



创建或修改访问策略语句

ONTAP 9

NetApp
February 12, 2026

目录

创建或修改访问策略语句	1
了解ONTAP S3存储分段和对象存储服务器策略	1
将访问规则添加到默认ONTAP S3存储分段策略	1
创建或修改ONTAP S3对象存储服务器策略	3
为ONTAP S3访问配置外部目录服务	6
为LDAP配置S3访问	6
使用LDAP快速绑定模式进行身份验证	7
为 Active Directory 或 SMB 服务器配置 S3 访问	8
允许LDAP或域用户生成自己的ONTAP S3访问密钥	9
配置用户以生成访问密钥	10
作为S3或LDAP用户、生成您自己的访问密钥	12

创建或修改访问策略语句

了解ONTAP S3存储分段和对象存储服务器策略

用户和组对 S3 资源的访问由存储分段和对象存储服务器策略控制。如果用户或组数量较少，则在存储分段级别控制访问可能就已足够，但如果用户和组数量众多，则在对象存储服务器级别控制访问更容易。

将访问规则添加到默认ONTAP S3存储分段策略

您可以向默认存储分段策略添加访问规则。其访问控制的范围是包含的存储分段，因此，只有一个存储分段时，它才是最合适的。

开始之前

必须已存在已启用S3且包含S3服务器和存储分段的Storage VM。

在授予权限之前，您必须已创建用户或组。

关于此任务

您可以为新用户和组添加新语句，也可以修改现有语句的属性。有关的详细信息 `vserver object-store-server bucket policy`，请参见["ONTAP 命令参考"](#)。

可以在创建存储分段时或稍后根据需要授予用户和组权限。您还可以修改存储分段容量和 QoS 策略组分配。

从ONTAP 9.9.1开始、如果您计划在ONTAP S3服务器上支持AWS客户端对象标记功能、请执行以下操作 `GetObjectTagging`，`PutObjectTagging`，和 `DeleteObjectTagging` 需要允许使用存储分段或组策略。

您关注的操作步骤 取决于您使用的界面—System Manager或命令行界面：

System Manager

步骤

1. 编辑存储分段：单击 * 存储 > 存储分段 *，单击所需分段，然后单击 * 编辑 *。添加或修改权限时，您可以指定以下参数：

- 主体：被授予访问权限的用户或组。
- 影响：允许或拒绝对用户或组的访问。
- 操作：给定用户或组在存储分段中允许执行的操作。
- 资源：允许或拒绝访问的存储分段中对象的路径和名称。

默认值 *； bucketname_* 和 *； bucketname/*； 用于授予对存储分段中所有对象的访问权限。您还可以授予对单个对象的访问权限，例如 *； bucketname/_*； readme.txt*。

- 条件(可选)：尝试访问时评估的表达式。例如，您可以指定允许或拒绝访问的 IP 地址列表。



从ONTAP 9.14.1开始，您可以在*Res型*字段中为存储分段策略指定变量。这些变量是占位符、在评估策略时、这些占位符将替换为上下文值。例如、If \${aws:username} 指定为策略的变量、然后此变量将替换为请求上下文用户名、并且可以按照为该用户配置的方式执行策略操作。

命令行界面

步骤

1. 向存储分段策略添加语句：

```
vserver object-store-server bucket policy add-statement -vserver svm_name  
-bucket bucket_name -effect {allow|deny} -action object_store_actions  
-principal user_and_group_names -resource object_store_resources [-sid  
text] [-index integer]
```

以下参数用于定义访问权限：

-effect	该语句可能允许或拒绝访问
-action	您可以指定 * 表示所有操作、或者包含以下一项或多项的列表： GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListBucketMultipartUploads, 和 ListMultipartUploadParts。
-principal	一个或多个 S3 用户或组的列表。 <ul style="list-style-type: none">• 最多可以指定 10 个用户或组。• 如果指定了S3组、则必须采用的格式 group/group_name。• * 可以指定为表示公共访问、即不使用访问密钥和机密密钥的访问。• 如果未指定主体、则会为Storage VM中的所有S3用户授予访问权限。

