Controllo degli accessi basato su attributi

ONTAP 9

NetApp
January 08, 2025

This PDF was generated from https://docs.netapp.com/it-it/ontap/abac/abac-overview.html on January 08, 2025. Always check docs.netapp.com for the latest.

Sommario

Controllo degli accessi basato su attributi 1
Controllo degli accessi basato su attributi con ONTAP 1
Approcci ad ABAC con ONTAP 1

Controllo degli accessi basato su attributi

Controllo degli accessi basato su attributi con ONTAP

Puoi implementare un RBAC avanzato con attributi e controllo degli accessi basato sugli attributi (ABAC) utilizzando ONTAP. ONTAP fornisce diversi approcci che un cliente potrebbe utilizzare per raggiungere il livello di file ABAC, inclusi quelli etichettati NFS 4,2 e XATTRS utilizzando NFS e SMB/CIFS.

ABAC (Attribute-based Access Control) è un metodo sofisticato per la gestione dei diritti di accesso che prende in considerazione gli attributi degli utenti, le risorse e le condizioni ambientali. Il National Institute of Standards and Technology (NIST) ha stabilito uno standard per ABAC, fornendo un quadro per la sua implementazione sicura e coerente.

A partire da ONTAP 9.12,1, è possibile configurare ONTAP con NFSv4,2 etichette di sicurezza e attributi estesi (XATTRS) in modo che possa essere integrato con un controllo di accesso basato sui ruoli (RBAC) e un'identità ABAC (Attribute-based Access Control). Questa integrazione consente a ONTAP di accedere al software di controllo che viene classificato come soluzione di gestione dei dati conforme agli standard ABAC NIST, offrendo un approccio solido e avanzato alla gestione dei diritti di accesso in ambienti complessi, tra cui il punto di applicazione delle policy (PEP), un punto di decisione sulle policy (PDP) e le policy che considerano gli attributi associati all'utente, alla risorsa e all'ambiente.

L'integrazione di NetApp ONTAP con il software XATTRS (Extended Attributes) e ABAC (Attribute-Based Access Control) è in linea con le linee guida esposte nella Pubblicazione speciale NIST 800-162, assicurando la conformità agli standard NIST per l'implementazione ABAC. L'uso di etichette di sicurezza NFS 4,2 e XATTRS consente l'associazione di attributi definiti dall'utente con i file, soddisfacendo il requisito dello standard ABAC NIST per la valutazione degli attributi delle risorse nelle decisioni relative al controllo dell'accesso. Il PEP e il PDP del software ABAC si allineano ai requisiti dello standard ABAC NIST per questi componenti nel processo di controllo dell'accesso. La capacità di definire policy complesse che considerano più attributi e condizioni è in linea con il requisito dello standard NIST ABAC per il controllo degli accessi basato su policy.

Informazioni correlate

- "Approcci ad ABAC con ONTAP"
- "NFS in NetApp ONTAP: Best practice e guida all'implementazione"
- Richiesta di commenti (RFC)
  - RFC 2203: Specifica del protocollo RPCSEC_GSS
  - RFC 3530: Protocollo NFS (Network file System) versione 4

Approcci ad ABAC con ONTAP

ONTAP fornisce diversi approcci che un cliente potrebbe utilizzare per raggiungere il livello di file ABAC, inclusi quelli etichettati NFSv4,2 e XATTRS mediante NFS e SMB/CIFS.

Etichettato NFSv4,2

A partire da ONTAP 9.9,1, è supportata la funzione NFSv4,2 denominata NFS.

Labeled NFS è un modo per gestire l'accesso granulare a file e cartelle utilizzando le etichette SELinux e il Mandatory Access Control (MAC). Queste etichette MAC sono memorizzate con file e cartelle e funzionano in combinazione con autorizzazioni UNIX e ACL NFSv4.x.

Il supporto per NFS etichettato significa che ONTAP ora riconosce e comprende le impostazioni dell'etichetta SELinux del client NFS. NFS etichettato è coperto in RFC-7204.

