



시작하기

Data Infrastructure Insights

NetApp
February 11, 2026

This PDF was generated from https://docs.netapp.com/ko-kr/data-infrastructure-insights/task_cs_getting_started.html on February 11, 2026. Always check docs.netapp.com for the latest.

목차

시작하기	1
워크로드 보안 시작하기	1
워크로드 보안 에이전트 요구 사항	1
추가 권장 사항	2
클라우드 네트워크 액세스 규칙	2
네트워크 내 규칙	4
시스템 크기 조정	5
워크로드 보안 에이전트 배포	5
시작하기 전에	5
모범 사례	6
에이전트 설치 단계	6
네트워크 구성	8
현재 버전에서 에이전트 "고정"	8
에이전트 오류 문제 해결	9
워크로드 보안 에이전트 삭제	12
에이전트 삭제	12
Active Directory(AD) 사용자 디렉터리 수집기 구성	13
사용자 디렉터리 수집기 구성 테스트	14
사용자 디렉터리 수집기 구성 오류 문제 해결	15
LDAP 디렉터리 서버 수집기 구성	17
사용자 디렉터리 수집기 구성 테스트	19
LDAP 디렉터리 수집기 구성 오류 문제 해결	20
ONTAP SVM 데이터 수집기 구성	22
시작하기 전에	22
데이터 수집기를 위한 테스트 연결	24
ONTAP 다중 관리자 확인(MAV) 시 유의 사항	25
사용자 액세스 차단을 위한 전제 조건	25
권한에 대한 참고 사항	25
데이터 수집기 구성	28
MetroCluster 에 권장되는 구성	29
서비스 정책	30
재생-일시 정지 데이터 수집기	30
영구 저장소	30
수집기 마이그레이션	31
문제 해결	32
ONTAP SVM 데이터 수집기 문제 해결	32
Amazon FSx for NetApp ONTAP Cloud Volumes ONTAP 및 Amazon FSx 구성	38
Cloud Volumes ONTAP 스토리지 구성	39
지원 플랫폼	39

에이전트 머신 구성	39
Workload Security Agent 설치	39
문제 해결	40
사용자 관리	40
이벤트 발생률 확인 도구: 에이전트 규모 산정 가이드	41
요구 사항:	41
예	42
문제 해결	44

시작하기

워크로드 보안 시작하기

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

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

데이터 수집을 시작하려면 먼저 다음을 구성해야 합니다.

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

워크로드 보안은 다른 도구와도 통합될 수 있습니다. 예를 들어, "[이 가이드를 참조하세요](#)" Splunk와의 통합에 관하여.

워크로드 보안 에이전트 요구 사항

최적의 모니터링 및 위협 탐지 성능을 보장하려면 최소 운영 체제, CPU, 메모리 및 디스크 공간 요구 사항을 충족하는 전용 서버에 Workload Security 에이전트를 배포하십시오. 이 가이드에서는 "[Workload Security 에이전트 설치](#)" 전에 필요한 하드웨어 및 네트워크 요구 사항을 명시하며, 지원되는 Linux 배포판, 네트워크 연결 규칙 및 시스템 크기 조정 지침을 포함합니다.

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

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

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

추가 권장 사항

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

클라우드 네트워크 액세스 규칙

미국 기반 워크로드 보안 환경의 경우:

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

유럽 기반 워크로드 보안 환경의 경우:

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

APAC 기반 워크로드 보안 환경의 경우:

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

네트워크 내 규칙

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

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

시스템 크기 조정

를 참조하십시오 ["이벤트 요금 확인기"](#) 사이즈에 대한 정보는 설명서를 참조하세요.

워크로드 보안 에이전트 배포

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

시작하기 전에

- 설치, 스크립트 실행, 설치 제거에는 sudo 권한이 필요합니다.
- 에이전트를 설치하는 동안 로컬 사용자 `_cssys_`와 로컬 그룹 `_cssys_`가 머신에 생성됩니다. 권한 설정에서 로컬 사용자 생성을 허용하지 않고 대신 Active Directory가 필요한 경우, 사용자 이름이 `_cssys_`인 사용자를 Active Directory 서버에 만들어야 합니다.
- Data Infrastructure Insights 보안에 대해 읽어보세요. ["여기"](#).

