ONTAP에서 로컬 사용자 및 그룹을 사용하는 방법

ONTAP 9

NetApp
September 12, 2024

목차

ONTAP에서 로컬 사용자 및 그룹을 사용하는 방법

로컬 사용자 및 그룹 개념

사용자 환경에서 로컬 사용자 및 그룹을 구성하고 사용할지 여부를 결정하기 전에 로컬 사용자 및 그룹의 정의 및 이에 대한 몇 가지 기본 정보를 알아야 합니다.

- * 로컬 사용자 *

  생성된 SVM(스토리지 가상 머신)만 볼 수 있는 고유한 SID(보안 식별자)를 가진 사용자 계정 로컬 사용자 계정에는 사용자 이름 및 SID를 비롯한 일련의 속성이 있습니다. 로컬 사용자 계정은 NTLM 인증을 사용하여 CIFS 서버에서 로컬로 인증됩니다.

  사용자 계정에는 여러 가지 용도가 있습니다.

  - 사용자에게 *User Rights Management* 권한을 부여하는 데 사용됩니다.
  - SVM이 소유한 파일 및 폴더 리소스에 대한 공유 레벨 및 파일 레벨 액세스를 제어하는 데 사용됩니다.

- * 로컬 그룹 *

  고유한 SID가 있는 그룹은 해당 SID가 생성된 SVM에서만 볼 수 있습니다. 그룹에는 구성원 집합이 포함됩니다. 구성원은 로컬 사용자, 도메인 사용자, 도메인 그룹 및 도메인 컴퓨터 계정일 수 있습니다. 그룹을 생성, 수정 또는 삭제할 수 있습니다.

  그룹은 여러 가지 용도로 사용됩니다.

  - 해당 구성원에게 *User Rights Management* 권한을 부여하는 데 사용됩니다.
  - SVM이 소유한 파일 및 폴더 리소스에 대한 공유 레벨 및 파일 레벨 액세스를 제어하는 데 사용됩니다.

- * 로컬 도메인 *

  SVM에서 범위가 지정된 로컬 영역 로컬 도메인의 이름은 CIFS 서버 이름입니다. 로컬 사용자 및 그룹은 로컬 도메인 내에 포함됩니다.

- * SID(보안 식별자) *

  SID는 Windows 스타일의 보안 주체를 식별하는 가변 길이 숫자 값입니다. 예를 들어 일반적인 SID는 S-1-5-21-3139654847-1303905135-2517279418-123456의 형태를 사용합니다.

- * NTLM 인증 *

  CIFS 서버에서 사용자를 인증하는 데 사용되는 Microsoft Windows 보안 방법입니다.

- * 클러스터 복제 데이터베이스(RDB) *

  클러스터의 각 노드에 인스턴스가 있는 복제된 데이터베이스입니다. 로컬 사용자 및 그룹 객체가 RDB에 저장됩니다.

로컬 사용자 및 로컬 그룹을 만드는 이유

SVM(스토리지 가상 시스템)에서 로컬 사용자 및 로컬 그룹을 생성하는 데는 여러 가지 이유가 있습니다. 예를 들어 DC(도메인 컨트롤러)를 사용할 수 없거나, 로컬 그룹을 사용하여 권한을 할당하거나, SMB 서버가 작업 그룹에 있는 경우 로컬 사용자 계정을 사용하여 SMB 서버에 액세스할 수 있습니다.

다음과 같은 이유로 하나 이상의 로컬 사용자 계정을 만들 수 있습니다.

- SMB 서버가 작업 그룹에 있고 도메인 사용자를 사용할 수 없습니다.

  로컬 사용자는 작업 그룹 구성에 필요합니다.

- 도메인 컨트롤러를 사용할 수 없는 경우 SMB 서버를 인증하고 로그인할 수 있어야 합니다.

  로컬 사용자는 도메인 컨트롤러가 다운되었을 때 NTLM 인증을 사용하여 SMB 서버를 인증할 수 있으며, 네트워크 문제로 인해 SMB 서버가 도메인 컨트롤러에 접속할 수 없게 되는 경우

- 로컬 사용자에게 사용자 권한 관리 권한을 할당하려고 합니다.

  User Rights Management 는 SMB 서버 관리자가 SVM에 대한 사용자 및 그룹의 권한을 제어할 수 있는 기능입니다. 사용자 계정에 권한을 할당하거나 해당 권한이 있는 로컬 그룹의 구성원으로 만들어 사용자에게 권한을 할당할 수 있습니다.

다음과 같은 이유로 하나 이상의 로컬 그룹을 만들 수 있습니다.

- SMB 서버가 작업 그룹에 있고 도메인 그룹을 사용할 수 없습니다.

