개의 SVM에 대해 자동 응답 정책이 구성되어 있다고 가정해 보겠습니다. 공격이 4개의 SVM 중 하나에서 시작된 경우, 사용자 액세스는 10개의 SVM 모두에서 차단됩니다. 원래 SVM에서 스냅샷이 계속 생성됩니다.

SMB용으로 구성된 SVM 1개, NFS용으로 구성된 SVM 1개, NFS와 SMB용으로 구성된 나머지 2개로 구성된 SVM이 4개 있는 경우, 공격이 4개 SVM 중 하나에서 시작되면 모든 SVM이 차단됩니다.

사용자 액세스 차단을 위한 전제 조건

이 기능을 사용하려면 클러스터 수준 자격 증명이 필요합니다.

클러스터 관리 자격 증명을 사용하는 경우 새로운 권한이 필요하지 않습니다.

사용자 지정 사용자(예: *csuser*)에게 권한이 부여된 경우 아래 단계에 따라 Workload Security에 사용자를 차단할 수 있는 권한을 부여하세요.

클러스터 자격 증명이 있는 csuser의 경우 ONTAP 명령줄에서 다음을 수행합니다.

```
security login role create -role csrole -cmddirname "vserver export-policy
rule" -access all
security login role create -role csrole -cmddirname set -access all
security login role create -role csrole -cmddirname "vserver cifs session"
-access all
security login role create -role csrole -cmddirname "vserver services
access-check authentication translate" -access all
security login role create -role csrole -cmddirname "vserver name-mapping"
-access all
```

권한 섹션을 검토하세요."ONTAP SVM 데이터 수집기 구성" 페이지도 마찬가지.

이 기능을 어떻게 활성화하나요?

- 워크로드 보안에서 *워크로드 보안 > 정책 > 자동 응답 정책*으로 이동합니다. *+공격 정책*을 선택하세요.
- _사용자 파일 액세스 차단_을 선택합니다.

사용자 접근 자동 차단을 설정하는 방법은 무엇입니까?

- 새로운 공격 정책을 만들거나 기존 공격 정책을 편집합니다.
- 공격 정책을 모니터링할 SVM을 선택합니다.

- "사용자 파일 액세스 차단" 확인란을 클릭합니다. 이 옵션을 선택하면 해당 기능이 활성화됩니다.
- "기간"에서 차단이 적용될 기간을 선택합니다.
- 자동 사용자 차단을 테스트하려면 다음을 통해 공격을 시뮬레이션할 수 있습니다."시뮬레이션된 스크립트" .

시스템에 차단된 사용자가 있는지 어떻게 알 수 있나요?

- 알림 목록 페이지에서는 사용자가 차단된 경우 화면 상단에 배너가 표시됩니다.
- 배너를 클릭하면 차단된 사용자 목록을 볼 수 있는 "사용자" 페이지로 이동합니다.
- "사용자" 페이지에 "사용자/IP 액세스"라는 열이 있습니다. 해당 열에는 현재 사용자 차단 상태가 표시됩니다.

사용자 액세스를 수동으로 제한하고 관리합니다.

- 알림 세부 정보 또는 사용자 세부 정보 화면으로 이동한 다음 해당 화면에서 사용자를 수동으로 차단하거나 복원할 수 있습니다.

사용자 접근 제한 내역

알림 세부 정보 및 사용자 세부 정보 페이지의 사용자 패널에서 사용자의 액세스 제한 기록에 대한 감사를 볼 수 있습니다. 여기에는 시간, 작업(차단, 차단 해제), 기간, 수행된 작업, 수동/자동, NFS에 대한 영향을 받은 IP가 포함됩니다.

해당 기능을 비활성화하려면 어떻게 해야 하나요?

언제든지 해당 기능을 비활성화할 수 있습니다. 시스템에 제한된 사용자가 있는 경우 먼저 해당 사용자의 접근 권한을 복구해야 합니다.

- 워크로드 보안에서 *워크로드 보안 > 정책 > 자동 응답 정책*으로 이동합니다. *+공격 정책*을 선택하세요.
- _사용자 파일 액세스 차단_을 선택 해제합니다.

해당 기능은 모든 페이지에서 숨겨집니다.

NFS에 대한 IP 수동 복원

Workload Security 평가판이 만료되거나 에이전트/수집기가 다운된 경우 다음 단계에 따라 ONTAP 에서 모든 IP를 수동으로 복원하세요.

1. SVM의 모든 내보내기 정책을 나열합니다.

```
contrail-qa-fas8020:> export-policy rule show -vserver <svm name>
             Policy          Rule    Access   Client                RO
Vserver      Name            Index   Protocol Match                 Rule
------------ --------------- ------  -------- --------------------
---------
svm0         default         1       nfs3,    cloudsecure_rule,     never
                                     nfs4,    10.11.12.13
                                     cifs
svm1         default         4       cifs,    0.0.0.0/0             any
                                     nfs
svm2         test            1       nfs3,    cloudsecure_rule,     never
                                     nfs4,    10.11.12.13
                                     cifs
svm3         test            3       cifs,    0.0.0.0/0             any
                                     nfs,
                                     flexcache
4 entries were displayed.
```

2. SVM의 모든 정책에서 클라이언트 일치 항목으로 "cloudsecure_rule"이 있는 규칙을 삭제하려면 해당 RuleIndex를 지정합니다. 워크로드 보안 규칙은 일반적으로 1입니다.

```
 contrail-qa-fas8020:*> export-policy rule delete -vserver <svm name>
-policyname * -ruleindex 1
. 워크로드 보안 규칙이 삭제되었는지 확인합니다(확인을 위한 선택 단계).
```

```
contrail-qa-fas8020:*> export-policy rule show -vserver <svm name>
             Policy          Rule    Access   Client                RO
Vserver      Name            Index   Protocol Match                 Rule
------------ --------------- ------  -------- --------------------
---------
svm0         default         4        cifs,    0.0.0.0/0             any
                                     nfs
svm2         test            3        cifs,    0.0.0.0/0             any
                                     nfs,
                                     flexcache
2 entries were displayed.
```

SMB에 대한 사용자 수동 복원

Workload Security 평가판이 만료되거나 에이전트/수집기가 다운된 경우 다음 단계에 따라 ONTAP 에서 모든 사용자를 수동으로 복원하세요.

Workload Security에서 차단된 사용자 목록은 사용자 목록 페이지에서 확인할 수 있습니다.

1. 클러스터 *admin* 자격 증명을 사용하여 ONTAP 클러스터(사용자 차단을 해제하려는 클러스터)에 로그인합니다. (Amazon FSx 의 경우 FSx 자격 증명으로 로그인하세요).
2. 다음 명령을 실행하여 모든 SVM에서 Workload Security for SMB에 의해 차단된 모든 사용자를 나열합니다.

```
vserver name-mapping show -direction win-unix -replacement " "
```

```
Vserver:   <vservername>
Direction: win-unix
Position Hostname         IP Address/Mask
-------- ---------------- ----------------
1        -                -                    Pattern: CSLAB\\US040
                                           Replacement:
2        -                -                    Pattern: CSLAB\\US030
                                           Replacement:
2 entries were displayed.
```

위의 출력에서 2명의 사용자(US030, US040)가 CSLAB 도메인을 사용하여 차단되었습니다.

1. 위의 출력에서 위치를 확인한 후 다음 명령을 실행하여 사용자 차단을 해제합니다.

```
 vserver name-mapping delete -direction win-unix -position <position>
```

. 다음 명령을 실행하여 사용자 차단이 해제되었는지 확인하세요.

```
vserver name-mapping show -direction win-unix -replacement " "
```

이전에 차단된 사용자에 대해서는 아무 항목도 표시되지 않습니다.

문제 해결

문제	이것을 시도해보세요
일부 사용자는 공격을 받고 있음에도 제한을 받지 않습니다.	1. SVM의 데이터 수집기와 에이전트가 실행 상태인지 확인하세요. 데이터 수집기와 에이전트가 중지되면 워크로드 보안이 명령을 보낼 수 없습니다. 2. 이는 사용자가 이전에 사용되지 않은 새로운 IP를 가진 컴퓨터에서 저장소에 액세스했을 수 있기 때문입니다. 제한은 사용자가 저장소에 액세스하는 호스트의 IP 주소를 통해 발생합니다. UI(경고 세부 정보 > 이 사용자에 대한 액세스 제한 기록 > 영향을 받는 IP)에서 제한된 IP 주소 목록을 확인하세요. 사용자가 제한된 IP와 다른 IP를 가진 호스트에서 스토리지에 액세스하는 경우에도 사용자는 제한되지 않은 IP를 통해 스토리지에 액세스할 수 있습니다. 사용자가 IP가 제한된 호스트에서 액세스하려고 하면 저장소에 액세스할 수 없습니다.
수동으로 액세스 제한을 클릭하면 "이 사용자의 IP 주소는 이미 제한되었습니다"라는 메시지가 표시됩니다.	제한할 IP는 이미 다른 사용자에게 제한을 받고 있습니다.
정책을 수정할 수 없습니다. 이유: 해당 명령에 대한 권한이 없습니다.	csuser를 사용하는지 확인하세요. 위에서 언급한 대로 사용자에게 권한이 부여됩니다.
NFS의 경우 사용자(IP 주소) 차단이 작동하지만 SMB/CIFS의 경우 "SID에서 DomainName으로의 변환에 실패했습니다."라는 오류 메시지가 표시됩니다. 사유 시간 초과: 소켓이 설정되지 않았습니다”	*csuser_*에게 *ssh*를 수행할 권한이 없는 경우 이런 일이 발생할 수 있습니다. *(*클러스터 수준에서 연결을 보장한 다음 사용자가 *ssh*를 수행할 수 있는지 확인합니다*).* *_csuser* 역할에는 이러한 권한이 필요합니다. https://docs.netapp.com/us-en/cloudinsights/cs_restrict_user_access.html#prerequisites-for-user-access-blocking 클러스터 자격 증명이 있는 _csuser_의 경우 ONTAP 명령줄에서 다음을 수행합니다. security login role create -role csrole -cmddirname "vserver export-policy rule" -access all security login role create -role csrole -cmddirname set -access all security login role create -role csrole -cmddirname "vserver cifs session" -access all security login role create -role csrole -cmddirname "vserver services access-check authentication translate" -access all security login role create -role csrole -cmddirname "vserver name-mapping" -access all _csuser_를 사용하지 않고 클러스터 수준에서 관리자 사용자를 사용하는 경우 관리자 사용자에게 ONTAP 에 대한 ssh 권한이 있는지 확인합니다.

문제	이것을 시도해보세요
사용자가 차단되어야 할 때 *SID* 변환에 실패했습니다. _이유: 255: 오류: 명령 실패: 해당 명령에 대한 권한이 없습니다. 오류: "access-check"는 인식할 수 없는 명령입니다._라는 오류 메시지가 나타납니다.	이는 _csuser_에게 올바른 권한이 없는 경우 발생할 수 있습니다. 보다 "사용자 액세스 차단을 위한 전제 조건" 자세한 내용은. 권한을 적용한 후에는 ONTAP 데이터 수집기와 사용자 디렉터리 데이터 수집기를 다시 시작하는 것이 좋습니다. 필요한 권한 명령은 아래와 같습니다. ---- 보안 로그인 역할 생성 -role csrole -cmddirname "vserver 내보내기 정책 규칙" -액세스 모두 보안 로그인 역할 생성 -role csrole -cmddirname 설정 -액세스 모두 보안 로그인 역할 생성 -role csrole -cmddirname "vserver cifs 세션" -액세스 모두 보안 로그인 역할 생성 -role csrole -cmddirname "vserver 서비스 액세스 확인 인증 변환" -액세스 모두 보안 로그인 역할 생성 -role csrole -cmddirname "vserver 이름 매핑" -액세스 모두 ----

워크로드 보안: 파일 변조 시뮬레이션

이 페이지의 지침에 따라 포함된 파일 변조 시뮬레이션 스크립트를 사용하여 워크로드 보안을 테스트하거나 시연하기 위한 파일 변조를 시뮬레이션할 수 있습니다.

시작하기 전에 주의할 사항

- 파일 변조 시뮬레이션 스크립트는 Linux에서만 작동합니다. 시뮬레이션 스크립트는 사용자가 ONTAP ARP를 워크로드 보안과 통합한 경우 높은 신뢰도의 경고를 생성해야 합니다.
- 워크로드 보안은 ONTAP 버전이 9.15 이상인 경우에만 NFS 4.1에서 생성된 이벤트와 알림을 감지합니다.
- 스크립트는 Workload Security 에이전트 설치 파일과 함께 제공됩니다. Workload Security 에이전트가 설치된 모든 컴퓨터에서 사용할 수 있습니다.
- Workload Security 에이전트 머신 자체에서 스크립트를 실행할 수 있으므로 다른 Linux 머신을 준비할 필요가 없습니다. 하지만 다른 시스템에서 스크립트를 실행하고 싶다면, 스크립트를 복사해서 해당 시스템에서 실행하면 됩니다.
- 사용자는 자신의 선호도와 시스템 요구 사항에 따라 Python이나 셸 스크립트를 선택할 수 있습니다.
- Python 스크립트에는 필수 설치가 필요합니다. 파이썬을 사용하고 싶지 않다면 쉘 스크립트를 사용하세요.

가이드라인:

이 스크립트는 암호화할 파일이 상당수(하위 폴더의 파일 포함, 이상적으로는 100개 이상) 있는 폴더가 있는 SVM에서 실행되어야 합니다. 파일이 비어 있지 않은지 확인하세요.

알림을 생성하려면 테스트 데이터를 생성하기 전에 수집기를 일시적으로 일시 중지하세요. 샘플 파일이 생성되면 수집기를 다시 시작하고 암호화 프로세스를 시작합니다.

단계:

시스템 준비:

먼저, 대상 볼륨을 머신에 마운트합니다. NFS 또는 CIFS 내보내기를 마운트할 수 있습니다.

Linux에서 **NFS** 내보내기를 마운트하려면:

```
mount -t nfs -o vers=4.0 10.193.177.158:/svmvol1 /mntpt
mount -t nfs -o vers=4.0 Vserver data IP>:/nfsvol /destinationlinuxfolder
```

NFS 버전 4.1을 마운트하지 마세요. Fpolicy에서 지원하지 않습니다.

Linux에서 **CIFS**를 마운트하려면:

```
mount -t cifs //10.193.77.91/sharedfolderincluster
/root/destinationfolder/ -o username=raisa
```

ONTAP Autonomous 랜섬웨어 보호 활성화**(**선택 사항**):**

ONTAP 클러스터 버전이 9.11.1 이상인 경우 ONTAP 명령 콘솔에서 다음 명령을 실행하여 ONTAP 랜섬웨어 보호 서비스를 활성화할 수 있습니다.

```
 security anti-ransomware volume enable -volume [volume_name] -vserver
[svm_name]
다음으로, 데이터 수집기를 설정합니다.
```

1. 아직 구성하지 않았다면 Workload Security 에이전트를 구성합니다.
2. 아직 SVM 데이터 수집기를 구성하지 않았다면 구성합니다.
3. 데이터 수집기를 구성하는 동안 마운트 프로토콜이 선택되었는지 확인하세요.

