本地存储管理员帐户
ONTAP 9

NetApp
July 18, 2024

目录

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。