



로깅 감사 ONTAP 9

NetApp
February 12, 2026

목차

로깅 감사	1
ONTAP 감사 로깅 구현에 대해 자세히 알아보십시오	1
ONTAP 감사 로깅의 변경 사항에 대해 알아보십시오	2
ONTAP 감사 로그 내용을 표시합니다	2
ONTAP 감사 가져오기 요청 설정을 관리합니다	3
ONTAP 클러스터 간 감사 활성화	4
클러스터 간 감사 활성화 또는 비활성화	4
GET 감사 활성화의 효과	5
ONTAP 감사 로그 대상을 관리합니다	5

로깅 감사

ONTAP 감사 로깅 구현에 대해 자세히 알아보십시오

감사 로그에 기록된 관리 활동은 표준 AutoSupport 보고서에 포함되고, 특정 로깅 활동은 EMS 메시지에 포함됩니다. 또한 감사 로그를 지정한 대상으로 전송할 수 있으며, ONTAP CLI 또는 웹 브라우저를 사용하여 감사 로그 파일을 표시할 수 있습니다.

ONTAP 9.11.1부터 시스템 관리자를 사용하여 감사 로그 내용을 표시할 수 있습니다.

ONTAP 9.12.1부터 ONTAP는 감사 로그에 대한 변조 경고를 제공합니다. ONTAP는 매일 백그라운드 작업을 실행하여 audit.log 파일의 변조를 확인하고 변경 또는 변조된 로그 파일이 발견되면 EMS 경고를 보냅니다.

ONTAP 9.17.1부터 ONTAP 9.16.1 P4 이상 9.16.1 패치 릴리스에서는 "[피어링된 클러스터에서 시작된 원격 관리 활동은 클러스터 간 작업을 사용하여 기록될 수도 있습니다](#)". 이러한 활동에는 다른 클러스터에서 발생하는 사용자 중심 작업과 내부 작업이 포함됩니다

ONTAP 에 기록된 관리 활동

ONTAP 클러스터에서 수행되는 관리 활동을 기록합니다. 여기에는 발행된 요청, 요청을 트리거한 사용자, 사용자의 액세스 방법, 요청 시간 등이 포함됩니다.

관리 활동은 다음 유형 중 하나일 수 있습니다.

• SET 요청:

- 이러한 요청은 일반적으로 표시되지 않는 명령이나 작업에 적용됩니다.
- 예를 들어, 'create', 'modify', 'delete' 명령을 실행하면 이러한 요청이 실행됩니다.
- SET 요청은 기본적으로 기록됩니다.

• GET 요청:

- 이러한 요청은 정보를 검색하여 관리 인터페이스에 표시합니다.
- 예를 들어 'show' 명령을 실행하면 이러한 요청이 실행됩니다.
- GET 요청은 기본적으로 기록되지 않지만 ONTAP CLI에서 전송된 GET 요청이 기록되는지 여부를 제어할 수 있습니다. (-cliget), ONTAP API에서 (-ontapiget), 또는 ONTAP REST API에서 (-httpget)이 파일에 기록됩니다.

감사 로그 기록 및 회전

ONTAP 기록 관리 활동 /mroot/etc/log/mlog/audit.log 노드 파일입니다. CLI 명령용 세 가지 셀(클러스터셀, 노드셀, 비대화형 시스템셀)과 API 명령이 여기에 기록됩니다. 대화형 시스템셀 명령은 기록되지 않습니다. 감사 로그에는 클러스터의 모든 노드가 동기화되었는지 여부를 보여주는 타임스탬프가 포함됩니다.

Audit.log 파일은 AutoSupport Tool에 의해 지정한 수신인에게 전송된다. 또한 Splunk 또는 syslog 서버와 같이 지정한 외부 대상에 콘텐츠를 안전하게 전달할 수 있습니다.

Audit.log 파일은 매일 순환한다. 회전은 크기가 100MB에 도달하고 이전 48개 사본이 보존될 때도 발생합니다(최대 총 49개 파일). 감사 파일이 매일 회전을 수행하면 EMS 메시지가 생성되지 않습니다. 파일 크기 제한이 초과되어 Audit 파일이 회전하면 EMS 메시지가 발생한다.

