DAC(Dynamic Access Control)를 사용하여 파일 액세스 보안

ONTAP 9

NetApp
September 12, 2024

목차

DAC(Dynamic Access Control)를 사용하여 파일 액세스 보안

DAC(Dynamic Access Control) 개요를 사용하여 파일 액세스 보호

동적 액세스 제어를 사용하고 Active Directory에서 중앙 액세스 정책을 생성한 후 적용된 GPO(그룹 정책 개체)를 통해 SVM의 파일 및 폴더에 적용하여 액세스를 보호할 수 있습니다. 중앙 액세스 정책 스테이징 이벤트를 사용하여 변경 내용을 적용하기 전에 중앙 액세스 정책에 대한 영향을 확인할 수 있도록 감사를 구성할 수 있습니다.

CIFS 자격 증명에 추가

동적 액세스 제어 전에 CIFS 자격 증명에는 보안 주체(사용자의) ID와 Windows 그룹 구성원이 포함되어 있습니다. 동적 액세스 제어를 사용하면 디바이스 ID, 디바이스 클레임 및 사용자 클레임을 비롯한 세 가지 유형의 정보가 자격 증명에 추가됩니다.

- 장치 ID

  사용자가 로그인하는 장치의 ID 및 그룹 멤버쉽은 제외하고 사용자의 ID 정보의 아날로그.

- 장치 요청

  장치 보안 주체에 대한 어설션. 예를 들어 장치 클레임은 특정 OU의 구성원일 수 있습니다.

- 사용자 클레임

  사용자 보안 주체에 대한 어설션. 예를 들어 사용자 클레임은 AD 계정이 특정 OU의 구성원일 수 있습니다.

중앙 액세스 정책

파일에 대한 중앙 액세스 정책을 사용하면 조직에서 사용자 그룹, 사용자 클레임, 장치 클레임 및 리소스 속성을 사용하는 조건부 식을 포함하는 인증 정책을 중앙에서 배포하고 관리할 수 있습니다.

예를 들어, 비즈니스에 큰 영향을 미치는 데이터에 액세스하려면 정규직 직원이어야 하며 관리되는 장치의 데이터만 액세스할 수 있어야 합니다. 중앙 액세스 정책은 Active Directory에서 정의되고 GPO 메커니즘을 통해 파일 서버로 배포됩니다.

고급 감사를 통한 중앙 액세스 정책 스테이징

중앙 액세스 정책은 '성질'일 수 있으며, 이 경우 파일 액세스 검사 중에 "what-if" 방식으로 평가됩니다. 정책이 적용된 경우 어떤 결과가 발생했는지, 현재 구성된 것과 어떻게 다른 결과가 감사 이벤트로 기록됩니다. 이렇게 하면 관리자가 감사 이벤트 로그를 사용하여 실제로 정책을 적용하기 전에 액세스 정책 변경의 영향을 확인할 수 있습니다. 액세스 정책 변경의 영향을 평가한 후 GPO를 통해 원하는 SVM에 정책을 배포할 수 있습니다.

관련 정보

지원되는 GPO

CIFS 서버에 그룹 정책 객체 적용

CIFS 서버에서 GPO 지원을 설정하거나 해제합니다

GPO 구성에 대한 정보 표시

중앙 액세스 정책에 대한 정보 표시

중앙 액세스 정책 규칙에 대한 정보 표시

CIFS 서버의 데이터를 보호하기 위해 중앙 액세스 정책 구성

동적 액세스 제어 보안에 대한 정보 표시

"SMB 및 NFS 감사 및 보안 추적"

지원되는 동적 액세스 제어 기능

CIFS 서버에서 DAC(동적 액세스 제어)를 사용하려면 ONTAP가 Active Directory 환경에서 동적 액세스 제어 기능을 지원하는 방법을 이해해야 합니다.

동적 액세스 제어에 지원됩니다

ONTAP는 CIFS 서버에서 동적 액세스 제어가 설정된 경우 다음 기능을 지원합니다.

