Control de acceso basado en atributos

ONTAP 9

NetApp
December 20, 2024

Tabla de contenidos

Control de acceso basado en atributos

Control de acceso basado en atributos con ONTAP

Puede implementar RBAC mejorado con atributos y control de acceso basado en atributos (ABAC) mediante ONTAP. ONTAP ofrece varios métodos que un cliente puede utilizar para conseguir ABAC a nivel de archivos, como NFS 4,2 y XATTRS mediante NFS y SMB/CIFS.

El control de acceso basado en atributos (ABAC) es un método sofisticado para administrar los derechos de acceso que tiene en cuenta los atributos del usuario, los atributos de los recursos y las condiciones ambientales. El Instituto Nacional de Estándares y Tecnología (NIST) ha establecido un estándar para ABAC, proporcionando un marco para su implementación segura y consistente.

A partir de ONTAP 9.12,1, puede configurar ONTAP con etiquetas de seguridad NFSv4,2 y atributos extendidos (XATTRS) para que se pueda integrar con una identidad de control de acceso basado en roles (RBAC) y control de acceso basado en atributos (ABAC). Esta integración permite a ONTAP acceder al software de control que se clasifica como una solución de gestión de datos compatible con NIST ABAC, que ofrece un enfoque sólido y avanzado para administrar los derechos de acceso en entornos complejos, incluidos el punto de aplicación de políticas (PEP), un punto de decisión de políticas (PDP) y políticas que consideran los atributos asociados con el usuario, el recurso y el entorno.

La integración de NetApp ONTAP con los atributos extendidos (XATTRS) y el software de control de acceso basado en atributos (ABAC) está en consonancia con las directrices establecidas en la Publicación especial del NIST 800-162, lo que garantiza el cumplimiento de los estándares del NIST para la implementación de ABAC. El uso de etiquetas de seguridad NFS 4,2 y XATTRS permite la asociación de atributos definidos por el usuario con archivos, cumpliendo con los requisitos del estándar NIST ABAC para considerar atributos de recursos en las decisiones de control de acceso. El PEP y el PDP del software ABAC se alinean con los requisitos del estándar NIST ABAC para estos componentes en el proceso de control de acceso. La capacidad de definir políticas complejas que tengan en cuenta varios atributos y condiciones se alinea con el requisito del estándar NIST ABAC para el control de acceso basado en políticas.

Información relacionada

- "Aproximaciones a ABAC con ONTAP"
- "NFS en NetApp ONTAP: Prácticas recomendadas y guía de implementación"
- Solicitud de comentarios (RFC)
  - RFC 2203: Especificación del protocolo RPCSEC_GSS
  - RFC 3530: Protocolo de sistema de archivos de red (NFS) versión 4

Aproximaciones a ABAC con ONTAP

ONTAP proporciona varias formas que un cliente puede utilizar para conseguir ABAC a nivel de archivo, por ejemplo, NFSv4,2 y XATTRS mediante NFS y SMB/CIFS.

Etiquetado como NFSv4,2

A partir de ONTAP 9.9,1, se admite la función NFSv4,2 llamada NFS.

NFS etiquetado es una forma de administrar el acceso granular a archivos y carpetas mediante el uso de

etiquetas SELinux y Control de Acceso Obligatorio (MAC). Estas etiquetas MAC se almacenan con archivos y carpetas, y funcionan junto con permisos UNIX y ACL NFSv4.x.

La compatibilidad con NFS etiquetado significa que ONTAP ahora reconoce y comprende la configuración de etiqueta SELinux del cliente NFS. La etiqueta NFS se trata en RFC-7204.

Entre los casos de uso de NFSv4,2 se incluyen los siguientes:

- Etiquetado MAC de imágenes de máquinas virtuales (VM)
- Clasificación de seguridad de datos para el sector público (secreto, alto secreto y otras clasificaciones)
- Cumplimiento de normativas de seguridad
- Linux sin disco

Habilitar con etiqueta NFSv4,2

Puede habilitar o deshabilitar NFS etiquetado con la siguiente opción de privilegio avanzado:

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

Este parámetro es opcional y el valor predeterminado es `disabled`.