모범 사례

Workload Security 에이전트를 구성하기 전에 다음 사항을 염두에 두십시오.

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

에이전트 설치 단계

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

시스템에 에이전트 추가 페이지가 표시됩니다.

Add an Agent

×

Cloud Secure collects device and user data using one or more Agents installed on local servers. Each Agent can host multiple Data Collectors, which send data to Cloud Secure for analysis.

Which Operating system are you using ?

CentOS

RHEL

Close

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

Linux Versions Supported: [?](#) Minimum Server Requirements: [?](#)

네트워크 구성

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

단계

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

플랫폼에 따라 다음 단계를 따르세요.

CentOS 7.x / RHEL 7.x:

1. `sudo iptables-save | grep 35000`

샘플 출력:

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

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

샘플 출력:

```
35000-55000/tcp
```

현재 버전에서 에이전트 "고정"

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

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

각각의 경우에서 에이전트는 다음 워크로드 보안 업데이트 시 업데이트됩니다.

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

cloudsecure_config.agents



GET /v1/cloudsecure/agents Retrieve all agents.



POST /v1/cloudsecure/agents/configuration Pin all agents under tenant



DELETE /v1/cloudsecure/agents/configuration Unpin all agents under tenant



POST /v1/cloudsecure/agents/{agentId}/configuration Pin an agent under tenant



DELETE /v1/cloudsecure/agents/{agentId}/configuration Unpin an agent under tenant



GET /v1/cloudsecure/agents/{agentUuid} Retrieve an agent by agentUuid.



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

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

Installed Agents (15)

Name ↑	IP Address	Version	Status
agent-1396	10.128.218.124	1.625.0	Connected

에이전트 오류 문제 해결

알려진 문제와 해결 방법은 다음 표에 설명되어 있습니다.

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

문제:	해결:
에이전트가 설치되어 실행 중입니다. 하지만 요원이 갑자기 멈췄습니다.	에이전트 머신에 SSH를 실행합니다. 에이전트 서비스 상태를 확인하세요. <code>sudo systemctl status cloudsecure-agent.service</code> . 1. 로그에 "Workload Security 데몬 서비스를 시작하지 못했습니다"라는 메시지가 표시되는지 확인하세요. 2. 에이전트 머신에 <code>cssys</code> 사용자가 있는지 확인하세요. 루트 권한으로 다음 명령을 하나씩 실행하고 <code>cssys</code> 사용자와 그룹이 있는지 확인하세요. <code>sudo id cssys</code> <code>sudo groups cssys</code> 3. 해당 사항이 없다면 중앙 모니터링 정책으로 인해 <code>cssys</code> 사용자가 삭제되었을 수 있습니다. 4. 다음 명령을 실행하여 <code>cssys</code> 사용자와 그룹을 수동으로 생성합니다. <code>sudo useradd cssys</code> <code>sudo groupadd cssys</code> 5. 다음 명령을 실행하여 에이전트 서비스를 다시 시작합니다. <code>sudo systemctl restart cloudsecure-agent.service</code> 6. 그래도 실행되지 않으면 다른 문제 해결 옵션을 확인해 보세요.
에이전트에 50개 이상의 데이터 수집기를 추가할 수 없습니다.	에이전트에 추가할 수 있는 데이터 수집기는 최대 50개입니다. 여기에는 Active Directory, SVM 및 기타 수집기 등 모든 수집기 유형이 결합될 수 있습니다.
UI에서 에이전트가 NOT_CONNECTED 상태임을 표시합니다.	에이전트를 다시 시작하는 단계입니다. 1. 에이전트 머신에 SSH를 실행합니다. 2. 다음 명령을 실행하여 에이전트 서비스를 다시 시작합니다. <code>sudo systemctl restart cloudsecure-agent.service</code> 3. 에이전트 서비스 상태를 확인하세요. <code>sudo systemctl status cloudsecure-agent.service</code> . 4. 에이전트는 CONNECTED 상태로 전환되어야 합니다.
에이전트 VM이 Zscaler 프록시 뒤에 있어 에이전트 설치에 실패했습니다. Zscaler 프록시의 SSL 검사로 인해 워크로드 보안 인증서는 Zscaler CA에서 서명한 것처럼 표시되므로 에이전트는 통신을 신뢰하지 않습니다.	Zscaler 프록시에서 *.cloudinsights.netapp.com URL에 대한 SSL 검사를 비활성화합니다. Zscaler가 SSL 검사를 수행하고 인증서를 교체하는 경우 Workload Security는 작동하지 않습니다.
에이전트를 설치하는 동안 압축을 풀면 설치가 중단됩니다.	" <code>chmod 755 -Rf</code> " 명령이 실패합니다. 작업 디렉토리에 다른 사용자의 파일이 있고 해당 파일의 권한을 변경할 수 없는 루트가 아닌 <code>sudo</code> 사용자가 에이전트 설치 명령을 실행하면 명령이 실패합니다. <code>chmod</code> 명령이 실패하여 나머지 설치 과정이 실행되지 않습니다. 1. "cloudsecure"라는 이름의 새 디렉토리를 만듭니다. 2. 해당 디렉토리로 가세요. 3. 전체 " <code>token=.....</code> ... <code>./cloudsecure-agent-install.sh</code> " 설치 명령을 복사하여 붙여넣고 Enter를 누릅니다. 4. 설치가 진행될 것입니다.

