DAC（ダイナミックアクセス制御）を使用したファイルアクセスの保護

ONTAP 9

NetApp
September 12, 2024

目次

DAC （ダイナミックアクセス制御）を使用したファイルアクセスの保護

Dynamic Access Control （ DAC ；ダイナミックアクセス制御）の概要を使用したファイルアクセスの保護

ダイナミックアクセス制御を使用してアクセスを保護できます。 Active Directory で集約型アクセスポリシーを作成し、適用された GPO を使用して SVM 上のファイルとフォルダにそのポリシーを適用します。集約型アクセスポリシーのステージングイベントを使用するように監査を設定すると、集約型アクセスポリシーの変更を適用する前にその影響を確認できます。

CIFS クレデンシャルの追加

ダイナミックアクセス制御が導入される前は、 CIFS クレデンシャルにセキュリティプリンシパル（ユーザ）の ID と Windows グループメンバーシップが含まれていました。ダイナミックアクセス制御では、デバイス ID 、デバイスの信頼性、ユーザの信頼性という 3 種類の情報がクレデンシャルに追加されます。

- デバイス ID

  ユーザ ID 情報に似ていますが、ユーザがログインに使用しているデバイスの ID とグループメンバーシップは例外です。

- デバイスの信頼性

  デバイスのセキュリティプリンシパルに関するアサーションです。たとえば、デバイスの信頼性として特定の OU のメンバーであることなどがあります。

- ユーザの信頼性

  ユーザのセキュリティプリンシパルに関するアサーションです。たとえば、ユーザの信頼性として AD アカウントが特定の OU のメンバーであることなどがあります。

集約型アクセスポリシー

ファイルの集約型アクセスポリシーを使用すると、ユーザグループ、ユーザの信頼性、デバイスの信頼性、およびリソースのプロパティを使用した条件式を含む許可ポリシーを一元的に導入して管理できます。

たとえば、ビジネスへの影響が大きいデータにアクセスする場合、ユーザーはフルタイムの従業員であり、管理対象デバイスからのみデータにアクセスできる必要があります。集約型アクセスポリシーは Active Directory で定義され、 GPO メカニズムを介してファイルサーバに配布されます。

高度な監査機能を備えた集約型アクセスポリシーのステージング

集約型アクセスポリシーは「集約型」にすることができます。この場合、ファイルアクセスチェック時に「 what if 」方式で評価されます。ポリシーが適用されていた場合の結果と、現在の設定との違いが、監査イベントとして記録されます。管理者は、実際にポリシーを有効にする前に、監査イベントログを使用してアクセ

スポリシーの変更による影響を確認できます。アクセスポリシーの変更による影響を評価したあと、ポリシーを目的の SVM に GPO 経由で導入できます。

関連情報

サポートされる GPO

CIFS サーバへのグループポリシーオブジェクトの適用

CIFS サーバ上で GPO サポートを有効または無効にします

GPO 設定に関する情報を表示します

集約型アクセスポリシーに関する情報を表示します

集約型アクセスポリシールールに関する情報を表示します

CIFS サーバ上のデータを保護する集約型アクセスポリシーの設定

ダイナミックアクセス制御セキュリティに関する情報を表示する

"SMB および NFS の監査とセキュリティトレース"

サポートされるダイナミックアクセス制御機能

CIFS サーバ上で DAC （ダイナミックアクセス制御）を使用する場合、 Active Directory 環境での ONTAP によるダイナミックアクセス制御機能のサポートについて理解しておく必要があります。

ダイナミックアクセス制御でサポートされます

CIFS サーバでダイナミックアクセス制御が有効になっている場合、 ONTAP は次の機能をサポートします。

機能性	コメント
ファイルシステムへの請求	請求とは、ユーザに関する何らかの真実を表す単純な名前と値のペアです。ユーザクレデンシャルにはクレーム情報が含まれており、ファイルのセキュリティ記述子はクレームチェックを含むアクセスチェックを実行できます。これにより、管理者は誰がファイルにアクセスできるかを細かく制御できます。
ファイルアクセスチェック用の条件式	ファイルのセキュリティパラメータを変更する場合、ユーザは任意に複雑な条件式をファイルのセキュリティ記述子に追加できます。条件式には、クレームのチェックを含めることができます。

