워크로드 보안

Data Infrastructure Insights

NetApp
January 10, 2025

목차

워크로드 보안

스토리지 워크로드 보안 정보

Data Infrastructure Insights 스토리지 워크로드 보안(이전의 Cloud Secure)은 내부자 위협에 대한 실행 가능한 인텔리전스를 사용하여 데이터를 보호하는 데 도움이 됩니다. 또한 하이브리드 클라우드 환경 전반에서 모든 기업 데이터 액세스에 대한 중앙 집중식 가시성과 제어를 제공하여 보안 및 규정 준수 목표를 충족할 수 있습니다.

가시성

온프레미스 또는 클라우드에 저장된 주요 기업 데이터에 대한 사용자 액세스를 중앙 집중식으로 파악하고 제어할 수 있습니다.

데이터 액세스 및 제어에 대한 시기 적절하고 정확한 가시성을 제공하지 못하는 도구 및 수동 프로세스를 대체합니다. 워크로드 보안은 클라우드 및 사내 스토리지 시스템 모두에서 고유하게 작동하며 악의적인 사용자 동작에 대한 실시간 경고를 제공합니다.

보호

악의적인 사용자 또는 손상된 사용자가 조직 데이터를 악용하지 못하도록 고급 머신 러닝 및 이상 징후 탐지를 통해 보호합니다.

고급 머신 러닝 및 사용자 동작에 대한 이상 탐지 기능을 통해 비정상적인 데이터 액세스를 경고합니다.

규정 준수

온프레미스 또는 클라우드에 저장된 중요한 기업 데이터에 대한 사용자 데이터 액세스를 감사하여 기업의 규정 준수를 보장할 수 있습니다.

시작하기

워크로드 보안 시작

워크로드 보안을 사용하여 사용자 작업을 모니터링하려면 먼저 완료해야 하는 구성 작업이 있습니다.

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

데이터 수집을 시작하려면 먼저 다음을 구성해야 합니다.

작업	관련 정보

Agent를 구성합니다	"상담원 요구 사항" "상담원 추가" "* 비디오 *: 에이전트 배포"
사용자 디렉터리 커넥터를 구성합니다	"사용자 디렉토리 커넥터를 추가합니다" "* 비디오 *: Active Directory 연결"
데이터 수집기를 구성합니다	Workload Security > Collectors * 를 클릭하여 구성할 데이터 수집기를 클릭합니다. 설명서의 Data Collector 공급업체 참조 섹션을 참조하십시오. "* 비디오 *: ONTAP SVM 연결"
사용자 계정을 생성합니다	"사용자 계정 관리"
문제 해결	"* 비디오 *: 문제 해결"

워크로드 보안은 다른 툴과도 통합될 수 있습니다. 예를 들어"이 가이드를 참조하십시오", Splunk와 통합할 수 있습니다.

워크로드 보안 에이전트 요구 사항

데이터 수집기에서 정보를 얻으려면 사용자가 있어야 "Agent를 설치합니다"합니다. Agent를 설치하기 전에 운영 체제, CPU, 메모리 및 디스크 공간 요구 사항을 충족하는지 확인해야 합니다.

구성 요소	**Linux** 요구 사항
운영 체제	다음 중 하나의 라이센스 버전을 실행하는 컴퓨터: * CentOS 8 Stream(64비트), CentOS 9 Stream, SELinux * OpenSUSE Leap 15.3 - 15.5(64비트) * Oracle Linux 8.6 - 8.8, 9.1 - 9.4 - 9.4(64비트) * Red Hat Enterprise Linux 8.6 - 9.4 - 9.4, SUSE Linux 9 - 64 비트 Linux * 9.4 - 64 비트 Linux * 9.4, SUSE Linux 8 전용 서버가 권장됩니다.
명령	설치를 위해 '압축 해제'가 필요합니다. 또한 설치, 스크립트 실행 및 제거에 'SUDO su –' 명령이 필요합니다.
CPU	CPU 코어 4개
메모리	16GB RAM
사용 가능한 디스크 공간입니다	디스크 공간은 /opt/NetApp 36GB(파일 시스템 생성 후 최소 35GB의 여유 공간)와 같은 방식으로 할당되어야 합니다. 참고: 파일 시스템을 생성할 수 있도록 추가 디스크 공간을 할당하는 것이 좋습니다. 파일 시스템에 최소 35GB의 여유 공간이 있는지 확인합니다. /opt가 NAS 스토리지에서 마운트된 폴더인 경우 로컬 사용자가 이 폴더에 액세스할 수 있는지 확인합니다. 로컬 사용자에게 이 폴더에 대한 권한이 없는 경우 Agent 또는 Data Collector가 설치되지 않을 수 있습니다. 자세한 내용은 섹션을 참조하십시오."문제 해결"
네트워크	100Mbps~1Gbps 이더넷 연결, 정적 IP 주소, 모든 디바이스에 대한 IP 연결 및 워크로드 보안 인스턴스(80 또는 443)에 대한 필수 포트.

참고: 워크로드 보안 에이전트는 Data Infrastructure Insights 수집 장치 및/또는 에이전트와 동일한 시스템에 설치할 수

있습니다. 그러나 별도의 컴퓨터에 설치하는 것이 가장 좋습니다. 동일한 시스템에 설치된 경우 아래와 같이 디스크 공간을 할당하십시오.

사용 가능한 디스크 공간입니다	Linux의 경우 디스크 공간을 50GB~55GB로, /opt/NetApp 25-30 GB/var/log/NetApp 25GB로 할당해야 합니다

추가 권장 사항

- NTP(Network Time Protocol) * 또는 * SNTP(Simple Network Time Protocol) * 를 사용하여 ONTAP 시스템과 에이전트 시스템의 시간을 동기화하는 것이 좋습니다.

클라우드 네트워크 액세스 규칙

미국 * 기반 * 워크로드 보안 환경:

프로토콜	포트	출처	목적지	설명
TCP	443	워크로드 보안 에이전트	site_name> .cs01.cloudinsights.netapp.com <site_name> .c01.cloudinsights.netapp.com <site_name> .c02.cloudinsights.netapp.com 을 참조하십시오	Data Infrastructure Insights에 액세스
TCP	443	워크로드 보안 에이전트	gateway.c01.cloudinsights.netapp.com agentlogin.cs01.cloudinsights.netapp.com	인증 서비스에 대한 액세스

유럽 기반 * 워크로드 보안 환경:

프로토콜	포트	출처	목적지	설명
TCP	443	워크로드 보안 에이전트	site_name> .cs01-eu-1.cloudinsights.netapp.com <site_name> .c01-eu-1.cloudinsights.netapp.com <site_name> .c02-eu-1.cloudinsights.netapp.com 을 참조하십시오	Data Infrastructure Insights에 액세스

프로토콜	포트	출처	목적지	설명
TCP	443	워크로드 보안 에이전트	gateway.c01.cloudinsights.netapp.com agentlogin.cs01-eu-1.cloudinsights.netapp.com	인증 서비스에 대한 액세스

APAC 기반 * 워크로드 보안 환경의 경우:

프로토콜	포트	출처	목적지	설명
TCP	443	워크로드 보안 에이전트	site_name> .cs01-ap-1.cloudinsights.netapp.com <site_name> .c01-ap-1.cloudinsights.netapp.com <site_name> .c02-ap-1.cloudinsights.netapp.com 을 참조하십시오	Data Infrastructure Insights에 액세스
TCP	443	워크로드 보안 에이전트	gateway.c01.cloudinsights.netapp.com agentlogin.cs01-ap-1.cloudinsights.netapp.com	인증 서비스에 대한 액세스

네트워크 내 규칙

프로토콜	포트	출처	목적지	설명
TCP	389(LDAP) 636(LDAPS/START-TLS)	워크로드 보안 에이전트	LDAP 서버 URL입니다	LDAP에 연결합니다
TCP	443	워크로드 보안 에이전트	클러스터 또는 SVM 관리 IP 주소(SVM 수집기 구성에 따라 다름)	ONTAP와의 API 통신

프로토콜	포트	출처	목적지	설명
TCP	35000-55000	SVM 데이터 LIF IP 주소	워크로드 보안 에이전트	Fpolicy 이벤트에 대해 ONTAP에서 워크로드 보안 에이전트로의 통신 ONTAP가 워크로드 보안 에이전트(있는 경우)에 방화벽을 포함하여 이벤트를 보내려면 이러한 포트를 워크로드 보안 에이전트에 개방해야 합니다. 이러한 포트를 * 모두 * 예약할 필요는 없지만 이 범위 내에 예약하는 포트가 있어야 합니다. 우선 100개 이하의 포트를 예약하여 필요한 경우 늘리는 것이 좋습니다.
TCP	7	워크로드 보안 에이전트	SVM 데이터 LIF IP 주소	Agent에서 SVM 데이터 LIF로 에코
SSH를 클릭합니다	22	워크로드 보안 에이전트	클러스터 관리	CIFS/SMB 사용자 차단에 필요합니다.

시스템 사이징

"이벤트 속도 검사기"크기 조정에 대한 자세한 내용은 설명서를 참조하십시오.

워크로드 보안 에이전트 설치

워크로드 보안(이전의 Cloud Secure)은 하나 이상의 에이전트를 사용하여 사용자 활동 데이터를 수집합니다. 에이전트는 테넌트의 장치에 연결하고 분석을 위해 워크로드 보안 SaaS 계층으로 전송되는 데이터를 수집합니다. 에이전트 VM을 구성하려면 을 "상담원 요구 사항"참조하십시오.

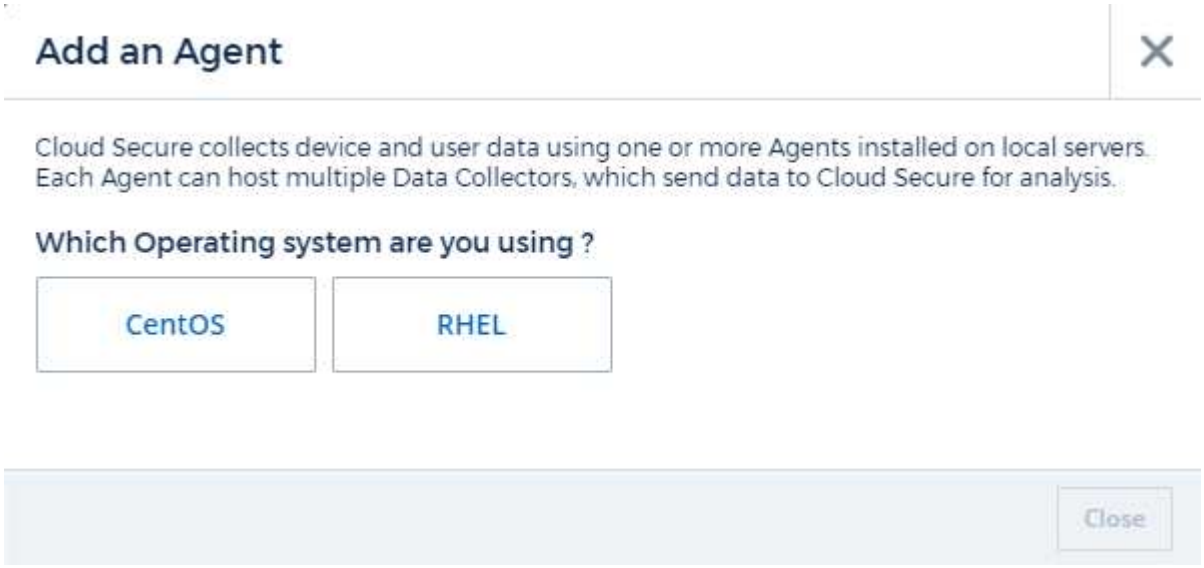
시작하기 전에

- 설치, 스크립트 실행 및 제거에 sudo 권한이 필요합니다.
- 에이전트를 설치하는 동안 로컬 user_cssys_와 로컬 group_cssys_가 시스템에 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 알아볼 수 "여기"있습니다.

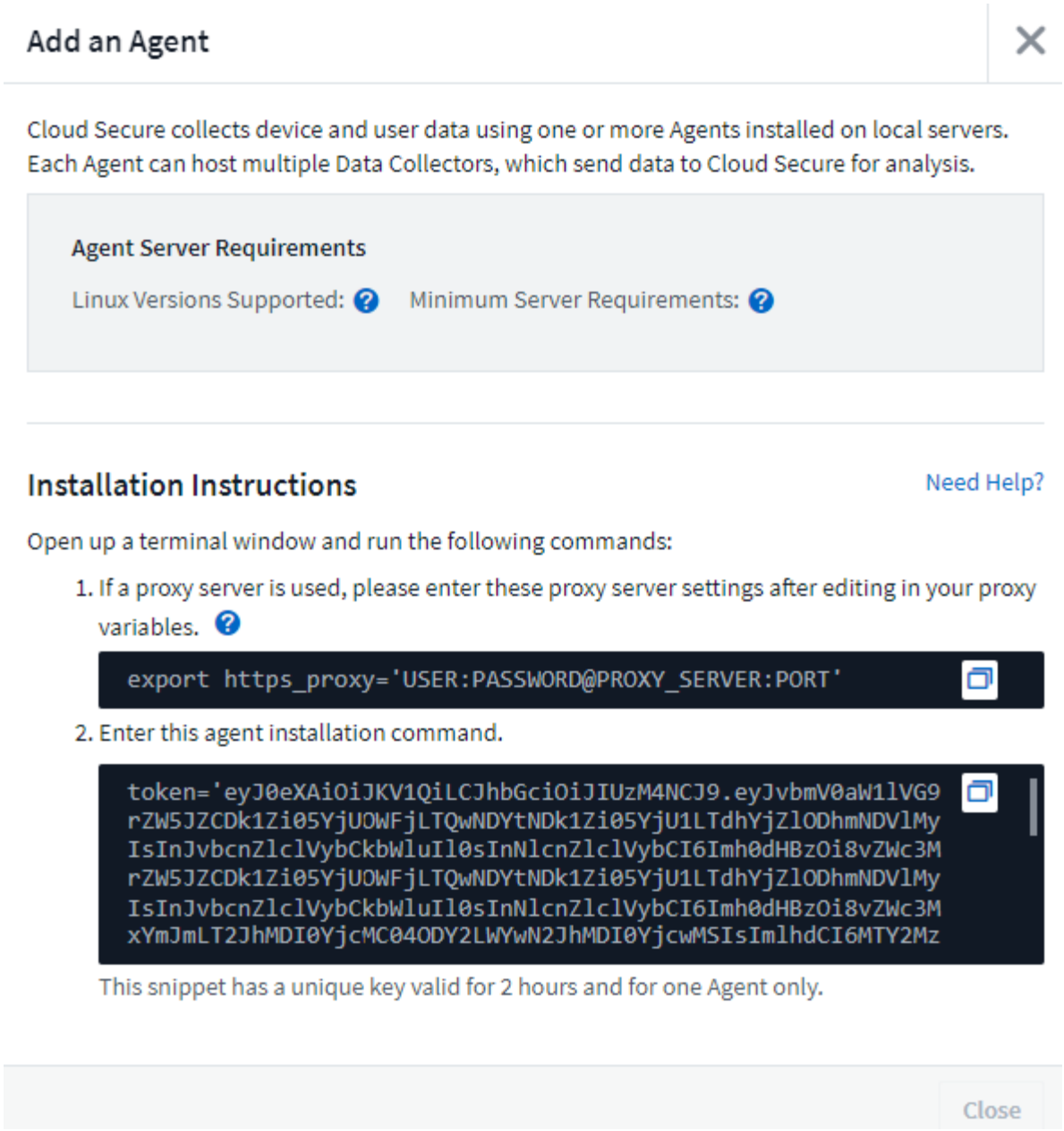
Agent 설치 단계

1. 워크로드 보안 환경에 관리자 또는 계정 소유자로 로그인합니다.
2. Collector > Agents > + Agent * 를 선택합니다

Agent 추가 페이지가 표시됩니다.



3. 에이전트 서버가 최소 시스템 요구 사항을 충족하는지 확인합니다.
4. 에이전트 서버가 지원되는 Linux 버전을 실행 중인지 확인하려면 _VERSION SUPPORTED (I) _ 을(를) 클릭합니다.
5. 네트워크에서 프록시 서버를 사용하는 경우 프록시 섹션의 지침에 따라 프록시 서버 세부 정보를 설정하십시오.



6. 클립보드로 복사 아이콘을 클릭하여 설치 명령을 복사합니다.
7. 터미널 창에서 설치 명령을 실행합니다.
8. 설치가 성공적으로 완료되면 다음과 같은 메시지가 표시됩니다.

작업을 마친 후

1. 를 구성해야 "사용자 디렉토리 수집기"합니다.
2. 하나 이상의 Data Collector를 구성해야 합니다.

네트워크 구성

로컬 시스템에서 다음 명령을 실행하여 워크로드 보안에서 사용할 포트를 엽니다. 포트 범위에 대한 보안 문제가 있는 경우, 보다 낮은 포트 범위를 사용할 수 있습니다(예: *35000:35100*). 각 SVM은 포트 2개를 사용합니다.

단계

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

플랫폼에 따라 다음 단계를 따르십시오.