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

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

워크로드 보안 에이전트 삭제

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

에이전트 삭제



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

시작하기 전에

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

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

에이전트를 삭제하는 단계:

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

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

2. *워크로드 보안 > 수집기 > 에이전트*를 클릭합니다.

시스템은 구성된 에이전트 목록을 표시합니다.

3. 삭제할 에이전트의 옵션 메뉴를 클릭합니다.

4. *삭제*를 클릭하세요.

시스템에 에이전트 삭제 페이지가 표시됩니다.

5. 삭제를 확인하려면 *삭제*를 클릭하세요.

Active Directory(AD) 사용자 디렉터리 수집기 구성

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

시작하기 전에

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

사용자 디렉터리 수집기를 구성하는 단계

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

시스템에 사용자 디렉터리 추가 화면이 표시됩니다.

다음 표에 필요한 데이터를 입력하여 사용자 디렉터리 수집기를 구성합니다.

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

BIND 비밀번호	디렉토리 서버 비밀번호(즉, Bind DN에 사용되는 사용자 이름에 대한 비밀번호)
규약	ldap, ldaps, ldap-start-tls
포트	포트 선택

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

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

다음 속성을 추가하려면 '선택적 속성 포함'을 클릭하세요.

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

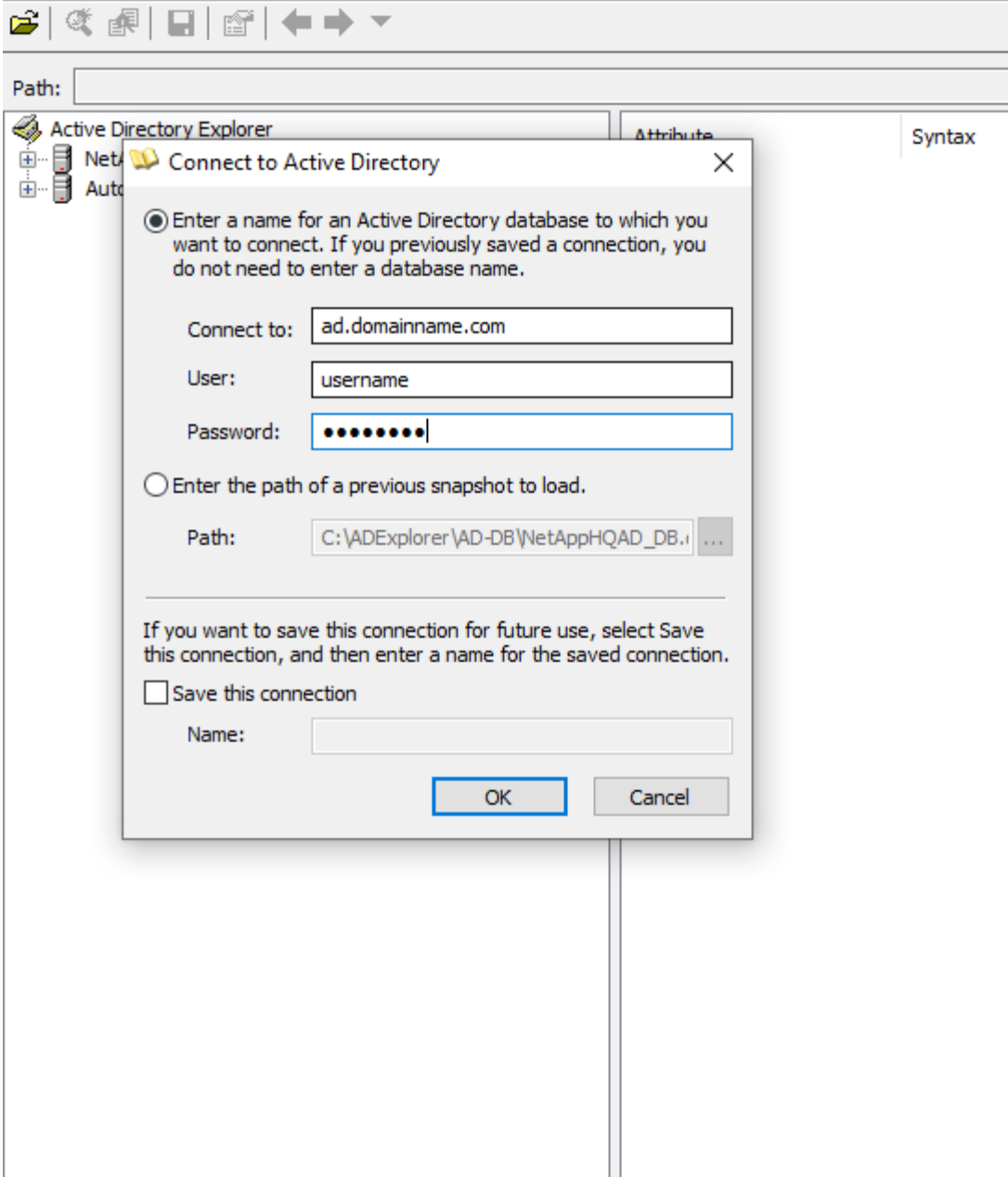
사용자 디렉토리 수집기 구성 테스트

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

- 다음 명령을 사용하여 Workload Security LDAP 사용자 권한을 확인합니다.

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

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



사용자 디렉터리 수집기 구성 오류 문제 해결

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

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

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

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

LDAP 디렉토리 서버 수집기 구성

LDAP 디렉터리 서버에서 사용자 속성을 수집하도록 Workload Security를 구성합니다.

시작하기 전에

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

사용자 디렉터리 수집기를 구성하는 단계

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

시스템에 사용자 디렉터리 추가 화면이 표시됩니다.

다음 표에 필요한 데이터를 입력하여 사용자 디렉터리 수집기를 구성합니다.

이름	설명
이름	사용자 디렉터리의 고유한 이름입니다. 예를 들어 <i>GlobalLDAPCollector</i>

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

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

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

다음 속성을 추가하려면 '선택적 속성 포함'을 클릭하세요.

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

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

사용자 디렉토리 수집기 구성 테스트

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

- 다음 명령을 사용하여 Workload Security LDAP 사용자 권한을 확인합니다.

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

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

LDAP 디렉터리 수집기 구성 오류 문제 해결

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

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

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

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

ONTAP SVM 데이터 수집기 구성

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

시작하기 전에

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

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

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

출력 예

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

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

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

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

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

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

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

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

데이터 수집기를 위한 테스트 연결

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

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



사용자 디렉토리 수집기에서는 테스트 연결이 지원되지 않습니다.

연결 테스트를 위한 전제 조건

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

Save Collector

Test Connection



반드시 검토하세요 [권한](#) 아래 섹션도 참조하세요.

연결 테스트

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

Add ONTAP SVM

[Need Help?](#)

An Agent is required to fetch data from the ONTAP SVM in to Storage Workload Security

Network Checks:

Https: Connection successful on port 443 (AGENT -> ONTAP)

Ontap Version: 9.14.1

Data Lifs: Found 1 (10.10.10.10) data interfaces in the SVM which contains service name data-fpolicy-client, admin/oper status as up.

