Accesso sicuro ai file utilizzando il controllo dinamico degli accessi (DAC)

ONTAP 9

NetApp
April 24, 2024

Sommario

Accesso sicuro ai file utilizzando il controllo dinamico degli accessi (DAC)

Proteggere l’accesso ai file utilizzando la panoramica del controllo dinamico dell’accesso (DAC)

È possibile proteggere l’accesso utilizzando il controllo dinamico degli accessi e creando policy di accesso centrali in Active Directory e applicandole a file e cartelle su SVM tramite oggetti Criteri di gruppo applicati (GPO). È possibile configurare il controllo in modo che utilizzi gli eventi di staging dei criteri di accesso centrale per visualizzare gli effetti delle modifiche ai criteri di accesso centrale prima di applicarli.

Aggiunte alle credenziali CIFS

Prima di Dynamic Access Control, una credenziale CIFS includeva l’identità di un’entità di protezione (l’utente) e l’appartenenza al gruppo Windows. Con Dynamic Access Control, alla credenziale vengono aggiunti altri tre tipi di informazioni: Identità del dispositivo, attestazioni del dispositivo e attestazioni dell’utente:

- Identità del dispositivo

  L’analogo delle informazioni di identità dell’utente, ad eccezione dell’identità e dell’appartenenza al gruppo del dispositivo da cui l’utente effettua l’accesso.

- Dichiarazioni dei dispositivi

  Asserzioni su un’entità di sicurezza del dispositivo. Ad esempio, un’attestazione del dispositivo potrebbe essere che è un membro di una specifica unità organizzativa.

- Richieste dell’utente

  Asserzioni su un’identità di sicurezza dell’utente. Ad esempio, un utente può affermare che il proprio account ad è membro di una specifica unità organizzativa.

Policy di accesso centrale

I criteri di accesso centrale per i file consentono alle organizzazioni di implementare e gestire centralmente policy di autorizzazione che includono espressioni condizionali utilizzando gruppi di utenti, attestazioni utente, attestazioni dispositivo e proprietà delle risorse.

Ad esempio, per accedere ai dati ad alto impatto sul business, un utente deve essere un dipendente a tempo pieno e avere accesso ai dati solo da un dispositivo gestito. I criteri di accesso centrale sono definiti in Active Directory e distribuiti ai file server tramite il meccanismo GPO.

Staging dei criteri di accesso centralizzato con auditing avanzato

Le policy di accesso centrale possono essere “staged”, nel qual caso vengono valutate in modo “what-if” durante i controlli di accesso ai file. I risultati di ciò che sarebbe accaduto se la policy fosse stata applicata e in che modo differisce da ciò che è attualmente configurato vengono registrati come evento di audit. In questo modo, gli amministratori possono utilizzare i registri degli eventi di audit per studiare l’impatto di una modifica dei criteri di accesso prima di mettere effettivamente in pratica i criteri. Dopo aver valutato l’impatto di una

modifica della policy di accesso, la policy può essere implementata tramite GPO nelle SVM desiderate.

Informazioni correlate

GPO supportati

Applicazione di oggetti Criteri di gruppo ai server CIFS

Attivazione o disattivazione del supporto GPO su un server CIFS

Visualizzazione delle informazioni sulle configurazioni dell'oggetto Criteri di gruppo

Visualizzazione di informazioni sui criteri di accesso centrale

Visualizzazione delle informazioni sulle regole dei criteri di accesso centrale

Configurazione delle policy di accesso centrale per proteggere i dati sui server CIFS

Visualizzazione di informazioni sulla sicurezza del controllo dinamico degli accessi

"Controllo SMB e NFS e tracciamento della sicurezza"

Funzionalità Dynamic Access Control supportata

Se si desidera utilizzare il controllo dinamico degli accessi (DAC) sul server CIFS, è necessario comprendere in che modo ONTAP supporta la funzionalità di controllo dinamico degli accessi negli ambienti Active Directory.

Supportato per Dynamic Access Control

ONTAP supporta le seguenti funzionalità quando il controllo dinamico degli accessi è attivato sul server CIFS:

Funzionalità	Commenti
Attestazioni nel file system	Le affermazioni sono semplici coppie di nomi e valori che indicano una certa verità su un utente. Le credenziali utente contengono informazioni sulle attestazioni e i descrittori di protezione sui file possono eseguire controlli di accesso che includono controlli delle attestazioni. In questo modo, gli amministratori possono avere un maggiore controllo sugli utenti che possono accedere ai file.
Espressioni condizionali per i controlli di accesso al file	Quando si modificano i parametri di protezione di un file, gli utenti possono aggiungere espressioni condizionali arbitrariamente complesse al descrittore di protezione del file. L'espressione condizionale può includere controlli per le attestazioni.

