Type text to search here...

Home > AAA TACACS+ and RADIUS Tutorial

AAA TACACS+ and RADIUS Tutorial

October 18th, 2018 Go to comments

AAA Configuration

The following steps are required to configure AAA:

1. Enable the "new model" of AAA.
2. Configure the server(s) to be used for AAA (e.g. TACACS+ or RADIUS servers).
3. Define authentication and authorization method lists.
4. Enforce AAA authentication on the relevant lines (e.g. console and VTY lines).

Example:

In this example we will do an **Authentication configuration** so that the users are authenticated when telnet to the device:

1. Globally enables AAA on a device:

```
Switch(config)#aaa new-model
```

2. We are going to configure the server to be used for AAA and the key; note that the key used is the same key that was configured on the RADIUS server.

```
Switch(config)#radius-server host 192.168.1.2 key MySecretP@ssword
```

In the above command we don't specify the ports used for RADIUS authentication and accounting so it will use the default values of 1645 and 1646, respectively (or we can specify them via the "radius-server host 192.168.1.2 **auth-port** 1645 **acct-port** 1646 key MySecretP@ssword" command). The full syntax of above command is:

Switch(config)# **radius-server host** { *hostname* | *ip-address* } [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [*alias* {hostname | ip address}]

3. We will activate authentication for logins to the device and specify that RADIUS is the preferred method but we should include the local user database as a fall back if RADIUS becomes unavailable. Note that users in the local database cannot be used if the user doesn't exist in RADIUS, it will only fall back if the RADIUS server is offline.

```
Switch(config)#aaa authentication login default group radius local
```

This command is broken down as follows:

+ The '**aaa authentication**' part is simply saying we want to configure authentication settings.
+ The '**login**' is stating that we want to prompt for a username/password when a connection is made to the device.
+ The '**default**' means we want to apply for all login connections (such as tty, vty, console and aux). If we

use this keyword, we don’t need to configure anything else under tty, vty and aux lines. If we don’t use this keyword then we have to specify which line(s) we want to apply the authentication feature. An example of not using the ‘default’ keyword is shown in step 4 below.
+ The ‘**group radius local**” means all users are authenticated using RADIUS servers (the first method). If the RADIUS servers don’t respond (unreachable), then the router’s local database is used (the second method). But notice that if the RADIUS server is **reachable** while the user has not configured on it, it will **not** fallback and try to search in the local database. It will display**% Authentication failed** message.

Note: If we don’t have the ‘local’ keyword (only ‘aaa authentication login default group radius’ command then the authentication will fail if the AAA server does not reply to the authentication request as there is no fallback authentication method)

For local authentication to work we need to create a local user. To create a new user, with password stored in plain text:

```
Switch(config)#username User1 password CCNA_cisco
```

But having passwords in plain text isn’t a good idea! The below command is better to create a new user, with password stored in encrypted text:

```
Switch(config)#username test2 secret Pa55w0rd
```

specify the RADIUS server and a group to be used.

4. In step 3, if we don’t use the ‘default’ login method list, for example:

```
Switch(config)#aaa authentication login MY_AUTHEN_GROUP group radius local
```

Then we have to configure the same group (MY_AUTHEN_GROUP in this case) to the specific line(s) with the “**login authentication** *list_name*” command. For example we want to apply to VTY lines (for telnet):

```
Switch(config)#line vty 0 4
Switch(config)# login authentication MY_AUTHEN_GROUP
```

Note:
+ We can configure different usernames/passwords on the local device and the remote AAA server but for normal users we should configure same usernames/passwords on both devices so that the transition (in case the remote AAA server fails) is transparent to them.
+ Use the **aaa authentication** global configuration command to define method lists for RADIUS authentication
+ Use the **aaa authorization** global command to authorize specific user functions
+ Use the **aaa accounting** command to enable accounting for RADIUS connections

So in conclusion this is all the config we need for a simple authentication using AAA:

```
Switch(config)#username test2 secret Pa55w0rd
Switch(config)#aaa new-model
Switch(config)#radius-server host 192.168.1.2 key MySecretP@ssword
Switch(config)#aaa authentication login MY_AUTHEN_GROUP group radius local
Switch(config)#line vty 0 4
Switch(config)# login authentication MY_AUTHEN_GROUP
```

A simple TACACS+ configuration for authentication would be:

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

```
tacacs-server host 10.10.10.1
tacacs-server key login@pass!
```

With this configured, when logging in, the password supplied will be attempted to be verified by the TACACS+ server before access is granted. If the server is unavailable/unreachable, then the switch will fall back to using the local authentication database.