기능	설명
파일 시스템에 대한 클레임입니다	청구는 사용자에 대한 일부 진실을 나타내는 간단한 이름 및 값 쌍입니다. 사용자 자격 증명에는 클레임 정보가 포함되며 파일의 보안 설명자는 클레임 검사가 포함된 액세스 검사를 수행할 수 있습니다. 따라서 관리자는 파일에 액세스할 수 있는 사용자를 보다 세밀하게 제어할 수 있습니다.
파일 액세스 검사에 대한 조건식입니다	파일의 보안 매개 변수를 수정할 때 사용자는 임의로 복잡한 조건식을 파일의 보안 설명자에 추가할 수 있습니다. 조건부 표현식에는 클레임 확인이 포함될 수 있습니다.
중앙 액세스 정책을 통해 파일 액세스를 중앙 집중식으로 제어	중앙 액세스 정책은 파일에 태그를 지정할 수 있는 Active Directory에 저장된 일종의 ACL입니다. 디스크에 있는 보안 설명자와 태그가 지정된 중앙 액세스 정책 모두의 액세스 검사가 액세스를 허용하는 경우에만 파일에 대한 액세스가 부여됩니다. 따라서 관리자는 디스크의 보안 설명자를 수정하지 않고도 중앙 위치(AD)에서 파일에 대한 액세스를 제어할 수 있습니다.

기능	설명
중앙 액세스 정책 스테이징	중앙 액세스 정책의 "변경"을 통해 실제 파일 액세스에 영향을 주지 않고 보안 변경 사항을 시도하는 기능을 추가하고 감사 보고서에서 변경 효과를 확인할 수 있습니다.
ONTAP CLI를 사용하여 중앙 액세스 정책 보안에 대한 정보 표시 지원	'vserver security file-directory show' 명령을 확장하여 적용된 중앙 액세스 정책에 대한 정보를 표시합니다.
중앙 액세스 정책을 포함하는 보안 추적	적용된 중앙 액세스 정책에 대한 정보가 포함된 결과를 표시하도록 'vserver security trace' 명령 제품군을 확장합니다.

동적 액세스 제어에 지원되지 않습니다

CIFS 서버에서 동적 액세스 제어가 설정된 경우 ONTAP는 다음 기능을 지원하지 않습니다.

기능	설명
NTFS 파일 시스템 객체의 자동 분류	이 확장명은 ONTAP에서 지원되지 않는 Windows 파일 분류 인프라스트럭처의 확장입니다.
중앙 액세스 정책 스테이징 이외의 고급 감사	고급 감사를 위해 중앙 액세스 정책 스테이징만 지원됩니다.

CIFS 서버에서 동적 액세스 제어 및 중앙 액세스 정책을 사용할 때의 고려 사항

DAC(Dynamic Access Control) 및 중앙 액세스 정책을 사용하여 CIFS 서버의 파일과 폴더를 보호할 때 고려해야 할 몇 가지 사항이 있습니다.

정책 규칙이 **DOMAIN\administrator** 사용자에게 적용되는 경우 **NFS** 액세스가 루트에 대해 거부될 수 있습니다

특정 상황에서는 루트 사용자가 액세스하려는 데이터에 중앙 액세스 정책 보안이 적용될 때 루트에 대한 NFS 액세스가 거부될 수 있습니다. 이 문제는 중앙 액세스 정책에 도메인\관리자에게 적용되는 규칙이 포함되어 있고 루트 계정이 도메인\관리자 계정에 매핑된 경우에 발생합니다.

도메인\관리자 사용자에게 규칙을 적용하는 대신 도메인\관리자 그룹과 같은 관리 권한이 있는 그룹에 규칙을 적용해야 합니다. 이렇게 하면 이 문제의 근본 영향을 받지 않고 root를 domain\administrator 계정에 매핑할 수 있습니다.

Active Directory에서 적용된 중앙 액세스 정책을 찾을 수 없는 경우 **CIFS** 서버의 **BUILTIN\Administrators** 그룹에 리소스에 대한 액세스 권한이 있습니다

CIFS 서버에 포함된 리소스에 중앙 액세스 정책이 적용될 수 있지만 CIFS 서버가 중앙 액세스 정책의 SID를 사용하여 Active Directory에서 정보를 검색하려고 하면 SID가 Active Directory의 기존 중앙 액세스 정책 SID와 일치하지

않습니다. 이러한 경우 CIFS 서버는 해당 리소스에 대한 로컬 기본 복구 정책을 적용합니다.

