



파일 및 폴더 감사 정책을 구성합니다

ONTAP 9

NetApp
April 24, 2024

목차

파일 및 폴더 감사 정책을 구성합니다.....	1
파일 및 폴더 감사 정책을 구성합니다.....	1
NTFS 보안 스타일 파일 및 디렉토리에 대한 감사 정책을 구성합니다	1
UNIX 보안 스타일 파일 및 디렉토리에 대한 감사를 구성합니다	4

파일 및 폴더 감사 정책을 구성합니다

파일 및 폴더 감사 정책을 구성합니다

파일 및 폴더 액세스 이벤트에 대한 감사를 구현하는 과정은 두 단계로 구성됩니다. 먼저 SVM(스토리지 가상 시스템)에서 감사 구성을 생성하고 활성화해야 합니다. 둘째, 모니터링할 파일과 폴더에 대해 감사 정책을 구성해야 합니다. 성공한 액세스 시도와 실패한 액세스 시도를 모두 모니터링하도록 감사 정책을 구성할 수 있습니다.

SMB 및 NFS 감사 정책을 모두 구성할 수 있습니다. SMB 및 NFS 감사 정책은 다양한 구성 요구사항 및 감사 기능을 갖습니다.

적절한 감사 정책이 구성된 경우 ONTAP는 SMB 또는 NFS 서버가 실행 중인 경우에만 감사 정책에 지정된 SMB 및 NFS 액세스 이벤트를 모니터링합니다.

NTFS 보안 스타일 파일 및 디렉터리에 대한 감사 정책을 구성합니다

파일 및 디렉터리 작업을 감사하려면 감사 정보를 수집할 파일 및 디렉터리에 대한 감사 정책을 구성해야 합니다. 감사 구성을 설정 및 활성화하는 것 외에 다른 기능도 있습니다. Windows 보안 탭을 사용하거나 ONTAP CLI를 사용하여 NTFS 감사 정책을 구성할 수 있습니다.

Windows 보안 탭을 사용하여 NTFS 감사 정책 구성

Windows 속성 창의 * Windows 보안 * 탭을 사용하여 파일 및 디렉터리에 대한 NTFS 감사 정책을 구성할 수 있습니다. 이는 Windows 클라이언트에 있는 데이터에 대한 감사 정책을 구성할 때 사용되는 것과 동일한 방법으로, 익숙한 GUI 인터페이스를 사용할 수 있습니다.

필요한 것

감사는 SACL(시스템 액세스 제어 목록)을 적용하는 데이터가 포함된 SVM(스토리지 가상 시스템)에서 구성해야 합니다.

이 작업에 대해

NTFS 감사 정책 구성은 NTFS 보안 설명자와 연결된 NTFS SACL에 항목을 추가하여 수행됩니다. 그런 다음 보안 설명자가 NTFS 파일 및 디렉터리에 적용됩니다. 이러한 작업은 Windows GUI에서 자동으로 처리됩니다. 보안 설명자는 파일 및 폴더 액세스 권한을 적용하기 위한 DACL(임의 액세스 제어 목록), 파일 및 폴더 감사를 위한 SACL 또는 SACL 및 DACL을 모두 포함할 수 있습니다.

Windows 보안 탭을 사용하여 NTFS 감사 정책을 설정하려면 Windows 호스트에서 다음 단계를 수행하십시오.

단계

1. Windows 탐색기의 * Tools * 메뉴에서 * Map network drive * 를 선택합니다.
2. 네트워크 드라이브 매핑 * 상자를 완료합니다.
 - a. 드라이브 * 문자를 선택합니다.
 - b. 폴더 * 상자에 감사할 데이터와 공유 이름을 가지고 있는 공유가 포함된 SMB 서버 이름을 입력합니다.

SMB 서버 이름 대신 SMB 서버에 대한 데이터 인터페이스의 IP 주소를 지정할 수 있습니다.

SMB 서버 이름이 "smb_server"이고 공유 이름이 "hay1"인 경우 \\smb_server\share1"을 입력해야 합니다.

c. 마침 * 을 클릭합니다.

선택한 드라이브가 마운트되고 공유 내에 포함된 파일 및 폴더를 표시하는 Windows 탐색기 창이 준비됩니다.

3. 감사 액세스를 설정할 파일 또는 디렉토리를 선택합니다.
4. 파일 또는 디렉토리를 마우스 오른쪽 단추로 클릭한 다음 * 속성 * 을 선택합니다.
5. 보안 * 탭을 선택합니다.
6. 고급 * 을 클릭합니다.
7. 감사 * 탭을 선택합니다.
8. 원하는 작업을 수행합니다.

원하는 경우	다음을 수행합니다
새 사용자 또는 그룹에 대한 감사를 설정합니다	<ol style="list-style-type: none">a. 추가 * 를 클릭합니다.b. 선택할 개체 이름을 입력하십시오. 상자에 추가할 사용자 또는 그룹의 이름을 입력합니다.c. 확인 * 을 클릭합니다.
사용자 또는 그룹에서 감사를 제거합니다	<ol style="list-style-type: none">a. 선택할 개체 이름을 입력하십시오. 상자에서 제거할 사용자 또는 그룹을 선택합니다.b. 제거 * 를 클릭합니다.c. 확인 * 을 클릭합니다.d. 이 절차의 나머지 부분을 건너웁니다.
사용자 또는 그룹에 대한 감사 변경	<ol style="list-style-type: none">a. 선택할 개체 이름을 입력하십시오. 상자에서 변경할 사용자 또는 그룹을 선택합니다.b. 편집 * 을 클릭합니다.c. 확인 * 을 클릭합니다.