I casi d'utilizzo per l'etichetta NFSv4,2 includono quanto segue:

- Etichettatura MAC delle immagini della macchina virtuale (VM)
- Classificazione di sicurezza dei dati per il settore pubblico (segreto, top secret e altre classificazioni)
- Conformità alla sicurezza
- Linux senza disco

Attivare etichettato NFSv4,2

È possibile attivare o disattivare NFS con la seguente opzione di privilegio avanzato:

```
[-v4.2-seclabel {enabled|disabled}] - NFSV4.2 Security Label Support
(privilege: advanced)
```

Questo parametro è facoltativo e l'impostazione predefinita è `disabled`.

Modalità di applicazione per etichettato NFSv4,2

A partire da ONTAP 9.9,1, ONTAP supporta le seguenti modalità di applicazione:

- **Modalità server limitata**: ONTAP non può applicare le etichette ma può memorizzarle e trasmetterle.

  Anche la possibilità di modificare le etichette MAC è compito del client.

- **Modalità ospite**: Se il client non è etichettato NFS-aware (v4,1 o inferiore), le etichette MAC non vengono trasmesse.

ONTAP attualmente non supporta la modalità completa (memorizzazione e applicazione delle etichette MAC).

Esempio di configurazione con etichetta NFSv4,2

Nell'esempio di configurazione riportato di seguito vengono illustrati i concetti che utilizzano Red Hat Enterprise Linux release 9,3 (Plow).

L'utente `jrsmith`, creato in base alle credenziali di John R. Smith, dispone del seguente account Privileges:

- Nome utente = `jrsmith`
- Privileges = `uid=1112(jrsmith) gid=1112(jrsmith) groups=1112(jrsmith) context=user_u:user_r:user_t:s0`

Esistono due ruoli: L'account admin che è un utente e un utente con privilegi `jrsmith`, come descritto nella seguente tabella MLS Privileges:

Utenti	Ruolo	Tipo	Livelli
admins	sysadm_r	sysadm_t	t:s0
jrsmith	user_r	user_t	t:s1 - t:s4

In questo ambiente di esempio, l'utente `jrsmith` ha accesso ai file ai `s3` livelli di `s0` . Possiamo migliorare le classificazioni di sicurezza esistenti, come descritto di seguito, per garantire che gli amministratori non abbiano accesso a dati specifici dell'utente.

- s0 = dati utente amministratore con privilegi
- s0 = dati non classificati
- s1 = riservato
- s2 = dati segreti
- s3 = dati top secret

Attenersi alle policy di sicurezza dell'organizzazione

Esempio di etichetta di sicurezza NFSv4,2 con MCS

Oltre alla protezione multilivello (MLS), un'altra funzionalità denominata protezione multi-categoria (MCS) consente di definire categorie come i progetti.

Etichetta di sicurezza NFS	Valore
entitySecurityMark	t:s01 = UNCLASSIFIED

Attributi estesi (XATTRS)

A partire da ONTAP 9.12,1, ONTAP supporta xattrs. Xattrs consente l'associazione dei metadati a file e directory oltre a quanto fornito dal sistema, come gli elenchi di controllo di accesso (ACL) o gli attributi definiti dall'utente.

Per implementare xattrs, è possibile utilizzare `setfattr` e `getfattr` le utilità della riga di comando in Linux per gestire xattrs di oggetti del file system. Questi strumenti forniscono un metodo efficace per gestire metadati aggiuntivi per file e directory. Devono essere utilizzati con cautela, anche se un uso improprio può causare comportamenti imprevisti o problemi di sicurezza. Per istruzioni dettagliate sull'uso, consultare sempre `setfattr` le pagine man e `getfattr` o altra documentazione affidabile.

Quando xattrs è abilitato su un filesystem ONTAP, gli utenti possono impostare, modificare e recuperare attributi arbitrari sui file. Questi attributi possono essere utilizzati per memorizzare informazioni aggiuntive sul file che non vengono acquisite dal set standard di attributi del file, come le informazioni sul controllo dell'accesso.

