ONTAP强化准则

ONTAP 9

NetApp
July 18, 2024

目录

ONTAP强化准则

ONTAP安全强化概述

ONTAP提供了一组控件、可用于加强ONTAP存储操作系统(行业领先的数据管理软件)的安全。使用ONTAP的指导和配置设置帮助您的组织满足规定的信息系统机密性、完整性和可用性安全目标。

当前威胁格局的演变为企业在保护数据和信息等最有价值的资产方面提出了独特的挑战。我们面临的高级动态威胁和漏洞越来越复杂。随着模糊和侦察技术对潜在的侵入者的效用的提高、系统管理员必须主动解决数据和信息的安全问题。

> 从2024年7月开始、以前以PDF格式发布的技术报告中的内容已与ONTAP产品文档集成。ONTAP安全文档现在包含了_TR-4569：《ONTAP安全强化指南》中的内容。

ONTAP映像验证

ONTAP提供了一些机制来确保ONTAP映像在升级和启动时有效。

升级映像验证

代码签名有助于验证通过无中断映像更新或自动化无中断映像更新、命令行界面或ONTAP API安装的ONTAP映像是否由NetApp真正生成且未被篡改。ONTAP 9.3引入了升级映像验证。

此功能是对ONTAP升级或恢复的非接触式安全增强功能。除了可以选择验证顶级"image.tgz"签名之外、用户不应执行任何其他操作。

启动时映像验证

从ONTAP 9.4开始、为NetApp AFF A800、AFF A220、FAS2750和FAS2720系统以及采用UEFI BIOS的后续下一代系统启用了统一可扩展固件接口(Unified可扩展固件接口、UEFI)安全启动。

启动期间、启动加载程序会验证安全启动密钥的白表数据库以及与所加载的每个模块关联的签名。验证并加载每个模块后、启动过程将继续进行ONTAP初始化。如果任何模块的签名验证失败，系统将重新启动。

> 这些项目适用于ONTAP映像和平台BIOS。

本地存储管理员帐户

角色、应用程序和身份验证

ONTAP使注重安全的企业能够通过不同的登录应用程序和方法为不同的管理员提供细粒度访问权限。这有助于客户创建以数据为中心的零信任模式。

这些角色可供管理员和Storage Virtual Machine管理员使用。系统将指定登录应用程序方法和登录身份验证方法。

角色

借助基于角色的访问控制(Role-Based Access Control、RBAC)、用户只能访问其工作角色和职能所需的系统和选项。ONTAP中的RBAC解决方案将用户的管理访问权限限制为为为其定义的角色所授予的级别、从而使管理员可以按分配的角色管理用户。ONTAP提供了多种预定义角色。操作员和管理员可以创建、修改或删除自定义访问控制角色、并且可以为特定角色指定帐户限制。

集群管理员的预定义角色

此角色 …	具有此访问级别 …	访问以下命令或命令目录
`admin`	全部	所有命令目录 (`DEFAULT`)
`admin-no-fsa` (从ONTAP 9.12.1开始提供)	读 / 写	• 所有命令目录 (`DEFAULT`) • `security login rest-role` • `security login role`
只读	• `security login rest-role create` • `security login rest-role delete` • `security login rest-role modify` • `security login rest-role show` • `security login role create` • `security login role create` • `security login role delete` • `security login role modify` • `security login role show` • `volume activity-tracking` • `volume analytics`	无
`volume file show-disk-usage`	`autosupport`	全部

• set • system node autosupport	无	所有其他命令目录 (DEFAULT)
backup	全部	vserver services ndmp
只读	volume	无
所有其他命令目录 (DEFAULT)	readonly	全部
• security login password 仅用于管理自己的用户帐户本地密码和密钥信息 • set	无	security
只读	所有其他命令目录 (DEFAULT)	none

。 autosupport 已将角色分配给预定义的 autosupport 帐户、由AutoSupport OnDemand使用。ONTAP会阻止您修改或删除 autosupport 帐户。ONTAP还会阻止您分配 autosupport 其他用户帐户的角色。

Storage Virtual Machine (SVM)管理员的预定义角色

Role name	功能
vsadmin	• 管理自己的用户帐户本地密码和密钥信息 • 管理卷、但卷移动除外 • 管理配额、qtrees、Snapshot副本和文件 • 管理LUN • 执行SnapLock操作、但特权删除除外 • 配置协议：NFS、SMB、iSCSI、FC、FCoE、NVMe/FC和NVMe/TCP • 配置服务：DNS、LDAP和NIS • 监控作业 • 监控网络连接和网络接口 • 监控SVM的运行状况

vsadmin-volume	• 管理自己的用户帐户本地密码和密钥信息 • 管理卷、包括卷移动 • 管理配额、qtrees、Snapshot副本和文件 • 管理LUN • 配置协议：NFS、SMB、iSCSI、FC、FCoE、NVMe/FC和NVMe/TCP • 配置服务：DNS、LDAP和NIS • 监控网络接口 • 监控SVM的运行状况
vsadmin-protocol	• 管理自己的用户帐户本地密码和密钥信息 • 配置协议：NFS、SMB、iSCSI、FC、FCoE、NVMe/FC和NVMe/TCP • 配置服务：DNS、LDAP和NIS • 管理LUN • 监控网络接口 • 监控SVM的运行状况
vsadmin-backup	• 管理自己的用户帐户本地密码和密钥信息 • 管理NDMP操作 • 将已还原的卷设置为读/写卷 • 管理SnapMirror关系和Snapshot副本 • 查看卷和网络信息
vsadmin-snaplock	• 管理自己的用户帐户本地密码和密钥信息 • 管理卷、但卷移动除外 • 管理配额、qtrees、Snapshot副本和文件 • 执行SnapLock操作、包括以特权方式删除 • 配置协议：NFS和SMB • 配置服务：DNS、LDAP和NIS • 监控作业 • 监控网络连接和网络接口

vsadmin-readonly	• 管理自己的用户帐户本地密码和密钥信息 • 监控SVM的运行状况 • 监控网络接口 • 查看卷和LUN • 查看服务和协议

应用程序方法

应用程序方法用于指定登录方法的访问类型。可能的值包括 `console`, `http`, `ontapi`, `rsh`, `snmp`, `service-processor`, `ssh`, 和 `telnet`。

将此参数设置为 `service-processor` 可授予用户对服务处理器的访问权限。如果此参数设置为 `service-processor`，则必须将该 `-authentication-method` 参数设置为 `password` ，因为服务处理器仅支持密码身份验证。SVM用户帐户无法访问服务处理器。因此，当参数设置为时，操作员和管理员不能使用 `-vserver` 参数 `service-processor`。

要进一步限制对的访问， `service-processor` 请使用命令 `system service-processor ssh add-allowed-addresses`。命令 `system service-processor api-service` 可用于更新配置和证书。

出于安全原因、Telnet和远程Shell (RSH)默认处于禁用状态、因为NetApp建议使用安全Shell (SSH)进行安全远程访问。如果需要或唯一需要Telnet或RSH、则必须启用它们。

命令用于 `security protocol modify` 修改RSH和Telnet的现有集群范围配置。通过将已启用字段设置为，在集群中启用RSH和Telnet `true`。

身份验证方法

authentication方法参数用于指定用于登录的身份验证方法。

身份验证方法	**Description**
`cert`	SSL证书身份验证
`community`	SNMP 团体字符串
`domain`	Active Directory 身份验证
`nsswitch`	LDAP或NIS身份验证
`password`	Password
`publickey`	公共密钥身份验证
`usm`	SNMP用户安全模型

由于协议安全漏洞、不建议使用NIS。

从ONTAP 9.3开始、本地SSH帐户可以使用和密码作为两种身份验证方法进行链式双因素身份验证 `admin publickey`。除了 `-authentication-method` 命令中的字段 `security login` 之外、还添加了一个名为的新字段 `-second-authentication-method`。公共密钥或密码可以指定为 `-authentication-method`

或 `-second-authentication-method`。但是、在SSH身份验证期间、顺序始终是部分身份验证的公共密钥、后跟用于完全身份验证的密码提示。

```
[user@host01 ~]$ ssh ontap.netapp.local
Authenticated with partial success.
Password:
cluster1::>
```

从ONTAP 9.4开始， `nsswitch` 可用作的第二种身份验证方法 `publickey`。

从ONTAP 9.12.1开始、FIDO2也可用于使用YukiKey硬件身份验证设备或其他FIDO2兼容设备进行SSH身份验证。

从ONTAP 9.13.1.开始：

- `domain` 帐户可用作中的第二种身份验证方法 `publickey`。
- 基于时间的一次性密码是由算法生成的临时密码 (`totp`，该算法使用当前时间作为第二种身份验证方法的身份验证因素之一。
- SSH公共密钥以及证书均支持公共密钥撤消、这些证书将在SSH期间进行到期/撤消检查。

有关ONTAP系统管理器、Active IQ Unified Manager和SSH的多因素身份验证(MFA)的详细信息，请参见 "TR-4647：《ONTAP 9中的多因素身份验证》"。

默认管理帐户

应限制管理员帐户、因为管理员角色可以使用所有应用程序进行访问。diag帐户允许访问系统Shell、并且只能由技术支持人员保留以执行故障排除任务。

有两个默认管理帐户： `admin` 和 `diag`。

孤立帐户是一个主要的安全媒介、通常会导致漏洞、包括特权升级。这些帐户是用户帐户存储库中保留的不必要和未使用的帐户。它们主要是从未使用过的默认帐户、或者从未更新或更改过密码的默认帐户。为了解决此问题、ONTAP支持删除和重命名帐户。

ONTAP无法删除或重命名内置帐户。但是、NetApp建议使用lock命令锁定任何不需要的内置帐户。

尽管孤立帐户是一个严重的安全问题、但NetApp强烈建议测试从本地帐户存储库中删除帐户的效果。

列出本地帐户

要列出本地帐户、请运行命令。 `security login show`

```
cluster1::*> security login show -vserver cluster1

Vserver: cluster1
                              Authentication              Acct   Is-Nsswitch
User/Group Name  Application  Method    Role Name         Locked Group
---------------- -----------  --------- ----------------- ------ -----------
admin            console      password  admin             no     no
admin            http         password  admin             no     no
admin            ontapi       password  admin             no     no
admin            service-processor password admin         no     no
admin            ssh          password  admin             no     no
autosupport      console      password  autosupport       no     no
6 entries were displayed.
```

