Contrôle d'accès basé sur les attributs

ONTAP 9

NetApp
January 10, 2025

Sommaire

Contrôle d’accès basé sur les attributs 1
Contrôle d’accès basé sur les attributs avec ONTAP 1
Approches de l’ABAC avec ONTAP 1

Contrôle d’accès basé sur les attributs

Contrôle d’accès basé sur les attributs avec ONTAP

Vous pouvez implémenter un contrôle d’accès basé sur des attributs et un contrôle d’accès basé sur des attributs à l’aide de ONTAP. ONTAP propose plusieurs approches que le client peut utiliser pour obtenir un ABAC de niveau fichier, notamment NFS 4.2 et XATTRS avec NFS et SMB/CIFS.

Le contrôle d’accès basé sur les attributs (ABAC) est une méthode sophistiquée de gestion des droits d’accès qui tient compte des attributs d’utilisateur, des attributs de ressource et des conditions environnementales. Le National Institute of Standards and Technology (NIST) a établi une norme pour ABAC, qui fournit un cadre pour sa mise en œuvre sécurisée et cohérente.

À partir de ONTAP 9.12.1, vous pouvez configurer ONTAP avec NFSv4.2 Security Labels and Extended Attributes (XATTRS) afin qu’il puisse être intégré à un contrôle d’accès basé sur les rôles (RBAC) et à une identité de contrôle d’accès basé sur les attributs (ABAC). Cette intégration permet à ONTAP d’accéder à des logiciels de contrôle classés en tant que solution de gestion des données conforme à la norme NIST ABAC, offrant une approche robuste et avancée de la gestion des droits d’accès dans des environnements complexes, notamment le point d’application des règles (PEP), un point de décision stratégique (PDP) et des stratégies qui tiennent compte des attributs associés à l’utilisateur, à la ressource et à l’environnement.

L’intégration du logiciel NetApp ONTAP avec les attributs étendus (XATTRS) et ABAC (Attribute-Based Access Control) est conforme aux directives énoncées dans la publication spéciale NIST 800-162, garantissant la conformité avec les normes NIST pour la mise en œuvre de l’ABAC. L’utilisation d’étiquettes de sécurité NFS 4.2 et de XATTRS permet d’associer des attributs définis par l’utilisateur à des fichiers, répondant ainsi aux exigences de la norme NIST ABAC en matière de prise en compte des attributs de ressources dans les décisions de contrôle d’accès. Le PEP et le PDP du logiciel ABAC s’alignent sur les exigences de la norme ABAC NIST pour ces composants dans le processus de contrôle d’accès. La capacité à définir des règles complexes qui tiennent compte de plusieurs attributs et conditions est conforme aux exigences de la norme NIST ABAC en matière de contrôle d’accès basé sur des règles.

Informations associées

- "Approches de l’ABAC avec ONTAP"
- "NFS dans NetApp ONTAP : guide des bonnes pratiques et d’implémentation"
- Demande de commentaires (RFC)
  - RFC 2203 : spécification du protocole RPCSEC_GSS
  - RFC 3530 : protocole NFS (Network File System) version 4

Approches de l’ABAC avec ONTAP

ONTAP propose diverses approches qu’un client peut utiliser pour réaliser un ABAC de niveau fichier, notamment NFSv4.2 et XATTRS avec NFS et SMB/CIFS.

Libellé NFSv4.2

À partir de ONTAP 9.9.1, la fonctionnalité NFSv4.2 appelée NFS est prise en charge.

Le protocole NFS marqué permet de gérer l’accès granulaire aux fichiers et aux dossiers à l’aide d’étiquettes

SELinux et du contrôle d'accès obligatoire (MAC). Ces étiquettes MAC sont stockées avec des fichiers et des dossiers et fonctionnent en conjonction avec les autorisations UNIX et les listes de contrôle d'accès NFSv4.x.

La prise en charge de l'étiquetage NFS signifie que ONTAP reconnaît et comprend désormais les paramètres d'étiquette SELinux du client NFS. Le protocole NFS marqué est couvert par la norme RFC-7204.