Modos de aplicación para la etiqueta NFSv4,2

A partir de ONTAP 9.9,1, ONTAP admite los siguientes modos de aplicación:

- **Modo de servidor limitado**: ONTAP no puede hacer cumplir las etiquetas, pero puede almacenarlas y transmitirlas.

  La posibilidad de cambiar las etiquetas MAC también depende del cliente para exigir la aplicación.

- **Modo invitado**: Si el cliente no está etiquetado como NFS-Aware (v4,1 o inferior), las etiquetas MAC no se transmiten.

ONTAP no admite actualmente el modo completo (almacenamiento y aplicación de etiquetas MAC).

Ejemplo de configuración de etiquetado NFSv4,2

En el siguiente ejemplo de configuración se muestran los conceptos que utilizan Red Hat Enterprise Linux versión 9,3 (Plow).

El usuario `jrsmith`, creado en función de las credenciales de John R. Smith, tiene el siguiente Privileges de cuenta:

- Nombre de usuario = `jrsmith`
- Privileges = `uid=1112(jrsmith) gid=1112(jrsmith) groups=1112(jrsmith) context=user_u:user_r:user_t:s0`

Hay dos roles: La cuenta admin que es un usuario y usuario con privilegios `jrsmith`, como se describe en la siguiente tabla Privileges MLS:

Usuarios	Función	Tipo	Niveles
admins	sysadm_r	sysadm_t	t:s0
jrsmith	user_r	user_t	t:s1 - t:s4

En este entorno de ejemplo, el usuario `jrsmith` tiene acceso a los archivos en los niveles `s0` a `s3`. Podemos mejorar las clasificaciones de seguridad existentes, como se describe a continuación, para garantizar que los administradores no tengan acceso a datos específicos del usuario.

- s0 = datos de usuario administrador de privilegios
- s0 = datos no clasificados
- s1 = confidencial
- s2 = datos secretos
- s3 = datos secretos superiores

Siga las políticas de seguridad de su organización

Ejemplo de etiqueta de seguridad NFSv4,2 con MCS

Además de la Seguridad multinivel (MLS), otra capacidad llamada Seguridad de varias categorías (MCS) le permite definir categorías como proyectos.

Etiqueta de seguridad de NFS	Valor
entitySecurityMark	t:s01 = UNCLASSIFIED

Atributos ampliados (XATTRS)

A partir de ONTAP 9.12,1, ONTAP admite xattrs. Xattrs permite que los metadatos se asocien a archivos y directorios más allá de lo que proporciona el sistema, como las listas de control de acceso (ACL) o los atributos definidos por el usuario.

Para implementar xattrs, puede usar `setfattr` utilidades de línea de comandos y `getfattr` en Linux para administrar xattrs de objetos del sistema de archivos. Estas herramientas proporcionan una manera poderosa de administrar metadatos adicionales para archivos y directorios. Se deben usar con cuidado, ya que el uso inadecuado puede conducir a un comportamiento inesperado o problemas de seguridad. Consulte siempre `setfattr` las páginas del manual y `getfattr` u otra documentación fiable para obtener instrucciones de uso detalladas.

Cuando xattrs está habilitado en un sistema de archivos ONTAP, los usuarios pueden configurar, modificar y recuperar atributos arbitrarios en los archivos. Estos atributos se pueden utilizar para almacenar información adicional sobre el archivo que no es capturado por el conjunto estándar de atributos de archivo, como la información de control de acceso.