-resource

分段及其包含的任何对象。通配符 * 和 ? 可用于形成用于指定资源的正则表达式。对于资源、您可以在策略中指定变量。这些策略变量是在评估策略时用上下文值替换的占位符。

您可以选择使用指定文本字符串作为注释 -sid 选项

示例

以下示例将为Storage VM svm1.example.com和bucket1创建对象存储服务器分段策略语句、指定允许对象存储服务器用户user1访问自述文件文件夹。

```
cluster1::> vservers object-store-server bucket policy statement create
-vserver svm1.example.com -bucket bucket1 -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket -principal user1 -resource
bucket1/readme/* -sid "fullAccessToReadmeForUser1"
```

以下示例将为Storage VM svm1.example.com和bucket1创建对象存储服务器分段策略语句、该语句指定允许访问对象存储服务器组group1的所有对象。

```
cluster1::> vservers object-store-server bucket policy statement create
-vserver svm1.example.com -bucket bucket1 -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket -principal group/group1
-resource bucket1/* -sid "fullAccessForGroup1"
```

从ONTAP 9.14.1开始、您可以为分段策略指定变量。以下示例将为Storage VM创建服务器分段策略语句 svm1 和 bucket1 和指定 ``_${aws:username}` 作为策略资源的变量。评估策略时、策略变量将替换为请求上下文用户名、并且可以按照为该用户配置的方式执行策略操作。例如、在评估以下策略语句时、`_${aws:username}` 替换为执行S3操作的用户。如果是用户 user1 执行此操作时、该用户将被授予访问权限 bucket1 作为 bucket1/user1/*。

```
cluster1::> object-store-server bucket policy statement create -vserver
svm1 -bucket bucket1 -effect allow -action * -principal - -resource
bucket1,bucket1/${aws:username}/*##
```

创建或修改ONTAP S3对象存储服务器策略

您可以创建可应用于对象存储中的一个或多个分段的策略。可以将对象存储服务器策略附加到用户组，从而简化跨多个存储分段的资源访问管理。

开始之前

包含 S3 服务器和存储分段且已启用 S3 的 SVM 必须已存在。

关于此任务

您可以通过在对象存储服务器组中指定默认或自定义策略来在 SVM 级别启用访问策略。只有在组定义中指定策略后，这些策略才会生效。



使用对象存储服务器策略时，您可以在组定义中指定主体（即用户和组），而不是在策略本身中指定主体。

访问 ONTAP S3 资源有三种只读默认策略：

- 完全访问
- NoS3 访问
- 只读访问

您也可以创建新的自定义策略，然后为新用户和组添加新语句，或者修改现有语句的属性。有关的详细信息 `vserver object-store-server policy`，请参见“[ONTAP 命令参考](#)”。

从 ONTAP 9.9.1 开始、如果您计划在 ONTAP S3 服务器上支持 AWS 客户端对象标记功能、请执行以下操作 `GetObjectTagging`，`PutObjectTagging`，和 `DeleteObjectTagging` 需要允许使用存储分段或组策略。

您关注的操作步骤 取决于您使用的界面—System Manager 或命令行界面：

System Manager

使用System Manager创建或修改对象存储服务器策略

步骤

1. 编辑Storage VM：单击*存储> Storage VM*、单击Storage VM、单击*设置*、然后单击  S3下的。
2. 添加用户：单击 * 策略 *，然后单击 * 添加 *。
 - a. 输入策略名称并从组列表中进行选择。
 - b. 选择现有默认策略或添加新策略。

添加或修改组策略时，您可以指定以下参数：

- group：授予访问权限的组。
 - 影响：允许或拒绝对一个或多个组的访问。
 - 操作：给定组的一个或多个分段中允许的操作。
 - 资源：授予或拒绝访问权限的一个或多个分段中的对象的路径和名称。例如：
 - * 授予对 Storage VM 中所有分段的访问权限。
 - * bucketname* 和 * bucketname/* 授予对特定存储分段中所有对象的访问权限。
 - *bucketname/readme.txt 授予对特定存储分段中某个对象的访问权限。
- c. 如果需要，可将语句添加到现有策略中。

命令行界面

使用命令行界面创建或修改对象存储服务器策略

步骤

1. 创建对象存储服务器策略：

```
vserver object-store-server policy create -vserver svm_name -policy policy_name [-comment text]
```