Funzionalità	Commenti
Controllo centralizzato dell'accesso ai file tramite policy di accesso centrali	I criteri di accesso centrale sono un tipo di ACL memorizzato in Active Directory che può essere contrassegnato in un file. L'accesso al file viene concesso solo se i controlli di accesso del descrittore di protezione su disco e del criterio di accesso centrale con tag consentono l'accesso. In questo modo, gli amministratori possono controllare l'accesso ai file da una posizione centrale (ad) senza dover modificare il descrittore di protezione su disco.
Staging dei criteri di accesso centrale	Aggiunge la possibilità di provare le modifiche di sicurezza senza influire sull'accesso effettivo ai file, "eseguendo `staging`" una modifica alle policy di accesso centrale e osservando l'effetto della modifica in un report di audit.
Supporto per la visualizzazione di informazioni sulla sicurezza dei criteri di accesso centrale mediante l'interfaccia utente di ONTAP	Estende `vserver security file-directory show` per visualizzare le informazioni sui criteri di accesso centrale applicati.
Analisi della sicurezza che include policy di accesso centralizzate	Estende `vserver security trace` famiglia di comandi per visualizzare i risultati che includono informazioni sui criteri di accesso centrale applicati.

Non supportato per Dynamic Access Control

ONTAP non supporta le seguenti funzionalità quando il controllo dinamico degli accessi è attivato sul server CIFS:

Funzionalità	Commenti
Classificazione automatica degli oggetti del file system NTFS	Si tratta di un'estensione dell'infrastruttura di classificazione dei file di Windows non supportata in ONTAP.
Auditing avanzato diverso dalla gestione temporanea dei criteri di accesso centrale	Solo lo staging dei criteri di accesso centrale è supportato per il controllo avanzato.

Considerazioni sull'utilizzo del controllo dinamico degli accessi e delle policy di accesso centrale con i server CIFS

È necessario tenere presente alcune considerazioni quando si utilizza il controllo dinamico dell'accesso (DAC) e i criteri di accesso centrale per proteggere file e cartelle sui server CIFS.

L’accesso NFS può essere negato all’utente root se la regola dei criteri si applica all’utente di dominio/amministratore

In alcuni casi, l’accesso NFS a root potrebbe essere negato quando la sicurezza del criterio di accesso centrale viene applicata ai dati a cui l’utente root sta tentando di accedere. Il problema si verifica quando il criterio di accesso centrale contiene una regola che viene applicata al dominio/amministratore e l’account root viene mappato all’account di dominio/amministratore.

Invece di applicare una regola all’utente di dominio/amministratore, è necessario applicarla a un gruppo con privilegi amministrativi, ad esempio il gruppo dominio/amministratori. In questo modo, è possibile mappare root all’account di dominio/amministratore senza che root sia interessato da questo problema.

Il gruppo BUILTIN/Administrators del server CIFS ha accesso alle risorse quando il criterio di accesso centrale applicato non viene trovato in Active Directory

È possibile che alle risorse contenute nel server CIFS siano applicati criteri di accesso centrale, ma quando il server CIFS utilizza il SID del criterio di accesso centrale per tentare di recuperare informazioni da Active Directory, il SID non corrisponde ai SID dei criteri di accesso centrale esistenti in Active Directory. In questi casi, il server CIFS applica il criterio di ripristino locale predefinito per tale risorsa.

Il criterio di ripristino locale predefinito consente al gruppo BUILTIN/Administrators del server CIFS di accedere a tale risorsa.

Attiva o disattiva la panoramica del controllo dinamico degli accessi

L’opzione che consente di utilizzare il controllo dinamico dell’accesso (DAC) per proteggere gli oggetti sul server CIFS è disattivata per impostazione predefinita. Attivare l’opzione se si desidera utilizzare Dynamic Access Control sul server CIFS. Se in seguito si decide di non utilizzare il controllo dinamico degli accessi per proteggere gli oggetti memorizzati nel server CIFS, è possibile disattivare l’opzione.

A proposito di questa attività

Una volta attivato il controllo dinamico degli accessi, il file system può contenere ACL con voci correlate al controllo dinamico degli accessi. Se Dynamic Access Control è disattivato, le voci correnti di Dynamic Access Control verranno ignorate e non saranno consentite le nuove.

Questa opzione è disponibile solo al livello di privilegio avanzato.

