Control de acceso basado en atributos

ONTAP Technical Reports

NetApp
January 23, 2026

Tabla de contenidos

Control de acceso basado en atributos

Control de acceso basado en atributos con ONTAP

A partir de la versión 9.12.1, puede configurar ONTAP con NFSv4,2 etiquetas de seguridad y atributos extendidos (xattrs) para admitir el control de acceso basado en roles (RBAC) con atributos y el control de acceso basado en atributos (ABAC).

ABAC es una estrategia de autorización que define permisos basados en atributos de usuario, atributos de recursos y condiciones ambientales. La integración de ONTAP con etiquetas de seguridad NFS v4,2 y xattrs cumple con los estándares NIST para soluciones ABAC, como se establece en la Publicación Especial 800-162 del NIST.

Puede utilizar etiquetas de seguridad NFS v4,2 y xattrs para asignar archivos atributos y etiquetas definidos por el usuario. ONTAP puede integrarse con el software de gestión de acceso e identidad orientado a ABAC para aplicar políticas de control de acceso granular a archivos y carpetas basadas en estos atributos y etiquetas.

Información relacionada

- "Aproximaciones a ABAC con ONTAP"
- "NFS en NetApp ONTAP: Prácticas recomendadas y guía de implementación"

Enfoques para el control de acceso basado en atributos (ABAC) en ONTAP

ONTAP proporciona varios métodos que puede utilizar para lograr el control de acceso basado en atributos (ABAC) a nivel de archivo, incluidas las etiquetas de seguridad de NFS v4,2 y los atributos extendidos (xattrs) mediante NFS.

Etiquetas de seguridad de NFS v4,2

A partir de ONTAP 9,9.1, se admite la función NFS v4,2 llamada NFS.

Las etiquetas de seguridad NFS v4,2 son una forma de administrar el acceso granular a archivos y carpetas mediante el uso de etiquetas SELinux y el control de acceso obligatorio (MAC). Estas etiquetas MAC se almacenan con archivos y carpetas y funcionan junto con permisos UNIX y ACL de NFS v4.x.

La compatibilidad con las etiquetas de seguridad NFS v4,2 implica que ONTAP ahora reconoce y comprende la configuración de etiqueta SELinux del cliente NFS. Las etiquetas de seguridad de NFS v4,2 se tratan en RFC-7204.

Entre los casos de uso de las etiquetas de seguridad de NFS v4,2 se encuentran 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

Habilite etiquetas de seguridad de NFS v4.2

Puede habilitar o deshabilitar las etiquetas de seguridad de NFS v4,2 con el siguiente comando (se requiere privilegio avanzado):

```
vserver nfs modify -vserver <svm_name> -v4.2-seclabel <disabled|enabled>
```

Obtenga más información sobre `vserver nfs modify` en el "Referencia de comandos del ONTAP".

Modos de aplicación de etiquetas de seguridad NFS v4,2

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 capacidad de cambiar las etiquetas MAC depende del cliente para hacer cumplir.

- **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).

Ejemplos de etiquetas de seguridad NFS v4,2

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

Ejemplo de etiquetas de seguridad NFS v4,2 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 extendidos (xattrs)

A partir de ONTAP 9.12.1, ONTAP admite xattrs. Xattrs permite que los metadatos se asocien con 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` las utilidades de línea de comandos y `getfattr` en Linux. 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.

Hay varios requisitos y límites 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

