시작하기
Data Infrastructure Insights

NetApp
January 10, 2025

목차

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.

구성 요소	**Linux** 요구 사항
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
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.

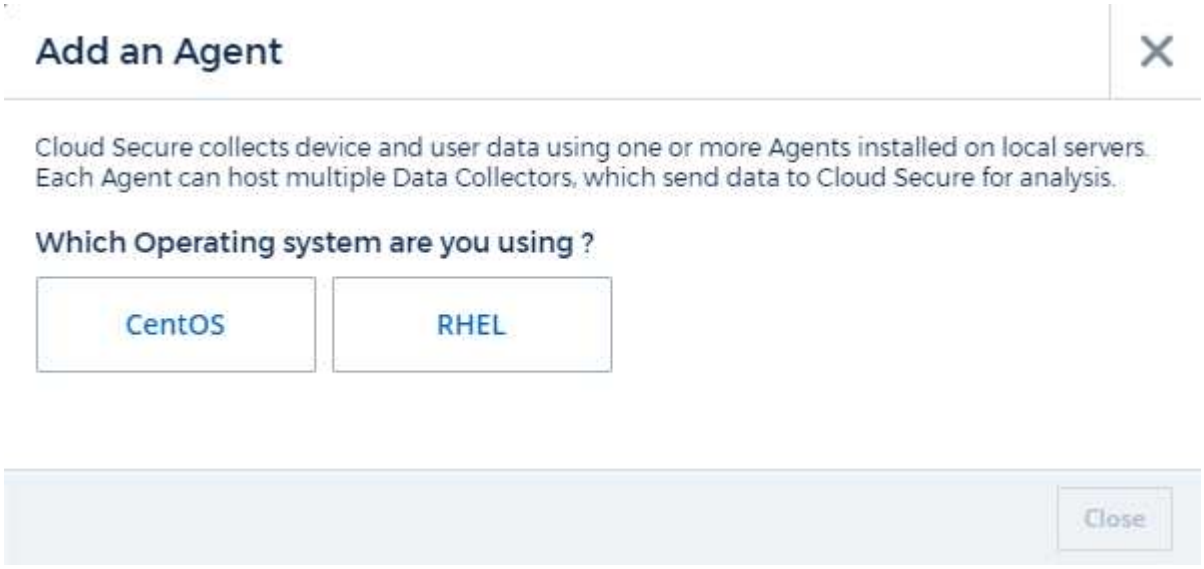
시작하기 전에

- 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.