  로컬 그룹은 작업 그룹 구성에 필요하지 않지만 로컬 작업 그룹 사용자에 대한 액세스 권한을 관리하는 데 유용할 수 있습니다.

- 공유 및 파일 액세스 제어를 위해 로컬 그룹을 사용하여 파일 및 폴더 리소스에 대한 액세스를 제어하려는 경우
- Customized_User Rights Management_Privileges를 사용하여 로컬 그룹을 생성하려고 합니다.

  일부 기본 제공 사용자 그룹에는 사전 정의된 권한이 있습니다. 사용자 지정된 권한 집합을 할당하려면 로컬 그룹을 생성하고 해당 그룹에 필요한 권한을 할당할 수 있습니다. 그런 다음 로컬 사용자, 도메인 사용자 및 도메인 그룹을 로컬 그룹에 추가할 수 있습니다.

관련 정보

로컬 사용자 인증의 작동 방식

지원되는 권한 목록입니다

로컬 사용자 인증의 작동 방식

로컬 사용자가 CIFS 서버의 데이터를 액세스하려면 먼저 인증된 세션을 생성해야 합니다.

SMB는 세션 기반이므로 세션이 처음 설정될 때 사용자 ID를 한 번만 결정할 수 있습니다. CIFS 서버는 로컬 사용자를 인증할 때 NTLM 기반 인증을 사용합니다. NTLMv1과 NTLMv2가 모두 지원됩니다.

ONTAP는 세 가지 사용 사례에서 로컬 인증을 사용합니다. 각 활용 사례는 사용자 이름의 도메인 부분(domain\user 형식)이 CIFS 서버의 로컬 도메인 이름(CIFS 서버 이름)과 일치하는지 여부에 따라 달라집니다.

- 도메인 부분이 일치합니다

  데이터에 대한 액세스를 요청할 때 로컬 사용자 자격 증명을 제공하는 사용자는 CIFS 서버에서 로컬로 인증됩니다.

- 도메인 부분이 일치하지 않습니다

  ONTAP는 CIFS 서버가 속한 도메인의 도메인 컨트롤러에서 NTLM 인증을 사용하려고 합니다. 인증에 성공하면 로그인이 완료된 것입니다. 성공하지 못하면 다음 단계는 인증이 성공하지 못한 이유에 따라 달라집니다.

  예를 들어 사용자가 Active Directory에 있지만 암호가 잘못되었거나 만료된 경우 ONTAP는 CIFS 서버에서 해당 로컬 사용자 계정을 사용하지 않습니다. 대신 인증에 실패합니다. ONTAP가 CIFS 서버에 있는 경우 NetBIOS 도메인 이름이 일치하지 않아도 인증을 위해 해당 로컬 계정을 사용하는 경우도 있습니다. 예를 들어 일치하는 도메인 계정이 있지만 비활성화된 경우 ONTAP는 CIFS 서버에서 해당 로컬 계정을 사용하여 인증합니다.

- 도메인 부분이 지정되지 않았습니다

  ONTAP는 먼저 로컬 사용자로 인증을 시도합니다. 로컬 사용자로 인증에 실패하면 ONTAP는 CIFS 서버가 속한 도메인의 도메인 컨트롤러를 사용하여 사용자를 인증합니다.

로컬 또는 도메인 사용자 인증이 성공적으로 완료되면 ONTAP는 로컬 그룹 구성원 자격 및 권한을 고려하여 전체 사용자 액세스 토큰을 생성합니다.

로컬 사용자의 NTLM 인증에 대한 자세한 내용은 Microsoft Windows 설명서를 참조하십시오.

관련 정보

로컬 사용자 인증 활성화 또는 비활성화

사용자 액세스 토큰을 구성하는 방법입니다

사용자가 공유를 매핑하면 인증된 SMB 세션이 설정되고 사용자, 사용자의 그룹 구성원 자격 및 누적 권한, 매핑된 UNIX 사용자에 대한 정보가 포함된 사용자 액세스 토큰이 생성됩니다.

이 기능을 사용하지 않는 한 로컬 사용자 및 그룹 정보도 사용자 액세스 토큰에 추가됩니다. 액세스 토큰이 구성되는 방식은 로컬 사용자에 대한 로그인인지 Active Directory 도메인 사용자에 대한 로그인인지에 따라 달라집니다.

- 로컬 사용자 로그인입니다

  로컬 사용자는 다른 로컬 그룹의 구성원이 될 수 있지만 로컬 그룹은 다른 로컬 그룹의 구성원이 될 수 없습니다. 로컬 사용자 액세스 토큰은 특정 로컬 사용자가 구성원인 그룹에 할당된 모든 권한의 합집합으로 구성됩니다.