Les cas d'utilisation pour NFSv4.2 portant le libellé sont les suivants :

- Étiquetage MAC des images de machines virtuelles (VM)
- Classification de sécurité des données pour le secteur public (secret, secret et autres classifications)
- Conformité en matière de sécurité
- Linux sans disque

Activer avec libellé NFSv4.2

Vous pouvez activer ou désactiver le protocole NFS marqué avec l'option de privilège avancé suivante :

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

Ce paramètre est facultatif et le paramètre par défaut est `disabled`.

Modes de mise en application pour NFSv4.2 étiqueté

À partir de ONTAP 9.9.1, ONTAP prend en charge les modes d'application suivants :

- **Mode serveur limité** : ONTAP ne peut pas appliquer les étiquettes mais peut les stocker et les transmettre.

  La possibilité de modifier les étiquettes MAC est également à la charge du client.

- **Mode invité** : si le client n'est pas étiqueté NFS-Aware (v4.1 ou inférieur), les étiquettes MAC ne sont pas transmises.

ONTAP ne prend actuellement pas en charge le mode complet (stockage et application des étiquettes MAC).

Exemple de configuration de NFSv4.2

L'exemple de configuration suivant illustre les concepts d'utilisation de Red Hat Enterprise Linux version 9.3 (Plough).

L'utilisateur `jrsmith`, créé à partir des informations d'identification de John R. Smith, possède le compte Privileges suivant :

- Nom d'utilisateur = `jrsmith`
- Privileges = `uid=1112(jrsmith) gid=1112(jrsmith) groups=1112(jrsmith) context=user_u:user_r:user_t:s0`

Il existe deux rôles : le compte admin qui est un utilisateur privilégié et un utilisateur `jrsmith` comme décrit dans le tableau Privileges MLS suivant :

Utilisateurs	Rôle	Type	Niveaux
admins	sysadm_r	sysadm_t	t:s0
jrsmith	user_r	user_t	t:s1 - t:s4

Dans cet exemple d'environnement, l'utilisateur `jrsmith` a accès aux fichiers aux niveaux de `s0 s3` . Nous pouvons améliorer les classifications de sécurité existantes, comme décrit ci-dessous, afin de nous assurer que les administrateurs n'ont pas accès aux données spécifiques aux utilisateurs.

- s0 = données utilisateur admin des privilèges
- s0 = données non classées
- s1 = confidentiel
- s2 = données secrètes
- s3 = données les plus secrètes

Respectez vos politiques de sécurité de votre organisation

Exemple d'étiquette de sécurité NFSv4.2 avec MCS

Outre la sécurité multi-niveaux (MLS), une autre fonctionnalité appelée sécurité multi-catégories (MCS) vous permet de définir des catégories telles que des projets.

Étiquette de sécurité NFS	Valeur
entitySecurityMark	t:s01 = UNCLASSIFIED

Attributs étendus (XATTRS)

À partir de ONTAP 9.12.1, ONTAP prend en charge xattrs. Xattrs permet d'associer des métadonnées à des fichiers et des répertoires au-delà de ce qui est fourni par le système, tels que les listes de contrôle d'accès (ACL) ou les attributs définis par l'utilisateur.

Pour implémenter xattrs, vous pouvez utiliser `setfattr` et les `getfattr` utilitaires de ligne de commande sous Linux pour gérer les xattrs des objets de système de fichiers. Ces outils fournissent un moyen puissant de gérer des métadonnées supplémentaires pour les fichiers et les répertoires. Elles doivent être utilisées avec précaution, mais une utilisation inappropriée peut entraîner des comportements inattendus ou des problèmes de sécurité. Reportez-vous toujours aux `setfattr` pages de manuel et `getfattr` ou à toute autre documentation fiable pour obtenir des instructions d'utilisation détaillées.

Lorsque xattrs est activé sur un système de fichiers ONTAP, les utilisateurs peuvent définir, modifier et récupérer des attributs arbitraires sur les fichiers. Ces attributs peuvent être utilisés pour stocker des informations supplémentaires sur le fichier qui ne sont pas capturées par l'ensemble standard d'attributs de fichier, telles que les informations de contrôle d'accès.