- 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
```

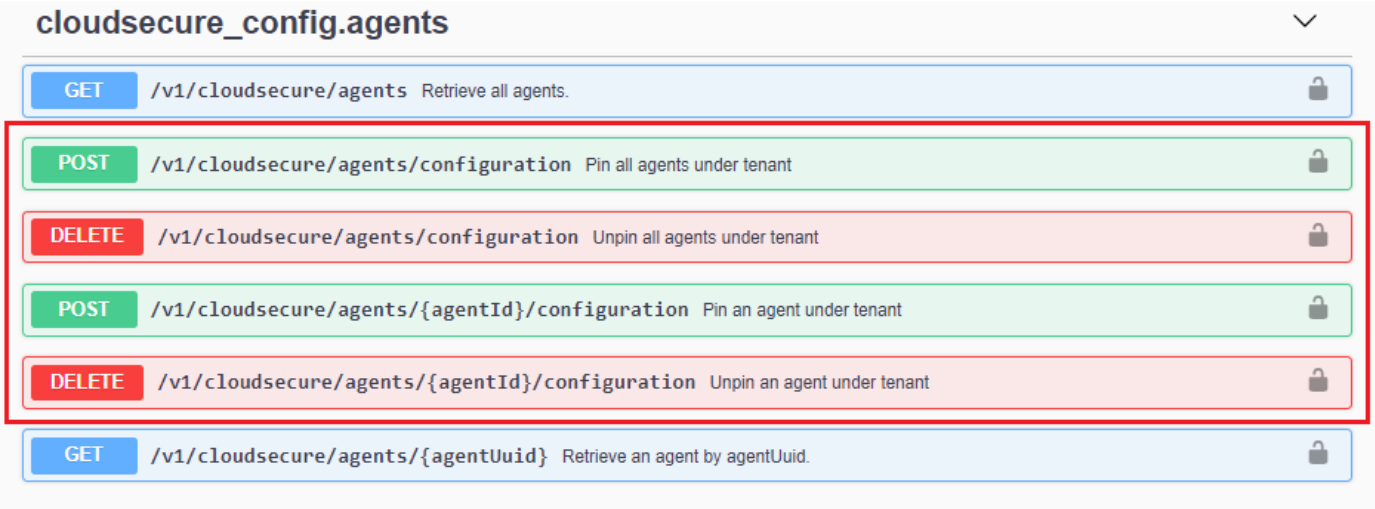
현재 버전에서 에이전트 **"고정"**

기본적으로 Data Infrastructure Insights 워크로드 보안은 에이전트를 자동으로 업데이트합니다. 일부 고객은 다음 중 하나가 발생할 때까지 Agent를 현재 버전으로 유지하는 자동 업데이트를 일시 중지할 수 있습니다.

- 고객이 Agent 자동 업데이트를 재개합니다.
- 30일이 지났습니다. 30일은 Agent가 일시 중지된 날이 아니라 가장 최근의 Agent 업데이트 날짜부터 시작됩니다.

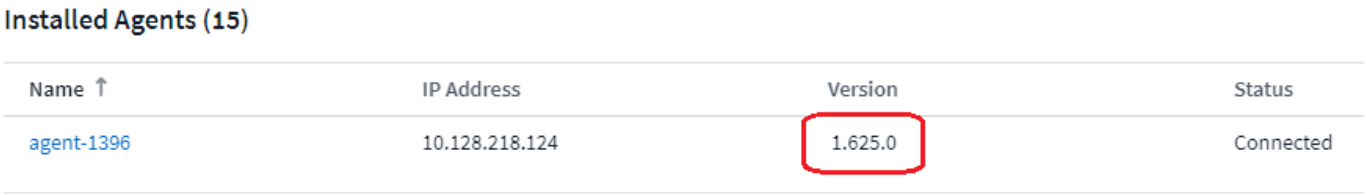
이러한 각 경우에 에이전트는 다음 워크로드 보안 새로 고침 시 업데이트됩니다.

자동 에이전트 업데이트를 일시 중지하거나 다시 시작하려면 _cloudsecure_config.agent_aps:



일시 중지 또는 다시 시작 작업이 적용되는 데 최대 5분이 소요될 수 있습니다.

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



상담원 오류 문제 해결

알려진 문제와 해결 방법은 다음 표에 설명되어 있습니다.

문제:	해상도:
Agent 설치가 /opt/netapp/cloudsecure/agent/logs/agent.log 폴더를 생성하지 못하고 install.log 파일은 관련 정보를 제공하지 않습니다.	이 오류는 에이전트의 부트스트래핑 중에 발생합니다. 로그 파일이 로거가 초기화되기 전에 발생하므로 이 오류는 로그 파일에 기록되지 않습니다. 오류는 표준 출력으로 리디렉션되며 `journalctl -u cloudsecure-agent.service` 명령을 사용하여 서비스 로그에 표시됩니다. 이 명령을 사용하여 문제를 추가로 해결할 수 있습니다. est
에이전트 설치가 '이 Linux 배포는 지원되지 않습니다. 설치를 종료하는 중입니다.	이 오류는 지원되지 않는 시스템에 Agent를 설치하려고 할 때 나타납니다. 을 "상담원 요구 사항"참조하십시오.
"-bash:unzip:command not found" 오류와 함께 에이전트 설치가 실패했습니다.	압축을 푼 다음 설치 명령을 다시 실행합니다. 시스템에 Yum이 설치되어 있는 경우 "yum install unzip"을 시도하여 unzip 소프트웨어를 설치합니다. 그런 다음 Agent 설치 UI에서 명령을 다시 복사하여 CLI에 붙여 넣어 설치를 다시 실행합니다.

문제:	해상도:

에이전트가 설치되어 실행 중입니다. 하지만 상담원이 갑자기 중지되었습니다.	Agent 시스템에 SSH를 연결합니다. 를 통해 상담원 서비스의 상태를 `sudo systemctl status cloudsecure-agent.service` 확인합니다. 1. 로그에 "Failed to start Workload Security daemon service"라는 메시지가 표시되는지 확인합니다. 2. Agent 시스템에 cssys 사용자가 있는지 확인하십시오. 루트 권한으로 다음 명령을 하나씩 실행하고 cssys 사용자 및 그룹이 있는지 확인합니다.
	`sudo id cssys`
	`sudo groups cssys` 3. 아무 것도 없는 경우 중앙 집중식 모니터링 정책이 cssys 사용자를 삭제했을 수 있습니다. 4. 다음 명령을 실행하여 cssys 사용자 및 그룹을 수동으로 생성합니다.
	`sudo useradd cssys`
	`sudo groupadd cssys` 5. 에이전트 서비스를 다시 시작한 후 다음 명령을 실행하여 에이전트 서비스를 다시 시작합니다
	`sudo systemctl restart cloudsecure-agent.service`. 6. 여전히 실행되지 않는 경우 다른 문제 해결 옵션을 확인하십시오.

Agent에 50개 이상의 데이터 수집기를 추가할 수 없습니다.	데이터 수집기는 50개만 에이전트에 추가할 수 있습니다. Active Directory, SVM 및 기타 수집기와 같은 모든 수집기 유형의 조합이 될 수 있습니다.
UI에 Agent가 NOT_Connected 상태임 이 표시됩니다.	Agent를 다시 시작하는 단계입니다. 1. Agent 시스템에 SSH를 연결합니다. 2. 그 후에 다음 명령을 실행하여 에이전트 서비스를 다시 시작합니다 `sudo systemctl restart cloudsecure-agent.service`. 3. 를 통해 상담원 서비스의 상태를 `sudo systemctl status cloudsecure-agent.service` 확인합니다. 4. 상담원은 연결된 상태로 이동해야 합니다.
에이전트 VM이 Zscaler 프록시 뒤에 있으며 에이전트 설치가 실패합니다. Zscaler 프록시의 SSL 검사로 인해 워크로드 보안 인증서는 Zscaler CA에 의해 서명된 것으로 표시되므로 에이전트가 통신을 신뢰하지 않습니다.	.cloudinsights.netapp.com URL의 Zscaler 프록시에서 SSL 검사를 비활성화합니다. Zscaler가 SSL 검사를 수행하고 인증서를 대체하는 경우 Workload Security가 작동하지 않습니다.
에이전트를 설치하는 동안 압축 해제 후 설치가 중단됩니다.	"chmod 755-rf" 명령이 실패했습니다. 작업 디렉토리에 파일이 있고 다른 사용자에게 속해 있으며 해당 파일의 사용 권한을 변경할 수 없는 루트가 아닌 sudo 사용자가 에이전트 설치 명령을 실행하는 경우 명령이 실패합니다. chmod 명령이 실패하여 나머지 설치가 실행되지 않습니다. 1. "cloudsecure"라는 새 디렉토리를 생성합니다. 2. 해당 디렉터리로 이동합니다. 3. 전체 "토큰 = ……..입니다./cloudsecure-agent-install.sh" 설치 명령을 복사하여 붙여 넣고 Enter 키를 누릅니다. 4. 설치를 계속 진행할 수 있어야 합니다.

문제:	해상도:
Agent가 여전히 SaaS에 연결할 수 없는 경우 NetApp Support로 사례를 여십시오. Data Infrastructure Insights 일련 번호를 제공하여 케이스를 생성하고 언급된 대로 로그에 로그를 첨부합니다.	케이스에 로그를 첨부하려면 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 공유합니다. a.id cssys b. groups cssys cat /etc/os-release
cloudsecure-agent-symptom-collector.sh 스크립트가 실패하고 다음 오류가 표시됩니다. [root@machine tmp]#/opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh 서비스 로그 수집 애플리케이션 로그 수집 에이전트 상태 스냅샷 생성 에이전트 디렉토리 구조 스냅샷 생성…… . …… . /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh:line 52:zip: 명령을 찾을 수 없음 오류: /tmp/cloudsecure-agent-symptoms.zip 생성하지 못했습니다	zip 도구가 설치되지 않았습니다. "yum install zip" 명령을 실행하여 zip 툴을 설치합니다. 그런 다음 cloudsecure-agent-symptom-collector.sh 를 다시 실행합니다.
useradd를 사용하여 에이전트 설치가 실패했습니다. 디렉토리 /home/cssys를 생성할 수 없습니다	이 오류는 권한 부족으로 인해 /home 아래에 사용자의 로그인 디렉토리를 만들 수 없는 경우에 발생할 수 있습니다. 해결 방법은 cssys 사용자를 생성하고 다음 명령을 사용하여 로그인 디렉토리를 수동으로 추가하는 것입니다. *sudo useradd user_name -m -d home_DIR* -m: 사용자의 홈 디렉토리가 없는 경우 생성합니다. d: 사용자의 로그인 디렉토리 값으로 HOME_DIR을 사용하여 새 사용자가 생성됩니다. 예를 들어, _sudo useradd cssys -m -d /cssys_는 user_cssys_를 추가하고 root 아래에 로그인 디렉토리를 만듭니다.
설치 후 에이전트가 실행되고 있지 않습니다. *Systemctl status cloudsecure-agent.service* NetApp cloudsecure-agent.service: 다음과 같이 표시됩니다.[root@demo~] #systemctl status cloudsecure-agent.service agent.service cloudsecure-agent.service – 워크로드 보안 에이전트 데몬 서비스가 로드됨(/usr/lib/systemd/system/cloudsecure-agent.service; 사용 8월 03 21:12:26 데모 시스템[1]: cloudsecure-agent.service 실패.	cssys_user에 설치 권한이 없을 수 있으므로 이 작업은 실패할 수 있습니다. /opt/netapp가 NFS 마운트이고 _cssys_user가 이 폴더에 대한 액세스 권한이 없는 경우 설치가 실패합니다. _cssys_는 워크로드 보안 설치 관리자가 생성한 로컬 사용자이며 마운트된 공유에 액세스할 권한이 없을 수 있습니다. cssys_user를 사용하여 /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent에 액세스하여 이를 확인할 수 있습니다. "사용 권한 거부"를 반환하면 설치 권한이 없는 것입니다. 마운트된 폴더 대신 컴퓨터에 로컬 디렉토리에 설치합니다.

문제:	해상도:
Agent가 처음에 프록시 서버를 통해 연결되었고 Agent 설치 중에 프록시가 설정되었습니다. 이제 프록시 서버가 변경되었습니다. Agent의 프록시 구성을 변경하려면 어떻게 해야 합니까?	agent.properties 를 편집하여 프록시 세부 정보를 추가할 수 있습니다. 다음 단계를 따르십시오. 1. 속성 파일이 포함된 폴더로 변경합니다. cd /opt/netapp/cloudsecure/conf 2. 즐겨찾기 텍스트 편집기를 사용하여 편집할 *agent.properties* 파일을 엽니다. 3. agent_proxy_host=scspa1950329001.vm.NetApp.com agent_proxy_port=80 agent_proxy_user=pxuser agent_proxy_password=pass1234 4 줄을 추가하거나 수정합니다. 파일을 저장합니다. 5. 에이전트를 다시 시작합니다. sudo systemctl restart cloudsecure-agent.service

워크로드 보안 에이전트를 삭제하는 중입니다

Workload Security Agent를 삭제하면 Agent와 연결된 모든 데이터 수집기가 먼저 삭제되어야 합니다.

상담원 삭제

Agent를 삭제하면 Agent와 연결된 모든 Data Collector가 삭제됩니다. 다른 에이전트로 데이터 수집기를 구성하려는 경우 에이전트를 삭제하기 전에 Data Collector 구성의 백업을 만들어야 합니다.

시작하기 전에

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

   참고: 연결된 모든 수집기가 중지 상태인 경우 이 단계를 무시하십시오.

에이전트를 삭제하는 단계:

1. 에이전트 VM에 SSH를 수행하고 다음 명령을 실행합니다. 메시지가 표시되면 "y"를 입력하여 계속합니다.

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

2. Workload Security > Collector > Agents * 를 클릭합니다

   구성된 에이전트 목록이 표시됩니다.

3. 삭제하려는 상담원의 옵션 메뉴를 누릅니다.
4. 삭제 * 를 클릭합니다.

   시스템에 * Delete Agent * 페이지가 표시됩니다.

5. 삭제를 확인하려면 * 삭제 * 를 클릭합니다.

AD(Active Directory) 사용자 디렉토리 수집기 구성

Active Directory 서버에서 사용자 속성을 수집하도록 워크로드 보안을 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 디렉터리 커넥터를 구성하기 전에 Agent를 구성해야 합니다.

사용자 디렉토리 수집기를 구성하는 단계입니다

1. 워크로드 보안 메뉴에서 * Collector > 사용자 디렉토리 수집기 > + 사용자 디렉토리 수집기 * 를 클릭하고 * Active Directory * 를 선택합니다

   사용자 디렉토리 추가 화면이 표시됩니다.

다음 표에 필요한 데이터를 입력하여 사용자 디렉토리 수집기를 구성합니다.

이름	설명
이름	사용자 디렉토리의 고유 이름입니다. 예: *GlobalADCollector*
에이전트	목록에서 구성된 에이전트를 선택합니다
서버 IP/도메인 이름	Active Directory를 호스팅하는 서버의 IP 주소 또는 FQDN(정규화된 도메인 이름)입니다
포리스트 이름	디렉터리 구조의 포리스트 수준입니다. 포리스트 이름을 사용하면 SVM에 있는 것과 같은 *x.x.y.z*⇒직접 도메인 이름을 사용할 수 있습니다. *dc=x, dc=y, dc=z*⇒ 상대 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 엔지니어링으로 필터링하기]*CN=username,OU=engineering,DC=CompanyName, DC=NetApp,DC=com*[OU<engineering>에서 특정 사용자만 가져오려면]_CN=Acrobat=Users,CN=Users,DC=Users,DC=Users,DC=CompanyName=Active,MA_DC=Users,CompanyName=Trusted,DC=Active_DC=CompanyName=CompanyName=Users=Active,DC=CompanyName=CompanyName=CompanyName=Users,DC=CompanyName=CompanyName=A,DC=Users,DC=CompanyName=
DN 바인딩	사용자가 디렉터리를 검색할 수 있습니다. 예를 들어 *username@companyname.com* 또는 *username@domainname.com* 도메인 읽기 전용 권한도 필요합니다. 사용자는 보안 그룹 _읽기 전용 도메인 컨트롤러_의 구성원이어야 합니다.
암호를 바인딩합니다	디렉터리 서버 암호(예: Bind DN에서 사용되는 사용자 이름의 암호)

프로토콜	LDAP, LDAPS, LDAP-START-TLS
포트	포트를 선택합니다

Active Directory에서 기본 속성 이름이 수정된 경우 다음 Directory Server 필수 속성을 입력합니다. 이러한 속성 이름은 대부분 Active Directory에서 _not_modified입니다. 이 경우 기본 속성 이름을 사용하여 간단하게 진행할 수 있습니다.

속성	Directory Server의 속성 이름입니다
표시 이름	이름
SID	객체 ID입니다
사용자 이름	sAMAccountName

다음 특성을 추가하려면 선택적 특성 포함 을 클릭합니다.

속성	Directory Server의 속성 이름입니다
이메일 주소	메일
전화 번호	전화 번호
역할	제목
국가	CO
상태	상태
부서	부서
사진	축소판 그림
관리자 DN	관리자
그룹	멤버

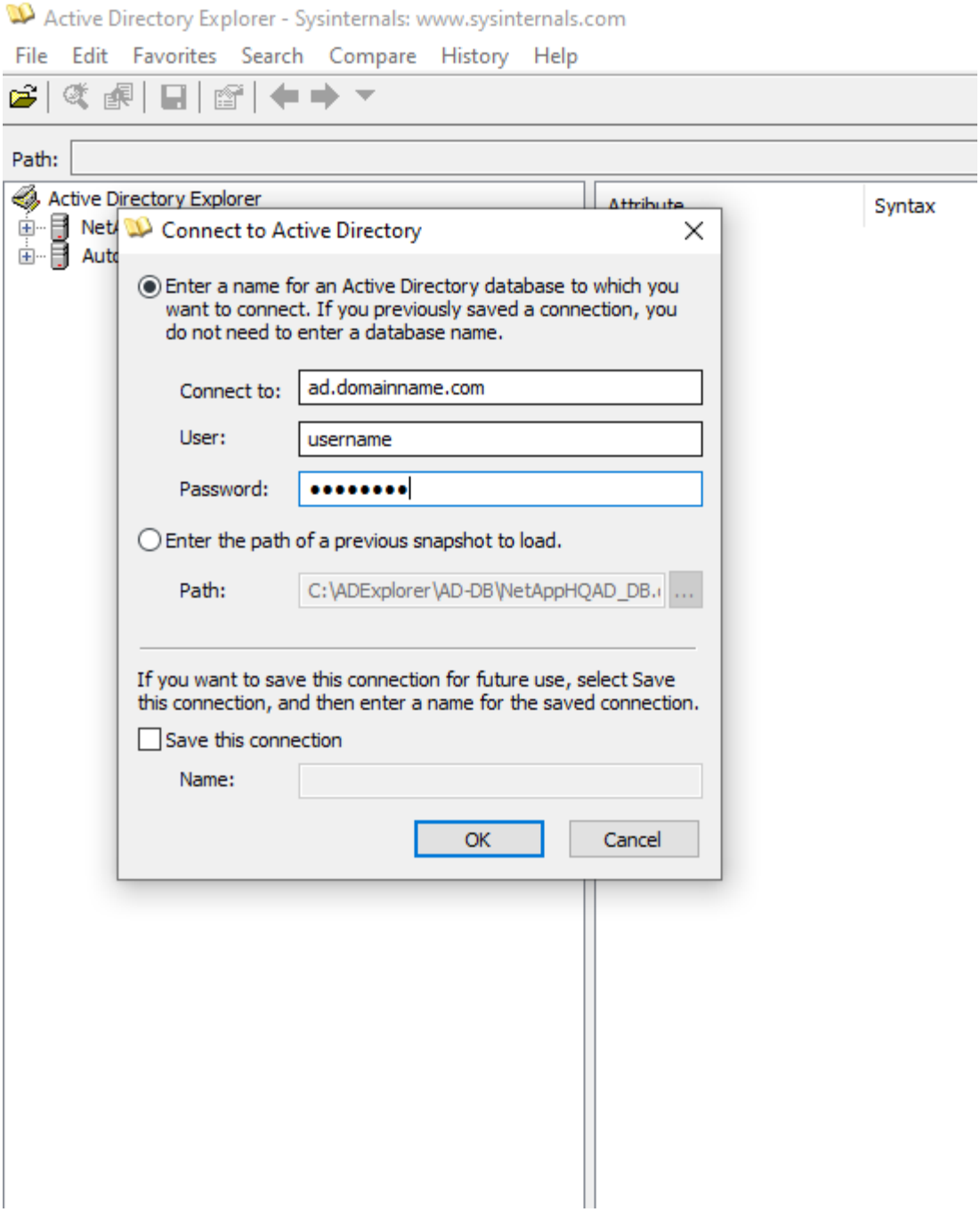
사용자 디렉토리 수집기 구성을 테스트하는 중입니다

다음 절차를 사용하여 LDAP 사용자 권한 및 속성 정의의 유효성을 검사할 수 있습니다.

- 다음 명령을 사용하여 워크로드 보안 LDAP 사용자 권한을 검증합니다.

```
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 탐색기를 사용하여 AD 데이터베이스를 탐색하고, 개체 속성 및 속성을 보고, 권한을 보고, 개체의 스키마를 보고, 저장하고 다시 실행할 수 있는 정교한 검색을 실행할 수 있습니다.
  - AD 서버에 연결할 수 있는 모든 Windows 시스템에 를 "AD 탐색기"설치합니다.
  - AD 디렉토리 서버의 사용자 이름/암호를 사용하여 AD 서버에 연결합니다.



사용자 디렉토리 수집기 구성 오류 문제 해결

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

문제:	해상도:
사용자 디렉토리 커넥터를 추가하면 '오류' 상태가 됩니다. "LDAP 서버에 대해 잘못된 자격 증명이 제공되었습니다 ."라는 오류가 표시됩니다.	잘못된 사용자 이름 또는 암호가 제공되었습니다. 올바른 사용자 이름 및 암호를 편집하고 제공하십시오.
사용자 디렉토리 커넥터를 추가하면 '오류' 상태가 됩니다. "DN=DC=HQ, DC=domainname, DC=com에 해당하는 객체를 포리스트 이름으로 가져오지 못했습니다."라는 오류가 표시됩니다.	잘못된 포리스트 이름이 제공되었습니다. 올바른 포리스트 이름을 편집하고 제공하십시오.

문제:	해상도:
도메인 사용자의 선택적 속성이 워크로드 보안 사용자 프로필 페이지에 나타나지 않습니다.	이는 CloudSecure에 추가된 선택적 속성의 이름과 Active Directory의 실제 속성 이름이 일치하지 않기 때문일 수 있습니다. 올바른 선택적 속성 이름을 편집하고 제공하십시오.
"LDAP 사용자를 검색하지 못했습니다. 실패 원인: 서버에 연결할 수 없습니다. 연결이 null입니다."	*Restart* 단추를 클릭하여 수집기를 다시 시작합니다.
사용자 디렉토리 커넥터를 추가하면 '오류' 상태가 됩니다.	필수 필드(서버, 포리스트-이름, 바인드-DN, 바인드-암호)에 대해 유효한 값을 제공했는지 확인합니다. bind-DN 입력이 항상 'Administrator@<domain_forest_name>' 또는 도메인 관리자 권한이 있는 사용자 계정으로 제공되는지 확인합니다.
사용자 디렉터리 커넥터를 추가하면 '다시 시도 중' 상태가 됩니다. "Collector의 상태를 정의할 수 없습니다. 원인 TCP 명령 [Connect(localhost:35012, None, List(), some(,seconds), true)] 오류가 java.net.ConnectionException:Connection refused 때문에 실패했습니다."	AD 서버에 대해 잘못된 IP 또는 FQDN이 제공되었습니다. 올바른 IP 주소 또는 FQDN을 편집하고 입력합니다.
사용자 디렉토리 커넥터를 추가하면 '오류' 상태가 됩니다. "LDAP 연결을 설정하지 못했습니다."라는 오류가 표시됩니다.	AD 서버에 대해 잘못된 IP 또는 FQDN이 제공되었습니다. 올바른 IP 주소 또는 FQDN을 편집하고 입력합니다.
사용자 디렉토리 커넥터를 추가하면 '오류' 상태가 됩니다. "설정을 로드하지 못했습니다. 원인: DataSource 구성에 오류가 있습니다. 특정 이유: /connector/conf/application.conf: 70: ldap.ldap-port에 숫자가 아닌 유형 문자열이 있습니다."	잘못된 포트 값이 제공되었습니다. AD 서버에 대한 기본 포트 값 또는 올바른 포트 번호를 사용해 보십시오.
나는 필수 속성을 시작했는데 효과가 있었습니다. 옵션 특성 데이터를 추가한 후 선택적 특성 데이터를 AD에서 가져오지 않습니다.	이는 CloudSecure에 추가된 옵션 속성과 Active Directory의 실제 속성 이름이 일치하지 않기 때문일 수 있습니다. 올바른 필수 또는 선택적 속성 이름을 편집하고 제공하십시오.
Collector를 다시 시작한 후 AD 동기화는 언제 이루어집니까?	AD 동기화는 수집기가 다시 시작된 직후에 수행됩니다. 약 30만 명의 사용자가 있는 사용자 데이터를 가져오는 데 약 15분이 소요되며, 12시간마다 자동으로 새로 고쳐집니다.
사용자 데이터가 AD에서 CloudSecure로 동기화됩니다. 언제 데이터가 삭제됩니까?	새로 고침이 없는 경우 사용자 데이터는 13개월 동안 유지됩니다. 테넌트가 삭제되면 데이터가 삭제됩니다.
사용자 디렉토리 커넥터를 사용하면 '오류' 상태가 됩니다. "커넥터가 오류 상태입니다. 서비스 이름: usersLdap. 실패 원인: LDAP 사용자를 검색하지 못했습니다. 실패 원인:80090308:LdapErr:DSID-0C090453, 설명:AcceptSecurityContext 오류, 데이터 52e, v3839"	잘못된 포리스트 이름이 제공되었습니다. 올바른 포리스트 이름을 제공하는 방법은 위의 을 참조하십시오.

문제:	해상도:
전화 번호가 사용자 프로필 페이지에 채워지지 않습니다.	이는 Active Directory의 속성 매핑 문제 때문일 수 있습니다. 1. Active Directory에서 사용자 정보를 가져오는 특정 Active Directory 수집기를 편집합니다. 2. 옵션 속성 아래에 Active Directory 속성 '전화 번호'에 매핑된 필드 이름 "전화 번호"가 있습니다. 4. 이제 위에서 설명한 대로 Active Directory 탐색기 도구를 사용하여 Active Directory를 탐색하고 올바른 속성 이름을 확인하십시오. 3. Active Directory에 사용자의 전화 번호가 있는 '전화 번호'라는 속성이 있는지 확인합니다. 5. Active Directory에서 '전화 번호'로 수정되었다고 가정해 보겠습니다. 6. 그런 다음 CloudSecure 사용자 디렉토리 수집기를 편집합니다. 옵션 속성 섹션에서 '전화 번호'를 '전화 번호'로 바꿉니다. 7. Active Directory Collector를 저장하면 Collector가 다시 시작되고 사용자의 전화 번호를 가져와 사용자 프로필 페이지에 동일한 정보를 표시합니다.
AD(Active Directory) 서버에서 암호화 인증서(SSL)가 활성화된 경우 워크로드 보안 사용자 디렉토리 수집기는 AD 서버에 연결할 수 없습니다.	사용자 디렉토리 수집기를 구성하기 전에 AD 서버 암호화를 비활성화하십시오. 사용자 세부 정보를 가져오면 13개월 동안 표시됩니다. 사용자 세부 정보를 가져온 후 AD 서버의 연결이 끊기면 AD에서 새로 추가된 사용자를 가져오지 않습니다. 다시 가져오려면 사용자 디렉토리 수집기를 AD에 연결해야 합니다.
Active Directory의 데이터는 CloudInsights Security에 있습니다. CloudInsights에서 모든 사용자 정보를 삭제하려는 경우	CloudInsights 보안에서는 Active Directory 사용자 정보만 삭제할 수 없습니다. 사용자를 삭제하려면 전체 테넌트를 삭제해야 합니다.

LDAP Directory Server Collector 구성

LDAP 디렉토리 서버에서 사용자 속성을 수집하도록 워크로드 보안을 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 Agent를 구성해야 합니다.

사용자 디렉토리 수집기를 구성하는 단계입니다

1. 워크로드 보안 메뉴에서 * Collector > 사용자 디렉토리 수집기 > + 사용자 디렉토리 수집기 * 를 클릭하고 * LDAP Directory Server * 를 선택합니다

   사용자 디렉토리 추가 화면이 표시됩니다.

다음 표에 필요한 데이터를 입력하여 사용자 디렉토리 수집기를 구성합니다.

이름	설명
이름	사용자 디렉토리의 고유 이름입니다. 예: *GlobalLDAPCollector*
에이전트	목록에서 구성된 에이전트를 선택합니다

서버 IP/도메인 이름	LDAP 디렉토리 서버를 호스팅하는 서버의 IP 주소 또는 FQDN(정규화된 도메인 이름)입니다
검색 기준	LDAP 서버 검색 기반의 검색 기준을 사용하면 SVM에 있는 대로 *x.x.y.z*⇒직접 도메인 이름 형식을 모두 사용할 수 있습니다. *dc=x, dc=y, dc=z*⇒ 상대 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 엔지니어링으로 필터링하기]*CN=username,OU=engineering,DC=CompanyName,DC=NetApp,DC=com*[OU<engineering>에서 특정 사용자만 가져오려면]_CN=Acrobat,Users,CN=Users,DC=Users,DC=CompanyName=Boston,DC=CompanyName=CompanyN,DC=CompanyUS,DC=CompanyName=Users,DC=CompanyName=CompanyS,DC=CompanyName=CompanyName=CompanyName=CompanyName=CompanyName=CompanyName=CompanyName=
DN 바인딩	사용자가 디렉터리를 검색할 수 있습니다. 예: uid=ldapuser,cn=users,cn=accounts,dc=domain,dc=CompanyName,dc dorp.company.com=com uid=john,cn=users,cn=accounts,dc=dorp,dc=company,dc=com 사용자 john@dorp.company.com
계정	사용자
요한입니다	강혜린
암호를 바인딩합니다	디렉터리 서버 암호(예: Bind DN에서 사용되는 사용자 이름의 암호)
프로토콜	LDAP, LDAPS, LDAP-START-TLS
포트	포트를 선택합니다

LDAP Directory Server에서 기본 속성 이름이 수정된 경우 다음 Directory Server 필수 속성을 입력합니다. 대부분의 경우 이러한 속성 이름은 LDAP Directory Server에서 _not_modified입니다. 이 경우 기본 속성 이름을 사용하여 간단하게 진행할 수 있습니다.

속성	Directory Server의 속성 이름입니다
표시 이름	이름
UNIXID	uidNumber(uidNumber)
사용자 이름	UID

다음 특성을 추가하려면 선택적 특성 포함 을 클릭합니다.

속성	Directory Server의 속성 이름입니다
이메일 주소	메일
전화 번호	전화 번호
역할	제목

국가	CO
상태	상태
부서	부서 번호
사진	사진
관리자 DN	관리자
그룹	멤버

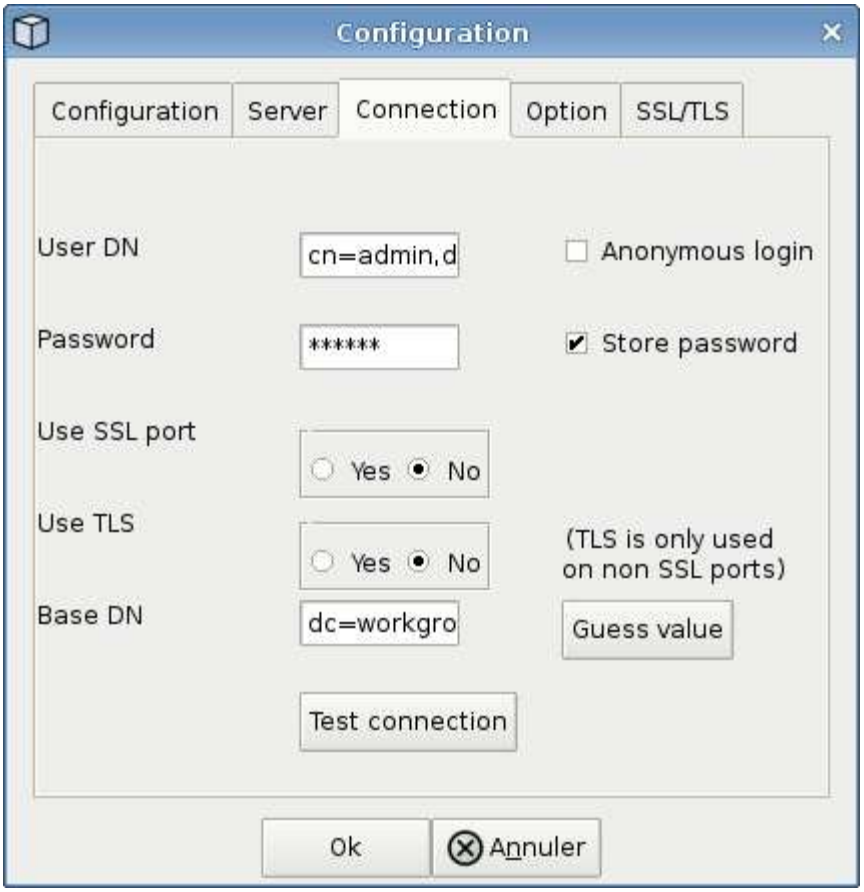
사용자 디렉토리 수집기 구성을 테스트하는 중입니다

다음 절차를 사용하여 LDAP 사용자 권한 및 속성 정의의 유효성을 검사할 수 있습니다.