Requisiti per l'utilizzo di xattrs in ONTAP

- Red Hat Enterprise Linux versione 8,4 o successiva
- Ubuntu 22.04 o versione successiva

- Ogni file può avere fino a 128 xattrs
- le chiavi xattr sono limitate a 255 byte
- La dimensione combinata della chiave o del valore è di 1.729 byte per xattr
- Directory e file possono avere xattrs
- Per impostare e recuperare xattrs, `w` o i bit di modalità di scrittura devono essere abilitati per l'utente e il gruppo

Casi di utilizzo per xattrs

Gli xattrs sono utilizzati all'interno dello spazio dei nomi utente e non hanno alcun significato intrinseco per ONTAP stesso. Le loro applicazioni pratiche sono invece determinate e gestite esclusivamente dall'applicazione lato client che interagisce con il file system.

esempi di casi di utilizzo di xattr:

- Registrazione del nome dell'applicazione responsabile della creazione di un file.
- Mantenere un riferimento al messaggio e-mail da cui è stato ottenuto un file.
- Definizione di un framework di categorizzazione per l'organizzazione degli oggetti file.
- Etichettare i file con l'URL della fonte di download originale.

Comandi per la gestione di xattrs

- `setfattr`: Imposta un attributo esteso di un file o di una directory:

  ```
  setfattr -n <attribute_name> -v <attribute_value> <file or directory name>
  ```

  Esempio di comando:

  ```
  setfattr -n user.comment -v test example.txt
  ```

- `getfattr`: Recupera il valore di un attributo esteso specifico o elenca tutti gli attributi estesi di un file o di una directory:

  Attributo specifico: `getfattr -n <attribute_name> <file or directory name>`

  Tutti gli attributi: `getfattr <file or directory name>`

  Esempio di comando:

  ```
  getfattr -n user.comment example.txt
  ```

xattr	Valore
`user.digitalIdentifier`	`CN=John Smith jrsmith, OU=Finance, OU=U.S.ACME, O=US, C=US`
`user.countryOfAffiliations`	`USA`

Autorizzazioni utente con ACE per attributi estesi

Una voce di controllo di accesso (ACE) è un componente di un elenco di controllo di accesso (ACL) che definisce i diritti di accesso o le autorizzazioni concessi a un singolo utente o a un gruppo di utenti per una risorsa specifica, ad esempio un file o una directory. Ogni ACE specifica il tipo di accesso consentito o negato ed è associato a un'identità di protezione particolare (identità utente o gruppo).

Tipo di file	Recupera xattr	Set xattrs
File	R	A, w, T
Directory	R	T

Spiegazione delle autorizzazioni richieste per xattrs:

Recupera xattr: Autorizzazioni necessarie per la lettura degli attributi estesi di un file o di una directory. La "R" indica che è necessario il permesso di lettura. **Set xattrs**: Le autorizzazioni necessarie per modificare o impostare gli attributi estesi. "A", "w" e "T" rappresentano diversi esempi di permessi, quali append, write e un permesso specifico relativo a xattrs. **Files**: Gli utenti hanno bisogno di aggiungere, scrivere e potenzialmente di un permesso speciale relativo a xattrs per impostare attributi estesi. **Directory**: Per impostare gli attributi estesi è necessaria un'autorizzazione specifica "T".

Supporto del protocollo SMB/CIFS per xattrs

Il supporto di ONTAP per il protocollo SMB/CIFS si estende alla gestione completa degli xattrs, che sono parte integrante dei metadati dei file negli ambienti Windows. Gli attributi estesi consentono agli utenti e alle applicazioni di memorizzare informazioni aggiuntive oltre all'insieme standard di attributi di file, come i dettagli dell'autore, i descrittori di protezione personalizzati o i dati specifici dell'applicazione. L'implementazione SMB/CIFS di ONTAP garantisce il supporto completo di questi xattrs, consentendo una perfetta integrazione con i servizi e le applicazioni Windows che dipendono da questi metadati per l'applicazione delle funzionalità e dei criteri.