Configuration requise pour l'utilisation de xattrs dans ONTAP

- Red Hat Enterprise Linux 8.4 ou version ultérieure

- Ubuntu 22.04 ou version ultérieure
- Chaque fichier peut avoir jusqu'à 128 xattrs
- les clés xattr sont limitées à 255 octets
- La taille de la clé ou de la valeur combinée est de 1,729 octets par xattr
- Les répertoires et les fichiers peuvent avoir des xattrs
- Pour définir et récupérer les xattrs, `w` ou les bits de mode d'écriture doivent être activés pour l'utilisateur et le groupe

Cas d'utilisation des xattrs

Les xattrs sont utilisés dans l'espace de nom de l'utilisateur et n'ont aucune signification intrinsèque à ONTAP lui-même. Au lieu de cela, leurs applications pratiques sont déterminées et gérées exclusivement par l'application côté client qui interagit avec le système de fichiers.

exemples de cas d'utilisation de xattr :

- Enregistrement du nom de l'application responsable de la création d'un fichier.
- Conservation d'une référence à l'e-mail à partir duquel un fichier a été obtenu.
- Établissement d'un cadre de catégorisation pour l'organisation des objets de fichier.
- Étiquetage des fichiers avec l'URL de leur source de téléchargement d'origine.

Commandes de gestion des xattrs

- `setfattr`: Définit un attribut étendu d'un fichier ou d'un répertoire :

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

  Exemple de commande :

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

- `getfattr`: Récupère la valeur d'un attribut étendu spécifique ou répertorie tous les attributs étendus d'un fichier ou d'un répertoire :

  Attribut spécifique : `getfattr -n <attribute_name> <file or directory name>`

  Tous les attributs : `getfattr <file or directory name>`

  Exemple de commande :

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

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

Autorisations utilisateur avec ACE pour les attributs étendus

Une entrée de contrôle d'accès (ACE) est un composant d'une liste de contrôle d'accès (ACL) qui définit les droits ou autorisations d'accès accordés à un utilisateur individuel ou à un groupe d'utilisateurs pour une ressource spécifique, comme un fichier ou un répertoire. Chaque ACE spécifie le type d'accès autorisé ou refusé et est associé à une entité de sécurité particulière (identité d'utilisateur ou de groupe).

Type de fichier	Récupérer xattr	Définissez xattrs
Fichier	R	A,W,T
Répertoire	R	T

Explication des autorisations requises pour xattrs :

Retrieve xattr : les autorisations nécessaires à un utilisateur pour lire les attributs étendus d'un fichier ou d'un répertoire. Le « R » signifie que l'autorisation de lecture est nécessaire. **Set xattrs** : les autorisations nécessaires pour modifier ou définir les attributs étendus. « A », « W » et « T » représentent différents exemples d'autorisations, telles que l'ajout, l'écriture et une autorisation spécifique liée aux xattrs. **Fichiers** : les utilisateurs doivent ajouter, écrire et potentiellement une autorisation spéciale liée aux xattrs pour définir des attributs étendus. **Répertoires** : une autorisation spécifique "T" est nécessaire pour définir des attributs étendus.

Prise en charge du protocole SMB/CIFS pour les xattrs

La prise en charge par ONTAP du protocole SMB/CIFS s'étend au traitement complet des xattrs, qui font partie intégrante des métadonnées de fichiers dans les environnements Windows. Les attributs étendus permettent aux utilisateurs et aux applications de stocker des informations supplémentaires au-delà de l'ensemble standard d'attributs de fichier, telles que les détails de l'auteur, les descripteurs de sécurité personnalisés ou les données spécifiques à l'application. L'implémentation SMB/CIFS de ONTAP garantit la prise en charge complète de ces xattrs, ce qui permet une intégration transparente aux services et applications Windows qui dépendent de ces métadonnées pour l'application des fonctionnalités et des règles.

