基于属性的访问控制

ONTAP Technical Reports

NetApp
February 23, 2026

目录

基于属性的访问控制

使用ONTAP进行基于属性的访问控制

从9.12.1开始、您可以为ONTAP配置NFSv4.2安全标签和扩展属性(xattrs)、以便使用属性和基于属性的访问控制(ABAC)支持基于角色的访问控制(Role-Based Access Control、RBAC)。

ABAC是一种授权策略、可根据用户属性、资源属性和环境条件定义权限。ONTAP与NFS v4.2安全标签和xattt的集成符合NIST特刊800-162中规定的ABAC解决方案NIST标准。

您可以使用NFS v4.2安全标签和xattrs分配文件用户定义的属性和标签。ONTAP可以与面向ABAC的身份和访问管理软件集成、以根据这些属性和标签实施精细的文件和文件夹访问控制策略。

相关信息

- "使用ONTAP进行ABAC的方法"
- "NetApp ONTAP中的NFS：最佳实践和实施指南"

ONTAP中基于属性的访问控制(ABAC)的方法

ONTAP提供了多种可用于实现文件级基于属性的访问控制(ABAC)的方法、包括NFS v4.2安全标签和使用NFS的扩展属性(xattrs)。

NFS v4.2安全标签

从ONTAP 9.9.1开始、支持名为标记NFS的NFS v4.2功能。

NFS v4.2安全标签是一种使用SELinux标签和强制访问控制(Mandat强制 访问控制、MAC)管理精细文件和文件夹访问的方法。这些MAC标签与文件和文件夹存储在一起、并与UNIX权限和NFS v4.x ACL结合使用。

支持NFS v4.2安全标签意味着ONTAP现在可以识别和了解NFS客户端的SELinux标签设置。RFC 7204中介绍了NFS v4.2安全标签。

NFS v4.2安全标签的使用情形如下：

- 虚拟机(VM)映像的MAC标签
- 公共部门的数据安全分类(机密、最高机密和其他分类)
- 安全合规性
- 无磁盘 Linux

启用 **NFS v4.2** 安全标签

您可以使用以下命令启用或禁用NFS v4.2安全标签(需要高级权限)：

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

有关的详细信息 `vserver nfs modify`，请参见"ONTAP命令参考"。

NFS v4.2安全标签的强制实施模式

从ONTAP 9.9.1开始、ONTAP支持以下强制实施模式：

- 受限服务器模式：ONTAP无法强制执行标签，但可以存储和传输标签。

  更改MAC标签的功能由客户端实施。

- 来宾模式：如果客户端未标记为NFS感知型(v4.1或更低版本)，则不会传输MAC标签。

  ONTAP当前不支持完整模式(存储和强制实施MAC标签)。

NFS v4.2安全标签示例

以下配置示例演示了使用Red Hat Enterprise Linux 9.3 (Plow)的概念。

根据John R. Smith的凭据创建的用户 `jrsmith`具有以下帐户Privileges：

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

角色有两个：具有特权的用户的管理员帐户和MLS Privileges表中所述的用户 `jrsmith`：

用户	角色	键入	级别
`admins`	`sysadm_r`	`sysadm_t`	`t:s0`
`jrsmith`	`user_r`	`user_t`	`t:s1 - t:s4`

在此示例环境中，用户 `jrsmith`可以访问级别为的 `s3`文件 `s0`。我们可以加强现有的安全分类、如下所述、以确保管理员无权访问用户特定的数据。

- Shu =特权管理员用户数据
- Shu =未分类数据
- S1 =机密
- S2 =机密数据
- S3 =排名靠前的机密数据

使用**MCS**的**NFS v4.2**安全标签示例

除了多级别安全性(MLS)之外、另一项称为多类别安全性(MCS)的功能还允许您定义项目等类别。

NFS安全标签	价值
entitySecurityMark	t:s01 = UNCLASSIFIED

扩展属性(xatts)

从ONTAP 9.12.1开始、ONTAP支持xattr。xattr允许元数据与系统提供的范围以外的文件和目录相关联、例如访问控制列表(ACL)或用户定义的属性。