Agent IP: Determined agent IP address to be used (10.10.10.10)

✔ Fpolicy Server: Connection successful on Agent IP (10.10.10.10), ports [35037, 35038, 35039] (ONTAP -> AGENT)

Features (User has permissions):

Snapshot, Ems, Access Denied, Persistent Store, Ontap ARP, User Blocking

Features (User does not have permissions):

Protobuf: Ontap version 9.14.1 is below minimum supported version 9.15.0

ONTAP 다중 관리자 확인(MAV) 시 유의 사항

스냅샷 생성 및 삭제 또는 사용자 차단(SMB)과 같은 일부 기능은 사용 중인 ONTAP 버전에 추가된 MAV 명령에 따라 작동하지 않을 수 있습니다.

아래 단계에 따라 MAV 명령에 제외를 추가하여 Workload Security에서 스냅샷을 생성 또는 삭제하고 사용자를 차단할 수 있도록 합니다.

스냅샷 생성 및 삭제를 허용하는 명령:

```
multi-admin-verify rule modify -operation "volume snapshot create" -query  
"-snapshot !*cloudsecure_*"  
multi-admin-verify rule modify -operation "volume snapshot delete" -query  
"-snapshot !*cloudsecure_*"
```

사용자 차단을 허용하는 명령어:

```
multi-admin-verify rule delete -operation set
```

사용자 액세스 차단을 위한 전제 조건

다음 사항을 염두에 두십시오. **"사용자 접근 차단"** :

이 기능을 사용하려면 클러스터 수준 자격 증명이 필요합니다.

클러스터 관리 자격 증명을 사용하는 경우 새로운 권한이 필요하지 않습니다.

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

권한에 대한 참고 사항

*클러스터 관리 IP*를 통해 추가할 때의 권한:

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

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

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

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

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

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

Vserver 관리 IP를 통해 추가할 때의 권한:

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

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

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

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

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

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

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

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

프로토콜 버퍼 모드

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

이 기능에 대한 자세한 내용은 다음에서 확인할 수 있습니다. ["ONTAP 문서"](#).

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

클러스터 모드:

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

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

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

클러스터 관리 자격 증명을 사용하는 경우 새로운 권한이 필요하지 않습니다.

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

자세한 내용은 다음을 읽어보세요. ["ONTAP 액세스와의 통합이 거부되었습니다."](#)

그리고 ["ONTAP 자율형 랜섬웨어 보호와 통합"](#)

데이터 수집기 구성

구성 단계

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

시스템은 사용 가능한 데이터 수집기를 표시합니다.

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

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

필드	설명
이름	데이터 수집기의 고유 이름
대리인	목록에서 구성된 에이전트를 선택합니다.
관리 IP를 통해 연결:	클러스터 IP 또는 SVM 관리 IP를 선택하세요

클러스터/SVM 관리 IP 주소	위에서 선택한 내용에 따라 클러스터 또는 SVM의 IP 주소가 결정됩니다.
SVM 이름	SVM의 이름(클러스터 IP를 통해 연결할 때 이 필드가 필요합니다)
사용자 이름	SVM/클러스터에 액세스하기 위한 사용자 이름 클러스터 IP를 통해 추가하는 경우 옵션은 다음과 같습니다. 1. 클러스터 관리자 2. 'csuser' 3. AD 사용자는 csuser와 비슷한 역할을 합니다. SVM IP를 통해 추가할 때 옵션은 다음과 같습니다. 4. vsadmin 5. 'csuser' 6. csuser와 비슷한 역할을 하는 AD 사용자 이름입니다.
비밀번호	위 사용자 이름에 대한 비밀번호
공유/볼륨 필터링	이벤트 수집에서 공유/볼륨을 포함할지 또는 제외할지 선택하세요.
제외/포함할 전체 공유 이름을 입력하세요.	이벤트 수집에서 제외하거나 포함할(해당되는 경우) 공유의 심표로 구분된 목록
제외/포함할 전체 볼륨 이름을 입력하세요.	이벤트 수집에서 제외하거나 포함할 볼륨의 심표로 구분된 목록(해당되는 경우)
폴더 액세스 모니터링	이 옵션을 선택하면 폴더 액세스 모니터링 이벤트가 활성화됩니다. 이 옵션을 선택하지 않아도 폴더 생성/이름 변경 및 삭제가 모니터링됩니다. 이 기능을 활성화하면 모니터링되는 이벤트 수가 늘어납니다.
ONTAP 전송 버퍼 크기 설정	ONTAP Fpolicy 전송 버퍼 크기를 설정합니다. 9.8p7 이전의 ONTAP 버전을 사용하고 성능 문제가 발생하는 경우 ONTAP 전송 버퍼 크기를 변경하여 ONTAP 성능을 향상시킬 수 있습니다. 이 옵션이 보이지 않고 이에 대해 알아보고 싶다면 NetApp 지원팀에 문의하세요.