删除默认管理员帐户

该 `admin` 帐户具有管理员角色、并允许使用所有应用程序进行访问。

步骤

1. 创建另一个管理员级别帐户。

   要完全删除默认 `admin` 帐户、必须先创建另一个使用登录应用程序的管理员级别帐户 `console` 。

   > 进行这些更改可能会产生一些不希望看到的影响。始终首先在非生产集群上测试可能影响解决方案安全状态的新设置。

   示例

   ```
   cluster1::*> security login create -user-or-group-name NewAdmin
   -application console -authentication-method password -vserver cluster1
   ```

```
cluster1::*> security login show -vserver cluster1

Vserver: cluster1
                             Authentication              Acct   Is-
Nsswitch
User/Group Name  Application Method    Role Name         Locked Group
---------------- ----------- --------- ----------------- ------
-----------
NewAdmin         console     password  admin             no     no
admin            console     password  admin             no     no
admin            http        password  admin             no     no
admin            ontapi      password  admin             no     no
admin            service-processor password admin        no     no
admin            ssh         password  admin             no     no
autosupport      console     password  autosupport       no     no
7 entries were displayed.
```

2. 创建新的管理员帐户后、请使用帐户登录测试对该帐户的访问权限 `NewAdmin` 。登录时 `NewAdmin` ，将帐户配置为与默认或以前的管理员帐户(例如、、或)具有相同的登录应用程序 `http ontapi service-processor ssh`。此步骤可确保保持访问控制。

   示例

```
cluster1::*> security login create -vserver cluster1 -user-or-group-name
NewAdmin -application ssh -authentication-method password
cluster1::*> security login create -vserver cluster1 -user-or-group-name
NewAdmin -application http -authentication-method password
cluster1::*> security login create -vserver cluster1 -user-or-group-name
NewAdmin -application ontapi -authentication-method password
cluster1::*> security login create -vserver cluster1 -user-or-group-name
NewAdmin -application service-processor -authentication-method password
```

3. 测试完所有功能后、您可以先禁用所有应用程序的管理员帐户、然后再从ONTAP中将其删除。此步骤可作为最终测试、以确认不存在依赖先前管理员帐户的持久功能。

```
cluster1::*> security login lock -vserver cluster1 -user-or-group-name
admin -application *
```

4. 要删除默认管理员帐户及其所有条目、请运行以下命令：

```
cluster1::*> security login delete -vserver cluster1 -user-or-group-name
admin -application *
cluster1::*> security login show -vserver cluster1

Vserver: cluster1
                             Authentication              Acct   Is-
Nsswitch
User/Group Name  Application Method    Role Name         Locked Group
---------------- ----------- --------- ----------------- ------
-----------
NewAdmin         console     password  admin             no     no
NewAdmin         http        password  admin             no     no
NewAdmin         ontapi      password  admin             no     no
NewAdmin         service-processor password admin        no     no
NewAdmin         ssh         password  admin             no     no
autosupport      console     password  autosupport       no     no
7 entries were displayed.
```

设置诊断(diag)帐户密码

存储系统会提供一个名为的诊断帐户 `diag` 。您可以使用 `diag` 帐户在中执行故障排除任务 `systemshell`。该 `diag` 帐户是唯一可用于通过特权命令访问systemshell的帐户 `diag systemshell`。

> systemshell和关联 `diag` 帐户用于进行低级诊断。其访问需要诊断权限级别、并且仅在技术支持指导下使用、以执行故障排除任务。帐户和均不 `diag systemshell` 用于一般管理目的。

开始之前

在访问之前 `systemshell`，您必须使用命令设置 `diag` 帐户密码 `security login password` 。您应使用强密码原则并定期更改 `diag` 密码。

步骤

1. 设置 `diag` 帐户用户密码：

```
cluster1::> set -privilege diag

Warning: These diagnostic commands are for use by NetApp personnel only.
Do you want to continue? \{y|n}: y

cluster1::*> systemshell -node node-01
    (system node systemshell)
diag@node-01's password:

Warning: The system shell provides access to low-level
diagnostic tools that can cause irreparable damage to
the system if not used properly. Use this environment
only when directed to do so by support personnel.

node-01%
```

多管理员验证

从ONTAP 9.11.1开始、您可以使用多管理员验证(MAV)来执行某些操作、例如删除卷或Snapshot副本、但这些操作必须经过指定管理员的批准。这样可以防止受到影响的管理员、恶意管理员或经验不足的管理员进行不希望的更改或删除数据。

配置MAV包括以下内容：

- "创建一个或多个管理员批准组。"
- "启用多管理员验证功能。"
- "添加或修改规则。"

完成初始配置后、只有MAV批准组中的管理员(MAV管理员)才能修改这些元素。

启用MAV后、完成每个受保护操作需要三个步骤：

1. 当用户启动操作时、将显示 "已生成请求。"
2. 在执行之前、需要指定的数量 "MAV管理员必须批准。"
3. 批准后、用户完成操作。

MAV不适用于涉及大量自动化的卷或工作流、因为每个自动化任务都需要经过批准才能完成操作。如果要同时使用自动化和MAV、NetApp建议您对特定MAV操作使用查询。例如、您只能将MAV规则应用 `volume delete` 于不涉及自动化的卷、并且可以使用特定的命名方案来指定这些卷。

有关MAV的更多详细信息，请参见 "ONTAP多管理员验证文档"。

Snapshot副本锁定

Snapshot副本锁定是一项SnapLock功能、通过此功能、可以手动或自动将Snapshot副本

呈现为不可删除的卷Snapshot策略保留期限。Snapshot副本锁定的目的是防止恶意或不可信的管理员删除主ONTAP系统或二级Snapshot。

ONTAP 9.12.1引入了Snapshot副本锁定功能。Snapshot副本锁定也称为防篡改Snapshot锁定。虽然它确实需要SnapLock许可证并初始化合规时钟、但Snapshot副本锁定与SnapLock合规性或SnapLock Enterprise无关。没有值得信赖的存储管理员、就像SnapLock Enterprise一样、它无法像SnapLock Compliance那样保护底层物理存储基础架构。与通过SnapVauling将Snapshot副本存储到二级系统相比、这是一项改进。可以快速恢复主系统上锁定的Snapshot、以还原被勒索软件损坏的卷。

有关Snapshot副本锁定的详细信息，请参见 "ONTAP 文档"。

设置基于证书的**API**访问

必须使用基于证书的身份验证、而不是用于REST API或NetApp易管理性SDK API访问ONTAP的用户ID和密码身份验证。

作为REST API基于证书的身份验证的替代方法，请使用 "基于OAuth2.0令牌的身份验证"。)

您可以按以下步骤中所述在ONTAP上生成并安装自签名证书。

步骤

1. 使用OpenSSL、通过运行以下命令生成证书：

```
openssl req -x509 -nodes -days 1095 -newkey rsa:2048 -keyout test.key
-out test.pem \> -subj "/C=US/ST=NC/L=RTP/O=NetApp/CN=cert_user"
Generating a 2048 bit RSA private key
..............+++
.........................+++
writing new private key to 'test.key'
```

此命令将生成名为的公共证书和名为的 `test.pem` 专用密钥 `key.out`。公用名CN与ONTAP用户ID相对应。

2. 通过运行以下命令并在出现提示时粘贴公共证书的内容、在ONTAP中以隐私增强邮件(prom)格式安装此证书的内容：

```
security certificate install -type client-ca -vserver cluster1

Please enter Certificate: Press <Enter> when done
```

3. 启用ONTAP以允许客户端通过SSL进行访问、并定义用于API访问的用户ID。

```
security ssl modify -vserver cluster1 -client-enabled true
security login create -user-or-group-name cert_user -application ontapi
-authmethod cert -role admin -vserver cluster1
```

在以下示例中、用户ID `cert_user` 现在已启用、可使用经过证书身份验证的API访问。用于显示ONTAP版本的简单易管理性SDK Python脚本 `cert_user` 如下所示：

```
#!/usr/bin/python

import sys
sys.path.append("/home/admin/netapp-manageability-sdk-9.5/netapp-
manageability-sdk-9.5/lib/python/NetApp")
from NaServer import *

cluster = "cluster1"
transport = "HTTPS"
port = 443
style = "CERTIFICATE"
cert = "test.pem"
key = "test.key"

s = NaServer(cluster, 1, 30)
s.set_transport_type(transport)
s.set_port(port)
s.set_style(style)
s.set_server_cert_verification(0)
s.set_client_cert_and_key(cert, key)

api = NaElement("system-get-version")
output = s.invoke_elem(api)
if (output.results_status() == "failed"):
    r = output.results_reason()
    print("Failed: " + str(r))
    sys.exit(2)

ontap_version = output.child_get_string("version")
print ("V: " + ontap_version)
```

该脚本的输出将显示ONTAP版本。

```
./version.py

V: NetApp Release 9.5RC1: Sat Nov 10 05:13:42 UTC 2018
```

4. 要使用ONTAP REST API执行基于证书的身份验证、请完成以下步骤：
   a. 在ONTAP中、定义http访问的用户ID：

```
security login create -user-or-group-name cert_user -application http
-authmethod cert -role admin -vserver cluster1
```

b. 在Linux客户端上、运行以下命令、以输出形式生成ONTAP版本：

```
curl -k --cert-type PEM --cert ./test.pem --key-type PEM --key
./test.key -X GET "https://cluster1/api/cluster?fields=version"
{
    "version": {
        "full": "NetApp Release 9.7P1: Thu Feb 27 01:25:24 UTC 2020",
        "generation": 9,
        "major": 7,
        "minor": 0
    },
    "_links": {
        "self": {
            "href": "/api/cluster"
        }
    }
}
```

更多信息

- "使用适用于ONTAP的NetApp易管理性SDK进行基于证书的身份验证"(英文)

适用于**REST API**的**ONTAP OAuth2.0**基于令牌的身份验证

作为基于证书的身份验证的替代方法、您可以对REST API使用基于OAuth2.0令牌的身份验证。

从ONTAP 9.14.1开始、您可以选择使用开放授权(OAuth2.0)框架控制对ONTAP集群的访问。您可以使用任何ONTAP管理界面配置此功能、包括ONTAP命令行界面、System Manager和REST API。但是、只有当客户端使用REST API访问ONTAP时、才能应用OAuth2.0授权和访问控制决策。