로컬 기본 복구 정책을 사용하면 CIFS 서버의 BUILTIN\Administrators 그룹이 해당 리소스에 액세스할 수 있습니다.

동적 액세스 제어 개요 활성화 또는 비활성화

DAC(Dynamic Access Control)를 사용하여 CIFS 서버의 객체를 보호할 수 있는 옵션은 기본적으로 해제되어 있습니다. CIFS 서버에서 동적 액세스 제어를 사용하려면 이 옵션을 설정해야 합니다. 나중에 동적 액세스 제어를 사용하여 CIFS 서버에 저장된 객체를 보호하지 않으려는 경우 이 옵션을 해제할 수 있습니다.

이 작업에 대해

동적 액세스 제어가 설정되면 파일 시스템에 동적 액세스 제어 관련 항목이 있는 ACL이 포함될 수 있습니다. 동적 액세스 제어를 사용하지 않으면 현재 동적 액세스 제어 항목은 무시되고 새 항목은 허용되지 않습니다.

이 옵션은 고급 권한 수준에서만 사용할 수 있습니다.

단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
2. 다음 작업 중 하나를 수행합니다.

동적 액세스 제어를 원하는 경우…	명령 입력…
활성화됨	'vserver cifs options modify -vserver_vserver_name_-is-dac-enabled true'
사용 안 함	'vserver cifs options modify -vserver_vserver_name_-is-dac-enabled false'

3. 관리자 권한 수준으로 복귀: 'Set-Privilege admin

관련 정보

CIFS 서버의 데이터를 보호하기 위해 중앙 액세스 정책 구성

동적 액세스 제어를 사용하지 않도록 설정한 경우 동적 액세스 제어 ACE를 포함하는 ACL을 관리합니다

동적 액세스 제어 ACE로 ACL이 적용된 리소스가 있고 SVM(스토리지 가상 시스템)에서 동적 액세스 제어를 사용하지 않도록 설정한 경우 해당 리소스에서 비 동적 액세스 제어 ACE를 관리하기 전에 동적 액세스 제어 ACE를 제거해야 합니다.

이 작업에 대해

동적 액세스 제어를 사용하지 않도록 설정한 후에는 기존 동적 액세스 제어 ACE를 제거하거나 기존 동적 액세스 제어 ACE를 제거해야 새로운 비 동적 액세스 제어 ACE를 추가할 수 있습니다.

일반적으로 ACL을 관리하는 데 사용하는 툴을 사용하여 이러한 단계를 수행할 수 있습니다.

단계

1. 리소스에 적용되는 동적 액세스 제어 ACE를 결정합니다.
2. 리소스에서 동적 액세스 제어 ACE를 제거합니다.
3. 리소스에서 원하는 대로 비 동적 액세스 제어 ACE를 추가하거나 제거합니다.

CIFS 서버의 데이터를 보호하기 위해 중앙 액세스 정책을 구성합니다

CIFS 서버에서 DAC(Dynamic Access Control) 활성화, Active Directory에서 중앙 액세스 정책 구성, GPO를 사용하여 Active Directory 컨테이너에 중앙 액세스 정책 적용 등 중앙 액세스 정책을 사용하여 CIFS 서버의 데이터에 안전하게 액세스하기 위해 수행해야 하는 몇 가지 단계가 있습니다. 그리고 CIFS 서버에서 GPO를 사용하도록 설정합니다.

시작하기 전에

- 중앙 액세스 정책을 사용하도록 Active Directory를 구성해야 합니다.
- 중앙 액세스 정책을 만들고 CIFS 서버가 포함된 컨테이너에 GPO를 만들고 적용하려면 Active Directory 도메인 컨트롤러에 대한 충분한 액세스 권한이 있어야 합니다.
- 필요한 명령을 실행하려면 SVM(스토리지 가상 머신)에 대한 충분한 관리 액세스 권한이 있어야 합니다.

이 작업에 대해

중앙 액세스 정책은 Active Directory의 GPO(그룹 정책 개체)에 정의되고 적용됩니다. 중앙 액세스 정책 및 GPO 구성에 대한 지침은 Microsoft TechNet 라이브러리를 참조하십시오.