사용자 또는 그룹에 대한 감사를 설정하거나 기존 사용자 또는 그룹에 대한 감사를 변경하는 경우 <object>에 대한 감사 항목 상자가 열립니다.

9. 적용 대상 * 상자에서 이 감사 항목을 적용할 방법을 선택합니다.

다음 중 하나를 선택할 수 있습니다.

- * 이 폴더, 하위 폴더 및 파일 *
- * 이 폴더 및 하위 폴더 *
- * 이 폴더만 *

- * 이 폴더 및 파일 *
- * 하위 폴더 및 파일만 *
- * 하위 폴더만 *
- * 파일만 * 단일 파일에 대한 감사를 설정하는 경우 * 적용 대상 * 상자가 활성화되지 않습니다. 적용 대상 * 상자 설정은 기본적으로 * 이 개체만 * 으로 설정됩니다.



감사는 SVM 리소스를 사용하기 때문에 보안 요구사항을 충족하는 감사 이벤트를 제공하는 최소 수준만 선택하십시오.

10. Access* 상자에서 감사할 내용과 성공한 이벤트, 실패 이벤트 또는 둘 모두를 감사할지 여부를 선택합니다.

- 성공한 이벤트를 감사하려면 성공 상자를 선택합니다.
- 실패 이벤트를 감사하려면 실패 상자를 선택합니다.

보안 요구 사항을 충족하기 위해 모니터링해야 하는 작업만 선택합니다. 이러한 감사 가능한 이벤트에 대한 자세한 내용은 Windows 설명서를 참조하십시오. 다음 이벤트를 감사할 수 있습니다.

- * 완전 제어 *
- * 폴더 트래버스/파일 실행 *
- * 폴더 나열/데이터 읽기 *
- * 읽기 속성 *
- * 확장 속성 읽기 *
- * 파일 생성/데이터 쓰기 *
- * 폴더 생성/데이터 추가 *
- * 속성 쓰기 *
- * 확장 속성 쓰기 *
- * 하위 폴더 및 파일 삭제 *
- * 삭제 *
- * 읽기 권한 *
- * 권한 변경 *
- * 소유권 가져오기 *

11. 감사 설정이 원본 컨테이너의 후속 파일 및 폴더에 전파되지 않도록 하려면 * 이 감사 항목을 이 컨테이너 내의 개체 및/또는 컨테이너에 적용 * 상자를 선택합니다.

12. 적용 * 을 클릭합니다.

13. 감사 항목 추가, 제거 또는 편집을 마친 후 * 확인 * 을 클릭합니다.

object>에 대한 감사 항목 상자가 닫힙니다.

14. 감사 * 상자에서 이 폴더의 상속 설정을 선택합니다.

보안 요구 사항을 충족하는 감사 이벤트를 제공하는 최소 수준만 선택합니다. 다음 중 하나를 선택할 수 있습니다.

- 이 개체의 부모 상자에서 상속 가능한 감사 항목 포함 을 선택합니다.
- 모든 하위 항목의 기존 상속 가능한 감사 항목을 이 개체의 상속 가능한 감사 항목으로 바꾸기 상자를 선택합니다.
- 두 상자를 모두 선택합니다.
- 어느 상자도 선택하지 않습니다. 단일 파일에 대해 SACL을 설정하는 경우 모든 하위 항목에 대해 상속 가능한 기존 감사 항목을 이 개체의 상속 가능한 감사 항목으로 바꾸기 상자는 감사 상자에 없습니다.

15. 확인 * 을 클릭합니다.

감사 상자가 닫힙니다.

ONTAP CLI를 사용하여 NTFS 감사 정책을 구성합니다

ONTAP CLI를 사용하여 파일 및 폴더에 대한 감사 정책을 구성할 수 있습니다. 따라서 Windows 클라이언트에서 SMB 공유를 사용하여 데이터에 연결할 필요 없이 NTFS 감사 정책을 구성할 수 있습니다.

'vserver security file-directory' 명령 제품군을 사용하여 NTFS 감사 정책을 구성할 수 있습니다.

CLI를 사용하는 NTFS SACL만 구성할 수 있습니다. 이 ONTAP 명령 제품군에는 NFSv4 SACL 구성이 지원되지 않습니다. 이러한 명령을 사용하여 파일과 폴더에 NTFS SACL을 구성 및 추가하는 방법에 대한 자세한 내용은 man 페이지를 참조하십시오.

UNIX 보안 스타일 파일 및 디렉토리에 대한 감사를 구성합니다

NFSv4.x ACL에 감사 ACE를 추가하여 UNIX 보안 스타일 파일 및 디렉토리에 대한 감사를 구성합니다. 이를 통해 보안을 위해 특정 NFS 파일 및 디렉토리 액세스 이벤트를 모니터링할 수 있습니다.

이 작업에 대해

NFSv4.x의 경우 임의의 ACE와 시스템 ACE가 모두 동일한 ACL에 저장됩니다. 이 파일은 별도의 DACL 및 SACL에 저장되지 않습니다. 따라서 기존 ACL을 덮어쓰거나 잃지 않도록 기존 ACL에 감사 ACE를 추가할 때는 주의해야 합니다. 감사 ACE를 기존 ACL에 추가하는 순서는 중요하지 않습니다.

단계

1. nfs4_getfacl 또는 이와 동등한 명령을 사용하여 파일 또는 디렉토리의 기존 ACL을 검색합니다.

ACL을 조작하는 방법에 대한 자세한 내용은 NFS 클라이언트의 man 페이지를 참조하십시오.

2. 원하는 감사 ACE를 추가합니다.
3. nfs4_setfacl 또는 이와 동등한 명령을 사용하여 파일 또는 디렉토리에 업데이트된 ACL을 적용합니다.

저작권 정보

Copyright © 2024 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.