OAuth2.0令牌取代了用户帐户身份验证的密码。

有关使用OAuth2.0的详细信息，请参见 "有关使用OAuth2.0进行身份验证和授权的ONTAP文档"。

登录和密码参数

有效的安全防护符合既定的组织策略、准则以及适用于组织的任何监管或标准。这些要求的示例包括用户名生命周期、密码长度要求、字符要求以及此类帐户的存储。ONTAP解决方案提供了一些特性和功能来解决这些安全结构问题。

新的本地帐户功能

要支持组织的用户帐户策略、准则或标准(包括监管)、ONTAP支持以下功能：

- 配置密码策略以强制实施最少数字、小写字符或大写字符数
- 登录尝试失败后需要延迟
- 定义帐户非活动限制
- 使用户帐户过期
- 显示密码到期警告消息
- 登录无效通知

可配置的设置可使用security login Role config修改命令进行管理。

SHA-512支持

为了增强密码安全性、ONTAP 9支持SHA-2密码哈希函数、并默认使用SHA-512对新创建或更改的密码进行哈希。操作员和管理员还可以根据需要使帐户过期或锁定帐户。

升级到ONTAP 9.0或更高版本后、未更改密码的原有ONTAP 9用户帐户仍可使用MD5哈希函数。但是、NetApp强烈建议用户更改密码、将这些用户帐户迁移到更安全的SHA-512解决方案。

通过密码哈希功能、您可以执行以下任务：

- 显示与指定哈希函数匹配的用户帐户：

```
cluster1::*> security login show -user-or-group-name NewAdmin -fields
hash-function
vserver  user-or-group-name application authentication-method hash-
function
-------- ------------------ ----------- ---------------------
-------------
cluster1 NewAdmin           console     password              sha512
cluster1 NewAdmin           ontapi      password              sha512
cluster1 NewAdmin           ssh         password              sha512
```

- 使使用指定哈希函数(例如MD5)的帐户过期、从而强制用户在下次登录时更改密码：

```
cluster1::*> security login expire-password -vserver * -username * -hash
-function md5
```

- 使用使用指定哈希函数的密码锁定帐户。

```
cluster1::*> security login lock -vserver * -username * -hash-function
md5
```

集群管理SVM中的内部用户无法识别密码哈希函数 `autosupport` 。此问题无关紧要。哈希函数未知、因为默认情况下、此内部用户未配置密码。

- 要查看用户的密码哈希函数 `autosupport` 、请运行以下命令：

```
::> set advanced
::> security login show -user-or-group-name autosupport -instance

                      Vserver: cluster1
      User Name or Group Name: autosupport
                  Application: console
        Authentication Method: password
     Remote Switch IP Address: -
                    Role Name: autosupport
                Account Locked: no
                  Comment Text: -
      Whether Ns-switch Group: no
       Password Hash Function: unknown
Second Authentication Method2: none
```

- 要设置密码哈希函数(默认值：SHA512)、请运行以下命令：

```
::> security login password -username autosupport
```

密码设置为什么无关紧要。

```
security login show -user-or-group-name autosupport -instance

                      Vserver: cluster1
      User Name or Group Name: autosupport
                  Application: console
        Authentication Method: password
     Remote Switch IP Address: -
                    Role Name: autosupport
                Account Locked: no
                  Comment Text: -
      Whether Ns-switch Group: no
       Password Hash Function: sha512
Second Authentication Method2: none
```

密码参数

ONTAP 解决方案提供满足并支持企业策略要求和准则的密码参数。

属性	Description	Default	范围
username-minlength	最短用户名长度限制	3.	3-16
username-alphanum	用户名字母数字	已禁用	启用/禁用
passwd-minlength	最短密码长度限制	8.	3-64
passwd-alphanum	密码字母数字	enabled	启用/禁用
passwd-min-special-chars	密码中的最少特殊字符数限制	0	0-64
passwd-expiry-time	密码到期时间（天）	无限制，表示密码永不过期	0-unlimited 0 == 立即过期
require-initial-passwd-update	需要在首次登录时更新初始密码	已禁用	启用/禁用 允许通过控制台或SSH进行更改
max-failed-login-attempts	尝试失败的最大次数	0，不锁定帐户	-
lockout-duration	最大锁定期限（天）	默认值为 0，表示帐户锁定一天	-
disallowed-reuse	禁止使用最后N个密码	6.	最小为 6
change-delay	密码更改之间的延迟（天）	0	-
delay-after-failed-login	每次登录尝试失败后的延迟（秒）	4.	-
passwd-min-lowercase-chars	密码中的最少小写字母字符数限制	0，表示不需要小写字母字符	0-64
passwd-min-uppercase-chars	最少大写字母字符数限制	0，表示不需要大写字母字符	0-64
passwd-min-digits	密码中的最小数字字符数限制	0，表示不需要数字字符	0-64
passwd-expiry-warn-time	在帐户到期之前显示警告消息（天）	无限制，表示从不发出密码过期警告	0，表示每次成功登录时均提醒用户密码即将过期
account-expiry-time	帐户将在N天后过期	无限制，表示帐户永不过期	帐户到期时间必须大于帐户非活动限制
account-inactive-limit	帐户过期之前处于非活动状态的最大持续时间（天）	无限制，表示非活动帐户永不过期	帐户非活动限制必须小于帐户到期时间

示例

```
cluster1::*> security login role config show -vserver cluster1 -role admin

                                          Vserver: cluster1
                                        Role Name: admin
                  Minimum Username Length Required: 3
                            Username Alpha-Numeric: disabled
                  Minimum Password Length Required: 8
                            Password Alpha-Numeric: enabled
Minimum Number of Special Characters Required in the Password: 0
                       Password Expires In (Days): unlimited
   Require Initial Password Update on First Login: disabled
                Maximum Number of Failed Attempts: 0
                    Maximum Lockout Period (Days): 0
                      Disallow Last 'N' Passwords: 6
            Delay Between Password Changes (Days): 0
     Delay after Each Failed Login Attempt (Secs): 4
Minimum Number of Lowercase Alphabetic Characters Required in the
Password: 0
Minimum Number of Uppercase Alphabetic Characters Required in the
Password: 0
Minimum Number of Digits Required in the Password: 0
Display Warning Message Days Prior to Password Expiry (Days): unlimited
                        Account Expires in (Days): unlimited
Maximum Duration of Inactivity before Account Expiration (Days): unlimited
```

从9.14.1开始、密码的复杂性和锁定规则将增加。这仅适用于全新安装的ONTAP。

系统管理方法

这些参数是加强ONTAP系统管理的重要参数。

命令行访问

建立对系统的安全访问是维护安全解决方案的关键部分。最常见的命令行访问选项包括SSH、Telnet和RSH。其中、SSH是远程命令行访问最安全的行业标准最佳实践。NetApp强烈建议使用SSH通过命令行访问ONTAP解决方案。

SSH配置

命令可 `security ssh show` 显示集群和SVM的SSH密钥交换算法、密码和MAC算法配置。密钥交换方法使用这些算法和密码来指定如何为加密和身份验证生成一次性会话密钥以及如何进行服务器身份验证。

```
cluster1::> security ssh show

Vserver       Ciphers       Key Exchange Algorithms     MAC Algorithms
--------  ----------------  --------------------------  --------------
nsadhanacluster-2
                aes256-ctr,   diffie-helman-group-      hmac-sha2-256
                aes192-ctr,    exchange-sha256,         hmac-sha2-512
                aes128-ctr    ecdh-sha2-nistp384
vs0             aes128-gcm    curve25519-sha256         hmac-sha1
vs1             aes256-ctr,   diffie-hellman-group-     hmac-sha1-96
                aes192-ctr,   exchange-sha256           hmac-sha2-256
                aes128-ctr,   ecdh-sha2-nistp384        hmac-sha2-256-
                3des-cbc,     ecdh-sha2-nistp512        etm
                aes128-gcm                              hmac-sha2-512
3 entries were displayed.
```

登录横幅

通过登录横幅、组织可以向任何操作员、管理员甚至入侵者提供可接受使用的条款和条件、并指明允许谁访问系统。这种方法有助于建立对系统访问和使用的预期。命令用于 `security login banner modify` 修改登录横幅。在SSH和控制台设备登录过程中、登录横幅显示在身份验证步骤的前面。横幅文本必须使用双引号(“”)，如以下示例所示。

```
cluster1::> security login banner modify -vserver cluster1 -message
“Authorized users ONLY!”
```

登录横幅参数

参数	**Description**
`vserver`	使用此参数指定带有已修改横幅的SVM。使用集群管理SVM的名称修改集群级别的消息。集群级别的消息用作未定义消息的数据SVM的默认消息。
`message`	此可选参数可用于指定登录横幅消息。如果集群设置了登录横幅消息、则所有数据SVM也会使用集群登录横幅。设置数据SVM的登录横幅将覆盖集群登录横幅的显示。要将数据SVM登录横幅重置为使用集群登录横幅、请将此参数与值"-"结合使用。 如果使用此参数、则登录横幅不能包含换行符(也称为行尾[EOLS]或换行符)。要输入包含换行符的登录横幅消息、请勿指定任何参数。系统将提示您以交互方式输入消息。以交互方式输入的消息可以包含换行符。 非ASCII字符必须使用Unicode UTF-8。
`uri`	`(ftp

参数	Description
http):///(hostname	IPv4` 使用此参数指定从中下载登录横幅的URI。 消息长度不得超过2048字节。非ASCII字符必须以Unicode UTF-8格式提供。

每日消息

`security login motd modify`命令用于更新每日消息(Message of the Day、MOTD)。

MOTD分为两类：集群级别的MOTD和数据SVM级别的MOTD。登录到数据SVM的集群Shell的用户可能会看到两条消息：集群级别的MOTD、后跟该SVM的SVM级别的MOTD。

如果需要、集群管理员可以在每个SVM上单独启用或禁用集群级别的MOTD。如果集群管理员为SVM禁用了集群级别的MOTD、则登录到此SVM的用户不会看到集群级别的消息。只有集群管理员才能启用或禁用集群级别的消息。