要实施xatts、您可以在Linux中使用 `setfattr`和 `getfattr`命令行实用程序。这些工具为管理文件和目录的其他元数据提供了一种强大的方式。使用时应小心、因为使用不当可能会导致意外行为或安全问题。有关详细的使用说明、请始终参考 `setfattr`和 `getfattr`手册页或其他可靠的文档。

在ONTAP文件系统上启用xatts后、用户可以设置、修改和检索文件的任意属性。这些属性可用于存储有关标准文件属性集未捕获的文件的其他信息、例如访问控制信息。

在ONTAP中使用xattrs有多个要求和限制：

- Red Hat Enterprise Linux 8.4或更高版本
- Ubuntu 22.04或更高版本
- 每个文件最多可以包含128个xatts
- XATTR密钥限制为255字节
- 组合键或值大小为每个xattr 1、729字节
- 目录和文件可以包含xatts
- 要设置和检索xattr、 `w`必须为用户和组启用写入模式位

Xatts在用户命名空间中使用、对ONTAP本身没有任何内在意义。而是由与文件系统交互的客户端应用程序来确定和管理它们的实际应用程序。

XATTR用例示例：

- 记录负责创建文件的应用程序的名称
- 维护对从中获取文件的电子邮件的引用
- 建立用于组织文件对象的分类框架
- 使用原始下载源的URL标记文件

用于管理**xattrs**的命令

- `setfattr`设置文件或目录的扩展属性：

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

  命令示例：

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

- `getfattr`检索特定扩展属性的值或列出文件或目录的所有扩展属性：

  特定属性： `getfattr -n <attribute_name> <file or directory name>`

  所有属性： `getfattr <file or directory name>`

  命令示例：

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

XATTR键值对示例

下表显示了两个xattr键值对示例：

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

ACE for xatts的用户权限

访问控制条目(ACE)是ACL中的一个组件、用于定义为特定资源(例如文件或目录)授予单个用户或一组用户的访问权限。每个ACE都指定允许或拒绝的访问类型、并与特定安全主体(用户或组身份)相关联。

xatts需要访问控制条目**(ACE)**

- RetrievE xattr：用户读取文件或目录的扩展属性所需的权限。"R"表示需要读取权限。
- set xattr：修改或设置扩展属性所需的权限。"a"、"w"和"T"表示不同的权限示例、例如附加、写入以及与xatts相关的特定权限。
- files：用户需要附加、写入以及可能与xatts相关的特殊权限来设置扩展属性。
- 目录：设置扩展属性需要特定权限"T"。

文件类型	检索**xattr**	设置**xattrs.**
文件	R	A、W、T
目录	R	T

与**ABAC**身份和访问控制软件集成

为了充分利用ABAC的功能、ONTAP可以与面向ABAC的身份和访问管理软件集成。

在ABAC系统中、政策执行点(PEP)和政策决策点(PDP)发挥着关键作用。PEP负责实施访问控制策略、而PDP则根据策略决定是授予还是拒绝访问。

在实际环境中、组织会混合使用NFS安全标签和xatts。它们用于表示各种元数据、包括分类、安全性、应用程序和内容、这些都有助于ABAC决策。例如、xatts可用于存储PDP决策过程所使用的资源属性。可以定义一个属性来表示文件的分类级别(例如、"未分类"、"机密"、"机密"或"最高机密")。然后、PDP可以使用此属性来强制实施一项策略、该策略将限制用户仅访问分类级别等于或低于其间隙级别的文件。