프로그래밍 방식으로 샘플 파일을 생성합니다.

파일을 생성하기 전에 먼저 중지하거나"데이터 수집기를 일시 중지합니다" 처리 중.

시뮬레이션을 실행하기 전에 먼저 암호화할 파일을 추가해야 합니다. 암호화할 파일을 대상 폴더에 수동으로 복사하거나, 포함된 스크립트 중 하나를 사용하여 프로그래밍 방식으로 파일을 생성할 수 있습니다. 어떤 방법을 사용하든 암호화할 파일이 최소 100개 이상 있는지 확인하세요.

프로그래밍 방식으로 파일을 생성하기로 선택한 경우 Shell이나 Python을 사용할 수 있습니다.

껍데기**:**

1. 에이전트 상자에 로그인하세요.
2. 파일러의 SVM에서 에이전트 머신으로 NFS 또는 CIFS 공유를 마운트합니다. 해당 폴더로 이동하세요.
3. 에이전트 설치 디렉토리(%AGENT_INSTALL_DIR/agent/install/ransomware_simulation/shell/create_dataset.sh)에서 스크립트를 대상 마운트 위치로 복사합니다.
4. 마운트된 디렉토리(예: /root/demo) 내의 스크립트를 사용하여 다음 명령을 실행하여 테스트 데이터 세트 폴더와 파일을 생성합니다.

```
'./create_dataset.sh'
```
. 이렇게 하면 "test_dataset"이라는 디렉토리 아래의 mount 폴더 안에 다양한 확장자를 가진 비어 있지 않은 파일 100개가 생성됩니다.

파이썬:

Python 스크립트 필수 조건:

- Python을 설치합니다(아직 설치되지 않았다면).
  - Python 3.5.2 이상을 다운로드하세요. https://www.python.org/ .
  - Python 설치를 확인하려면 다음을 실행하세요. `python --version` .
  - Python 스크립트는 3.5.2 버전부터 테스트되었습니다.
- 아직 pip가 설치되어 있지 않다면 설치하세요:
  - get-pip.py 스크립트를 다운로드하세요. https://bootstrap.pypa.io/ .
  - pip를 사용하여 설치하세요 `python get-pip.py` .
  - pip 설치를 확인하세요 `pip --version` .
- PyCryptodome 라이브러리:
  - 이 스크립트는 PyCryptodome 라이브러리를 사용합니다.
  - PyCryptodome을 설치하세요 `pip install pycryptodome` .
  - PyCryptodome 설치를 실행하여 확인하세요. `pip show pycryptodome` .

Python 파일 생성 스크립트:

1. 에이전트 상자에 로그인하세요.
2. 파일러의 SVM에서 에이전트 머신으로 NFS 또는 CIFS 공유를 마운트합니다. 해당 폴더로 이동하세요.
3. 에이전트 설치 디렉토리(%AGENT_INSTALL_DIR/agent/install/ransomware_simulation/python/create_dataset.py)에서 스크립트를 대상 마운트 위치로 복사합니다.
4. 마운트된 디렉토리(예: /root/demo) 내의 스크립트를 사용하여 다음 명령을 실행하여 테스트 데이터 세트 폴더와 파일을 생성합니다.

```
'python create_dataset.py'
```
. 이렇게 하면 "test_dataset"이라는 디렉토리 아래의 마운트 폴더 내부에 다양한 확장자를 가진 비어 있지 않은 파일 100개가 생성됩니다.

수집기를 재개합니다

이 단계를 따르기 전에 수집기를 일시 중지한 경우 샘플 파일이 생성되면 수집기를 다시 시작하세요.

프로그래밍 방식으로 샘플 파일을 생성합니다.

파일을 생성하기 전에 먼저 중지하거나"데이터 수집기를 일시 중지합니다" 처리 중.

파일 변조 경고를 생성하려면 워크로드 보안에서 파일 변조 경고를 시뮬레이션하는 포함된 스크립트를 실행하면 됩니다.

껍데기:

1. 에이전트 설치 디렉토리(%AGENT_INSTALL_DIR/agent/install/ransomware_simulation/shell/simulate_attack.sh)에서 스크립트를 대상 마운트 위치로 복사합니다.
2. 마운트된 디렉토리(예: /root/demo) 내의 스크립트를 사용하여 다음 명령을 실행하여 테스트 데이터 세트를 암호화합니다.

```
 './simulate_attack.sh'
. 이렇게 하면 "test_dataset" 디렉토리에 생성된 샘플 파일이 암호화됩니다.
```

파이썬:

1. 에이전트 설치 디렉토리(%AGENT_INSTALL_DIR/agent/install/ransomware_simulation/python/simulate_attack.py)에서 스크립트를 대상 마운트 위치로 복사합니다.
2. Python 스크립트 필수 구성 요소 섹션에 따라 Python 필수 구성 요소가 설치되었음을 참고하세요.
3. 마운트된 디렉토리(예: /root/demo) 내의 스크립트를 사용하여 다음 명령을 실행하여 테스트 데이터 세트를 암호화합니다.

```
 'python simulate_attack.py'
. 이렇게 하면 "test_dataset" 디렉토리에 생성된 샘플 파일이 암호화됩니다.
```

워크로드 보안에서 경고 생성

시뮬레이터 스크립트 실행이 완료되면 몇 분 내에 웹 UI에 알림이 표시됩니다.

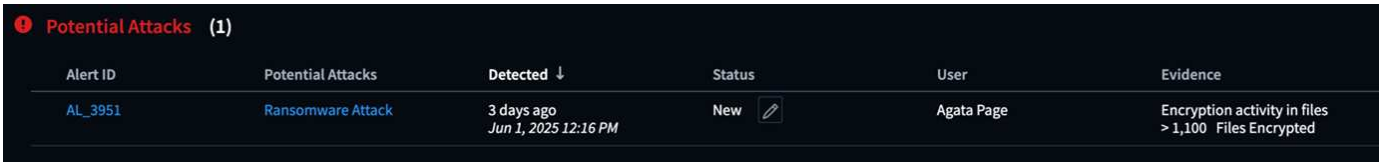
참고: 다음 조건이 모두 충족되는 경우, 높은 신뢰도 경보가 생성됩니다.

1. 9.11.1보다 높은 SVM의 ONTAP 버전을 모니터링했습니다.
2. ONTAP 자율 랜섬웨어 보호 구성됨
3. 워크로드 보안 데이터 수집기가 클러스터 모드에 추가되었습니다.

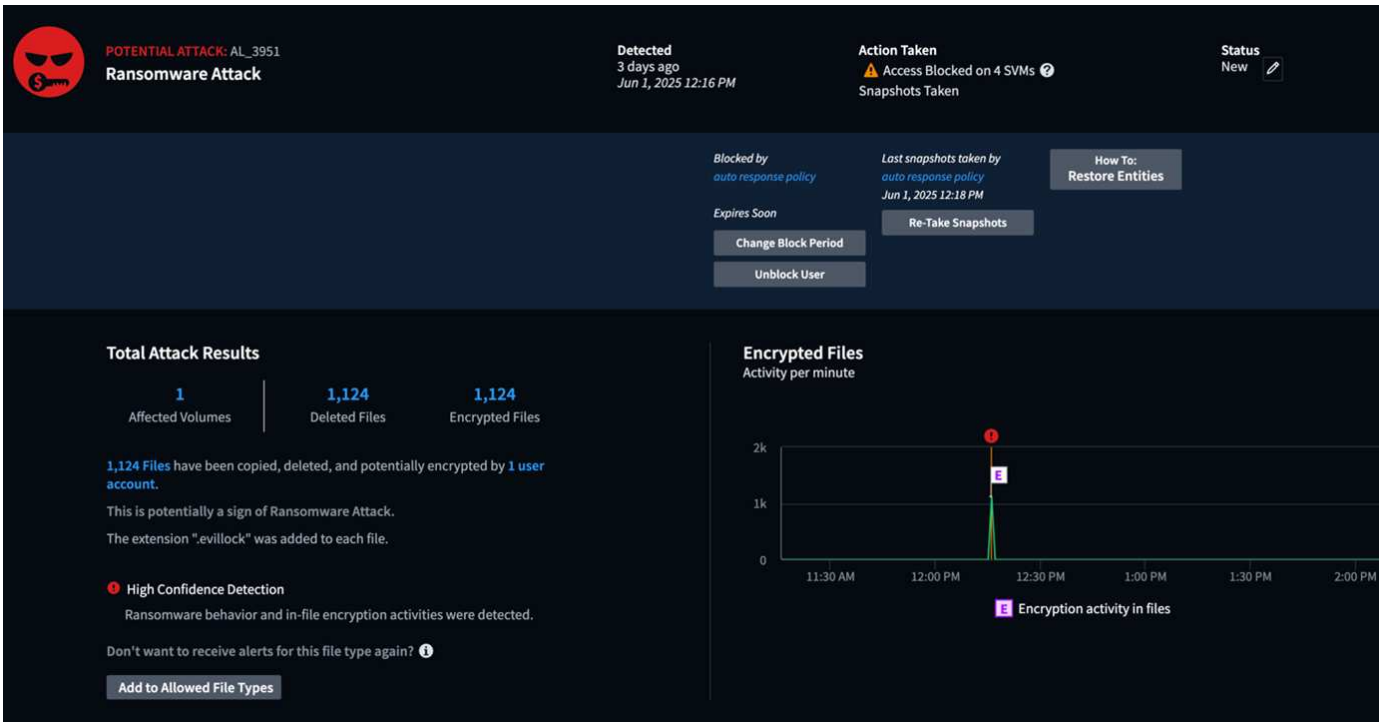
워크로드 보안은 사용자 행동을 기반으로 파일 변조 패턴을 감지하는 반면, ONTAP ARP는 파일 내 암호화 활동을 기반으로 파일 변조 활동을 감지합니다.

조건이 충족되면 Workload Security는 알림을 높은 신뢰도 알림으로 표시합니다.

알림 목록 페이지의 높은 신뢰도 알림 예:



높은 신뢰도 경보 세부 정보의 예:



경고를 여러 번 트리거합니다.

워크로드 보안은 사용자 행동을 학습하여 동일 사용자에 대해 24시간 이내에 파일 변조 공격이 반복될 경우 경고를 생성하지 않습니다.

다른 사용자로 새로운 알림을 생성하려면 동일한 단계(테스트 데이터를 만든 다음 테스트 데이터를 암호화)를 다시 따르세요.

알림, 경고 및 에이전트/데이터 소스 수집기 상태에 대한 이메일 알림 구성

이메일 알림을 통해 잠재적인 공격, 보안 경고 및 인프라 상태 문제에 대한 정보를 발생 즉시 받아볼 수 있습니다. 관리자 > 알림 설정에서 수신자 이메일 주소를 구성하여 각 수신자의 역할에 맞춘 실시간 알림을 받도록 설정하세요.

잠재적 공격 경고 및 알림

잠재적 공격 경고 알림을 보내려면 잠재적 공격 경고 보내기 섹션에 수신자의 이메일 주소를 입력하세요. 알림에 대한 모든 작업에 대해 알림 수신자 목록에 이메일 알림이 전송됩니다.

경고 알림을 보내려면 경고 알림 보내기 섹션에 수신자의 이메일 주소를 입력하세요.

에이전트 및 데이터 수집기 상태 모니터링

알림을 통해 에이전트와 데이터 소스의 상태를 모니터링할 수 있습니다.

에이전트 또는 데이터 소스 수집기가 작동하지 않을 경우 알림을 받으려면 데이터 수집 상태 알림 섹션에 수신자의 이메일 주소를 입력하세요.

다음 사항을 명심하세요.

- 건강 경고는 담당자/수금원이 최소 1시간 이상 보고를 중단한 후에만 전송됩니다.
- 에이전트나 데이터 수집기가 장시간 연결이 끊긴 경우에도 지정된 24시간 동안 의도된 수신자에게 이메일 알림이 한 번만 전송됩니다.
- 에이전트에 오류가 발생하는 경우, 알림이 한 번 전송됩니다(수집기당 하나가 아님). 이메일에는 영향을 받은 모든 SVM 목록이 포함됩니다.
- Active Directory 컬렉션 실패는 경고로 보고되며 위협 탐지에는 영향을 미치지 않습니다.
- 시작하기 설정 목록에 이제 새로운 이메일 알림 구성 단계가 포함되었습니다.

에이전트 및 데이터 수집기 업그레이드 알림 수신

- "데이터 수집 건강 알림"에 이메일 ID를 입력하세요.
- "업그레이드 알림 사용" 확인란이 활성화됩니다.
- 에이전트 및 데이터 수집기 업그레이드 이메일 알림은 계획된 업그레이드 1일 전에 해당 이메일 ID로 전송됩니다.

문제 해결

문제:	이걸 시도해보세요:
"데이터 수집기 상태 알림"에 이메일 ID가 있지만 알림을 받지 못하고 있습니다.	알림 이메일은 NetApp Data Infrastructure Insights 도메인(*accounts@service.cloudinsights.netapp.com*)에서 전송됩니다. 일부 회사는 외부 도메인에서 들어오는 이메일을 차단합니다. NetApp Data Infrastructure Insights 도메인의 외부 알림이 허용 목록에 포함되어 있는지 확인하세요.

웹훅 알림

웹후크를 사용한 워크로드 보안 알림

웹후크를 사용하면 사용자는 사용자 정의된 웹후크 채널을 사용하여 다양한 애플리케이션에 중요하거나 경고 알림 메시지를 보낼 수 있습니다.

Slack, PagerDuty, Teams, Discord 등 많은 상업용 애플리케이션은 표준 입력 인터페이스로 웹훅을 지원합니다. Workload Security는 일반적이고 사용자 정의 가능한 웹훅 채널을 지원함으로써 이러한 다양한 전달 채널을 지원할 수 있습니다. 웹후크 구성에 대한 정보는 해당 애플리케이션 웹사이트에서 확인할 수 있습니다. 예를 들어 Slack은 다음을 제공합니다."이 유용한 가이드" .

여러 개의 웹훅 채널을 만들 수 있으며, 각 채널은 다른 목적, 별도의 애플리케이션, 다른 수신자 등을 대상으로 합니다.

