



基于属性的访问控制 ONTAP 9

NetApp
January 17, 2025

目录

基于属性的访问控制	1
使用ONTAP进行基于属性的访问控制	1
使用ONTAP进行ABAC的方法	1

基于属性的访问控制

使用ONTAP进行基于属性的访问控制

您可以使用ONTAP实施具有属性和基于属性的访问控制(ABAC)的增强RBAC。ONTAP提供了多种客户可用于实现文件级ABAC的方法、包括使用NFS和SMB/CCIFS的标记NFS 4.2和XATTRS。

基于属性的访问控制(ABAC)是一种管理访问权限的复杂方法、该方法会考虑用户属性、资源属性和环境条件。国家标准和技术研究所(NIST)为ABAC制定了一个标准、为安全一致地实施该标准提供了一个框架。

从NFS.12.1开始、您可以ONTAP使用ONTAP 9 4.2安全标签和扩展属性(XATTRS)配置NFSv4.2、以便将其与基于角色的访问控制(Role-Based Access Control、RBAC)和基于属性的访问控制(ABAC)身份集成。通过这种集成、ONTAP可以访问归类为符合NIST ABAC标准的数据管理解决方案的控制软件、从而提供一种强大而高级的方法来管理复杂环境中的访问权限、包括策略实施点(PEP)、策略决策点(PDP)以及考虑与用户、资源和环境相关属性的策略。

NetApp ONTAP与扩展属性(XATTRS)和基于属性的访问控制(ABAC)软件的集成符合NIST特刊800-162中规定的准则、确保符合ABAC实施的NIST标准。通过使用NFS 4.2安全标签和XATTRS、可以将用户定义的属性与文件关联起来、从而满足NIST ABAC标准在做出访问控制决策时考虑资源属性的要求。ABAC软件的PEP和PDP符合NIST ABAC标准对访问控制流程中这些组件的要求。定义考虑多个属性和条件的复杂策略的能力符合NIST ABAC标准对基于策略的访问控制的要求。

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"](#)
- 请求注释(RFC)
 - 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》

使用ONTAP进行ABAC的方法

ONTAP提供了多种客户可用于实现文件级ABAC的方法、包括使用NFS和SMB/CCIFS的标记NFSv4.2和XATTRS。

标记为NFSv4.2

从NFS.9.1开始、支持名为标记ONTAP 9的NFSv4.2功能。

标记NFS是一种使用SELinux标签和强制访问控制(Mandatory Access Control、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NFSv4.x ACL结合使用。

支持标记NFS意味着ONTAP现在可以识别和了解NFS客户端的SELinux标签设置。标记的NFS在RFC 7204中进行了介绍。

标记为NFSv4.2的使用情形包括以下内容：

- 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

启用带标签的NFSv4.2

您可以使用以下高级权限选项启用或禁用带标签的NFS:

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

此参数是可选的，默认设置为 disabled。

已标记NFSv4.2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 标签的功能也由客户端强制实施。

- 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)。

标记为NFSv4.2的配置示例

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	Role	Type	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



遵循您组织的安全策略

使用MCS的NFSv4.2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(XATTRS)

从ONTAP 9. 12.1开始, ONTAP支持xattr。xattr允许元数据与超出系统提供范围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`命令行实用程序来管理文件系统对象的xatts。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。应谨慎使用、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xatts的要求

- 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的用例

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

ACE的用户权限(用于扩展属性)

访问控制条目(ACE)是访问控制列表(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。

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

xatts所需权限的说明:

REQUERVE 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 xatts:** 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"。

xattrs的SMB/CCIFS协议支持

ONTAP对SMB/CCIFS协议的支持扩展到对xattrs的全面处理、xattrs是Windows环境中文件元数据不可或缺的一部分。通过扩展属性、用户和应用程序可以存储标准文件属性集之外的其他信息、例如作者详细信息、自定义安全描述符或应用程序特定的数据。ONTAP的SMB/CCIFS实施可确保完全支持这些xattrs、从而可以与依赖此元数据执行功能和策略的Windows服务和应用程序无缝集成。