"Microsoft TechNet 라이브러리"

단계

1. "vserver cifs options modify" 명령을 사용하여 아직 활성화되지 않은 SVM에서 동적 액세스 제어를 활성화하십시오.

   'vserver cifs options modify -vserver vs1-is-dac-enabled true'

2. "vserver cifs group-policy modify" 명령을 사용하여 CIFS 서버가 아직 설정되지 않은 경우 CIFS 서버에서 GPO(그룹 정책 개체)를 사용하도록 설정합니다.

   'vserver cifs group-policy modify - vserver vs1-status enabled'

3. Active Directory에 중앙 액세스 규칙 및 중앙 액세스 정책을 생성합니다.
4. GPO(그룹 정책 개체)를 만들어 Active Directory에 중앙 액세스 정책을 배포합니다.
5. CIFS 서버 컴퓨터 계정이 있는 컨테이너에 GPO를 적용합니다.
6. 'vserver cifs group-policy update' 명령을 사용하여 CIFS 서버에 적용된 GPO를 수동으로 업데이트합니다.

   'vserver cifs group-policy update-vserver vs1'을 선택합니다

7. "vserver cifs group-policy show-applied" 명령을 사용하여 GPO 중앙 액세스 정책이 CIFS 서버의 리소스에 적용되는지 확인합니다.

   다음 예에서는 기본 도메인 정책에 CIFS 서버에 적용되는 두 가지 중앙 액세스 정책이 있음을 보여 줍니다.

'vserver cifs group-policy show-applied'

```
Vserver: vs1
-----------------------------
    GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: all-versions
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
```

```
    GPO Name: Resultant Set of Policy
       Level: RSOP
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: all-versions
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
2 entries were displayed.
```

관련 정보

GPO 구성에 대한 정보 표시

중앙 액세스 정책에 대한 정보 표시

중앙 액세스 정책 규칙에 대한 정보 표시

동적 액세스 제어 활성화 또는 비활성화

동적 액세스 제어 보안에 대한 정보를 표시합니다

DAC(Dynamic Access Control) 보안에 대한 정보를 NTFS 볼륨과 NTFS 유효 보안 데이터가 혼합된 보안 스타일 볼륨에서 표시할 수 있습니다. 여기에는 조건부 ACE, 리소스 ACE 및 중앙 액세스 정책 ACE에 대한 정보가 포함됩니다. 결과를 사용하여 보안 구성을 확인하거나 파일 액세스 문제를 해결할 수 있습니다.

이 작업에 대해

SVM(스토리지 가상 시스템)의 이름과 파일 또는 폴더 보안 정보를 표시할 데이터의 경로를 제공해야 합니다. 출력을 요약 양식 또는 상세 목록으로 표시할 수 있습니다.

단계

1. 파일 및 디렉터리 보안 설정을 원하는 수준으로 표시합니다.

정보를 표시하려면...	다음 명령을 입력합니다...
요약 양식	'vserver security file-directory show -vserver vserver_name -path path path'
세부 정보가 확장됩니다	'vserver security file-directory show -vserver vserver_name -path path path -expand-mask true'
여기서 출력은 그룹 및 사용자 SID와 함께 표시됩니다	'vserver security file-directory show -vserver vserver_name -path path -lookup-names false'
16진수 비트 마스크가 텍스트 형식으로 변환되는 파일과 디렉토리의 파일 및 디렉토리 보안에 대해 설명합니다	'vserver security file-directory show -vserver vserver_name -path path path -텍스트 마스크 true'