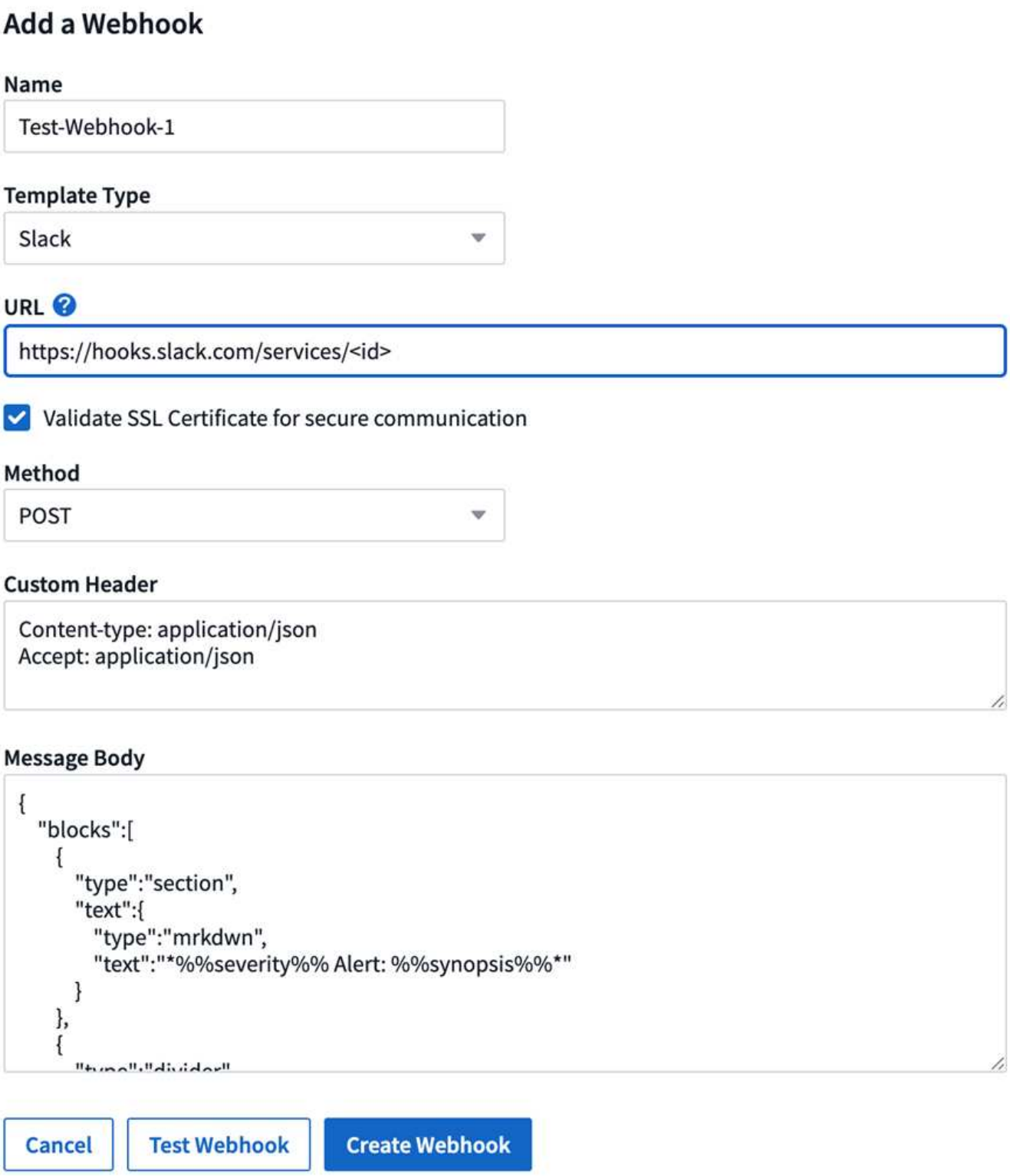
웹훅 채널 인스턴스는 다음 요소로 구성됩니다.

이름	설명
URL	URL 매개변수와 함께 http:// 또는 https:// 접두사를 포함한 웹훅 대상 URL
방법	GET/POST - 기본값은 POST입니다.
사용자 정의 헤더	여기에 사용자 정의 헤더를 지정하세요
메시지 본문	여기에 메시지 본문을 입력하세요
기본 알림 매개변수	웹훅의 기본 매개변수를 나열합니다.
사용자 정의 매개변수 및 비밀	사용자 정의 매개변수 및 비밀을 사용하면 비밀번호와 같은 고유한 매개변수 및 보안 요소를 추가할 수 있습니다.

웹훅 만들기

워크로드 보안 웹훅을 생성하려면 관리 > 알림으로 이동하여 "워크로드 보안 웹훅" 탭을 선택하세요. 다음 이미지는 Slack 웹훅 생성 화면의 샘플을 보여줍니다.

참고: Workload Security Webhook을 생성하고 관리하려면 사용자는 Workload Security _Admin_이어야 합니다.



- 각 필드에 적절한 정보를 입력하고 "저장"을 클릭하세요.
- "웹훅 테스트" 버튼을 클릭하여 연결을 테스트할 수도 있습니다. 이렇게 하면 선택된 방법에 따라 정의된 URL로 "메시지 본문"(대체 없음)이 전송됩니다.
- SWS 웹훅은 여러 개의 기본 매개변수로 구성됩니다. 또한, 사용자 정의 매개변수나 비밀번호를 직접 만들 수도 있습니다.

매개변수: 매개변수란 무엇이고 어떻게 사용하나요?

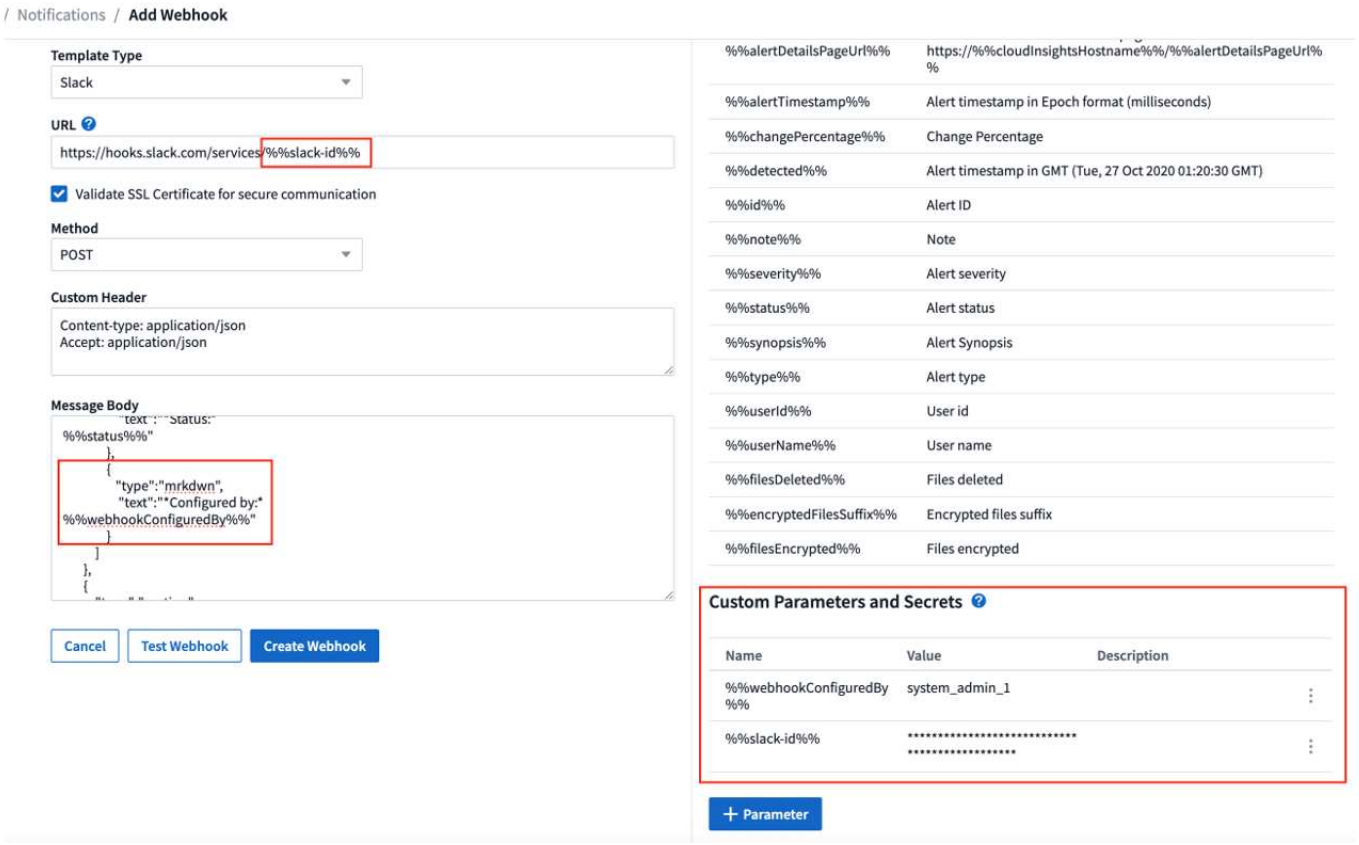
알림 매개변수는 알림마다 채워지는 동적 값입니다. 예를 들어, *%%severity%%* 매개변수는 경고의 심각도 유형으로 대체됩니다.

"웹후크 테스트" 버튼을 클릭해도 대체가 수행되지 않는다는 점에 유의하세요. 테스트는 매개변수의 플레이스홀더(*%%<param-name>%%*)를 보여주는 페이로드를 전송하지만 이를 데이터로 바꾸지는 않습니다.

사용자 정의 매개변수 및 비밀

이 섹션에서는 원하는 사용자 정의 매개변수 및/또는 비밀번호를 추가할 수 있습니다. 사용자 정의 매개변수나 비밀번호는 URL이나 메시지 본문에 포함될 수 있습니다. 비밀을 사용하면 사용자가 비밀번호, API 키 등과 같은 안전한 사용자 정의 매개변수를 구성할 수 있습니다.

다음 샘플 이미지는 사용자 정의 매개변수가 웹훅 생성에 어떻게 사용되는지 보여줍니다.



워크로드 보안 웹훅 목록 페이지

웹후크 목록 페이지에는 이름, 생성자, 생성일, 상태, 보안 및 마지막 보고 필드가 표시됩니다. 참고: '상태' 열의 값은 마지막 웹훅 트리거 결과에 따라 계속 변경됩니다. 다음은 상태 결과의 예입니다.

상태	설명
OK	알림이 성공적으로 전송되었습니다.
403	금지됨.
404	URL을 찾을 수 없습니다.

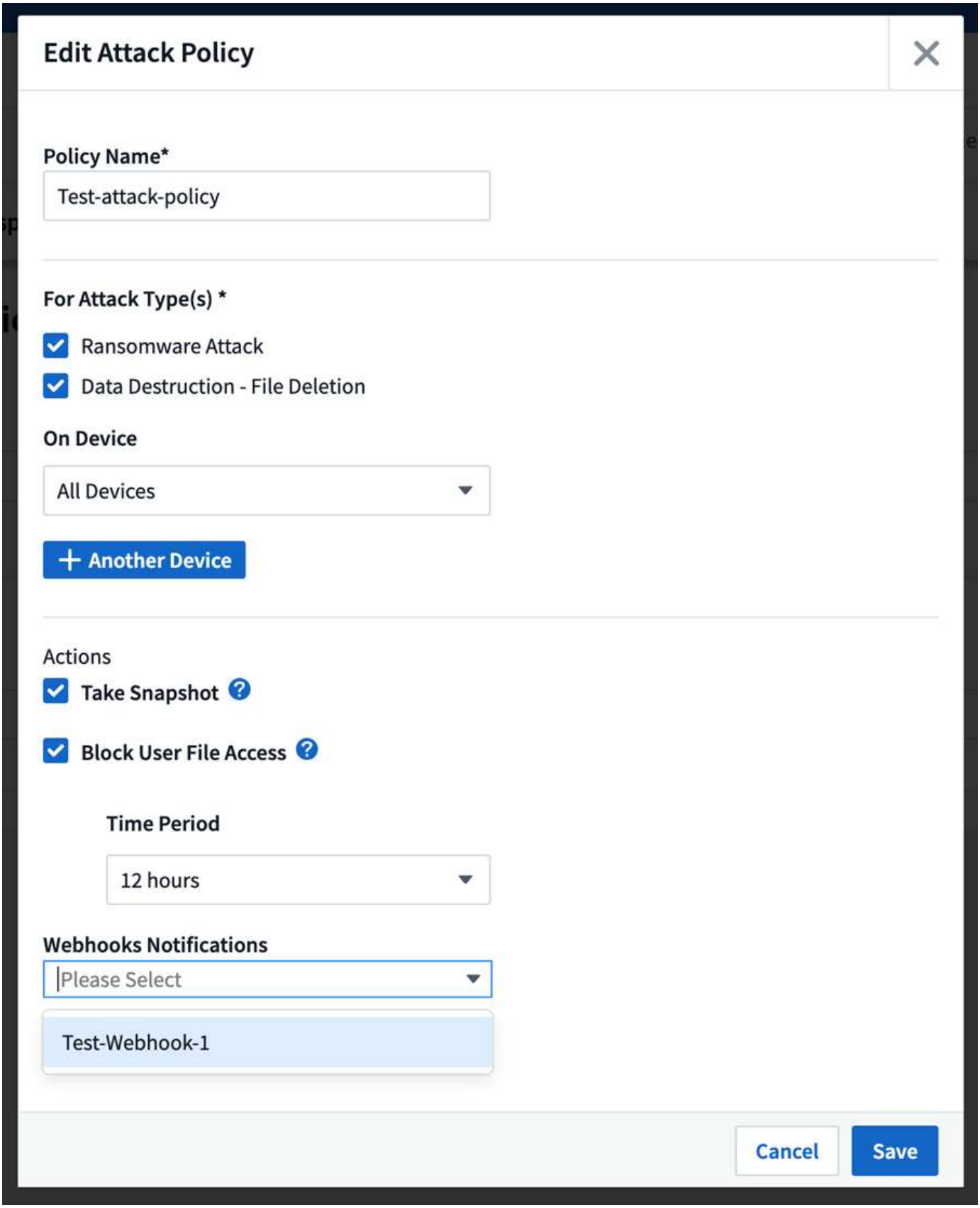
400	잘못된 요청입니다. 메시지 본문에 다음과 같은 오류가 있는 경우 이 상태가 표시될 수 있습니다. • 형식이 잘못된 JSON입니다. • 예약된 키에 잘못된 값을 제공했습니다. 예를 들어, PagerDuty는 "심각도"에 대해 중요/경고/오류/정보만 허용합니다. 다른 결과는 400 상태를 나타낼 수 있습니다. • 애플리케이션별 검증 오류. 예를 들어, Slack은 섹션 내에 최대 10개의 필드를 허용합니다. 10개 이상을 포함하면 400 상태가 될 수 있습니다.
410	더 이상 리소스를 사용할 수 없습니다.

"마지막 보고" 열은 웹훅이 마지막으로 트리거된 시간을 나타냅니다.