在通过ONTAP管理的SMB/CCIFS共享访问或传输文件时、系统会保留xattr的完整性、从而确保所有元数据都得以保留并保持一致。这对于维护安全设置以及使用xattr进行配置或操作的应用程序来说尤其重要。ONTAP在SMB/CCIFS环境中对xattrs的强大处理可确保不同平台和环境之间的文件共享可靠且安全、从而为用户提供无缝体验、并确保管理员遵守数据监管策略。无论是协作、数据归档还是合规性、ONTAP对SMB/CCIFS共享中的xattr的关注体现了其在混合操作系统环境中实现卓越数据管理和互操作性的承诺。

ABAC中的政策执行点(PEP)和政策决策点(PDP)

在基于属性的访问控制(ABAC)系统中、策略实施点(PEP)和策略决策点(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。

在所提供的Python代码段上下文中、脚本本身充当PEP。它可以通过打开文件并读取其内容来授予对该文件的访问权限、也可以通过提出来拒绝访问来强制执行访问控制决策 `PermissionError`。

另一方面、PDP将是底层SELinux系统的一部分。当脚本尝试打开具有特定SELinux环境的文件时、SELinux系统会检查其策略以确定是授予还是拒绝访问。然后、该脚本将强制执行此决定。

下面是此代码在ABAC环境中的工作原理的分步示例细分：

1. 该脚本使用函数将SELinux上下文设置为 `jrsmith`上下文`` `selinux.setcon()`。这相当于 `jrsmith`尝试访问文件`。
2. 该脚本将尝试打开该文件。这就是PEP发挥作用的地方。
3. SELinux系统会检查其策略、以确定是否 `jrsmith`允许`` (更具体地说、是具有SELinux环境的用户 `jrsmith)`访问该文件。这是PDP的角色。
4. 如果 `jrsmith`允许访问该文件``、则SELinux系统允许该脚本打开该文件、该脚本将读取并打印该文件的内容。
5. 如果 `jrsmith`不允许访问该文件``、SELinux系统将阻止该脚本打开该文件、并且该脚本将发出 `PermissionError`。
6. 该脚本将还原初始SELinux上下文、以确保临时上下文更改不会影响其他操作。