당신이 완료한 후

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

MetroCluster 에 권장되는 구성

MetroCluster 에 권장되는 사항은 다음과 같습니다.

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

서비스 정책

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

예:

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

ONTAP 9.9.1 이전 버전에서는 `_data-fpolicy-client_`를 설정할 필요가 없습니다.

재생-일시 정지 데이터 수집기

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

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



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

다음 사항을 명심하세요.

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

영구 저장소

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

영구 저장소는 수집기 편집/추가 페이지에서 확인란을 선택하여 활성화할 수 있습니다. 체크박스를 선택하면 볼륨

이름을 입력할 수 있는 텍스트 필드가 표시됩니다. 볼륨 이름은 영구 저장소를 활성화하는 데 필요한 필수 필드입니다.

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

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

클러스터 모드:

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

Vserver 모드:

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

수집기 마이그레이션

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

필수 조건

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

메모:

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

수집기 마이그레이션

수집기를 마이그레이션하려면 다음 단계를 따르세요.

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

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

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

Edit ONTAP SVM

Name*

Agent

fp-cs-1-agent (CONNECTED)
agent-1537 (CONNECTED)
agent-jptsc (CONNECTED)
fp-cs-1-agent (CONNECTED)
fp-cs-2-agent (CONNECTED)
GSSC_girton (CONNECTED)

Connect via Management IP for:
☒ Cluster
☐ SVM

문제 해결

를 참조하십시오"[SVM 수집기 문제 해결](#)" 문제 해결 팁을 보려면 여기를 클릭하세요.


ONTAP SVM 데이터 수집기 문제 해결

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

를 참조하십시오"[SVM 수집기 구성](#)" 이 수집기를 구성하는 방법에 대한 지침은 페이지를 참조하세요.

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

Installed Data Collectors

Name	Status	Type	Agent
9.8_vs1	 Error more detail	ONTAP SVM	agent-11

알려진 문제와 해결 방법은 아래와 같습니다.

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

연결이 끊어졌을 때 CloudSecure에서 최대 트래픽을 확인하세요. **CloudSecure > 활동 포렌식 > 모든 활동**

페이지에서 확인할 수 있습니다.

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

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

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

크기를 조정한 후 UI에서 수집기를 다시 시작합니다.

{비어 있는}

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

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

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

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

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

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

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

```
https://<cluster_mgmt_ip>/spi/<clustername>/etc/log/packet_traces/
```

.. ONTAP 에서 Agent 상자로 SYN이 있는지 확인하세요.
.. ONTAP 에서 SYN이 없으면 ONTAP 의 방화벽에 문제가 있습니다.
.. ONTAP 에서 방화벽을 열어 ONTAP 에이전트 상자에 연결할 수 있도록 합니다.

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

{비어 있는}

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

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

{비어 있는}

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

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

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

샘플 출력은 다음과 같습니다.

```
-A IN_public_allow -p tcp -m tcp --dport 35000 -m conntrack -ctstate  
NEW -j ACCEPT
```

. SVM에 로그인하고 다음 명령을 입력한 후 ONTAP 과의 통신을 차단하는 방화벽이 설정되어
있지 않은지 확인합니다.

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

"방화벽 명령 확인"ONTAP 측에서.

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

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

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

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

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

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

{비어 있는}

문제: 활동 페이지에서 이벤트가 보이지 않습니다. 이걸 시도해보세요:

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

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

fpolicy와 관련된 오류가 없는지 확인하세요.

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

```
<SVM>fpolicy show
```

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

{비어 있는}

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

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

{비어 있는}

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

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

"방화벽 명령 확인" ONTAP 측에서.

