

知 某局点SSL VPN用户iNode无法登陆，web界面可以登陆

SSL VPN 方志伟 2019-11-25 发表

组网及说明

不涉及

问题描述

现场反馈，同一账户，使用同一台终端。通过iNode无法登陆，通过web可以正常登陆

过程分析

首先需要现场反馈iNode报错信息，报错信息如下



观察现场配置，发现现场是通过identity-member命令来加组的。现场的想法是通过加组，从而继承组中的授权属性（SSL VPN策略组）。

现场的配置

```
user-group H3C
```

```
authorization-attribute sslvpn-policy-group H3C
```

```
identity-member user H3C
```

收集用户iNode登陆时的debug发现有如下报错

```
*Nov 17 11:28:55:2019 F1030-NEW SSLVPNK/7/SSLVPN_DEBUG_KSSL_INFO: -COntext=1;
SSL_accept: SSLv3/TLS write server done.
```

```
*Nov 17 11:28:55:2019 F1030-NEW SSLVPNK/7/SSLVPN_DEBUG_KSSL_INFO: -COntext=1;
SSL_accept: error in SSLv3/TLS write server done.
```

解决方法

查看官网命令手册发现

Identity隶属于用户管理部分（缺省情况：用户未加入身份识别用户组）；**group才是加组**（缺省情况：本地用户属于用户组system）

遂让现场通过在本地用户下，通过group加组，经测试，用户通过iNode可以正常上线。

修正后的配置：

```
#
local-user H3C class network
  group H3C
#
```

出现web可登陆，iNode无法登陆，一般是因为未给用户授权属性（SSL VPN策略组） authorization-attribute sslvpn-policy-group H3C，或者是SSL VPN策略组中filter ip-tunnel所引用的acl（filter ip-tunnel acl xxxx）未放通对应IP。