GET 감사를 활성화할 때, 빠른 로그 순환으로 인한 데이터 손실을 방지하기 위해 로그 전달을 구성하는 것이 좋습니다. 자세한 내용은 다음 기술 자료 문서를 참조하세요. "[감사 로그 전달 활성화](#)".

ONTAP 감사 로깅의 변경 사항에 대해 알아봅니다

ONTAP 9부터는 Command-history.log 파일이 audit.log로 대체되고, mgwd.log 파일은 더 이상 Audit 정보를 포함하지 않는다. ONTAP 9로 업그레이드하는 경우 기존 파일과 해당 콘텐츠를 참조하는 스크립트나 도구를 검토해야 합니다.

ONTAP 9로 업그레이드한 후 기존 명령어 이력.log 파일을 보존한다. 새 감사.로그 파일이 (작성됨) 회전되면 해당 파일이 삭제(삭제)됩니다.

명령어-히스토리.로그 파일을 체크하는 툴과 스크립트는 업그레이드 시 명령어-히스토리.로그부터 audit.log로의 소프트 링크가 생성되기 때문에 계속 동작할 수 있다. 그러나 mgwd.log 파일을 확인하는 도구와 스크립트는 해당 파일에 더 이상 감사 정보가 없기 때문에 실패합니다.

또한 ONTAP 9 이상의 감사 로그에는 유용하지 않고 불필요한 로깅 활동을 유발하기 때문에 다음 항목이 더 이상 포함되지 않습니다.

- ONTAP에서 실행되는 내부 명령(즉, username=root)
- 명령 별칭(해당 명령이 가리키는 명령과는 별개)

ONTAP 9부터는 TCP 및 TLS 프로토콜을 사용하여 감사 로그를 외부 대상으로 안전하게 전송할 수 있습니다.

ONTAP 감사 로그 내용을 표시합니다

ONTAP CLI, System Manager 또는 웹 브라우저를 사용하여 클러스터의 `/mroot/etc/log/mlog/audit.log` 파일의 내용을 표시할 수 있습니다.

클러스터의 로그 파일 항목은 다음과 같습니다.

시간

로그 항목 타임 스탬프입니다.

응용 프로그램

클러스터에 연결하는 데 사용되는 애플리케이션입니다. 가능한 값의 예는 internal, console, ssh, http, , ontapi, 입니다. snmp rsh, , telnet 및 service-processor.

사용자

원격 사용자의 사용자 이름입니다.

상태

감사 요청의 현재 상태는, pending 또는 일 수 있습니다 success. error

메시지

명령 상태에 대한 오류 또는 추가 정보를 포함할 수 있는 선택적 필드입니다.

세션 ID입니다

요청이 수신된 세션 ID입니다. 각 SSH_SESSION_에는 세션 ID가 할당되고 각 HTTP, ONTAPI 또는 SNMP_REQUEST_에는 고유한 세션 ID가 할당됩니다.

스토리지 VM

사용자가 연결하는 데 사용되는 SVM.

범위

데이터 스토리지 VM에 요청이 있으면 'VM'을 표시하고, 그렇지 않으면 '클러스터'를 표시합니다.

명령 ID입니다

CLI 세션에서 수신한 각 명령의 ID입니다. 이렇게 하면 요청과 응답을 서로 연관시킬 수 있습니다. ZAPI, HTTP 및 SNMP 요청에는 명령 ID가 없습니다.

웹 브라우저에서 ONTAP CLI의 클러스터의 로그 항목을 표시하고 시스템 관리자에서 ONTAP 9.11.1로 시작할 수 있습니다.

시스템 관리자

- 인벤토리를 표시하려면 * 이벤트 및 작업 > 감사 로그 * 를 선택합니다. + 각 열에는 필터링, 정렬, 검색, 표시 및 인벤토리 범주를 제어하는 컨트롤이 있습니다. 재고 세부 정보는 Excel 통합 문서로 다운로드할 수 있습니다.
- 필터를 설정하려면 오른쪽 위에 있는 * Filter * (필터 *) 버튼을 클릭하고 원하는 필드를 선택합니다. +세션 ID 링크를 클릭하여 장애가 발생한 세션에서 실행된 모든 명령을 볼 수도 있습니다.