Lorsque des fichiers sont lus ou transférés via des partages SMB/CIFS gérés par ONTAP, le système préserve l'intégrité des xattrs, garantissant ainsi la cohérence de toutes les métadonnées. Ceci est particulièrement important pour maintenir les paramètres de sécurité et pour les applications qui dépendent de xattrs pour la configuration ou le fonctionnement. La gestion fiable des xattrs par ONTAP dans le contexte SMB/CIFS garantit la fiabilité et la sécurité du partage de fichiers entre différentes plateformes et différents environnements. Les utilisateurs bénéficient ainsi d'une expérience transparente et les administrateurs sont assurés du respect des politiques de gouvernance des données. Qu'il s'agisse de collaboration, d'archivage de données ou de conformité, l'attention de ONTAP aux xattrs au sein des partages SMB/CIFS témoigne de son engagement en faveur de l'excellence et de l'interopérabilité de la gestion des données dans des environnements de systèmes d'exploitation mixtes.

Point d'application de la politique (PPE) et point de décision de la politique (PDP) dans ABAC

Dans un système de contrôle d'accès basé sur des attributs (ABAC), le point d'application des politiques (PEP) et le point de décision stratégique (PDP) jouent des rôles cruciaux. Le PPE est responsable de l'application des politiques de contrôle d'accès, tandis que le PDP prend la décision d'accorder ou de refuser l'accès en fonction des politiques.

Dans le contexte de l'extrait de code Python fourni, le script lui-même agit comme une PPE. Il applique la décision de contrôle d'accès en accordant l'accès au fichier en l'ouvrant et en lisant son contenu ou en

refusant l'accès en levant un `PermissionError`.

Le PDP, en revanche, ferait partie du système sous-jacent SELinux. Lorsque le script tente d'ouvrir le fichier avec un contexte SELinux spécifique, le système SELinux vérifie ses stratégies pour décider d'accorder ou de refuser l'accès. Cette décision est ensuite appliquée par le script.

Vous trouverez ci-dessous un exemple détaillé du fonctionnement de ce code dans un environnement ABAC :

1. Le script définit le contexte SELinux en contexte à `jrsmith` l'aide de la `selinux.setcon()` fonction. Cela revient à `jrsmith` essayer d'accéder au fichier.
2. Le script tente d'ouvrir le fichier. C'est là que la PPE entre en jeu.
3. Le système SELinux vérifie ses stratégies pour voir si `jrsmith` (ou plus précisément, un utilisateur avec un `jrsmith` contexte SELinux) est autorisé à accéder au fichier. Il s'agit du rôle du PDP.
4. Si `jrsmith` est autorisé à accéder au fichier, le système SELinux permet au script d'ouvrir le fichier et le script lit et imprime le contenu du fichier.
5. Si `jrsmith` n'est pas autorisé à accéder au fichier, le système SELinux empêche le script d'ouvrir le fichier et le script émet un `PermissionError`.
6. Le script restaure le contexte SELinux d'origine pour s'assurer que la modification temporaire du contexte n'affecte pas les autres opérations.

