Controle de acesso baseado em atributos

ONTAP 9

NetApp
January 17, 2025

Índice

Controle de acesso baseado em atributos

Controle de acesso baseado em atributos com ONTAP

É possível implementar RBAC aprimorado com atributos e controle de acesso baseado em atributos (ABAC) usando o ONTAP. O ONTAP fornece várias abordagens que um cliente pode usar para obter ABAC no nível do arquivo, incluindo NFS 4,2 e XATTRS rotulados usando NFS e SMB/CIFS.

O controle de acesso baseado em atributos (ABAC) é um método sofisticado para gerenciar direitos de acesso que considera atributos do usuário, atributos de recursos e condições ambientais. O Instituto Nacional de padrões e tecnologia (NIST) estabeleceu um padrão para a ABAC, fornecendo uma estrutura para sua implementação segura e consistente.

A partir do ONTAP 9.12,1, você pode configurar o ONTAP com rótulos de segurança NFSv4,2 e atributos estendidos (XATTRS) para que ele possa ser integrado a uma identidade de controle de acesso baseado em função (RBAC) e controle de acesso baseado em atributos (ABAC). Essa integração permite que o ONTAP acesse softwares de controle que são categorizados como uma solução de gerenciamento de dados compatível com ABAC NIST, oferecendo uma abordagem robusta e avançada para gerenciar direitos de acesso em ambientes complexos, incluindo ponto de aplicação de políticas (PEP), ponto de Decisão de políticas (PDP) e políticas que consideram atributos associados ao usuário, ao recurso e ao ambiente.

A integração do software NetApp ONTAP com atributos estendidos (XATTRS) e Controle de Acesso baseado em Atributo (ABAC) está alinhada com as diretrizes estabelecidas na publicação especial do NIST 800-162, garantindo o cumprimento das normas NIST para implementação da ABAC. O uso de rótulos de segurança NFS 4,2 e XATTRS permite a associação de atributos definidos pelo usuário com arquivos, atendendo aos requisitos do padrão NIST ABAC para considerar atributos de recursos nas decisões de controle de acesso. O PEP e PDP do software ABAC estão alinhados com o requisito do padrão NIST ABAC para esses componentes no processo de controle de acesso. A capacidade de definir políticas complexas que considerem vários atributos e condições alinha-se ao requisito do padrão NIST ABAC para controle de acesso baseado em políticas.

Informações relacionadas

- "Abordagens para ABAC com ONTAP"
- "NFS no NetApp ONTAP: Guia de práticas recomendadas e implementação"
- Pedido de comentários (RFC)
  - RFC 2203: Especificação do protocolo RPCSEC_GSS
  - RFC 3530: Protocolo NFS (Network File System) versão 4

Abordagens para ABAC com ONTAP

O ONTAP fornece abordagens variadas que um cliente pode usar para obter ABAC no nível do arquivo, incluindo NFSv4,2 e XATTRS rotulados usando NFS e SMB/CIFS.

Identificada como NFSv4,2

A partir do ONTAP 9.9,1, o recurso NFSv4,2 chamado NFS é suportado.

O NFS rotulado é uma maneira de gerenciar o acesso granular a arquivos e pastas usando rótulos SELinux e

Controle de Acesso obrigatório (MAC). Esses rótulos MAC são armazenados com arquivos e pastas e funcionam em conjunto com permissões UNIX e ACLs NFSv4.x.

O suporte para NFS rotulado significa que a ONTAP agora reconhece e compreende as configurações de rótulo SELinux do cliente NFS. O NFS rotulado é coberto pela RFC-7204.

Os casos de uso do rotulado NFSv4,2 incluem o seguinte:

- MAC rotulagem de imagens de máquina virtual (VM)
- Classificação de segurança de dados para o setor público (segredo, segredo principal e outras classificações)
- Conformidade de segurança
- Linux sem disco

Ative o rótulo NFSv4,2

Você pode ativar ou desativar o NFS rotulado com a seguinte opção de privilégio avançado:

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

Este parâmetro é opcional e a predefinição é `disabled`.

Modos de aplicação para o rótulo NFSv4,2

A partir do ONTAP 9.9,1, o ONTAP suporta os seguintes modos de aplicação:

- **Modo de servidor limitado**: O ONTAP não pode impor as etiquetas, mas pode armazená-las e transmiti-las.

  A capacidade de alterar rótulos MAC também depende do cliente para impor.

- **Modo convidado**: Se o cliente não estiver identificado como NFS-Aware (v4,1 ou inferior), os rótulos MAC não serão transmitidos.

