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

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
```