웹후크 목록 페이지에서 사용자는 웹후크를 편집/복제/삭제할 수도 있습니다.

알림 정책에서 **Webhook** 알림 구성

알림 정책에 웹훅 알림을 추가하려면 -워크로드 보안 > 정책-으로 이동하여 기존 정책을 선택하거나 새 정책을 추가합니다. 작업 섹션 > 웹훅 알림 드롭다운에서 필요한 웹훅을 선택합니다.



웹훅 알림은 정책에 연결됩니다. 공격(RW/DD/WARN)이 발생하면 구성된 작업(스냅샷 촬영/사용자 차단)이 수행되고 관련 웹훅 알림이 트리거됩니다.

참고: 이메일 알림은 정책과 무관하며 평소와 같이 트리거됩니다.

- 정책이 일시 중지되면 웹후크 알림이 트리거되지 않습니다.
- 하나의 정책에 여러 개의 웹훅을 첨부할 수 있지만 정책에 5개 이상의 웹훅을 첨부하지 않는 것이 좋습니다.

워크로드 보안 웹훅 예제

웹후크"느슨하게"

웹후크"페이저듀티" 웹후크"팀" 웹후크"불화"

Discord를 위한 워크로드 보안 웹훅 예시

웹훅을 사용하면 사용자는 사용자 정의된 웹훅 채널을 사용하여 다양한 애플리케이션에 알림을 보낼 수 있습니다. 이 페이지에서는 Discord에 대한 웹훅을 설정하는 방법에 대한 예를 제공합니다.

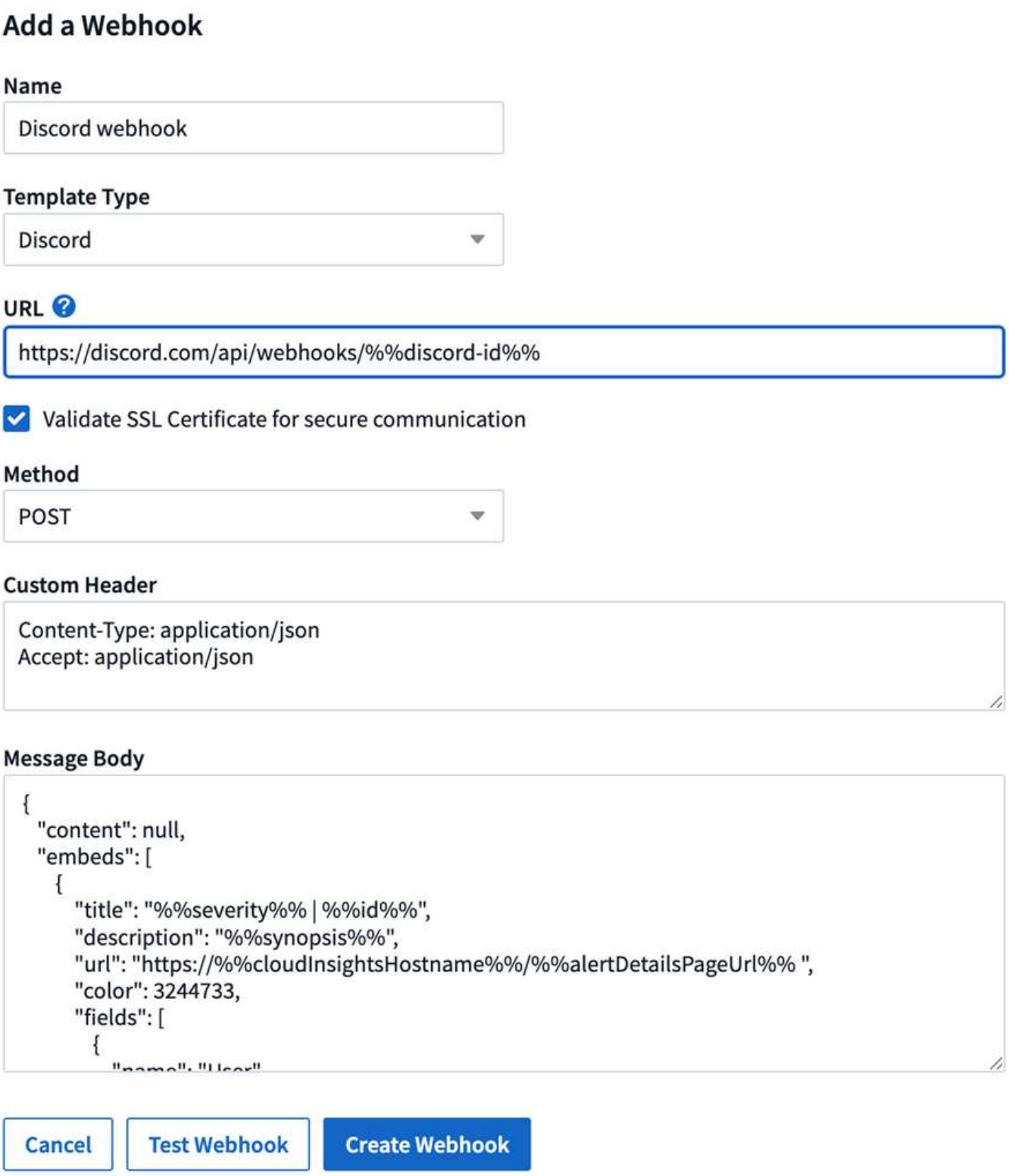
이 페이지는 제3자 지침을 참조하며, 해당 지침은 변경될 수 있습니다. 를 참조하세요"Discord 문서" 최신 정보를 확인하세요.

Discord 설정**:**

- Discord에서 서버를 선택하고 텍스트 채널 아래에서 채널 편집(기어 아이콘)을 선택합니다.
- *통합 > 웹훅 보기*를 선택하고 *새 웹훅*을 클릭합니다.
- Webhook URL을 복사합니다. 이것을 Workload Security 웹훅 구성에 붙여넣어야 합니다.

워크로드 보안 웹훅 생성**:**

1. 관리 > 알림으로 이동하여 워크로드 보안 웹훅 탭을 선택합니다. 새로운 웹훅을 만들려면 '+ 웹훅'을 클릭하세요.
2. 웹훅에 의미 있는 이름을 지정하세요.
3. 템플릿 유형 드롭다운에서 *Discord*를 선택합니다.
4. 위의 Discord URL을 *URL* 필드에 붙여넣습니다.



웹훅을 테스트하려면 메시지 본문의 URL 값을 유효한 URL(예: https://netapp.com)로 임시로 바꾼 다음 웹훅 테스트 버튼을 클릭합니다. Discord에서는 Test Webhook 기능이 작동하려면 유효한 URL을 제공해야 합니다.

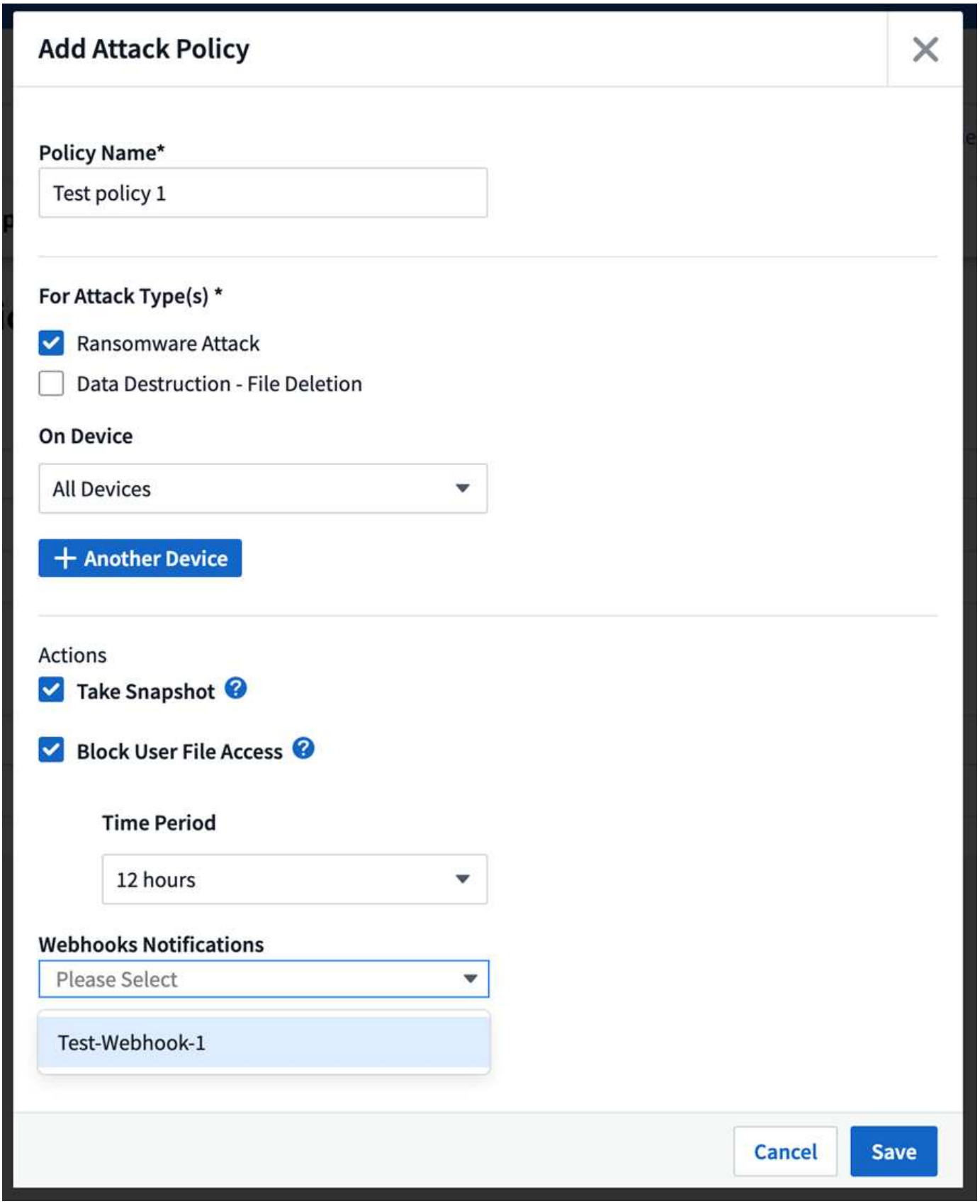
테스트가 완료되면 메시지 본문을 원래대로 설정하세요.

Webhook을 통한 알림

웹훅을 통해 이벤트를 알리려면 워크로드 보안 > 정책_으로 이동하세요. _+공격 정책 또는 _+경고 정책_을 클릭하세요.

- 의미 있는 정책 이름을 입력하세요.
- 필요한 공격 유형, 정책을 첨부할 장치 및 필요한 작업을 선택합니다.
- 웹훅 알림 드롭다운에서 필요한 Discord 웹훅을 선택하고 저장합니다.

참고: 웹후크는 기존 정책을 편집하여 첨부할 수도 있습니다.



PagerDuty를 위한 워크로드 보안 웹훅 예제

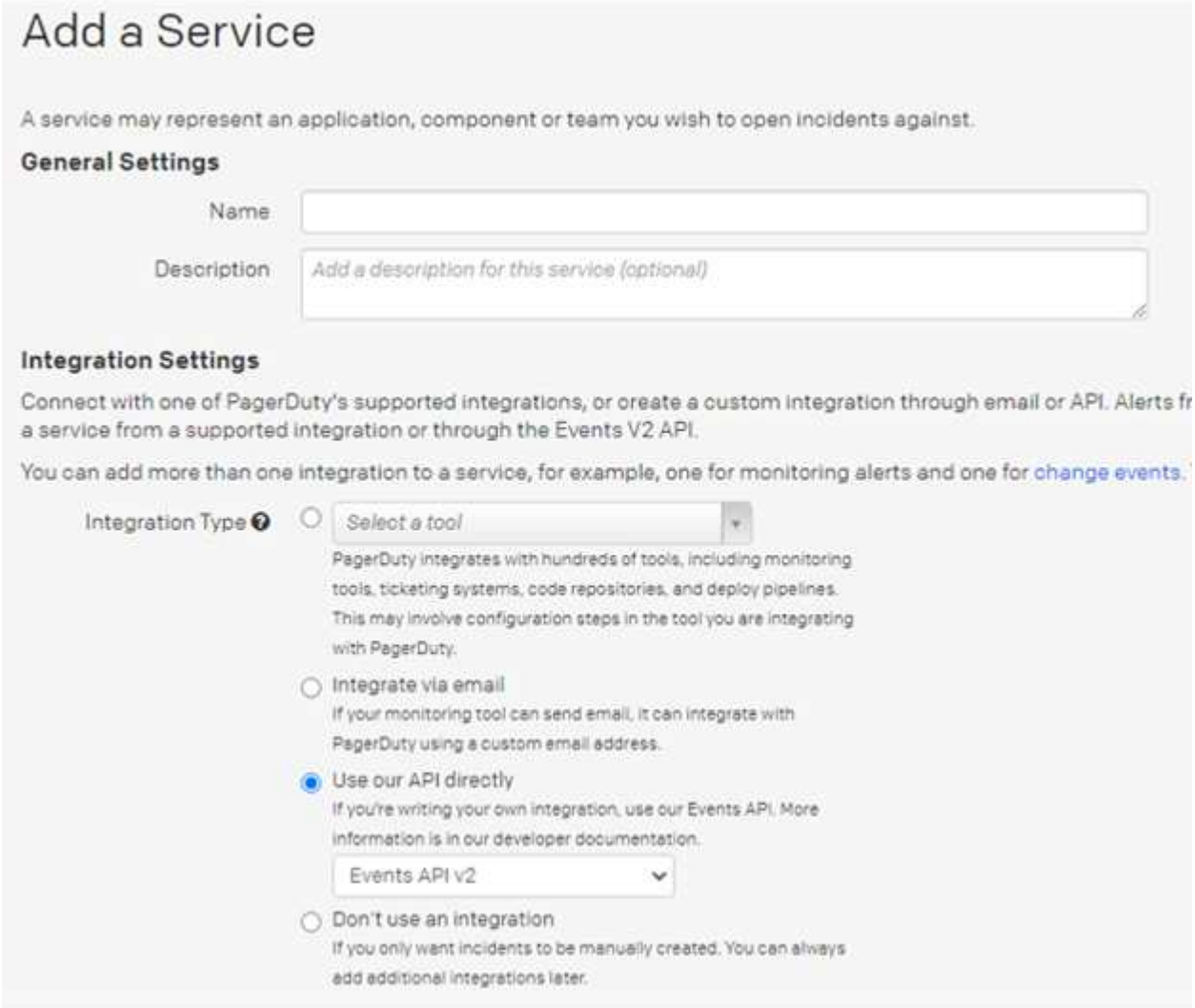
웹훅을 사용하면 사용자는 사용자 정의된 웹훅 채널을 사용하여 다양한 애플리케이션에 알림을

보낼 수 있습니다. 이 페이지에서는 PagerDuty에 대한 웹훅을 설정하는 방법에 대한 예를 제공합니다.