- 다음 명령을 사용하여 워크로드 보안 LDAP 사용자 권한을 검증합니다.

```
 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 사용하여 LDAP 데이터베이스를 탐색하고, 개체 속성 및 속성을 보고, 권한을 보고, 개체의 스키마를 보고, 저장하고 다시 실행할 수 있는 정교한 검색을 실행할 수 있습니다.
```

  - (http://jxplorer.org/LDAP 서버에 연결할 수 있는 모든 Windows 시스템에 LDAP Explorer)(http://ldaptool.sourceforge.net/ 또는 Java LDAP 탐색기를 설치합니다.
  - LDAP 디렉토리 서버의 사용자 이름/암호를 사용하여 LDAP 서버에 연결합니다.



LDAP 디렉토리 수집기 구성 오류 문제 해결

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

문제:	해상도:
LDAP 디렉토리 커넥터를 추가하면 '오류' 상태가 됩니다. "LDAP 서버에 대해 잘못된 자격 증명이 제공되었습니다 ."라는 오류가 표시됩니다.	잘못된 바인딩 DN 또는 바인딩 비밀번호 또는 검색 기준을 제공했습니다. 올바른 정보를 편집하고 제공하십시오.
LDAP 디렉토리 커넥터를 추가하면 '오류' 상태가 됩니다. "DN=DC=HQ, DC=domainname, DC=com에 해당하는 객체를 포리스트 이름으로 가져오지 못했습니다."라는 오류가 표시됩니다.	잘못된 검색 기준을 제공했습니다. 올바른 포리스트 이름을 편집하고 제공하십시오.
도메인 사용자의 선택적 속성이 워크로드 보안 사용자 프로필 페이지에 나타나지 않습니다.	이는 CloudSecure에 추가된 선택적 속성의 이름과 Active Directory의 실제 속성 이름이 일치하지 않기 때문일 수 있습니다. 필드는 대/소문자를 구분합니다. 올바른 선택적 속성 이름을 편집하고 제공하십시오.
"LDAP 사용자를 검색하지 못했습니다. 실패 원인: 서버에 연결할 수 없습니다. 연결이 null입니다."	*Restart* 단추를 클릭하여 수집기를 다시 시작합니다.
LDAP 디렉토리 커넥터를 추가하면 '오류' 상태가 됩니다.	필수 필드(서버, 포리스트-이름, 바인드-DN, 바인드-암호)에 대해 유효한 값을 제공했는지 확인합니다. bind-DN 입력은 항상 uid=ldapuser,cn=users,cn=accounts,dc=domain,dc=companyName,dc=com으로 제공되어야 합니다.

문제:	해상도:
LDAP 디렉토리 커넥터를 추가하면 '다시 시도 중' 상태가 됩니다. "수집기의 상태를 확인하지 못하여 다시 시도하는 중" 오류가 표시됩니다.	올바른 서버 IP 및 검색 기준이 /// 제공되었는지 확인합니다
LDAP 디렉토리를 추가하는 동안 다음과 같은 오류가 표시됩니다. “2회 재시도 내에 Collector의 상태를 확인하지 못했습니다. 수집기를 다시 시작하십시오(오류 코드: AGENT008).”	올바른 서버 IP 및 검색 기준을 제공했는지 확인합니다
LDAP 디렉토리 커넥터를 추가하면 '다시 시도 중' 상태가 됩니다. "Collector의 상태를 정의할 수 없습니다. 원인 TCP 명령 [Connect(localhost:35012, None, List(), some(,seconds), true)] 오류가 java.net.ConnectionException:Connection refused 때문에 실패했습니다."	AD 서버에 대해 잘못된 IP 또는 FQDN이 제공되었습니다. 올바른 IP 주소 또는 FQDN을 편집하고 입력합니다. / / / / /
LDAP 디렉토리 커넥터를 추가하면 '오류' 상태가 됩니다. "LDAP 연결을 설정하지 못했습니다."라는 오류가 표시됩니다.	LDAP 서버에 대해 잘못된 IP 또는 FQDN이 제공되었습니다. 올바른 IP 주소 또는 FQDN을 편집하고 입력합니다. 또는 잘못된 포트 값이 제공되었습니다. LDAP 서버에 대한 기본 포트 값 또는 올바른 포트 번호를 사용해 보십시오.
LDAP 디렉토리 커넥터를 추가하면 '오류' 상태가 됩니다. "설정을 로드하지 못했습니다. 원인: DataSource 구성에 오류가 있습니다. 특정 이유: /connector/conf/application.conf: 70: ldap.ldap-port에 숫자가 아닌 유형 문자열이 있습니다."	잘못된 포트 값이 제공되었습니다. AD 서버에 대한 기본 포트 값 또는 올바른 포트 번호를 사용해 보십시오.
나는 필수 속성을 시작했는데 효과가 있었습니다. 옵션 특성 데이터를 추가한 후 선택적 특성 데이터를 AD에서 가져오지 않습니다.	이는 CloudSecure에 추가된 옵션 속성과 Active Directory의 실제 속성 이름이 일치하지 않기 때문일 수 있습니다. 올바른 필수 또는 선택적 속성 이름을 편집하고 제공하십시오.
Collector를 다시 시작한 후 LDAP 동기화는 언제 이루어집니까?	LDAP 동기화는 수집기가 다시 시작된 직후에 수행됩니다. 약 30만 명의 사용자가 있는 사용자 데이터를 가져오는 데 약 15분이 소요되며, 12시간마다 자동으로 새로 고쳐집니다.
사용자 데이터가 LDAP에서 CloudSecure로 동기화됩니다. 언제 데이터가 삭제됩니까?	새로 고침이 없는 경우 사용자 데이터는 13개월 동안 유지됩니다. 테넌트가 삭제되면 데이터가 삭제됩니다.
LDAP 디렉토리 커넥터를 사용하면 '오류' 상태가 됩니다. "커넥터가 오류 상태입니다. 서비스 이름: usersLdap. 실패 원인: LDAP 사용자를 검색하지 못했습니다. 실패 원인:80090308:LdapErr:DSID-0C090453, 설명:AcceptSecurityContext 오류, 데이터 52e, v3839"	잘못된 포리스트 이름이 제공되었습니다. 올바른 포리스트 이름을 제공하는 방법은 위의 을 참조하십시오.

문제:	해상도:
전화 번호가 사용자 프로필 페이지에 채워지지 않습니다.	이는 Active Directory의 속성 매핑 문제 때문일 수 있습니다. 1. Active Directory에서 사용자 정보를 가져오는 특정 Active Directory 수집기를 편집합니다. 2. 옵션 속성 아래에 Active Directory 속성 '전화 번호'에 매핑된 필드 이름 "전화 번호"가 있습니다. 4. 이제 위에서 설명한 대로 Active Directory 탐색기 도구를 사용하여 LDAP 디렉터리 서버를 탐색하고 올바른 속성 이름을 확인하십시오. 3. LDAP 디렉터리에는 사용자의 전화 번호가 있는 '전화 번호'라는 속성이 있는지 확인합니다. 5. LDAP 디렉토리에서 '전화 번호'로 수정되었다고 가정해 보겠습니다. 6. 그런 다음 CloudSecure 사용자 디렉토리 수집기를 편집합니다. 옵션 속성 섹션에서 '전화 번호'를 '전화 번호'로 바꿉니다. 7. Active Directory Collector를 저장하면 Collector가 다시 시작되고 사용자의 전화 번호를 가져와 사용자 프로필 페이지에 동일한 정보를 표시합니다.
AD(Active Directory) 서버에서 암호화 인증서(SSL)가 활성화된 경우 워크로드 보안 사용자 디렉토리 수집기는 AD 서버에 연결할 수 없습니다.	사용자 디렉토리 수집기를 구성하기 전에 AD 서버 암호화를 비활성화하십시오. 사용자 세부 정보를 가져오면 13개월 동안 표시됩니다. 사용자 세부 정보를 가져온 후 AD 서버의 연결이 끊기면 AD에서 새로 추가된 사용자를 가져오지 않습니다. 다시 가져오려면 사용자 디렉토리 수집기를 AD에 연결해야 합니다.

ONTAP SVM Data Collector 구성

워크로드 보안은 데이터 수집기를 사용하여 디바이스에서 파일 및 사용자 액세스 데이터를 수집합니다.

시작하기 전에

- 이 데이터 수집기는 다음 구성 요소를 통해 지원됩니다.
  - Data ONTAP 9.2 이상 버전 최상의 성능을 얻으려면 9.13.1 이상의 Data ONTAP 버전을 사용하십시오.
  - SMB 프로토콜 버전 3.1 이하
  - ONTAP 9.15.1 이상이 설치된 NFS 4.1까지의 NFS 버전
  - FlexGroup는 ONTAP 9.4 이상 버전에서 지원됩니다
  - ONTAP Select가 지원됩니다
- 데이터 유형 SVM만 지원됩니다. 무한 확장 볼륨이 있는 SVM은 지원되지 않습니다.
- SVM에는 여러 가지 하위 유형이 있습니다. 이 중 *DEFAULT*, *SYNC_SOURCE* 및 *SYNC_DESTINATION* 만 지원됩니다.
- 데이터 수집기를 구성하기 전에 Agent"구성해야 합니다"가 필요합니다.
- 올바르게 구성된 사용자 디렉토리 커넥터가 있는지 확인합니다. 그렇지 않으면 이벤트가 인코딩된 사용자 이름을 표시하고 “Activity Forensics(활동 포렌식)” 페이지에 사용자의 실제 이름(Active Directory에 저장된 이름)을 표시하지 않습니다.
- • ONTAP 영구 저장소는 9.14.1부터 지원됩니다.
- 최적의 성능을 위해 FPolicy 서버를 스토리지 시스템과 동일한 서브넷에 구성해야 합니다.

- 다음 두 가지 방법 중 하나를 사용하여 SVM을 추가해야 합니다.
  - 클러스터 IP, SVM 이름, 클러스터 관리 사용자 이름 및 암호를 사용합니다. 이 방법은 * _ 을(를) 사용하는 것이 좋습니다
    - SVM 이름은 ONTAP에 표시된 대로 대소문자를 구분합니다.
  - SVM Vserver 관리 IP, 사용자 이름 및 암호를 사용합니다
  - 전체 관리자 클러스터/SVM 관리 사용자 이름 및 암호를 사용할 수 없거나 사용할 의향이 없는 경우 아래 섹션에서 설명한 것처럼 더 작은 Privileges로 사용자 지정 사용자를 생성할 수 "권한에 대한 참고 사항 "있습니다. 이 맞춤형 사용자는 SVM 또는 클러스터 액세스를 위해 생성할 수 있습니다.
    - o 아래 "권한에 대한 참고 사항" 섹션에서 언급한 csrole 이상의 권한이 있는 역할을 가진 AD 사용자를 사용할 수도 있습니다. 도 "ONTAP 설명서"참조하십시오.
- 다음 명령을 실행하여 SVM에 올바른 애플리케이션이 설정되었는지 확인합니다.

```
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 확인합니다. clustershell:> `vserver cifs show`

  SVM 이름, CIFS 서버 이름 및 추가 필드가 반환됩니다.

- SVM vsadmin 사용자의 암호를 설정합니다. 사용자 지정 사용자 또는 클러스터 관리자를 사용하는 경우 이 단계를 건너뜁니다. clustershell:> `security login password -username vsadmin -vserver svmname`
- 외부 액세스를 위해 SVM vsadmin 사용자의 잠금을 해제합니다. 사용자 지정 사용자 또는 클러스터 관리자를 사용하는 경우 이 단계를 건너뜁니다. clustershell:> `security login unlock -username vsadmin -vserver svmname`
- 데이터 LIF의 방화벽 정책이 'GMT'(이하 '데이터')로 설정되어 있는지 확인합니다. 전용 관리 lif를 사용하여 SVM.clustershell::> 을 추가하는 경우 이 단계를 건너뜁니다 `network interface modify -lif <SVM_data_LIF_name> -firewall-policy mgmt`
- 방화벽이 활성화된 경우 Data ONTAP 데이터 수집기를 사용하여 포트에 대한 TCP 트래픽을 허용하도록 정의된 예외가 있어야 합니다.

  구성 정보는 을 "상담원 요구 사항"참조하십시오. 이는 클라우드에 설치된 온프레미스 에이전트 및 에이전트에 적용됩니다.

- Cloud ONTAP SVM을 모니터링하기 위해 AWS EC2 인스턴스에 에이전트를 설치한 경우 에이전트와 스토리지는 동일한 VPC에 있어야 합니다. 개별 VPC에 있는 경우 VPC 간에 유효한 경로가 있어야 합니다.

사용자 액세스 차단을 위한 필수 조건

다음 사항에 유의하십시오."사용자 액세스 차단"

이 기능을 사용하려면 클러스터 레벨 자격 증명이 필요합니다.

클러스터 관리 자격 증명을 사용하는 경우 새 권한이 필요하지 않습니다.

사용자에게 부여된 권한으로 사용자 지정 사용자(예: *CsUser*)를 사용하는 경우 아래 단계에 따라 사용자를 차단하는 워크로드 보안에 권한을 부여합니다.

클러스터 자격 증명이 있는 CsUser의 경우 ONTAP 명령줄에서 다음을 수행하십시오.

```
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
```

사용 권한에 대한 참고 사항

클러스터 관리 **IP** * 를 통해 추가할 때의 권한:

클러스터 관리 관리자 사용자를 사용하여 워크로드 보안이 ONTAP SVM 데이터 수집기에 액세스할 수 없는 경우 아래 명령에 나와 있는 역할을 사용하여 "CsUser"라는 새 사용자를 생성할 수 있습니다. 클러스터 관리 IP를 사용하도록 워크로드 보안 데이터 수집기를 구성할 때 "CsUser"의 사용자 이름 "CsUser"와 암호를 사용합니다.

새 사용자를 생성하려면 클러스터 관리 관리자 사용자 이름/암호를 사용하여 ONTAP에 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 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
```

vVserver 관리 **IP *** 를 통해 추가할 때의 권한**:**

클러스터 관리 관리자 사용자를 사용하여 워크로드 보안이 ONTAP SVM 데이터 수집기에 액세스할 수 없는 경우 아래 명령에 나와 있는 역할을 사용하여 "CsUser"라는 새 사용자를 생성할 수 있습니다. 워크로드 보안 데이터 수집기에서 SVM 관리 IP를 사용하도록 구성할 때 "CsUser"의 사용자 이름 "CsUser"와 암호를 사용합니다.

새 사용자를 생성하려면 클러스터 관리 관리자 사용자 이름/암호를 사용하여 ONTAP에 로그인하고 ONTAP 서버에서 다음 명령을 실행합니다. 쉽게 사용할 수 있도록 이러한 명령을 텍스트 편집기에 복사하고 ONTAP에서 다음 명령을 실행하기 전에 <vservername>을(를) SVM 이름으로 바꾸십시오.

```
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>
```

Protobuf 모드

이 옵션이 Collector의 _Advanced Configuration_settings에서 활성화되면 워크로드 보안은 FPolicy 엔진을 protebuf 모드로 구성합니다. Protobuf 모드는 ONTAP 버전 9.15 이상에서 지원됩니다.

이 기능에 대한 자세한 내용은 을 "ONTAP 설명서"참조하십시오.

protbuf에 대한 특정 권한이 필요합니다(일부 또는 전부가 이미 있을 수 있음).

클러스터 모드:

```
security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <cluster_name>
security login create -user-or-group-name csuser -application http
-authmethod password -role csrestrole
```

SVM 모드:

```
security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <svm_name>
security login create -user-or-group-name csuser -application http
-authmethod password -role csrestrole -vserver <svm_name>
```

ONTAP 자율적 랜섬웨어 방어 및 **ONTAP** 액세스에 대한 권한이 거부되었습니다

클러스터 관리 자격 증명을 사용하는 경우 새 권한이 필요하지 않습니다.

사용자에게 부여된 권한으로 사용자 지정 사용자(예: *CsUser*)를 사용하는 경우, 아래 단계를 따라 워크로드 보안에 권한을 부여하여 ONTAP에서 ARP 관련 정보를 수집합니다.

자세한 내용은 정보 를 참조하십시오 "ONTAP 액세스와의 통합이 거부되었습니다"

및 "ONTAP Autonomous 랜섬웨어 Protection과 통합"

데이터 수집기를 구성합니다

구성 단계

1. Data Infrastructure Insights 환경에 관리자 또는 계정 소유자로 로그인합니다.
2. Workload Security > Collector > + Data Collector * 를 클릭합니다

   사용 가능한 데이터 Collector가 표시됩니다.

3. NetApp SVM 타일 위로 마우스를 가져가 * + Monitor * 를 클릭합니다.

   ONTAP SVM 구성 페이지가 표시됩니다. 각 필드에 필요한 데이터를 입력합니다.

필드에 입력합니다	설명
이름	Data Collector의 고유 이름입니다
에이전트	목록에서 구성된 에이전트를 선택합니다.
관리 IP를 통해 연결 대상:	클러스터 IP 또는 SVM 관리 IP를 선택합니다
클러스터/SVM 관리 IP 주소	위에서 선택한 항목에 따라 클러스터 또는 SVM의 IP 주소입니다.
SVM 이름	SVM 이름(클러스터 IP를 통해 연결할 때 이 필드 필요)
사용자 이름	클러스터 IP를 통해 추가할 때 SVM/클러스터에 액세스하는 사용자 이름 옵션은 1입니다. 클러스터 관리 2. 'CsUser' 3. CsUser와 유사한 역할을 가진 AD 사용자. SVM IP를 통해 추가할 때 옵션은 4.vsadmin 5입니다. 'CsUser' 6. CsUser와 유사한 역할을 하는 AD-사용자 이름입니다.
암호	위의 사용자 이름에 대한 암호입니다
공유/볼륨 필터링	이벤트 컬렉션에서 공유/볼륨을 포함할지 또는 제외할지 여부를 선택합니다
제외/포함할 전체 공유 이름을 입력합니다	이벤트 컬렉션에서 제외하거나 포함할(적절한 경우) 공유의 쉼표로 구분된 목록입니다
제외/포함할 전체 볼륨 이름을 입력합니다	이벤트 컬렉션에서 제외하거나 포함할(적절한 경우) 쉼표로 구분된 볼륨 목록입니다

폴더 액세스를 모니터링합니다	이 옵션을 선택하면 폴더 액세스 모니터링에 대한 이벤트가 활성화됩니다. 이 옵션을 선택하지 않아도 폴더 생성/이름 변경 및 삭제가 모니터링됩니다. 이 기능을 활성화하면 모니터링되는 이벤트 수가 증가합니다.
ONTAP 전송 버퍼 크기를 설정합니다	ONTAP Fpolicy 전송 버퍼 크기를 설정합니다. 9.8p7 이전의 ONTAP 버전을 사용하고 성능 문제가 발생하면 ONTAP 전송 버퍼 크기를 변경하여 ONTAP 성능을 향상시킬 수 있습니다. 이 옵션이 표시되지 않고 탐색 중인 경우 NetApp 지원에 문의하십시오.

작업을 마친 후

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

MetroCluster의 권장 구성

다음은 MetroCluster에 권장됩니다.

1. 데이터 수집기 2개를 소스 SVM에 연결하고 다른 데이터 수집기를 타겟 SVM에 연결합니다.
2. 데이터 수집기는 _Cluster IP_로 연결해야 합니다.
3. 언제든지 한 데이터 수집기가 실행 중이어야 하며, 다른 데이터 수집기는 오류가 발생합니다.

   현재 '실행 중인' SVM의 데이터 수집기는 _ running _ 으로 표시됩니다. 현재 '가장 위에 있는' SVM의 데이터 수집기는 _Error_로 표시됩니다.

4. 전환이 있을 때마다 데이터 수집기의 상태가 '실행 중'에서 '오류'로, 또는 그 반대로 변경됩니다.
5. 데이터 수집기가 오류 상태에서 실행 상태로 이동하는 데 최대 2분이 걸립니다.

서비스 정책

ONTAP* 버전 9.9.1 이상 * 과 함께 서비스 정책을 사용하는 경우 데이터 소스 수집기에 연결하려면 *data-FPolicy-client_service*가 *data service_data-nfs* 및 /or_data-cifs_와 함께 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)
```

9.9.1 이전의 ONTAP 버전에서는 _data-FPolicy-client_를 설정할 필요가 없습니다.

데이터 수집기 재생 **-** 일시 중지

이제 컬렉터의 kebab 메뉴에 2개의 새 작업이 표시됩니다(일시 중지 및 다시 시작).

Data Collector가 _running_state인 경우 수집을 일시 중지할 수 있습니다. 수집기에 대한 "세 개의 점" 메뉴를 열고 일시 중지를 선택합니다. Collector가 일시 중지되는 동안 ONTAP에서 수집된 데이터는 없고 Collector에서 ONTAP로

전송되는 데이터는 없습니다. 즉, Fpolicy 이벤트가 ONTAP에서 데이터 수집기로, 그리고 그 안에서 데이터 인프라 Insights로 이동하지 않습니다.

Collector가 일시 중지된 동안 ONTAP에 새 볼륨 등이 생성되면 워크로드 보안이 데이터를 수집하지 않고 해당 볼륨 등이 대시보드나 테이블에 반영되지 않습니다.

다음 사항에 유의하십시오.

- 일시 중지된 수집기에 구성된 설정에 따라 스냅샷 삭제가 수행되지 않습니다.
- ONTAP ARP와 같은 EMS 이벤트는 일시 중지된 Collector에서 처리되지 않습니다. 즉, ONTAP에서 랜섬웨어 공격을 식별하면 Data Infrastructure Insights 워크로드 보안이 해당 이벤트를 파악할 수 없습니다.
- 일시 중지된 수집기에 대해 상태 알림 이메일이 전송되지 않습니다.
- 수동 또는 자동 작업(예: 스냅샷 또는 사용자 차단)은 일시 중지된 수집기에서 지원되지 않습니다.
- 에이전트 또는 수집기 업그레이드, 에이전트 VM 다시 시작/재부팅 또는 에이전트 서비스 다시 시작 시 일시 중지된 수집기는 _Paused_state에 남아 있습니다.
- 데이터 수집기가 _Error_state 인 경우 수집기를 _Paused_state 로 변경할 수 없습니다. 일시 중지 버튼은 수집기의 상태가 _running_인 경우에만 활성화됩니다.
- 에이전트의 연결이 끊어진 경우 수집기를 _Paused_state 로 변경할 수 없습니다. Collector가 _stopped_state로 이동하고 Pause 버튼이 비활성화됩니다.

영구 저장

영구 저장소는 ONTAP 9.14.1 이상에서 지원됩니다. 볼륨 이름 지침은 ONTAP 9.14부터 9.15까지 다양합니다.

영구 저장소는 수집기 편집/추가 페이지에서 확인란을 선택하여 활성화할 수 있습니다. 이 확인란을 선택하면 볼륨 이름을 수락할 수 있는 텍스트 필드가 표시됩니다. 볼륨 이름은 영구 저장을 활성화하기 위한 필수 필드입니다.

- ONTAP 9.14.1의 경우 기능을 활성화하기 전에 볼륨을 생성하고 *Volume Name* 필드에 동일한 이름을 제공해야 합니다. 권장 볼륨 크기는 16GB입니다.
- ONTAP 9.15.1의 경우 수집기에서 *Volume Name* 필드에 제공된 이름을 사용하여 16GB 크기로 볼륨이 자동으로 생성됩니다.

영구 저장소에 대한 특정 권한이 필요합니다(일부 또는 모두 이미 존재할 수 있음).

클러스터 모드:

```
security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <cluster-name>
security login rest-role create -role csrestrole -api /api/cluster/jobs/
-access readonly -vserver <cluster-name>
```

SVM 모드:

```
security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <vserver-name>
security login rest-role create -role csrestrole -api /api/cluster/jobs/
-access readonly -vserver <vserver-name>
```

문제 해결

"SVM Collector 문제 해결"문제 해결 정보는 페이지를 참조하십시오.

NetApp ONTAP Collector용 Cloud Volumes ONTAP 및 Amazon FSx 구성

워크로드 보안은 데이터 수집기를 사용하여 디바이스에서 파일 및 사용자 액세스 데이터를 수집합니다.

Cloud Volumes ONTAP 스토리지 구성

워크로드 보안 에이전트를 호스팅하도록 단일 노드/HA AWS 인스턴스를 구성하려면 OnCommand Cloud Volumes ONTAP 설명서를 참조하십시오. https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/index.html

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

지원되는 플랫폼

- Cloud Volumes ONTAP - 사용 가능한 모든 클라우드 서비스 공급자에서 지원됩니다. 예: Amazon, Azure, Google Cloud
- ONTAP 아마존 FSx

에이전트 시스템 구성

에이전트 시스템은 클라우드 서비스 공급자의 각 서브넷에 구성되어야 합니다. [Agent Requirements] 에서 네트워크 액세스에 대해 자세히 알아보십시오.

다음은 AWS에서 Agent를 설치하는 단계입니다. 클라우드 서비스 공급자에 적용되는 것과 동일한 단계를 Azure 또는 Google Cloud에서 설치를 위해 수행할 수 있습니다.

AWS에서 다음 단계를 수행하여 워크로드 보안 에이전트로 사용할 시스템을 구성합니다.

다음 단계를 수행하여 워크로드 보안 에이전트로 사용할 시스템을 구성합니다.

단계

1. AWS 콘솔에 로그인하고 EC2-Instances 페이지로 이동한 후 _Launch instance_를 선택합니다.
2. 이 페이지에서 설명한 대로 적절한 버전의 RHEL 또는 CentOS AMI를 선택합니다. https://docs.netapp.com/us-en/cloudinsights/concept_cs_agent_requirements.html
3. Cloud ONTAP 인스턴스가 상주하는 VPC 및 서브넷을 선택합니다.
4. 할당된 리소스로 *T2.xLarge*(vCPU 4개 및 16GB RAM)를 선택합니다.

a. EC2 인스턴스를 만듭니다.

5. YUM 패키지 관리자를 사용하여 필요한 Linux 패키지를 설치합니다.

a. install_wget_and_unzip_native Linux 패키지를 설치합니다.

워크로드 보안 에이전트를 설치합니다

1. Data Infrastructure Insights 환경에 관리자 또는 계정 소유자로 로그인합니다.
2. Workload Security * Collector * 로 이동한 후 * Agents * 탭을 클릭합니다.
3. * + Agent * 를 클릭하고 RHEL을 대상 플랫폼으로 지정합니다.
4. Agent 설치 명령을 복사합니다.
5. 로그인한 RHEL EC2 인스턴스에 Agent Installation 명령을 붙여 넣습니다. 그러면 워크로드 보안 에이전트가 설치되고 모든 가 "상담원 필수 구성 요소"충족됩니다.

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

문제 해결

알려진 문제와 해결 방법은 다음 표에 설명되어 있습니다.

문제	해상도
"워크로드 보안: Amazon FxSN 데이터 수집기에 대한 ONTAP 유형을 확인하지 못했습니다." 오류가 데이터 수집기에 표시됩니다. 고객은 새로운 Amazon FSxN 데이터 수집기를 워크로드 보안에 추가할 수 없습니다. 에이전트에서 포트 443의 FSxN 클러스터에 대한 연결이 시간 초과입니다. 방화벽 및 AWS 보안 그룹에는 통신을 허용하는 데 필요한 규칙이 활성화되어 있습니다. 에이전트가 이미 구축되어 있으며 동일한 AWS 계정에도 있습니다. 이 동일한 에이전트를 사용하여 나머지 NetApp 장치를 연결 및 모니터링합니다(모두 작동).	fsxadmin LIF 네트워크 세그먼트를 에이전트의 보안 규칙에 추가하여 이 문제를 해결합니다. 포트가 확실하지 않은 경우 모든 포트가 허용됩니다.

사용자 관리

워크로드 보안 사용자 계정은 Data Infrastructure Insights를 통해 관리됩니다.

Data Infrastructure Insights는 계정 소유자, 관리자, 사용자 및 게스트의 4가지 사용자 계정 수준을 제공합니다. 각 계정에는 특정 권한 수준이 할당됩니다. 관리자 권한이 있는 사용자 계정은 사용자를 생성 또는 수정하고 각 사용자에게 다음 워크로드 보안 역할 중 하나를 할당할 수 있습니다.

역할	워크로드 보안 액세스
관리자	알림, Forensics, 데이터 수집기, 자동화된 응답 정책 및 워크로드 보안을 위한 API를 비롯한 모든 워크로드 보안 기능을 수행할 수 있습니다. 관리자는 다른 사용자를 초대할 수도 있지만 워크로드 보안 역할만 할당할 수 있습니다.

사용자	알림을 확인 및 관리하고 Forensics를 볼 수 있습니다. 사용자 역할은 알림 상태를 변경하고, 메모를 추가하고, 스냅샷을 수동으로 생성하고, 사용자 액세스를 제한할 수 있습니다.
게스트	알림 및 Forensics를 볼 수 있습니다. 게스트 역할은 알림 상태를 변경하거나, 메모를 추가하거나, 스냅샷을 수동으로 생성하거나, 사용자 액세스를 제한할 수 없습니다.

단계

1. 워크로드 보안에 로그인합니다
2. 메뉴에서 * Admin > User Management * 를 클릭합니다

   Data Infrastructure Insights의 사용자 관리 페이지로 전달됩니다.

3. 각 사용자에 대해 원하는 역할을 선택합니다.

새 사용자를 추가하는 동안 원하는 역할(일반적으로 사용자 또는 게스트)을 선택하기만 하면 됩니다.

사용자 계정 및 역할에 대한 자세한 내용은 Data Infrastructure Insights "사용자 역할" 설명서를 참조하십시오.

SVM Event Rate Checker(에이전트 크기 지정 가이드)

이벤트 속도 검사기는 ONTAP SVM 데이터 수집기를 설치하기 전에 SVM에서 NFS/SMB의 결합된 이벤트 속도를 확인하여 에이전트 시스템 한 대를 모니터링할 수 있는 SVM의 수를 확인하는 데 사용됩니다. 이벤트 속도 검사기를 크기 조정 가이드로 사용하여 보안 환경을 계획할 수 있습니다.

Agent는 최대 50개의 데이터 수집기를 지원할 수 있습니다.

요구 사항:

- 클러스터 IP입니다
- 클러스터 관리자 사용자 이름 및 암호입니다

이 스크립트를 실행할 때 이벤트 속도를 확인할 SVM을 위해 ONTAP SVM Data Collector를 실행해야 합니다.

단계:

1. CloudSecure의 지침에 따라 Agent를 설치합니다.
2. 에이전트가 설치되면 sudo 사용자로 _server_data_rate_checker.sh_script를 실행합니다.

```
 /opt/netapp/cloudsecure/agent/install/svm_event_rate_checker.sh
. 이 스크립트를 사용하려면 Linux 시스템에 _sshpass_를 설치해야 합니다. 두 가지 방법으로 설치할 수 있습니다.
```

a. 다음 명령을 실행합니다.

```
 linux_prompt> yum install sshpass
.. 그렇지 않으면 웹에서 Linux 시스템으로 _sshpass_를 다운로드하고 다음 명령을 실행합니다.
```

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

3. 메시지가 표시되면 올바른 값을 입력합니다. 예를 보려면 아래를 참조하십시오.
4. 스크립트는 약 5분 정도 소요됩니다.
5. 실행이 완료되면 스크립트가 SVM의 이벤트 속도를 인쇄합니다. 콘솔 출력에서 SVM당 이벤트 속도를 확인할 수 있습니다.

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

각 ONTAP SVM Data Collector를 단일 SVM과 연결할 수 있습니다. 즉, 각 데이터 수집기에서 단일 SVM에서 생성되는 이벤트 수를 받을 수 있습니다.

다음 사항에 유의하십시오.

a) 이 표를 일반 사이징 가이드로 사용합니다. 코어 및/또는 메모리의 수를 늘려 지원되는 데이터 수집기 수를 최대 50개까지 늘릴 수 있습니다.

에이전트 시스템 구성	SVM 데이터 수집기 수	Agent Machine이 처리할 수 있는 최대 이벤트 속도
4코어, 16GB	10개의 데이터 수집기	초당 20,000개의 이벤트
4코어, 32GB	20개의 데이터 수집기	초당 20,000개의 이벤트

b) 총 이벤트를 계산하려면 해당 에이전트에 대해 생성된 모든 SVM에 대해 생성된 이벤트를 추가합니다.

c) 피크 시간 동안 스크립트가 실행되지 않거나 피크 트래픽을 예측하기 어려운 경우 이벤트 속도 버퍼를 30%로 유지합니다.

B+C는 A보다 작아야 합니다. 그렇지 않으면 Agent 시스템이 모니터링하지 못합니다.

즉, 단일 에이전트 시스템에 추가할 수 있는 데이터 수집기의 수는 아래 공식을 준수해야 합니다.

```
 Sum of all Event rate of all Data Source Collectors + Buffer Event rate
of 30% < 20000 events/second
xref:{relative_path}concept_cs_agent_requirements.html["상담원 요구 사항"]추가 필수 구성 요소 및 요구 사항은 페이지를 참조하십시오.
```

예

SVM이 각각 100개, 200개, 300개의 이벤트를 생성한다고 가정해 보겠습니다.

다음 수식을 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 파일 이름 *FPolicy_stat_<SVM* 이름>*.log*에서 Agent 시스템에서 사용할 수 있습니다.

스크립트는 다음과 같은 경우에 잘못된 결과를 제공할 수 있습니다.

- 잘못된 자격 증명, IP 또는 SVM 이름이 제공됩니다.
- 이름, 시퀀스 번호 등이 동일한 기존 FPolicy에서 오류가 발생합니다.
- 실행 중에 스크립트가 갑자기 중지됩니다.

스크립트 실행의 예는 다음과 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
```

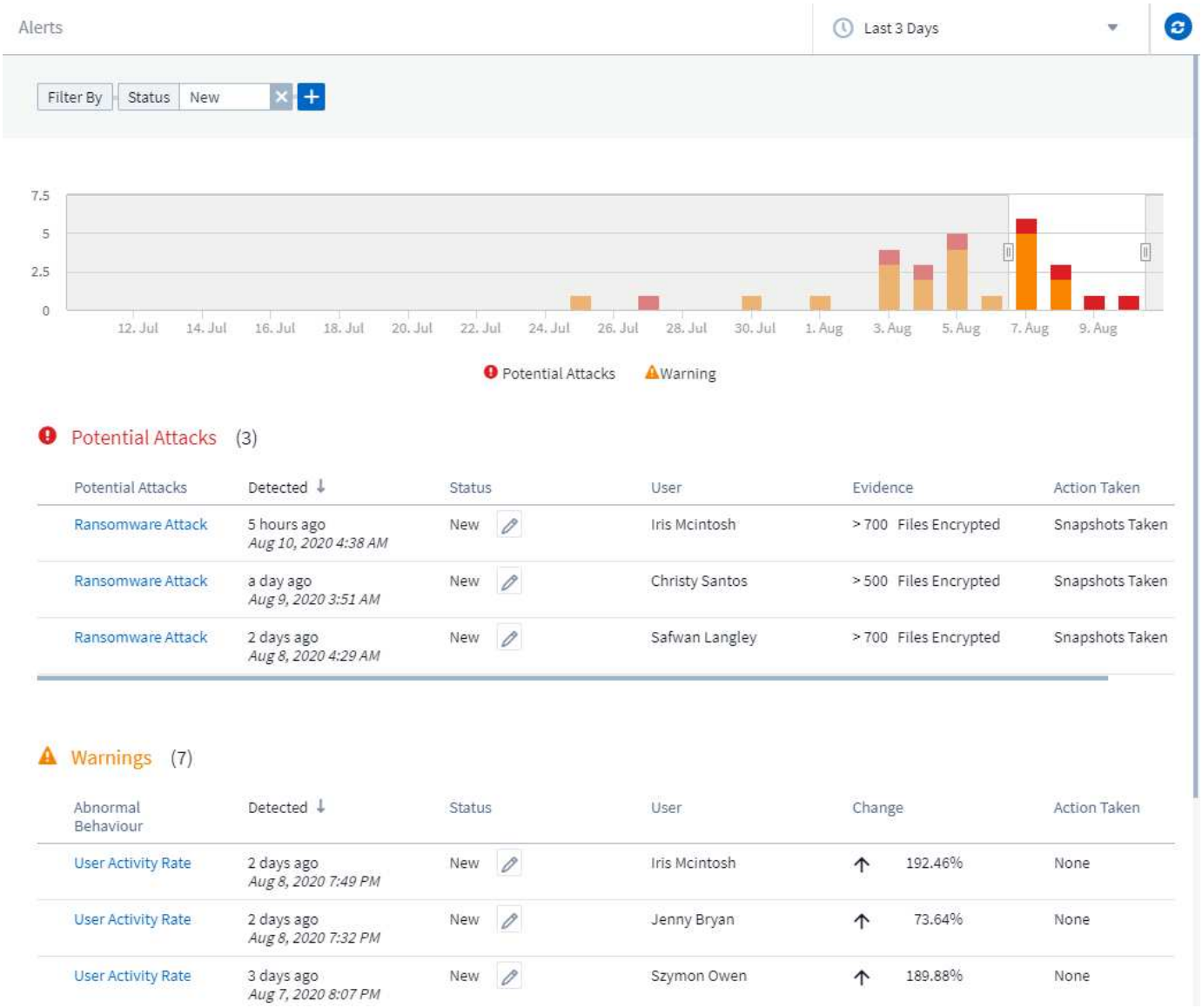
```
[root@ci-cs-data agent]#
```

문제 해결

질문	답변
워크로드 보안용으로 이미 구성된 SVM에서 이 스크립트를 실행하면 SVM에서 기존 FPolicy 구성을 사용하기만 합니까, 아니면 임시 FPolicy 구성을 사용하여 프로세스를 실행합니까?	워크로드 보안용으로 이미 구성된 SVM에 대해서도 이벤트 속도 검사기를 실행할 수 있습니다. 아무런 영향도 미치지 않아야 합니다.
스크립트를 실행할 수 있는 SVM의 수를 늘릴 수 있습니까?	예. 스크립트를 편집하고 SVM의 최대 수를 5개에서 원하는 수로 변경하면 됩니다.
SVM 수를 늘릴 경우 스크립트 실행 시간이 늘어집니까?	아니오. SVM 수가 늘어난 경우에도 스크립트는 최대 5분 동안 실행됩니다.
스크립트를 실행할 수 있는 SVM의 수를 늘릴 수 있습니까?	예. 스크립트를 편집하고 SVM의 최대 수를 5개에서 원하는 수로 변경해야 합니다.
SVM 수를 늘릴 경우 스크립트 실행 시간이 늘어집니까?	아니오. 이 스크립트는 SVM 수가 증가하더라도 최대 5분 동안 실행됩니다.
기존 에이전트에서 이벤트 속도 검사기를 실행하면 어떻게 됩니까?	이미 있는 에이전트에 대해 이벤트 속도 검사기를 실행하면 SVM에서 지연 시간이 증가할 수 있습니다. 이 증가율은 기본적으로 이벤트 속도 검사기가 실행되는 동안 일시적으로 발생합니다.

경고

워크로드 보안 경고 페이지에는 최근 공격 및/또는 경고의 타임라인이 표시되며 각 문제에 대한 세부 정보를 볼 수 있습니다.



경고

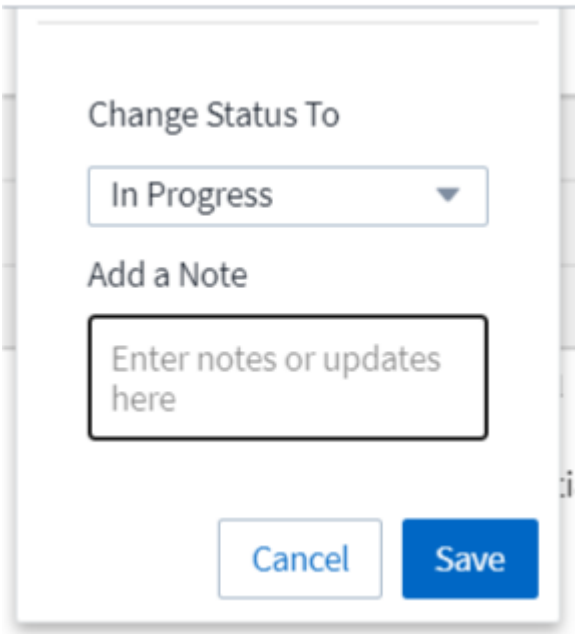
경고 목록에는 선택한 시간 범위에서 발생한 잠재적 공격 및/또는 경고의 총 수와 해당 시간 범위에서 발생한 공격 및/또는 경고 목록이 표시된 그래프가 표시됩니다. 그래프에서 시작 시간 및 종료 시간 슬라이더를 조정하여 시간 범위를 변경할 수 있습니다.

각 경고에 대해 다음이 표시됩니다.

- 잠재적 공격: *
- The_potential attack_type(예: 랜섬웨어 또는 태업)
- 잠재적 공격이 _ 탐지된 날짜 및 시간입니다 _

- 알림의 _ 상태 _:
  - * New * (새로 만들기 *): 새 경고의 기본값입니다.
  - * 진행 중 *: 팀 구성원 또는 구성원이 알림을 조사 중입니다.
  - * 해결됨 *: 팀 구성원이 경고를 해결됨으로 표시했습니다.
  - * 해제됨 *: 경고가 거짓 긍정 또는 예상된 동작으로 무시되었습니다.

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



- 동작을 통해 경고가 트리거된 _User_입니다
- _evidence_of the attack(예: 많은 수의 파일이 암호화됨)
- 수행된 조치 _ (예: 스냅샷이 촬영됨)
- 경고: *
- 경고를 트리거한 _ 비정상적인 동작 _
- 동작이 _detected_인 날짜 및 시간입니다
- 알림의 *Status*(신규, 진행 중 등)
- 동작을 통해 경고가 트리거된 _User_입니다
- Change _ 에 대한 설명(예: 파일 액세스의 비정상적인 증가)
- 조치 _

필터 옵션

경고를 필터링하는 방법은 다음과 같습니다.

- 알림의 _ 상태 _
- Note_의 특정 텍스트입니다

- 공격 유형/경고 _
- 작업이 경고/경고를 트리거한 _User_입니다

경고 세부 정보 페이지

경고 목록 페이지에서 경고 링크를 클릭하여 경고에 대한 세부 정보 페이지를 열 수 있습니다. 경고 세부 정보는 공격 유형 또는 경고 유형에 따라 다를 수 있습니다. 예를 들어, 랜섬웨어 공격 세부 정보 페이지에 다음 정보가 표시될 수 있습니다.

요약 섹션:

- 공격 유형(랜섬웨어, 태업) 및 경고 ID(워크로드 보안에서 할당)
- 공격이 감지된 날짜 및 시간입니다
- 작업이 수행됨(예: 자동 스냅샷이 작성됨) 스냅샷 시간은 요약 섹션 바로 아래에 표시됩니다.)
- 상태(신규, 진행 중 등)

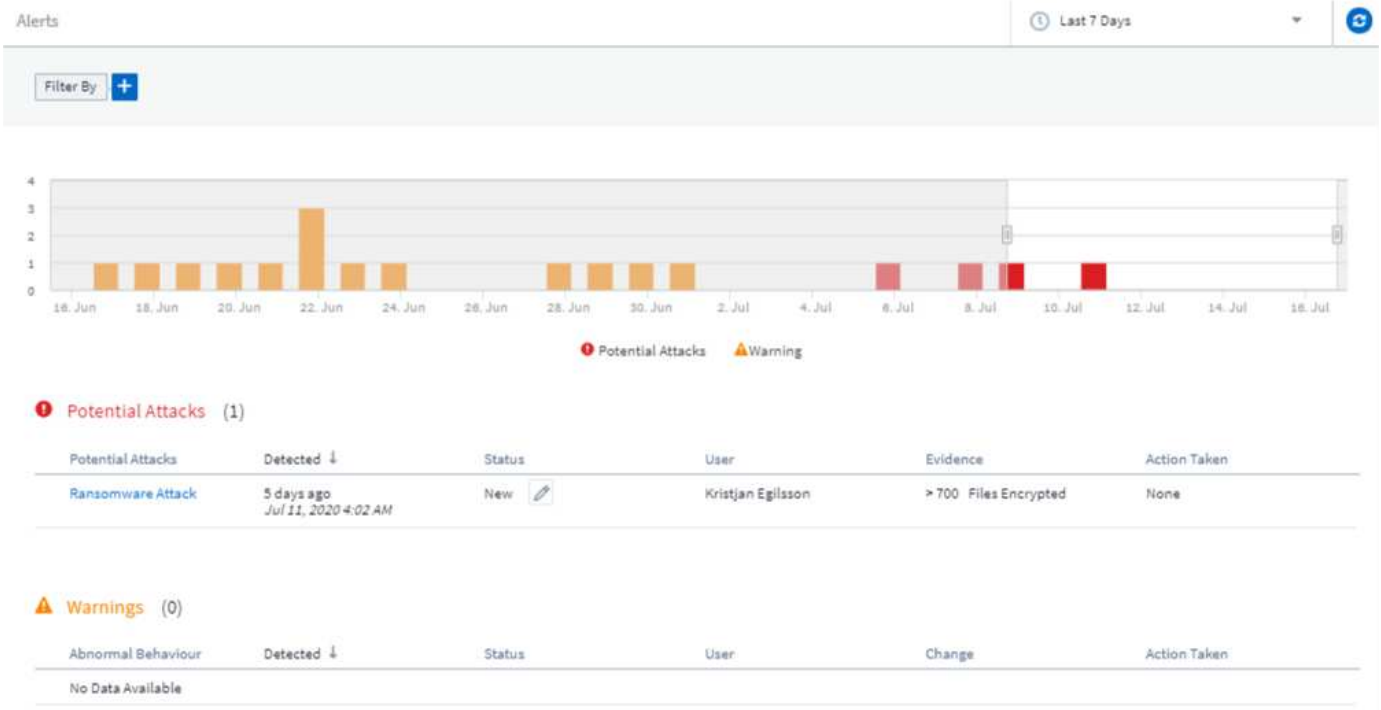
공격 결과 섹션:

- 영향을 받는 볼륨 및 파일 수
- 감지에 대한 관련 요약
- 공격 중 파일 작업을 보여주는 그래프입니다

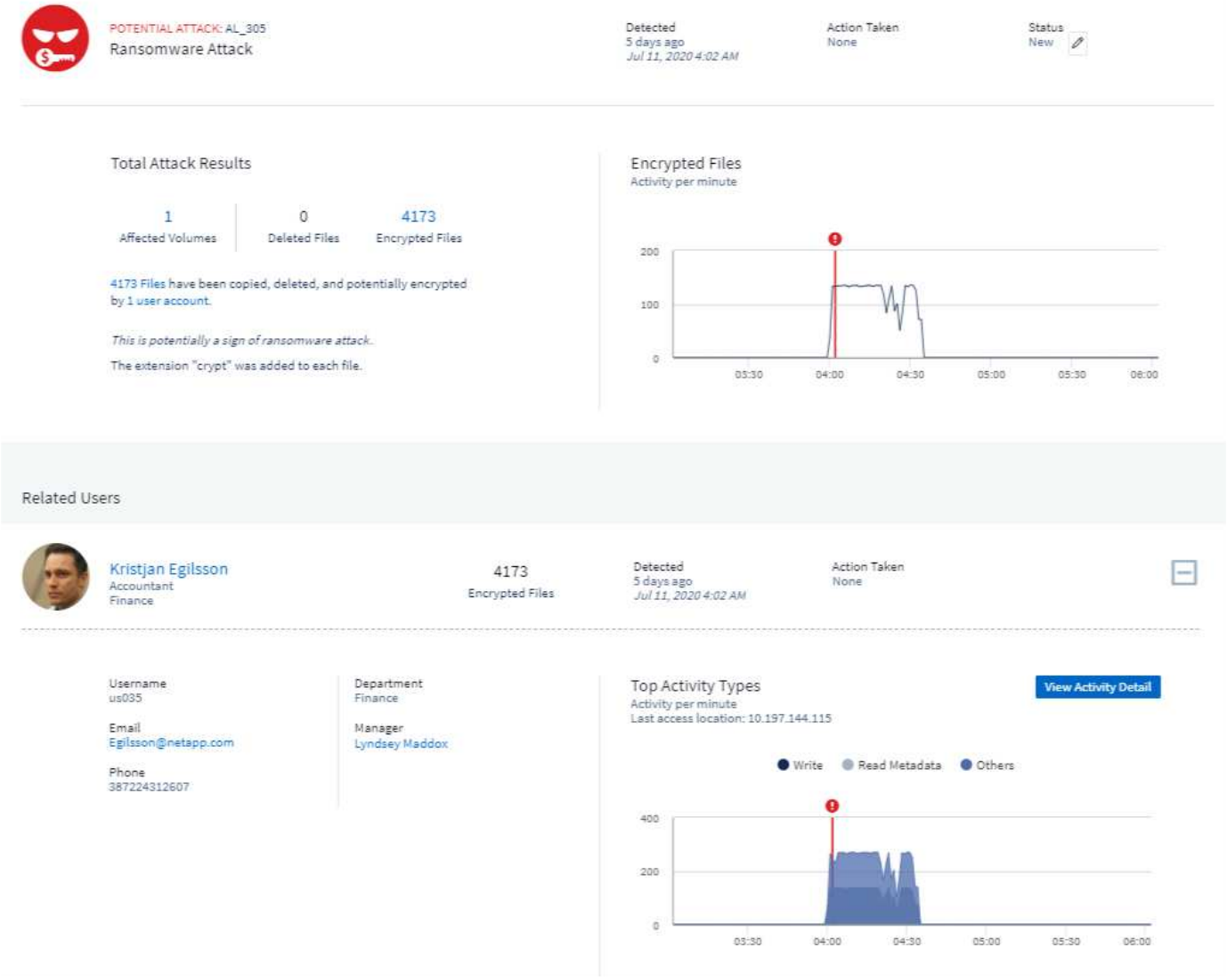
관련 사용자 섹션:

이 섹션에서는 잠재적 공격에 관련된 사용자에 대한 상세 정보를 보여 주며, 여기에는 사용자의 상위 활동 그래프가 포함됩니다.