Fase

1. Impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`
2. Eseguire una delle seguenti operazioni:

Se si desidera che Dynamic Access Control sia…	Immettere il comando…
Attivato	`vserver cifs options modify -vserver` *`vserver_name`* `-is-dac-enabled true`

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

3. Tornare al livello di privilegi di amministratore: `set -privilege admin`

Informazioni correlate

Configurazione delle policy di accesso centrale per proteggere i dati sui server CIFS

Gestire gli ACL che contengono le ACE di controllo dinamico degli accessi quando il controllo dinamico degli accessi è disattivato

Se si dispone di risorse con ACL applicati con ACE di controllo dinamico degli accessi e si disattiva il controllo dinamico degli accessi sulla macchina virtuale di storage (SVM), è necessario rimuovere le ACE di controllo dinamico degli accessi prima di poter gestire le ACE di controllo degli accessi non dinamico su tale risorsa.

A proposito di questa attività

Una volta disattivato il controllo dinamico degli accessi, non è possibile rimuovere le ACE di controllo degli accessi non dinamiche esistenti o aggiungere nuove ACE di controllo degli accessi non dinamiche fino a quando non sono state rimosse le ACE di controllo degli accessi dinamici esistenti.

È possibile utilizzare lo strumento utilizzato normalmente per gestire gli ACL per eseguire questi passaggi.

Fasi

1. Determinare quali ACE di controllo dinamico degli accessi vengono applicati alla risorsa.
2. Rimuovere le ACE di controllo dinamico degli accessi dalla risorsa.
3. Aggiungere o rimuovere ACE di controllo degli accessi non dinamici come desiderato dalla risorsa.

Configurare le policy di accesso centrale per proteggere i dati sui server CIFS

Per proteggere l'accesso ai dati sul server CIFS mediante criteri di accesso centrali, è necessario eseguire diversi passaggi, tra cui l'attivazione del controllo dinamico dell'accesso (DAC) sul server CIFS, la configurazione dei criteri di accesso centrale in Active Directory, l'applicazione dei criteri di accesso centrale ai container Active Directory con GPO, E abilitazione degli oggetti Criteri di gruppo sul server CIFS.

Prima di iniziare

- Active Directory deve essere configurato per utilizzare criteri di accesso centrali.
- È necessario disporre di un accesso sufficiente sui domain controller di Active Directory per creare criteri di accesso centrali e per creare e applicare gli oggetti Criteri di gruppo ai container che contengono i server CIFS.
- Per eseguire i comandi necessari, è necessario disporre di un accesso amministrativo sufficiente sulla macchina virtuale di storage (SVM).

A proposito di questa attività

I criteri di accesso centrale vengono definiti e applicati agli oggetti Criteri di gruppo (GPO) in Active Directory. Per istruzioni sulla configurazione dei criteri di accesso centrale e degli oggetti Criteri di gruppo, consultare la Microsoft TechNet Library.

"Microsoft TechNet Library"

Fasi

1. Attivare Dynamic Access Control (controllo dinamico degli accessi) su SVM se non è già attivato utilizzando `vserver cifs options modify` comando.

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

2. Abilitare gli oggetti Criteri di gruppo (GPO) sul server CIFS se non sono già abilitati mediante `vserver cifs group-policy modify` comando.

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

3. Creare regole di accesso centrali e policy di accesso centrali in Active Directory.
4. Creare un oggetto Criteri di gruppo (GPO) per implementare i criteri di accesso centrale in Active Directory.
5. Applicare l'oggetto Criteri di gruppo al container in cui si trova l'account del computer del server CIFS.
6. Aggiornare manualmente gli oggetti Criteri di gruppo applicati al server CIFS utilizzando `vserver cifs group-policy update` comando.

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

7. Verificare che il criterio di accesso centrale dell'oggetto Criteri di gruppo sia applicato alle risorse sul server CIFS utilizzando `vserver cifs group-policy show-applied` comando.

   L'esempio seguente mostra che il criterio di dominio predefinito dispone di due criteri di accesso centrali applicati al server CIFS:

   ```
   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.
```

Informazioni correlate

Visualizzazione delle informazioni sulle configurazioni dell'oggetto Criteri di gruppo

Visualizzazione di informazioni sui criteri di accesso centrale

Visualizzazione delle informazioni sulle regole dei criteri di accesso centrale

Attivazione o disattivazione del controllo dinamico degli accessi

Visualizza informazioni sulla sicurezza del controllo dinamico degli accessi

È possibile visualizzare informazioni sulla sicurezza del controllo dinamico degli accessi (DAC) sui volumi NTFS e sui dati con protezione effettiva NTFS su volumi misti di tipo sicurezza. Ciò include informazioni su ACE condizionali, ACE di risorse e ACE di policy di accesso centrale. È possibile utilizzare i risultati per convalidare la configurazione di sicurezza o per risolvere i problemi di accesso ai file.