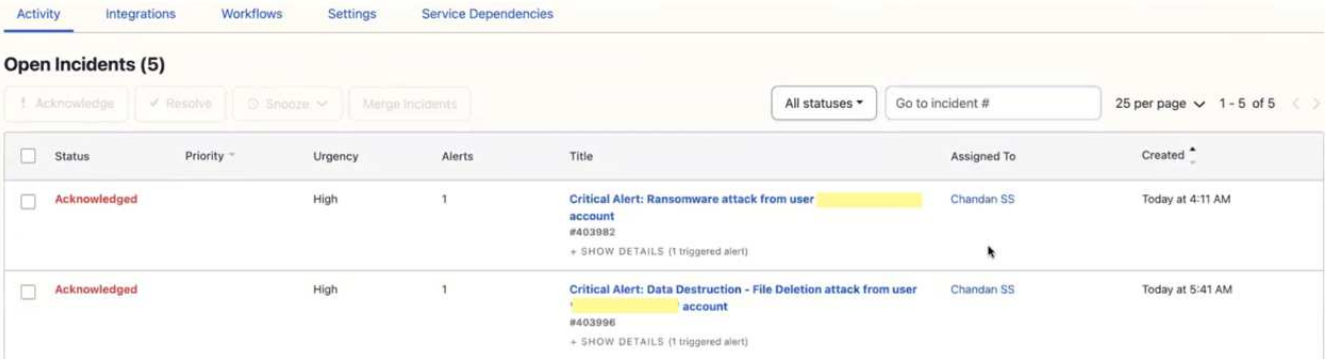
이 페이지는 변경될 수 있는 제3자 지침을 참조합니다. 를 참조하세요"PagerDuty 문서" 최신 정보를 확인하세요.

PagerDuty 설정**:**

1. PagerDuty에서 서비스 **>** 서비스 디렉터리*로 이동한 다음 *+새 서비스 버튼을 클릭합니다.
2. _이름_을 입력하고 _API를 직접 사용_을 선택하세요. _서비스 추가_를 선택하세요.

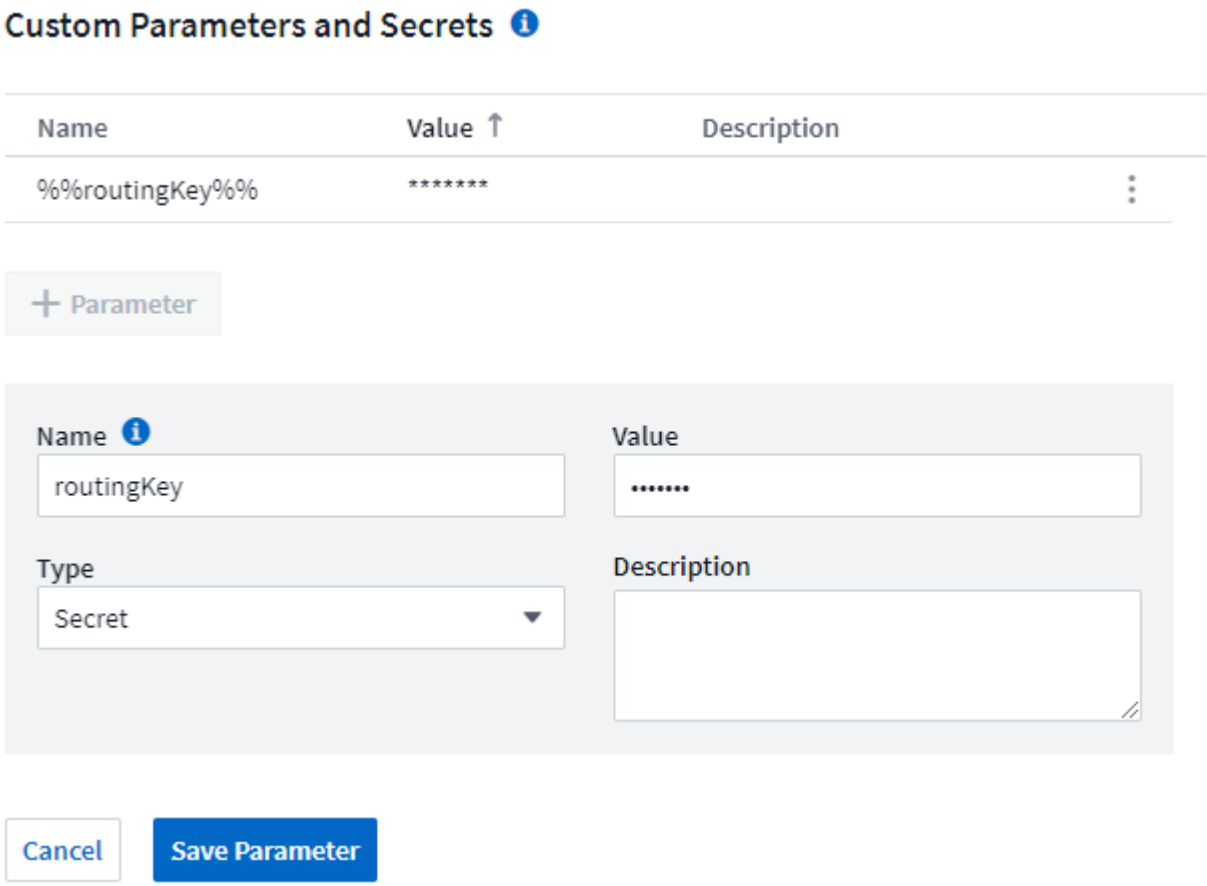


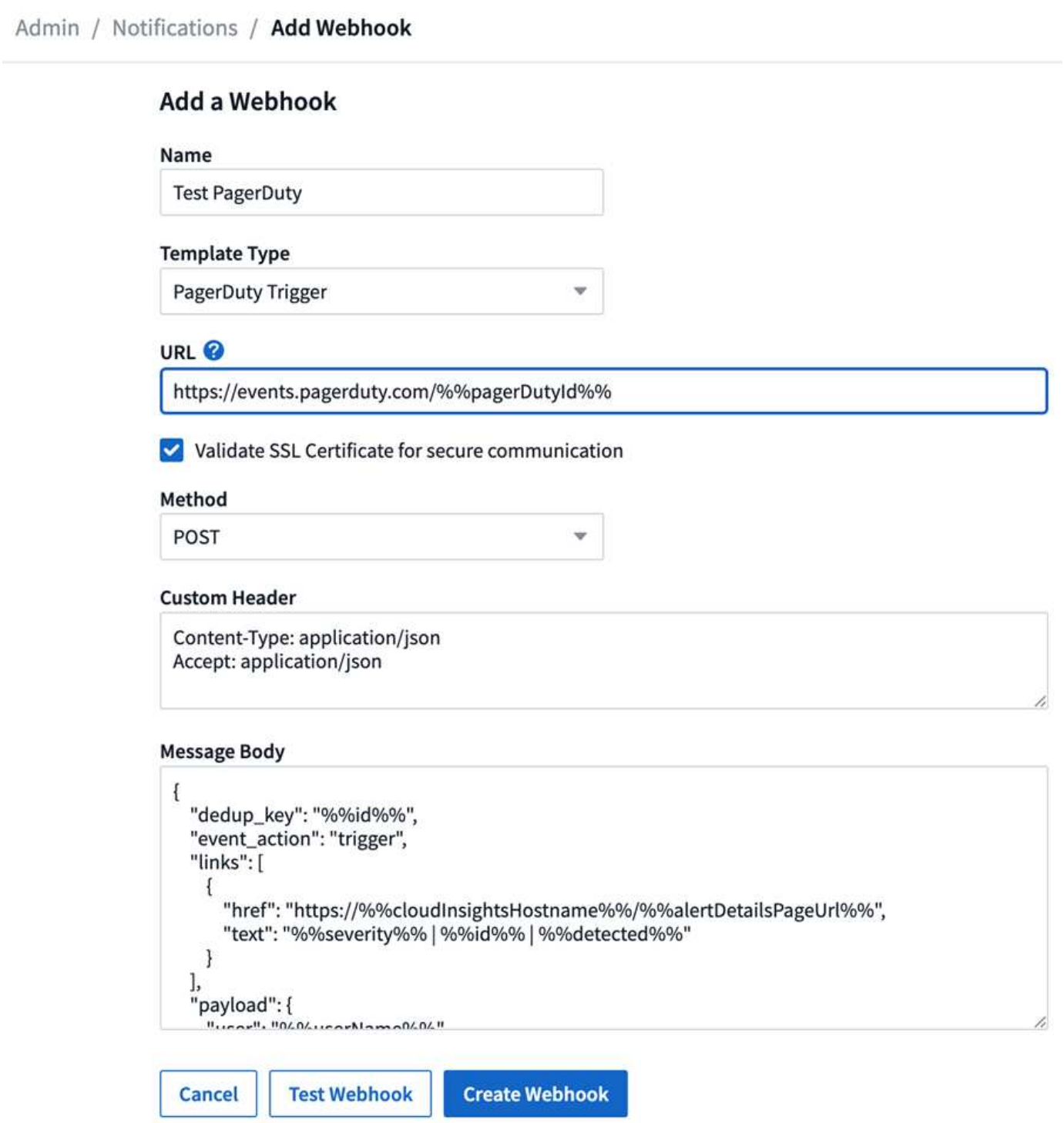
3. 통합 탭을 선택하여 *통합 키*를 확인하세요. 아래의 워크로드 보안 웹후크를 생성할 때 이 키가 필요합니다.
4. 알림을 보려면 사건 또는 *서비스*로 이동하세요.



워크로드 보안 **PagerDuty** 웹훅 생성**:**

- 관리 > 알림으로 이동하여 워크로드 보안 웹훅 탭을 선택합니다. 새로운 웹훅을 만들려면 '+ 웹훅'을 선택하세요.
- 웹훅에 의미 있는 이름을 지정하세요.
- 템플릿 유형 드롭다운에서 _PagerDuty Trigger_를 선택합니다.
- _routingKey_라는 사용자 지정 매개변수 비밀번호를 만들고 값을 위에서 만든 PagerDuty _Integration Key_로 설정합니다.

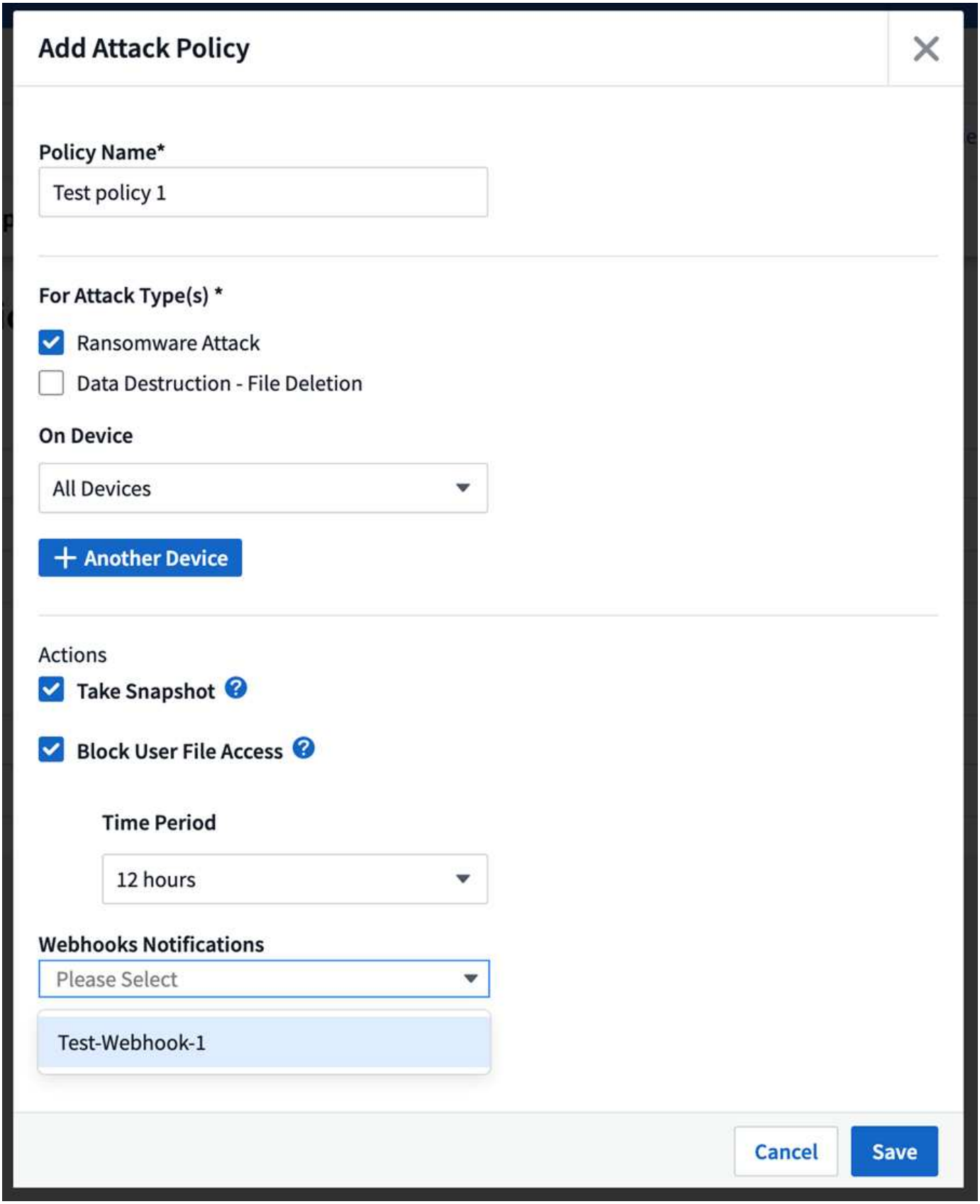




Webhook을 통한 알림

- 웹훅을 통해 이벤트를 알리려면 워크로드 보안 > 정책_으로 이동하세요. _+공격 정책 또는 _+경고 정책_을 선택하세요.
- 의미 있는 정책 이름을 입력하세요.
- 필요한 공격 유형, 정책을 첨부할 장치 및 필요한 작업을 선택합니다.
- 웹훅 알림 드롭다운에서 필요한 PagerDuty 웹훅을 선택합니다. 정책을 저장합니다.

참고: 웹후크는 기존 정책을 편집하여 첨부할 수도 있습니다.



Slack을 위한 워크로드 보안 웹훅 예시

웹훅을 사용하면 사용자는 사용자 정의된 웹훅 채널을 사용하여 다양한 애플리케이션에 알림을 보낼 수 있습니다. 이 페이지에서는 Slack에 대한 웹훅을 설정하는 방법에 대한 예를 제공합니다.