Atualmente, o ONTAP não suporta o modo completo (armazenamento e aplicação de etiquetas MAC).

Exemplo de configuração do rotulado NFSv4,2

A configuração de exemplo a seguir demonstra conceitos usando o Red Hat Enterprise Linux versão 9,3 (Plow).

O usuário `jrsmith`, criado com base nas credenciais de John R. Smith, tem o seguinte Privileges de conta:

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

Há duas funções: A conta de administrador que é um usuário privilegiado e usuário `jrsmith`, conforme descrito na seguinte tabela MLS Privileges:

Usuários	Função	Tipo	Níveis
admins	sysadm_r	sysadm_t	t:s0
jrsmith	user_r	user_t	t:s1 - t:s4

Neste ambiente de exemplo, o usuário `jrsmith` tem acesso a arquivos nos níveis `s0 s3` de . Podemos aprimorar as classificações de segurança existentes, conforme descrito abaixo, para garantir que os administradores não tenham acesso a dados específicos do usuário.

- s0: dados de usuário do administrador de privilégios
- s0: dados não classificados
- s1: confidencial
- s2: dados secretos
- s3: dados secretos principais

Siga as políticas de segurança da sua organização

Exemplo de etiqueta de segurança NFSv4,2 com MCS

Além do MLS (Multi-Level Security), outro recurso chamado MCS (Multi-Category Security) permite definir categorias como projetos.

Etiqueta de segurança NFS	Valor
entitySecurityMark	t:s01 = UNCLASSIFIED

Atributos estendidos (XATTRS)

A partir do ONTAP 9.12,1, o ONTAP suporta xattrs. Os xattrs permitem que os metadados sejam associados a arquivos e diretórios além do que é fornecido pelo sistema, como listas de controle de acesso (ACLs) ou atributos definidos pelo usuário.

Para implementar o xattrs, você pode usar `setfattr` e `getfattr` utilitários de linha de comando no Linux para gerenciar xattrs de objetos de sistema de arquivos. Essas ferramentas fornecem uma maneira poderosa de gerenciar metadados adicionais para arquivos e diretórios. Eles devem ser usados com cuidado, pois o uso inadequado pode levar a comportamentos inesperados ou problemas de segurança. Consulte sempre as `setfattr` páginas de manual e `getfattr` ou outra documentação fiável para obter instruções de utilização detalhadas.

Quando o xattrs está habilitado em um sistema de arquivos ONTAP, os usuários podem definir, modificar e recuperar atributos arbitrários em arquivos. Esses atributos podem ser usados para armazenar informações adicionais sobre o arquivo que não é capturado pelo conjunto padrão de atributos de arquivo, como informações de controle de acesso.

Requisitos para usar xattrs em ONTAP

- Red Hat Enterprise Linux 8,4 ou posterior

- Ubuntu 22,04 ou posterior
- Cada arquivo pode ter até 128 xattrs
- as chaves xattr estão limitadas a 255 bytes
- O tamanho combinado da chave ou do valor é de 1.729 bytes por xattr
- Diretórios e arquivos podem ter xattrs
- Para definir e recuperar xattrs `w`, ou bits de modo de gravação devem estar ativados para o usuário e grupo

Casos de uso para xattrs

Os xattrs são utilizados dentro do namespace do usuário e não carregam nenhum significado intrínseco para o próprio ONTAP. Em vez disso, suas aplicações práticas são determinadas e gerenciadas exclusivamente pelo aplicativo do lado do cliente que interage com o sistema de arquivos.

exemplos de casos de uso do xattr:

- Gravando o nome do aplicativo responsável pela criação de um arquivo.
- Manter uma referência à mensagem de e-mail a partir da qual um arquivo foi obtido.
- Estabelecendo uma estrutura de categorização para organizar objetos de arquivo.
- Rotular arquivos com o URL de sua fonte de download original.

