

了解AAA Authentication Login Default Local Group TACACS+命令

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[验证](#)

[故障排除](#)

[相关信息](#)

简介

本文档介绍aaa authentication login default local group tacacs+命令在Cisco IOS®设备上的行为。

先决条件

要求

思科建议：

- 设备上启用了aaa new-model。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

注意：使用Cisco Tool Catalog中的[Cisco CLI Analyzer](#)可获取有关本节中使用的命令的详细信息。只有注册思科用户才能访问内部思科工具和信息。

在全局配置模式下在设备上配置以下命令：

```
aaa new-model
aaa authentication login default local group tacacs+
```

只要 aaa new model 配置后，本地身份验证将应用于所有线路和接口(控制台线路line con 0除外)。

在这里，AAA方法列表应用于设备的所有线路上的所有登录尝试，其中首先检查本地数据库，然后如果需要，尝试终端访问控制器访问控制系统(TACACS)服务器。

```
username cisco privilege 15 password 0 cisco
```

本地用户数据库：

```
tacacs-server host 10.20.220.141
```

```
tacacs-server key cisco
```

TACACS服务器现已配置。

验证

使用本部分可确认配置能否正常运行。

1. 在测试的设备上启用Debug TACACS和Debug AAA Authentication。

```
RUT#show debug
```

```
General OS:
```

```
  TACACS access control debugging is on
```

```
  AAA Authentication debugging is on
```

2. 在设备上执行telnet:

```
RUT#show ip interface brief | exclude unassigned
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/1	10.197.235.96	YES	DHCP	up	up
Loopback0	192.168.1.2	YES	manual	up	up

```
RUT#telnet 192.168.1.2
```

```
Trying 192.168.1.2 ... Open
```

```
User Access Verification
```

```
Username: cisco
```

```
*Jul 23 09:34:37.023: AAA/BIND(0000001E): Bind i/f
```

```
*Jul 23 09:34:37.023: AAA/AUTHEN/LOGIN (0000001E): Pick method list 'default'
```

```
Password:
```

```
RUT>
```

您注意到它没有尝试访问TACACS服务器，因为用户名cisco是在本地找到的。

现在，如果您尝试使用未在设备上本地配置的凭证：

```
RUT#telnet 192.168.1.2
```

```
Trying 192.168.1.2 ... Open
```

```
User Access Verification
```

```
Username:
```

```
*Jul 23 09:36:01.099: AAA/BIND(0000001F): Bind i/f
```

```
*Jul 23 09:36:01.099: AAA/AUTHEN/LOGIN (0000001F): Pick method list 'default'
```

```
Username: cisco1
```

```
*Jul 23 09:36:11.095: TPLUS: Queuing AAA Authentication request 31 for processing
```

```
*Jul 23 09:36:11.095: TPLUS: processing authentication start request id 31
*Jul 23 09:36:11.095: TPLUS: Authentication start packet created for 31(cisco1)
*Jul 23 09:36:11.095: TPLUS: Using server 10.20.220.141
*Jul 23 09:36:11.095: TPLUS(0000001F)/0/NB_WAIT/47A14C34: Started 5 sec timeout
*Jul 23 09:36:16.095: TPLUS(0000001F)/0/NB_WAIT/47A14C34: timed out
*Jul 23 09:36:16.095: TPLUS(0000001F)/0/NB_WAIT/47A14C34: timed out, clean up
*Jul 23 09:36:16.095: TPLUS(0000001F)/0/47A14C34: Processing the reply packet
% Authentication failed
```

您可以看到它尝试访问TACACS服务器10.20.220.141。这是预期的默认行为。TACACS服务器上未配置用户名cisco1，因此显示Authentication failed。

如果设备在配置中的默认组tacacs+ local中具有AAA身份验证日志，则其第一个首选项为TACACS。如果TACACS可访问，但用户未对其进行配置，则它不会回退并尝试在本地数据库中搜索。显示消息Authentication failed。

故障排除

当前没有故障排除此配置的特定可用资料。

相关信息

- [在接入服务器上配置基本AAA](#)
- [思科技术支持和下载](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。