En utilisant python, le code pour obtenir le contexte est indiqué ci-dessous où le chemin du fichier variable est le document à vérifier :

```
#Get the current context

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

Clonage ONTAP et SnapMirror

Les technologies de clonage et de SnapMirror de ONTAP sont conçues pour fournir des fonctionnalités de réplication et de clonage des données efficaces et fiables, garantissant que tous les aspects des données de fichiers, y compris les attributs étendus (xattrs), sont conservés et transférés avec le fichier. Les xattrs sont essentiels car ils stockent des métadonnées supplémentaires associées à un fichier, telles que les étiquettes de sécurité, les informations de contrôle d'accès et les données définies par l'utilisateur, qui sont essentielles au maintien de l'intégrité des fichiers.

Lorsqu'un volume est cloné à l'aide de la technologie FlexClone de ONTAP, une réplique inscriptible exacte du volume est créée. Ce processus de clonage est instantané et compact. Il inclut toutes les données de fichiers et métadonnées, garantissant ainsi la réplication complète des fichiers xattrs. De même, SnapMirror garantit la mise en miroir parfaite des données vers un système secondaire. Cela inclut les xattrs, qui sont essentiels pour que les applications qui s'appuient sur ces métadonnées fonctionnent correctement.

En incluant les xattrs dans les opérations de clonage et de réplication, NetApp ONTAP s'assure que l'ensemble du dataset, avec toutes ses caractéristiques, est disponible et cohérent sur l'ensemble des systèmes de stockage primaire et secondaire. Cette approche globale de la gestion des données est cruciale pour les entreprises qui ont besoin d'une protection cohérente des données, d'une restauration rapide et du respect des normes de conformité et réglementaires. Elle simplifie également la gestion des données entre différents environnements, sur site ou dans le cloud, garantissant ainsi aux utilisateurs que leurs données sont complètes et non modifiées au cours de ces processus.

Les avertissements des étiquettes de sécurité NFSv4.2 sont définis dans Libellé NFSv4.2.

Exemples de contrôle de l'accès aux données

L'exemple d'entrée ci-dessous pour les données stockées dans le certificat PKI de John R Smith montre comment l'approche de NetApp peut être appliquée à un fichier et fournit un contrôle d'accès précis.

Ces exemples sont donnés à titre d'exemple et il incombe au gouvernement de définir les métadonnées qui sont le label de sécurité NFSv4.2 et les xattrs. Les détails sur la mise à jour et la conservation des étiquettes sont omis pour plus de simplicité.

Clé	Valeur
EntitySecurityMark	t:s01 = non confidentiel

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"
	}
	}

spécifications	« DOD »
uuid	b4111349-7875-4115-ad30-0928565f2e15

Clé	Valeur

AdminOrganisation	{
	"value": "DoD"
	}

réunions d'information	[
	{
	"value": "ABC1000"
	},
	{
	"value": "DEF1001"
	},
	{
	"value": "EFG2000"
	}
	]

État de la citoyenneté	{
	"value": "US"
	}

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

Clé	Valeur
PaysOfaffiliations	`[ { "value": "USA" } ]`
Identificateur numérique	`{ "classification": "UNCLASSIFIED", "value": "cn=smith john r jrsmith, ou=dod, o=u.s. government, c=us" }`
Démontez	`{ "value": "DoD" }`
DutyOrganisation	`{ "value": "DoD" }`
EntityType	`{ "value": "GOV" }`

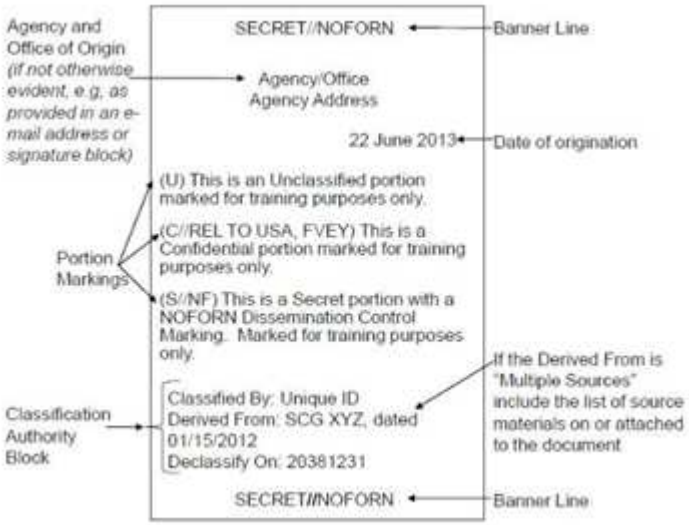
Clé	Valeur

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

Ces droits ICP montrent les détails d'accès de John R. Smith, y compris l'accès par type de données et l'attribution.

Si John R. Smith a créé et enregistré un document appelé *« sample_Analysis.doc »*, selon les directives pertinentes, l'utilisateur ajouterait la bannière et les marquages de portion appropriés, l'agence et le bureau d'origine, ainsi que le bloc d'autorité de classification approprié en fonction de la classification du document, comme indiqué dans l'image suivante. Ces métadonnées riches ne sont compréhensibles qu'après analyse du langage naturel (NLP) et application de règles pour donner du sens aux marquages. Des outils tels que la classification NetApp BlueXP peuvent le faire, mais sont moins efficaces pour les décisions de contrôle d'accès parce qu'ils ont besoin d'autorisation pour regarder à l'intérieur du document.

Marquage de la portion de document CAPCO non classifié



Dans les cas où les métadonnées IC-TDF sont stockées séparément du fichier, NetApp préconise une couche supplémentaire de contrôle d'accès granulaire. Cela implique le stockage des informations de contrôle d'accès au niveau du répertoire et en association avec chaque fichier. Prenons l'exemple des balises suivantes liées à un fichier :

- Étiquettes de sécurité NFSv4.2 : utilisées pour prendre des décisions en matière de sécurité

- Xattrs : fournir des renseignements supplémentaires pertinents au dossier et aux exigences du programme organisationnel

Les paires clé-valeur suivantes sont des exemples de métadonnées qui peuvent être stockées sous forme de xattrs et fournissent des informations détaillées sur le créateur du fichier et les classifications de sécurité associées. Ces métadonnées peuvent être exploitées par les applications client pour prendre des décisions éclairées en matière d'accès et organiser les fichiers en fonction des normes et des exigences de l'entreprise.

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

Clé	Valeur

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"
	},

Clé	Valeur
user.geo_point	[-78.7941, 35.7956]

