ONTAP 是否支持完全正向保密 (PFS) ？

https://kb-cn-stage.netapp.com/on-prem/ontap/da/NAS/NAS-KBs/Does_ONTAP_support_Perfect_Forw…
Updated: Wed, 22 Apr 2026 07:28:57 GMT

适用于

ONTAP

解答

完全转发保密 (PFS) 是一种密钥交换方法，当与加密协议（如 TLS 1.2 ）结合使用时，它有助于防止攻击者解密客户端和服务器之间的所有网络会话。

注意：安全标准组织和实体强烈建议使用 TLS 1.2 或更高版本、仅使用支持 PFS 的加密套件。事实上，德国 IT 安全机构 (BSI) 为政府机构规定 TLS 1.2 以上（含 PFS ）。

PFS 要求在客户端和服务器之间的密钥交换部分中，在网络通信期间每个会话都使用唯一的密钥。这样做是为了防止已经解密单个网络会话的攻击者解密客户端和服务器之间的所有网络会话。

可以将 ONTAP 配置为仅使用遵循 PFS 的密钥交换原则的加密程序套件。配置 ONTAP 以利用这些加密程序套件时，您可以确保受到破坏的单个会话密钥不会直接导致客户端和服务器之间的所有网络会话受到破坏。

例如，假设攻击者利用 " 中间人攻击 " 记录了几个以前的网络会话、然后能够成功地破坏服务器的私用密钥。在这种情况下、如果使用了 PFS 加密套件、则所有以前记录的网络会话仍将受到保护、因为它们将使用不同的密钥。攻击者仍需要尝试对每个单个会话进行解密、然后才能访问以前会话的数据。

默认情况下， ONTAP 不要求仅使用支持 PFS 的密码。但是，可以将 ONTAP 集群配置为仅允许使用 PFS 的密钥交换。下面的过程介绍了配置此操作的步骤。

从高级权限级别使用命令 "Security Config Modify" 仅启用支持 PFS 的 DHE 和 ECDHE 密码。

注意：在更改 SSL 接口配置之前，请务必记住，客户端在连接到 ONTAP 时必须支持所提到的密码（ DHE 、 ECDHE ）。否则将不允许连接。

示例：

```
Cluster01::*> security config modify -interface SSL -supported-ciphers
PSK:DHE:ECDHE:!LOW:!aNULL:!EXP:!eNULL:!3DES:!kDH:!kECDH
```

注：务必将 PSK-AS 作为支持的加密算法包括在内、而不是将其删除。要使集群对等工作，需要从 ONTAP 9.5 (PSK) 开始。有关详细信息，请参见错误 1222233 。

其他信息

附加信息 _text