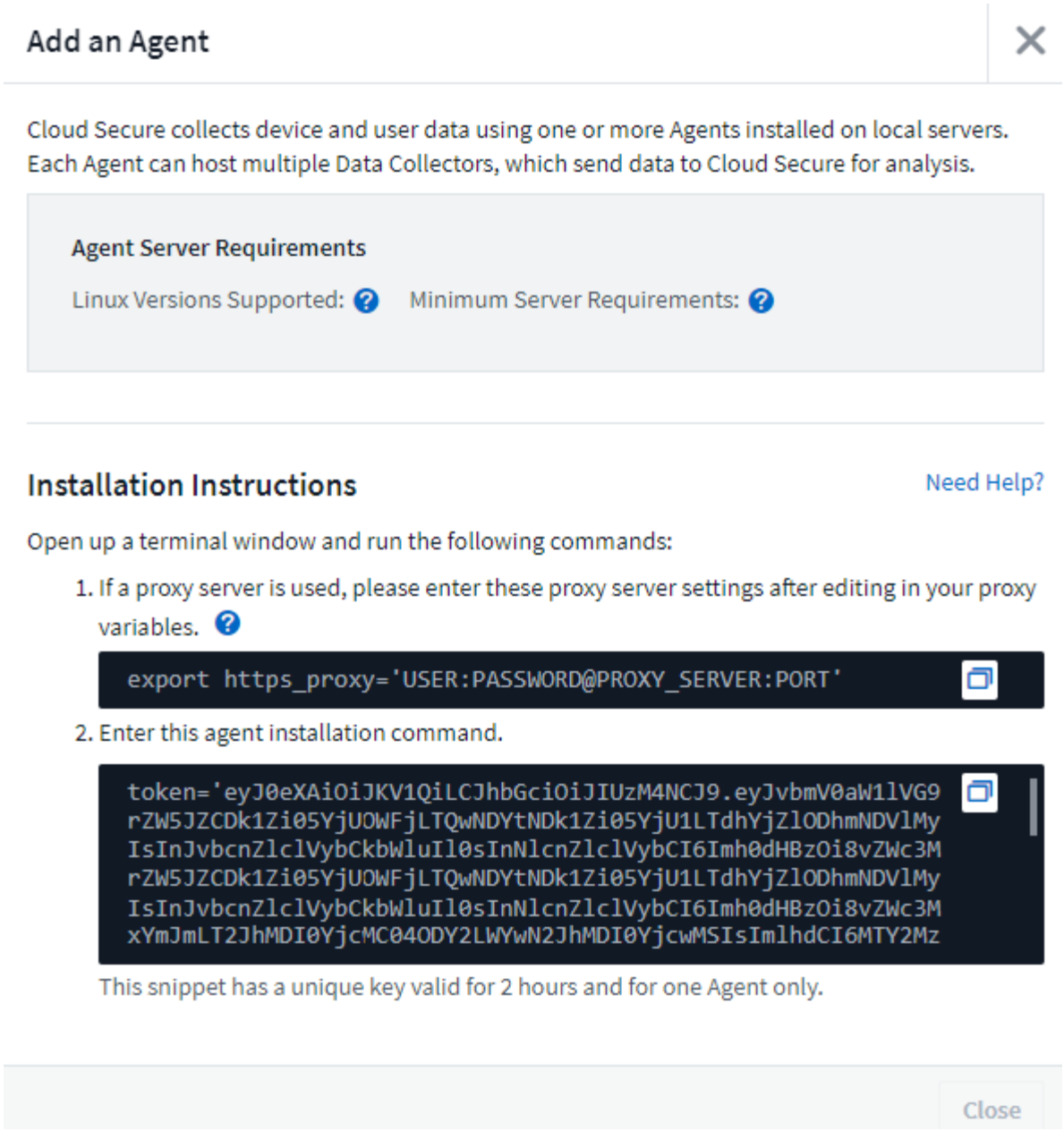
Agent 설치 단계

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
```

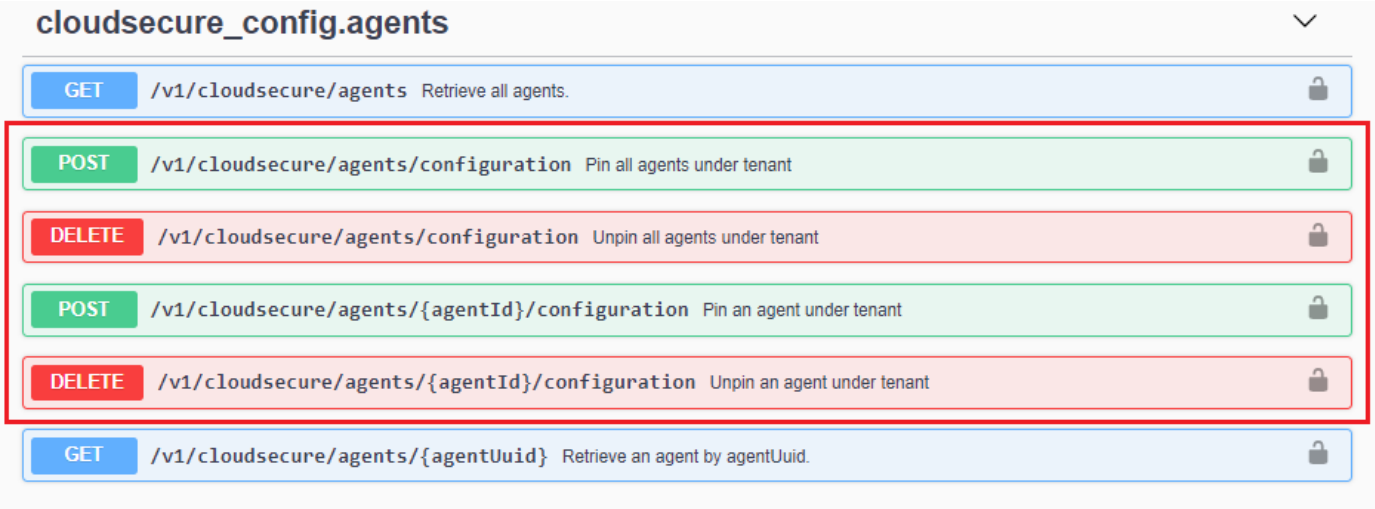
현재 버전에서 에이전트 "고정"

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.