Comandos para gerenciar xattrs

- `setfattr`: Define um atributo estendido de um arquivo ou diretório:

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

  Exemplo de comando:

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

- `getfattr`: Recupera o valor de um atributo estendido específico ou lista todos os atributos estendidos de um arquivo ou diretório:

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

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

  Exemplo de comando:

  ```
  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`

Permissões de usuário com ACE para atributos estendidos

Uma entrada de controle de acesso (ACE) é um componente dentro de uma lista de controle de acesso (ACL) que define os direitos de acesso ou permissões concedidos a um usuário individual ou a um grupo de usuários para um recurso específico, como um arquivo ou diretório. Cada ACE especifica o tipo de acesso permitido ou negado e está associado a um responsável de segurança específico (identidade de usuário ou grupo).

Tipo de ficheiro	Recuperar xattr	Definir xattrs
Ficheiro	R	A, W, T
Diretório	R	T

Explicação das permissões necessárias para o xattrs:

Retrieve xattr: As permissões necessárias para um usuário ler os atributos estendidos de um arquivo ou diretório. O "R" significa que a permissão de leitura é necessária. * Definir xattrs*: As permissões necessárias para modificar ou definir os atributos estendidos. "A", "W" e "T" representam diferentes exemplos de permissões, como anexar, escrever e uma permissão específica relacionada ao xattrs. **Files**: Os usuários precisam anexar, escrever e potencialmente uma permissão especial relacionada ao xattrs para definir atributos estendidos. **Diretórios**: Uma permissão específica "T" é necessária para definir atributos estendidos.

Suporte ao protocolo SMB/CIFS para xattrs

O suporte da ONTAP para o protocolo SMB/CIFS se estende ao tratamento abrangente de xattrs, que são parte integrante dos metadados de arquivos em ambientes Windows. Os atributos estendidos permitem que usuários e aplicativos armazenem informações adicionais além do conjunto padrão de atributos de arquivo, como detalhes do autor, descritores de segurança personalizados ou dados específicos do aplicativo. A implementação SMB/CIFS da ONTAP garante que esses xatrs sejam totalmente suportados, permitindo uma integração perfeita com serviços e aplicativos do Windows que dependem desses metadados para a funcionalidade e aplicação de políticas.

Quando os arquivos são acessados ou transferidos por compartilhamentos SMB/CIFS gerenciados pelo ONTAP, o sistema preserva a integridade dos xatrs, garantindo que todos os metadados sejam mantidos e permaneçam consistentes. Isso é particularmente importante para manter as configurações de segurança e para aplicativos que dependem do xattrs para configuração ou operação. O manuseio robusto de xatrs da ONTAP no contexto SMB/CIFS garante que o compartilhamento de arquivos entre diferentes plataformas e ambientes seja confiável e seguro, proporcionando aos usuários uma experiência perfeita e aos administradores a garantia de que as políticas de governança de dados são mantidas. Seja para colaboração, arquivamento de dados ou conformidade, a atenção da ONTAP aos xatrs em compartilhamentos SMB/CIFS representa seu compromisso com a excelência no gerenciamento de dados e interoperabilidade em ambientes de sistemas operacionais mistos.

Ponto de aplicação da política (PEP) e ponto de decisão da política (PDP) na ABAC

Em um sistema de controle de acesso baseado em atributos (ABAC), o ponto de aplicação de políticas (PEP) e o PDP (Policy Decision Point) desempenham papéis cruciais. O PEP é responsável pela aplicação de políticas de controle de acesso, enquanto o PDP toma a decisão de conceder ou negar acesso com base nas políticas.

No contexto do snippet de código Python fornecido, o próprio script atua como um PEP. Ele impõe a decisão de controle de acesso, quer concedendo acesso ao arquivo abrindo-o e lendo seu conteúdo ou negando acesso através da criação de um `PermissionError`.

O PDP, por outro lado, faria parte do sistema SELinux subjacente. Quando o script tenta abrir o arquivo com um contexto específico do SELinux, o sistema SELinux verifica suas políticas para decidir se deseja conceder ou negar acesso. Esta decisão é então aplicada pelo script.

Abaixo está um exemplo detalhado de como esse código funciona em um ambiente ABAC:

1. O script define o contexto SELinux para `jrsmith` contexto usando a `selinux.setcon()` função. Isso é equivalente a `jrsmith` tentar acessar o arquivo.
2. O script tenta abrir o arquivo. É aqui que o PEP entra em jogo.
3. O sistema SELinux verifica suas políticas para ver se `jrsmith` (ou mais especificamente, um usuário com `jrsmith` contexto SELinux) tem permissão para acessar o arquivo. Esta é a função do PDP.
4. Se `jrsmith` for permitido acessar o arquivo, o sistema SELinux permite que o script abra o arquivo e o script leia e imprima o conteúdo do arquivo.
5. Se `jrsmith` não for permitido acessar o arquivo, o sistema SELinux impede que o script abra o arquivo e o script gera um `PermissionError`.
6. O script restaura o contexto original do SELinux para garantir que a alteração temporária do contexto não afete outras operações.

Usando Python, o código para obter o contexto é mostrado abaixo onde o caminho do arquivo variável é o documento que deve ser verificado:

```
#Get the current context

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

Clonagem de ONTAP e SnapMirror

As tecnologias de clonagem e SnapMirror da ONTAP foram projetadas para fornecer recursos de replicação e clonagem de dados eficientes e confiáveis, garantindo que todos os aspetos dos dados de arquivos, incluindo atributos estendidos (xattrs), sejam preservados e transferidos junto com o arquivo. Os xattrs são críticos, pois armazenam metadados adicionais associados a um arquivo, como rótulos de segurança, informações de controle de acesso e dados definidos pelo usuário, essenciais para manter o contexto e integridade do arquivo.

Quando um volume é clonado usando a tecnologia FlexClone da ONTAP, uma réplica gravável exata do volume é criada. Esse processo de clonagem é instantâneo e eficiente em espaço, e inclui todos os dados e metadados de arquivos, garantindo que os xatrs sejam totalmente replicados. Da mesma forma, o SnapMirror garante que os dados sejam espelhados para um sistema secundário com fidelidade total. Isso inclui xattrs, que são cruciais para aplicativos que dependem desses metadados para funcionar corretamente.

Ao incluir xatrs nas operações de clonagem e replicação, o NetApp ONTAP garante que todo o conjunto de dados, com todas as suas características, esteja disponível e consistente em sistemas de storage primário e secundário. Essa abordagem abrangente ao gerenciamento de dados é vital para organizações que exigem proteção de dados consistente, recuperação rápida e adesão a padrões regulatórios e de conformidade. Ele também simplifica o gerenciamento de dados em diferentes ambientes, seja no local ou na nuvem, fornecendo aos usuários a confiança de que seus dados estão completos e inalterados durante esses processos.

NFSv4,2 as etiquetas de segurança têm as ressalvas definidas no 2.

Exemplos de controle do acesso aos dados

A seguinte entrada de exemplo para dados armazenados no cert PKI de John R Smith mostra como a abordagem do NetApp pode ser aplicada a um arquivo e fornecer controle de acesso refinado.

Esses exemplos são para fins ilustrativos, e é responsabilidade do governo definir quais metadados são rótulos de segurança NFSv4,2 e xattrs. Detalhes sobre a atualização e retenção de rótulos são omitidos para simplificar.

Chave	Valor
EntitySecurityMark	t:S01 NÃO CLASSIFICADO

Informações	{
	"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"
	}
	}

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

Chave	Valor

AdminOrganization	{
	"value": "DoD"
	}

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

CitizensaStatus	{
	"value": "US"
	}

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

Chave	Valor
CountryOfAffiliations	`[ { "value": "USA" } ]`
DigitalIdentifier	`{ "classification": "UNCLASSIFIED", "value": "cn=smith john r jrsmith, ou=dod, o=u.s. government, c=us" }`
It is always	`{ "value": "DoD" }`
DutyOrganization	`{ "value": "DoD" }`
Tipo de entidade	`{ "value": "GOV" }`

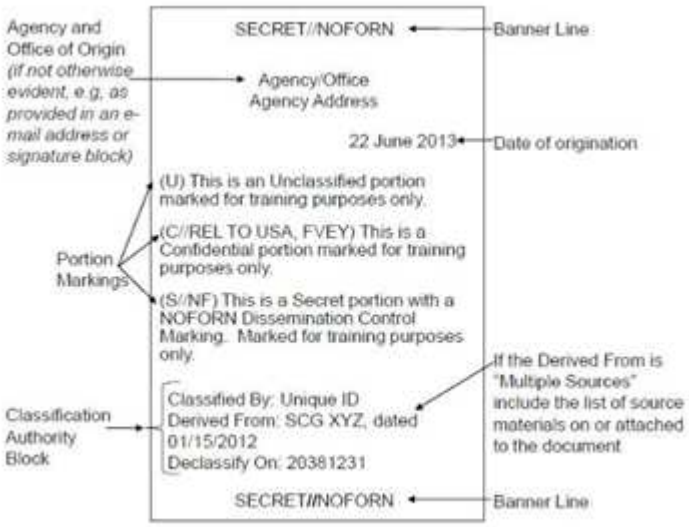
Chave	Valor

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

Esses direitos PKI mostram os detalhes de acesso de John R. Smith, incluindo acesso por tipo de dados e atribuição.

