



## 配置名称映射 ONTAP 9

NetApp  
April 24, 2024

# 目录

- 配置名称映射 ..... 1
  - 配置名称映射概述 ..... 1
  - 名称映射的工作原理 ..... 1
  - 多域搜索 UNIX 用户到 Windows 用户名映射 ..... 2
  - 名称映射转换规则 ..... 3
  - 创建名称映射 ..... 3
  - 配置默认用户： ..... 4
  - 用于管理名称映射的命令 ..... 5

# 配置名称映射

## 配置名称映射概述

ONTAP 使用名称映射将 SMB 身份映射到 UNIX 身份，将 Kerberos 身份映射到 UNIX 身份以及将 UNIX 身份映射到 SMB 身份。无论用户是从 NFS 客户端还是从 SMB 客户端进行连接，IT 都需要此信息来获取用户凭据并提供正确的文件访问权限。

除了两个例外情况，您无需使用名称映射：

- 您配置的是纯 UNIX 环境，不打算在卷上使用 SMB 访问或 NTFS 安全模式。
- 您可以配置要使用的默认用户。

在这种情况下，不需要进行名称映射，因为所有客户端凭据都映射到同一默认用户，而不是映射每个客户端凭据。

请注意，您只能对用户使用名称映射，而不能对组使用名称映射。

但是，您可以将一组用户映射到特定用户。例如，您可以将以 SALES 开头或结尾的所有 AD 用户映射到特定 UNIX 用户和用户的 UID。

## 名称映射的工作原理

当 ONTAP 必须映射用户的凭据时，它会首先检查本地名称映射数据库和 LDAP 服务器中是否存在现有映射。它是检查一个还是同时检查这两者，以及检查顺序取决于 SVM 的名称服务配置。

- 适用于 Windows 到 UNIX 的映射

如果未找到映射，ONTAP 将检查小写的 Windows 用户名是否为 UNIX 域中的有效用户名。如果此操作不起作用，则只要配置了默认 UNIX 用户，它就会使用默认 UNIX 用户。如果未配置默认 UNIX 用户，并且 ONTAP 也无法通过这种方式获取映射，则映射将失败并返回错误。

- UNIX 到 Windows 的映射

如果未找到映射，ONTAP 将尝试查找与 SMB 域中的 UNIX 名称匹配的 Windows 帐户。如果此操作不起作用，则会使用默认 SMB 用户，但前提是已配置此用户。如果未配置默认 SMB 用户、并且 ONTAP 也无法通过此方式获取映射、则映射将失败并返回错误。

默认情况下，计算机帐户映射到指定的默认 UNIX 用户。如果未指定默认 UNIX 用户，计算机帐户映射将失败。

- 从 ONTAP 9.5 开始，您可以将计算机帐户映射到默认 UNIX 用户以外的用户。
- 在 ONTAP 9.4 及更早版本中，您无法将计算机帐户映射到其他用户。

即使为计算机帐户定义了名称映射，也会忽略这些映射。

# 多域搜索 UNIX 用户到 Windows 用户名映射

在将 UNIX 用户映射到 Windows 用户时，ONTAP 支持多域搜索。系统将搜索所有已发现的受信任域以查找与替换模式匹配的匹配项，直到返回匹配结果为止。或者，您也可以配置首选受信任域列表，该列表将代替发现的受信任域列表使用，并按顺序进行搜索，直到返回匹配结果为止。

## 域信任如何影响 UNIX 用户到 Windows 用户名称映射搜索

要了解多域用户名映射的工作原理，您必须了解域信任如何与 ONTAP 配合使用。与 SMB 服务器主域的 Active Directory 信任关系可以是双向信任、也可以是两种类型的单向信任之一、即入站信任或出站信任。主域是 SVM 上的 SMB 服务器所属的域。

### • \_ 双向信任 \_

通过双向信任，两个域相互信任。如果 SMB 服务器的主域与另一个域具有双向信任、则主域可以对属于受信任域的用户进行身份验证和授权、反之亦然。

UNIX 用户到 Windows 用户名映射搜索只能在主域和另一个域之间具有双向信任的域上执行。

### • 出站信任 \_

对于出站信任，主域信任另一个域。在这种情况下，主域可以对属于出站受信任域的用户进行身份验证和授权。

执行 UNIX 用户到 Windows 用户名映射搜索时，系统会搜索与主域具有出站信任的域。

### • Inbound trust


对于入站信任、另一个域信任 SMB 服务器的主域。在这种情况下，主域无法对属于入站受信任域的用户进行身份验证或授权。

在执行 UNIX 用户到 Windows 用户名映射搜索时，系统会搜索与主域具有入站信任的域。

## 如何使用通配符（\*）配置名称映射的多域搜索

在 Windows 用户名的域部分使用通配符有助于进行多域名称映射搜索。下表说明了如何在名称映射条目的域部分使用通配符来启用多域搜索：

Pattern	更换	结果
root	{ asterisk } { 反斜杠 } { 反斜杠 } 管理员	UNIX 用户 "root" 将映射到名为 "administrator" 的用户。系统会按顺序搜索所有受信任域，直到找到第一个名为 "administrator" 的匹配用户为止。