2. 为策略创建语句：

```
vserver object-store-server policy statement create -vserver svm_name -policy policy_name -effect {allow|deny} -action object_store_actions -resource object_store_resources [-sid text]
```

以下参数用于定义访问权限：

-effect	该语句可能允许或拒绝访问
---------	--------------

-action	您可以指定 * 表示所有操作、或者包含以下一项或多项的列表: GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListAllMyBuckets, ListBucketMultipartUploads, 和 ListMultipartUploadParts。
-resource	分段及其包含的任何对象。通配符 * 和 ? 可用于形成用于指定资源的正则表达式。

您可以选择使用指定文本字符串作为注释 -sid 选项

默认情况下, 新的语句将添加到语句列表的末尾, 并按顺序进行处理。以后添加或修改语句时、您可以选择修改该语句的 -index 设置以更改处理顺序。

有关此过程中所述命令的更多信息, 请参见["ONTAP 命令参考"](#)。

为ONTAP S3访问配置外部目录服务

从ONTAP 9.14.1开始、外部目录服务已与ONTAP S3对象存储集成。这种集成通过外部目录服务简化了用户和访问管理。

您可以为属于外部目录服务的用户组提供对ONTAP对象存储环境的访问权限。轻型目录访问协议(LDAP)是一个用于与目录服务(如Active Directory)通信的接口、这些服务为身份和访问管理(IAM)提供数据库和服务。要提供访问权限、您需要在ONTAP S3环境中配置LDAP组。配置访问权限后、组成员将有权访问ONTAP S3存储分段。有关LDAP的信息, 请参见["了解如何在 ONTAP NFS SVM 上使用 LDAP 名称服务"](#)。

您还可以将Active Directory用户组配置为快速绑定模式、以便验证用户凭据、并通过LDAP连接对第三方和开源S3应用程序进行身份验证。

开始之前

在配置LDAP组并为组访问启用快速绑定模式之前、请确保满足以下要求:

1. 已创建一个包含S3服务器且已启用S3的Storage VM。请参见 ["为 S3 创建 SVM"](#)。
2. 已在此Storage VM中创建存储分段。请参见 ["创建存储分段"](#)。
3. 已在Storage VM上配置DNS。请参阅 ["配置 DNS 服务"](#)
4. 此Storage VM上安装了LDAP服务器的自签名根证书颁发机构(CA)证书。请参阅 ["在 SVM 上安装自签名根 CA 证书"](#)
5. LDAP客户端在SVM上配置为启用TLS。请参阅["为 ONTAP NFS 访问创建 LDAP 客户端配置"](#)和["将 LDAP 客户端配置与 ONTAP NFS SVM 关联以获取信息"](#)。

为LDAP配置S3访问

1. 指定LDAP作为组的SVM的_name service database _、并将密码指定给LDAP:

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

有关链接：[https://docs NetApp. ONTAP—CLI/vserver-services-name-service-ns-switch-modify.html](https://docs.netapp.com/ontap-8.4/CLI/vserver-services-name-service-ns-switch-modify.html)^的更多信息，请[`vserver services name-service ns-switch modify`]参阅ONTAP命令参考。

2. 使用创建对象存储分段策略语句 `principal` 设置为要授予访问权限的LDAP组：

```
object-store-server bucket policy statement create -bucket <bucket-name>
-effect allow -principal nasgroup/<ldap-group-name> -resource <bucket-
name>, <bucket-name>/*
```

示例：以下示例将为创建存储分段策略语句 `buck1`。此策略允许对LDAP组进行访问 `group1` 资源(存储分段及其对象) `buck1`。

```
vserver object-store-server bucket policy add-statement -bucket buck1
-effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,Li
stBucketMultipartUploads,ListMultipartUploadParts,
ListBucketVersions,GetObjectTagging,PutObjectTagging,DeleteObjectTagging
,GetBucketVersioning,PutBucketVersioning -principal nasgroup/group1
-resource buck1, buck1/*
```