In the next part we will see some examples of configuring AAA.

Pages: 1 2 3

Comments (4) Comments

Comment pages
« Previous 1 2 4228

1. Zoarexpro
   February 17th, 2020

   Glad to tell you PASSED my exam, 866 points, on 14th Feb 2020.
   lots of the questions from here but not entirely from here. there were many new technology infrastructure questions. Sims and drag and drop concepts are in here but still not exactly like what you see them in here. Exam time was sufficient. if you wisely use it, you can even be done before time. I had about 20 min answering my last questing.

2. Anonymous
   February 27th, 2020

   Hi Guys,

   Any advice for me as a beginner for this tutorial?
   what will be the first topic/s i need to study in order to understand the basic networking?

3. kevin
   July 14th, 2020

   Hello, In the book Official Cert Guide CCNA 200-301 there is no configuration for AAA TACACS+ and RADIUS, just a very brief introduction to them. Do you know if the configuration for AAA TACACS+ and RADIUS is still part of the exam?

4. miau
   March 5th, 2022

   miau?

Comment pages
« Previous 1 2 4228

Add a Comment

Name

Submit Comment

Subscribe to comments feed
Drag and Drop 4 CCNAv3 – New Questions

Premium Member Zone

Welcome Gurjeet singh!

- Welcome Premium Member
- CCNA – New Questions Part 5
- CCNA – New Questions Part 6
- CCNA – New Questions Part 7
- CCNA – New Questions Part 8
- CCNA – New Questions Part 9
- Composite Quizzes

- Logout

CCNA 200-301

- Basic Questions
- Topology Architecture Questions
- Cloud & Virtualization Questions
- CDP & LLDP Questions
- Switch Questions
- VLAN & Trunking Questions
- VLAN & Trunking Questions 2
- STP & VTP Questions
- EtherChannel Questions
- TCP & UDP Questions
- IP Address & Subnetting Questions
- IP Routing Questions
- IP Routing Questions 2
- OSPF Questions
- OSPF Questions 2
- EIGRP Questions
- NAT Questions
- NTP Questions
- Syslog Questions
- HSRP Questions
- Access-list Questions
- AAA Questions
- Security Questions
- Security Questions 2
- DAI Questions
- IPv6 Questions
- DNS Questions
- QoS Questions
- Port Security Questions
- Wireless Questions
- Wireless Questions 2
- SDN Questions
- DNA Center Questions
- Drag Drop Questions
- Drag Drop Questions 2
- Drag Drop Questions 3

- VPN Questions
- DHCP Questions
- Automation Questions
- Miscellaneous Questions
- CCNA FAQs & Tips
- Share your new CCNA Experience

CCNA Self-Study

- Practice CCNA GNS3 Labs
- CCNA Knowledge
- CCNA Lab Challenges
- Puppet Tutorial
- Chef Tutorial
- Ansible Tutorial
- JSON Tutorial
- Layer 2 Threats and Security Features
- AAA TACACS+ and RADIUS Tutorial
- STP Root Port Election Tutorial
- GRE Tunnel Tutorial
- Basic MPLS Tutorial
- TCP and UDP Tutorial
- Border Gateway Protocol BGP Tutorial
- Point to Point Protocol (PPP) Tutorial
- WAN Tutorial
- DHCP Tutorial
- Simple Network Management Protocol SNMP Tutorial
- Syslog Tutorial
- Gateway Load Balancing Protocol GLBP Tutorial
- EtherChannel Tutorial
- Hot Standby Router Protocol HSRP Tutorial
- InterVLAN Routing Tutorial
- Cisco Command Line Interface CLI
- Cisco Router Boot Sequence Tutorial
- OSI Model Tutorial
- Subnetting Tutorial – Subnetting Made Easy
- Frame Relay Tutorial
- Wireless Tutorial
- Virtual Local Area Network VLAN Tutorial
- VLAN Trunking Protocol VTP Tutorial
- IPv6 Tutorial
- Rapid Spanning Tree Protocol RSTP Tutorial
- Spanning Tree Protocol STP Tutorial
- Network Address Translation NAT Tutorial
- Access List Tutorial
- RIP Tutorial
- EIGRP Tutorial
- OSPF Tutorial

Network Resources

- Free Router Simulators
    - CCNA Website
    - ENCOR Website

- ENSDWI Website
- ENARSI Website
- DevNet Website
- CCIE R&S Website
- Security Website
- Wireless Website
- Design Website
- Data Center Website
- Service Provider Website
- Collaboration Website

Top