ONTAP가 NFS 클라이언트 인증을 처리하는 방식

ONTAP 9

NetApp
April 24, 2024

This PDF was generated from https://docs.netapp.com/ko-kr/ontap/nfs-admin/nfs-client-authentication-concept.html on April 24, 2024. Always check docs.netapp.com for the latest.

목차

ONTAP가 NFS 클라이언트 인증을 처리하는 방식 1
ONTAP에서 NFS 클라이언트 인증을 처리하는 방법 개요 1
ONTAP에서 이름 서비스를 사용하는 방법 1
ONTAP가 NFS 클라이언트에서 SMB 파일 액세스를 허용하는 방법 2
NFS 자격 증명 캐시의 작동 방식 2

ONTAP가 NFS 클라이언트 인증을 처리하는 방식

ONTAP에서 NFS 클라이언트 인증을 처리하는 방법 개요

NFS 클라이언트가 SVM에서 데이터에 액세스하려면 먼저 제대로 인증되어야 합니다. ONTAP는 UNIX 자격 증명을 구성하는 이름 서비스와 비교하여 클라이언트를 인증합니다.

NFS 클라이언트가 SVM에 연결되면 ONTAP는 SVM의 이름 서비스 구성에 따라 다른 이름 서비스를 확인하여 사용자의 UNIX 자격 증명을 얻습니다. ONTAP는 로컬 UNIX 계정, NIS 도메인 및 LDAP 도메인에 대한 자격 증명을 확인할 수 있습니다. ONTAP가 사용자를 성공적으로 인증할 수 있도록 하나 이상의 사용자를 구성해야 합니다. 여러 개의 이름 서비스와 ONTAP가 서비스를 검색하는 순서를 지정할 수 있습니다.

UNIX 볼륨 보안 스타일을 사용하는 순수 NFS 환경에서는 이 구성으로 NFS 클라이언트에서 접속하는 사용자에 대해 적절한 파일 액세스를 인증하고 제공할 수 있습니다.

혼합, NTFS 또는 통합 볼륨 보안 스타일을 사용하는 경우 ONTAP는 Windows 도메인 컨트롤러에서 인증을 위해 UNIX 사용자의 SMB 사용자 이름을 얻어야 합니다. 이 문제는 로컬 UNIX 계정이나 LDAP 도메인을 사용하여 개별 사용자를 매핑하거나 기본 SMB 사용자를 대신 사용하여 발생할 수 있습니다. ONTAP에서 검색할 이름 서비스를 순서대로 지정하거나 기본 SMB 사용자를 지정할 수 있습니다.

ONTAP에서 이름 서비스를 사용하는 방법

ONTAP는 이름 서비스를 사용하여 사용자 및 클라이언트에 대한 정보를 얻습니다. ONTAP는 이 정보를 사용하여 스토리지 시스템의 데이터에 액세스하거나 데이터를 관리하는 사용자를 인증하고 혼합 환경에서 사용자 자격 증명을 매핑합니다.

스토리지 시스템을 구성할 때 ONTAP에서 인증에 사용할 사용자 자격 증명을 얻기 위해 사용할 이름 서비스를 지정해야 합니다. ONTAP는 다음과 같은 이름 서비스를 지원합니다.

- 로컬 사용자(파일)
- 외부 NIS 도메인(NIS)
- 외부 LDAP 도메인(LDAP)

'vserver services name-service ns-switch' 명령 제품군을 사용하여 소스로 SVM을 구성하여 네트워크 정보 및 검색 순서를 검색할 수 있습니다. 이러한 명령은 UNIX 시스템에서 '/etc/nsswitch.conf' 파일과 동일한 기능을 제공합니다.

NFS 클라이언트가 SVM에 연결되면 ONTAP는 지정된 이름 서비스를 확인하여 사용자의 UNIX 자격 증명을 얻습니다. 이름 서비스가 올바르게 구성되어 있고 ONTAP에서 UNIX 자격 증명을 얻을 수 있는 경우 ONTAP는 사용자를 성공적으로 인증합니다.

보안 스타일이 혼합된 환경에서는 ONTAP가 사용자 자격 증명을 매핑해야 할 수 있습니다. ONTAP가 사용자 자격 증명을 적절하게 매핑할 수 있도록 사용자 환경에 맞게 이름 서비스를 구성해야 합니다.

ONTAP에서는 SVM 관리자 계정을 인증하는 데에도 이름 서비스를 사용합니다. 이름 서비스 스위치를 구성하거나 수정할 때 실수로 SVM 관리자 계정에 대한 인증을 비활성화하지 않도록 주의해야 합니다. SVM 관리 사용자에 대한 자세한 내용은 를 참조하십시오 "관리자 인증 및 RBAC".