Quando si accede ai file o li si trasferisce su condivisioni SMB/CIFS gestite da ONTAP, il sistema preserva l'integrità degli xattrs, garantendo che tutti i metadati vengano conservati e rimangano coerenti. Ciò è particolarmente importante per mantenere le impostazioni di protezione e per le applicazioni che si basano su xattrs per la configurazione o il funzionamento. La solida gestione degli xattrs di ONTAP all'interno del contesto SMB/CIFS garantisce che la condivisione dei file su piattaforme e ambienti diversi sia affidabile e sicura, offrendo agli utenti un'esperienza perfetta e agli amministratori la garanzia che le policy di governance dei dati siano rispettate. Sia per la collaborazione, l'archiviazione dei dati o la conformità, l'attenzione di ONTAP agli xattrs all'interno delle condivisioni SMB/CIFS rappresenta il suo impegno per l'eccellenza nella gestione dei dati e l'interoperabilità in ambienti con sistemi operativi misti.

Punto di applicazione delle policy (PEP) e punto di decisione policy (PDP) in ABAC

In un sistema ABAC (Attribute-based Access Control), il PEP (Policy Enforcement Point) e il PDP (Policy Decision Point) svolgono ruoli fondamentali. Il PEP è responsabile dell'applicazione dei criteri di controllo degli accessi, mentre il PDP decide se concedere o negare l'accesso in base ai criteri.

Nel contesto del frammento di codice Python fornito, lo script stesso agisce come PEP. Applica la decisione di controllo dell'accesso concedendo l'accesso al file aprendolo e leggendo il suo contenuto o negando l'accesso sollevando un `PermissionError`.

Il PDP, d'altro canto, sarebbe parte del sistema SELinux sottostante. Quando lo script tenta di aprire il file con un contesto SELinux specifico, il sistema SELinux controlla le proprie policy per decidere se concedere o negare l'accesso. Questa decisione viene quindi imposta dallo script.

Di seguito è riportato un esempio dettagliato di come funziona questo codice in un ambiente ABAC:

1. Lo script imposta il contesto SELinux sul contesto `jrsmith` utilizzando la `selinux.setcon()` funzione. Ciò equivale a `jrsmith` tentare di accedere al file.
2. Lo script tenta di aprire il file. È qui che entra in gioco il PEP.
3. Il sistema SELinux controlla i propri criteri per vedere se `jrsmith` (o più specificamente, un utente con `jrsmith` contesto SELinux) è autorizzato ad accedere al file. Questo è il ruolo del PDP.
4. Se `jrsmith` è consentito accedere al file, il sistema SELinux consente allo script di aprire il file e lo script legge e stampa il contenuto del file.
5. Se `jrsmith` non è consentito accedere al file, il sistema SELinux impedisce allo script di aprire il file e lo script genera un `PermissionError`.
6. Lo script ripristina il contesto SELinux originale per garantire che la modifica temporanea del contesto non influisca su altre operazioni.

Utilizzando python, il codice per ottenere il contesto è mostrato di seguito dove il percorso del file variabile è il documento che deve essere controllato:

```
#Get the current context

context = selinux.getfilecon(file_path)[1]
```

Clonazione ONTAP e SnapMirror

Le tecnologie di clonazione e SnapMirror di ONTAP sono progettate per fornire funzionalità di replica e clonazione dei dati efficienti e affidabili, garantendo che tutti gli aspetti dei dati dei file, compresi gli attributi estesi (xattrs), vengano preservati e trasferiti insieme al file. Le xattrs sono fondamentali per la memorizzazione di metadati aggiuntivi associati a un file, come etichette di sicurezza, informazioni di controllo degli accessi e dati definiti dall'utente, essenziali per mantenere il contesto e l'integrità del file.