Requisitos para el uso de xattrs en ONTAP

- Red Hat Enterprise Linux 8,4 o posterior

- Ubuntu 22.04 o posterior
- Cada archivo puede tener hasta 128 xattrs
- las claves xattr están limitadas a 255 bytes
- El tamaño de clave o valor combinado es de 1.729 bytes por xattr
- Los directorios y archivos pueden tener xattrs
- Para establecer y recuperar xattrs, `w` o bits de modo de escritura deben estar activados para el usuario y el grupo

Casos de uso para xattrs

Los xattrs se utilizan dentro del espacio de nombres del usuario y no tienen ningún significado intrínseco al propio ONTAP. En cambio, sus aplicaciones prácticas son determinadas y gestionadas exclusivamente por la aplicación del lado cliente que interactúa con el sistema de archivos.

ejemplos de casos de uso de xattr:

- Registro del nombre de la aplicación responsable de la creación de un archivo.
- Mantener una referencia al mensaje de correo electrónico del que se obtuvo un archivo.
- Establecimiento de un marco de categorización para organizar objetos de archivo.
- Etiquetar archivos con la URL de su fuente de descarga original.

Comandos para gestionar xattrs

- `setfattr`: Establece un atributo extendido de un archivo o directorio:

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

  Comando de ejemplo:

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

- `getfattr`: Recupera el valor de un atributo extendido específico o muestra todos los atributos extendidos de un archivo o directorio:

  Atributo Específico: `getfattr -n <attribute_name> <file or directory name>`

  Todos los atributos: `getfattr <file or directory name>`

  Comando de ejemplo:

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

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

Permisos de usuario con ACE para atributos ampliados

Una entrada de control de acceso (ACE) es un componente dentro de una lista de control de acceso (ACL) que define los derechos o permisos de acceso otorgados a un usuario individual o a un grupo de usuarios para un recurso específico, como un archivo o un directorio. Cada ACE especifica el tipo de acceso permitido o denegado y está asociado a un principal de seguridad en particular (identidad de usuario o grupo).

Tipo de archivo	Recuperar xattr	Establezca xattrs
Archivo	R	A,w,T
Directorio	R	T

Explicación de los permisos requeridos para xattrs:

Recuperar xattr: Los permisos necesarios para que un usuario lea los atributos extendidos de un archivo o directorio. La “R” significa que el permiso de lectura es necesario. **Set xattrs**: Los permisos necesarios para modificar o establecer los atributos extendidos. “A”, “w” y “T” representan diferentes ejemplos de permisos, tales como agregar, escribir y un permiso específico relacionado con xattrs. **Archivos**: Los usuarios necesitan agregar, escribir y potencialmente un permiso especial relacionado con xattrs para establecer atributos extendidos. **Directorios**: Se requiere un permiso específico “T” para establecer atributos extendidos.

Compatibilidad con el protocolo SMB/CIFS para xattrs

La compatibilidad de ONTAP con el protocolo SMB/CIFS se amplía hasta el manejo completo de xattrs, que es una parte integral de los metadatos de archivos en entornos Windows. Los atributos ampliados permiten a los usuarios y a las aplicaciones almacenar información adicional más allá del conjunto estándar de atributos de archivo, como detalles de autor, descriptores de seguridad personalizados o datos específicos de la aplicación. La implementación de SMB/CIFS de ONTAP garantiza que estos xattrs sean totalmente compatibles, lo que permite una integración perfecta con las aplicaciones y los servicios de Windows que dependen de estos metadatos para garantizar la funcionalidad y la aplicación de políticas.

Cuando se accede a los archivos o se transfieren a través de recursos compartidos SMB/CIFS que gestiona ONTAP, el sistema conserva la integridad de xattrs, lo que garantiza que todos los metadatos se conservan y permanecen consistentes. Esto es particularmente importante para mantener la configuración de seguridad y para las aplicaciones que dependen de xattrs para la configuración o el funcionamiento. Gracias a la sólida gestión de xattrs por parte de ONTAP en el contexto de SMB/CIFS, el uso compartido de archivos entre diferentes plataformas y entornos es fiable y seguro, lo que proporciona a los usuarios una experiencia fluida y a los administradores la seguridad de que se mantendrán las políticas de gobierno de datos. Ya sea para la colaboración, el archivado de datos o el cumplimiento de normativas, la atención de ONTAP hacia los puntos xattrs en recursos compartidos de SMB/CIFS representa su compromiso con la excelencia en la gestión de datos y la interoperabilidad en entornos de sistemas operativos mixtos.