MOTD参数	Description
Vserver	使用此参数指定要修改其MOTD的SVM。使用集群管理SVM的名称修改集群级别的消息。

MOTD参数	Description
message	此可选参数可用于指定消息。如果使用此参数、则MOTD不能包含换行符。如果未指定除参数以外的任何参数 `-vserver` 、系统将提示您以交互方式输入消息。以交互方式输入的消息可以包含换行符。非ASCII字符必须以Unicode UTF-8格式提供。消息可以包含使用以下转义序列动态生成的内容： • `\\` -单个反冲字符 • `\b` -无输出(仅支持与Linux兼容) • `\C` -集群名称 • `\d` -在登录节点上设置的当前日期 • `\t` -在登录节点上设置的当前时间 • `\I` -传入LIF IP地址(输出控制台以进行 `console` 登录) • `\l` -登录设备名称(打印登录控制台 `console`) • `\L` -用户在集群中任何节点上的上次登录 • `\m` -机器架构 • `\n` -节点或数据SVM名称 • `\N` -登录用户的名称 • `\o` -与\O相同用于实现Linux兼容性。 • `\O` -节点的DNS域名。请注意、输出取决于网络配置、可能为空。 • `\r` -软件版本号 • `\s` -操作系统名称 • `\u` 本地节点上活动的集群Shell会话数。对于集群管理员：所有clustershell用户。对于数据SVM管理员：仅限该数据SVM的活动会话。 • `\U` -与相同 `\u`，但已 `user` 附加或 `users` 附加 • `\v` -有效的集群版本字符串 • `\W` -登录用户在集群中的活动会话 (`who`)

有关在ONTAP中配置每日消息的详细信息，请参见 "有关每日消息的ONTAP文档"。

命令行界面会话超时

默认命令行界面会话超时为30分钟。超时对于防止陈旧会话和会话备份非常重要。

使用 `system timeout show` 命令查看当前命令行界面会话超时。要设置超时值、请使用 `system timeout modify -timeout <minutes>` 命令。

使用NetApp ONTAP系统管理器进行Web访问

如果ONTAP管理员更喜欢使用图形界面而不是命令行界面来访问和管理集群、请使用NetApp ONTAP系统管理

器。它作为Web服务随ONTAP附带、默认情况下处于启用状态、并可通过浏览器进行访问。如果使用的是DNS或IPv4或IPv6地址，请通过将浏览器指向主机名 `https://cluster-management-LIF`。

如果集群使用自签名数字证书，浏览器可能会显示一条警告，指示此证书不可信。您可以确认风险以继续访问、也可以在集群上安装证书颁发机构(CA)签名的数字证书以进行服务器身份验证。

从ONTAP 9.3开始、ONTAP系统管理器可以选择使用安全断言标记语言(SAML)身份验证。

ONTAP系统管理器的**SAML**身份验证

SAML 2.0是一种广泛采用的行业标准、它允许任何符合SAML的第三方身份提供程序(Identity Provider、Idp)使用企业所选Idp独有的机制执行MFA、并将其作为单点登录(Single Sign On、SSO)的源。

SAML规范中定义了三个角色：主体、Idp和服务提供商。在ONTAP实施中、主体是通过ONTAP系统管理器或NetApp Active IQ Unified Manager访问ONTAP的集群管理员。Idp是第三方Idp软件。从ONTAP 9.3开始、支持Microsoft Active Directory联合服务(ADFS)和开源Shbboleth Idp。从ONTAP 9.12.1开始、Cisco双核是受支持的Idp。服务提供商是内置在ONTAP中的SAML功能、可供ONTAP系统管理器或Active IQ Unified Manager Web应用程序使用。

与SSH双因素配置过程不同、在激活SAML身份验证后、ONTAP系统管理器或ONTAP服务处理器访问要求所有现有管理员通过SAML Idp进行身份验证。不需要更改集群用户帐户。启用SAML身份验证后、将向具有和应用程序管理员角色的现有用户添加新的身份验证方法 `saml http ontapi` 。

启用SAML身份验证后、应在ONTAP中使用管理员角色以及和应用程序的SAML身份验证方法定义需要SAML Idp访问的其他新帐户 `http ontapi` 。如果在某个时刻禁用了SAML身份验证、则这些新帐户需要 `password` 使用和应用程序的管理员角色定义身份验证方法 `http ontapi` 、并将用于本地ONTAP身份验证的控制台应用程序添加到ONTAP系统管理器中。

启用SAML IdP后、IdP将使用IdP可用的方法(例如轻型目录访问协议(Lightweight-Directory Access Protocol、LDAP)、Active Directory (AD)、Kerberos、密码等)执行ONTAP System Manager访问身份验证。可用方法对于Idp是唯一的。请务必确保在ONTAP中配置的帐户具有映射到Idp身份验证方法的用户ID。

已通过NetApp验证的IdPs包括Microsoft ADFS、Cisco Duo和开源Shbboleth IdP.

从ONTAP 9.14.1开始、Cisco Duo可用作SSH的第二个身份验证因素。

有关适用于ONTAP系统管理器、Active IQ Unified Manager和SSH的MFA的详细信息，请参见 "TR-4647：《ONTAP 9中的多因素身份验证》"。

ONTAP System Manager洞察力

从ONTAP 9.11.1开始、ONTAP系统管理器可提供深入见解、帮助集群管理员简化日常任务。这些安全洞察基于本技术报告中的建议。

Security Insight	决心
已启用Telnet	NetApp 建议使用安全 Shell （ SSH ）进行安全远程访问。
已启用远程Shell (RSH)	NetApp建议使用SSH进行安全远程访问。
AutoSupport正在使用不安全协议	AutoSupport未配置为通过链路：HTTPS发送。
集群级别未配置登录横幅	如果未为集群配置登录横幅、则显示警告。
SSH 正在使用不安全密码	如果SSH使用不安全的用户身份验证、则显示警告。

Security Insight	决心
配置的NTP服务器太少	如果配置的NTP服务器数量小于3、则显示警告。
默认管理员用户未锁定	如果不使用任何默认管理帐户(admin或diag)登录到System Manager、并且这些帐户未锁定、则建议将其锁定。
勒索软件防护—卷没有Snapshot策略	一个或多个卷未附加足够的Snapshot策略。
勒索软件防护—禁用Snapshot自动删除	已为一个或多个卷设置Snapshot自动删除。
不会监控卷的勒索软件攻击	多个卷支持自主勒索软件保护、但尚未进行配置。
没有为SVM配置自主勒索软件保护	多个SVM支持自主勒索软件保护、但尚未配置。
未配置本机FPolicy	未为NAS SVM设置FPolicy。
启用自主勒索软件保护活动模式	多个卷已完成其学习模式、您可以打开活动模式
已禁用全局FIPS 140-2合规性	未启用全局FIPS 140-2合规性。
没有为集群配置通知	电子邮件、webhook或SNMP陷阱主机未配置为接收通知。

有关ONTAP System Manager洞察的详细信息，请参见 "ONTAP System Manager洞察力文档"。

ONTAP自主勒索软件保护

为了对存储工作负载安全性的用户行为分析进行补充、ONTAP自主勒索软件保护功能可分析卷工作负载和熵、以检测勒索软件并创建Snapshot、并在怀疑发生攻击时通知管理员。

除了通过NetApp Cloud Insights / Cloud Secure和NetApp FPolicy合作伙伴生态系统使用外部FPolicy用户行为分析(UBA)进行勒索软件检测和预防之外、ONTAP 9.10.1还引入了自主勒索软件保护。ONTAP自主勒索软件保护功能使用内置的机载机器学习(ML)功能、可查看卷工作负载活动和数据熵、从而自动检测勒索软件。它可以监控与UBA不同的活动、以便检测UBA不会检测到的攻击。

有关此功能的更多详细信息，请参见 "TR-4572：《NetApp解欲软件》" 或 "ONTAP自主勒索软件保护文档"。

存储管理系统审核

通过将ONTAP事件卸载到远程系统日志服务器来确保事件审核的完整性。此服务器可以是Splunk等安全信息事件管理系统。

发送系统日志

从支持和可用性角度来看、日志和审核信息对于企业来说非常重要。此外、日志(系统日志)以及审核报告和输出中包含的信息和详细信息通常具有敏感性。为了保持安全控制和防护、企业必须以安全的方式管理日志和审核数据。

要将违规范围或占用空间限制为单个系统或解决方案 、必须卸载系统日志信息。因此、NetApp建议将系统日志信息安全地卸载到安全的存储或保留位置。

创建日志转发目标位置

使用 `cluster log-forwarding create` 命令为远程日志记录创建日志转发目标。

Parameters

使用以下参数配置 `cluster log-forwarding create` 命令：

- *目标主机。*此名称是要将日志转发到的服务器的主机名或IPv4或IPv6地址。

```
-destination <Remote InetAddress>
```

- *目标端口。*这是目标服务器侦听的端口。

```
[-port <integer>]
```

- *日志转发协议。*此协议用于向目标发送消息。

```
[-protocol \{udp-unencrypted|tcp-unencrypted|tcp-encrypted}]
```

  日志转发协议可以使用以下值之一：

  - `udp-unencrypted`(英文)无安全保障的用户数据报协议。
  - `tcp-unencrypted`(英文)无安全性的TCP。
  - `tcp-encrypted`(英文)采用传输层安全(Transport Layer Security、TLS)的TCP。

- *验证目标服务器标识。*如果此参数设置为true、则会通过验证日志转发目标的证书来验证其身份。仅当在协议字段中选择了值时、该值才能设置为true `tcpencrypted` 。

```
[-verify-server \{true|false}]
```

- *系统日志工具。*此值是用于转发日志的系统日志工具。

```
[-facility <Syslog Facility>]
```

- *跳过连接测试。*通常、该 `cluster log-forwarding create` 命令会通过发送Internet控制消息协议(Internet Control Message Protocol、ICMP) ping检查目标是否可访问、如果无法访问、则该命令将失败。将此值设置为 `true` 可绕过ping检查、以便在无法访问目标时配置目标。

```
[-force [true]]
```

NetApp建议使用 `cluster log-forwarding` 命令强制连接到 `-tcp-encrypted` 类型。

事件通知

保护离开系统的信息和数据对于维护和管理系统的安全防护至关重要。ONTAP解决方案生成的事件提供了大量有关解决方案遇到的情况、处理的信息等信息。这些数据的活力凸显了以安全方式管理和迁移数据的必要性。

`event notification create`命令会将事件筛选器定义的一组事件的新通知发送到一个或多个通知目标。以下示例显示了事件通知配置和 `event notification show`命令、其中显示了已配置的事件通知筛选器和目标。

```
cluster1::> event notification create -filter-name filter1 -destinations
 email_dest,syslog_dest,snmp-traphost

cluster1::> event notification show
ID     Filter Name       Destinations
-----  ----------------  -----------------
1 filter1 email_dest, syslog_dest, snmp-traphost
```