예

다음 예제는 SVM VS1 경로의 동적 액세스 제어 보안 정보 /vol1 을 보여줍니다.

```
cluster1::> vserver security file-directory show -vserver vs1 -path /vol1
                            Vserver: vs1
                          File Path: /vol1
                  File Inode Number: 112
                     Security Style: mixed
                    Effective Style: ntfs
                     DOS Attributes: 10
             DOS Attributes in Text: ----D---
             Expanded Dos Attribute: -
                       Unix User Id: 0
                      Unix Group Id: 1
                     Unix Mode Bits: 777
             Unix Mode Bits in Text: rwxrwxrwx
                               ACLs: NTFS Security Descriptor
                                     Control:0xbf14
                                     Owner:CIFS1\Administrator
                                     Group:CIFS1\Domain Admins
                                     SACL - ACEs
                                        ALL-Everyone-0xf01ff-OI|CI|SA|FA
                                        RESOURCE ATTRIBUTE-Everyone-0x0

("Department_MS",TS,0x10020,"Finance")
                                        POLICY ID-All resources - No Write-
0x0-OI|CI
                                     DACL - ACEs
                                        ALLOW-CIFS1\Administrator-0x1f01ff-
OI|CI
                                        ALLOW-Everyone-0x1f01ff-OI|CI
                                        ALLOW CALLBACK-DAC\user1-0x1200a9-
OI|CI

((@User.department==@Resource.Department_MS&&@Resource.Impact_MS>1000)&&@D
evice.department==@Resource.Department_MS)
```

관련 정보

GPO 구성에 대한 정보 표시

중앙 액세스 정책에 대한 정보 표시

중앙 액세스 정책 규칙에 대한 정보 표시

동적 액세스 제어에 대한 복원 고려 사항

DAC(동적 액세스 제어)를 지원하지 않는 ONTAP 버전으로 되돌릴 경우 어떤 일이 발생할지, 되돌리기 전과 후에 무엇을 해야 하는지 알고 있어야 합니다.

하나 이상의 SVM(스토리지 가상 머신)에서 동적 액세스 제어와 동적 액세스 제어를 지원하지 않는 ONTAP 버전으로 클러스터를 되돌리려면 되돌리기 전에 다음을 수행해야 합니다.

- 클러스터에서 활성화된 모든 SVM에서 동적 액세스 제어를 해제해야 합니다.
- "file-op" 이벤트 유형만 사용하려면 "cap-staging" 이벤트 유형이 포함된 클러스터의 감사 구성을 수정해야 합니다.

동적 액세스 제어 ACE가 있는 파일 및 폴더에 대한 몇 가지 중요한 복원 고려 사항을 이해하고 이에 대한 조치를 취해야 합니다.

- 클러스터를 되돌린 경우 기존 동적 액세스 제어 ACE는 제거되지 않지만 파일 액세스 검사에서는 무시됩니다.
- 동적 액세스 제어 ACE는 재버전 후에 무시되므로 동적 액세스 제어 ACE가 있는 파일에서 파일에 대한 액세스가 변경됩니다.

  이렇게 하면 사용자가 이전에는 액세스할 수 없었던 파일에 액세스하거나 이전에 액세스할 수 없었던 파일에 액세스할 수 있습니다.

- 영향을 받는 파일에 비동적 액세스 제어 ACE를 적용하여 이전 보안 수준을 복원해야 합니다.

  되돌리기 전에 또는 다시 버전이 완료된 직후 작업을 수행할 수 있습니다.

> 동적 액세스 제어 ACE는 다시 버전 변경 후 무시되므로 영향을 받는 파일에 비동적 액세스 제어 ACE를 적용할 때 제거할 필요가 없습니다. 그러나 필요한 경우 수동으로 제거할 수 있습니다.

동적 액세스 제어 및 중앙 액세스 정책을 구성하고 사용하는 방법에 대한 추가 정보를 찾을 수 있는 위치

동적 액세스 제어 및 중앙 액세스 정책을 구성하고 사용하는 데 도움이 되는 추가 리소스를 사용할 수 있습니다.

Active Directory에서 동적 액세스 제어 및 중앙 액세스 정책을 구성하는 방법에 대한 자세한 내용은 Microsoft TechNet 라이브러리 를 참조하십시오.

"Microsoft TechNet: 동적 액세스 제어 시나리오 개요"

"Microsoft TechNet: 중앙 액세스 정책 시나리오"

다음 참조는 동적 액세스 제어 및 중앙 액세스 정책을 사용하고 지원하도록 SMB 서버를 구성하는 데 도움이 됩니다.

- * SMB 서버의 GPO 사용 *

  SMB 서버에 그룹 정책 개체 적용

- * SMB 서버에서 NAS 감사 구성 *

  "SMB 및 NFS 감사 및 보안 추적"