Punto de aplicación de políticas (PEP) y Punto de decisión de políticas (PDP) en ABAC

En un sistema de control de acceso basado en atributos (ABAC), el punto de aplicación de políticas (PEP) y el punto de decisión de políticas (PDP) desempeñan funciones cruciales. El PEP es responsable de hacer cumplir las políticas de control de acceso, mientras que el PDP toma la decisión de conceder o denegar el acceso basado en las políticas.

En el contexto del fragmento de código Python proporcionado, el script en sí actúa como PEP. Hace cumplir la decisión de control de acceso ya sea otorgando acceso al archivo abriéndolo y leyendo su contenido o denegando el acceso mediante la elevación de un `PermissionError`.

El PDP, por otro lado, sería parte del sistema SELinux subyacente. Cuando el script intenta abrir el archivo con un contexto SELinux específico, el sistema SELinux comprueba sus políticas para decidir si otorgar o denegar el acceso. Esta decisión es entonces aplicada por el script.

A continuación se muestra un ejemplo detallado de cómo funciona este código en un entorno ABAC:

1. El script define el contexto SELinux en `jrsmith` el contexto mediante la `selinux.setcon()` función. Esto equivale a `jrsmith` intentar acceder al archivo.
2. El script intenta abrir el archivo. Aquí es donde entra en juego el PEP.
3. El sistema SELinux comprueba sus políticas para ver si `jrsmith` (o más específicamente, un usuario con `jrsmith` contexto SELinux) puede acceder al archivo. Este es el papel del PDP.
4. Si `jrsmith` se permite acceder al archivo, el sistema SELinux permite que el script abra el archivo y el script lea e imprima el contenido del archivo.
5. Si `jrsmith` no se permite acceder al archivo, el sistema SELinux impide que el script abra el archivo y el script emite un `PermissionError`.
6. El script restaura el contexto SELinux original para asegurarse de que el cambio de contexto temporal no afecta a otras operaciones.