A proposito di questa attività

Specificare il nome della macchina virtuale di storage (SVM) e il percorso dei dati di cui si desidera visualizzare le informazioni di sicurezza relative al file o alla cartella. È possibile visualizzare l'output in forma

di riepilogo o come elenco dettagliato.

Fase

1. Visualizzare le impostazioni di sicurezza di file e directory con il livello di dettaglio desiderato:

Se si desidera visualizzare le informazioni…	Immettere il seguente comando…
In forma riassuntiva	`vserver security file-directory show -vserver vserver_name -path path`
Con dettagli più dettagliati	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`
Dove viene visualizzato l'output con SID di gruppo e utente	`vserver security file-directory show -vserver vserver_name -path path -lookup-names false`
Informazioni sulla sicurezza di file e directory per file e directory in cui la bit mask esadecimale viene convertita in formato testuale	`vserver security file-directory show -vserver vserver_name -path path -textual-mask true`

Esempi

Nell'esempio riportato di seguito vengono visualizzate le informazioni di sicurezza del controllo dinamico degli accessi relative al percorso `/vol1` In 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)
```

Informazioni correlate

Visualizzazione delle informazioni sulle configurazioni dell'oggetto Criteri di gruppo

Visualizzazione di informazioni sui criteri di accesso centrale

Visualizzazione delle informazioni sulle regole dei criteri di accesso centrale

Considerazioni sul revert per il controllo dinamico degli accessi

È necessario essere consapevoli di cosa accade quando si torna a una versione di

ONTAP che non supporta il controllo dinamico degli accessi (DAC) e di cosa si deve fare prima e dopo il ripristino.

Se si desidera ripristinare il cluster a una versione di ONTAP che non supporta il controllo dinamico degli accessi e che il controllo dinamico degli accessi sia attivato su una o più macchine virtuali dello storage (SVM), prima di eseguire il ripristino è necessario eseguire le seguenti operazioni:

- È necessario disattivare il controllo dinamico degli accessi su tutte le SVM che lo hanno attivato nel cluster.
- È necessario modificare le configurazioni di controllo del cluster che contengono `cap-staging` tipo di evento per utilizzare solo `file-op` tipo di evento.

È necessario comprendere e agire in base ad alcune importanti considerazioni di revert per file e cartelle con le ACE di controllo dinamico degli accessi:

- Se il cluster viene invertito, le ACE di controllo dinamico degli accessi esistenti non vengono rimosse; tuttavia, verranno ignorate nei controlli di accesso ai file.
- Poiché le ACE di controllo dinamico degli accessi vengono ignorate dopo la revisione, l'accesso ai file cambia nei file con le ACE di controllo dinamico degli accessi.

  Ciò potrebbe consentire agli utenti di accedere a file che in precedenza non potevano o che non potevano accedere a file che in precedenza potevano.

- Per ripristinare il livello di protezione precedente, è necessario applicare ACE di controllo degli accessi non dinamici ai file interessati.

  Questa operazione può essere eseguita prima del ripristino o immediatamente dopo il completamento della revisione.

> Poiché le ACE di controllo dinamico degli accessi vengono ignorate dopo la reversione, non è necessario rimuoverle quando si applicano ACE di controllo degli accessi non dinamici ai file interessati. Tuttavia, se lo si desidera, è possibile rimuoverli manualmente.

Dove trovare ulteriori informazioni sulla configurazione e l'utilizzo del controllo dinamico degli accessi e delle policy di accesso centrali

Sono disponibili risorse aggiuntive per la configurazione e l'utilizzo di Dynamic Access Control e policy di accesso centrali.

Nella Microsoft TechNet Library sono disponibili informazioni su come configurare il controllo dinamico degli accessi e i criteri di accesso centrale in Active Directory.

"Microsoft TechNet: Panoramica dello scenario di controllo dinamico degli accessi"

"Microsoft TechNet: Scenario dei criteri di accesso centrale"

I seguenti riferimenti consentono di configurare il server SMB in modo che utilizzi e supporti il controllo dinamico degli accessi e le policy di accesso centrale:

- **Utilizzo di GPO sul server SMB**

Applicazione di oggetti Criteri di gruppo ai server SMB

- **Configurazione del controllo NAS sul server SMB**

  "Controllo SMB e NFS e tracciamento della sicurezza"