CLI를 참조하십시오

클러스터의 여러 노드에서 병합된 감사 항목을 표시하려면 + 를 입력합니다 security audit log show <[parameters]>

명령을 사용하여 개별 노드에 대한 감사 항목을 표시하거나 클러스터의 여러 노드에서 병합할 수 security audit log show 있습니다. 웹 브라우저를 사용하여 단일 노드에 디렉토리의 콘텐츠를 표시할 수도 /mroot/etc/log/mlog 있습니다. 에 대한 자세한 내용은 security audit log show **"ONTAP 명령 참조입니다"**을 참조하십시오.

웹 브라우저


웹 브라우저를 사용하여 단일 노드에 디렉토리의 콘텐츠를 표시할 수 /mroot/etc/log/mlog 있습니다. **"웹 브라우저를 사용하여 노드의 로그, 코어 덤프 및 MIB 파일에 액세스하는 방법에 대해 알아봅니다"**..

ONTAP 감사 가져오기 요청 설정을 관리합니다

설정된 요청이 기본적으로 기록되지만 GET 요청은 기록되지 않습니다. 그러나 ONTAP HTML('HttpGet'), ONTAP CLI('-cliget') 또는 ONTAP API('-ontapiget')에서 보낸 GET 요청이 파일에 기록되는지 여부를 제어할 수 있습니다.

시스템 관리자에서 감사 로깅 설정을 ONTAP CLI에서 수정할 수 있으며 ONTAP 9.11.1부터 시작할 수 있습니다.

시스템 관리자

1. 이벤트 및 작업 > 감사 로그 * 를 선택합니다.
2.  오른쪽 상단 모서리를 클릭한 다음 추가 또는 제거할 요청을 선택합니다.

CLI를 참조하십시오

- ONTAP CLI 또는 API의 GET 요청을 감사 로그(audit.log 파일)에 기록하도록 지정하려면 기본 설정 요청 외에 + '보안 감사 수정[-cliget{on|off}][-HttpGet{ on|off}][-ontapiget{on|off}]'을 입력합니다
- 현재 설정을 표시하려면 + 보안 감사 표시 를 입력합니다

에 대한 자세한 내용은 `security audit show` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

ONTAP 클러스터 간 감사 활성화

ONTAP 9.17.1부터, 그리고 ONTAP 9.16.1 P4 및 이후 9.16.1 패치 릴리스부터 ONTAP 에서 클러스터 간 감사를 활성화하여 피어링된 클러스터에서 시작된 작업을 기록할 수 있습니다. 이 원격 감사는 여러 ONTAP 클러스터가 상호 작용하는 환경에서 특히 유용하며, 원격 작업에 대한 추적성과 책임 소재를 제공합니다.

클러스터 간 감사는 사용자가 시작한 GET(읽기) 또는 SET(생성/수정/제거) 작업을 구분할 수 있습니다. 기본적으로 대상 클러스터에서는 사용자가 시작한 SET 작업만 감사됩니다. GET 또는 `show` CLI에서 명령을 실행하면 요청이 클러스터 간인지 여부에 관계없이 기본적으로 감사되지 않습니다.

시작하기 전에

- 당신은 있어야합니다 advanced 레벨 권한
- 클러스터는 다른 클러스터와 피어링되어야 하며, 두 클러스터 모두 ONTAP 9.16.1 P4 이상을 실행해야 합니다.



일부 노드만 ONTAP 9.16.1 P4 이상으로 업그레이드된 환경에서는 업그레이드된 버전을 실행하는 노드에서만 감사 로깅이 실행됩니다. 일관된 감사 동작을 보장하려면 모든 노드를 지원되는 버전으로 업그레이드하는 것이 좋습니다.

클러스터 간 감사 활성화 또는 비활성화

단계

1. 클러스터에서 크로스 클러스터 감사를 활성화(또는 비활성화)하려면 다음을 설정합니다. `cluster-peer` 매개변수 `on` 또는 `off` :

```
security audit modify -cluster-peer {on|off}
```

2. 현재 감사 상태를 확인하여 클러스터 피어 설정이 활성화 또는 비활성화되었는지 확인하세요.

```
security audit show
```

응답:

```
Audit Setting State
-----
CLI GET: off
HTTP GET: off
ONTAPI GET: off
Cluster Peer: on
```

GET 감사 활성화의 효과

ONTAP 9.17.1부터 "[CLI, HTTP, ONTAPI GET 감사 활성화](#)" 피어링된 클러스터에서는 클러스터 간 사용자 시작 GET 요청에 대한 감사도 활성화할 수 있습니다. 이전 ONTAP 버전에서는 GET 감사가 로컬 클러스터의 요청에만 적용되었습니다. ONTAP 9.17.1에서는 `cluster-peer` 옵션 설정 `on` 로컬 클러스터와 클러스터 간 요청이 모두 감사합니다.