Quando un volume viene clonato utilizzando la tecnologia FlexClone di ONTAP, viene creata una replica scrivibile esatta del volume. Questo processo di cloning è istantaneo, efficiente in termini di spazio e include tutti i dati e i metadati dei file per assicurare la replica completa delle xattrs. Allo stesso modo, SnapMirror garantisce che i dati vengano mirrorati su un sistema secondario, con piena fedeltà. Questo include xattrs, che sono fondamentali per le applicazioni che si basano su questi metadati per funzionare correttamente.

Includendo xattrs in operazioni di cloning e replica, NetApp ONTAP garantisce che il set di dati completo, con tutte le sue caratteristiche, sia disponibile e coerente nei sistemi di storage primario e secondario. Questo approccio completo alla gestione dei dati è fondamentale per le organizzazioni che richiedono una data Protection coerente, un recovery rapido e il rispetto degli standard normativi e di compliance. Inoltre, semplifica la gestione dei dati in diversi ambienti, sia on-premise che nel cloud, offrendo agli utenti la certezza che i loro dati saranno completi e inalterati durante i processi.

Le etichette di sicurezza NFSv4,2 hanno le avvertenze definite in 2.

Esempi di controllo dell'accesso ai dati

La seguente voce di esempio per i dati memorizzati nel cert PKI di John R Smith mostra come l'approccio di NetApp può essere applicato a un file e fornire un controllo di accesso dettagliato.

Questi esempi sono a scopo illustrativo ed è responsabilità del governo definire quali metadati sono NFSv4,2 Security label e xattrs. I dettagli sull'aggiornamento e sulla conservazione delle etichette vengono omessi per semplicità.

Chiave	Valore
EntitySecurityMark	t:S01 = NON CLASSIFICATO

Info	{
	"commonName": {
	"value": "Smith John R jrsmith"
	},
	"emailAddresses": [
	{
	"value": "jrsmith@dod.mil"
	}
	],
	"employeeId": {
	"value": "00000387835"
	},
	"firstName": {
	"value": "John"
	},
	"lastName": {
	"value": "Smith"
	},
	"telephoneNumber": {
	"value": "938/260-9537"
	},
	"uid": {
	"value": "jrsmith"
	}
	}

specifiche	"DoD"
uuid	b4111349-7875-4115-ad30-0928565f2e15

AdminOrganization	{
	"value": "DoD"
	}

Chiave	Valore

briefing	[
	{
	"value": "ABC1000"
	},
	{
	"value": "DEF1001"
	},
	{
	"value": "EFG2000"
	}
	]

CitizenshipStatus	{
	"value": "US"
	}

giochi	[
	{
	"value": "TS"
	},
	{
	"value": "S"
	},
	{
	"value": "C"
	},
	{
	"value": "U"
	}
	]

CountryOfAffiliations	[
	{
	"value": "USA"
	}
	]

Chiave	Valore

DigitalIdentifier	{
	"classification": "UNCLASSIFIED",
	"value": "cn=smith john r jrsmith, ou=dod, o=u.s. government, c=us"
	}

DissemTos	{
	"value": "DoD"
	}

DutyOrganization	{
	"value": "DoD"
	}

EntityType	{
	"value": "GOV"
	}

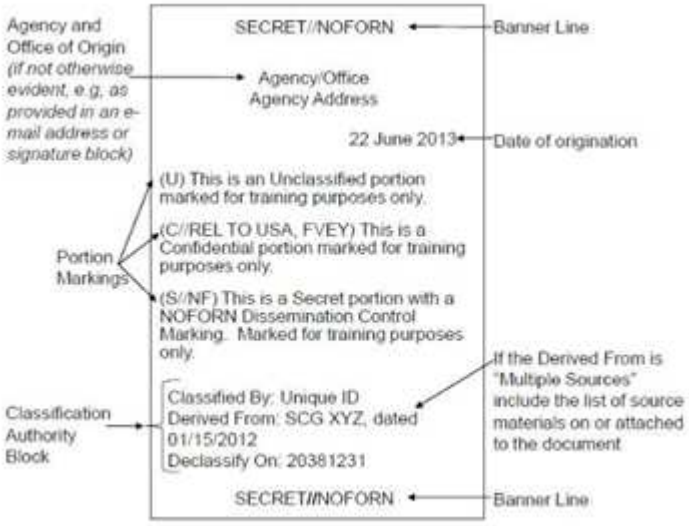
FineAccessControls	[
	{
	"value": "SI"
	},
	{
	"value": "TK"
	},
	{
	"value": "NSYS"
	}
	]