이 페이지는 변경될 수 있는 제3자 지침을 참조합니다. 최신 정보는 Slack 문서를 참조하세요.

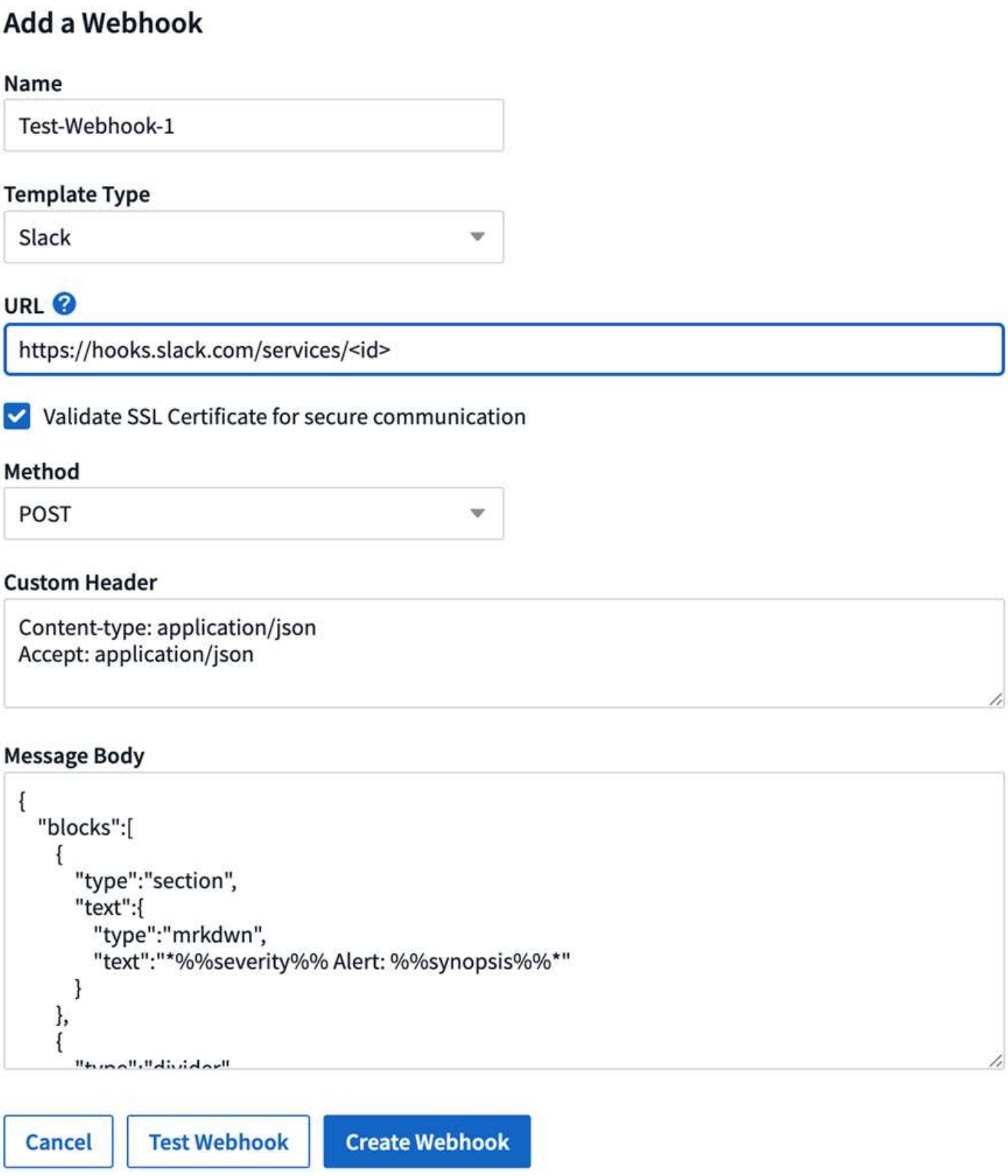
슬랙 예시

- 로 가다 https://api.slack.com/apps 새로운 앱을 만드세요. 의미 있는 이름을 지정하고 작업 공간을 선택하세요.

- 수신 웹훅으로 이동하여 _수신 웹훅 활성화_를 클릭하고 _새 웹훅 추가_를 선택한 다음 게시할 채널을 선택합니다.
- Webhook URL을 복사합니다. 이 URL은 워크로드 보안 웹훅을 생성할 때 제공됩니다.

워크로드 보안 **Slack** 웹훅 만들기

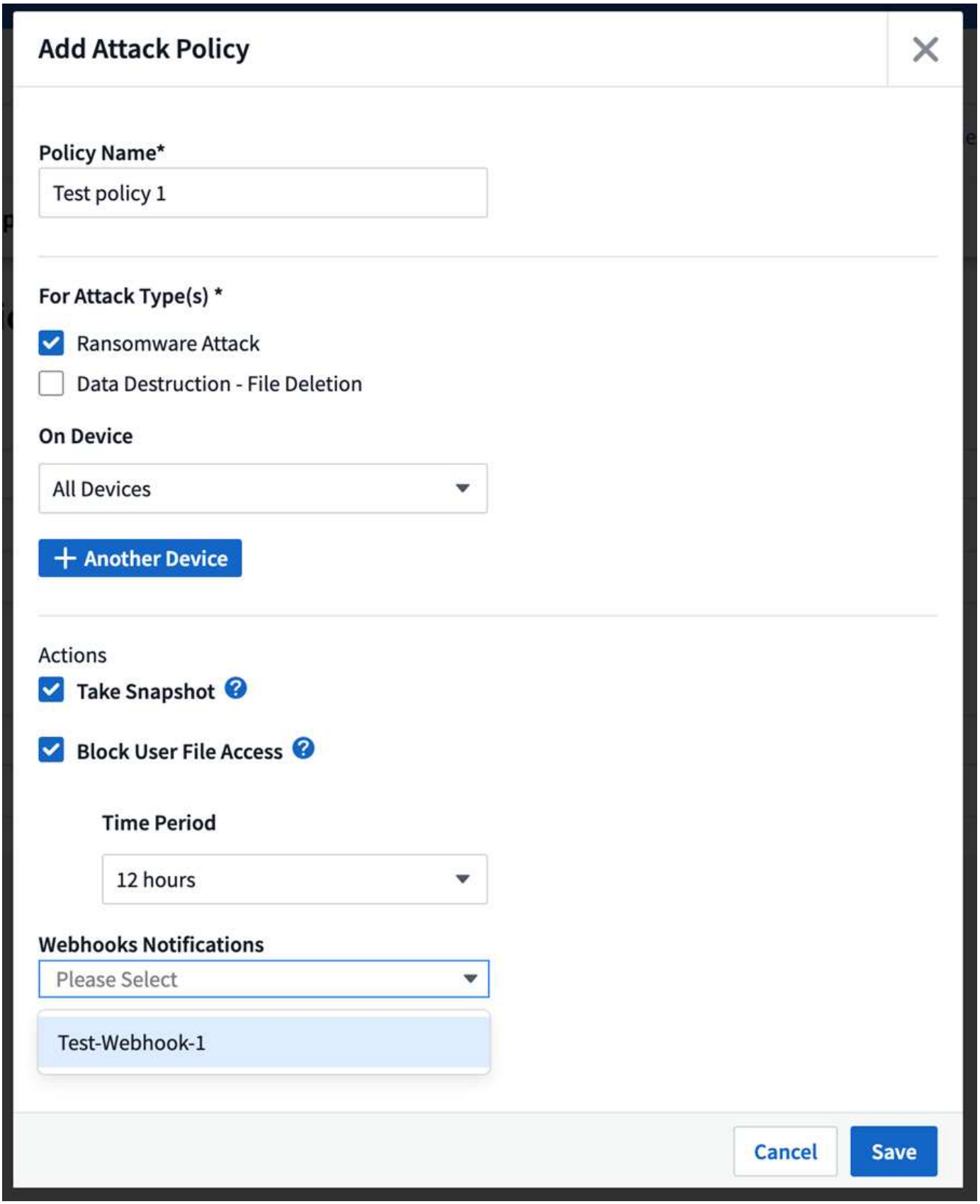
1. 관리 > 알림으로 이동하여 워크로드 보안 웹훅 탭을 선택합니다. _+ Webhook_을 선택하여 새 웹훅을 만듭니다.
2. 웹훅에 의미 있는 이름을 지정하세요.
3. 템플릿 유형 드롭다운에서 _Slack_을 선택합니다.
4. 위에서 복사한 URL을 붙여넣으세요.



웹훅을 통한 알림

- 웹훅을 통해 이벤트를 알리려면 워크로드 보안 > 정책_으로 이동하세요. _+공격 정책 또는 _+경고 정책_을 클릭하세요.
- 의미 있는 정책 이름을 입력하세요.
- 필요한 공격 유형, 정책을 첨부할 장치 및 필요한 작업을 선택합니다.
- 웹후크 알림 드롭다운에서 필요한 웹후크를 선택합니다. 정책을 저장합니다.

참고: 웹후크는 기존 정책을 편집하여 첨부할 수도 있습니다.



Microsoft Teams를 위한 워크로드 보안 웹훅 예시

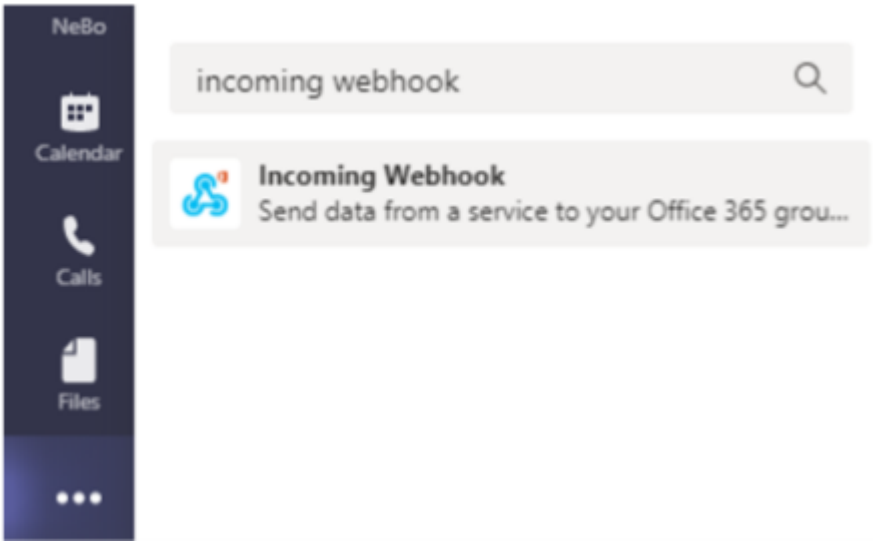
웹훅을 사용하면 사용자는 사용자 정의된 웹훅 채널을 사용하여 다양한 애플리케이션에 알림을

보낼 수 있습니다. 이 페이지에서는 Teams에 대한 웹훅을 설정하는 방법에 대한 예를 제공합니다.

이 페이지는 변경될 수 있는 제3자 지침을 참조합니다. 를 참조하세요"팀 문서" 최신 정보를 확인하세요.

팀 설정:

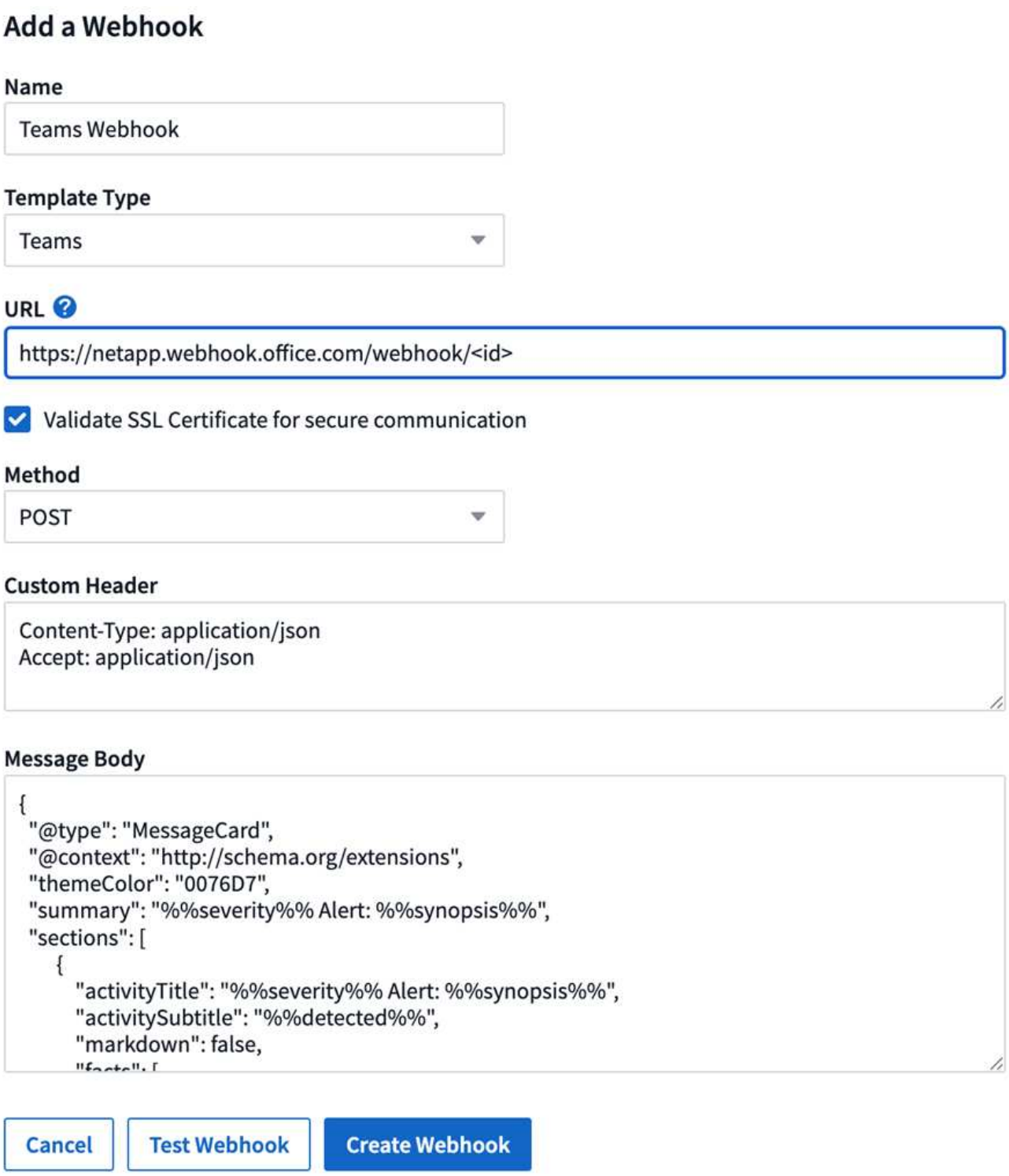
1. Teams에서 케밥을 선택하고 수신 웹훅을 검색합니다.