```
    }
}
```

Audit des modifications apportées aux étiquettes

L'audit des modifications apportées aux étiquettes de sécurité xattrs ou NFS constitue un aspect essentiel de la gestion et de la sécurité du système de fichiers. Les outils d'audit standard du système de fichiers permettent de surveiller et de consigner toutes les modifications apportées à un système de fichiers, y compris les modifications apportées aux attributs étendus et aux étiquettes de sécurité.

Dans les environnements Linux, le `auditd` démon est généralement utilisé pour établir un audit pour les événements du système de fichiers. Il permet aux administrateurs de configurer des règles pour surveiller des appels système spécifiques liés aux modifications xattr, telles que `setxattr`, `lsetxattr` et pour définir des attributs et, `lremovexattr` et `fsetxattr` `fremovexattr` pour supprimer des attributs `removexattr`.

ONTAP FPolicy étend ces fonctionnalités en fournissant une structure robuste pour la surveillance et le contrôle en temps réel des opérations de fichiers. FPolicy peut être configuré pour prendre en charge divers événements xattr, offrant un contrôle granulaire des opérations sur fichiers et la possibilité d'appliquer des règles complètes de gestion des données.

Pour les utilisateurs de xattrs, en particulier dans les environnements NFSv3 et NFSv4, seules certaines combinaisons d'opérations sur fichiers et de filtres sont prises en charge pour la surveillance. La liste des combinaisons de filtres et d'opérations de fichiers prises en charge pour la surveillance FPolicy des événements d'accès aux fichiers NFSv3 et NFSv4 est détaillée ci-dessous :

Opérations de fichiers prises en charge	Filtres pris en charge
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

Exemple de fragment de journal auditd pour une opération 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'activation de ONTAP FPolicy pour les utilisateurs travaillant avec xattrs offre une couche de visibilité et de contrôle essentielle pour préserver l'intégrité et la sécurité du système de fichiers. Grâce aux fonctionnalités

avancées de surveillance de FPolicy, les entreprises peuvent s'assurer que toutes les modifications apportées aux xattrs font l'objet d'un suivi, d'un audit et d'une mise en adéquation avec leurs normes de sécurité et de conformité. Cette approche proactive de la gestion du système de fichiers explique pourquoi l'activation de ONTAP FPolicy est fortement recommandée pour toute entreprise qui souhaite améliorer ses stratégies de gouvernance et de protection des données.

Intégration au logiciel ABAC Identity and Access Control

Pour exploiter pleinement les capacités du contrôle d'accès basé sur les attributs (ABAC), ONTAP peut s'intégrer à un logiciel de gestion des identités et des accès orienté ABAC.