Se John R. Smith criou e salvou um documento chamado *"sample_analysis.doc"*, de acordo com as questões relevantes de orientação política, o usuário adicionaria as marcas apropriadas de banner e porção, agência e escritório de origem e bloco de autoridade de classificação adequado com base na classificação do documento, conforme mostrado na imagem a seguir. Estes metadados ricos só são compreensíveis depois de terem sido digitalizados pelo processamento de linguagem Natural (PNL) e terem regras aplicadas para fazer sentido a partir das marcações. Ferramentas como a classificação NetApp BlueXP podem fazer isso, mas são menos eficientes para decisões de controle de acesso, porque exigem permissão para olhar dentro do documento.

Marcação da parte do documento CAPCO não classificada



Em cenários em que os metadados IC-TDF são armazenados separadamente do arquivo, o NetApp defende uma camada adicional de controle de acesso refinado. Isso envolve o armazenamento de informações de controle de acesso tanto no nível de diretório quanto em associação com cada arquivo. Como exemplo, considere as seguintes tags vinculadas a um arquivo:

- NFSv4,2 rótulos de segurança: Utilizados para tomar decisões de segurança
- Xattrs: Fornecer informações complementares pertinentes ao arquivo e aos requisitos do programa organizacional

Os pares chave-valor a seguir são exemplos de metadados que podem ser armazenados como xattrs e oferecer informações detalhadas sobre o criador do arquivo e classificações de segurança associadas. Esses metadados podem ser aproveitados por aplicativos clientes para tomar decisões de acesso informado e organizar arquivos de acordo com os padrões e requisitos organizacionais.

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

Chave	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"
	},

Chave	Valor
user.geo_point	[-78.7941, 35.7956]

```
    }
}
```

Auditoria de alterações em rótulos

A auditoria de alterações em rótulos de segurança xattrs ou NFS é um aspeto crítico do gerenciamento e da segurança do sistema de arquivos. As ferramentas padrão de auditoria do sistema de arquivos permitem o monitoramento e o Registro de todas as alterações em um sistema de arquivos, incluindo modificações em atributos estendidos e rótulos de segurança.

Em ambientes Linux, o `auditd` daemon é comumente usado para estabelecer auditoria para eventos de sistema de arquivos. Ele permite que os administradores configurem regras para observar chamadas específicas do sistema relacionadas a alterações xattr, como `setxattr`, `lsetxattr` e `fsetxattr` para definir atributos e, `lremovexattr` e `fremovexattr` para `removexattr` remover atributos.

O ONTAP FPolicy amplia esses recursos fornecendo uma estrutura robusta para monitoramento e controle em tempo real de operações de arquivos. O FPolicy pode ser configurado para oferecer suporte a vários eventos xattr, oferecendo controle granular sobre as operações de arquivos e a capacidade de aplicar políticas abrangentes de gerenciamento de dados.

Para usuários que utilizam xattrs, especialmente em ambientes NFSv3 e NFSv4, apenas determinadas combinações de operações de arquivos e filtros são suportadas para monitoramento. A lista de combinações de filtros e operação de arquivos compatíveis para monitoramento FPolicy de eventos de acesso a arquivos NFSv3 e NFSv4 é detalhada abaixo:

Operações de arquivos compatíveis	Filtros suportados
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