此内容假定客户的身份、身份验证和访问服务至少包括PEP和PDP、它们充当文件系统访问的中间人。

ABAC流程示例

1. 用户提供系统访问PEP的凭据(例如PKI、OAuth、SAML)、并从PDP获取结果。

   PEP的角色是截获用户的访问请求并将其转发到PDP。

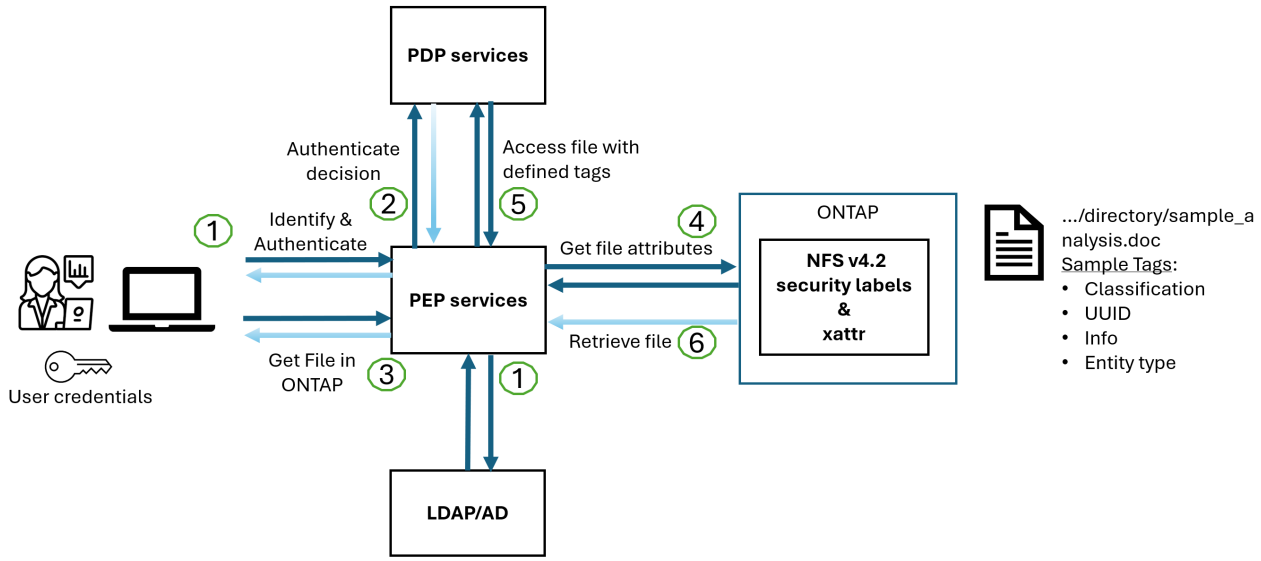
2. 然后、PDP会根据已建立的ABAC策略评估此请求。

   这些策略会考虑与用户、相关资源和周围环境相关的各种属性。根据这些政策、PDP做出允许或拒绝访问决定、然后将该决定传达给PEP。

   PDP为PEP提供了要强制实施的策略。然后、PEP会根据PDP的决定批准或拒绝用户的访问请求、从而强制执行此决定。

3. 请求成功后、用户将请求存储在ONTAP中的文件(例如AFF、AFF C)。
4. 如果请求成功、PEP将从文档中获取精细的访问控制标签。
5. PEP根据该用户的证明请求该用户的策略。
6. PEP根据策略和标记决定用户是否有权访问该文件、并允许用户检索该文件。

实际访问可能使用令牌完成。



ONTAP克隆和SnapMirror

ONTAP的克隆和SnapMirror技术旨在提供高效可靠的数据复制和克隆功能、确保文件数据的所有方面(包括xattrs)都与文件一起保留和传输。xattrs非常重要、因为它们存储与文件关联的其他元数据、例如安全标签、访问控制信息和用户定义的数据、这些对于维护文件的上下文和完整性至关重要。

使用ONTAP的FlexClone技术克隆卷时、系统会为该卷创建一个精确的可写副本。此克隆过程可瞬时完成、并且节省空间、其中包括所有文件数据和元数据、从而确保完全复制xatts。同样、SnapMirror可确保以完全保真的方式将数据镜像到二级系统。其中包括xatts、对于依赖此元数据的应用程序正常运行至关重要。

通过在克隆和复制操作中使用xatts、NetApp ONTAP可确保整个数据集及其所有特征在主存储系统和二级存储系统中可用且一致。这种全面的数据管理方法对于需要一致的数据保护、快速恢复以及遵守合规性和法规标准的组织至关重要。同时、它还可以简化不同环境(无论是内部环境还是云环境)中的数据管理、让用户确信其数据在这些过程中是完整的、不会被更改。

NFS v4.2安全标签具有中定义的说明NFS v4.2安全标签。

审核标签更改

审核对xattr或NFS安全标签的更改是文件系统管理和安全性的一个关键方面。通过标准文件系统审核工具、可以监控和记录对文件系统的所有更改、包括对xattrs和安全标签的修改。