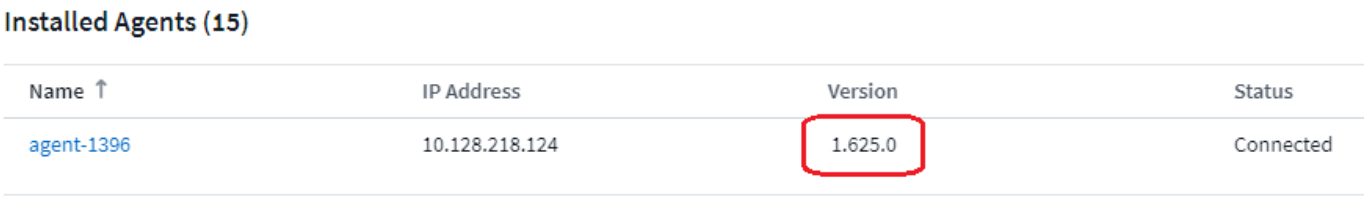
이러한 각 경우에 에이전트는 다음 워크로드 보안 새로 고침 시 업데이트됩니다.

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

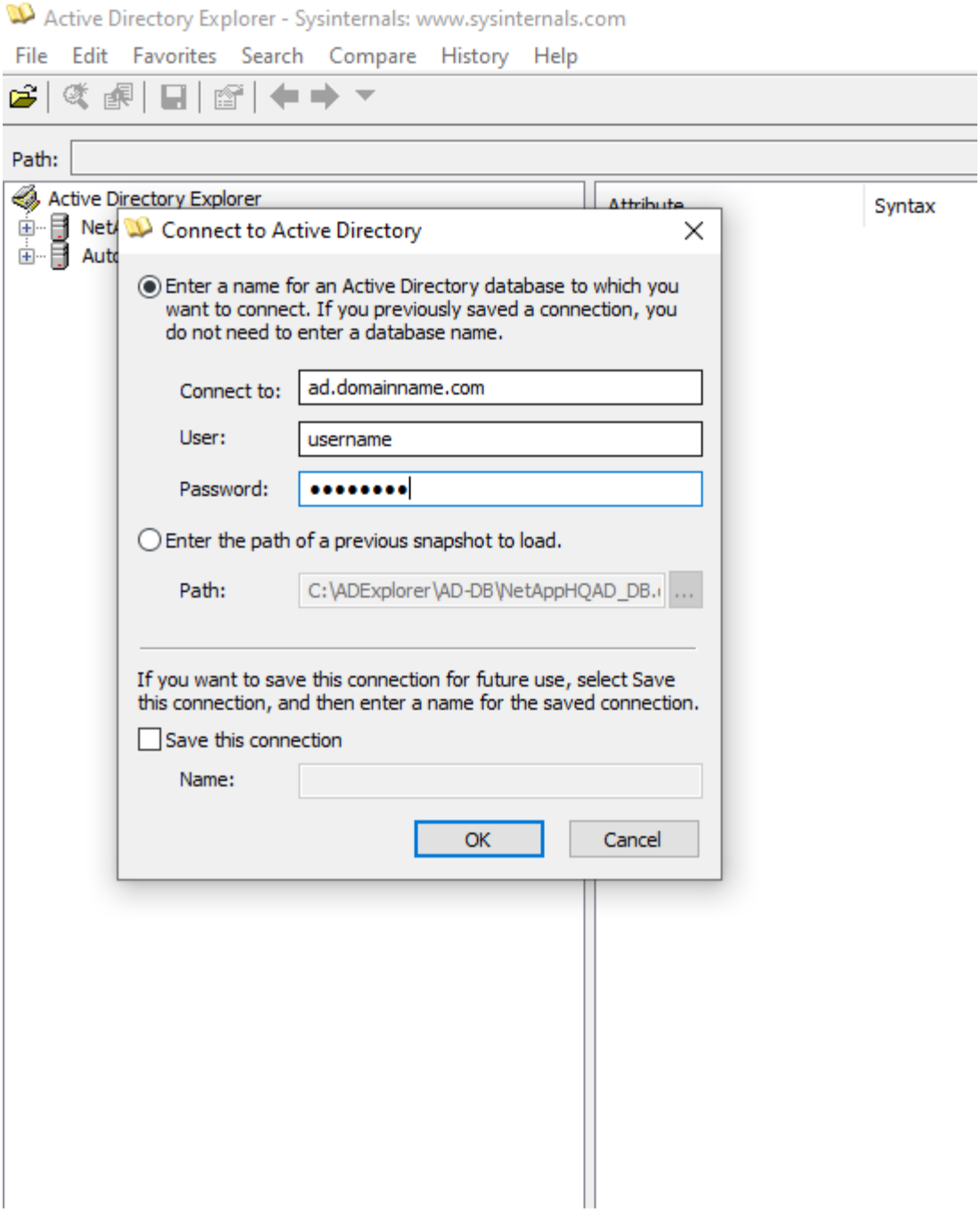