存储加密

要在磁盘被盗、退回或重新利用时保护敏感数据、请使用基于硬件的NetApp存储加密或基于软件的NetApp卷加密/NetApp聚合加密。这两种机制均经过FIPS-140-2验证、如果将基于硬件的机制与基于软件的机制结合使用、该解决方案符合分类商业解决方案(CSFC)计划的要求。它可以为硬件层和软件层的机密和顶级机密空闲数据提供增强的安全保护。

空闲数据加密对于在磁盘被盗、退回或重新利用时保护敏感数据非常重要。

ONTAP 9具有三个符合联邦信息处理标准(Federal Information Processing Standard、FIPS) 140-2的空闲数据加密解决方案：

- NetApp存储加密(NSE)是一种使用自加密驱动器的硬件解决方案。
- NetApp 卷加密 (NVE) 是一种软件解决方案，支持对任何驱动器类型上的任何数据卷进行加密，在这种情况下，每个卷都有一个唯一密钥。
- NetApp 聚合加密 (NAE) 是一种软件解决方案，支持对任何驱动器类型上的任何数据卷进行加密，在这种情况下，每个聚合都有唯一密钥。

NSE、NVE和NAE可以使用外部密钥管理或板载密钥管理器(OKM)。NSE、NVE 和 NAE 的使用不影响 ONTAP 的存储效率功能。但是，NVE 卷将从聚合重复数据删除中排除。NAE 卷参与聚合重复数据消除并从中受益。

借助 NSE、NVE 或 NAE，OKM 为空闲数据提供了独立的加密解决方案。

NVE、NAE和OKM使用ONTAP加密模块。CryptoMod列在CMVP FIPS 140-2验证模块列表中。请参阅。 "FIPS 140-2证书编号4144"

要开始OKM配置、请使用 `security key-manager onboard enable` 命令。要配置外部密钥管理互操作性协议(Key Management互操作性协议、KMIP)密钥管理器、请使用 `security key-manager external`

enable 命令。从ONTAP 9.6开始、外部密钥管理器支持多租户。使用 -vserver <vserver name> 参数为特定SVM启用外部密钥管理。在9.6之前的版本中、此 security key-manager setup 命令用于配置OKM和外部密钥管理器。对于板载密钥管理、此配置将引导操作员或管理员完成用于配置OKM的密码短语设置和其他参数。

以下示例提供了部分配置：

```
cluster1::> security key-manager setup
Welcome to the key manager setup wizard, which will lead you through
the steps to add boot information.

Enter the following commands at any time
"help" or "?" if you want to have a question clarified,
"back" if you want to change your answers to previous questions, and
"exit" if you want to quit the key manager setup wizard. Any changes
you made before typing "exit" will be applied.

Restart the key manager setup wizard with "security key-manager setup". To
accept a default
or omit a question, do not enter a value.

Would you like to configure onboard key management? {yes, no} [yes]:
Enter the cluster-wide passphrase for onboard key management. To continue
the configuration, enter the passphrase, otherwise
type "exit":
Re-enter the cluster-wide passphrase:
After configuring onboard key management, save the encrypted configuration
data
in a safe location so that you can use it if you need to perform a manual
recovery
operation. To view the data, use the “security key-manager backup show”
command.
```

从ONTAP 9.4开始、您可以将true选项与结合使用 -enable-cc-mode security key-manager setup 、以要求用户在重新启动后输入密码短语。对于ONTAP 9.6及更高版本，命令语法为 security key-manager onboard enable -cc-mode-enabled yes。

从ONTAP 9.4开始、您可以使用具有高级权限的 secure-purge 功能无故障"擦除"启用了NVE的卷上的数据。擦洗加密卷上的数据可确保无法从物理介质中恢复数据。以下命令可安全清除SVM VS1上vol1上已删除的文件：

```
cluster1::> volume encryption secure-purge start -vserver vs1 -volume vol1
```

从ONTAP 9.7开始、如果已安装VE许可证、已配置OKM或外部密钥管理器、但未使用NSE、则默认情况下会启用NAE和NVE。默认情况下、会在NAE聚合上创建NAE卷、而在非NAE聚合上会默认创建NVE卷。您可以输入以下命令来覆盖此设置：

```
cluster1::*> options -option-name
encryption.data_at_rest_encryption.disable_by_default true
```

从ONTAP 9.6开始、您可以使用SVM范围为集群中的数据SVM配置外部密钥管理。如果多租户环境中的每个租户都使用一个或一组不同的SVM来提供数据、则此方法最适合此环境。只有给定租户的 SVM 管理员才能访问该租户的密钥。有关详细信息、请参见 "在ONTAP 9.6及更高版本中启用外部密钥管理" ONTAP文档中的。

从ONTAP 9.11.1开始、您可以通过在SVM上指定主密钥服务器和二级密钥服务器来配置与集群模式外部密钥管理服务器的连接。有关详细信息、请参见 "配置集群模式外部密钥服务器" ONTAP文档中的。

从ONTAP 9.131开始、您可以在System Manager中配置外部密钥管理器服务器。有关详细信息、请参见 "管理外部密钥管理器" ONTAP文档中的。

数据复制加密

为了补充空闲数据加密功能、您可以使用TLS 1.2和SnapMirror、SnapVault或FlexCache的预共享密钥对集群之间的ONTAP数据复制流量进行加密。

在为灾难恢复、缓存或备份复制数据时、您必须在通过线缆从一个ONTAP 集群传输到另一个集群期间保护这些数据。这样可以防止在敏感数据传输过程中对其进行恶意中间人攻击。

从ONTAP 9.6开始、集群对等加密可为SnapMirror、SnapVault和FlexCache等ONTAP数据复制功能提供TLS 1.2 AES-256 GCM加密支持。加密可通过两个集群对等方之间的预共享密钥（ PSk ）进行设置。

如果客户使用NSE、NVE和NAE等技术来保护空闲数据、则还可以升级到ONTAP 9.6或更高版本以使用集群对等加密来使用端到端数据加密。

集群对等会对集群对等之间的所有数据进行加密。例如、在使用SnapMirror时、源集群对等方与目标集群对等方之间的所有对等信息以及所有SnapMirror关系都会进行加密。您不能在启用了集群对等加密的集群对等之间发送明文数据。

从ONTAP 9.6开始、新的集群对等关系会默认启用加密。要对ONTAP 9.6之前创建的集群对等关系启用加密、必须将源集群和目标集群升级到9.6。此外、您必须使用 `cluster peer modify` 命令将源集群对等方和目标集群对等方更改为使用集群对等加密。

您可以转换现有对等关系、以便在ONTAP 9.6中使用集群对等加密、如以下示例所示：

```
On the Destination Cluster Peer

cluster2::> cluster peer modify cluster1 -auth-status-admin use-
authentication -encryption-protocol-proposed tls-psk

When prompted enter a passphrase.

On the Source Cluster Peer

cluster1::> cluster peer modify cluster2 -auth-status-admin use-
authentication -encryption-protocol-proposed tls-psk

When prompted enter the same passphrase you created in the previous step.
```

IPsec传输中数据加密

现在、如果客户对数据复制流量使用NetApp存储加密(NSE)或NetApp卷加密(NVE)和集群对等加密(CPE)等空闲数据加密技术、则可以升级到ONTAP 9.8或更高版本并使用、从而在混合多云Data Fabric中的客户端和存储之间使用端到端加密 IPsec。IPsec提供了NFS或SMB/CCIFS加密的替代方案、并且是iSCSI流量唯一的加密传输中选项。

在某些情况下、可能需要保护通过缆线(或传输中)传输到ONTAP SVM的所有客户端数据。这样可以防止对传输中的敏感数据进行重放和恶意中间人攻击。

从ONTAP 9.8开始、互联网协议安全性(Internet Protocol Security、IPsec)为客户端和ONTAP SVM之间的所有IP流量提供端到端加密支持。所有 IP 流量的 IPsec 数据加密包括 NFS ， iSCSI 和 SMB/CIFS 协议。IPsec 为 iSCSI 流量提供了唯一的传输加密选项。

通过缆线提供NFS加密是IPsec的主要用例之一。在ONTAP 9.8之前的版本中、NFS线上加密需要设置和配置Kerberos、才能利用krb5p对传输中的NFS数据进行加密。在每个客户环境中、这并不总是简单或容易实现的。

现在、如果客户对数据复制流量使用NetApp存储加密(NSE)或NetApp卷加密(NVE)和集群对等加密(CPE)等空闲数据加密技术、则可以升级到ONTAP 9.8或更高版本并使用、从而在混合多云Data Fabric中的客户端和存储之间使用端到端加密 IPsec。

IPsec是IETF标准。ONTAP在传输模式下使用IPsec。它还利用Internet密钥交换(Internet Key Exchange、IKE)协议版本2、该协议使用预共享密钥(PSK)在客户端与使用IPv4或IPv6的ONTAP之间协商密钥材料。默认情况下，IPsec使用Suite-B AES-GCM 256位加密。此外、还支持采用256位加密的Suite B AES-GMAC256和AES-CBC256。

尽管必须在集群上启用IPsec功能、但它通过使用安全策略数据库(SPD)条目应用于单个SVM IP地址。策略(SPD)条目包含客户端IP地址(远程IP子网)、SVM IP地址(本地IP子网)、要使用的加密密码套件以及通过IKEv2进行身份验证并建立IPsec连接所需的预共享密钥(PSK)。除了IPsec策略条目之外，还必须为客户端配置相同的信息(本地和远程IP、PSK和密码套件)，然后流量才能通过IPsec连接进行传输。从ONTAP 9.10.1开始，增加了对IPsec证书身份验证的支持。这将删除IPsec策略限制并启用Windows操作系统对IPsec的支持。

如果客户端和SVM IP地址之间存在防火墙、则必须允许ESP和UDP (端口500和4500)协议(入站(入站)和出站(出

站))、以便成功进行I可 得2协商、从而允许IPsec流量。

对于 NetApp SnapMirror 和集群对等流量加密，仍然建议使用基于 IPsec 的集群对等加密（ Cluster peering encryption ， CPE ），以便通过线缆安全地进行传输。CPE对这些工作负载的性能优于IPsec。您不需要IPsec许可证，并且没有导入或导出限制。