在Linux环境中、 `auditd`守护进程通常用于为文件系统事件建立审核。它允许管理员配置规则，以监视与`xattr`更改相关的特定系统调用，例如 `setxattr`、、 `lsetxattr`以及 `fsetxattr`设置属性和 `removexattr`、 `lremovexattr`以及 `fremovexattr`删除属性。

ONTAP FPolicy通过提供一个用于实时监控和控制文件操作的强大框架、扩展了这些功能。可以对FPolicy进行配置、使其支持各种xattr事件、从而对文件操作进行精细控制、并能够实施全面的数据管理策略。

对于使用xattrs的用户、尤其是在NFS v3和NFS v4环境中、仅支持使用特定的文件操作和筛选器组合进行监控。下面详细列出了对NFS v3和NFS v4文件访问事件进行FPolicy监控时支持的文件操作和筛选器组合：

支持的文件操作	支持的筛选器
`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`

setattr操作的**auditd**日志段示例：

```
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"
```

为使用xatts的用户启用"ONTAP FPolicy"可提供一层可见性和控制、这对于维护文件系统的完整性和安全性至关重要。通过利用FPolicy的高级监控功能、企业可以确保跟踪、审核对xatts的所有更改、并使其符合其安全和合规性标准。这种主动式文件系统管理方法是强烈建议任何希望增强数据监管和保护策略的组织启用ONTAP FPolicy的原因。

控制数据访问的示例

以下John R. Smith的PKI证书中存储的数据条目示例显示了如何将NetApp的方法应用于文件并提供精细的访问控制。

> 这些示例仅用于说明目的、客户负责确定与NFS v4.2安全标签和xatts关联的元数据。为了简便起见、省略了有关更新和标签保留的详细信息。

示例**PKI**证书值

密钥	价值
实体SecurityMark	T：S01 =未分类

密钥	价值

信息	{
	"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"
	}
	}

规格	" DoD"
UUID	b4111349-7875-4115-AD30-0928565f2e15

管理组织	{
	"value": "DoD"
	}

密钥	价值

简报会	[
	{
	"value": "ABC1000"
	},
	{
	"value": "DEF1001"
	},
	{
	"value": "EFG2000"
	}
	]

"Stat.shipStatus"	{
	"value": "US"
	}

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

国家或地区附属机构	[
	{
	"value": "USA"
	}
	]

密钥	价值

Digital标识 符	<pre>{
	  "classification": "UNCLASSIFIED",
	  "value": "cn=smith john r jrsmith, ou=dod, o=u.s.
	government, c=us"
	}</pre>

DissemTos	<pre>{
	  "value": "DoD"
	}</pre>

双重组织	<pre>{
	  "value": "DoD"
	}</pre>

实体类型	<pre>{
	  "value": "GOV"
	}</pre>

FineAccessControl	<pre>[
	  {
	  "value": "SI"
	  },
	  {
	  "value": "TK"
	  },
	  {
	  "value": "NSYS"
	  }
	]</pre>

这些PKI授权显示John R. Smith的访问详细信息、包括按数据类型和属性进行的访问。

如果IC-TDF元数据与文件分开存储、则NetApp主张增加一层精细的访问控制。这涉及到在目录级别以及与每个文件关联的情况下存储访问控制信息。例如、请考虑以下链接到文件的标记：

- NFS v4.2安全标签：用于制定安全决策

- xatts：提供与文件和组织计划要求相关的补充信息

以下键-值对是可存储为xatts的元数据示例、并提供有关文件创建者和关联安全分类的详细信息。客户端应用程序可以利用这些元数据做出明智的访问决策、并根据组织标准和要求组织文件。

- xattr键值对的示例*

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

密钥	价值

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"
	},

密钥	价值
user.geo_point	[-78.7941, 35.7956]

```
    }
  }
```

相关信息

- "NetApp ONTAP中的NFS：最佳实践和实施指南"
- "ONTAP命令参考"
- 请求注释(RFC)
  - "RFC 7204：标记NFS的要求"
  - "RFC 2203：《RPCSEC_GSS协议规范》"
  - "RFC 3530：《网络文件系统(Network File System、NFS)版本4协议》"