3. 验证LDAP组中的用户 `group1` 能够从S3客户端执行S3操作。

使用LDAP快速绑定模式进行身份验证

1. 指定LDAP作为组的SVM的 `_name service database _`、并将密码指定给LDAP：

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

有关链接：[https://docs NetApp. ONTAP—CLI/vserver-services-name-service-ns-switch-modify.html](https://docs.netapp.com/ontap-8.4/CLI/vserver-services-name-service-ns-switch-modify.html)^的更多信息，请[`vserver services name-service ns-switch modify`]参阅ONTAP命令参考。

2. 确保访问S3存储分段的LDAP用户具有存储分段策略中定义的权限。有关详细信息，请参见 ["修改存储分段策略"](#)。
3. 验证LDAP组中的用户是否可以执行以下操作：

- a. 按以下格式在S3客户端上配置访问密钥:

"NTAPFASTBIND" + base64-encode (user-name:password) 例如: "NTAPFASTBIND"+
base64-encode (LDAPUser: password)、结果为
NTAPFASTBINDbGRhcHVzZXI6cGFzc3dvcmQ=



S3客户端可能会提示输入机密密钥。如果没有机密密钥、则可以输入任何至少包含16个字符的密码。

- b. 从用户拥有权限的S3客户端执行基本S3操作。

Base64 凭据

ONTAP S3的默认配置不包括HTTP、而是仅使用HTTPS和传输层安全(Transport Layer Security、TLS)连接。ONTAP可以生成自签名证书、但建议的最佳实践是使用第三方证书颁发机构(CA)提供的证书。使用CA证书时、需要在客户端应用程序和ONTAP对象存储服务器之间创建受信任关系。

请注意、使用Base64编码的凭据很容易解码。使用HTTPS可以防止中间人数据包发现器捕获编码凭据。

创建预签名URL时、请勿使用LDAP快速绑定模式进行身份验证。身份验证仅基于预签名URL中包含的Base64访问密钥。将向解码Base64访问密钥的任何人显示用户名和密码。

例如、身份验证方法为nsswitch、已启用LDAP

```
$curl -siku <user>:<user_password> -X POST  
https://<LIF_IP_Address>/api/protocols/s3/services/<SVM_UUID>/users -d  
{ "comment": "<S3_user_name>", "name":<user>, "key_time_to_live": "PT6H3M" }
```



将API定向到集群管理LIF、而不是SVM的数据LIF。如果要允许用户生成自己的密钥、则必须向其角色添加HTTP权限才能使用CURL。此权限是对S3 API权限的补充。

为 Active Directory 或 SMB 服务器配置 S3 访问

如果在b分 段策略语句中指定的鼻组或属于鼻组的用户未设置UID和GID、则在未找到这些属性时、查找将失败。Active Directory使用SID、而不是UID。如果SID条目无法映射到UID、则需要将必要的数据提供给ONTAP。

为此、请使用"[Vserver active-directory create](#)"、以便SVM可以向Active Directory进行身份验证并获取所需的用户和组信息。

或者、使用"[创建Vserver CIFS](#)"在Active Directory域中创建SMB服务器。

如果名称服务器和对象存储使用不同的域名、则可能会遇到查找失败的情况。为避免查找失败、NetApp建议使用 UPN 格式的受信任域进行资源授权: `nasgroup/group@trusted_domain.com` 受信任域是指已添加到 SMB 服务器受信任域列表中的域。了解如何"[添加、删除和修改首选信任域](#)"在 SMB 服务器列表中。

当身份验证方法为domain且在Active Directory中配置了受信任域时、生成密钥

对以UPN格式指定的用户使用 s3/services/<svm_uuid>/users 端点。示例:

```
$curl -siku FQDN\\user:<user_password> -X POST
https://<LIF_IP_Address>/api/protocols/s3/services/<SVM_UUID>/users -d
{"comment":"<S3_user_name>",
"name":<user@fqdn>,"key_time_to_live":"PT6H3M"}
```



将API定向到集群管理LIF、而不是SVM的数据LIF。如果要允许用户生成自己的密钥、则必须向其角色添加HTTP权限才能使用CURL。此权限是对S3 API权限的补充。