2. *팀에 추가 > 팀 선택 > 커넥터 설정*을 선택합니다.
3. Webhook URL을 복사합니다. 이것을 Workload Security 웹훅 구성에 붙여넣어야 합니다.

워크로드 보안 팀 웹훅 만들기:

1. 관리 > 알림으로 이동하여 “워크로드 보안 웹훅 탭을 선택합니다. _+ Webhook_을 선택하여 새 웹훅을 만듭니다.
2. 웹훅에 의미 있는 이름을 지정하세요.
3. 템플릿 유형 드롭다운에서 *팀*을 선택합니다.



4. 위의 URL을 *URL* 필드에 붙여넣으세요.

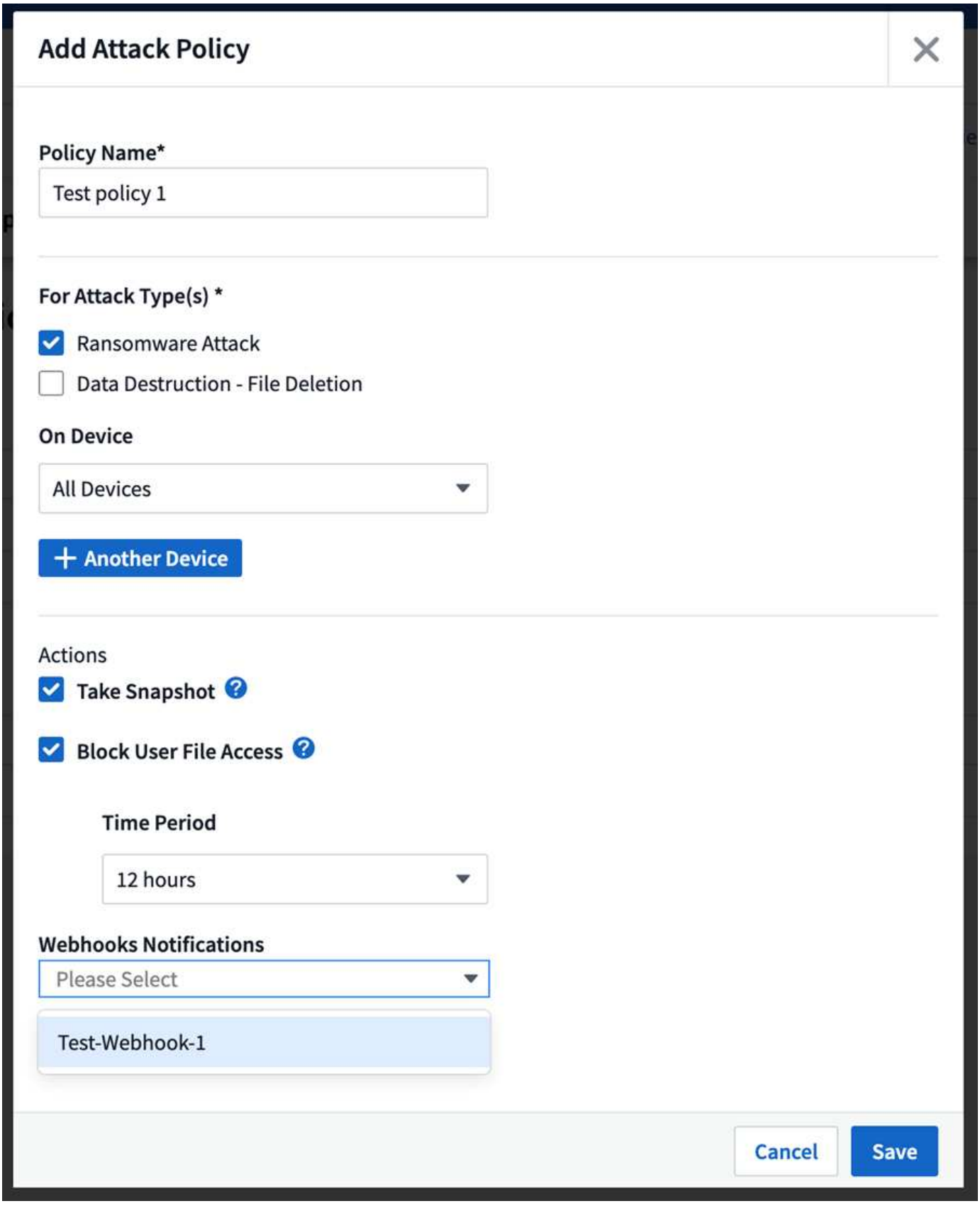
Webhook을 통한 알림

웹훅을 통해 이벤트를 알리려면 워크로드 보안 > 정책_으로 이동하세요. _+공격 정책 또는 _+경고 정책_을 선택하세요.

- 의미 있는 정책 이름을 입력하세요.
- 필요한 공격 유형, 정책을 첨부할 장치 및 필요한 작업을 선택합니다.

- 웹후크 알림 드롭다운에서 필요한 Teams 웹후크를 선택합니다. 정책을 저장합니다.

참고: 웹후크는 기존 정책을 편집하여 첨부할 수도 있습니다.



워크로드 보안 **API**

Workload Security API를 사용하면 NetApp 고객과 ISV(독립 소프트웨어 공급업체)가 Workload Security를 CMDB나 다른 티켓팅 시스템 등의 다른 애플리케이션과 통합할 수 있습니다.

API 접근을 위한 요구 사항:

- API 액세스 토큰 모델은 액세스 권한을 부여하는 데 사용됩니다.
- API 토큰 관리 작업은 관리자 역할을 가진 Workload Security 사용자가 수행합니다.

API 문서**(Swagger)**

최신 API 정보는 Workload Security에 로그인하여 관리자 **> API** 액세스*로 이동하면 확인할 수 있습니다**. *API** 문서 링크를 클릭하세요. API 문서는 Swagger 기반으로, API에 대한 간략한 설명과 사용 정보를 제공하고 테넌트에서 API를 시험해 볼 수 있도록 해줍니다.

Forensics Activity API를 호출하는 경우 cloudsecure_forensics.activities.**v2** API를 사용하세요. 이 API에 여러 번 호출하는 경우 호출이 병렬로가 아닌 순차적으로 발생하는지 확인하세요. 여러 개의 병렬 호출로 인해 API 시간이 초과될 수 있습니다.

API 액세스 토큰

Workload Security API를 사용하기 전에 하나 이상의 *API 액세스 토큰*을 만들어야 합니다. 액세스 토큰은 읽기 권한을 부여합니다. 각 액세스 토큰의 만료일을 설정할 수도 있습니다.

액세스 토큰을 생성하려면:

- *관리자 > API 액세스*를 클릭하세요.
- *+API 액세스 토큰*을 클릭하세요.
- *토큰 이름*을 입력하세요
- 토큰 만료 지정

귀하의 토큰은 생성 과정에서 클립보드에 복사하고 저장하는 데만 사용할 수 있습니다. 토큰은 생성된 후에는 검색할 수 없으므로 토큰을 복사하여 안전한 곳에 저장하는 것이 좋습니다. 토큰 생성 화면을 닫기 전에 API 액세스 토큰 복사 버튼을 클릭하라는 메시지가 표시됩니다.

토큰을 비활성화, 활성화 및 취소할 수 있습니다. 비활성화된 토큰을 활성화할 수 있습니다.

토큰은 고객 관점에서 API에 대한 일반적인 액세스 권한을 부여하고 자체 테넌트 범위 내에서 API에 대한 액세스를 관리합니다.

사용자가 성공적으로 인증하고 액세스를 승인하면 애플리케이션은 액세스 토큰을 받은 다음 대상 API를 호출할 때 액세스 토큰을 자격 증명으로 전달합니다. 전달된 토큰은 토큰 보유자가 API에 액세스하고 권한 부여 시 부여된 범위에 따라 특정 작업을 수행할 권한이 있음을 API에 알립니다.

액세스 토큰이 전달되는 HTTP 헤더는 *X-CloudInsights-ApiKey:*입니다.

예를 들어, 다음을 사용하여 저장소 자산을 검색합니다.

```
 curl https://<Workload Security tenant>/rest/v1/cloudsecure/activities -H
'X-CloudInsights-ApiKey: <API_Access_Token>'
```

여기서 _<API_Access_Token>_은 API 액세스 키 생성 중에 저장한 토큰이고 _<Workload Security Tenant>_는 Workload Security 환경의 테넌트 URL입니다.

자세한 내용은 관리자 **> API** 액세스 아래의 *API* 문서 링크에서 확인할 수 있습니다.

API를 통해 데이터를 추출하는 스크립트

Workload Security 에이전트에는 요청된 시간 범위를 더 작은 배치로 나누어 v2 API에 대한 병렬 호출을 용이하게 하는 내보내기 스크립트가 포함되어 있습니다.

스크립트는 _/opt/netapp/cloudsecure/agent/export-script_에 있습니다. 같은 디렉토리에 있는 README 파일에 사용 지침이 나와 있습니다.

스크립트를 호출하는 명령의 예는 다음과 같습니다.

```
python3 data-export.py --tenant_url <Workload Security tenant>
--access_key %ACCESS_KEY% --path_filter "<dir path>" --user_name "<user>"
--from_time "01-08-2024 00:00:00" --to_time "31-08-2024 23:59:59"
--iteration_interval 12 --num_workers 3
```

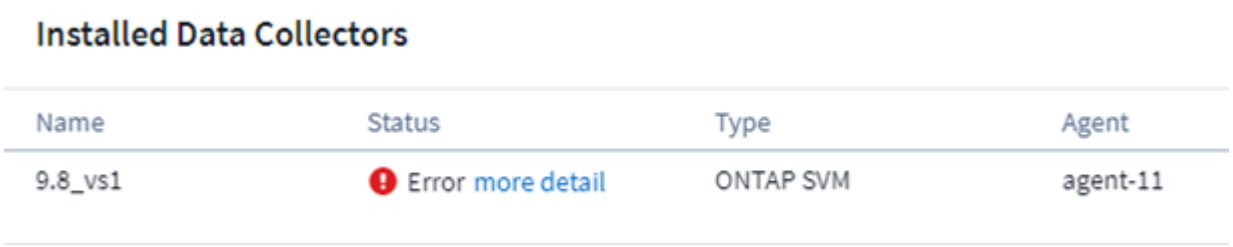
주요 매개변수: - `--iteration_interval 12` : 요청된 시간 범위를 12시간 간격으로 나눕니다. - `--num_workers 3` : 3개의 스레드를 사용하여 이러한 간격을 병렬로 가져옵니다.

ONTAP SVM 데이터 수집기 문제 해결

워크로드 보안은 데이터 수집기를 사용하여 장치에서 파일 및 사용자 액세스 데이터를 수집합니다. 여기에서는 이 수집기와 관련된 문제를 해결하기 위한 팁을 찾을 수 있습니다.

를 참조하십시오"SVM 수집기 구성" 이 수집기를 구성하는 방법에 대한 지침은 페이지를 참조하세요.

오류가 발생한 경우, 설치된 데이터 수집기 페이지의 상태 열에서 _자세한 내용_을 클릭하면 오류에 대한 자세한 내용을 볼 수 있습니다.



알려진 문제와 해결 방법은 아래와 같습니다.

문제**:** 데이터 수집기가 잠시 실행되다가 임의의 시간 후에 중지되고 "오류 메시지: 커넥터가 오류 상태입니다."라는 오류 메시지가 나타납니다. 서비스 이름: 감사. 실패 이유: 외부 fpolicy 서버가 과부하되었습니다. 다음을 시도해 보세요**.** ONTAP 의 이벤트 비율은 에이전트 상자가 처리할 수 있는 것보다 훨씬 높았습니다. 그래서 연결이 종료되었습니다.

연결이 끊어졌을 때 CloudSecure에서 최대 트래픽을 확인하세요. **CloudSecure >** 활동 포렌식 **>** 모든 활동 페이지에서 확인할 수 있습니다.

최대 집계 트래픽이 Agent Box에서 처리할 수 있는 것보다 높은 경우 Agent Box에서 Collector 배포 크기를 조정하는 방법에 대한 이벤트 속도 검사기 페이지를 참조하세요.

2021년 3월 4일 이전에 에이전트가 에이전트 상자에 설치된 경우 에이전트 상자에서 다음 명령을 실행하세요.

```
echo 'net.core.rmem_max=8388608' >> /etc/sysctl.conf
echo 'net.ipv4.tcp_rmem = 4096 2097152 8388608' >> /etc/sysctl.conf
sysctl -p
```

크기를 조정한 후 UI에서 수집기를 다시 시작합니다.

{비어 있는}

문제**:** 수집기에서 "SVM의 데이터 인터페이스에 도달할 수 있는 커넥터에서 로컬 IP 주소를 찾을 수 없습니다"라는 오류 메시지가 보고됩니다. 다음을 시도해 보세요**:** 이는 ONTAP 측의 네트워킹 문제로 인해 발생할 가능성이 가장 높습니다. 다음 단계를 따르세요.

1. SVM 데이터 영역이나 관리 영역에 SVM의 연결을 차단하는 방화벽이 없는지 확인하세요.
2. 클러스터 관리 IP를 통해 SVM을 추가하는 경우 에이전트 VM에서 SVM의 데이터 레벨과 관리 레벨에 ping을 보낼 수 있는지 확인하세요. 문제가 발생한 경우, 해당 게이트웨이, 넷마스크, 경로를 확인하세요.

   클러스터 관리 IP를 사용하여 ssh를 통해 클러스터에 로그인하고 에이전트 IP를 ping해 볼 수도 있습니다. 에이전트 IP가 ping 가능한지 확인하세요.

   ```
   network ping -vserver <vserver name> -destination <Agent IP> -lif <Lif
   Name> -show-detail
   ```

   ping을 사용할 수 없는 경우 ONTAP 의 네트워크 설정이 올바른지 확인하여 Agent 머신이 ping을 사용할 수 있도록 하세요.