機能性	コメント
集約型アクセスポリシーによるファイルアクセスの集中管理	集約型アクセスポリシーは、ファイルへのタグ付けが可能な Active Directory 内に格納される一種の ACL です。ファイルへのアクセスは、ディスク上のセキュリティ記述子とタグ付きの集約型アクセスポリシーの両方のアクセスチェックでアクセスが許可されている場合にのみ許可されます。これにより、管理者はディスク上のセキュリティ記述子を変更することなく、一元的な場所（ AD ）からファイルへのアクセスを制御できます。
集約型アクセスポリシーのステージング	集約型アクセスポリシーへの変更を「集約型アクセスポリシー」し、監査レポートで変更の影響を確認することで、実際のファイルアクセスに影響を与えずにセキュリティの変更を試す機能を追加します。
ONTAP CLI を使用した集約型アクセスポリシーセキュリティに関する情報の表示のサポート	を拡張します `vserver security file-directory show` 適用されている集約型アクセスポリシーに関する情報を表示するコマンド。
集約型アクセスポリシーを含むセキュリティトレース	を拡張します `vserver security trace` 適用されている集約型アクセスポリシーに関する情報を含む結果を表示するコマンドファミリー。

ダイナミックアクセス制御ではサポートされません

CIFS サーバでダイナミックアクセス制御が有効になっている場合、 ONTAP は次の機能をサポートしません。

機能性	コメント
NTFS ファイルシステムオブジェクトの自動分類	これは、 ONTAP でサポートされていない Windows ファイル分類インフラストラクチャの拡張機能です。
集約型アクセスポリシーのステージング以外の高度な監査	高度な監査では、集約型アクセスポリシーのステージングのみがサポートされます。

CIFS サーバでダイナミックアクセス制御と集約型アクセスポリシーを使用する際の考慮事項

CIFS サーバ上のファイルとフォルダを保護するために Dynamic Access Control （ DAC ；ダイナミックアクセス制御）と集約型アクセスポリシーを使用する際は、一定の考慮事項に注意する必要があります。

ポリシールール「環境 **domain\administrator user** 」の場合、 **root** に対して **NFS** アクセスが拒否されることがあります

特定の状況では、 root ユーザがアクセスしようとしているデータに集約型アクセスポリシーセキュリティが適用されていると、 root に対して NFS アクセスが拒否されることがあります。問題は、集約型アクセスポリシーに domain\administrator に適用されるルールが含まれており、 root アカウントが domain\administrator アカウントにマッピングされている場合に実行されます。

domain\administrator ユーザにルールを適用する代わりに、 domain\administrators グループなど、管理者権限を持つグループにルールを適用してください。これにより、 root を domain\administrator アカウントにマッピングしても、 root はこの問題の影響を受けなくなります。

適用された集約型アクセスポリシーが**Active Directory**に見つからないと、**CIFS**サーバの**BUILTIN\Administrators**グループにリソースへのアクセスが許可されます

CIFS サーバに格納されたリソースに集約型アクセスポリシーが適用されている場合に、 CIFS サーバが集約型アクセスポリシーの SID を使用して Active Directory から情報を取得しようとしても、 SID が Active Directory 内の既存の集約型アクセスポリシーの SID と一致しないことがあります。このような場合、 CIFS サーバはそのリソースにローカルのデフォルトのリカバリポリシーを適用します。

ローカルのデフォルトのリカバリポリシーでは、 CIFS サーバの BUILTIN\Administrators グループにそのリソースへのアクセスが許可されます。

ダイナミックアクセス制御の概要を有効または無効にします

Dynamic Access Control （ DAC ；ダイナミックアクセス制御）を使用して CIFS サーバ上のオブジェクトを保護するオプションは、デフォルトでは無効になっています。CIFS サーバでダイナミックアクセス制御を使用する場合は、このオプションを有効にする必要があります。CIFS サーバに格納されたオブジェクトの保護にダイナミックアクセス制御を使用する必要がなくなった場合は、このオプションを無効にすることができます。

このタスクについて

ダイナミックアクセス制御を有効にすると、ダイナミックアクセス制御関連のエントリを使用する ACL をファイルシステムに含めることができます。ダイナミックアクセス制御を無効にすると、現在のダイナミックアクセス制御エントリは無視され、新しいエントリは許可されません。