Questi diritti PKI mostrano i dettagli di accesso di John R. Smith, incluso l'accesso per tipo di dati e attribuzione.

Se John R. Smith creasse e salvasse un documento denominato *"sample_analysis.doc"*, in base alle pertinenti direttive politiche, l'utente aggiungerebbe i contrassegni di intestazione e porzione appropriati, l'agenzia e l'ufficio di origine e il blocco dell'autorità di classificazione appropriato in base alla classificazione del documento come mostrato nell'immagine seguente. Questi metadati ricchi sono comprensibili solo dopo che

sono stati scansionati da Natural Language Processing (NLP) e che sono state applicate regole per rendere il significato dai contrassegni. Strumenti come la classificazione NetApp BlueXP possono fare questo, ma sono meno efficienti per le decisioni relative al controllo dell'accesso perché richiedono l'autorizzazione a esaminare il documento.

Marcatura non classificata della porzione del documento CAPCO



Negli scenari in cui i metadati IC-TDF vengono archiviati separatamente dal file, NetApp sostiene la necessità di un ulteriore livello di controllo degli accessi dettagliato. Ciò comporta l'archiviazione delle informazioni di controllo dell'accesso sia a livello di directory che in associazione con ciascun file. Ad esempio, considerare i seguenti tag collegati a un file:

- NFSv4,2 etichette di sicurezza: Utilizzate per prendere decisioni sulla sicurezza
- Xattrs: Fornire informazioni supplementari pertinenti al file e ai requisiti del programma organizzativo

Le seguenti coppie di valori chiave sono esempi di metadati che possono essere memorizzati come xattrs e offrono informazioni dettagliate sull'autore del file e sulle relative classificazioni di sicurezza. Tali metadati possono essere utilizzati dalle applicazioni client per prendere decisioni di accesso informate e organizzare i file in base a standard e requisiti organizzativi.

Chiave	Valore
`user.uuid`	`"761d2e3c-e778-4ee4-997b-3bb9a6a1d3fa"`
`user.entitySecurityMark`	`"UNCLASSIFIED"`
`user.specification`	`"INFO"`

Chiave	Valore

user.Info	{
	"commonName": {
	"value": "Smith John R jrsmith"
	},
	"currentOrganization": {
	"value": "TUV33"
	},
	"displayName": {
	"value": "John Smith"
	},
	"emailAddresses": [
	"jrsmith@example.org"
	],
	"employeeId": {
	"value": "00000405732"
	},
	"firstName": {
	"value": "John"
	},
	"lastName": {
	"value": "Smith"
	},
	"managers": [
	{
	"value": ""
	}
	],
	"organizations": [
	{
	"value": "TUV33"
	},
	{
	"value": "WXY44"
	}
	],
	"personalTitle": {
	"value": ""
	},
	"secureTelephoneNumber": {
	"value": "506-7718"
	},
	"telephoneNumber": {
	"value": "264/160-7187"
	},
	"title": {
	"value": "Software Engineer"
	},

Chiave	Valore
user.geo_point	[-78.7941, 35.7956]

```
    }
```

Controllo delle modifiche alle etichette

Il controllo delle modifiche alle etichette di sicurezza xattrs o NFS è un aspetto critico della gestione e della sicurezza del file system. Gli strumenti standard di audit del file system consentono il monitoraggio e la registrazione di tutte le modifiche apportate a un file system, incluse le modifiche agli attributi estesi e alle etichette di sicurezza.