您可以在集群上启用IPsec、并为单个客户端和单个SVM IP地址创建SPD条目、如以下示例所示：

```
On the Destination Cluster Peer

cluster1::> security ipsec config modify -is-enabled true

cluster1::> security ipsec policy create -vserver vs1 -name test34 -local
-ip-subnets 192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32

When prompted enter and confirm the pre shared secret (PSK).
```

TLS和SSL管理

您可以通过在ONTAP命令中将参数设置为true来为控制平台接口启用FIPS 140-2合规性模式 `is-fips-enabled` `security config modify` 。

从 ONTAP 9 开始，您可以为集群范围的控制面板接口启用 FIPS 140-2 合规模式。默认情况下，仅 FIPS 140-2 模式处于禁用状态。您可以通过将命令的参数设置为来启用FIPS 140-2合规性模式 `is-fips-enabled` `true` `security config modify` 。然后、您可以使用 `security config show command` 确认联机状态。

启用FIPS 140-2合规性后、TLSv1和SSLv3将被禁用、只有TLSv1.1和TLSv1.2保持启用状态。启用FIPS 140-2合规性后、ONTAP 会阻止您启用TLSv1和SSLv3。如果在启用FIPS 140-2后又将其禁用、TLSv1和SSLv3将保持禁用状态、但TLSv1.2将保持启用状态、或者TLSv1.1和TLSv1.2同时保持启用状态、具体取决于先前的配置。

命令用于 `security config modify` 修改现有集群范围的安全配置。如果启用 FIPS 合规模式，集群会自动仅选择 TLS 协议。使用 `-supported-protocols` 参数可独立于FIPS模式包含或排除TLS协议。默认情况下，FIPS 模式处于禁用状态，ONTAP 支持 TLSv1.2、TLSv1.1 和 TLSv1 协议。

为了实现向后兼容性、ONTAP支持在FIPS模式处于禁用状态时将SSLv3添加到列表中 `supported-protocols` 。使用 `-supported-cipher-suites` 参数仅配置高级加密标准(Advanced Encryption Standard、AES)或AES和3DES。您也可以通过指定!RC4来禁用RC4等弱加密。默认情况下，支持的密码设置为 `ALL:!LOW:!aNULL:!EXP:!eNULL`。此设置表示已启用协议支持的所有密码套件、但不具有身份验证、不加密、不导出和低加密密码套件的密码套件除外。这些套件使用64位或56位加密算法。

选择可与相应选定协议一起使用的密码套件。配置无效可能会导致某些功能无法正常运行。

有关正确的密码字符串语法、请参见OpenSSL上的 "ciphers" 页面(由OpenSSL软件基金会发布)。从ONTAP 9.9.1及更高版本开始、您无需在修改安全配置后手动重新启动所有节点。

启用FIPS 140-2合规性会影响ONTAP 9内部和外部的其他系统和通信。NetApp强烈建议在具有控制台访问权限的非生产系统上测试这些设置。

如果使用SSH管理ONTAP 9、则必须使用OpenSSH 5.7或更高版本的客户端。SSH客户端必须使用椭圆曲线数字签名算法(ECDSA)公共密钥算法协商、才能成功建立连接。

通过仅启用TLS 1.2并使用支持完全正向保密(PFS)的密码套件、可以进一步加强TLS安全性。PFS是一种密钥交换方法、与TLS 1.2等加密协议结合使用时、有助于防止攻击者解密客户端和服务器之间的所有网络会话。要仅启用TLS 1.2和支持PFS的加密套件、请在高级权限级别使用命令、 `security config modify` 如以下示例所示。

在更改SSL接口配置之前、请务必记住、在连接到ONTAP时、客户端必须支持所述的密码(DHE、ECDHE)。否则、不允许连接。

```
cluster1::*> security config modify -interface SSL -supported-protocols
TLSv1.2 -supported-cipher-suites
PSK:DHE:ECDHE:!LOW:!aNULL:!EXP:!eNULL:!3DES:!kDH:!kECDH
```

确认 `y` 每个提示。有关PFS的详细信息，请参见 "此NetApp博客"。

从ONTAP 9.11.1和TLS 1.3支持开始、您可以验证FIPS 140-2。

FIPS配置适用于ONTAP和平台BMC。

创建CA签名的数字证书

对于许多组织而言、用于ONTAP Web访问的自签名数字证书不符合其InfoSec策略。在生产系统上、NetApp最佳做法是安装CA签名的数字证书、以便将集群或SVM作为SSL服务器进行身份验证。

您可以使用 `security certificate generate-csr` 命令生成证书签名请求(CSR)、并使用 `security certificate install` 命令安装从CA收到回的证书。

步骤

1. 要创建由组织的CA签名的数字证书、请执行以下操作：
   a. 生成CSR。
   b. 按照组织的过程从组织的CA使用CSR请求数字证书。例如、使用Microsoft Active Directory证书服务Web界面、转到 `<CA_server_name>/certsrv` 并请求证书。
   c. 在ONTAP中安装数字证书。

联机证书状态协议

启用联机证书状态协议(Online Certificate Status Protocol、OCSP)后、使用TLS通信(例如LDAP或TLS)的ONTAP应用程序可以接收数字证书状态。应用程序将收到签名响应、表示请求的证书正常、已撤销或未知。

OCSP无需证书吊销列表(Certificate Revocation List、CRL)即可确定数字证书的当前状态。

默认情况下， OCSP 证书状态检查处于禁用状态。可以使用命令打开 `security config ocsp enable -app name`应用程序，其中应用程序名可以是 `autosupport、、 audit_log、 fabricpool、 ems、 kmip ldap_ad `ldap_nis_namemap`或全部。此命令需要高级权限级别。

SSHv2管理

`security ssh modify`命令会将集群或SVM的SSH密钥交换算法、密码或MAC算法的现有配置替换为您指定的配置设置。

NetApp建议执行以下操作：

- 对用户会话使用密码。
- 使用公共密钥访问计算机。

支持的密码和密钥交换

密码	密钥交换
aes256-ctr	迪夫-赫尔曼-组-交换- SHA256 (SHA-2)
aes192-ctr	迪比-赫尔曼-组-交换- SHA1 (SH-1)
aes128-ctr	迪比-赫尔曼-组14-SHA1 (SHA-1)
aes256-cbc	迪夫-赫尔曼-组1-SHA1 (SH-1)
aes192-cbc	-
aes128-cbc	-
ES128-GCM	-
ES256-GCM	-
3des-cbc	-

支持AES和3DES对称加密

ONTAP还支持以下类型的AES和3DES对称加密(也称为密码)：

- HMAC-SHA1
- hmac-sha1-96
- HMAC-MD5
- hmac-md5-96
- HMAC-里 布姆德160
- UMAC-64
- UMAC-64
- UMAC-128

- hmac-sha2-256
- hmac-sha2-512
- HMAC-SHA1-ETM
- HMAC-SHA1-96-ETM
- HMAC-SHA2-256-ETM
- HMAC-SHA2-512 ETM
- HMAC-MD5-ETM
- HMAC-MD5-96-ETM
- HMAC-提供160-ETM
- UMAC-64-ETM
- UMAC-128-ETM

SSH管理配置适用于ONTAP和平台BMC。

NetApp AutoSupport

通过ONTAP的AutoSupport功能、您可以主动监控系统的运行状况、并自动向NetApp技术支持、组织的内部支持团队或支持合作伙伴发送消息和详细信息。默认情况下、首次配置存储系统时、系统会启用向NetApp技术支持发送的AutoSupport消息。此外、AutoSupport在启用后24小时开始向NetApp技术支持发送消息。此24小时时间段是可配置的。要利用与组织内部支持团队的通信、必须完成邮件主机配置。

只有集群管理员才能执行AutoSupport管理(配置)。SVM 管理员没有 AutoSupport 访问权限。可以禁用 AutoSupport 功能。但是、NetApp建议启用此功能、因为AutoSupport有助于在存储系统出现问题时加快问题识别和解决速度。默认情况下、即使禁用AutoSupport、系统也会收集AutoSupport信息并将其存储在本地。

有关AutoSupport消息的更多详细信息、包括各种消息中包含的内容以及不同类型的消息的发送位置、请参见文档。 "NetApp Active IQ Digital Advisor"

AutoSupport消息包含敏感数据、包括但不限于以下各项：

- 日志文件
- 有关特定子系统的上下文相关数据
- 配置和状态数据
- 性能数据

对于传输协议， AutoSupport 支持 HTTPS ， HTTP 和 SMTP 。由于 AutoSupport 消息的敏感性， NetApp 强烈建议使用 HTTPS 作为向 NetApp 支持部门发送 AutoSupport 消息的默认传输协议。

此外、您还应利用 `system node autosupport modify` 命令指定AutoSupport数据的目标(例如、NetApp技术支持、组织的内部运营或合作伙伴)。此命令还允许您指定要发送的特定AutoSupport详细信息(例如性能数据、日志文件等)。

要完全禁用AutoSupport、请使用 `system node autosupport modify -state disable` 命令。

网络时间协议

尽管您可以通过ONTAP手动设置集群上的时区、日期和时间、但您必须配置网络时间协议(NTP)服务器、以便至少与三个外部NTP服务器同步集群时间。

如果集群时间不准确，可能会出现问题。尽管您可以通过ONTAP手动设置集群上的时区、日期和时间、但您必须配置网络时间协议(NTP)服务器、以便将集群时间与外部NTP服务器同步。

从 ONTAP 9.5 开始，您可以为 NTP 服务器配置对称身份验证。

使用命令最多可以关联10个外部NTP服务器 `cluster time-service ntp server create` 。为了保证冗余和时间服务质量、应至少将三个外部NTP服务器与集群相关联。

有关在ONTAP中配置NTP的详细信息，请参见 "管理集群时间（仅限集群管理员）"。

NAS文件系统本地帐户(CIFS工作组)

工作组客户端身份验证为ONTAP解决方案提供了与传统域身份验证态势一致的额外一层安全保护。使用 `vserver cifs session show` 命令可显示许多与状态相关的详细信息、包括IP信息、身份验证机制、协议版本和身份验证类型。