ONTAP 감사 로그 대상을 관리합니다

감사 로그를 최대 10개의 대상으로 전달할 수 있습니다. 예를 들어, 모니터링, 분석 또는 백업을 위해 로그를 Splunk 또는 syslog 서버로 전달할 수 있습니다.

이 작업에 대해

전달을 구성하려면 syslog 또는 Splunk 호스트의 IP 주소, 포트 번호, 전송 프로토콜 및 전달된 로그에 사용할 syslog 기능을 제공해야 합니다. "[syslog 기능에 대해 자세히 알아보십시오](#)".

``-protocol`` 매개 변수를 사용하여 다음 전송 값 중 하나를 선택할 수 있습니다.

UDP 암호화되지 않음

보안이 없는 사용자 데이터그램 프로토콜(기본값)

TCP 암호화되지 않음

보안 기능이 없는 전송 제어 프로토콜

TCP 암호화

전송 계층 보안(TLS)이 있는 전송 제어 프로토콜 + A * 서버 확인 * 옵션은 TCP 암호화 프로토콜이 선택된 경우에 사용할 수 있습니다.

기본 포트는 UDP의 경우 514, TCP의 경우 6514이지만 네트워크 요구를 충족하는 포트를 지정할 수 있습니다.

``-message-format`` 명령을 사용하여 다음 메시지 형식 중 하나를 선택할 수 있습니다.

레거시 - NetApp

RFC-3164 Syslog 형식의 변형(형식: <PRIVAL> 타임스탬프 HOSTNAME:MSG)

RFC-5424

RFC-5424에 따른 syslog 형식(형식: <PRIVAL> 버전 타임스탬프 HOSTNAME:MSG)

ONTAP CLI에서 감사 로그를 전달하고 ONTAP 9.11.1부터 System Manager에서 전달할 수 있습니다.

시스템 관리자

- 감사 로그 대상을 표시하려면 * 클러스터 > 설정 * 을 선택합니다. +로그 대상 수가 * 알림 관리 타일 * 에 표시됩니다. 세부 정보를 표시하려면 클릭하십시오.
- 감사 로그 대상을 추가, 수정 또는 삭제하려면 * 이벤트 및 작업 > 감사 로그 * 를 선택한 다음 화면 오른쪽 상단의 * 감사 대상 관리 * 를 클릭합니다. + 를 **Add** 클릭하거나 * 호스트 주소 * 열을 클릭하여 항목을 편집하거나 삭제합니다.

CLI를 참조하십시오

1. 감사 로그를 전달할 각 대상에 대해 대상 IP 주소 또는 호스트 이름 및 보안 옵션을 지정합니다.

```
cluster1::> cluster log-forwarding create -destination
192.168.123.96
-port 514 -facility user

cluster1::> cluster log-forwarding create -destination
192.168.123.98
-port 6514 -protocol tcp-encrypted -facility user
```

- "cluster log-forwarding create" 명령이 대상 호스트를 ping하여 연결을 확인할 수 없으면 명령이 실패하고 오류가 표시됩니다. 권장하지는 않지만 명령과 함께 '-force' 매개 변수를 사용하면 연결 확인이 생략됩니다.
- '-verify-server' 매개 변수를 'true'로 설정하면 로그 전달 대상 ID가 인증서의 유효성을 확인하여 확인됩니다. 프로토콜 필드에서 TCP 암호화 값을 선택한 경우에만 이 값을 'true'로 설정할 수 있습니다.

2. cluster log-forwarding show 명령을 사용하여 대상 레코드가 올바른지 확인합니다.

```
cluster1::> cluster log-forwarding show
```

Destination Host	Port	Protocol	Verify Server	Syslog Facility
192.168.123.96	514	udp-unencrypted	false	user
192.168.123.98	6514	tcp-encrypted	true	user

2 entries were displayed.

관련 정보

- ["클러스터 로그 전달 표시"](#)
- ["클러스터 로그 전달 생성"](#)

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.