Pattern	更换	结果
*	{ asterisk } { 反斜杠 } { 反斜杠 } { asterisk }	<p>有效的 UNIX 用户将映射到相应的 Windows 用户。系统将按顺序搜索所有受信任域，直到找到具有该名称的第一个匹配用户为止。</p> <div>  <p>模式 { asterisk } { un斜杠 } { un斜杠 } { asterisk } 仅适用于从 UNIX 到 Windows 的名称映射，而不是相反。</p> </div>

## 如何执行多域名搜索

您可以选择以下两种方法之一来确定用于多域名搜索的受信任域列表：

- 使用由 ONTAP 编译的自动发现的双向信任列表
- 使用您编译的首选受信任域列表

如果将 UNIX 用户映射到使用通配符用于用户名的域部分的 Windows 用户，则会在所有受信任域中查找此 Windows 用户，如下所示：

- 如果配置了首选受信任域列表，则只会在此搜索列表中按顺序查找映射的 Windows 用户。
- 如果未配置首选受信任域列表，则会在主域的所有双向受信任域中查找 Windows 用户。
- 如果主域没有双向受信任的域，则会在主域中查找用户。

如果 UNIX 用户映射到用户名中没有域部分的 Windows 用户，则会在主域中查找此 Windows 用户。

## 名称映射转换规则

ONTAP 系统会为每个 SVM 保留一组转换规则。每个规则都包含两部分：*pattern* 和 *replacement*。转换从相应列表的开头开始，并根据第一个匹配规则执行替换。模式是 UNIX 模式的正则表达式。替换项是一个字符串、其中包含表示模式中的子表达式的转义序列、与 UNIX 中的情况一样 sed 计划。

## 创建名称映射

您可以使用 `vserver name-mapping create` 命令以创建名称映射。您可以使用名称映射使 Windows 用户能够访问 UNIX 安全模式卷，反之亦然。

关于此任务

对于每个 SVM，ONTAP 支持每个方向最多 12，500 个名称映射。

步骤

## 1. 创建名称映射：

```
vserver name-mapping create -vserver vserver_name -direction {krb-unix|win-unix|unix-win} -position integer -pattern text -replacement text
```



。 -pattern 和 -replacement 语句可以表达为正则表达式。您也可以使用 -replacement 用于使用空替换字符串明确拒绝映射到用户的语句 " " (空格字符)。请参见 vserver name-mapping create 有关详细信息、请参见手册页。

创建 Windows 到 UNIX 映射时，在创建新映射时与 ONTAP 系统建立了打开连接的任何 SMB 客户端都必须注销并重新登录才能查看新映射。

### 示例

以下命令将在名为 vs1 的 SVM 上创建名称映射。此映射是指优先级列表中位置 1 处从 UNIX 到 Windows 的映射。映射会将 UNIX 用户 johnd 映射到 Windows 用户 ENG\JohnDoe。

```
vs1::> vserver name-mapping create -vserver vs1 -direction unix-win  
-position 1 -pattern johnd  
-replacement "ENG\\JohnDoe"
```

以下命令会在名为 vs1 的 SVM 上创建另一个名称映射。此映射是指优先级列表中位置 1 处从 Windows 到 UNIX 的映射。此处的模式和替换项包括正则表达式。此映射会将域 ENG 中的每个 CIFS 用户映射到与 SVM 关联的 LDAP 域中的用户。

```
vs1::> vserver name-mapping create -vserver vs1 -direction win-unix  
-position 1 -pattern "ENG\\(.+)"  
-replacement "\\1"
```

以下命令会在名为 vs1 的 SVM 上创建另一个名称映射。此处的模式将 " \$" 作为必须转义的 Windows 用户名中的一个元素。映射会将 Windows 用户 ENG\john\$ops 映射到 UNIX 用户 john\_ops。

```
vs1::> vserver name-mapping create -direction win-unix -position 1  
-pattern ENG\\john$ops  
-replacement john_ops
```

## 配置默认用户：

您可以配置一个默认用户，以便在用户的所有其他映射尝试均失败或不希望在 UNIX 和 Windows 之间映射单个用户时使用。或者，如果您希望对未映射用户的身份验证失败，则不应配置默认用户。

### 关于此任务

对于 CIFS 身份验证，如果不希望将每个 Windows 用户映射到单个 UNIX 用户，则可以改为指定默认 UNIX 用户。

对于 NFS 身份验证，如果不希望将每个 UNIX 用户映射到单个 Windows 用户，则可以改为指定一个默认 Windows 用户。

#### 步骤

1. 执行以下操作之一：

如果您要 ...	输入以下命令 ...
配置默认 UNIX 用户	<code>vserver cifs options modify -default-unix-user user_name</code>
配置默认 Windows 用户	<code>vserver nfs modify -default-win-user user_name</code>

## 用于管理名称映射的命令

您可以使用特定的 ONTAP 命令来管理名称映射。

如果您要 ...	使用此命令 ...
创建名称映射	<code>vserver name-mapping create</code>
在特定位置插入名称映射	<code>vserver name-mapping insert</code>
显示名称映射	<code>vserver name-mapping show</code>
交换两个名称映射的位置 注意：如果为名称映射配置了 IP 限定符条目、则不允许进行交换。	<code>vserver name-mapping swap</code>
修改名称映射	<code>vserver name-mapping modify</code>
删除名称映射	<code>vserver name-mapping delete</code>
验证名称映射是否正确	<code>vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1</code>

有关详细信息，请参见每个命令的手册页。

## 版权信息

版权所有 © 2024 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，本文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。