使用 AAA 服务器管理网络访问服务器的 IP 池

目录
简介
开始使用前
规则
先决条件
使用的组件
IP 池
RADIUS NAS 配置
AAA 服务器 NAS 池配置文件
AAA 服务器用户配置文件
验证
TACACS+ NAS 配置
AAA 服务器 NAS 池配置文件
AAA 服务器用户配置文件
调试输出
相关信息

简介
本文为使用AAA服务器管理网络接入服务器(NAS)的IP池提供配置示例。

开始使用前
规则
有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

先决条件
本文档没有任何特定的前提条件。

使用的组件
本文档中的信息基于以下软件和硬件版本。

- Cisco IOS®软件版本12.0.7.T

本文档中的信息都是基于特定实验室环境中的设备创建的。本文档中使用的所有设备最初均采用原始(默认)配置。如果您是在真实网络上操作，请确保您在使用任何命令前已经了解其潜在影响。
IP 池

在IP控制协议(IPCP)地址协商中，如果IP池名为用户指定，NAS会核实指定池是否定义本地。如果是，就不会要求特殊操作，并且本地池被咨询IP地址。如果所需的池不存在，则获取它的授权呼叫被做，使用特殊用户名“pools-nas-name”“nas名称”是NAS的配置的主机名的地方。合情合理AAA服务器下载所需的池的配置。您能配置一个不同的池用户名用aaa configuration config-username name of your choosing命令。

此命令有更改使用下载从默认名称的池定义“pools-nas-name”到“name-of-your-choosing的用户名效果”。

普尔斯在非易失性存储器下载到Cisco NAS没有保留和自动地消失，每当接入服务器或路由器重新启动。下载池可能通过添加一个适当的AV对也使自动地暂停。下载池被标记作为动态在show ip local pools命令输出中。

RADIUS NAS 配置

aaa new-model
aaa authentication login default group radius
aaa authentication ppp default if-needed group radius
aaa authorization network default group radius
aaa configuration config-username nas1-pools
radius-server host 172.18.124.114 auth-port 1645 acct-port 1646
radius-server key cisco

AAA 服务器 NAS 池配置文件

./ViewProfile -p 9900 -u nas1-pools
User Profile Information
user = nas1-pools
profile_id=63
profile_cycle = 7
member = nas_profiles
password = pap "********"
radius=Cisco {
reply_attributes={
6=5
9,1="ip:pool-def#1= pool1 172.22.83.2 172.22.83.253"
}
}

此示例显示用户在CiscoSecure UNIX (CSU)服务器创建的“nas1-pools”。此条目指定a user-service-type出站用户{6=5}。NAS供应此属性防止普通的登录使用nas1-pools/cisco的著名的用户名和密码组合。