从ONTAP 9开始、您可以在工作组中配置CIFS服务器、其中CIFS客户端会使用本地定义的用户和组向该服务器进行身份验证。工作组客户端身份验证为ONTAP解决方案提供了与传统域身份验证态势一致的额外一层安全保护。要配置CIFS服务器、请使用 `vserver cifs create` 命令。创建CIFS服务器后、您可以将其加入CIFS域或工作组。要加入工作组、请使用 `-workgroup` 参数。示例配置如下：

```
cluster1::> vserver cifs create -vserver vs1 -cifs-server CIFSSERVER1
-workgroup Sales
```

工作组模式下的CIFS服务器仅支持Windows NT LAN Manager (NTLM)身份验证、而不支持Kerberos身份验证。

NetApp建议对CIFS工作组使用NTLM身份验证功能、以维护组织的安全防护。要验证CIFS安全防护、NetApp建议使用 `vserver cifs session show` 命令显示与防护相关的大量详细信息、包括IP信息、身份验证机制、协议版本和身份验证类型。

NAS文件系统审核

NAS文件系统在当今的威胁形势下占用的空间越来越大、审核功能对于支持可见性至关重要。

安全性需要验证。ONTAP 9在整个解决方案中提供了更多的审核事件和详细信息。由于NAS文件系统在当今的威胁形势下占用的空间越来越大、因此审核功能对于支持可见性至关重要。由于ONTAP 9改进了审核功能、因此CIFS审核详细信息比以往任何时候都更加丰富。密钥详细信息(包括以下内容)会随创建的事件一起记录：

- 文件、文件夹和共享访问

- 创建、修改或删除的文件
- 文件读取访问成功
- 读取或写入文件的尝试失败
- 文件夹权限更改

创建审核配置

您必须启用CIFS审核才能生成审核事件。使用 `vserver audit create` 命令创建审核配置。默认情况下、审核日志会根据大小使用轮换方法。如果在"旋转参数"字段中指定了基于时间的旋转选项、则可以使用该选项。其他日志审核轮换配置详细信息包括轮换计划、轮换限制、一周的轮换日期和轮换大小。以下文本提供了一个示例配置、其中描述了一个审核配置、该配置使用基于时间的每月轮换、计划在一周中的所有日期的12：30进行轮换。

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log
-rotate-schedule-month all -rotate-schedule-dayofweek all -rotate-schedule
-hour 12 -rotate-schedule-minute 30
```

CIFS审核事件

CIFS审核事件如下：

- 文件共享：在使用相关命令添加、修改或删除CIFS网络共享时生成审核事件 `vserver cifs share` 。
- **Audit policy change**：使用相关命令禁用、启用或修改审核策略时生成审核事件 `vserver audit` 。
- 用户帐户：在创建或删除本地CIFS或UNIX用户、启用、禁用或修改本地用户帐户或重置或更改密码时生成审核事件。此事件使用 `vserver cifs users-and-groups local-group` 命令或相关 `vserver services name-service unix-user` 命令。
- 安全组：使用命令或相关命令创建或删除本地CIFS或UNIX安全组时、生成审核事件 `vserver cifs users-and-groups local-group` `vserver services name-service unix-group` 。
- 授权策略更改：在使用命令授予或撤消CIFS用户或CIFS组的权限时生成审核事件 `vserver cifs users-and-groups privilege` 。

此功能基于系统审核功能、管理员可以通过此功能从数据用户的角度查看系统允许执行的操作。

REST API对NAS审核的影响

ONTAP允许管理员帐户使用REST API访问和操作SMB/CIFS/NFS或NFS文件。虽然REST API只能由ONTAP管理员运行、但REST API命令会绕过系统NAS审核日志。此外、使用REST API时、ONTAP管理员也可以绕过文件权限。但是、系统命令历史记录日志中会捕获管理员对文件使用REST API执行的操作。

创建无访问权限**REST API**角色

您可以通过创建不能通过REST访问ONTAP卷的REST API角色来防止ONTAP管理员使用REST API进行文件访问。要配置此角色、请完成以下步骤。

步骤

1. 创建一个新的REST角色、此角色不能访问存储卷、但可以访问所有其他REST API。

```
cluster1::> security login rest-role create nofiles -vserver cluster1
"/api/storage/volumes" -access none
cluster1::> security login rest-role create nofiles -vserver cluster1
"/api" -access all
```

2. 将管理员帐户分配给您在上一步中创建的新REST API角色。

```
cluster1::> security login modify -user-or-group-name user1 -application
http -authentication-method password -vserver cluster1 -role nofile
```

如果要阻止内置ONTAP集群管理员帐户使用REST API进行文件访问，则需要首先 "创建新的管理员帐户并禁用或删除此内置帐户"。

配置和启用CIFS SMB签名和签章

您可以配置和启用SMB签名、通过确保存储系统和客户端之间的流量不会受到重放攻击或中间人攻击的影响来保护Data Fabric的安全性。SMB签名通过验证SMB消息是否具有有效签名来进行保护。

关于此任务

SMB协议是文件系统和架构的一个常见威胁媒介。为了应对这一载体、ONTAP 9解决方案使用行业标准SMB签名和密封。SMB签名可确保存储系统和客户端之间的流量不会受到重放攻击或中间人攻击的影响、从而保护Data Fabric的安全性。它通过验证SMB消息是否具有有效签名来实现此目的。

虽然出于性能考虑、默认情况下会禁用SMB签名、但NetApp强烈建议启用它。此外、ONTAP解决方案还支持SMB加密、也称为密封。这种方法可以在共享的基础上安全地传输数据。默认情况下， SMB 加密处于禁用状态。但是、NetApp建议您启用SMB加密。

SMB 2.0及更高版本现在支持LDAP签名和签章。签名(防止篡改)和签章(加密)可确保SVM和Active Directory服务器之间的安全通信。SMB 3.0及更高版本现在支持加速AES新指令(Intel AES NI)加密。Intel AES NI改进了AES算法、并在支持的处理器系列中加快了数据加密速度。

步骤

1. 要配置和启用SMB签名，请使用 `vserver cifs security modify` 命令并验证参数是否 `-is-signing-required` 设置为 `true`。请参见以下配置示例：

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock
-skew 3 -kerberos-ticket-age 8 -is-signing-required true
```

2. 要配置和启用SMB密封和加密，请使用 `vserver cifs security modify` 命令并验证参数是否 `-is-smb-encryption-required` 设置为 `true`。请参见以下配置示例：

```
cluster1::> vserver cifs security modify -vserver vs1 -is-smb-encryption
-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-smb-
encryption-required
vserver  is-smb-encryption-required
-------- --------------------------
vs1      true
```

NFS安全

导出规则是导出策略的功能要素。导出规则会将卷的客户端访问请求与您配置的特定参数进行匹配、以确定如何处理客户端访问请求。导出策略必须至少包含一个导出规则，才能访问客户端。如果导出策略包含多个规则，则这些规则将按照它们在导出策略中的显示顺序进行处理。

访问控制是保持安全防护的核心。因此、ONTAP会使用导出策略功能限制NFS卷访问权限、使其只能访问与特定参数匹配的客户端。导出策略包含一个或多个导出规则，用于处理每个客户端访问请求。导出策略与每个卷关联、用于配置客户端对卷的访问。此过程的结果将确定是授予还是拒绝(并显示权限被拒绝的消息)客户端对卷的访问权限。此过程还会确定为卷提供的访问级别。

要使客户端能够访问数据、SVM上必须存在具有导出规则的导出策略。一个SVM可以包含多个导出策略。

规则顺序由规则索引编号决定。如果某个规则与客户端匹配、则会使用该规则的权限、而不会处理其他规则。如果没有匹配的规则，客户端将被拒绝访问。

导出规则通过应用以下条件来确定客户端访问权限：

- 发送请求的客户端使用的文件访问协议(例如、NFSv4或SMB)
- 客户端标识符（例如，主机名或 IP 地址）
- 客户端用于进行身份验证的安全类型(例如、Kerberos v5、NTLM或AUATT_SYS)

如果某个规则指定了多个条件、而客户端与其中一个或多个条件不匹配、则该规则不适用。

示例导出策略包含具有以下参数的导出规则：

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

安全类型决定了客户端接收的访问级别。这三个访问级别分别为只读、读写和超级用户(对于具有用户ID的客户端 `0`)。由于按此顺序评估由安全类型确定的访问级别、因此您必须遵守列出的规则：

导出规则中访问级别参数的规则

使客户端能够获得以下访问级别	这些访问参数必须与客户端的安全类型匹配
普通用户只读	只读 (`-rorule`)
普通用户读写	只读 (`-rorule`)和读写 (`-rwrule`)
超级用户只读	只读 (`-rorule`)和 `-superuser`
超级用户读写	只读 (`-rorule`)和读写 (`-rwrule`)和 `-superuser`

以下是这三个访问参数中每一个参数的有效安全类型：

- 任意
- 无
- 从不

以下安全类型不适用于 `-superuser` 参数：

- krb5.
- NTLM
- 系统

访问参数结果的规则

如果客户端的安全类型为...	然后单击...
与访问参数中指定的安全类型匹配。	客户端使用自己的用户ID接收该级别的访问。
与指定的安全类型不匹配，但访问参数包括选项 `none`。	客户端接收该级别的访问权限、并接收用户ID由参数指定的匿名用户 `-anon` 。
与指定的安全类型不匹配，并且访问参数不包括选项 `none`。	客户端不会收到该级别的任何访问权限。 此限制不适用于 `-superuser` 参数、因为此参数始终包括none、即使未指定也是如此。

Kerberos 5和Krb5p

从 ONTAP 9 开始，支持具有隐私服务的 Kerberos 5 身份验证 (krb5p)。Krbp5 身份验证模式具有较高的安全性，可通过使用校验和对客户端和服务器之间的所有流量进行加密，避免数据被篡改和窃听，达到保护目的。ONTAP解决方案支持Kerberos 128位和256位AES加密。隐私服务包括验证所接收数据的完整性、对用户进行身份验证以及在传输之前对数据进行加密。

krb5p选项在导出策略功能中最常用、并设置为加密选项。krb5p身份验证方法可用作身份验证参数、如以下示例所示：

```
cluster1::> vserver export-policy check-access -vserver vs1 -client-ip
10.22.32.42 -volume flex_vol -authentication-method krb5p -protocol nfs3
-access- type read
```