ONTAP가 NFS 클라이언트에서 SMB 파일 액세스를 허용하는 방법

ONTAP는 Windows NT 파일 시스템(NTFS) 보안 의미를 사용하여 NFS 클라이언트의 UNIX 사용자가 NTFS 권한이 있는 파일에 액세스할 수 있는지 여부를 결정합니다.

ONTAP는 사용자의 UNIX UID(사용자 ID)를 SMB 자격 증명으로 변환한 다음 SMB 자격 증명을 사용하여 사용자에게 파일에 대한 액세스 권한이 있는지 확인합니다. SMB 자격 증명은 일반적으로 사용자의 Windows 사용자 이름인 기본 SID(보안 식별자)와 사용자가 구성원인 Windows 그룹에 해당하는 하나 이상의 그룹 SID로 구성됩니다.

프로세스가 도메인 컨트롤러에 접속하기 때문에 ONTAP가 UNIX UID를 SMB 자격 증명으로 변환하는 데 걸리는 시간은 수십 밀리초에서 수백 밀리초로 지정할 수 있습니다. ONTAP는 UID를 SMB 자격 증명에 매핑하고 자격 증명 캐시에 매핑을 입력하여 변환으로 인한 검증 시간을 줄입니다.

NFS 자격 증명 캐시의 작동 방식

NFS 사용자가 스토리지 시스템의 NFS 내보내기에 대한 액세스를 요청할 경우 ONTAP는 외부 이름 서버 또는 로컬 파일에서 사용자 자격 증명을 검색하여 사용자를 인증해야 합니다. 그런 다음 ONTAP는 나중에 참조할 수 있도록 이러한 자격 증명을 내부 자격 증명 캐시에 저장합니다. NFS 자격 증명 캐시의 작동 방식을 이해하면 잠재적인 성능 및 액세스 문제를 처리할 수 있습니다.

자격 증명 캐시가 없으면 ONTAP는 NFS 사용자가 액세스를 요청할 때마다 이름 서비스를 쿼리해야 합니다. 사용량이 많은 스토리지 시스템에서 많은 사용자가 액세스하는 경우 심각한 성능 문제가 신속하게 발생하여 원치 않는 지연이 발생하거나 NFS 클라이언트 액세스가 거부 될 수 있습니다.

ONTAP는 자격 증명 캐시를 사용하여 사용자 자격 증명을 검색한 다음 NFS 클라이언트가 다른 요청을 보낼 때 빠르고 쉽게 액세스할 수 있도록 미리 결정된 시간 동안 저장합니다. 이 방법은 다음과 같은 이점을 제공합니다.

- NIS 또는 LDAP와 같은 외부 이름 서버에 대한 요청 수를 줄여 스토리지 시스템의 로드를 간소화합니다.
- 외부 네임 서버에 대한 요청 수를 줄여 부하를 덜어줍니다.
- 외부 소스에서 자격 증명을 얻기 위한 대기 시간을 없애 사용자 액세스 속도를 높입니다.

ONTAP는 자격 증명 캐시에 양의 자격 증명과 음의 자격 증명을 모두 저장합니다. 양의 자격 증명은 사용자가 인증되고 액세스 권한이 부여되었음을 의미합니다. 음수 자격 증명은 사용자가 인증되지 않고 액세스가 거부되었음을 의미합니다.

기본적으로 ONTAP는 24시간 동안 양의 자격 증명을 저장합니다. 즉, 처음에 사용자를 인증한 후 ONTAP는 해당 사용자의 액세스 요청에 대해 24시간 동안 캐시된 자격 증명을 사용합니다. 사용자가 24시간 후에 액세스를 요청하면 주기가 다시 시작됩니다. ONTAP 는 캐시된 자격 증명을 삭제하고 해당 이름 서비스 소스에서 자격 증명을 다시 가져옵니다. 이전 24시간 동안 이름 서버에서 자격 증명이 변경된 경우 ONTAP는 다음 24시간 동안 사용할 수 있도록 업데이트된 자격 증명을 캐시합니다.

기본적으로 ONTAP는 2시간 동안 부정 자격 증명을 저장합니다. 즉, 처음에 사용자에 대한 액세스를 거부하면 ONTAP는 해당 사용자의 액세스 요청을 2시간 동안 계속 거부합니다. 사용자가 2시간 후에 액세스를 요청하는 경우 주기가 다시 시작됩니다. ONTAP 는 해당 이름 서비스 소스에서 자격 증명을 다시 가져옵니다. 이전 2시간 동안 이름 서버에서 자격 증명이 변경된 경우 ONTAP는 다음 2시간 동안 사용할 수 있도록 업데이트된 자격 증명을 캐시합니다.

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 라이센스와 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 라이센스도 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 라이센스를 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 라이센스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

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