- 도메인 사용자 로그인

  도메인 사용자가 로그인하면 ONTAP는 사용자가 구성원인 모든 도메인 그룹의 사용자 SID 및 SID가 포함된 사용자 액세스 토큰을 얻습니다. ONTAP는 도메인 사용자 액세스 토큰의 조합과 사용자의 도메인 그룹(있는 경우)의 로컬 멤버십에서 제공하는 액세스 토큰, 도메인 사용자 또는 해당 도메인 그룹 구성원에 할당된 모든 직접 권한을 사용합니다.

로컬 및 도메인 사용자 로그인의 경우 사용자 액세스 토큰에 대해 기본 그룹 제거도 설정됩니다. 기본 RID는 Domain

Users(RID 513)입니다. 기본값을 변경할 수 없습니다.

Windows-to-UNIX 및 UNIX-to-Windows 이름 매핑 프로세스는 로컬 및 도메인 계정에 대해 동일한 규칙을 따릅니다.

> UNIX 사용자에서 로컬 계정으로 자동 매핑은 암시적으로 수행되지 않습니다. 이 작업이 필요한 경우 기존 이름 매핑 명령을 사용하여 명시적 매핑 규칙을 지정해야 합니다.

로컬 그룹이 포함된 SVM에서 SnapMirror 사용 지침

로컬 그룹이 포함된 SVM이 소유한 볼륨에 SnapMirror를 구성할 때는 지침을 숙지해야 합니다.

SnapMirror에서 다른 SVM으로 복제된 파일, 디렉토리 또는 공유에 적용된 ACE의 로컬 그룹은 사용할 수 없습니다. SnapMirror 기능을 사용하여 다른 SVM의 볼륨에 DR 미러를 생성하고 볼륨에 로컬 그룹에 ACE가 있는 경우 ACE는 미러에서 유효하지 않습니다. 데이터를 다른 SVM으로 복제하면 데이터가 다른 로컬 도메인에 효과적으로 교차합니다. 로컬 사용자 및 그룹에 부여되는 사용 권한은 원래 생성된 SVM의 범위 내에서만 유효합니다.

CIFS 서버를 삭제할 때 로컬 사용자 및 그룹이 어떻게 됩니까

CIFS 서버가 생성될 때 로컬 사용자 및 그룹의 기본 세트가 생성되고 CIFS 서버를 호스팅하는 SVM(스토리지 가상 머신)과 연결됩니다. SVM 관리자는 언제든지 로컬 사용자 및 그룹을 생성할 수 있습니다. CIFS 서버를 삭제할 때 로컬 사용자 및 그룹에 어떤 일이 발생하는지 알고 있어야 합니다.

로컬 사용자 및 그룹은 SVM에 연결되어 있으므로 보안 고려 사항으로 인해 CIFS 서버를 삭제할 때 삭제되지 않습니다. CIFS 서버가 삭제되어도 로컬 사용자 및 그룹은 삭제되지 않지만 숨겨집니다. SVM에서 CIFS 서버를 다시 생성할 때까지 로컬 사용자 및 그룹을 보거나 관리할 수 없습니다.

> CIFS 서버 관리 상태는 로컬 사용자 또는 그룹의 표시에는 영향을 주지 않습니다.

로컬 사용자 및 그룹과 함께 Microsoft Management Console을 사용하는 방법

Microsoft 관리 콘솔에서 로컬 사용자 및 그룹에 대한 정보를 볼 수 있습니다. 이 ONTAP 릴리스에서는 Microsoft 관리 콘솔에서 로컬 사용자 및 그룹에 대한 다른 관리 작업을 수행할 수 없습니다.

되돌리기 지침

로컬 사용자 및 그룹을 지원하지 않는 ONTAP 릴리즈로 클러스터를 되돌리려는 경우 로컬 사용자 및 그룹을 사용하여 파일 액세스 또는 사용자 권한을 관리하려면 특정 고려 사항을 알고 있어야 합니다.

- 보안상의 이유로 ONTAP가 로컬 사용자 및 그룹 기능을 지원하지 않는 버전으로 되돌려지면 구성된 로컬 사용자, 그룹 및 권한에 대한 정보가 삭제되지 않습니다.
- ONTAP의 이전 주요 버전으로 되돌릴 때 ONTAP는 인증 및 자격 증명 생성 중에 로컬 사용자 및 그룹을 사용하지

않습니다.

- 로컬 사용자 및 그룹은 파일 및 폴더 ACL에서 제거되지 않습니다.
- 로컬 사용자 또는 그룹에 부여된 권한으로 인해 부여되는 액세스에 의존하는 파일 액세스 요청이 거부됩니다.

  액세스를 허용하려면 로컬 사용자 및 그룹 개체 대신 도메인 개체를 기반으로 액세스를 허용하도록 파일 권한을 다시 구성해야 합니다.