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` define 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
  ```

Ejemplos de pares de valores de clave xattr

En la siguiente tabla se muestran dos ejemplos de pares de valores de clave xattr:

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 xattrs

Una entrada de control de acceso (ACE) es un componente dentro de una 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 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).

Entrada de control de acceso (ACE) necesaria 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 definir 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.

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

Integración con el software de control de acceso e identidad ABAC

Para aprovechar al máximo las capacidades de ABAC, ONTAP puede integrarse con un software de gestión de acceso e identidad orientado a ABAC.

En un sistema ABAC, el Punto de Aplicación de Políticas (PEP) y el Punto de Decisión de Políticas (PDP) desempeñan un papel crucial. 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 una configuración práctica, una organización utilizaría una combinación de etiquetas de seguridad NFS y xattrs. Estos se utilizan para representar una variedad de metadatos, incluida la clasificación, la seguridad, la aplicación y el contenido, que son fundamentales en la toma de decisiones ABAC.xattrs, 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.

> Este contenido asume que los servicios de identidad, autenticación y acceso del cliente incluyen como mínimo un PEP y un PDP que actúan como intermediarios para el acceso al sistema de archivos.

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.

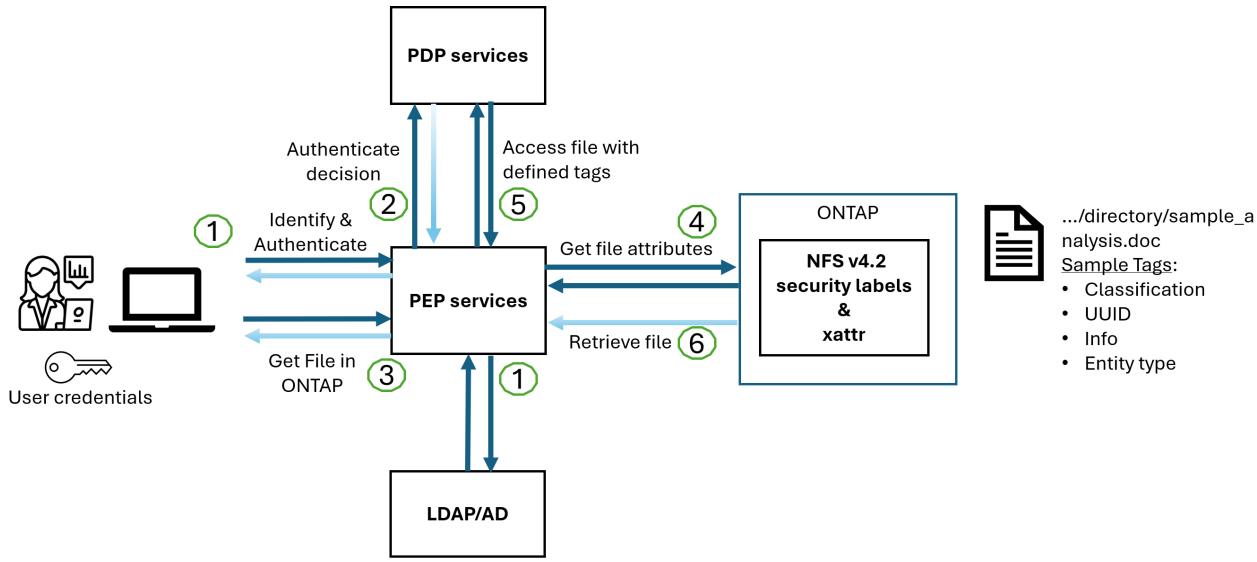
2. A continuación, el PDP evalúa esta solicitud con respecto a las políticas establecidas de ABAC.

   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.



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 archivos, incluidos los xattrs, se preservan y transfieren junto con el fichero. Los xattrs son esenciales al almacenar metadatos adicionales asociados a un archivo, como etiquetas de seguridad, información de control de acceso y datos definidos por el usuario, lo que son esenciales para mantener el contexto y la integridad del archivo.

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 NFS v4,2 tienen las advertencias definidas en 2.

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 la supervisión y el registro de todos los cambios en un sistema de archivos, incluidas las modificaciones en xattrs 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 NFS v3 y NFS v4, 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 operaciones de archivos admitidas para la supervisión de FPolicy de los eventos de acceso a archivos NFS v3 y NFS v4:

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 los 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.

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 tienen fines ilustrativos y es responsabilidad del cliente determinar los metadatos asociados a las etiquetas de seguridad y xattrs de NFS v4,2. Los detalles sobre la actualización y la retención de etiquetas se omiten para mayor simplicidad.

Ejemplo de valores de certificado PKI

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

Clave	Valor
uuid	b4111349-7875-4115-ad30-0928565f2e15

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.

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 de NFS v4,2: 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.

Ejemplo de pares clave-valor xattr

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]`

```
    }
}
```

Información relacionada

- "NFS en NetApp ONTAP: Prácticas recomendadas y guía de implementación"
- "Referencia de comandos del ONTAP"
- Solicitud de comentarios (RFC)
  - "RFC 7204: Requisitos para NFS con etiqueta"
  - "RFC 2203: Especificación del protocolo RPCSEC_GSS"
  - "RFC 3530: Protocolo de sistema de archivos de red (NFS) versión 4"

Información de copyright

Información de la marca comercial