> Parallèlement à ce contenu, NetApp dispose d'une implémentation de référence utilisant GrayBox. Une hypothèse pour ce contenu est que les services d'identité, d'authentification et d'accès du gouvernement comprennent au moins un point d'application des politiques (PEP) et un point de décision stratégique (PDP) qui servent d'intermédiaires pour l'accès au système de fichiers.

Dans la pratique, une entreprise utiliserait un mélange d'étiquettes de sécurité NFS et de xattrs. Ils sont utilisés pour représenter une variété de métadonnées, y compris la classification, la sécurité, l'application et le contenu, qui sont toutes essentielles à la prise de décisions ABAC. XATTR, par exemple, peut être utilisé pour stocker les attributs de ressource que le PDP utilise pour son processus de prise de décision. Un attribut peut être défini pour représenter le niveau de classification d'un fichier (par exemple, « non classé », « confidentiel », « secret » ou « secret supérieur »). Le PDP pourrait alors utiliser cet attribut pour appliquer une stratégie qui limite les utilisateurs à accéder uniquement aux fichiers dont le niveau de classification est égal ou inférieur à leur niveau d'autorisation.

Exemple de flux de processus pour ABAC

1. L'utilisateur présente les informations d'identification (par exemple, PKI, OAuth, SAML) pour accéder au système à PEP et obtient les résultats du PDP.

   Le rôle du PPE est d'intercepter la demande d'accès de l'utilisateur et de la transférer au PDP.

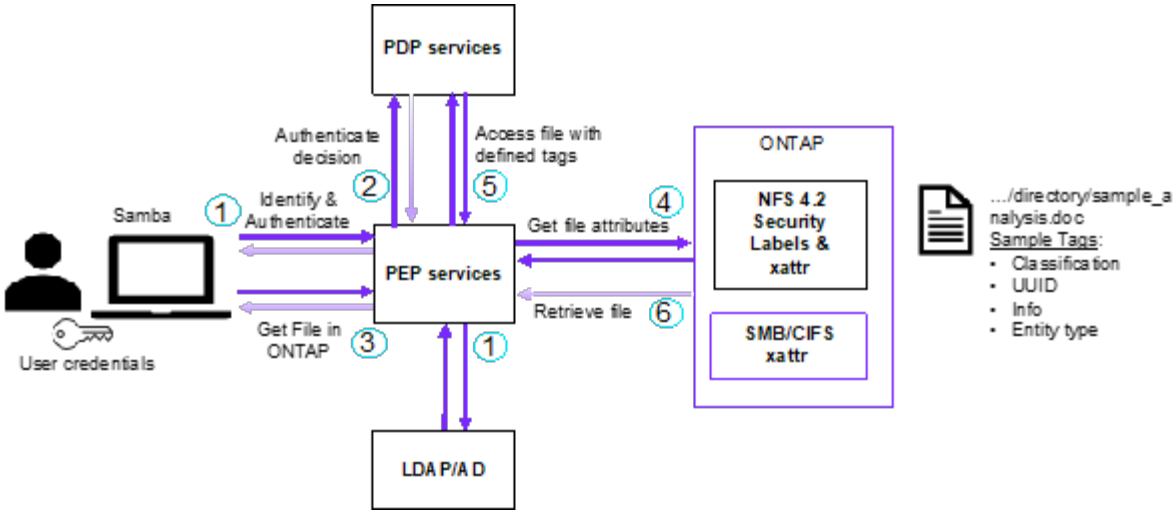
2. Le PDP évalue ensuite cette demande par rapport aux politiques établies de l'ABAC.

   Ces stratégies tiennent compte de divers attributs liés à l'utilisateur, à la ressource en question et à l'environnement environnant. En fonction de ces politiques, le PDP prend une décision d'accès d'autoriser ou de refuser, puis communique cette décision à la PPE.

   PDP fournit une politique à PEP pour qu'elle l'applique. Le PPE applique ensuite cette décision, en accordant ou en refusant la demande d'accès de l'utilisateur conformément à la décision du PDP.

3. Après une demande réussie, l'utilisateur demande un fichier stocké dans ONTAP (AFF, AFF-C, par exemple).
4. Si la demande réussit, PEP obtient des étiquettes de contrôle d'accès à grain fin à partir du document.
5. PEP demande la politique de l'utilisateur en fonction des certificats de cet utilisateur.
6. PEP prend une décision en fonction de la politique et des balises si l'utilisateur a accès au fichier et permet à l'utilisateur de le récupérer.

> L'accès réel peut être effectué à l'aide de jetons non proxiés.



Informations associées

- "NFS dans NetApp ONTAP : guide des bonnes pratiques et d'implémentation"
- Demande de commentaires (RFC)
  - RFC 2203 : spécification du protocole RPCSEC_GSS
  - RFC 3530 : protocole NFS (Network File System) version 4

Informations sur le copyright

Informations sur les marques commerciales