3. 클러스터 IP를 통해 연결을 시도했지만 작동하지 않는 경우 SVM IP를 통해 직접 연결을 시도하세요. SVM IP를 통해 연결하는 단계는 위를 참조하세요.
4. SVM IP 및 vsadmin 자격 증명을 통해 수집기를 추가하는 동안 SVM Lif에 데이터 및 관리 역할이 활성화되어 있는지 확인하세요. 이 경우 SVM Lif에 대한 ping은 작동하지만 SVM Lif에 대한 SSH는 작동하지 않습니다. 그렇다면 SVM 관리 전용 Lif를 만들고 이 SVM 관리 전용 Lif를 통해 연결을 시도하세요.
5. 그래도 작동하지 않는다면 새로운 SVM Lif를 생성하고 해당 Lif를 통해 연결을 시도해보세요. 서브넷 마스크가 올바르게 설정되었는지 확인하세요.
6. 고급 디버깅:

a. ONTAP 에서 패킷 추적을 시작합니다.

b. CloudSecure UI에서 SVM에 데이터 수집기를 연결해 보세요.

c. 오류가 나타날 때까지 기다리세요. ONTAP 에서 패킷 추적을 중지합니다.

d. ONTAP 에서 패킷 추적을 엽니다. 이 위치에서 사용 가능합니다

```
 https://<cluster_mgmt_ip>/spi/<clustername>/etc/log/packet_traces/
.. ONTAP 에서 Agent 상자로 SYN이 있는지 확인하세요.
.. ONTAP 에서 SYN이 없으면 ONTAP 의 방화벽에 문제가 있습니다.
.. ONTAP 에서 방화벽을 열어 ONTAP 에이전트 상자에 연결할 수 있도록 합니다.
```

7. 그래도 작동하지 않으면 네트워킹 팀에 문의하여 외부 방화벽이 ONTAP 에서 Agent 상자로의 연결을 차단하고 있지 않은지 확인하세요.
8. 위의 방법으로도 문제가 해결되지 않으면 사례를 열어주세요."넷앱 지원" 추가 지원이 필요하면.

{비어 있는}

문제: 메시지: "[호스트 이름: <IP 주소>에 대한 ONTAP 유형을 확인하지 못했습니다. 이유: 스토리지 시스템 <IP 주소>에 대한 연결 오류: 호스트에 접근할 수 없습니다(Host unreachable)" 다음을 시도해 보세요:

1. 올바른 SVM IP 관리 주소 또는 클러스터 관리 IP가 제공되었는지 확인하세요.
2. 연결하려는 SVM이나 클러스터에 SSH를 실행합니다. 연결되면 SVM 또는 클러스터 이름이 올바른지 확인하세요.

{비어 있는}

문제: 오류 메시지: "커넥터가 오류 상태입니다. 서비스 이름: 감사. 실패 이유: 외부 fpolicy 서버가 종료되었습니다. 이걸 시도해보세요:

1. 방화벽이 에이전트 머신의 필수 포트를 차단하고 있을 가능성이 큽니다. 에이전트 머신이 SVM에서 연결할 수 있도록 포트 범위 35000-55000/tcp가 열려 있는지 확인하세요. 또한 ONTAP 측에서 에이전트 머신과의 통신을 차단하는 방화벽이 활성화되어 있지 않은지 확인하세요.
2. 에이전트 상자에 다음 명령을 입력하고 포트 범위가 열려 있는지 확인하세요.

```
sudo iptables-save | grep 3500*
```

샘플 출력은 다음과 같습니다.

```
 -A IN_public_allow -p tcp -m tcp --dport 35000 -m conntrack -ctstate
NEW -j ACCEPT
. SVM에 로그인하고 다음 명령을 입력한 후 ONTAP 과의 통신을 차단하는 방화벽이 설정되어 있지 않은지 확인합니다.
```

```
system services firewall show
system services firewall policy show
```

"방화벽 명령 확인"ONTAP 측에서.

3. 모니터링하려는 SVM/클러스터에 SSH를 실행합니다. SVM 데이터 lif(CIFS, NFS 프로토콜 지원)에서 Agent 상자에 ping을 보내고 ping이 작동하는지 확인합니다.

```
network ping -vserver <vserver name> -destination <Agent IP> -lif <Lif
Name> -show-detail
```

ping을 사용할 수 없는 경우 ONTAP 의 네트워크 설정이 올바른지 확인하여 Agent 머신이 ping을 사용할 수 있도록 하세요.

4. 2개의 데이터 수집기를 통해 하나의 SVM이 테넌트에 두 번 추가되면 이 오류가 표시됩니다. UI를 통해 데이터 수집기 중 하나를 삭제합니다. 그런 다음 UI를 통해 다른 데이터 수집기를 다시 시작합니다. 그러면 데이터 수집기가 "실행 중" 상태를 표시하고 SVM에서 이벤트를 수신하기 시작합니다.

   기본적으로 테넌트에서는 1개의 SVM이 1개의 데이터 수집기를 통해 한 번만 추가되어야 합니다. 1 SVM은 2개의 데이터 수집기를 통해 두 번 추가되어서는 안 됩니다.

5. 두 개의 서로 다른 워크로드 보안 환경(테넌트)에 동일한 SVM이 추가된 경우, 항상 마지막에 추가된 SVM이 성공합니다. 두 번째 수집기는 자체 IP 주소로 fpolicy를 구성하고 첫 번째 수집기를 제거합니다. 따라서 첫 번째 수집기는 이벤트 수신을 중단하고 해당 "감사" 서비스는 오류 상태로 전환됩니다. 이를 방지하려면 각 SVM을 단일 환경에 구성하세요.
6. 서비스 정책이 올바르게 구성되지 않은 경우에도 이 오류가 발생할 수 있습니다. ONTAP 9.8 이상에서 데이터 소스 수집기에 연결하려면 data-nfs 및/또는 data-cifs 데이터 서비스와 함께 data-fpolicy-client 서비스가 필요합니다. 또한, data-fpolicy-client 서비스는 모니터링되는 SVM의 데이터 라이프와 연결되어야 합니다.

{비어 있는}

문제**:** 활동 페이지에서 이벤트가 보이지 않습니다. 이걸 시도해보세요**:**

1. ONTAP 수집기가 "실행 중" 상태인지 확인하세요. 그렇다면 일부 파일을 열어서 cifs 클라이언트 VM에서 일부 cifs 이벤트가 생성되는지 확인하세요.
2. 활동이 보이지 않으면 SVM에 로그인하여 다음 명령을 입력하세요.

```
<SVM>event log show -source fpolicy
```

fpolicy와 관련된 오류가 없는지 확인하세요.

3. 활동이 보이지 않으면 SVM에 로그인하세요. 다음 명령을 입력하세요:

```
<SVM>fpolicy show
```

"cloudsecure_" 접두사가 붙은 fpolicy 정책이 설정되었고 상태가 "on"인지 확인하세요. 설정하지 않으면 에이전트가 SVM에서 명령을 실행할 수 없을 가능성이 큽니다. 이 페이지의 시작 부분에 설명된 모든 전제 조건이 충족되었는지 확인하세요.

{비어 있는}

문제: SVM 데이터 수집기가 오류 상태이며 오류 메시지는 "에이전트가 수집기에 연결하지 못했습니다"입니다. 다음을 시도해 보세요.

1. 에이전트가 과부하되어 데이터 소스 수집기에 연결할 수 없는 것 같습니다.
2. 에이전트에 연결된 데이터 소스 수집기의 수를 확인합니다.
3. 또한 UI의 "모든 활동" 페이지에서 데이터 흐름 속도를 확인하세요.
4. 초당 활동 수가 상당히 높은 경우 다른 에이전트를 설치하고 일부 데이터 소스 수집기를 새 에이전트로 이동합니다.

{비어 있는}

문제: SVM 데이터 수집기가 "fpolicy.server.connectError: 노드가 FPolicy 서버 "12.195.15.146"과 연결을 설정하지 못했습니다(이유: "선택 시간 초과")"라는 오류 메시지를 표시합니다. 다음을 시도해 보세요: SVM/클러스터에서 방화벽이 활성화되어 있습니다. 따라서 fpolicy 엔진이 fpolicy 서버에 연결할 수 없습니다. 더 많은 정보를 얻는 데 사용할 수 있는 ONTAP 의 CLI는 다음과 같습니다.

```
event log show -source fpolicy which shows the error
event log show -source fpolicy -fields event,action,description which
shows more details.
```

"방화벽 명령 확인"ONTAP 측에서.

{비어 있는}

문제: 오류 메시지: "커넥터가 오류 상태입니다. 서비스 이름: 감사. 실패 이유: SVM에서 유효한 데이터 인터페이스(역할: 데이터, 데이터 프로토콜: NFS 또는 CIFS 또는 둘 다, 상태: 작동)를 찾을 수 없습니다. 다음을 시도해 보세요. CIFS/NFS로서 데이터 역할과 데이터 프로토콜을 갖는 운영 인터페이스가 있는지 확인하세요.

{비어 있는}

문제: 데이터 수집기가 오류 상태로 전환된 후 얼마 후 실행 상태로 전환되고 다시 오류 상태로 돌아갑니다. 이런 순환이 반복됩니다. 다음을 시도해 보세요: 이는 일반적으로 다음 시나리오에서 발생합니다.

1. 여러 개의 데이터 수집기가 추가되었습니다.
2. 이런 종류의 행동을 보이는 데이터 수집기에는 해당 데이터 수집기에 1개의 SVM이 추가됩니다. 즉, 2개 이상의 데이터 수집기가 1개의 SVM에 연결되어 있습니다.
3. 1개의 데이터 수집기가 1개의 SVM에만 연결되도록 하세요.
4. 동일한 SVM에 연결된 다른 데이터 수집기를 삭제합니다.

{비어 있는}

문제: 커넥터가 오류 상태입니다. 서비스 이름: 감사. 실패 이유: (SVM svmname에 대한 정책을 구성하지 못했습니다.) 이유: 'fpolicy.policy.scope-modify: "Federal" 내의 'shares-to-include' 요소에 잘못된 값이 지정되었습니다. 다음을 시도해 보세요. *공유 이름은 따옴표 없이 지정해야 합니다. ONTAP SVM DSC 구성을 편집하여 공유 이름을 수정합니다.

_주식 포함 및 제외_는 긴 주식 이름 목록에는 적용되지 않습니다. 포함하거나 제외할 주식 수가 많은 경우 대신 거래량별 필터링을 사용하세요.

{비어 있는}

문제: 클러스터에 사용되지 않는 기존 fpolicies가 있습니다. Workload Security를 설치하기 전에 무엇을 해야 합니까? 다음을 시도해 보세요. 연결이 끊긴 상태라도 기존의 사용되지 않는 모든 fpolicy 설정을 삭제하는 것이 좋습니다. Workload Security는 "cloudsecure_" 접두사로 fpolicy를 생성합니다. 나머지 사용되지 않는 fpolicy 구성은 모두 삭제할 수 있습니다.

fpolicy 목록을 표시하는 CLI 명령:

```
 fpolicy show
fpolicy 구성을 삭제하는 단계:
```

```
fpolicy disable -vserver <svmname> -policy-name <policy_name>
fpolicy policy scope delete -vserver <svmname> -policy-name <policy_name>
fpolicy policy delete -vserver <svmname> -policy-name <policy_name>
fpolicy policy event delete -vserver <svmname> -event-name <event_list>
fpolicy policy external-engine delete -vserver <svmname> -engine-name
<engine_name>
```

{비어 있는}

문제점: 워크로드 보안을 활성화한 후 ONTAP 성능에 문제가 발생합니다. 지연 시간이 간헐적으로 높아지고, IOP가 간헐적으로 낮아집니다. 다음과 같이 시도해 보세요: ONTAP 워크로드 보안과 함께 사용할 때 ONTAP 에서 지연 문제가 발생할 수 있습니다. 다음과 같이 몇 가지 가능한 이유가 있습니다."1372994" , "1415152" , "1438207" , "1479704" , "1354659" . 이러한 문제는 모두 ONTAP 9.13.1 이상에서 해결되었습니다. 이후 버전 중 하나를 사용하는 것이 좋습니다.

{비어 있는}

문제**:** 데이터 수집기에서 다음 오류 메시지가 표시됩니다. "오류: 2번의 재시도 내에 수집기의 상태를 확인하지 못했습니다. 수집기를 다시 시작해 보세요(오류 코드: AGENT008)". 이걸 시도해보세요**:**

1. 데이터 수집기 페이지에서 오류가 발생한 데이터 수집기의 오른쪽으로 스크롤하여 3개 점 메뉴를 클릭합니다. 편집 _을 선택하세요. 데이터 수집기의 비밀번호를 다시 입력하세요. _저장 버튼을 눌러 데이터 수집기를 저장합니다. 데이터 수집기가 다시 시작되면 오류가 해결될 것입니다.
2. 에이전트 머신에는 CPU나 RAM 여유 공간이 충분하지 않아 DSC가 실패하는 것입니다. 머신의 에이전트에 추가된 데이터 수집기의 수를 확인하세요. 20이 넘을 경우, Agent 머신의 CPU와 RAM 용량을 늘려주세요. CPU와 RAM이 늘어나면 DSC는 초기화 상태로 전환되고, 그다음에는 자동으로 실행 상태로 전환됩니다. 사이즈 가이드를 살펴보세요"이 페이지" .

{비어 있는}

문제**:** SVM 모드를 선택하면 데이터 수집기에서 오류가 발생합니다. 다음을 시도해 보세요**.** SVM 모드에서 연결하는 동안 SVM 관리 IP 대신 클러스터 관리 IP를 사용하여 연결하면 연결 오류가 발생합니다. 올바른 SVM IP가 사용되었는지 확인하세요.

{비어 있는}

문제**:** 액세스 거부 기능이 활성화된 경우 데이터 수집기에서 "커넥터가 오류 상태입니다."라는 오류 메시지가 표시됩니다. 서비스 이름: 감사. 실패 이유: SVM test_svm에서 fpolicy를 구성하지 못했습니다. 사유: 사용자에게 권한이 없습니다. 다음을 시도해 보세요**.** 사용자에게 액세스 거부 기능에 필요한 REST 권한이 없을 수 있습니다. 다음 지침을 따르십시오."이 페이지" 권한을 설정하려면.

권한이 설정되면 수집기를 다시 시작합니다.

{비어 있는}

문제**:** 컬렉터가 "커넥터가 오류 상태입니다"라는 메시지와 함께 오류 상태에 있습니다. 실패 원인: SVM <SVM 이름>에 영구 저장소를 구성하는 데 실패했습니다. 이유: SVM "<SVM 이름>"에서 볼륨 "<볼륨 이름>"에 적합한 집계를 찾을 수 없습니다. 이유: 현재 집계 "<aggregateName>"에 대한 성능 정보를 사용할 수 없습니다. 몇 분 기다렸다가 명령어를 다시 시도해 보세요. 서비스 이름: 감사. 실패 이유: SVM에서 영구 저장소를 구성하지 못했습니다 <svm name="">.</svm> 이유: <volumename>SVM "<svm name="">"</svm>에서</volumename> 볼륨 ""에 적합한 애그리게이트를 찾을 수 없습니다. 이유: 애그리게이트 ""에 대한 성능 정보를 <aggregatename>현재 사용할 수 없습니다.</aggregatename> 몇 분 정도 기다렸다가 명령을 다시 시도하십시오.

다음 방법을 시도해 보세요**:** 몇 분 정도 기다린 후 수집기를 다시 시작하세요.

{비어 있는}

여전히 문제가 발생하는 경우, 도움말 **>** 지원 페이지에 언급된 지원 링크로 문의하세요.