사용자 디렉토리 수집기 구성을 테스트하는 중입니다

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

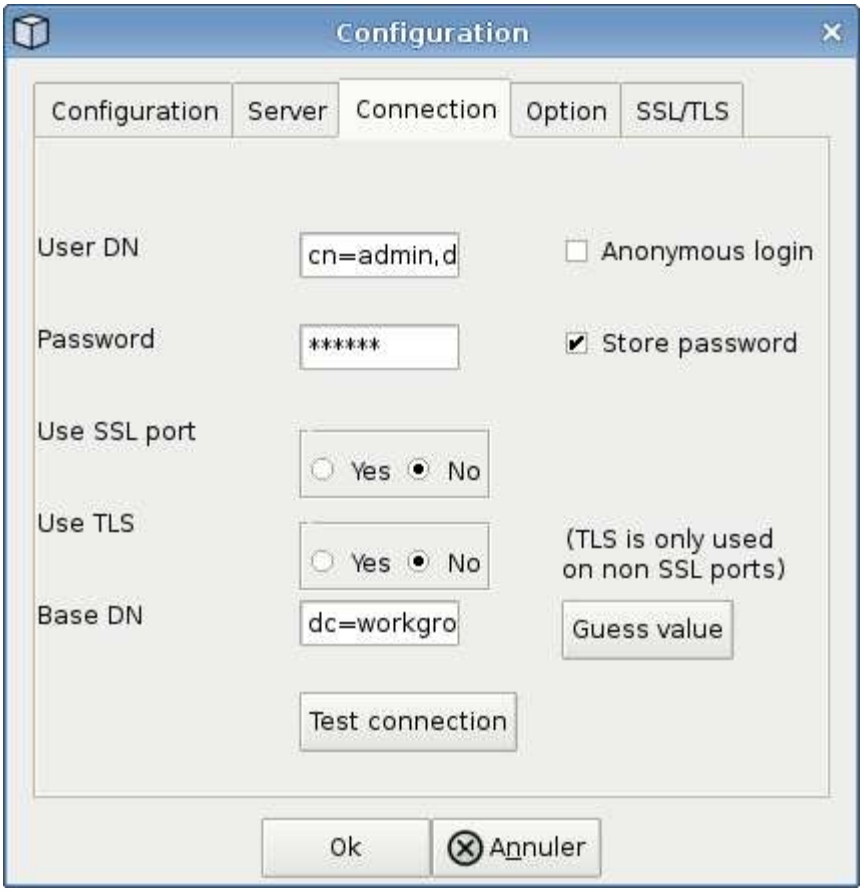
사용자 디렉토리 수집기 구성을 테스트하는 중입니다

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.