AAA 服务器用户配置文件

./ViewProfile -p 9900 -u pool_test
user = pool_test{
profile_id = 46
profile_cycle = 14
member = dial_rad
password = pap "********"
radius=Cisco {
reply_attributes={
7=1
用户“pool_test”拨和分配从pool1的一个IP地址在AAA服务器。
Received from id 10 172.18.124.114:1645, Access-Accept, len 58 00:26:06: Attribute 7 6 00000001 00:26:06: Attribute 6 6 00000002 00:26:06: Attribute 26 26 0000000901146970 00:26:06: RADIUS: saved authorization data for user 618FFB80 at 618FEE4E 00:26:06: AAA/AUTHEN (2962877775): status = PASS 00:26:06: As5 AAA/AUTHOR/LCP: Start IPCP 00:26:06: As5 AAA/AUTHOR/LCP (3264835197): Port="Async5" list='' service=NET 00:26:06: AAA/AUTHOR/LCP: As5 (3264835197) user="pool_test" 00:26:06: As5 AAA/AUTHOR/LCP (3264835197): send AV service=ppp 00:26:06: As5 AAA/AUTHOR/LCP (3264835197): send AV protocol-lcp 00:26:06: As5 AAA/AUTHOR/LCP (3264835197): found list "default" 00:26:06: As5 AAA/AUTHOR/LCP (3264835197): Method-radius (radius) 00:26:06: RADIUS: cisco AVPair "ip:addr-pool=pool1" not applied for lcp 00:26:06: As5 AAA/AUTHOR (3264835197): Post authorization status = PASS_REPL 00:26:06: As5 AAA/AUTHOR/LCP: We can start IPCP 00:26:06: As5 IPCP: O CONFREQ [Closed] id 1 len 10 00:26:06: As5 IPCP: Address 14.36.1.53 (0x03060E240135) 00:26:07: As5 CCP: I CONFREQ [Not negotiated] id 4 len 10 00:26:07: As5 CCP: O PROTREJ [Open] id 4 len 16 protocol CCP (0x80FD0104000A120600000001) 00:26:07: As5 IPCP: O CONFREQ [Not negotiated] id 4 len 10 00:26:07: As5 CCP: I CONFACK 00:26:07: As5 PrimaryDNS 0.0.0.0 (0x810600000000) 00:26:07: As5 AAA/AUTHOR/LCP: Authorization succeeded 00:26:07: As5 AAA/AUTHOR/LCP: Done. Her address pool=pool1 00:26:07: As5 AAA/AUTHOR/LCP: Processing AV addr=1.2.3.4 00:26:07: As5 AAA/AUTHOR/LCP: Processing AV service=ppp 00:26:07: As5 AAA/AUTHOR/LCP: Start. Her address 0.0.0.0, we want 1.2.3.4 00:26:07: As5 IPCP: I CONFREQ [ACKrcvd] id 7 len 10 00:26:07: As5 IPCP: SecondaryWINS 0.0.0.0 (0x840600000000) 00:26:07: As5 PrimaryDNS 0.0.0.0 (0x810600000000) 00:26:07: As5 SecondaryDNS 0.0.0.0 (0x830600000000) 00:26:07: As5 SecondaryDNS 0.0.0.0 (0x840600000000) 00:26:07: As5 AAA/AUTHOR/LCP: IP address returned 1.2.3.4 00:26:07: As5 AAA/AUTHOR/LCP: Processing AV addr-pool=pool1 00:26:07: As5 AAA/AUTHOR/LCP: AAA/AUTHOR/LCP: Pool returned 1.2.3.4 00:26:07: As5 AAA/AUTHOR/LCP: Processing AV service=ppp rem_addr='9194722001/9194724101' authen_type=NONE service=NONE priv=1 00:26:07: AAA/AUTHOR/LCP (3265270977): Method-radius (radius) 00:26:07: RADIUS: authenticating to get author data 00:26:07: RADIUS: ustruct (3562270977): found list "default" 00:26:07: As5 AAA/AUTHOR/LCP (3562270977): send AV protocol=ip 00:26:07: As5 AAA/AUTHOR/LCP (3562270977) user='pool_test' 