当身份验证方法为**domain**且不存在受信任域时、生成密钥

如果禁用了LDAP或非POSIX用户未配置UID和GID、则可以执行此操作。示例：

```
$curl -siku FQDN\\user:<user_password> -X POST
https://<LIF_IP_Address>/api/protocols/s3/services/<SVM_UUID>/users -d
{"comment":"<S3_user_name>",
"name":<user[@fqdn]>,"key_time_to_live":"PT6H3M"}
```



将API定向到集群管理LIF、而不是SVM的数据LIF。如果要允许用户生成自己的密钥、则必须向其角色添加HTTP权限才能使用CURL。此权限是对S3 API权限的补充。只有在不存在受信任域的情况下、才需要向用户名添加可选域值(@FQDN)。

允许LDAP或域用户生成自己的ONTAP S3访问密钥

从ONTAP 9.14.1开始、作为ONTAP管理员、您可以创建自定义角色并将其授予本地或域组或轻型目录访问协议(Lightweight-Directory Access Protocol、LDAP)组、以便属于这些组的用户可以生成自己的访问权限和机密密钥来进行S3客户端访问。

您必须在Storage VM上执行一些配置步骤、才能创建自定义角色并将其分配给调用API以生成访问密钥的用户。



如果LDAP被禁用，您可以["为ONTAP S3访问配置外部目录服务"](#)允许用户生成访问密钥。

开始之前

确保满足以下要求：

1. 已创建一个包含S3服务器且已启用S3的Storage VM。请参见 ["为 S3 创建 SVM"](#)。
2. 已在此Storage VM中创建存储分段。请参见 ["创建存储分段"](#)。
3. 已在Storage VM上配置DNS。请参阅。 ["配置 DNS 服务"](#)
4. 此Storage VM上安装了LDAP服务器的自签名根证书颁发机构(CA)证书。请参阅。 ["在 SVM 上安装自签名根 CA 证书"](#)
5. LDAP客户端已在Storage VM上配置为启用TLS。请参阅。 ["为 ONTAP NFS 访问创建 LDAP 客户端配置"](#)
6. 将客户端配置与Vserver相关联。请参阅。 ["将 LDAP 客户端配置与 ONTAP NFS SVM 关联"](#)有关的详细信息 `vserver services name-service ldap create`，请参见["ONTAP 命令参考"](#)。

7. 如果您使用的是数据Storage VM、请在此VM上创建管理网络接口(LIF)和、并为此LIF创建一个服务策略。有关和的 `network interface service-policy create` `详细信息` `network interface create` , 请参见"[ONTAP 命令参考](#)"。

配置用户以生成访问密钥

示例 1. 步骤

LDAP 用户

1. 指定LDAP作为组的Storage VM的_name service database _、并为LDAP设置密码:

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

有关的详细信息 `vserver services name-service ns-switch modify`, 请参见["ONTAP 命令参考"](#)。

2. 创建可访问S3用户REST API端点的自定义角色:

```
security login rest-role create -vserver <vserver-name> -role <custom-role-
name> -api "/api/protocols/s3/services/*/users" -access <access-type>
```

在此示例中、将显示 `s3-role` 此角色是为Storage VM上的用户生成的 `svm-1`, 授予所有访问权限, 包括读取、创建和更新权限。

```
security login rest-role create -vserver svm-1 -role s3role -api
"/api/protocols/s3/services/*/users" -access all
```

有关的详细信息 `security login rest-role create`, 请参见["ONTAP 命令参考"](#)。

3. 使用以下方式创建 LDAP 用户组 `'security login'` 命令并添加用于访问 S3 用户 REST API 端点的新自定义角色。详细了解 `'security login create'` 在["ONTAP 命令参考"](#)。

```
security login create -user-or-group-name <ldap-group-name>
-application http -authentication-method nsswitch -role <custom-
role-name> -is-ns-switch-group yes
```

在此示例中、为LDAP组 `ldap-group-1` 在中创建 `svm-1` 和自定义角色 `s3role` 添加到其中、用于访问API端点、并在快速绑定模式下启用LDAP访问。

```
security login create -user-or-group-name ldap-group-1 -application
http -authentication-method nsswitch -role s3role -is-ns-switch
-group yes -second-authentication-method none -vserver svm-1 -is
-ldap-fastbind yes
```

