



CIFS Kerberos 的 ONTAP 要求

https://kb-cn-stage.netapp.com/on-prem/ontap/da/NAS/NAS-KBs/ONTAP_Requirements_for_CIFS_Ke...

Updated: Wed, 22 Apr 2026 03:53:51 GMT

适用场景

- ONTAP 9
- Microsoft Windows
- CIFS/SMB
- Kerberos

问题解答

- [Kerberos是Active Directory的主要身份验证服务](#)
- Microsoft [建议限制NTLM身份验证](#)
- 要确保 从ONTAP CIFS SVM使用Kerberos身份验证、需要满足以下条件：
 1. 按照 [映射DNS服务器](#) 操作步骤上的SMB服务器进行操作。
 2. [1] 使用 `setspn -l` 带有 [SVM SMB Server Name的windows命令确认UNC的服务器名部分中用于访问SMB共享的主机名、别名、完全限定域名\(Fqdn\)或IP地址](#)。 如果 未返回与所用的Service VNAME匹配的条目，请按照 [How](#)

'NetApp provides no representations or warranties regarding the accuracy or reliability or serviceability of any information or recommendations provided in this publication or with respect to any results that may be obtained by the use of the information or observance of any recommendations provided herein. The information in this document is distributed AS IS and the use of this information or the implementation of any recommendations or techniques herein is a customers responsibility and depends on the customers ability to evaluate and integrate them into the customers operational environment. This document and the information

to [Set an SPN](#)(如何设置SPN)进行操作。

```
C:\>setspn -l svm1
Registered ServicePrincipalNames for CN=SVM1,CN=Computers,DC=domain,DC=local:
    HOST/svm1.domain.local
    HOST/SVM1
```

3. 对于 [ONTAP和Active Directory](#)，ONTAP与Active Directory域控制器之间的时间差不超过默认值5分钟 [2]。
4. 如果 [已在所有域控制器上禁用对Kerberos的RC4支持](#)，则 [为CIFS SVM的基于Kerberos的通信启用AES加密](#)。

追加信息

- [如何识别已建立CIFS会话的身份验证机制](#)
- [无法访问CIFS/SMB、因为如果 DNS别名/CCNAME 未配置为SPN、则身份验证将失败](#)
- Kerberos 是一种行业标准、不是NetApp专用标准
 - [Kerberos Microsoft Kerberos身份验证概述](#)
 - [Kerberos：网络身份验证协议](#)