Negli ambienti Linux, il `auditd` demone è comunemente usato per stabilire il controllo degli eventi del file system. Consente agli amministratori di configurare le regole per controllare chiamate di sistema specifiche correlate alle modifiche xattr, quali `setxattr`, `lsetxattr` e per impostare gli attributi e, `lremovexattr` e `fsetxattr` per la `fremovexattr` rimozione degli attributi `removexattr`.

ONTAP FPolicy estende queste funzionalità fornendo un solido framework per il monitoraggio e il controllo in tempo reale delle operazioni sui file. FPolicy può essere configurato per supportare vari eventi xattr, offrendo un controllo granulare sulle operazioni dei file e la capacità di applicare policy di gestione dei dati complete.

Per gli utenti che utilizzano xattrs, specialmente negli ambienti NFSv3 e NFSv4, sono supportate solo alcune combinazioni di operazioni e filtri per il monitoraggio. L'elenco delle combinazioni di operazioni e filtri supportate per il monitoraggio FPolicy degli eventi di accesso ai file NFSv3 e NFSv4 è descritto di seguito:

Operazioni di file supportate	Filtri supportati
setattr	offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_modify_time_change, setattr_with_access_time_change, setattr_with_size_change, exclude_directory

Esempio di un frammento di registro auditd per un'operazione setattr:

```
type=SYSCALL msg=audit(1713451401.168:106964): arch=c000003e syscall=188
success=yes exit=0 a0=7fac252f0590 a1=7fac251d4750 a2=7fac252e50a0 a3=25
items=1 ppid=247417 pid=247563 auid=1112 uid=1112 gid=1112 euid=1112
suid=1112 fsuid=1112 egid=1112 sgid=1112 fsgid=1112 tty=pts0 ses=141
comm="python3" exe="/usr/bin/python3.9"
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
key="*set-xattr*"ARCH=x86_64 SYSCALL=**setxattr** AUID="jrsmith"
UID="jrsmith" GID="jrsmith" EUID="jrsmith" SUID="jrsmith"
FSUID="jrsmith" EGID="jrsmith" SGID="jrsmith" FSGID="jrsmith"
```

L'attivazione di ONTAP FPolicy per gli utenti che lavorano con xattrs fornisce un livello di visibilità e controllo essenziale per mantenere l'integrità e la sicurezza del file system. Sfruttando le funzionalità di monitoraggio avanzate di FPolicy, le organizzazioni possono garantire che tutte le modifiche apportate agli xattrs vengano monitorate, controllate e allineate ai loro standard di sicurezza e conformità. Questo approccio proattivo alla

gestione del file system è per questo motivo l'attivazione di ONTAP FPolicy è vivamente consigliata a tutte le organizzazioni che desiderano migliorare le proprie strategie di data governance e protezione.

Integrazione con il software ABAC Identity and Access Control

Per sfruttare appieno le funzionalità del controllo degli accessi basato sugli attributi (ABAC), ONTAP può integrarsi con un software di gestione degli accessi e delle identità orientato all'ABAC.

> In parallelo a questo contenuto, NetApp dispone di un'implementazione di riferimento che utilizza GreyBox. Un presupposto per questo contenuto è che i servizi di identità, autenticazione e accesso del governo includano almeno un punto di applicazione delle policy (PEP, Policy Enforcement Point) e un punto di decisione delle policy (PDP, Policy Decision Point) che fungono da intermediari per l'accesso al file system.

In un ambiente pratico, un'organizzazione impiegherebbe una combinazione di etichette di sicurezza NFS e xattrs. Vengono utilizzati per rappresentare una varietà di metadati, tra cui classificazione, protezione, applicazione e contenuto, che sono tutti elementi fondamentali per prendere decisioni ABAC. XATTR, ad esempio, può essere utilizzato per memorizzare gli attributi delle risorse utilizzati da PDP per il processo decisionale. È possibile definire un attributo per rappresentare il livello di classificazione di un file (ad esempio, "non classificato", "riservato", "segreto" o "Segreto principale"). Il PDP potrebbe quindi utilizzare questo attributo per applicare un criterio che limita l'accesso degli utenti solo ai file con un livello di classificazione uguale o inferiore al livello di verifica.