Usando python, el código para obtener el contexto se muestra a continuación donde la ruta de archivo variable es el documento que se debe comprobar:

```
#Get the current context

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

Clonado ONTAP y SnapMirror

Las tecnologías de clonado y SnapMirror de ONTAP están diseñadas para proporcionar funciones de replicación y clonado de datos eficientes y fiables, lo que garantiza que todos los aspectos de los datos de ficheros, incluidos los atributos extendidos (xattrs), se preserven y se transfieren junto con el fichero. Los xattrs son fundamentales al almacenar metadatos adicionales asociados con un fichero, como etiquetas de seguridad, información de control de acceso y datos definidos por el usuario, que son esenciales para mantener el contexto y la integridad del fichero.

Cuando se clona un volumen con tecnología FlexClone de ONTAP, se crea una réplica exacta del volumen que puede escribirse. Este proceso de clonación es instantáneo y ocupa poco espacio, e incluye todos los datos y metadatos de ficheros, lo que garantiza que xattrs se repliquen en su totalidad. De igual modo, SnapMirror garantiza que los datos se dupliquen en un sistema secundario con una fidelidad total. Esto incluye xattrs, que son cruciales para las aplicaciones que dependen de estos metadatos para funcionar correctamente.

Al incluir xattrs en operaciones de clonado y de replicación, NetApp ONTAP garantiza que todo el conjunto de datos, con todas sus características, esté disponible y sea consistente en sistemas de almacenamiento primario y secundario. Este enfoque integral de la gestión de datos es vital para las organizaciones que necesitan una protección de datos consistente, una recuperación rápida y el cumplimiento de normativas y estándares normativos. También simplifica la gestión de los datos en diferentes entornos, ya sea local o en el cloud, lo que proporciona a los usuarios la seguridad de que los datos están completos y que no se alteran durante estos procesos.

Las etiquetas de seguridad NFSv4,2 tienen las advertencias definidas en 2.

Ejemplos de control del acceso a los datos

La siguiente entrada de ejemplo para los datos almacenados en el certificado PKI de John R Smith muestra cómo se puede aplicar el enfoque de NetApp a un archivo y proporcionar un control de acceso detallado.

Estos ejemplos son para fines ilustrativos, y es responsabilidad del gobierno definir qué metadatos son la etiqueta de seguridad NFSv4,2 y xattrs. Los detalles sobre la actualización y la retención de etiquetas se omiten para mayor simplicidad.

Clave	Valor
Entidad SecurityMark	t:S01 = SIN CLASIFICAR

Información	{
	"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"
	}
	}

especificación	DoD
uuid	b4111349-7875-4115-ad30-0928565f2e15

Clave	Valor

AdminOrganization	{
	"value": "DoD"
	}

reuniones informativas	[
	{
	"value": "ABC1000"
	},
	{
	"value": "DEF1001"
	},
	{
	"value": "EFG2000"
	}
	]

CitizenshipStatus	{
	"value": "US"
	}

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

Clave	Valor

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

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

DissemTos	{
	"value": "DoD"
	}

DutyOrganization	{
	"value": "DoD"
	}

Tipo de entidad	{
	"value": "GOV"
	}

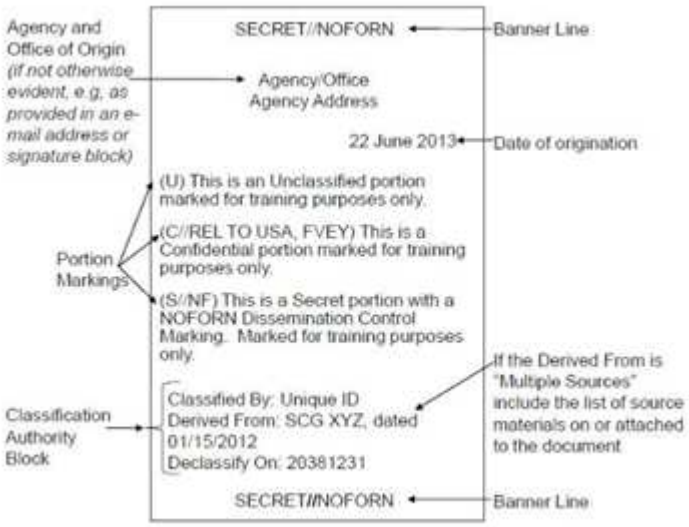
Clave	Valor

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

Estos derechos de PKI muestran los detalles de acceso de John R. Smith, incluido el acceso por tipo de datos y atribución.

Si John R. Smith creara y guardara un documento llamado *"sample_analysis.doc"*, de acuerdo con las emisiones pertinentes de la guía de políticas, el usuario agregaría el banner y las marcas de porciones apropiadas, la agencia y la oficina de origen, y el bloque de autoridad de clasificación apropiado basado en la clasificación del documento como se muestra en la siguiente imagen. Estos metadatos enriquecidos solo son comprensibles después de que han sido escaneados por Natural Language Processing (NLP) y se han aplicado reglas para hacer significado a partir de las marcas. Las herramientas como la Clasificación NetApp BlueXP pueden hacerlo, pero son menos eficientes para las decisiones de control de acceso, ya que requieren permiso para mirar dentro del documento.

Marcado de partes de documentos CAPCO sin clasificar



En situaciones en las que los metadatos de IC-TDF se almacenan por separado del archivo, NetApp aboga por una capa adicional de control de acceso detallado. Esto implica almacenar la información de control de acceso tanto a nivel de directorio como en asociación con cada archivo. Por ejemplo, considere las siguientes etiquetas vinculadas a un archivo:

- Etiquetas de seguridad NFSv4,2: Se utilizan para tomar decisiones de seguridad
- Xattrs: Proporcionar información complementaria pertinente al archivo y los requisitos del programa organizativo

Los siguientes pares clave-valor son ejemplos de metadatos que podrían almacenarse como xattrs y ofrecen información detallada sobre el creador del archivo y las clasificaciones de seguridad asociadas. Estos metadatos pueden ser aprovechados por las aplicaciones cliente para tomar decisiones de acceso informadas y para organizar archivos de acuerdo con los estándares y requisitos de la organización.

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

Clave	Valor

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"
	},

Clave	Valor
`user.geo_point`	`[-78.7941, 35.7956]`

