ダイナミックアクセス制御（DAC）を使用したファイルアクセスの保護

ONTAP 9

NetApp
December 20, 2024

目次

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

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クレデンシャルへの追加

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、さらに3種類の情報（デバイスID、デバイス要求、およびユーザ要求）がクレデンシャルに追加されます。

- デバイスID

  ユーザーのID情報と類似していますが、ユーザーがログインしているデバイスのIDとグループメンバーシップが異なります。

- デバイスの信頼性

  デバイスセキュリティプリンシパルに関するアサーション。たとえば、デバイスが特定のOUのメンバーであることが要求される場合があります。

- ユーザの信頼性

  ユーザセキュリティプリンシパルに関するアサーション。たとえば、ADアカウントが特定のOUのメンバーであることをユーザが要求する場合があります。

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、ユーザ要求、デバイス要求、およびリソース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および管理できます。

たとえば、ビジネスに影響の大きいデータにアクセスするには、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。

高度な監査を使用し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。ポリシーが有効になっていた場合に発生した結果、および現在の設定とどのように異なるかが監査イベントとして記録されます。このようにして、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調べることができます。アクセスポリシーの変更による影響を評価したら、GPOを使用して目的のSVMにポリシーを導入できます。

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サーバでのGPOサポートの有効化と無効化

GPO設定に関する情報の表示

集約型アクセスポリシーに関する情報の表示

集約型アクセスポリシールールに関する情報の表示

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の表示

"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サーバでダイナミックアクセス制御（DAC）を使用する場合は、ONTAPがActive Directory環境でどのようにダイナミックアクセス制御機能をサポートするかを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

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	コメント
ファイルシステムへの要求	クレームは単純な名前と値のペアで、ユーザーについての真実を記述します。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より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	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一元管理	集約型アクセスポリシーは、Active Directoryに格納されるACLの一種で、ファイルへのタグ付けが可能です。ファイルへのアクセスは、ディスクのセキュリティ記述子とタグ付けされた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	コマンドを拡張し `vserver security file-directory show`て、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します。
集約型アクセスポリシーを含むセキュリティトレース	コマンドファミリーを拡張し、 `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します。

ダイナミックアクセス制御でサポートされない

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	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有効化または無効化の概要

ダイナミックアクセス制御（DAC）を使用してCIFSサーバ上のオブジェクトを保護できるオプションは、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しない場合は、オプションを無効にすることができます。

タスクの内容

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含む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`

無効にする	`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が設定さ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を削除してから、そのリソースの非ダイナミックアクセス制御ACEを管理する必要があります。

タスクの内容

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する

集約型アクセスポリシーを使用してCIFSサーバ上のデータへのアクセスを保護するには、CIFSサーバでのダイナミックアクセス制御（DAC）の有効化、Active Directoryでの集約型アクセスポリシーの設定、GPOを含むActive Directoryコンテナへの集約型アクセスポリシーの適用、CIFSサーバでのGPOの有効化など、いくつかの手順を実行する必要があります。

開始する前に

- 集約型アクセスポリシーを使用するように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を作成して適用するには、Active Directoryドメインコントローラに対する十分なアクセスが必要です。
- 必要なコマンドを実行するには、Storage Virtual Machine（SVM）に対する十分な管理アクセスが必要です。

タスクの内容

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）に定義されて適用されます。集約型アクセスポリシーとGPOの設定手順については、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. コマンドを使用して、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 `vserver cifs options modify`ます。

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

2. コマンドを使用して、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 `vserver cifs group-policy modify`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サーバのコンピュータアカウントが配置されているコンテナにGPOを適用します。
6. コマンドを使用して、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`。

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

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

   次の例は、デフォルトのドメインポリシーに2つの集約型アクセスポリシーがあり、それらがCIFSサーバに適用されてい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設定に関する情報の表示

集約型アクセスポリシーに関する情報の表示

集約型アクセスポリシールールに関する情報の表示

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する

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の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、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。

タスクの内容

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。出力は要約形式で表示することも、詳細なリストとして表示することもできます。

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	`vserver security file-directory show -vserver vserver_name -path path`
詳細を表示	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`
出力にはグループSIDとユーザSIDが表示されます。	`vserver security file-directory show -vserver vserver_name -path path -lookup-names false`
16進数のビットマスクがテキスト形式に変換されるファイルおよびディレクトリのファイルおよび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

次の例では、SVM vs1の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`。

```
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設定に関する情報の表示

集約型アクセスポリシーに関する情報の表示

集約型アクセスポリシールールに関する情報の表示

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。
- イベントタイプを含むクラスタでは、イベントタイプのみを使用するように `file-op`監査の設定を変更する必要があります `cap-staging`。

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および使用に関する詳細情報の参照先

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方法については、その他のリソースを参照してください。

Active Directoryに対する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は、Microsoft TechNetライブラリを参照してください。

"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してサポートするようにSMBサーバを設定するには、次の資料を参照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"

著作権に関する情報

商標に関する情報