00:26:07: As5 AAA/AUTHOR/LCP (3562270977): send AV service=ppp 00:26:07: As5 AAA/AUTHOR/LCP (3562270977): send AV protocol-lcp 00:26:07: As5 AAA/AUTHOR/LCP (3562270977): found list "default" 00:26:07: As5 AAA/AUTHOR/LCP (3562270977): Method-radius (radius) 00:26:07: RADIUS: cisco AVPair "ip:addr-pool=pool1" not applied for lcp 00:26:07: As5 AAA/AUTHOR (3264835197): Post authorization status = PASS_REPL 00:26:06: As5 AAA/AUTHOR/LCP: We can start IPCP 00:26:06: As5 IPCP: O CONFREQ [Closed] id 1 len 10 00:26:06: As5 IPCP: Address 14.36.1.53 (0x03060E240135) 00:26:07: As5 CCP: I CONFREQ [Not negotiated] id 4 len 10 00:26:07: As5 CCP: O PROTREJ [Open] id 4 len 16 protocol CCP (0x80FD0104000A120600000001) 00:26:07: As5 IPCP: O CONFREQ [Not negotiated] id 4 len 10 00:26:07: As5 CCP: I CONFACK 00:26:07: As5 PrimaryDNS 0.0.0.0 (0x810600000000) 00:26:07: As5 PrimaryDNS 0.0.0.0 (0x820600000000) 00:26:07: As5 SecondaryDNS 0.0.0.0 (0x830600000000) 00:26:07: As5 SecondaryDNS 0.0.0.0 (0x840600000000) 00:26:07: As5 AAA/AUTHOR/LCP: Start. Her address 0.0.0.0, we want 1.2.3.4 00:26:07: As5 IPCP: I CONFREQ [ACKrcvd] id 7 len 10 00:26:07: As5 IPCP: SecondaryWINS 0.0.0.0 (0x840600000000) 00:26:07: As5 PrimaryDNS 0.0.0.0 (0x810600000000) 00:26:07: As5 SecondaryDNS 0.0.0.0 (0x820600000000) 00:26:07: As5 SecondaryDNS 0.0.0.0 (0x830600000000) 00:26:07: As5 SecondaryDNS 0.0.0.0 (0x840600000000) 00:26:07: As5 AAA/AUTHOR/LCP: Authorization succeeded 00:26:07: As5 AAA/AUTHOR/LCP: Done. Her address 0.0.0.0, we want 1.2.3.4 00:26:07: As5 IPCP: O CONFNAK [ACKrcvd] id 6 len 10 00:26:07: As5 IPCP: Address 1.2.3.4 (0x030601020304) 00:26:07: As5 IPCP: I CONFREQ [ACKrcvd] id 7 len 10 00:26:07:
As5 IPCP: Address 1.2.3.4 (0x030601020304) 00:26:07: As5 AAA/AUTHOR/IPCP: Start. Her address 1.2.3.4, we want 1.2.3.4 00:26:07: As5 AAA/AUTHOR/IPCP: Request 1.2.3.4 from pool pool1 00:26:07: As5 AAA/AUTHOR/IPCP: Pool grants 1.2.3.4 00:26:07: As5 AAA/AUTHOR/IPCP: Processing AV service=ppp 00:26:07: As5 AAA/AUTHOR/IPCP: Processing AV addr-pool=pool1 00:26:07: As5 AAA/AUTHOR/IPCP: Processing AV addr=1.2.3.4 00:26:07: As5 AAA/AUTHOR/IPCP: Authorization succeeded 00:26:07: As5 AAA/AUTHOR/IPCP: Done. Her address 1.2.3.4, we want 1.2.3.4 00:26:07: As5 IPCP: O CONFACK [ACK/rcvd] id 7 len 10 00:26:07: As5 IPCP: Address 1.2.3.4 (0x030601020304) 00:26:07: As5 IPCP: State is Open 00:26:07: As5 IPCP: Install route to 1.2.3.4 00:26:07: %LINEPROTO-5-UPDOWN: Line protocol on Interface Async5, changed state to up as5300# show caller ip Line User IP Address Local Number Remote Number <-> As5 pool_test 1.2.3.4 9194724101 9194722001 as5300# show ip local pool Pool Begin End Free In use pool1 1.2.3.4 1.2.3.5 1 1 (dynamic)