使用Python，获取上下文的代码如下所示，其中可变文件路径是要检查的文档：

```
#Get the current context

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

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(包括扩展属性(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。



NFSv4.2安全标签具有中定义的说明[标记为NFSv4.2。](#)

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、政府有责任定义什么是NFSv4.2安全标签和xattl。为了简便起见、省略了有关更新和标签保留的详细信息。

密钥	价值
实体SecurityMark	T: S01 =未分类

密钥	价值
信息	<pre> { "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" } } </pre>
规格	" DoD"
UUID	b4111349-7875-4115-AD30-0928565f2e15
管理组织	<pre> { "value": "DoD" } </pre>

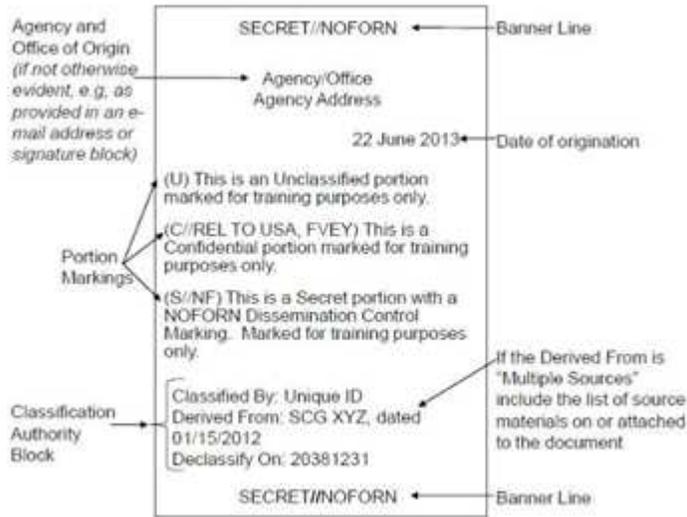
密钥	价值
简报会	<pre>[{ "value": "ABC1000" }, { "value": "DEF1001" }, { "value": "EFG2000" }]</pre>
"Stat.shipStatus"	<pre>{ "value": "US" }</pre>
间隙	<pre>[{ "value": "TS" }, { "value": "S" }, { "value": "C" }, { "value": "U" }]</pre>
国家或地区附属机构	<pre>[{ "value": "USA" }]</pre>

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John R. Smith创建并保存了一个名为"samp_mannation_doc"的文档、则根据相关的政策指导发布、用户将根据文档的分类添加适当的横幅和部分标记、机构和原产地以及相应的分类授权块、如下图所示。只有在自然语言处理(NLR)对这种丰富的元数据进行扫描并应用规则使标记有意义之后、才能理解这种元数据。NetApp BlueXP 分类等工具可以做到这一点、但对于访问控制决策来说效率较低、因为它们需要权限才能查看文档内部。

未分类的CA去 文部分标记



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：

- NFSv4.2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。

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

密钥	价值
user.Info	<pre>{ "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" }, }</pre>

密钥	价值
user.geo_point	[-78.7941, 35.7956]

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、包括对扩展属性和安全标签的修改。

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NFSv3和NFSv4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。下面详细列出了在对NFSv3和NFSv4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。

与ABAC身份和访问控制软件集成

为了充分利用基于属性的访问控制(ABAC)的功能、ONTAP可以与面向ABAC的身份和访问管理软件集成。



与此内容并行的是、NetApp具有一个使用GrayBox的参考实施。此内容的一个假设是、政府的身份、身份验证和访问服务至少包括一个策略实施点(PEP)和一个策略决策点(PDP)、它们充当文件系统访问的中间人。

在实际环境中、组织会混合使用NFS安全标签和xattrs。这些元数据用于表示各种元数据、包括分类、安全性、应用程序和内容、它们都有助于ABAC决策。例如、xattr可用于存储PDP用于其决策过程的资源属性。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。

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。

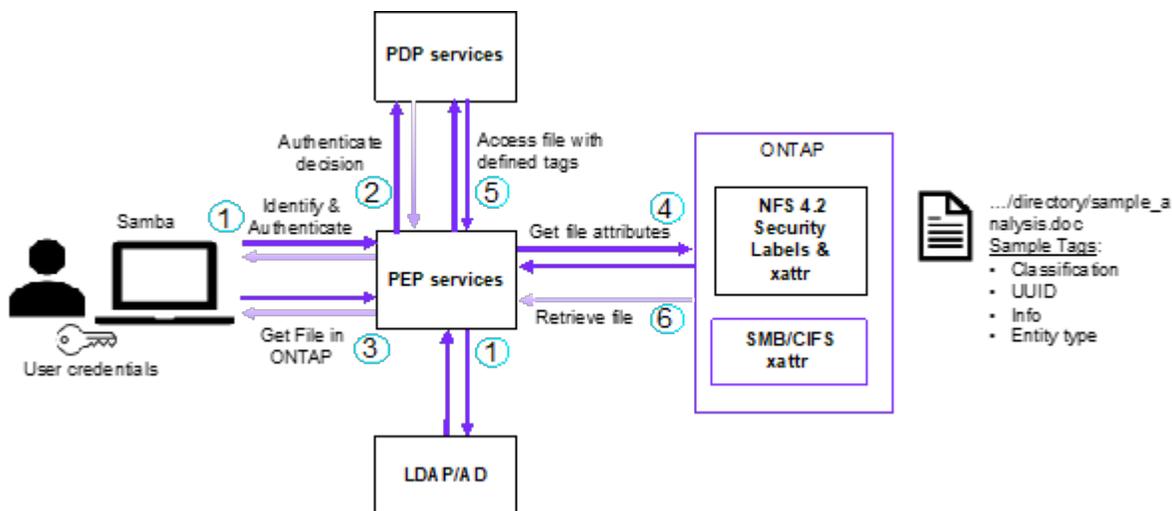
这些策略会考虑与用户、相关资源和周围环境相关的各种属性。根据这些政策、PDP做出允许或拒绝访问决定、然后将该决定传达给PEP。

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。



实际访问可以使用非代理令牌来完成。



相关信息

- "NetApp ONTAP中的NFS: 最佳实践和实施指南"
- 请求注释(RFC)
 - 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》

版权信息

版权所有 © 2025 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。