```
    }
}
```

Auditoría de cambios en las etiquetas

La auditoría de cambios en xattrs o etiquetas de seguridad NFS es un aspecto crítico de la administración y seguridad del sistema de archivos. Las herramientas de auditoría estándar del sistema de archivos permiten supervisar y registrar todos los cambios en un sistema de archivos, incluidas las modificaciones en atributos ampliados y etiquetas de seguridad.

En entornos Linux, el `auditd` daemon se utiliza comúnmente para establecer la auditoría de eventos del sistema de archivos. Permite a los administradores configurar reglas para vigilar las llamadas del sistema específicas relacionadas con los cambios de xattr, `setxattr` como , `lsetxattr` y `fsetxattr` para definir atributos y, `lremovexattr` y `fremovexattr` para `removexattr` eliminar atributos.

FPolicy de ONTAP amplía estas funciones al proporcionar un sólido marco para la supervisión en tiempo real y el control de las operaciones de archivos. FPolicy se puede configurar para admitir diversos eventos xattr, lo que ofrece un control granular de las operaciones de archivos y la capacidad de aplicar directivas de gestión de datos completas.

Para los usuarios que utilizan xattrs, especialmente en entornos NFSv3 y NFSv4, solo se admiten ciertas combinaciones de operaciones de archivos y filtros para la supervisión. A continuación se detalla la lista de combinaciones de filtros y funcionamiento de archivos compatibles para la supervisión de FPolicy de eventos de acceso a archivos NFSv3 y NFSv4:

Operaciones de archivos admitidas	Filtros compatibles
`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`

Ejemplo de un fragmento de log auditd para una operación 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"
```

Habilitar FPolicy de ONTAP para usuarios que trabajan con xattrs proporciona una capa de visibilidad y control que es esencial para mantener la integridad y la seguridad del sistema de archivos. Al aprovechar las

capacidades avanzadas de supervisión de FPolicy, las organizaciones pueden garantizar que se realicen un seguimiento, se auditen y se alineen con sus estándares de seguridad y cumplimiento. Este enfoque proactivo de la gestión de sistemas de archivos es la razón por la que habilitar FPolicy de ONTAP es una opción muy recomendada para cualquier organización que busque mejorar sus estrategias de protección y gobierno de los datos.

Integración con el software de control de acceso e identidad ABAC

Para aprovechar al máximo las capacidades del control de acceso basado en atributos (ABAC), ONTAP puede integrarse con un software de gestión de acceso e identidad orientado a ABAC.

> En paralelo a este contenido, NetApp tiene una implementación de referencia usando GreyBox. Una suposición para este contenido es que los servicios de identidad, autenticación y acceso del gobierno incluyen, como mínimo, un punto de aplicación de políticas (PEP) y un punto de decisión de políticas (PDP) que actúan como intermediarios para el acceso al sistema de archivos.

En una configuración práctica, una organización utilizaría una combinación de etiquetas de seguridad NFS y xattrs. Estos se usan para representar una gran variedad de metadatos, incluida la clasificación, la seguridad, las aplicaciones y el contenido, los cuales juegan un papel decisivo en la toma de decisiones sobre ABAC. XATTR, por ejemplo, se puede utilizar para almacenar los atributos de recursos que el PDP utiliza para su proceso de toma de decisiones. Se puede definir un atributo para representar el nivel de clasificación de un archivo (por ejemplo, «Sin clasificar», «Confidencial», «Secreto» o «Secreto superior»). A continuación, el PDP podría utilizar este atributo para aplicar una política que restringe el acceso de los usuarios a archivos que tienen un nivel de clasificación igual o inferior a su nivel de autorización.