启用轻型目录访问协议签名和签章

支持签名和签章、以便对LDAP服务器的查询启用会话安全性。此方法提供了一种替代基于TLS的LDAP会话安全性的方法。

签名功能使用密钥技术确认LDAP有效负载数据的完整性。密封功能会对LDAP有效负载数据进行加密、以避免以明文形式传输敏感信息。SVM上的会话安全设置与LDAP服务器上可用的设置相对应。默认情况下、LDAP签名和签章处于禁用状态。

步骤

1. 要启用此功能、请使用参数运行 `vserver cifs security modify` 命令 `session-security-for-ad-ldap` 。

   LDAP安全功能选项：

   - 无：默认值，无签名或签章
   - **Sign**：对LDAP流量进行签名
   - **Seal**：对LDAP流量进行签名和加密

   > 符号和签章参数是累积的、这意味着如果使用签名选项、则结果为LDAP与签名。但是、如果使用了密封选项、则结果为符号和密封。此外、如果未为此命令指定参数、则默认值为none。

   以下是配置示例：

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock
-skew 3 -kerberos-ticket-age 8 -session-security-for-ad-ldap seal
```

创建并使用NetApp FPolicy

您可以创建和使用FPolicy、这是ONTAP解决方案的基础架构组件、支持合作伙伴应用程序监控和设置文件访问权限。更强大的应用程序之一是存储工作负载安全性、这是一款NetApp SaaS应用程序、可集中查看和控制混合云环境中的所有企业数据访问、以确保满足安全性和合规性目标。

访问控制是一个关键的安全概念。可见性以及对文件访问和文件操作的响应能力对于维护您的安全防护至关重要。为了提供文件可见性和访问控制、ONTAP解决方案使用NetApp FPolicy功能。

可以根据文件类型设置文件策略。FPolicy用于确定存储系统如何处理来自各个客户端系统的操作请求、例如创建、打开、重命名和删除。从ONTAP 9开始、FPolicy文件访问通知框架得到了增强、具有筛选控件和短时网络

中断故障恢复能力。

步骤

1. 要利用FPolicy功能、必须先使用命令创建FPolicy策略 `vserver fpolicy policy create` 。

   此外、如果使用FPolicy查看和收集事件、请使用 `-events` 参数。通过ONTAP提供的额外粒度、可以筛选和访问用户名级别的控制。要使用用户名控制权限和访问、请指定 `-privilege-user-name` 参数。

   以下文本提供了创建FPolicy的示例：

   ```
   cluster1::> vserver fpolicy policy create -vserver vs1.example.com
   -policy-name vs1_pol -events cserver_evt,v1e1 -engine native -is
   -mandatory true -allow-privileged-access no -is-passthrough-read-enabled
   false
   ```

2. 创建FPolicy策略后、必须使用命令启用它 `vserver fpolicy enable` 。此命令还会设置FPolicy条目的优先级或顺序。

   FPolicy顺序非常重要、因为如果多个策略订阅了同一个文件访问事件、则该顺序指示授予或拒绝访问的顺序。

   以下文本提供了用于启用FPolicy策略并使用命令验证配置的示例配置 `vserver fpolicy show` ：

   ```
   cluster1::> vserver fpolicy enable -vserver vs2.example.com -policy-name
   vs2_pol -sequence-number 5

   cluster1::> vserver fpolicy show
   Vserver                 Policy Name                     Sequence  Status
   Engine
   ----------------------- ------------------------------ --------  -------
   -------
   vs1.example.com         vs1_pol
   vs2.example.com         vs2_pol
    external
   2 entries were displayed.
   ```

FPolicy增强功能

ONTAP 9包括以下各节所述的FPolicy增强功能。

筛选控件

新筛选器可用于 `SetAttr` 和删除有关目录活动的通知。

如果在异步模式下运行的 FPolicy 服务器发生网络中断，则在中断期间生成的 FPolicy 通知将存储在存储节点上。当 FPolicy 服务器恢复联机时，它会收到存储的通知警报，并可从存储节点提取这些通知。在中断期间可以存储通知的时间长度可配置为长达 10 分钟。

LIF 安全性

LIF是具有相关特征的IP地址或全球通用端口名称(WWPN)、例如角色、主端口、主节点、要故障转移到的端口列表以及防火墙策略。您可以在集群通过网络发送和接收通信的端口上配置 LIF 。了解每个LIF角色的安全特征至关重要。

LIF角色

LIF角色可以是以下角色：

- 数据**LIF**：与SVM关联的用于与客户端通信的LIF。
- 集群**LIF**：用于在集群中的节点之间传输集群内流量的LIF。
- 节点管理**LIF**：提供专用IP地址以管理集群中的特定节点的LIF。
- 集群管理**LIF**：为整个集群提供单一管理接口的LIF。
- 集群间**LIF**：用于跨集群通信、备份和复制的LIF。

每个LIF角色的安全特征

	数据 LIF	集群 LIF	节点管理 LIF	集群管理 LIF	集群间 LIF
是否需要专用IP子网？	否	是的。	否	否	否
是否需要安全网络?	否	是的。	否	否	是的。
默认防火墙策略	限制性很强	完全开放	中等	中等	限制性很强
防火墙是否可自定义？	是的。	否	是的。	是的。	是的。

- 由于集群LIF已完全打开、没有可配置的防火墙策略、因此它必须位于安全隔离网络上的专用IP子网上。
- 在任何情况下、LIF角色都不应暴露在互联网上。

要了解有关保护生命周期的更多信息，请参见 "为 LIF 配置防火墙策略"。

协议和端口安全性

除了执行机载安全操作和功能之外、解决方案的强化还必须包括机下安全机制。利用防火墙、入侵防御系统(IPS)和其他安全设备等其他基础架构设备来过滤和限制对ONTAP的访问、是建立和保持严格安全防护的有效方法。此信息是筛选和限制对环境及其资源的访问

的关键组成部分。

常用协议和端口

服务	端口 / 协议	**Description**
SSH	22/TCP	SSH登录
telnet	23TCP	远程登录
Domain	53/TCP	域名服务器
HTTP	80/TCP 80/UDP	HTTP
rpcbind	111/TCP 111/UDP	远程操作步骤调用
NTP	123/UDP	网络时间协议
msrpc	135/UDP	Microsoft远程过程调用
Netbios-name	137/TCP 137/UDP	NetBIOS 名称服务
netbios-ssn	139/TCP	NetBIOS 服务会话
SNMP	161/UDP	SNMP
HTTPS	443/TCP	安全链接：http
microsoft-ds	445/TCP	Microsoft目录服务
IPsec	500/UDP	互联网协议安全性
mount	635/UDP	NFS 挂载
named	953/UDP	名称守护进程
NFS	2049/UDP 2049/TCP	NFS 服务器守护进程
nrv	20205/TCP	NetApp远程卷协议
iscsi	3260/TCP	iSCSI 目标端口
Lockd	4045/TCP 4045/UDP	NFS 锁定守护进程
NFS	4046/ TCP	NFS mountf协议
acp-proto	4046/UDP	记帐协议
rquotad	4049/UDP	NFS Rquotad 协议
krb524	444/UDP	Kerberos 524
IPsec	4500/UDP	互联网协议安全性
acp	5125/UDP 5133/UDP 5144/TCP	磁盘的备用控制端口

服务	端口 / 协议	Description
Mdns	5533/UDP	多播 DNS
HTTPS	5986/UDP	HTTPS端口：侦听二进制协议
TELNET	8023/TCP	节点范围Telnet
HTTPS	843/TCP	通过链接：HTTPS使用7MTT图形用户界面工具
RSH	8514/TCP	节点范围 RSH
KMIP	9877/TCP	KMIP客户端端口(仅限内部本地主机)
ndmp	10000/TCP	NDMP
cifs 见证端口	40001/TCP	CIFS见证端口
TLS	50000/TCP	传输层安全性
Iscsi	65200/TCP	iSCSI端口
SSH	65502/TCP	安全外壳
vsun	65503/TCP	vsun

NetApp内部端口

端口 / 协议	Description
900	NetApp 集群 RPC
902.	NetApp 集群 RPC
904	NetApp 集群 RPC
905	NetApp 集群 RPC
910.	NetApp 集群 RPC
911	NetApp 集群 RPC
913	NetApp 集群 RPC
914	NetApp 集群 RPC
91.	NetApp 集群 RPC
918	NetApp 集群 RPC
92.	NetApp 集群 RPC
921.	NetApp 集群 RPC
924	NetApp 集群 RPC
925	NetApp 集群 RPC
927	NetApp 集群 RPC
928	NetApp 集群 RPC
929.	NetApp 集群 RPC
931	NetApp 集群 RPC

端口 / 协议	Description
932	NetApp 集群 RPC
933	NetApp 集群 RPC
934	NetApp 集群 RPC
935)	NetApp 集群 RPC
936	NetApp 集群 RPC
937	NetApp 集群 RPC
939	NetApp 集群 RPC
940	NetApp 集群 RPC
951	NetApp 集群 RPC
954	NetApp 集群 RPC
955	NetApp 集群 RPC
956	NetApp 集群 RPC
958	NetApp 集群 RPC
961.	NetApp 集群 RPC
963	NetApp 集群 RPC
9664	NetApp 集群 RPC
966	NetApp 集群 RPC
967	NetApp 集群 RPC
7810.	NetApp 集群 RPC
7811.	NetApp 集群 RPC
7812.	NetApp 集群 RPC
7813.	NetApp 集群 RPC
7814.	NetApp 集群 RPC
7815.	NetApp 集群 RPC
7816.	NetApp 集群 RPC
7817.	NetApp 集群 RPC
7818.	NetApp 集群 RPC
7819.	NetApp 集群 RPC
7820.	NetApp 集群 RPC
7821.	NetApp 集群 RPC
7822.	NetApp 集群 RPC
7823.	NetApp 集群 RPC
7824.	NetApp 集群 RPC

安全资源

要了解有关本ONTAP安全文档中所述信息的详细信息、请参阅以下附加信息和安全概念。

有关报告漏洞和事件、NetApp安全响应以及客户机密性的信息，请参见 "NetApp安全门户"。

- "《 ONTAP 9 发行说明》"
- "ONTAP 9命令参考"
- "系统管理"
- "管理员身份验证和RBAC"
- "NetApp加密"
- "TR-4647：《ONTAP 9.3中的多因素身份验证》"
- "《OPENSSL 密码》"
- "CryptoMod, FIPS-140-2 1级"
- "使用适用于ONTAP的NetApp易管理性SDK进行基于证书的身份验证"
- "网络管理"