알림 페이지(이 예제는 잠재적 랜섬웨어 공격을 보여줍니다.):



세부 페이지 (이 예제는 잠재적 랜섬웨어 공격을 보여줍니다.):

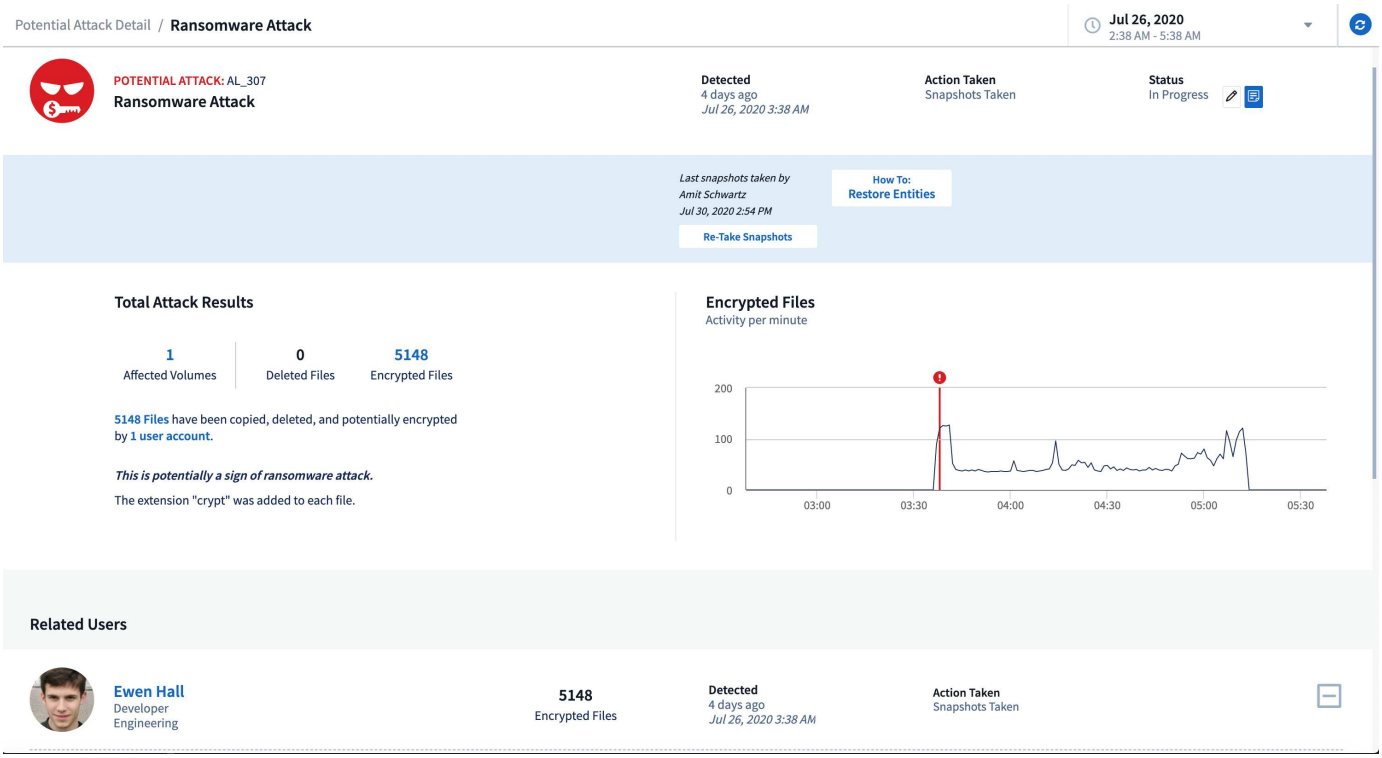


_스냅샷 작업 수행

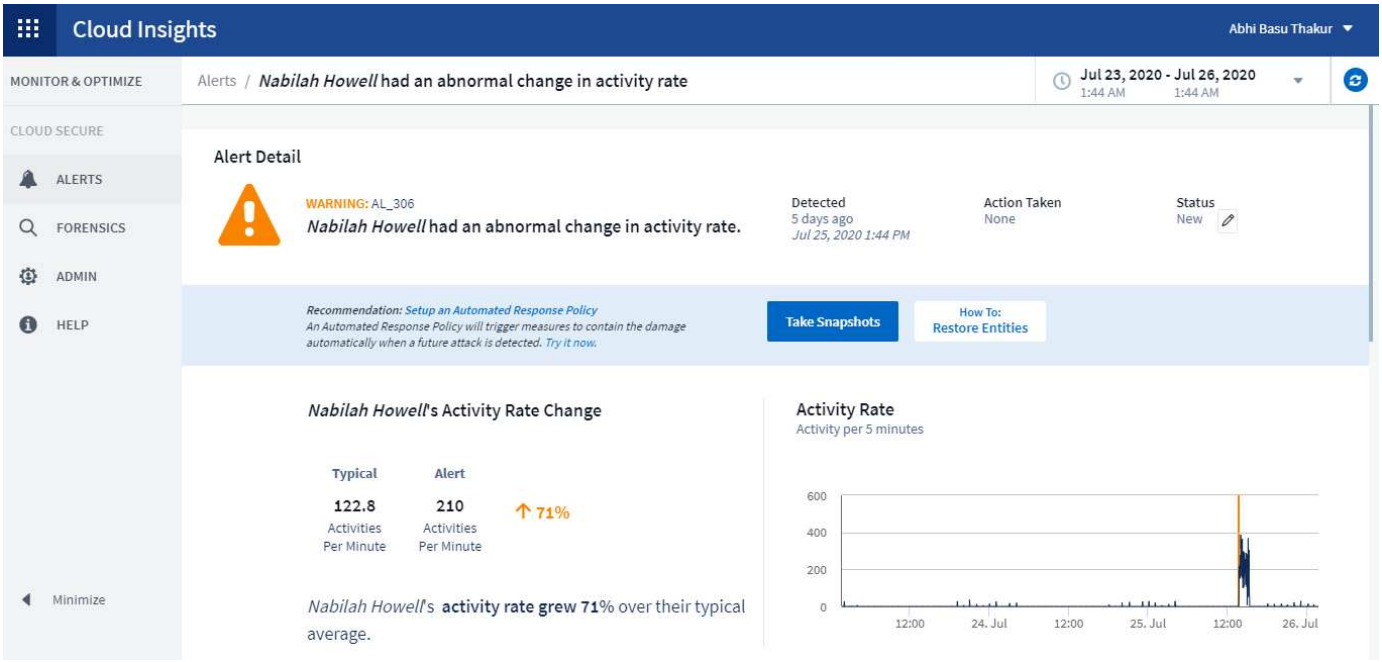
워크로드 보안은 악의적인 활동이 감지되면 스냅샷을 자동으로 생성하여 데이터를 보호하고 데이터가 안전하게 백업되도록 합니다.

랜섬웨어 공격 또는 기타 비정상적인 사용자 활동이 감지될 때 스냅샷을 생성하도록 정의할 수 "자동화된 응답 정책 "있습니다. 알림 페이지에서 수동으로 스냅샷을 생성할 수도 있습니다.

자동 스냅샷 생성됨:



수동 스냅샷:



경고 알림

알림의 전자 메일 알림은 알림의 모든 작업에 대해 알림 받는 사람 목록으로 전송됩니다. 알림 수신자를 구성하려면 * Admin > Notifications * 를 클릭하고 각 수신자의 이메일 주소를 입력합니다.

보존 정책

경고 및 경고는 13개월 동안 유지됩니다. 13개월 이전의 경고 및 경고가 삭제됩니다. 워크로드 보안 환경이 삭제된 경우 환경과 관련된 모든 데이터도 삭제됩니다.

문제 해결

문제:	다음을 시도해 보십시오.
ONTAP에서 매일 매시간 스냅샷을 생성하는 경우가 있습니다. WS(Workload Security) 스냅샷이 영향을 줍니까? WS 스냅샷은 시간별 스냅샷 위치를 차지합니까? 기본 시간별 스냅샷이 중지됩니까?	워크로드 보안 스냅샷은 시간별 스냅샷에 영향을 주지 않습니다. WS 스냅샷은 매시간 스냅샷 공간을 차지하지 않으며 이전과 같이 계속되어야 합니다. 기본 시간별 스냅샷은 중지되지 않습니다.
ONTAP에서 최대 스냅샷 수에 도달하면 어떻게 됩니까?	최대 스냅샷 수에 도달하면 후속 스냅샷 찍기가 실패하고 워크로드 보안에서 스냅샷이 가득 찼다는 오류 메시지가 표시됩니다. 사용자는 가장 오래된 스냅샷을 삭제하기 위해 스냅샷 정책을 정의해야 합니다. 그렇지 않으면 스냅샷이 생성되지 않습니다. ONTAP 9.3 이전 버전에서는 볼륨에 최대 255개의 스냅샷 복사본이 포함될 수 있습니다. ONTAP 9.4 이상에서는 볼륨에 최대 1023개의 스냅샷 복사본을 포함할 수 있습니다. 에 대한 자세한 내용은 ONTAP 설명서를 "스냅샷 삭제 정책 설정 중 "참조하십시오.
워크로드 보안에서 스냅샷을 생성할 수 없습니다.	스냅샷을 생성하는 데 사용되는 역할에 https://docs .NetApp.com/us-en/cloudinsights/task_add_collector_svm.html#a-note-about-permissions [적절한 권한 할당됨] 링크가 있는지 확인합니다. 스냅샷 촬영을 위한 적절한 액세스 권한으로 _csrole_이(가) 생성되었는지 확인합니다. 보안 로그인 역할 create -vserver <vservername> -role csrole -cmddirname "volume snapshot" -access all
워크로드 보안에서 제거된 SVM에 대한 이전 경고에 대해 스냅샷이 실패하고, 이후에 다시 추가됩니다. SVM을 다시 추가한 후에 발생하는 새 경고의 경우 스냅샷이 생성됩니다.	이는 드문 시나리오입니다. 이 문제가 발생하는 경우 ONTAP에 로그인하고 이전 알림에 대해 스냅샷을 수동으로 생성합니다.
Alert Details_ 페이지에서 *Take Snapshot* 버튼 아래에 "Last attempt failed" 오류 메시지가 표시됩니다. 오류 위로 마우스를 가져가면 "ID가 있는 데이터 수집기에 대해 API 호출 명령이 시간 초과되었습니다"라는 메시지가 표시됩니다.	이는 SVM의 LIF가 ONTAP에서 _ disabled_state인 경우 SVM 관리 IP를 통해 데이터 수집기를 워크로드 보안에 추가할 때 발생할 수 있습니다. ONTAP에서 특정 LIF를 설정하고 워크로드 보안에서 _trigger_Take Snapshot manually_를 트리거합니다. 그러면 스냅샷 작업이 성공합니다.

법의학

법의학 - 모든 활동

모든 활동 페이지에서는 워크로드 보안 환경의 엔터티에 대해 수행되는 작업을 이해할 수 있습니다.

모든 활동 데이터 검토

Forensics > Activity Forensics * 를 클릭하고 * All Activity * 탭을 클릭하여 All Activity 페이지에 액세스합니다. 이 페이지에서는 테넌트의 활동에 대한 개요를 제공하고 다음 정보를 강조합니다.

- 활동 기록 _ 을(를) 보여주는 그래프(선택한 글로벌 시간 범위 기준)

  그래프에서 사각형을 드래그하여 그래프를 확대할 수 있습니다. 확대/축소된 시간 범위를 표시하기 위해 전체 페이지가 로드됩니다. 확대하면 사용자가 축소할 수 있는 버튼이 표시됩니다.

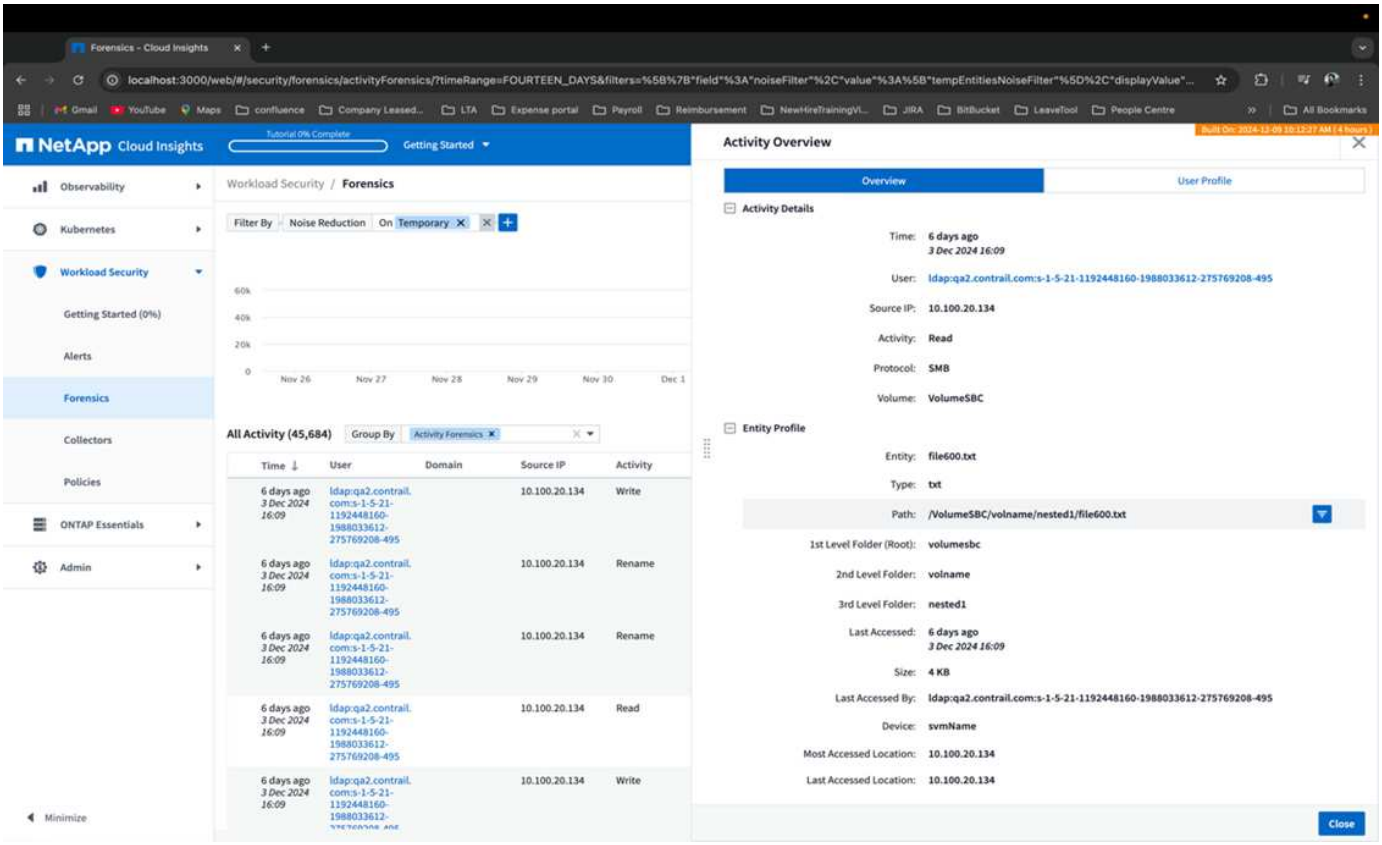
- 모든 활동 데이터 목록
- 그룹별 드롭다운은 사용자, 경로, 엔티티 유형 등을 기준으로 활동을 그룹화할 수 있는 옵션을 제공합니다
- 테이블 위에 있는 공통 경로 버튼을 클릭하면 엔터티 경로 세부 정보가 있는 슬라이드 아웃 패널을 볼 수 있습니다.

_ * All Activity * _ 표에는 다음 정보가 표시됩니다. 이러한 열 중 일부만 기본적으로 표시됩니다. "기어" 아이콘을 클릭하여 표시할 열을 선택할 수 있습니다.

- 마지막 액세스의 연도, 월, 일 및 시간을 포함하여 엔티티에 액세스한 * 시간.
- 슬라이드 아웃 패널로 에 대한 링크를 사용하여 엔티티에 액세스한 * 사용자 *"사용자 정보".
- 사용자가 수행한 * 작업 *. 지원되는 유형은 다음과 같습니다.
  - * 그룹 소유권 변경 * - 파일 또는 폴더의 그룹 소유권이 변경됩니다. 그룹 소유권에 대한 자세한 내용은 을 참조하십시오 "이 링크."
  - * 소유자 변경 * - 파일 또는 폴더의 소유권이 다른 사용자로 변경됩니다.
  - * 권한 변경 * - 파일 또는 폴더 권한이 변경됩니다.
  - * 생성 * - 파일 또는 폴더를 생성합니다.
  - * 삭제 * - 파일 또는 폴더를 삭제합니다. 폴더가 삭제되면 해당 폴더 및 하위 폴더에 있는 모든 파일에 대해 _DELETE_events가 획득됩니다.
  - * 읽기 * - 파일을 읽습니다.
  - * 메타데이터 읽기 * - 폴더 모니터링 활성화 옵션만 해당. Windows에서 폴더를 열거나 Linux의 폴더 내에서 "ls"를 실행하면 생성됩니다.
  - * 이름 바꾸기 * - 파일 또는 폴더의 이름을 바꿉니다.
  - * 쓰기 * - 데이터가 파일에 기록됩니다.
  - * 메타데이터 쓰기 * - 파일 메타데이터는 예를 들어 권한이 변경되었습니다.
  - * 기타 변경 * - 위에 설명되지 않은 기타 이벤트. 매핑되지 않은 모든 이벤트는 "기타 변경" 작업 유형에 매핑됩니다. 파일 및 폴더에 적용됩니다.
- Path * 는 _entity_path 입니다.
- 첫 번째 레벨 폴더(루트) * 는 소문자인 엔터티 경로의 루트 디렉토리입니다.
- 2nd Level Folder * 는 소문자인 엔터티 경로의 두 번째 레벨 디렉토리입니다.
- 세 번째 수준 폴더 * 는 소문자로 엔터티 경로의 세 번째 수준 디렉터리입니다.
- 4단계 폴더 * 는 소문자인 엔터티 경로의 상위 레벨 디렉토리입니다.
- 엔티티(예: 파일) 확장자를 포함한 * 엔티티 유형 *. doc, .docx, .tmp 등.
- 요소가 상주하는 * 장치 *.
- 이벤트를 가져오는 데 사용되는 * 프로토콜 * 입니다.
- 원본 파일의 이름을 바꿀 때 이름 바꾸기 이벤트에 사용되는 * Original Path * 입니다. 이 열은 기본적으로 표에 표시되지 않습니다. 열 선택기를 사용하여 이 열을 테이블에 추가합니다.

- 요소가 있는 * 볼륨 *. 이 열은 기본적으로 표에 표시되지 않습니다. 열 선택기를 사용하여 이 열을 테이블에 추가합니다.

테이블 행을 선택하면 한 탭에 사용자 프로필이 있고 다른 탭에 활동 및 엔터티 개요가 있는 슬라이드 아웃 패널이 열립니다.



default_Group by_method는 _ 활동 포렌식 _ 입니다. 예를 들어, 엔티티 유형 과 같은 다른_Group By_method 를 선택하면 entity_Group By_table 이 표시됩니다. 선택하지 않으면 *Group by* * All * 가 표시됩니다.

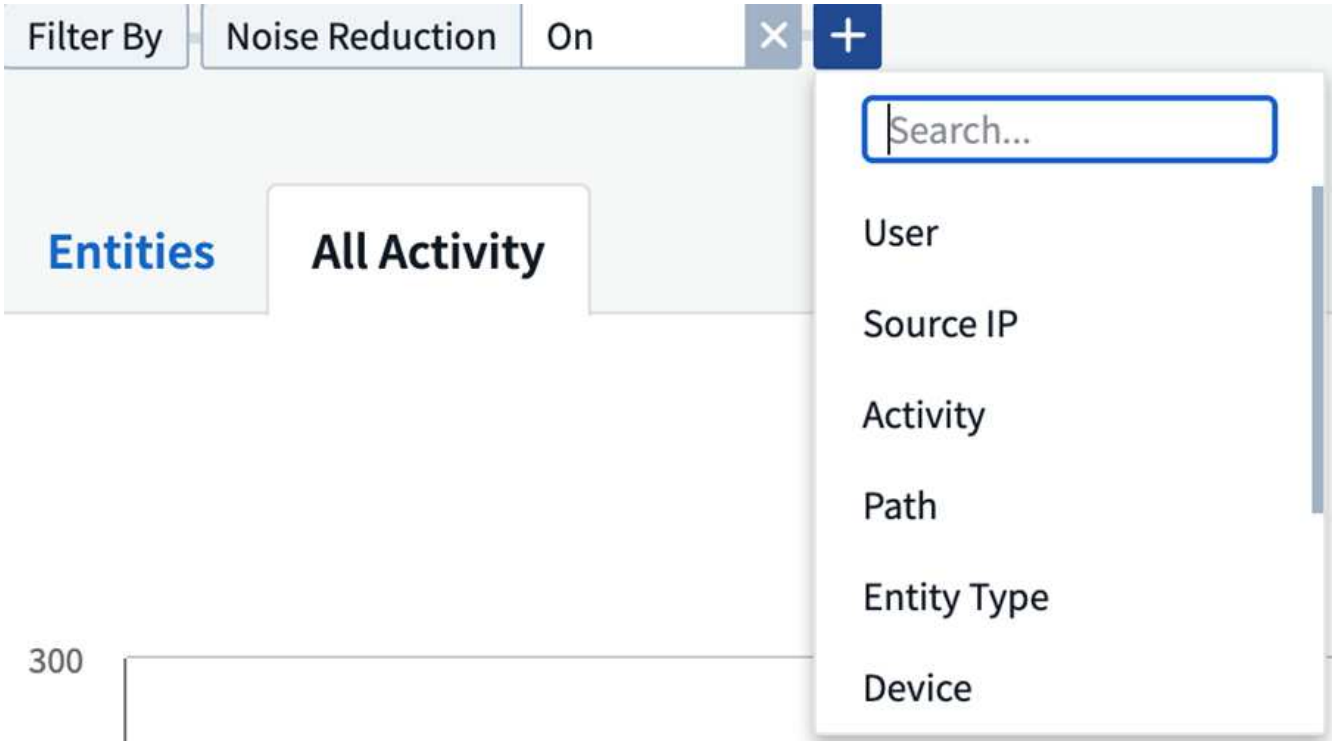
- 작업 수는 하이퍼링크로 표시됩니다. 이 항목을 선택하면 선택한 그룹이 필터로 추가됩니다. 활동 표는 해당 필터에 따라 업데이트됩니다.
- 필터를 변경하거나 시간 범위를 변경하거나 화면을 새로 고치면 필터를 다시 설정하지 않으면 필터링된 결과로 돌아갈 수 없습니다.

Forensic 활동 기록 데이터 필터링

데이터를 필터링하는 데 사용할 수 있는 두 가지 방법이 있습니다.

- 필터는 슬라이드 아웃 패널에서 추가할 수 있습니다. 이 값은 top_Filter by_list의 해당 필터에 추가됩니다.
- Filter by_필드에 입력하여 데이터를 필터링합니다.

  상단 '필터 기준' 위젯에서 * [+] * 버튼을 클릭하여 적절한 필터를 선택합니다.



검색 텍스트를 입력합니다

Enter 키를 누르거나 필터 상자 바깥쪽을 클릭하여 필터를 적용합니다.

다음 필드를 사용하여 Forensic Activity 데이터를 필터링할 수 있습니다.

- Activity * 유형.
- 엔터티에 액세스한 소스 IP * 입니다. 유효한 소스 IP 주소를 큰따옴표로 묶어야 합니다(예: “10.1.1.1.”). “10.1.1.**”, “10.1.**.*” 등과 같은 불완전한 IP는 작동하지 않습니다.
- 프로토콜 특정 작업을 가져오려면 * 프로토콜 * 을 선택합니다.
- * 작업을 수행하는 사용자의 사용자 이름 * 입니다. 필터링할 정확한 사용자 이름을 입력해야 합니다. 부분 사용자 이름 또는 접두사가 붙은 부분 사용자 이름 또는 ' * '로 접미사를 바꾼 검색은 작동하지 않습니다.
- * 노이즈 감소 * - 사용자가 최근 2시간 내에 생성한 파일을 필터링합니다. 사용자가 액세스하는 임시 파일(예: .tmp 파일)을 필터링하는 데에도 사용됩니다.
- 활동을 수행하는 사용자의 * 도메인 *. 필터링할 * 정확한 도메인 * 을 제공해야 합니다. 부분 도메인 또는 부분 도메인 앞에 와일드카드(' * ')가 있거나 접미사가 붙은 부분 도메인 검색은 작동하지 않습니다. _None_은(는) 누락된 도메인을 검색하기 위해 지정할 수 있습니다.

다음 필드에는 특수 필터링 규칙이 적용됩니다.

- **Entity Type**, entity(파일) 확장자를 사용하는 경우 - 따옴표 안에 정확한 엔터티 유형을 지정하는 것이 좋습니다. 예: _ "txt" _.
- *엔터티의 경로 * - 디렉터리 경로 필터(경로 문자열 / 로 끝나는)를 최대 4개까지 입력하여 더 빠른 결과를 얻을 수 있습니다. 예: *"/home/userX/nested1/nested2/"*. 자세한 내용은 아래 표를 참조하십시오.
- 1단계 폴더(루트) - 엔티티 경로의 루트 디렉토리입니다. 예를 들어, 엔터티 경로가 /home/userX/nested1/nested2/이면 home 또는 "home"을 사용할 수 있습니다.

- 두 번째 수준 폴더 - 엔터티 경로 필터의 두 번째 수준 디렉터리입니다. 예를 들어, 엔터티 경로가 /home/userX/nested1/nested2/이면 userX 또는 "userX"를 사용할 수 있습니다.
- 3rd 레벨 폴더 – 엔티티 경로 필터의 세 번째 레벨 디렉토리입니다.
- 예를 들어, 엔터티 경로가 /home/userX/nested1/nested2/이면 nested1 또는 "nested1"을 사용할 수 있습니다.
- 4th Level Folder - 엔티티 경로 필터의 디렉토리 4번째 수준 디렉토리입니다. 예를 들어, 엔터티 경로가 /home/userX/nested1/nested2/이면 nested2 또는 "nested2"를 사용할 수 있습니다.
- * 사용자 * 활동 수행 - 따옴표 안에 정확한 사용자를 지정하는 것이 좋습니다. 예: _ "관리자" _.
- 엔터티가 상주하는 * 장치 * (SVM
- * 볼륨 * 요소가 상주하는 곳입니다
- 원본 파일의 이름을 바꿀 때 이름 바꾸기 이벤트에 사용되는 * Original Path * 입니다.