Ejemplo de flujo de proceso para ABAC

1. El usuario presenta credenciales (por ejemplo, PKI, OAuth, SAML) para acceder al sistema a PEP y obtiene resultados de PDP.

   La función del PEP es interceptar la solicitud de acceso del usuario y reenviarla al PDP.

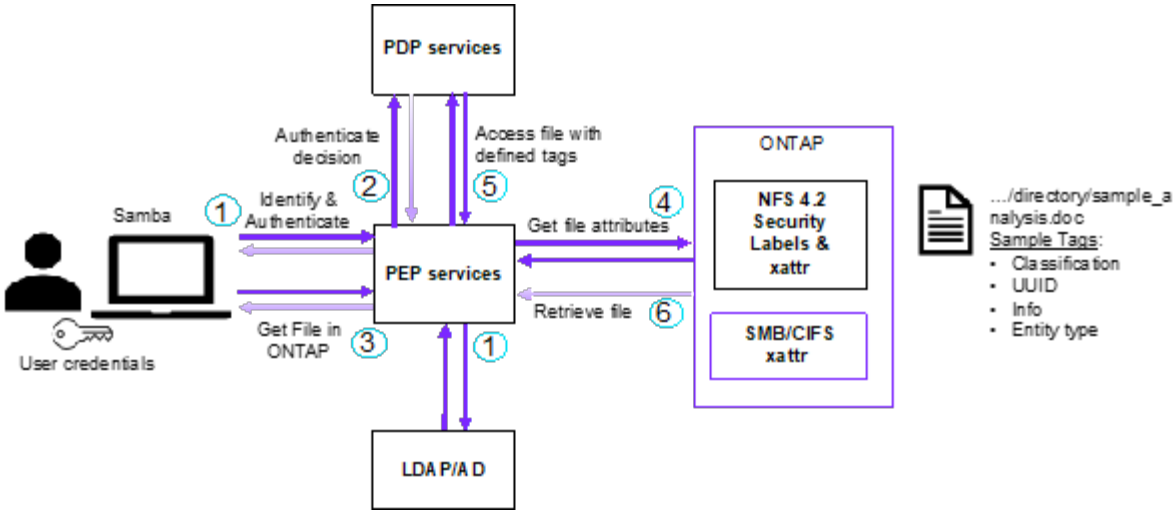
2. A continuación, el PDP evalúa esta solicitud con respecto a las políticas establecidas de ABAC.

   Estas políticas tienen en cuenta varios atributos relacionados con el usuario, el recurso en cuestión y el entorno circundante. Basándose en estas políticas, el PDP toma una decisión de acceso para permitir o denegar y luego comunica esta decisión al PEP.

   PDP proporciona una política a PEP para hacer cumplir. El PEP entonces aplica esta decisión, ya sea otorgando o denegando la solicitud de acceso del usuario según la decisión del PDP.

3. Después de una solicitud correcta, el usuario solicita un archivo almacenado en ONTAP (AFF, AFF-C, por ejemplo).
4. Si la solicitud se realiza correctamente, PEP obtiene etiquetas de control de acceso de granularidad fina del documento.
5. PEP solicita una política para el usuario basada en los certificados de ese usuario.
6. PEP toma una decisión basada en la política y las etiquetas si el usuario tiene acceso al archivo y permite al usuario recuperar el archivo.

> El acceso real se puede realizar mediante tokens que no son proxy a través de.



Información relacionada

- "NFS en NetApp ONTAP: Prácticas recomendadas y guía de implementación"
- Solicitud de comentarios (RFC)
  - RFC 2203: Especificación del protocolo RPCSEC_GSS
  - RFC 3530: Protocolo de sistema de archivos de red (NFS) versión 4