このオプションは、 advanced 権限レベルでのみ使用できます。

ステップ

1. 権限レベルを advanced に設定します。 `set -privilege advanced`
2. 次のいずれかを実行します。

ダイナミックアクセス制御の設定	入力するコマンド
有効	`vserver cifs options modify -vserver` *`vserver_name`* `-is-dac-enabled true`

無効	`vserver cifs options modify -vserver` *`vserver_name`* `-is-dac-enabled false`

3. 管理者権限レベルに戻ります。 `set -privilege admin`

関連情報

CIFS サーバ上のデータを保護する集約型アクセスポリシーの設定

ダイナミックアクセス制御が無効な場合に、ダイナミックアクセス制御 ACE を含む ACL を管理します

ダイナミックアクセス制御 ACE が適用された ACL が割り当てられたリソースがある場合に Storage Virtual Machine （ SVM ）でダイナミックアクセス制御を無効にすると、ダイナミックアクセス制御 ACE を削除するまではそのリソースの非ダイナミックアクセス制御 ACE を管理できません。

このタスクについて

ダイナミックアクセス制御を無効にした場合、既存のダイナミックアクセス制御 ACE を削除するまでは、既存の非ダイナミックアクセス制御 ACE の削除や新しい非ダイナミックアクセス制御 ACE の追加はできません。

これらの手順は、通常 ACL の管理に使用している任意のツールを使用して実行できます。

手順

1. リソースに適用されているダイナミックアクセス制御 ACE を確認します。
2. リソースからダイナミックアクセス制御 ACE を削除します。
3. 必要に応じて、リソースに対して非ダイナミックアクセス制御 ACE を追加または削除します。

CIFS サーバ上のデータを保護する集約型アクセスポリシーを設定します

集約型アクセスポリシーを使用した CIFS サーバ上のデータへのアクセスを保護するためには、 CIFS サーバでの Dynamic Access Control （ DAC ；ダイナミックアクセス制御）の有効化、 Active Directory での集約型アクセスポリシーの設定、 GPO を使用した Active Directory コンテナへの集約型アクセスポリシーの適用、 CIFS サーバで GPO を有効にします。

作業を開始する前に

- 集約型アクセスポリシーを使用するには、 Active Directory を設定する必要があります。
- 集約型アクセスポリシーを作成し、 CIFS サーバを含むコンテナに GPO の作成と適用を行うには、 Active Directory ドメインコントローラに対して十分なアクセスが必要です。
- 必要なコマンドを実行するためには、 Storage Virtual Machine （ SVM ）で十分な管理アクセスが必要です。

このタスクについて

集約型アクセスポリシーは、 Active Directory のグループポリシーオブジェクト（ GPO ）に対して定義および適用されます。集約型アクセスポリシーと GPO の設定については、 Microsoft TechNet ライブラリを参照してください。

"Microsoft TechNet ライブラリ"

手順

1. を使用してSVMのダイナミックアクセス制御を有効にしていない場合は、有効にします `vserver cifs options modify` コマンドを実行します

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

2. を使用してCIFSサーバでグループポリシーオブジェクト（GPO）を有効にしていない場合は、有効にします `vserver cifs group-policy modify` コマンドを実行します

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

3. Active Directory で集約型アクセスルールと集約型アクセスポリシーを作成します。
4. グループポリシーオブジェクト（ GPO ）を作成して Active Directory に集約型アクセスポリシーを導入します。
5. CIFS サーバコンピュータアカウントが存在するコンテナに GPO を適用します。
6. を使用して、CIFSサーバに適用されたGPOを手動で更新します `vserver cifs group-policy update` コマンドを実行します

   ```
   vserver cifs group-policy update -vserver vs1
   ```

7. を使用して、GPO集約型アクセスポリシーがCIFSサーバ上のリソースに適用されていることを確認します `vserver cifs group-policy show-applied` コマンドを実行します

   次の例は、デフォルトのドメインポリシーに、 CIFS サーバに適用される 2 つの集約型アクセスポリシーがあることを示しています。

   ```
   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.
```

関連情報

GPO 設定に関する情報を表示します

集約型アクセスポリシーに関する情報を表示します

集約型アクセスポリシールールに関する情報を表示します

ダイナミックアクセス制御の有効化と無効化

ダイナミックアクセス制御セキュリティに関する情報を表示します

NTFS ボリューム、および mixed セキュリティ形式のボリューム上の NTFS 対応セキュリティを使用するデータについて、ダイナミックアクセス制御（ DAC ）セキュリティに関する情報を表示できます。これには、条件付き ACE 、リソース ACE 、および集約型アクセスポリシー ACE に関する情報が含まれます。この結果を使用して、セキュリティ設定の検証や、ファイルアクセスに関する問題のトラブルシューティングを行うことができます。