Exemplo de um snippet de log auditd para uma operação 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"
```

Ativar o ONTAP FPolicy para usuários que trabalham com o xattrs fornece uma camada de visibilidade e controle essencial para manter a integridade e a segurança do sistema de arquivos. Ao aproveitar os recursos

avançados de monitoramento da FPolicy, as organizações podem garantir que todas as alterações aos xattrs sejam rastreadas, auditadas e alinhadas com seus padrões de segurança e conformidade. Essa abordagem proativa para o gerenciamento do sistema de arquivos é por isso que habilitar o ONTAP FPolicy é altamente recomendado para qualquer organização que queira aprimorar suas estratégias de governança e proteção de dados.

Integração com software de controle de acesso e identidade ABAC

Para aproveitar totalmente os recursos do controle de acesso baseado em atributos (ABAC), o ONTAP pode se integrar com um software de gerenciamento de identidade e acesso orientado para ABAC.

> Em paralelo a este conteúdo, o NetApp tem uma implementação de referência usando GreyBox. Uma suposição para este conteúdo é que os serviços de identidade, autenticação e acesso do governo incluem, no mínimo, um ponto de aplicação da Política (PEP) e um ponto de Decisão da Política (PDP) que atuam como intermediários para o acesso ao sistema de arquivos.

Em um ambiente prático, uma organização empregaria uma mistura de rótulos de segurança NFS e xattrs. Eles são usados para representar uma variedade de metadados, incluindo classificação, segurança, aplicativo e conteúdo, que são todos fundamentais para tomar decisões ABAC. O XATTR, por exemplo, pode ser usado para armazenar os atributos de recursos que o PDP usa para seu processo de tomada de decisão. Um atributo pode ser definido para representar o nível de classificação de um arquivo (por exemplo, "não classificado", "confidencial", "segredo" ou "segredo superior"). O PDP poderia então utilizar este atributo para impor uma política que restringe os utilizadores a aceder apenas a ficheiros que tenham um nível de classificação igual ou inferior ao nível de autorização.

Exemplo de fluxo de processo para ABAC

1. O usuário apresenta credenciais (por exemplo, PKI, OAuth, SAML) para acesso ao sistema ao PEP e obtém resultados do PDP.

   A função do PEP é intercetar a solicitação de acesso do usuário e encaminhá-la para o PDP.

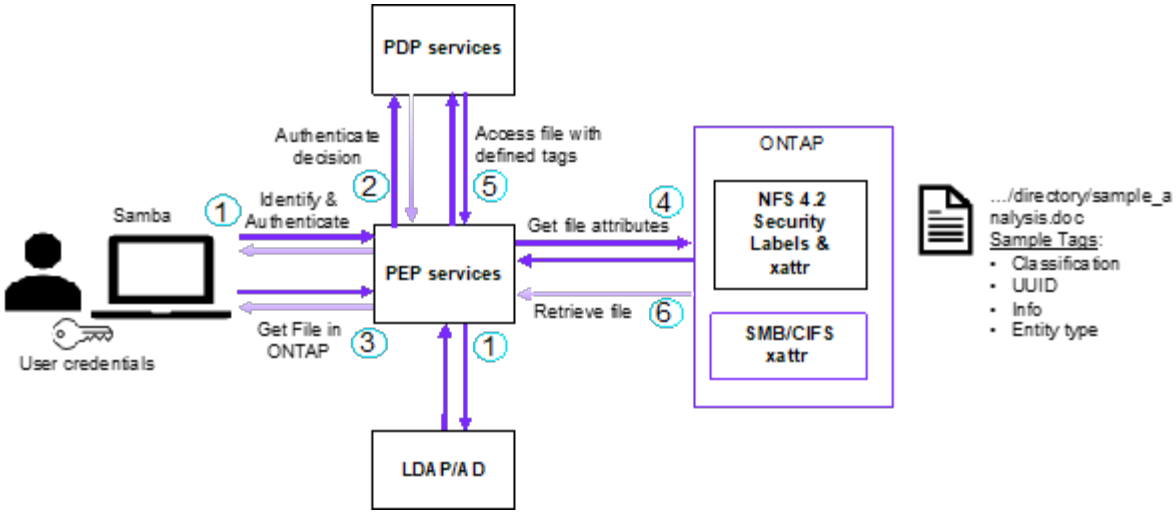
2. Em seguida, o PDP avalia essa solicitação em relação às políticas estabelecidas da ABAC.

   Essas políticas consideram vários atributos relacionados ao usuário, ao recurso em questão e ao ambiente circundante. Com base nessas políticas, o PDP toma uma decisão de acesso para permitir ou negar e, em seguida, comunica essa decisão de volta ao PEP.

   PDP fornece política para PEP para fazer cumprir. O PEP então impõe essa decisão, concedendo ou negando o pedido de acesso do usuário conforme decisão do PDP.

3. Após uma solicitação bem-sucedida, o usuário solicita um arquivo armazenado no ONTAP (AFF, AFF-C, por exemplo).
4. Se a solicitação for bem-sucedida, o PEP obtém tags de controle de acesso de grãos finos do documento.
5. PEP solicita política para o utilizador com base nos certificados desse utilizador.
6. O PEP toma uma decisão com base na política e nas tags se o usuário tiver acesso ao arquivo e permitir que o usuário recupere o arquivo.

> O acesso real pode ser feito usando tokens que não são protegidos.



Informações relacionadas

- "NFS no NetApp ONTAP: Guia de práticas recomendadas e implementação"
- Pedido de comentários (RFC)
  - RFC 2203: Especificação do protocolo RPCSEC_GSS
  - RFC 3530: Protocolo NFS (Network File System) versão 4

Informações sobre direitos autorais

Informações sobre marcas comerciais