有关详细信息, 请参见 ["使用 LDAP 快速绑定对 ONTAP NFS SVM 进行 nsswitch 身份验证"](#)。

有关的详细信息 `security login create`, 请参见["ONTAP 命令参考"](#)。

将自定义角色添加到 LDAP 组允许该组中的用户对ONTAP进行有限的访问

`/api/protocols/s3/services/{svm.uuid}/users`` 端点。通过调用 API，LDAP 组用户可以生成自己的访问密钥和密钥来访问 S3 客户端。他们只能为自己生成密钥，而不能为其他用户生成密钥。

域用户

1. 创建可以访问 S3 用户 REST API 端点的自定义角色：

```
security login rest-role create -vserver <vserver-name> -role <custom-role-name> -api "/api/protocols/s3/services/*/users" -access <access-type>
```

在此示例中，`s3-role`` 为存储虚拟机上的用户生成角色 ``svm-1``，授予所有访问权限，即读取、创建和更新。

```
security login rest-role create -vserver svm-1 -role s3role -api "/api/protocols/s3/services/*/users" -access all
```

有关的详细信息 `security login rest-role create`，请参见["ONTAP 命令参考"](#)。

1. 使用以下方式创建域用户组 ``security login`` 命令并添加用于访问 S3 用户 REST API 端点的新自定义角色。详细了解 ``security login create`` 在["ONTAP 命令参考"](#)。

```
security login create -vserver <vserver-name> -user-or-group-name domain\<group-name> -application http -authentication-method domain -role <custom-role-name>
```

在此示例中，域组 ``domain\group1`` 创建于 ``svm-1`` 以及自定义角色 ``s3role`` 添加到其中以访问 API 端点。

```
security login create -user-or-group-name domain\group1 -application http -authentication-method domain -role s3role -vserver svm-1
```

有关的详细信息 `security login create`，请参见["ONTAP 命令参考"](#)。

将自定义角色添加到域组允许该组中的用户对 ONTAP 进行有限的访问 `/api/protocols/s3/services/{svm.uuid}/users`` 端点。通过调用 API，域组用户可以生成自己的访问密钥和密钥来访问 S3 客户端。他们只能为自己生成密钥，而不能为其他用户生成密钥。

作为 S3 或 LDAP 用户、生成您自己的访问密钥

从 ONTAP 9.14.1 开始、如果管理员已授予您生成自己密钥的角色、您可以生成自己的访问权限和机密密钥来访问 S3 客户端。您只能使用以下 ONTAP REST API 端点为自己生成密钥。

创建 S3 用户并生成密钥

此 REST API 调用使用以下方法和端点。有关此端点的更多信息，请参阅参考 ["API文档"](#)。

HTTP 方法	路径
发布	/api/protocols、s3/services / {svm.unid} /用户

对于域用户，请使用以下格式作为 S3 用户名：user@fqdn，在哪里`fqdn`是域的完全限定域名。

curl 示例

```
curl
--request POST \
--location "https://$FQDN_IP /api/protocols/s3/services/{svm.uuid}/users "
\
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
--data '{"name":"user1@example.com"}'
```

JSON 输出示例

```
{
  "records": [
    {
      "access_key": "4KX07KF7ML8YNWY01JWG",
      "_links": {
        "next": {
          "href": "/api/resourcelink"
        },
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "user1@example.com",
      "secret_key": "<secret_key_value>"
    }
  ],
  "num_records": "1"
}
```

为 S3 用户重新生成密钥

如果 S3 用户已存在，您可以重新生成其访问密钥和密钥。此 REST API 调用使用以下方法和端点。

HTTP 方法	路径
修补	/api/protocols/s3/services/{svm.uuid}/用户/{名称}

curl 示例

```
curl
--request PATCH \
--location "https://$FQDN_IP
/api/protocols/s3/services/{svm.uuid}/users/{name} " \
--include \
--header "Authorization: Basic $BASIC_AUTH" \
--data '{"regenerate_keys":"True"}'
```

JSON 输出示例

```
{
  "records": [
    {
      "access_key": "DX12U609DMRVD8U30Z1M",
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "user1@example.com",
      "secret_key": "<secret_key_value>"
    }
  ],
  "num_records": "1"
}
```

版权信息

版权所有 © 2026 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。