Esempio di flusso di processo per ABAC

1. L'utente presenta le credenziali (ad esempio, PKI, OAuth, SAML) per l'accesso al sistema PEP e ottiene i risultati da PDP.

   Il ruolo del PEP è quello di intercettare la richiesta di accesso dell'utente e inoltrarla al PDP.

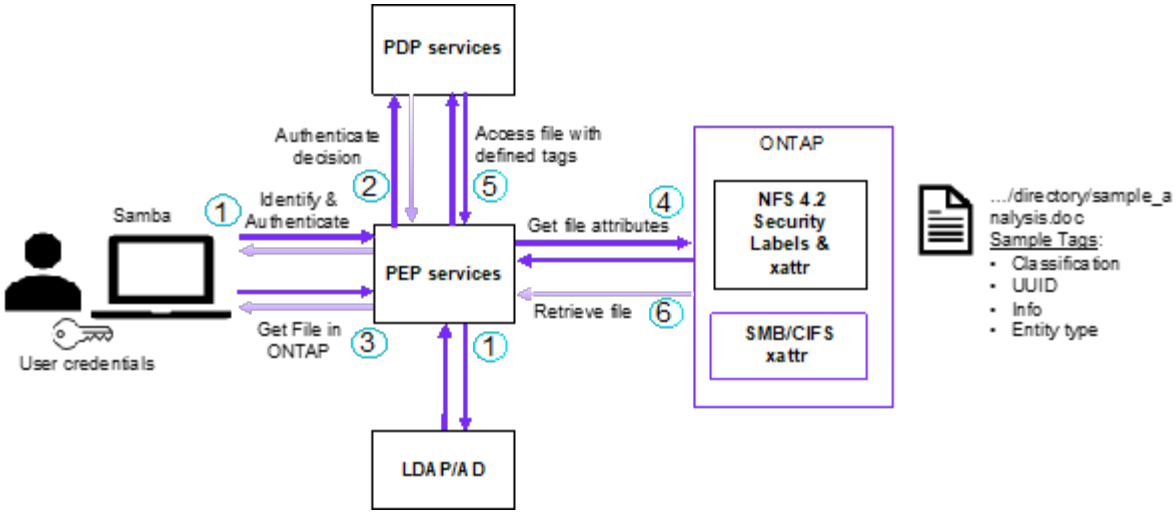
2. Il PDP valuta quindi questa richiesta in base ai criteri ABAC stabiliti.

   Questi criteri considerano diversi attributi correlati all'utente, alla risorsa in questione e all'ambiente circostante. Sulla base di questi criteri, il PDP prende una decisione di accesso per consentire o negare e quindi comunica questa decisione al PEP.

   PDP fornisce criteri a PEP da applicare. Il PEP applica quindi questa decisione, concedendo o negando la richiesta di accesso dell'utente in base alla decisione del PDP.

3. Dopo una richiesta riuscita, l'utente richiede un file memorizzato in ONTAP (ad esempio, AFF, AFF-C).
4. Se la richiesta viene eseguita correttamente, PEP riceve dal documento i tag di controllo dell'accesso con precisione.
5. PEP richiede un criterio per l'utente in base ai certificati di quell'utente.
6. PEP prende una decisione in base a criteri e tag se l'utente ha accesso al file e consente all'utente di recuperare il file.

> L'accesso effettivo potrebbe essere eseguito utilizzando token non proxy attraverso.



Informazioni correlate

- "NFS in NetApp ONTAP: Best practice e guida all'implementazione"
- Richiesta di commenti (RFC)
  - RFC 2203: Specifica del protocollo RPCSEC_GSS
  - RFC 3530: Protocollo NFS (Network file System) versione 4

Informazioni sul copyright

Copyright © 2025 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEQUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina http://www.netapp.com/TM sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.