필터링 시 위의 필드는 다음 항목의 대상이 됩니다.

- 정확한 값은 따옴표 안에 있어야 합니다. 예: "searchText"
- 와일드카드 문자열은 따옴표를 포함하지 않아야 합니다. 예: searchText, * searchText*, 는 'earchtext'가 포함된 문자열을 필터링합니다.
- 접두사가 있는 문자열(예: searchText*)은 'earchtext'로 시작하는 문자열을 검색합니다.

활동 포렌식 필터 예**:**

사용자가 필터 식을 적용했습니다	예상 결과	성능 평가	설명
경로="/home/userX/nested1/nested2/"	지정된 디렉토리 아래의 모든 파일과 폴더의 반복적인 조회	빠릅니다	디렉터리 검색은 최대 4개의 디렉터리가 빠릅니다.
경로="/home/userX/nested1/"	지정된 디렉토리 아래의 모든 파일과 폴더의 반복적인 조회	빠릅니다	디렉터리 검색은 최대 4개의 디렉터리가 빠릅니다.
경로 = "/home/userX/nested1/test"	지정된 경로 regex 아래의 모든 파일과 폴더의 반복적인 조회(테스트 * 는 파일 또는 디렉토리 또는 둘 다를 의미할 수 있음)	느린 속도	디렉터리+파일 정규식 검색은 디렉터리 검색보다 검색 속도가 느립니다.
경로="/home/userX/nested1/nested2/nested3/"	지정된 디렉토리 아래의 모든 파일과 폴더의 반복적인 조회	느린 속도	4개 이상의 디렉터리 검색은 검색 속도가 느립니다.
기타 모든 비 경로 기반 필터. 사용자 및 엔터티 유형 필터는 따옴표로 묶는 것이 좋습니다. 예: User="Administrator" Entity Type="txt"		빠릅니다	

참고:

1. 선택한 시간 범위가 3일 이상인 경우 모든 활동 아이콘 옆에 표시된 활동 수는 30분으로 반올림됩니다. 예: _9월 1일 오전 10시 15분부터 9월 7일 오전 10시 15분까지의 시간 범위에는 9월 1일 오전 10시부터 9월 7일 오전 10시 30분까지 활동 카운트가 표시됩니다.
2. 마찬가지로 선택한 시간 범위가 3일 이상이면 활동 기록 그래프에 표시된 카운트 메트릭은 30분으로 반올림됩니다.

법의학적 활동 기록 데이터 정렬

활동 기록 데이터를 시간*,* 사용자*,* 소스 *IP,* 활동*, _, _Entity Type*, 1단계 폴더(루트), 2단계 폴더, 3단계 폴더 및 4단계 폴더별로 정렬할 수 있습니다. 기본적으로 테이블은 Descending_time_order를 기준으로 정렬됩니다. 즉, 최신 데이터가 먼저 표시됩니다. Device_and_Protocol_fields에 대해 정렬이 사용되지 않습니다.

비동기 내보내기에 대한 사용자 안내서

개요

스토리지 워크로드 보안의 비동기식 내보내기 기능은 대규모 데이터 내보내기를 처리하도록 설계되었습니다.

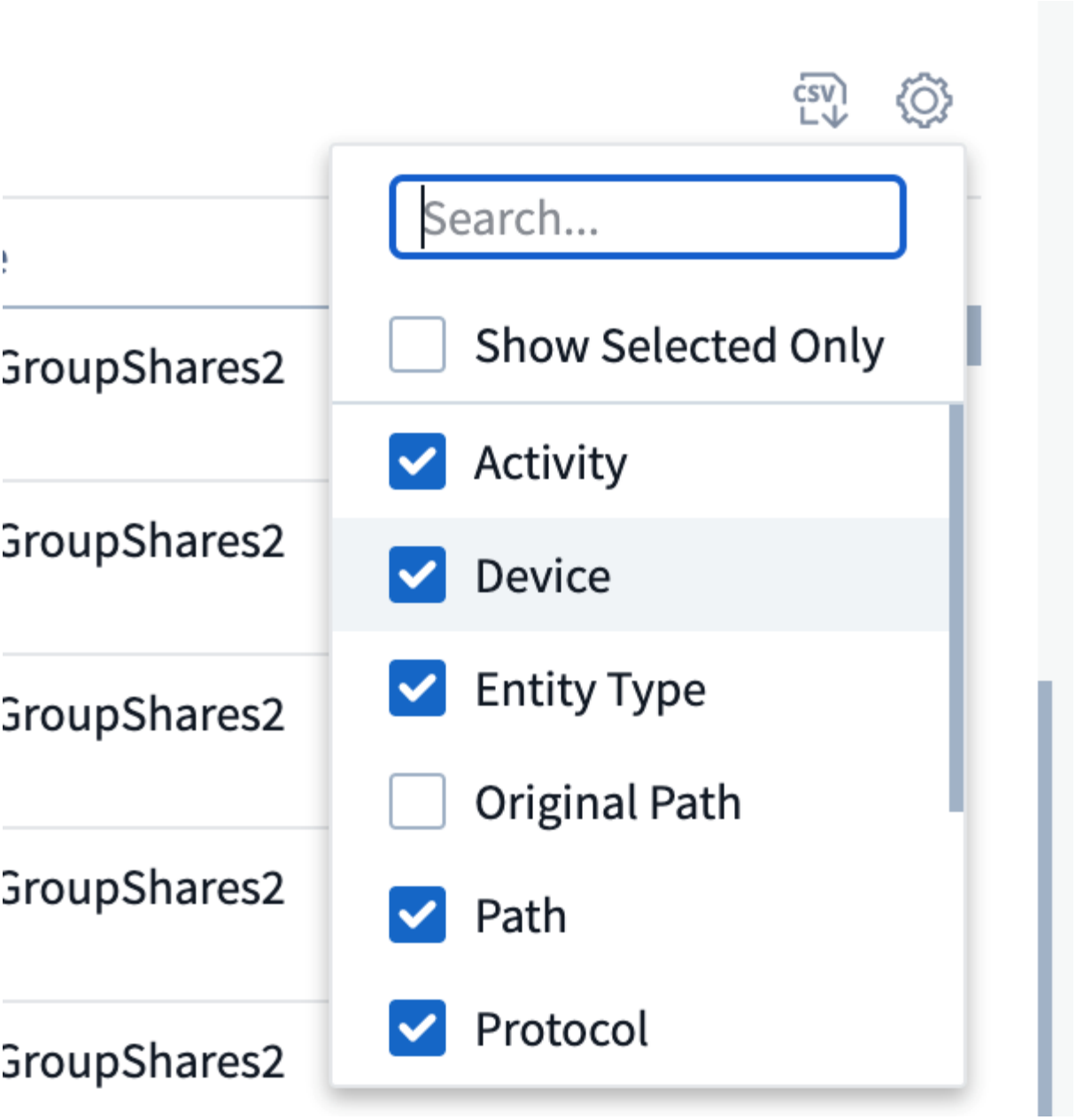
단계별 가이드**:** 비동기 내보내기를 사용하여 데이터 내보내기

1. * 내보내기 시작 * : 내보내기에 대해 원하는 시간 기간과 필터를 선택하고 내보내기 버튼을 클릭합니다.
2. * 내보내기가 완료될 때까지 대기 *: 처리 시간은 몇 분에서 몇 시간까지 소요될 수 있습니다. 포렌식 페이지를 몇 번 새로 고쳐야 할 수 있습니다. 내보내기 작업이 완료되면 "마지막 내보내기 CSV 파일 다운로드" 버튼이 활성화됩니다.
3. * 다운로드 *: "마지막 생성 내보내기 파일 다운로드" 버튼을 클릭하여 .zip 형식으로 내보낸 데이터를 가져옵니다. 이 데이터는 사용자가 다른 비동기 내보내기를 시작하거나 3일이 경과할 때까지 다운로드할 수 있습니다. 이 버튼은 다른 비동기 내보내기가 시작될 때까지 활성화된 상태로 유지됩니다.
4. * 제한 사항 *:
    - 비동기 다운로드 수는 현재 사용자당 1개, 테넌트당 3개로 제한됩니다.
    - 내보낸 데이터는 최대 100만 개의 레코드로 제한됩니다.

API를 통해 포렌식 데이터를 추출하는 샘플 스크립트는 에이전트의 _/opt/NetApp/cloudsecure/agent/export-script/_에 있습니다. 스크립트에 대한 자세한 내용은 이 위치에 있는 Readme 파일을 참조하십시오.

모든 활동에 대한 열 선택

ALL ACTIVITY_TABLE에는 기본적으로 선택 열이 표시됩니다. 열을 추가, 제거 또는 변경하려면 테이블 오른쪽에 있는 기어 아이콘을 클릭하고 사용 가능한 열 목록에서 선택합니다.



활동 기록 보존

활성 워크로드 보안 환경에서는 활동 기록이 13개월 동안 유지됩니다.

포렌식 페이지의 필터 적용 가능성

필터	기능	예	이 필터에 적용 가능합니다	이러한 필터에는 적용되지 않습니다	결과
* (별표)	모든 것을 검색할 수 있습니다	Auto * 03172022 검색 텍스트에 하이픈 또는 밑줄이 포함된 경우 대괄호로 표현식을 지정합니다. 예: svm-123 검색에는 (svm *)	사용자, 엔터티 유형, 장치, 볼륨, 원래 경로, 1stLevel 폴더, 2ndLevel 폴더, 3rdLevel 폴더, 4thLevel 폴더		"Auto"로 시작하여 "03172022"로 끝나는 모든 리소스를 반환합니다.
? (물음표)	특정 수의 문자를 검색할 수 있습니다	AutoSabotageUser1_03172022?	사용자, 엔티티 유형, 디바이스, 볼륨, 1stLevel 폴더, 2ndLevel 폴더, 3rdLevel 폴더, 4thLevel 폴더		AutoSabotageUser1_03172022A, AutoSabotageUser1_03172022B, AutoSabotageUser1_031720225 등을 반환합니다
또는	여러 요소를 지정할 수 있습니다	AutoSabotageUser1_03172022 또는 AutoRansomUser4_03162022	사용자, 도메인, 엔터티 유형, 원래 경로		AutoSabotageUser1_03172022 또는 AutoRansomUser4_03162022 중 하나를 반환합니다
아닙니다	검색 결과에서 텍스트를 제외할 수 있습니다	AutoRansomUser4_03162022가 아닙니다	사용자, 도메인, 엔터티 유형, 원래 경로, 1stLevel 폴더, 2ndLevel 폴더, 3rdLevel 폴더, 4thLevel 폴더	장치	"AutoRansomUser4_03162022"로 시작하지 않는 모든 항목을 반환합니다.
없음	모든 필드에서 NULL 값을 검색합니다	없음	도메인		대상 필드가 비어 있는 결과를 반환합니다

경로/원래 경로 검색

/ 을(를) 사용하거나 사용하지 않고 검색 결과는 다릅니다

"/AutoDir1/AutoFile03242022"	정확한 검색만 작동합니다. 정확한 경로가 /AutoDir1/AutoFile03242022 인 모든 활동을 반환합니다(대/소문자 구분 없음).
"/AutoDir1/"	Works; AutoDir1과 일치하는 1단계 디렉터리의 모든 작업을 반환합니다(대/소문자 구분 없음).
"/AutoDir1/AutoFile03242022/"	Works; AutoDir1 및 AutoFile03242022와 일치하는 2단계 디렉터리와 일치하는 1단계 디렉터리의 모든 작업을 반환합니다(대소문자 구분 없음).
/AutoDir1/AutoFile03242022 또는 /AutoDir1/AutoFile03242022	작동하지 않습니다

NOT/AutoDir1/AutoFile03242022	작동하지 않습니다
NOT/AutoDir1	작동하지 않습니다
NOT/AutoFile03242022	작동하지 않습니다
*	작동하지 않습니다

로컬 루트 **SVM** 사용자 활동 변경

로컬 루트 SVM 사용자가 작업을 수행하는 경우 NFS 공유가 마운트된 클라이언트의 IP가 사용자 이름에 고려되며, 이 IP는 포렌식 작업 및 사용자 활동 페이지 모두에서 root@<ip-address-of-the-client>로 표시됩니다.

예를 들면 다음과 같습니다.

- SVM-1이 워크로드 보안에 의해 모니터링되고 해당 SVM의 루트 사용자가 IP 주소가 10.197.12.40인 클라이언트에 공유를 마운트하는 경우, 포렌식 활동 페이지에 표시되는 사용자 이름은 *root@10.197.12.40* 입니다.
- 동일한 SVM-1이 IP 주소가 10.197.12.41인 다른 클라이언트에 마운트되는 경우 법의학 활동 페이지에 표시되는 사용자 이름은 *root@10.197.12.41* 입니다.
- • IP 주소별로 NFS 루트 사용자 활동을 분리하는 데 사용됩니다. 이전에는 모든 활동이 IP 구분 없이 _root_user 만 수행하는 것으로 간주되었습니다.

문제 해결

문제	시도해 보십시오
“All Activities(모든 활동)” 테이블의 ‘User(사용자)’ 열 아래에 사용자 이름이 “LDAP:HQ.COMPANYNAME.COM:S-1-5-21-3577637-1906459482-1437260136-1831817” 또는 “LDAP:default:80038003”으로 표시됩니다.	가능한 원인은 다음과 같습니다. 1. 아직 구성된 사용자 디렉토리 Collector가 없습니다. 하나를 추가하려면 * Workload Security > Collector > User Directory Collector * 로 이동하고 * + User Directory Collector * 를 클릭합니다. Active Directory_or_LDAP Directory Server_를 선택합니다. 2. 사용자 디렉터리 수집기가 구성되었지만 중지되었거나 오류 상태입니다. Collectors > User Directory Collectors * 로 이동하여 상태를 확인하십시오. "사용자 디렉토리 수집기 문제 해결"문제 해결 팁은 설명서의 섹션을 참조하십시오. 올바르게 구성하면 24시간 내에 자동으로 이름이 확인됩니다. 그래도 해결되지 않으면 올바른 사용자 데이터 수집기를 추가했는지 확인합니다. 사용자가 실제로 추가된 Active Directory/LDAP Directory Server에 속하는지 확인합니다.
일부 NFS 이벤트는 UI에서 표시되지 않습니다.	다음을 확인하십시오. 1. POSIX 속성이 설정된 AD 서버의 사용자 디렉토리 수집기는 UI에서 활성화된 unixid 속성으로 실행해야 합니다. 2. UI 3의 사용자 페이지에서 NFS 액세스를 수행하는 모든 사용자를 검색할 때 표시됩니다. 원시 이벤트(사용자가 아직 검색되지 않은 이벤트)는 NFS 4에서 지원되지 않습니다. NFS 내보내기에 대한 익명 액세스는 모니터링되지 않습니다. 5. NFS 버전이 NFS4.1 미만에서 사용되는지 확인합니다.

Forensics_All Activity_or_Entities_pages의 필터에 별표(*)와 같은 와일드카드 문자가 포함된 일부 문자를 입력하면 페이지가 매우 느리게 로드됩니다.	검색 문자열의 별표(\ )는 모든 항목을 검색합니다. 그러나 _ * <searchTerm>_또는 _ * <searchTerm> * _ 과(와) 같은 선행 와일드카드 문자열은 쿼리 속도를 느리게 만듭니다. 보다 나은 성능을 얻으려면 접두사 문자열을 대신 ***<searchTerm>**** 형식으로 사용합니다(즉, 별표( )*after_a* 검색 용어를 추가합니다*).* 예*: _ * testvolume_or* * test * volume_ 대신 *testvolume* * 문자열을 사용하십시오. 디렉토리 검색을 사용하여 지정된 폴더 아래의 모든 활동을 재귀적으로 봅니다(계층 검색). 예: "/path1/path2/path3/"는 /path1/path2/path3 아래에 재귀적으로 모든 활동을 나열합니다. 또는 All Activity(모든 활동) 탭 아래의 "Add to Filter(필터에 추가)" 옵션을 사용합니다.
경로 필터를 사용할 때 "상태 코드 500/503으로 요청 실패" 오류가 발생합니다.	레코드를 필터링하려면 더 작은 날짜 범위를 사용하십시오.
Forensic UI에서 _PATH_FILTER를 사용할 때 데이터가 느리게 로드되고 있습니다.	더 빠른 결과를 얻으려면 디렉터리 경로 필터(경로 문자열 / 로 끝나는)를 최대 4개까지 사용하는 것이 좋습니다. 예를 들어 디렉터리 경로가 /aa/bbb/ccc/dd인 경우 "/aa/bb/ccc/dd/"를 검색하여 데이터를 더 빨리 로드하십시오.

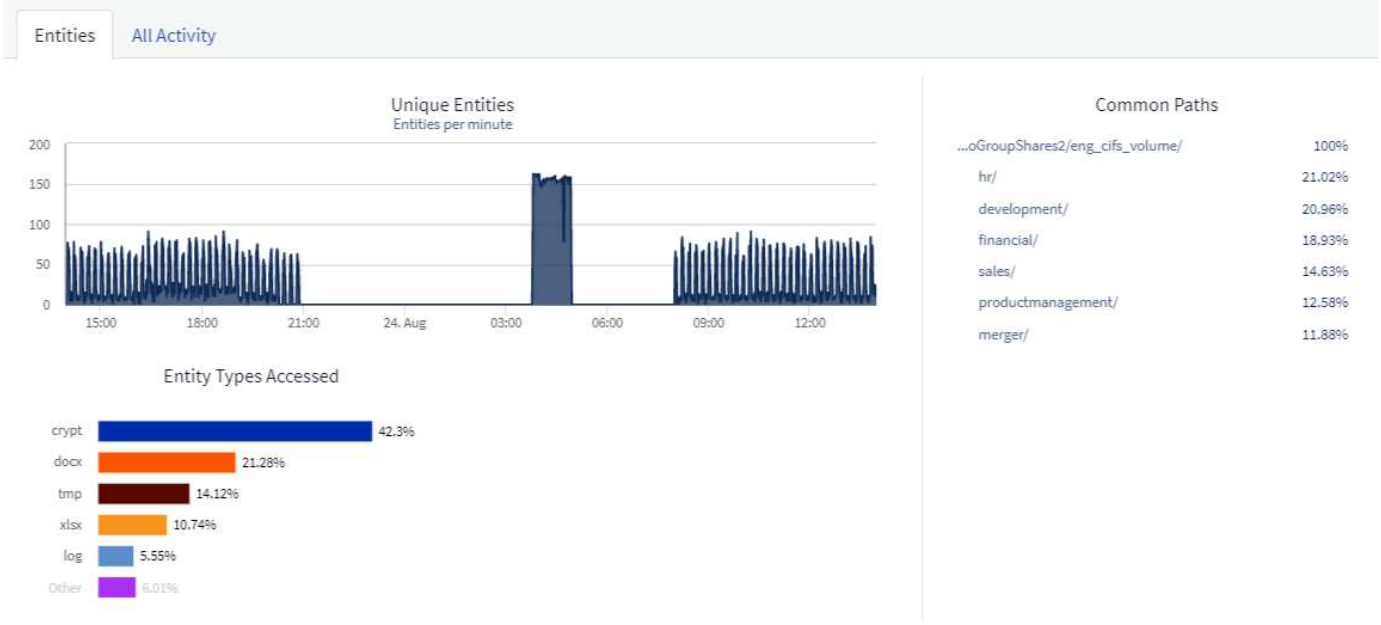
포렌식 엔터티 페이지

포렌식 엔터티 페이지에서는 테넌트의 엔터티 활동에 대한 자세한 정보를 제공합니다.

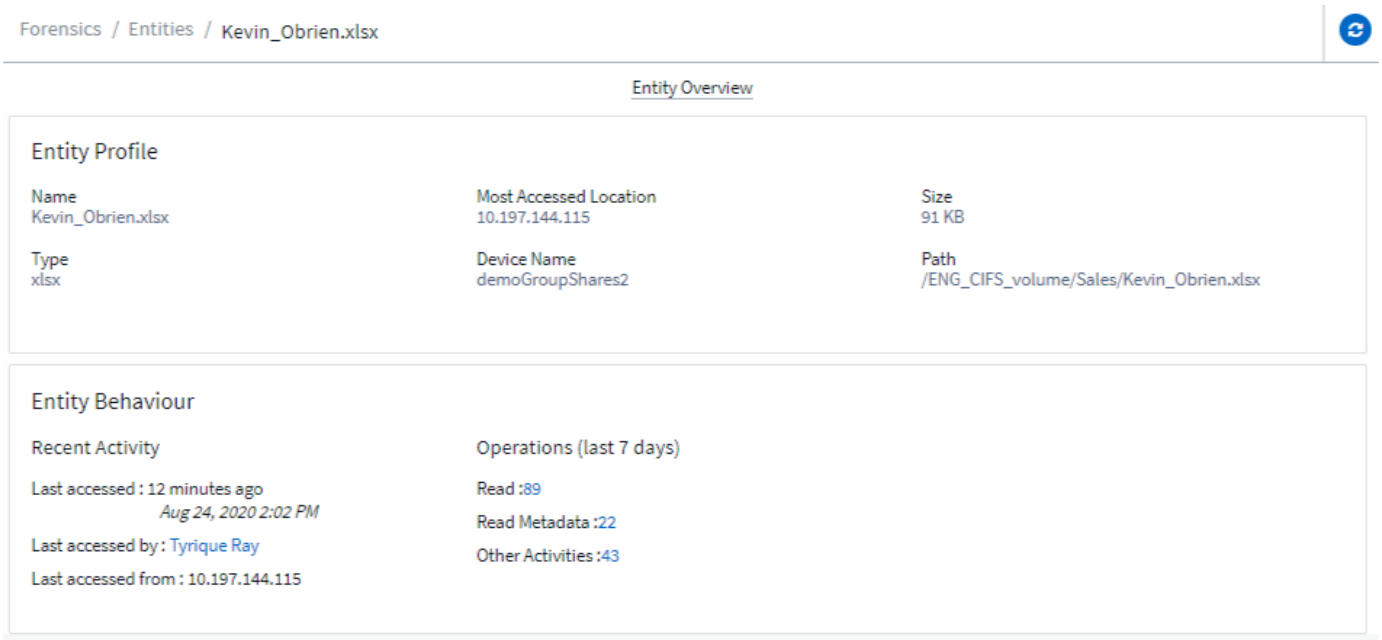
엔터티 정보 검사

Forensics > Activity Forensics * 를 클릭하고 _Entities_탭을 클릭하여 Entities 페이지에 액세스합니다.

이 페이지에서는 테넌트의 엔터티 활동에 대한 개요를 제공하고 다음 정보를 강조합니다. * 분당 *UNIQUE_ACCESS_ACCESS_ACCESS_*를 보여 주는 그래프 * *_Entity Types ACCESS* * 전체 엔터티 수 중 *Common Paths* * 에 대한 분석 결과



목록에서 엔티티를 클릭하면 엔티티의 개요 페이지가 열리고 이름, 유형, 장치 이름, 가장 많이 액세스되는 위치 IP 및 경로 등의 세부 정보와 사용자, IP, 경로 등의 엔터티 동작이 표시됩니다. 엔티티에 마지막으로 액세스한 시간입니다.



Forensic 사용자 개요

각 사용자에 대한 정보는 사용자 개요 에 나와 있습니다. 이러한 뷰를 사용하여 사용자 특성, 관련

엔터티 및 최근 활동을 파악할 수 있습니다.

사용자 프로필

사용자 프로필 정보에는 사용자의 연락처 정보 및 위치가 포함됩니다. 프로필은 다음 정보를 제공합니다.

- 사용자의 이름입니다
- 사용자의 이메일 주소입니다
- 사용자 관리자
- 사용자의 전화 연락처입니다
- 사용자의 위치입니다

사용자 행동

사용자 동작 정보는 사용자가 수행한 최근 작업 및 작업을 식별합니다. 이 정보에는 다음이 포함됩니다.

- 최근 활동
  - 마지막 액세스 위치입니다
  - 활동 그래프
  - 경고
- 최근 7일 동안의 작업
  - 작업 수

새로 고침 간격

사용자 목록은 12시간마다 새로 고쳐집니다.

