



使用空会话访问非 **Kerberos** 环境中的存储 ONTAP 9

NetApp
September 12, 2024

目录

- 使用空会话访问非 Kerberos 环境中的存储 1
 - 使用空会话访问非 Kerberos 环境中的存储概述 1
 - 存储系统如何提供空会话访问 1
 - 授予空用户对文件系统共享的访问权限 1

使用空会话访问非 Kerberos 环境中的存储

使用空会话访问非 Kerberos 环境中的存储概述

空会话访问可为存储系统数据等网络资源以及在本地系统下运行的基于客户端的服务提供权限。当客户端进程使用 `ssystem` 帐户访问网络资源时，将发生空会话。空会话配置专用于非 Kerberos 身份验证。

存储系统如何提供空会话访问

由于空会话共享不需要身份验证，因此需要空会话访问的客户端必须在存储系统上映射其 IP 地址。

默认情况下，未映射的空会话客户端可以访问某些 ONTAP 系统服务，例如共享枚举，但会限制它们访问任何存储系统数据。



ONTAP通过支持Windows注册表设置值 `-restrict-anonymous` 选项这样，您可以控制未映射的空用户查看或访问系统资源的范围。例如，您可以禁用共享枚举和对 `IPC$` 共享（隐藏的命名管道共享）的访问。。 `vserver cifs options modify` 和 `vserver cifs options show` 手册页提供了有关的详细信息 `-restrict-anonymous` 选项

除非另有配置，否则运行通过空会话请求存储系统访问的本地进程的客户端仅是非限制性组的成员，例如 `"everyone"`。要限制对选定存储系统资源的空会话访问，您可能需要创建所有空会话客户端所属的组；通过创建此组，您可以限制存储系统访问并设置专门应用于空会话客户端的存储系统资源权限。

ONTAP在中提供了映射语法 `vserver name-mapping` 用于指定允许使用空用户会话访问存储系统资源的客户端的IP地址的命令集。为空用户创建组后，您可以指定存储系统资源的访问限制以及仅适用于空会话的资源权限。空用户标识为匿名登录。空用户无权访问任何主目录。

从映射的 IP 地址访问存储系统的任何空用户都将获得映射的用户权限。请考虑适当的预防措施，以防止未经授权访问与空用户映射的存储系统。要获得最大保护，请将存储系统和所有需要空用户存储系统访问的客户端置于单独的网络上，以消除 IP 地址 spoofing 的可能性。

相关信息

[配置匿名用户的访问限制](#)

授予空用户对文件系统共享的访问权限

您可以通过分配空会话客户端要使用的组并记录空会话客户端的 IP 地址以添加到允许使用空会话访问数据的客户端列表，从而允许空会话客户端访问存储系统资源。

步骤

1. 使用 `vserver name-mapping create` 命令、用于将空用户映射到任何有效的Windows用户、并使用IP限定符。

以下命令使用有效主机名 `google.com` 将空用户映射到 `user1`：

```
vserver name-mapping create -direction win-unix -position 1 -pattern  
"ANONYMOUS LOGON" -replacement user1 - hostname google.com
```

以下命令使用有效 IP 地址 10.238.2.54/32 将空用户映射到 user1：

```
vserver name-mapping create -direction win-unix -position 2 -pattern  
"ANONYMOUS LOGON" -replacement user1 -address 10.238.2.54/32
```

2. 使用 `vserver name-mapping show` 命令以确认名称映射。

```
vserver name-mapping show
```

```
Vserver:    vs1
```

```
Direction: win-unix
```

```
Position Hostname          IP Address/Mask
```

```
-----
```

```
1          -              10.72.40.83/32      Pattern: anonymous logon  
                                           Replacement: user1
```

3. 使用 `vserver cifs options modify -win-name-for-null-user` 用于将Windows成员资格分配给空用户的命令。

只有当空用户具有有效的名称映射时，此选项才适用。

```
vserver cifs options modify -win-name-for-null-user user1
```

4. 使用 `vserver cifs options show` 命令以确认将空用户映射到Windows用户或组。

```
vserver cifs options show
```

```
Vserver :vs1
```

```
Map Null User to Windows User of Group: user1
```

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。