**TACACS+ NAS 配置**

aaa new-model
aaa authentication login default group tacacs+
aaa authentication ppp default if-needed group tacacs+
aaa authorization network default group tacacs+
aaa configuration config-username nas1-pools
    tacacs-server host 172.18.124.114
    tacacs-server key cisco

**AAA 服务器 NAS 池配置文件**

```
./ViewProfile -p 9900 -u nas1-pools
User Profile Information
user = nas1-pools
    profile_id = 63
    profile_cycle = 8
    service=ppp {
        protocol=ip {
            set pool-def#1="pool1 1.2.3.4 1.2.3.5"
        }
    }
```

**AAA 服务器用户配置文件**

```
./ViewProfile -p 9900 -u pool_test
User Profile Information
user = pool_test{
    profile_id = 46
    profile_cycle = 15
    password = pap "********"
    service=ppp {
        protocol=lcp {
        }
        protocol=ip {
            set addr-pool=pool1
        }
    }
```

**调试输出**

```
Script started on Mon Dec 10 13:22:05 2001
ddu@rtp-cse-353% telnet 172.18.124.114
Trying 172.18.124.114...
Connected to 172.18.124.114.
Escape character is '^]'.
```
User Access Verification

Username: testuser
Password:

as5300>en
Password:

as5300#show debug
General OS: TACACS access control debugging is on AAA Authorization debugging is on PPP: PPP protocol negotiation debugging is on as5300#terminal monitor

as5300# telnet 14.36.1.53
Trying 14.36.1.53...
Connected to 14.36.1.53.
Escape character is '^]'.