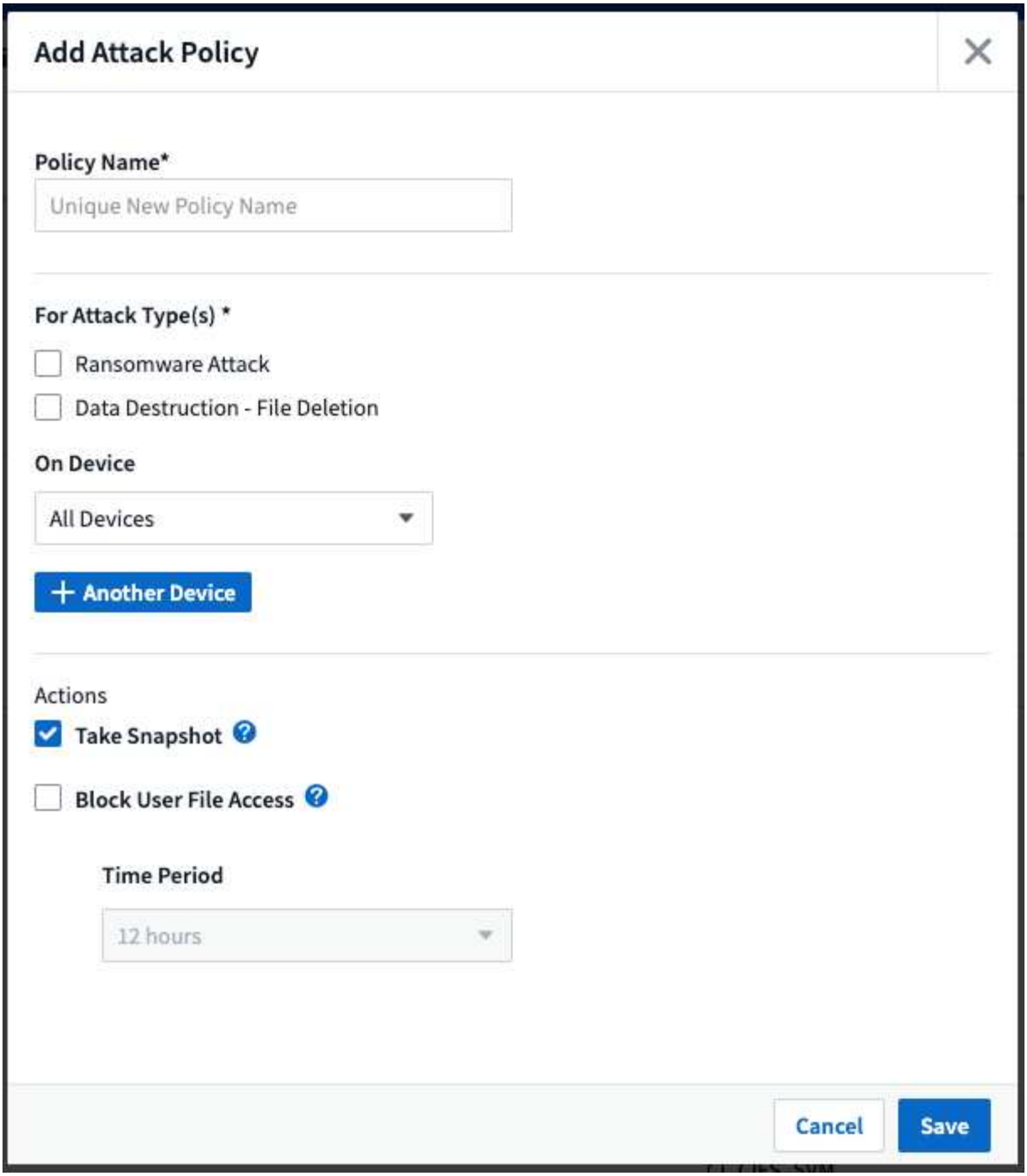
보존 정책

다시 새로 고치지 않으면 사용자 목록이 13개월 동안 유지됩니다. 13개월 후 데이터가 삭제됩니다. 워크로드 보안 환경이 삭제된 경우 환경과 관련된 모든 데이터가 삭제됩니다.

자동 응답 정책

응답 정책은 공격 또는 비정상적인 사용자 동작이 발생하는 경우 스냅샷을 생성하거나 사용자 액세스를 제한하는 등의 작업을 트리거합니다.

특정 장치 또는 모든 장치에 정책을 설정할 수 있습니다. 응답 정책을 설정하려면 * Admin > Automated Response Policies * 를 선택하고 해당 * + Policy * 버튼을 클릭합니다. 공격에 대한 정책 또는 경고에 대한 정책을 만들 수 있습니다.



고유한 이름으로 정책을 저장해야 합니다.

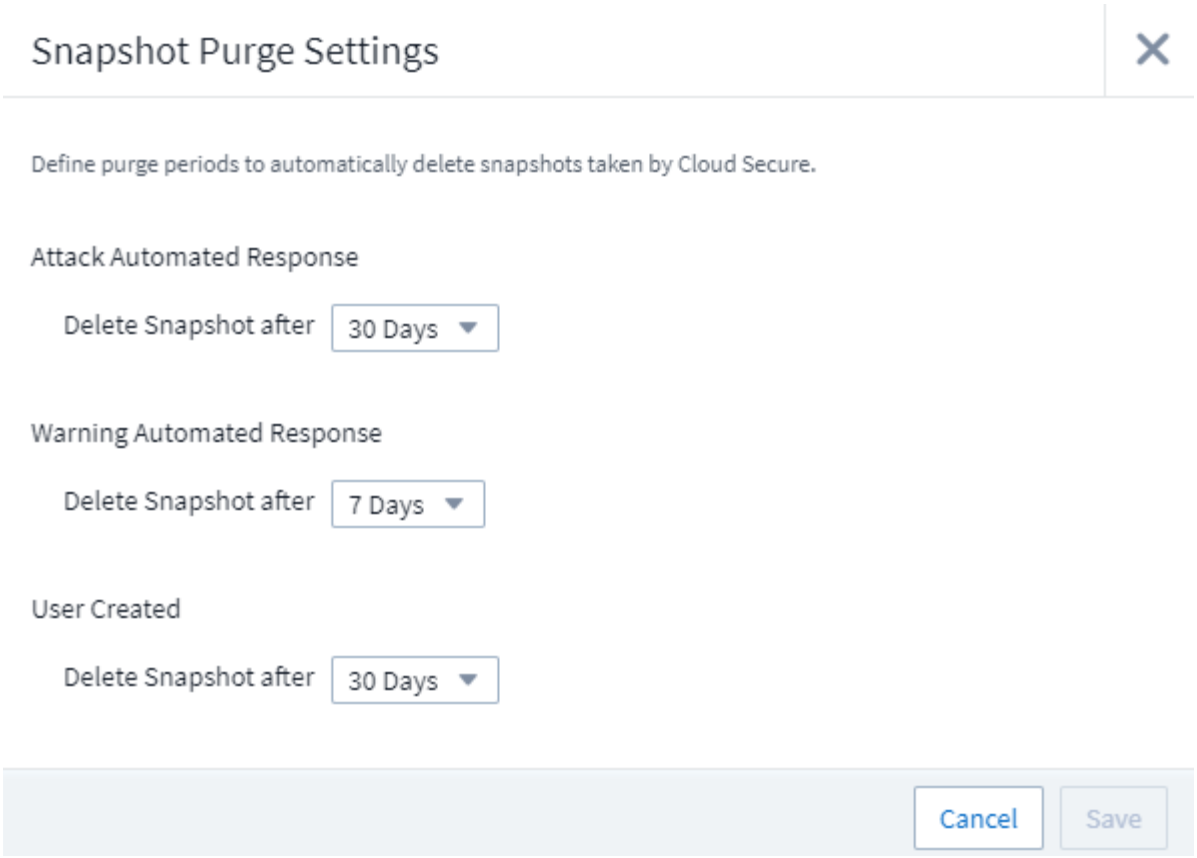
자동 응답 작업(예: 스냅샷 생성)을 사용하지 않으려면 해당 작업을 선택 해제하고 정책을 저장하면 됩니다.

지정된 디바이스 또는 모든 디바이스(선택된 경우)에 대해 알림이 트리거되면 자동 응답 정책이 데이터의 스냅샷을 생성합니다. 에서 스냅샷 상태를 볼 수 "경고 세부 정보 페이지"있습니다.

"사용자 액세스 제한"IP를 통한 사용자 액세스 제한에 대한 자세한 내용은 페이지를 참조하십시오.

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

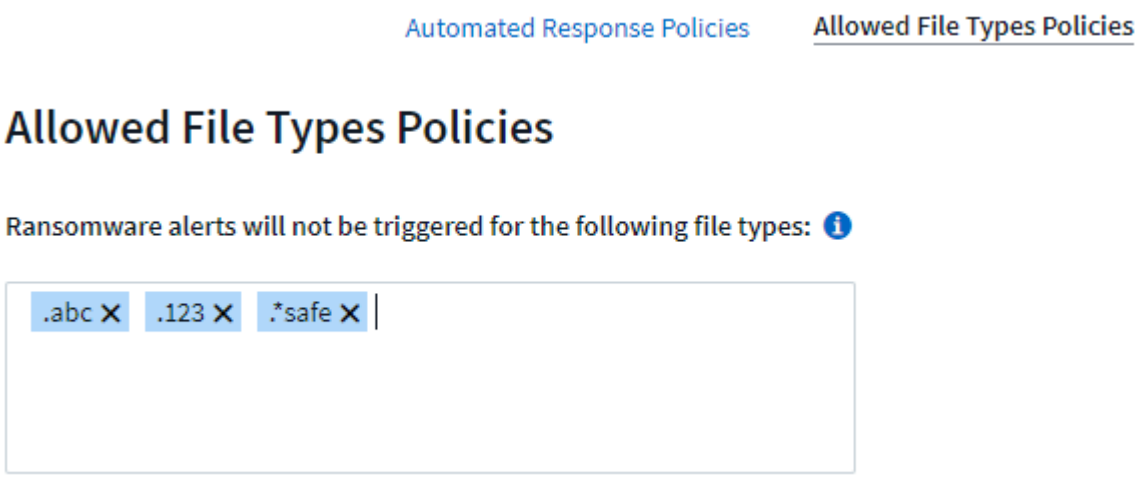
워크로드 보안은 스냅샷 삭제 설정에 따라 하루에 한 번씩 스냅샷을 자동으로 삭제합니다.



허용된 파일 형식 정책

알려진 파일 확장명에 대한 랜섬웨어 공격이 감지되고 경고 화면에서 경고가 생성되는 경우 불필요한 경고를 방지하기 위해 해당 파일 확장명을 _allowed file types_list 에 추가할 수 있습니다.

Workload Security > Policies * 로 이동한 후 _Allowed File Type Policies_tab으로 이동합니다.



허용된 파일 유형_목록에 추가되면 해당 허용된 파일 유형에 대한 랜섬웨어 공격 경고가 생성되지 않습니다. _allowed File Types_policy는 랜섬웨어 탐지에만 적용됩니다.

예를 들어, 이름이 _test.txt_인 파일의 이름이 _test.txt.abc_로 변경되고 Workload Security가 _.abc_extension으로 인해 랜섬웨어 공격을 감지하는 경우 _.abc_extension을 _allowed file types_list에 추가할 수 있습니다. 목록에 추가된 후에는 _.abc_extension을 가진 파일에 대해 랜섬웨어 공격이 더 이상 생성되지 않습니다.

허용되는 파일 형식은 정확히 일치하는 파일(예: ".abc") 또는 식(예: ". * type", ".type *" 또는 " * type *")일 수 있습니다. ".a * c", ".p * f" 형식의 식은 지원되지 않습니다.

ONTAP Autonomous 랜섬웨어 Protection과 통합

ONTAP ARP(Autonomous 랜섬웨어 보호) 기능은 NAS(NFS 및 SMB) 환경에서 워크로드 분석을 사용하여 랜섬웨어 공격을 나타낼 수 있는 비정상적인 파일 내 작업을 사전에 감지하여 경고합니다.

ARP에 대한 추가 세부 정보 및 라이센스 요구 사항을 찾을 수 "여기"있습니다.

워크로드 보안은 ONTAP와 통합되어 ARP 이벤트를 수신하고 추가 분석 및 자동 응답 계층을 제공합니다.

워크로드 보안은 ONTAP에서 ARP 이벤트를 수신하고 다음 작업을 수행합니다.

1. 볼륨 암호화 이벤트와 사용자 활동의 상관 관계를 분석하여 손상을 일으키는 원인을 식별합니다.
2. 자동 응답 정책 구축(정의된 경우)
3. 포렌식 기능 제공:
   - 고객이 데이터 침해 조사를 수행할 수 있도록 허용합니다.
   - 영향을 받은 파일을 파악하여 복구 시간을 단축하고 데이터 침해 조사를 수행할 수 있습니다.

필수 구성 요소

1. 최소 ONTAP 버전: 9.11.1
2. ARP 사용 볼륨. ARP 활성화에 대한 세부 정보를 찾을 "여기"수 있습니다. ARP는 OnCommand 시스템 관리자를 통해 활성화해야 합니다. 워크로드 보안은 ARP를 활성화할 수 없습니다.
3. 워크로드 보안 수집기는 클러스터 IP를 통해 추가해야 합니다.
4. 이 기능을 사용하려면 클러스터 레벨 자격 증명이 필요합니다. 즉, SVM을 추가할 때 클러스터 레벨 자격 증명을 사용해야 합니다.

사용자 권한이 필요합니다

클러스터 관리 자격 증명을 사용하는 경우 새 권한이 필요하지 않습니다.

사용자에게 부여된 권한으로 사용자 지정 사용자(예: *CsUser*)를 사용하는 경우, 아래 단계를 따라 워크로드 보안에 권한을 부여하여 ONTAP에서 ARP 관련 정보를 수집합니다.

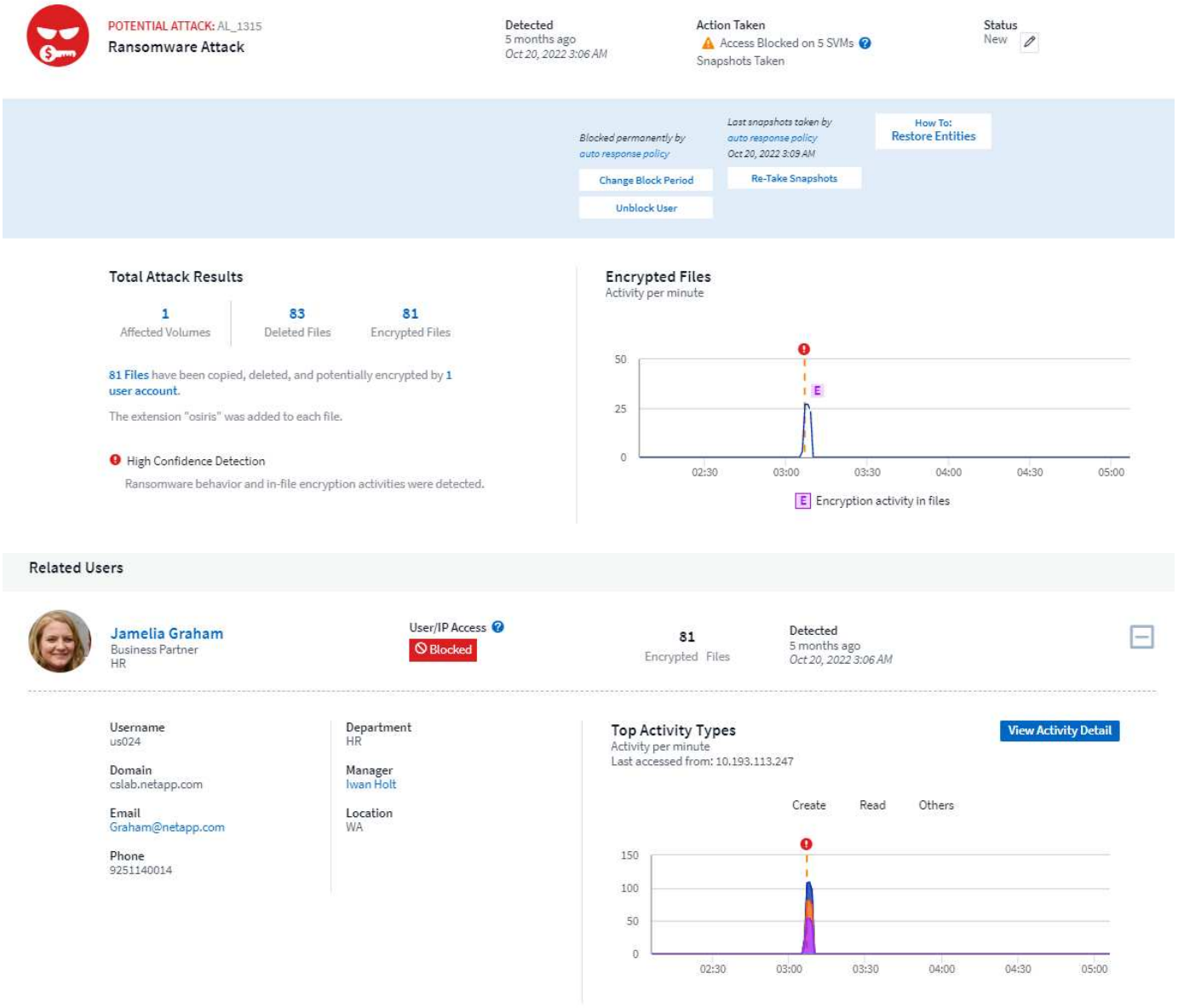
클러스터 자격 증명을 사용하여 _CsUser_의 경우 ONTAP 명령줄에서 다음을 수행합니다.

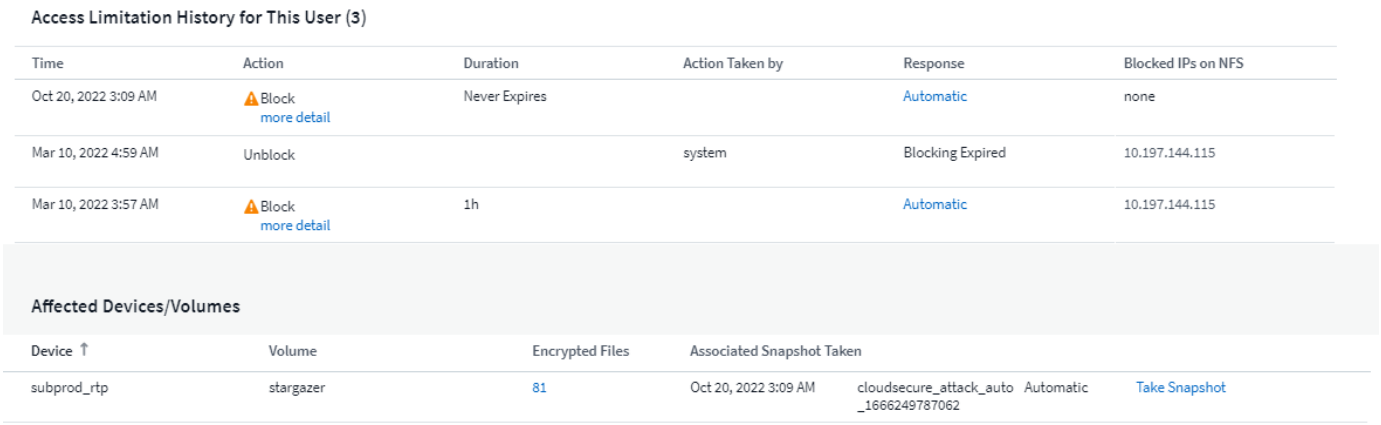
```
security login rest-role create -role arwrole -api /api/storage/volumes
-access readonly -vserver <cluster_name>
security login rest-role create -api /api/security/anti-ransomware -access
readonly  -role arwrole -vserver <cluster_name>
security login create -user-or-group-name csuser -application http
-authmethod password -role arwrole
```

기타 구성에 대한 자세한 "ONTAP 권한"정보

샘플 알림

ARP 이벤트로 인해 생성된 샘플 경고는 다음과 같다.





고신뢰도 배너는 공격이 파일 암호화 활동과 함께 랜섬웨어 동작을 보여발생했음을 나타냅니다. 암호화된 파일 그래프는 ARP 솔루션이 볼륨 암호화 작업을 감지한 타임스탬프를 나타냅니다.

제한 사항

SVM이 워크로드 보안에 의해 모니터링되지 않지만 ONTAP에서 생성된 ARP 이벤트가 있는 경우, 해당 이벤트는 워크로드 보안에서 계속 수신되고 표시됩니다. 그러나 알림과 관련된 Forensic 정보 및 사용자 매핑은 캡처되거나 표시되지 않습니다.

문제 해결

알려진 문제와 해결 방법은 다음 표에 설명되어 있습니다.

문제:	해상도:
공격이 감지된 후 24시간 이내에 이메일 경고가 수신됩니다. UI에 Data Infrastructure Insights 워크로드 보안이 이메일을 수신하기 24시간 전에 경고가 표시됩니다.	ONTAP이 Data Infrastructure Insights 워크로드 보안(예: 워크로드 보안)으로 _ Ransomware detected_Event를 전송하면 이메일이 전송됩니다. 이벤트에는 공격 목록과 타임 스탬프가 포함됩니다. 워크로드 보안 UI는 첫 번째 공격 파일의 경고 타임스탬프를 표시합니다. ONTAP은 특정 개수의 파일이 인코딩될 때 _Ransomware Detected_Event를 데이터 인프라 인사이트 로 전송합니다. 따라서 알림이 UI에 표시되는 시간과 이메일을 보낸 시간 사이에 차이가 있을 수 있습니다.

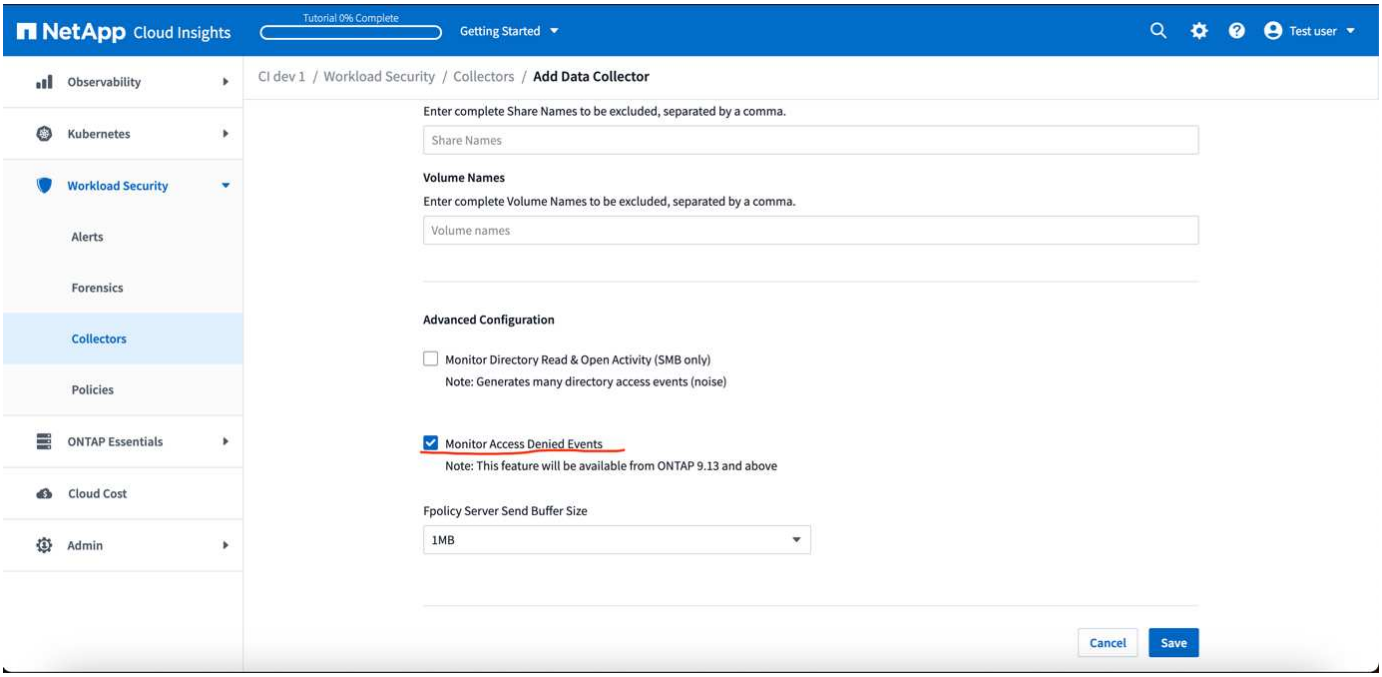
ONTAP 액세스와의 통합이 거부되었습니다

ONTAP 액세스 거부 기능은 NAS 환경(NFS 및 SMB)에서 워크로드 분석을 사용하여 실패한 파일 작업을 사전에 감지하여 경고합니다(예: 권한이 없는 작업을 수행하려는 사용자). 특히 보안 관련 오류의 경우 이러한 파일 작업 알림 실패 시 초기에 내부자 공격을 차단하는 데 도움이 됩니다.

Data Infrastructure Insights 워크로드 보안은 ONTAP과 통합되어 액세스 거부 이벤트를 수신하고 추가적인 분석 및 자동 응답 계층을 제공합니다.

필수 구성 요소

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



사용자 권한이 필요합니다

클러스터 관리 자격 증명을 사용하여 Data Collector를 추가하는 경우 새 권한이 필요하지 않습니다.