{비어 있는}

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

{비어 있는}

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

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

{비어 있는}

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

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

{비어 있는}

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

fpolicy 목록을 표시하는 CLI 명령:

```
fpolicy show
```

fpolicy 구성을 삭제하는 단계:

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

{비어 있는}

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

{비어 있는}

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

1. 데이터 수집기 페이지에서 오류가 발생한 데이터 수집기의 오른쪽으로 스크롤하여 3개 점 메뉴를 클릭합니다. 편집
_을 선택하세요. 데이터 수집기의 비밀번호를 다시 입력하세요. _저장 버튼을 눌러 데이터 수집기를 저장합니다.
데이터 수집기가 다시 시작되면 오류가 해결될 것입니다.

2. 에이전트 머신에는 CPU나 RAM 여유 공간이 충분하지 않아 DSC가 실패하는 것입니다. 머신의 에이전트에 추가된 데이터 수집기의 수를 확인하세요. 20이 넘을 경우, Agent 머신의 CPU와 RAM 용량을 늘려주세요. CPU와 RAM이 늘어나면 DSC는 초기화 상태로 전환되고, 그다음에는 자동으로 실행 상태로 전환됩니다. 사이즈 가이드를 살펴보세요"[이 페이지](#)".

{비어 있는}

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

{비어 있는}

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

권한이 설정되면 수집기를 다시 시작합니다.

{비어 있는}

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

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

{비어 있는}

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

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

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

Cloud Volumes ONTAP 스토리지 구성

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

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

지원 플랫폼

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

에이전트 머신 구성

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

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

AWS에서 다음 단계에 따라 워크로드 보안 에이전트로 사용할 머신을 구성합니다.

다음 단계에 따라 워크로드 보안 에이전트로 사용할 머신을 구성하세요.

단계

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

Workload Security Agent 설치

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

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

문제 해결

알려진 문제와 해결 방법은 다음 표에 설명되어 있습니다.

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

사용자 관리

워크로드 보안 사용자 계정은 Data Infrastructure Insights 통해 관리됩니다.

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

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

단계

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

Data Infrastructure Insights의 사용자 관리 페이지로 이동하게 됩니다.

3. 각 사용자별로 원하는 역할을 선택하세요.

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

사용자 계정 및 역할에 대한 자세한 내용은 Data Infrastructure Insights 에서 확인할 수 있습니다. "[사용자 역할](#)" 섹션
서류 비치.

이벤트 발생률 확인 도구: 에이전트 규모 산정 가이드

데이터 수집기를 배포하기 전에 SVM에서 생성되는 NFS 및 SMB 이벤트 발생률을 측정하여
최적의 Agent 시스템 크기를 결정하십시오. Event Rate Checker 스크립트를 사용하면 용량
제한(Agent당 최대 50개의 데이터 수집기)을 파악하고 Agent 인프라가 예상되는 이벤트 볼륨을
처리하여 안정적인 위협 탐지를 수행할 수 있는지 확인할 수 있습니다.

요구 사항:

- 클러스터 IP
- 클러스터 관리자 사용자 이름 및 비밀번호



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

단계:

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

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

a. 다음 명령을 실행하세요.

```
linux_prompt> yum install sshpass
```

.. 그래도 작동하지 않으면 웹에서 Linux 머신에 `_sshpass_`를 다운로드하고 다음 명령을
실행하세요.

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

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

```
"Svm svm_rate is generating 100 events/sec".
```

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

다음 사항을 명심하세요.

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

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

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

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

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

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

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

를 참조하십시오 [link:concept_cs_agent_requirements.html](#) ["에이전트 요구 사항"] 추가
전제 조건 및 요구 사항은 페이지를 참조하세요.

예

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

우리는 다음 공식을 적용합니다:

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

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

다음과 같은 경우 스크립트가 잘못된 결과를 제공할 수 있습니다.

- 잘못된 자격 증명, IP 또는 SVM 이름이 제공되었습니다.

- 동일한 이름, 시퀀스 번호 등을 가진 이미 존재하는 fpolicy가 있으면 오류가 발생합니다.
- 스크립트가 실행 중에 갑자기 중단됩니다.

스크립트 실행 예는 아래와 같습니다.

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

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

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

문제 해결

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

저작권 정보

Copyright © 2026 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.