User Access Verification

Username: testuser
Password:

as5300>en
Password:
as5300#
TAC+: Closing TCP/IP \(0x61B3BA9C\) connection to 172.18.124.114/49 00:06:32: AAA/AUTHEN (4053426223): status = PASS 00:06:32: TAC+: Closing TCP/IP \(0x61B3BA9C\) connection to 172.18.124.114/49 00:06:32: AAA/AUTH/LOGIN/PAP processed 00:06:32: TAC+::ver=193 id=4053426223 received AUTHEN status = PASS 00:06:32: AAA/AUTHEN (4053426223): status = PASS 00:06:32: TAC+: Closing TCP/IP \(0x61B3BA9C\) connection to 172.18.124.114/49 00:06:32: AAA/AUTH/LOGIN/PAP processed 00:06:32: TAC+: Closing TCP/IP \(0x61B3BA9C\) connection to 172.18.124.114/49 00:06:32: AAA/AUTH/LOGIN/PAP processed 00:06:32: TAC+: Closing TCP/IP \(0x61B3BA9C\) connection to 172.18.124.114/49 00:06:32: AAA/AUTH/LOGIN/PAP processed 00:06:32: TAC+: Closing TCP/IP \(0x61B3BA9C\) connection to 172.18.124.114/49 00:06:32: AAA/AUTH/LOGIN/PAP processed 00:06:32: TAC+: Closing TCP/IP \(0x61B3BA9C\) connection to 172.18.124.114/49 00:06:32: AAA/AUTH/LOGIN/PAP processed 00:06:32: TAC+: Closing TCP/IP \(0x61B3BA9C\) connection to 172.18.124.114/49 00:06:32: AAA/AUTH/LOGIN/PAP processed 00:06:32: TAC+: Closing TCP/IP \(0x61B3BA9C\) connection to 172.18.124.114/49 00:06:32: AAA/AUTH/LOGIN/PAP processed 00:06:32: TAC+: Closing TCP/IP \(0x61B3BA9C\) connection to 172.18.124.114/49 00:06:32: AAA/AUTH/LOGIN/PAP processed 00:06:32: TAC+: Closing TCP/IP \(0x61B3BA9C\) connection to 172.18.124.114/49 00:06:32: AAA/AUTH/LOGIN/PAP processed 00:06:32: TAC+: Closing TCP/IP \(0x61B3BA9C\) connection to 172.18.124.114/49 00:06:32: AAA/AUTH/LOGIN/PAP processed 00:06:32: TAC+: Closing TCP/IP \(0x61B3BA9C\) connection to 172.18.124.114/49 00:06:32: AAA/AUTH/LOGIN/PAP processed 00:06:32: TAC+: Closing TCP/IP \(0x61B3BA9C\) connection to 172.18.124.114/49 00:06:32: AAA/AUTH/LOGIN/PAP processed 00:06:32: TAC+: Closing TCP/IP \(0x61B3BA9C\) connection to 172.18.124.114/49 00:06:32: AAA/AUTH/LOGIN/PAP processed 00:06:32: TAC+: Closing TCP/IP \(0x61B3BA9C\) connection to 172.18.124.114/49 00:06:32: AAA/AUTH/LOGIN/PAP processed 00:06:32: TAC+: Closing TCP/IP \(0x61B3BA9C\) connection to 172.18.124.114/49 00:06:32: AAA/AUTH/LOGIN/PAP processed 00:06:32: TAC+: Closing TCP/IP \(0x61B3BA9C\) connection to 172.18.124.114/49 00:06:32: AAA/AUTH/LOGIN/PAP processed 00:06:32: TAC+: Closing TCP/IP \(0x61B3BA9C\) connection to 172.18.124.114/49 00:06:32: AAA/AUTH/LOGIN/PAP processed 00:06:32: TAC+: Closing TCP/IP \(0x61B3BA9C\) connection to 172.18.124.114/49 00:06:32: AAA/AUTH/LOGIN/PAP processed 00:06:32: TAC+: Closing TCP/IP \(0x61B3BA9C\) connection to 172.18.124.114/49 00:06:32: AAA/AUTH/LOGIN/PAP processed 00:06:32: TAC+: Closing TCP/IP \(0x61B3BA9C\) connection to 172.18.124.114/49 00:06:32: AAA/AUTH/LOGIN/PAP processed 00:06:32: TAC+: Closing TCP/IP \(0x61B3BA9C\) connection to 172.18.124.114/49 00:06:32: AAA/AUTH/LOGIN/PAP processed 00:06:32: TAC+: Closing TCP/IP \(0x61B3BA9C\) connection to 172.18.124.114/49 00:06:32: AAA/AUTH/LOGIN/PAP processed 00:06:32: TAC+: Closing TCP/IP \(0x61B3BA9C\) connection to 172.18.124.114/49 00:06:32: AAA/AUTH/LOGIN/PAP processed 00:06:32: TAC+: Closing TCP/IP \(0x61B3BA9C\) connection to 172.18.124.114/49 00:06:32: AAA/AUTH/LOGIN/PAP processed 00:06:32: TAC+: Closing TCP/IP \(0x61B3BA9C\) connection to 172.18.124.114/49 00:06:32: AAA/AUTH/LOGIN/PAP processed 00:06:32: TAC+: Closing TCP/IP \(0x61B3BA9C\) connection to 172.18.124.114/49 00:06:32: AAA/AUTH/LOGIN/PAP processed 00:06:32: TAC+: Closing TCP/IP \(0x61B3BA9C\) connection to 172.18.124.114/49 00:06:32: AAA/AUTH/LOGIN/PAP processed 00:06:32: TAC+: Closing TCP/IP \(0x61B3BA9C\) connection to 172.18.124.114/49 00:06:32: AAA/AUTH/LOGIN/PAP processed 00:06:32: TAC+: Closing TCP/IP \(0x61B3BA9C\) connection to 172.18.124.114/49 00:06:32: AAA/AUTH/LOGIN/PAP processed 00:06:32: TAC+: Closing TCP/IP \(0x61B3BA9C\) connection to 172.18.124.114/49 00:06:32: AAA/AUTH/LOGIN/PAP processed 00:06:32: TAC+: Closing TCP/IP \(0x61B3BA9C\) connection to 172.18.124.114/49 00:06:32: AAA/AUTH/LOGIN/PAP processed 00:06:32: TAC+: Closing TCP/IP \(0x61B3BA9C\) connection to 172.18.124.114/49 00:06:32: AAA/AUTH/LOGIN/PAP processed 00:06:32: TAC+: Closing TCP/IP \(0x61B3BA9C\) connection to 172.18.124.114/49 00:06:32: AAA/AUTH/LOGIN/PAP processed 00:06:32: TAC+: Closing TCP/IP \(0x61B3BA9C\) connection to 172.18.124.114/49 00:06:32: AAA/AUTH/LOGIN/PAP processed 00:06:32: TAC+: Closing TCP/IP \(0x61B3BA9C\) connection to 172.18.124.114/49 00:06:32: AAA/AUTH/LOGIN/PAP processed 00:06:32: TAC+: Closing TCP/IP \(0x61B3BA9C\) connection to 172.18.124.114/49 00:06:32: AAA/AUTH/LOGIN/PAP processed 00:06:32: TAC+: Closing TCP/IP \(0x61B3BA9C\) connection to 172.18.124.114/49 00:06:32: AAA/AUTH...
Cisco Secure UNIX 支持页面
RADIUS 支持页面
请求注解（RFC）
TACACS+ 支持页面
技术支持和文档 - Cisco Systems