사용자에게 부여된 권한이 있는 사용자 지정 사용자(예: *CsUser*)를 사용하여 수집기를 추가하는 경우, 아래 단계에 따라 ONTAP에 액세스 거부 이벤트를 등록하는 데 필요한 권한을 워크로드 보안에 부여합니다.

cluster_credentials를 사용하는 CsUser의 경우 ONTAP 명령줄에서 다음 명령을 실행합니다. _csrestrole_은(는) 사용자 지정 역할이고 _csUser_는 ONTAP 사용자 지정 사용자입니다.

```
 security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <cluster_name>
 security login create -user-or-group-name csuser -application http
-authmethod password -role csrestrole
```

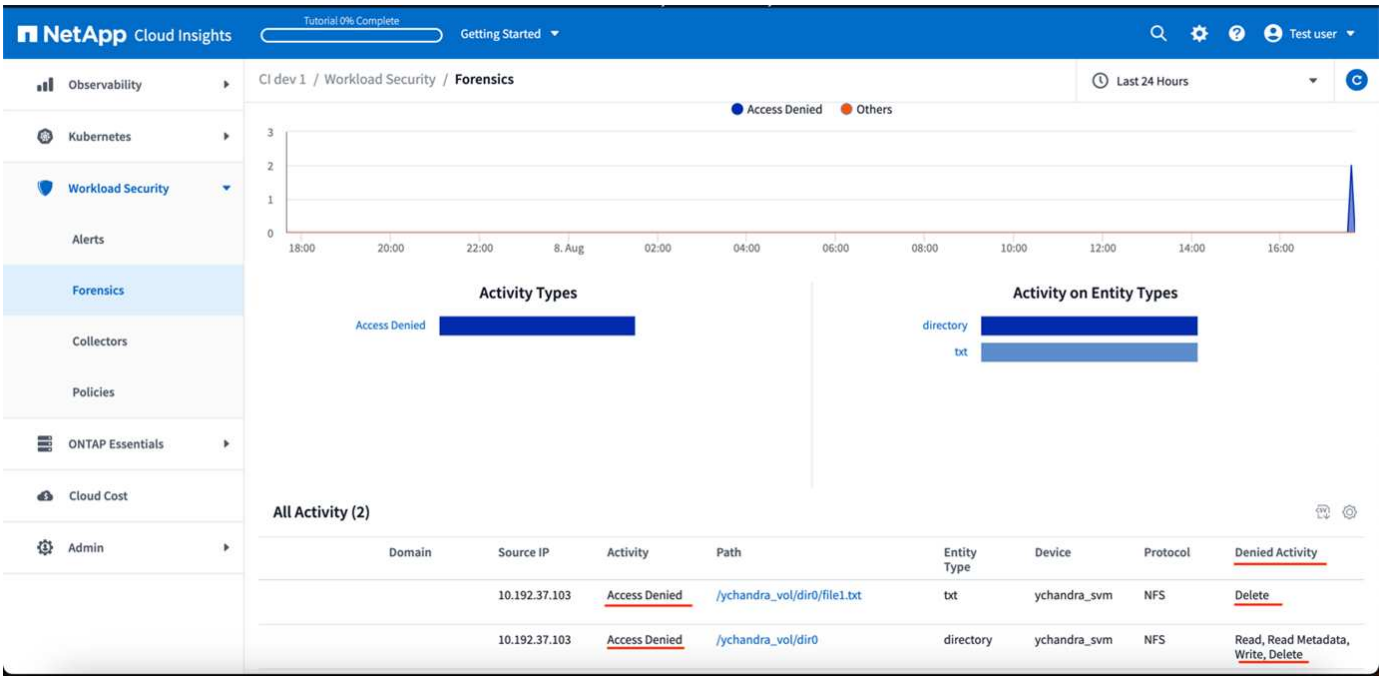
csUser with_SVM_credentials의 경우 ONTAP 명령줄에서 다음 명령을 실행합니다.

```
 security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <svm_name>
 security login create -user-or-group-name csuser -application http
-authmethod password -role csrestrole -vserver <svm_name>
```

기타 구성에 대한 자세한 "ONTAP 권한"정보

액세스가 거부되었습니다

ONTAP 시스템에서 이벤트를 가져오면 워크로드 보안 포렌식 페이지에 액세스 거부 이벤트가 표시됩니다. 표시되는 정보 외에도 기어 아이콘에서 테이블에 *WARGED Activity* 열을 추가하여 특정 작업에 대해 누락된 사용자 권한을 볼 수 있습니다.



사용자 액세스 차단

공격이 감지되면 워크로드 보안에서 파일 시스템에 대한 사용자 액세스를 차단하여 공격을 차단할 수 있습니다. 자동 응답 정책을 사용하거나 알림 또는 사용자 세부 정보 페이지에서 수동으로 액세스를 차단할 수 있습니다.

사용자 액세스를 차단할 때는 차단 기간을 정의해야 합니다. 선택한 기간이 끝나면 사용자 액세스가 자동으로 복원됩니다. 액세스 차단은 SMB 및 NFS 프로토콜 모두에서 지원됩니다.

사용자가 SMB 및 호스트 시스템의 IP 주소에 대해 직접 차단되어 NFS에 대한 공격이 차단됩니다. 이러한 시스템 IP 주소는 워크로드 보안에서 모니터링하는 SVM(Storage Virtual Machine)에 액세스하지 못하도록 차단됩니다.

예를 들어, 워크로드 보안이 10개의 SVM을 관리하고 자동 응답 정책이 4개의 SVM에 대해 구성되었다고 가정해 보겠습니다. 4개의 SVM 중 하나에서 공격이 발생한 경우 10개의 SVM에서 사용자의 액세스가 차단됩니다. 원래 SVM에 대해 스냅샷이 여전히 촬영됩니다.

SMB용으로 구성된 SVM 4개, NFS용으로 구성된 SVM 1개와 NFS 및 SMB용으로 구성된 나머지 2개가 있는 경우 4개의 SVM 중 하나에서 공격이 발생한 경우 모든 SVM이 차단됩니다.

사용자 액세스 차단을 위한 필수 조건

이 기능을 사용하려면 클러스터 레벨 자격 증명이 필요합니다.

클러스터 관리 자격 증명을 사용하는 경우 새 권한이 필요하지 않습니다.

사용자에게 부여된 권한으로 사용자 지정 사용자(예: *CsUser*)를 사용하는 경우 아래 단계에 따라 사용자를 차단하는 워크로드 보안에 권한을 부여합니다.

클러스터 자격 증명이 있는 CsUser의 경우 ONTAP 명령줄에서 다음을 수행하십시오.

```
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
```

페이지의 사용 권한 섹션도 "ONTAP SVM Data Collector 구성" 검토해야 합니다.

이 기능을 활성화하는 방법은 무엇입니까?

- 워크로드 보안에서 * 워크로드 보안 > 정책 > 자동화된 대응 정책 * 으로 이동합니다. 공격 정책 * 을 선택합니다.
- 사용자 파일 액세스 차단 _ 을(를) 선택합니다.

자동 사용자 액세스 차단을 설정하는 방법은 무엇입니까?

- 새 공격 정책을 만들거나 기존 공격 정책을 편집합니다.
- 공격 정책을 모니터링해야 하는 SVM을 선택합니다.
- “Block User File Access(사용자 파일 액세스 차단)” 확인란을 클릭합니다. 이 옵션을 선택하면 기능이 활성화됩니다.
- “Time Period(기간)”에서 차단 적용 기간을 선택합니다.
- 자동 사용자 차단을 테스트하기 위해 를 통해 공격을 시뮬레이션할 수 "시뮬레이션된 스크립트"있습니다.

시스템에 차단된 사용자가 있는지 어떻게 알 수 있습니까?

- 경고 목록 페이지에서 사용자가 차단된 경우 화면 상단에 배너가 표시됩니다.
- 배너를 클릭하면 “Users(사용자)” 페이지로 이동합니다. 여기에서 차단된 사용자 목록을 볼 수 있습니다.
- “Users(사용자)” 페이지에는 “User/IP Access(사용자/IP 액세스)”라는 열이 있습니다. 이 열에서 현재 사용자 차단 상태가 표시됩니다.

사용자 액세스를 수동으로 제한 및 관리합니다

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

사용자 액세스 제한 기록

경고 세부 정보 및 사용자 세부 정보 페이지의 사용자 패널에서 사용자의 액세스 제한 기록에 대한 감사(시간, 작업(차단, 차단 해제), 기간, 수행한 작업, NFS에 대한 수동/자동 및 영향을 받는 IP

이 기능을 비활성화하는 방법은 무엇입니까?

언제든지 이 기능을 비활성화할 수 있습니다. 시스템에 제한된 사용자가 있는 경우 먼저 액세스 권한을 복원해야 합니다.

- 워크로드 보안에서 * 워크로드 보안 > 정책 > 자동화된 대응 정책 * 으로 이동합니다. 공격 정책 * 을 선택합니다.
- 선택 취소(선택 취소) _ 사용자 파일 액세스 차단 _.

이 기능은 모든 페이지에서 숨겨집니다.

NFS에 대한 IP를 수동으로 복구합니다

워크로드 보안 평가판이 만료되었거나 에이전트/수집기가 중단된 경우 다음 단계를 사용하여 ONTAP에서 IP를 수동으로 복원합니다.

1. SVM에 모든 엑스포트 정책을 나열하십시오.

```
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. 각 RuleIndex를 지정하여 "cloudsecure_rule"이 Client match인 SVM의 모든 정책 전반에 걸쳐 규칙을 삭제합니다. 워크로드 보안 규칙은 일반적으로 1입니다.

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

```
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.
```

SMB용 사용자를 수동으로 복원합니다

워크로드 보안 평가판이 만료되었거나 에이전트/수집기가 중단된 경우 다음 단계를 사용하여 ONTAP에서 사용자를 수동으로 복원합니다.

사용자 목록 페이지에서 워크로드 보안에서 차단된 사용자 목록을 가져올 수 있습니다.

1. cluster_admin_credentials를 사용하여 ONTAP 클러스터(사용자 차단을 해제할 위치)에 로그인합니다. (Amazon FSx의 경우 FSx 자격 증명으로 로그인합니다.)
2. 다음 명령을 실행하여 모든 SVM에서 SMB용 워크로드 보안으로 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.
```

위 출력에서 두 명의 사용자가 CSLAB 도메인과 함께 차단되었습니다(US030, US040).

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

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

. 다음 명령을 실행하여 사용자의 차단 해제 여부를 확인합니다.

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

이전에 차단한 사용자에 대해서는 어떤 항목도 표시되지 않아야 합니다.

문제 해결

문제	시도해 보십시오
일부 사용자는 공격이 있어도 제한을 받지 않습니다.	1. SVM의 Data Collector 및 Agent가 _running_state인지 확인합니다. Data Collector와 Agent가 중지된 경우 워크로드 보안에서 명령을 전송할 수 없습니다. 2. 이는 사용자가 이전에 사용되지 않은 새 IP를 사용하여 시스템에서 스토리지에 액세스했을 수 있기 때문입니다. 제한은 사용자가 스토리지에 액세스하는 데 사용하는 호스트의 IP 주소를 통해 수행됩니다. 제한된 IP 주소 목록을 보려면 UI(알림 세부 정보 > 이 사용자의 액세스 제한 기록 > 영향을 받는 IP)를 확인하십시오. 사용자가 제한된 IP와 다른 IP를 가진 호스트에서 스토리지에 액세스하는 경우 사용자는 여전히 제한되지 않은 IP를 통해 스토리지를 액세스할 수 있습니다. 사용자가 IP가 제한된 호스트에서 액세스를 시도하는 경우 스토리지를 액세스할 수 없습니다.
액세스 제한을 수동으로 클릭하면 "이 사용자의 IP 주소가 이미 제한되었습니다"라는 메시지가 나타납니다.	제한할 IP가 이미 다른 사용자로부터 제한되어 있습니다.
정책을 수정할 수 없습니다. 원인: 해당 명령에 대해 권한이 없습니다.	CsUser 사용 시, 위에서 설명한 대로 사용자에게 권한이 부여되는지 확인
NFS에 대한 사용자(IP 주소) 차단은 작동하지만 SMB/CIFS에 대해서는 "SID를 DomainName으로 변환하지 못했습니다. 이유 시간 초과: 소켓이 설정되지 않았습니다."	ssh를 수행할 권한이 _CsUser_에 없는 경우 이 문제가 발생할 수 있습니다. (클러스터 레벨에서 접속한 다음 사용자가 ssh를 수행할 수 있는지 확인합니다.) _CsUser_role에는 이러한 권한이 필요합니다. https://docs.netapp.com/us-en/cloudinsights/cs_restrict_user_access.html#prerequisites-for-user-access-blocking cssuser_with cluster credentials의 경우 ONTAP 명령줄에서 다음을 수행하십시오. 보안 로그인 역할 create-role csrole-cmddirname "vserver export-policy rule" -access 모든 보안 로그인 역할 create ONTAP-role
Error Message_SID translate failed. __reason: 255: Error: command failed: 해당 명령에 대해 승인되지 않았습니다. Error: "access-check"는 인식할 수 없는 command _ 입니다. 사용자가 차단되어야 합니다.	이 문제는 _CsUser_에 올바른 권한이 없을 때 발생할 수 있습니다. 자세한 내용은 을 "사용자 액세스 차단을 위한 필수 조건" 참조하십시오. 권한을 적용한 후에는 ONTAP 데이터 수집기 및 사용자 디렉터리 데이터 수집기를 다시 시작하는 것이 좋습니다. 필요한 권한 명령은 다음과 같습니다. --- 보안 로그인 역할 create-role csrole-cmddirname "vserver export-policy rule" - 모든 보안 로그인 역할 create-role csrole-cmdirname "vserver cifs session" - access 모든 보안 로그인 역할 create-role 로그인 역할 -dirname role create -role csrole -cmddirname "vserver name -mapping" -access all-----

워크로드 보안: 공격 시뮬레이션

이 페이지의 지침을 사용하여 포함된 랜섬웨어 시뮬레이션 스크립트를 사용하여 워크로드 보안을 테스트 또는 시연하기 위한 공격을 시뮬레이션할 수 있습니다.

시작하기 전에 주의해야 할 사항

- 랜섬웨어 시뮬레이션 스크립트는 Linux에서만 작동합니다.
- 이 스크립트는 워크로드 보안 에이전트 설치 파일과 함께 제공됩니다. 워크로드 보안 에이전트가 설치된 모든 시스템에서 사용할 수 있습니다.
- 워크로드 보안 에이전트 시스템 자체에서 스크립트를 실행할 수 있으며 다른 Linux 시스템을 준비할 필요가 없습니다. 그러나 스크립트를 다른 시스템에서 실행하려면 스크립트를 복사하여 거기에서 실행하기만 하면 됩니다.

샘플 파일이 **1,000**개 이상 있어야 합니다

이 스크립트는 암호화할 파일이 있는 폴더가 있는 SVM에서 실행되어야 합니다. 해당 폴더 및 하위 폴더 내에 1,000개 이상의 파일이 있는 것이 좋습니다. 파일이 비어 있으면 안 됩니다. 같은 사용자를 사용하여 파일을 만들고 암호화하지 마십시오. 워크로드 보안은 이 작업을 저위험 작업으로 간주하므로 경고를 생성하지 않습니다(즉, 동일한 사용자가 방금 생성한 파일을 수정함).

에 대한 지침은 아래를 "비어 있지 않은 파일을 프로그래밍 방식으로 만듭니다"참조하십시오.

시뮬레이터를 실행하기 전에 필요한 지침:

1. 암호화된 파일이 비어 있지 않은지 확인합니다.
2. 50개 이상의 파일을 암호화해야 합니다. 적은 수의 파일이 무시됩니다.
3. 동일한 사용자로 여러 번 공격을 실행하지 마십시오. 몇 번 지나면 워크로드 보안에서는 이 사용자 동작을 학습하고 이것이 사용자의 정상적인 동작이라고 가정합니다.
4. 동일한 사용자가 방금 만든 파일은 암호화하지 마십시오. 사용자가 방금 만든 파일을 변경하는 것은 위험한 작업으로 간주되지 않습니다. 대신 다른 사용자가 만든 파일을 사용하거나 파일을 만들고 암호화하는 데 몇 시간이 걸릴 수 있습니다.

시스템을 준비합니다

먼저 타겟 볼륨을 시스템에 마운트합니다. NFS 마운트 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 마십시오. Fpolicy에서 지원되지 않습니다.

Linux에서 CIFS를 마운트하려면

```
 mount -t cifs //10.193.77.91/sharedfolderincluster
/root/destinationfolder/ -o username=raisa
```
다음으로 `Data Collector`를 설정합니다.

1. 아직 수행하지 않은 경우 워크로드 보안 에이전트를 구성합니다.
2. 아직 수행하지 않은 경우 SVM 데이터 수집기를 구성합니다.

랜섬웨어 시뮬레이터 스크립트를 실행합니다

1. 워크로드 보안 에이전트 시스템에 로그인(ssh)합니다.
2. _/opt/NetApp/cloudsecure/agent/install_로 이동합니다
3. 매개 변수 없이 시뮬레이터 스크립트를 호출하여 사용 현황을 확인합니다.

```
# pwd
/opt/netapp/cloudsecure/agent/install
# ./ransomware_simulator.sh
Error: Invalid directory  provided.
Usage: ./ransomware_simulator.sh [-e] [-d] [-i <input_directory>]
       -e to encrypt files (default)
       -d to restore files
       -i <input_directory> - Files under the directory to be encrypted
```

```
Encrypt command example: ./ransomware_simulator.sh -e -i
/mnt/audit/reports/
Decrypt command example: ./ransomware_simulator.sh -d -i
/mnt/audit/reports/
```

테스트 파일을 암호화합니다

파일을 암호화하려면 다음 명령을 실행합니다.

```
# ./ransomware_simulator.sh -e -i /root/for/
Encryption key is saved in /opt/netapp/cloudsecure/cloudsecure-agent-
1.251.0/install/encryption-key,
which can be used for restoring the files.
Encrypted /root/for/File000.txt
Encrypted /root/for/File001.txt
Encrypted /root/for/File002.txt
...
```

파일을 복원합니다

암호를 해독하려면 다음 명령을 실행합니다.

```
[root@scspa2527575001 install]# ./ransomware_simulator.sh -d -i /root/for/
File /root/for/File000.txt is restored.
File /root/for/File001.txt is restored.
File /root/for/File002.txt is restored.
...
```

스크립트를 여러 번 실행합니다

사용자에 대한 랜섬웨어 공격을 생성한 후 다른 사용자로 전환하여 추가 공격을 생성하십시오. 워크로드 보안은 사용자 행동을 학습하고 동일한 사용자에 대해 짧은 기간 내에 반복되는 랜섬웨어 공격에 대해 경고하지 않습니다.

프로그래밍 방식으로 파일을 만듭니다

파일을 만들기 전에 먼저 데이터 수집기 처리를 중지하거나 일시 중지해야 합니다. 데이터 수집기를 Agent에 추가하기 전에 다음 단계를 수행하십시오. 이미 데이터 수집기를 추가한 경우 데이터 수집기를 편집하고 잘못된 암호를 입력한 다음 저장합니다. 이렇게 하면 데이터 수집기가 일시적으로 오류 상태가 됩니다. 참고: 원래 암호를 기록해 두십시오!

권장 옵션은 파일을 만들기 전에 하는 것입니다"수집기를 일시 중지합니다".]

시뮬레이션을 실행하기 전에 먼저 암호화할 파일을 추가해야 합니다. 암호화할 파일을 대상 폴더에 수동으로 복사하거나 스크립트(아래 예 참조)를 사용하여 프로그래밍 방식으로 파일을 만들 수 있습니다. 어떤 방법을 사용하든 1,000개 이상의 파일을 복사합니다.

프로그래밍 방식으로 파일을 만들도록 선택한 경우 다음을 수행합니다.

1. 에이전트 상자에 로그인합니다.
2. 파일러의 SVM에서 Agent 시스템으로 NFS 내보내기를 마운트합니다. CD를 해당 폴더에 넣습니다.
3. 이 폴더에서 createfiles.sh 라는 파일을 만듭니다
4. 다음 줄을 해당 파일에 복사합니다.

```
for i in {000..1000}
do
   echo hello > "File${i}.txt"
done
echo 3 > /proc/sys/vm/drop_caches ; sync
```

5. 파일을 저장합니다.
6. 파일에 대한 실행 권한 확인:

```
 chmod 777 ./createfiles.sh
```
. 스크립트를 실행합니다.

```
./createfiles.sh
```

현재 폴더에 1000개의 파일이 생성됩니다.

7. 데이터 수집기를 다시 활성화합니다

   1단계에서 데이터 수집기를 비활성화한 경우 데이터 수집기를 편집하고 올바른 암호를 입력한 후 저장합니다. 데이터 수집기가 다시 실행 중 상태인지 확인합니다.

8. 다음 단계를 수행하기 전에 수집기를 일시 중지한 경우 을 "수집기를 다시 시작합니다"참조하십시오.

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

워크로드 보안 경고 수신자를 구성하려면 * Admin > Notifications * 를 클릭하고 각 수신자의 적절한 섹션에 이메일 주소를 입력합니다.

잠재적 공격 경고 및 경고

potential attack_alert 알림을 보내려면 _ Send potential attack Alerts _ 섹션에 받는 사람의 전자 메일 주소를 입력합니다. e-메일 알림은 알림의 모든 작업에 대해 알림 받는 사람 목록으로 전송됩니다.

*Warning_notifications*를 보내려면 *_Send Warning Alerts* 섹션에 받는 사람의 이메일 주소를 입력합니다.

에이전트 및 **Data Collector** 상태 모니터링

알림을 통해 에이전트 및 데이터 소스의 상태를 모니터링할 수 있습니다.

에이전트 또는 데이터 소스 수집기가 작동하지 않는 경우 알림을 받으려면 _ 데이터 수집 상태 경고 _ 섹션에 받는 사람의 전자 메일 주소를 입력합니다.

다음 사항에 유의하십시오.

- 상태 알림은 에이전트/수집기가 최소 1시간 동안 보고를 중지한 후에만 전송됩니다.
- 특정 24시간 동안 에이전트 또는 데이터 수집기의 연결이 끊어진 경우에도 지정된 수신자에게 하나의 이메일 알림만 전송됩니다.
- Agent가 고장 날 경우 한 번에 하나의 경고가 전송됩니다(수집기당 1개가 아님). 이메일에는 영향을 받는 모든 SVM의 목록이 포함됩니다.
- Active Directory 수집 장애는 경고로 보고되며 랜섬웨어 감지에 영향을 주지 않습니다.
- 이제 시작 설정 목록에 새 _Configure email notifications_단계가 포함됩니다.

Agent 및 Data Collector 업그레이드 알림을 받는 중입니다

- "Data Collection Health Alerts"에 이메일 ID를 입력합니다.
- "업그레이드 알림 활성화" 확인란이 활성화됩니다.
- 에이전트 및 Data Collector 업그레이드 이메일 알림은 계획된 업그레이드 하루 전에 이메일 ID로 전송됩니다.

문제 해결

* 문제: *	* 사용해 보세요. *
이메일 ID가 "Data Collector Health Alerts"에 있지만 알림을 받지 않습니다.	알림 이메일은 NetApp Data Infrastructure Insights 도메인, 즉 _accounts@service.clou dinsights.NetApp.com_에서 발송되었습니다. 일부 회사는 외부 도메인에서 보낸 전자 메일을 차단합니다. NetApp Data Infrastructure Insights 도메인의 외부 알림을 화이트리스트로 등록했는지 확인합니다.

워크로드 보안 API

워크로드 보안 API를 통해 NetApp 고객과 ISV(독립 소프트웨어 공급업체)는 워크로드 보안을 CMDB 또는 기타 티켓 시스템과 같은 다른 애플리케이션과 통합할 수 있습니다.

API 액세스 요구 사항:

- 액세스 권한을 부여하기 위해 API 액세스 토큰 모델이 사용됩니다.
- API 토큰 관리는 관리자 역할을 가진 워크로드 보안 사용자에 의해 수행됩니다.

API 설명서(Swagger)

최신 API 정보는 Workload Security에 로그인하고 * Admin > API Access * 로 이동하여 확인할 수 있습니다. API Documentation * 링크를 클릭합니다. API 설명서는 Swagger 기반이며 API에 대한 간략한 설명 및 사용 정보를 제공하고 테넌트에서 시험해 볼 수 있습니다.

Forensics Activity API를 호출하는 경우 cloudsecure_forensics.activities. * v2 * API를 사용합니다. 이 API를 여러 번 호출하는 경우 호출이 병렬로 발생하지 않고 순차적으로 발생했는지 확인합니다. 여러 병렬 호출로 인해 API 시간이 초과될 수 있습니다.

API 액세스 토큰

워크로드 보안 API를 사용하기 전에 하나 이상의 * API 액세스 토큰 * 을 생성해야 합니다. 액세스 토큰은 읽기 권한을 부여합니다. 각 액세스 토큰의 만료일을 설정할 수도 있습니다.

액세스 토큰을 만들려면 다음을 수행합니다.

- Admin > API Access * 를 클릭합니다
- API 액세스 토큰 * 을 클릭합니다
- 토큰 이름 * 을 입력합니다

- 토큰 만료 * 를 지정합니다

> 토큰은 클립보드로 복사하고 생성 과정 중에 저장하는 경우에만 사용할 수 있습니다. 토큰을 만든 후에는 검색할 수 없으므로 토큰을 복사하여 안전한 위치에 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 고객의 관점에서 API에 대한 일반 용도의 액세스를 허용하여 자체 테넌트의 범위에서 API에 대한 액세스를 관리합니다.

응용 프로그램은 사용자가 액세스를 성공적으로 인증 및 승인한 후 액세스 토큰을 받은 다음 대상 API를 호출할 때 액세스 토큰을 자격 증명으로 전달합니다. 전달된 토큰은 API에 토큰의 베어러가 API에 액세스할 수 있는 권한이 있음을 알리고 권한 부여 중에 부여된 범위에 따라 특정 작업을 수행하도록 합니다.

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

예를 들어, 다음을 사용하여 스토리지 자산을 검색할 수 있습니다.

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

여기서 _<API_Access_Token>_은 API 액세스 키를 생성하는 동안 저장한 토큰입니다.

자세한 정보는 * Admin > API Access * 의 _API Documentation_link에서 확인할 수 있습니다.

API를 통해 데이터를 추출하는 스크립트

워크로드 보안 에이전트에는 요청된 시간 범위를 더 작은 배치로 나누어 v2 API에 대한 병렬 호출을 용이하게 하기 위한 내보내기 스크립트가 포함되어 있습니다.

스크립트는 _/opt/NetApp/cloudsecure/agent/export-script _ 에 있습니다. 동일한 디렉토리에 있는 README 파일은 사용 지침을 제공합니다.

다음은 스크립트를 호출하는 명령 예입니다.

```
python3 data-export.py --tenant_url <tenant
id>.cs01.cloudinsights.netapp.com --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 파라미터: - `--iteration_interval 12`: 요청한 시간 범위를 12시간 간격으로 분할합니다.
`--num_workers 3`-: 3개의 스레드를 사용하여 이러한 간격을 병렬로 가져옵니다.