このタスクについて

Storage Virtual Machine （ SVM ）の名前、およびファイルまたはフォルダのセキュリティ情報を表示するデータのパスを入力する必要があります。出力は要約形式または詳細なリストで表示できます。

ステップ

1. ファイルとディレクトリのセキュリティ設定を必要な詳細レベルで表示します。

表示する情報	入力するコマンド
要約形式で表示されます	`vserver security file-directory show -vserver vserver_name -path path`
詳細が表示されます	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`
出力は、グループ SID とユーザ SID とともに表示されます	`vserver security file-directory show -vserver vserver_name -path path -lookup-names false`
16 進数のビットマスクをテキスト形式に変換するファイルとディレクトリのセキュリティについて	`vserver security file-directory show -vserver vserver_name -path path -textual-mask true`

例

次の例は、パスに関するダイナミックアクセス制御セキュリティの情報を表示します `/vol1` SVM vs1：

```
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)
```

関連情報

GPO 設定に関する情報を表示します

集約型アクセスポリシーに関する情報を表示します

集約型アクセスポリシールールに関する情報を表示します

ダイナミックアクセス制御のリバートに関する考慮事項

ダイナミックアクセス制御（ DAC ）をサポートしないバージョンの ONTAP にリバートする場合に発生する状況と、リバートの前後に必要な処理を把握しておく必要がありま

す。

ダイナミックアクセス制御がサポートされていないバージョンの ONTAP にクラスタをリバートし、 1 つ以上の Storage Virtual Machine （ SVM ）でダイナミックアクセス制御が有効になっている場合、リバート前に次の処理を実行する必要があります。

- クラスタでダイナミックアクセス制御が有効になっているすべての SVM で、ダイナミックアクセス制御を無効にする必要があります。
- を含むクラスタで監査の設定を変更する必要があります `cap-staging` のみを使用するイベントタイプ `file-op` イベントタイプ。

ダイナミックアクセス制御 ACE が設定されているファイルやフォルダについて、リバートに関する重要な考慮事項を理解し、対応する必要があります。

- クラスタをリバートした場合、既存のダイナミックアクセス制御 ACE は削除されませんが、ファイルアクセスチェックで無視されます。
- リバート後はダイナミックアクセス制御 ACE は無視されるため、ダイナミックアクセス制御 ACE が設定されたファイルへのアクセスには変更が発生します。

  これにより、ユーザは以前にアクセスできなかったファイルにアクセスできるようになり、以前にアクセスできたファイルにアクセスできなくなる可能性があります。

- 以前のセキュリティレベルに戻すには、影響を受けるファイルに非ダイナミックアクセス制御 ACE を適用する必要があります。

  この処理は、リバート前またはリバート完了直後に実行できます。

> リバート後はダイナミックアクセス制御 ACE は無視されるため、影響を受けるファイルに非ダイナミックアクセス制御 ACE を適用する際にダイナミックアクセス制御 ACE を削除する必要はありません。ただし、必要に応じて手動で削除することもできます。

ダイナミックアクセス制御と集約型アクセスポリシーの設定方法および使用方法に関する追加情報の参照先

ダイナミックアクセス制御と集約型アクセスポリシーを設定および使用する際には、参考資料を利用することができます。

Active Directory のダイナミックアクセス制御と集約型アクセスポリシーの設定方法についての情報は、Microsoft TechNet ライブラリにあります。

"Microsoft TechNet ：「ダイナミックアクセス制御のシナリオの概要"

"Microsoft TechNet ：「集約型アクセスポリシーのシナリオ"

ダイナミックアクセス制御と集約型アクセスポリシーを使用およびサポートするように SMB サーバを設定するには、次の参考資料を使用することができます。

- * SMBサーバーでのGPOの使用*

SMBサーバへのグループポリシーオブジェクトの適用

- * SMBサーバでのNAS監査の設定*

  "SMB および NFS の監査とセキュリティトレース"